

Elektronische Gesundheitskarte und Telematikinfrastruktur

Systemspezifisches Konzept ePA

Version: 1.0.0
Revision: 72060
Stand: 18.12.2018
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemSysL_ePA

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	18.12.18		freigegeben	gematik

Inhaltsverzeichnis

1	Einführung.....	7
1.1	Zielsetzung.....	7
1.2	Dokumentenlandschaft	7
1.3	Zielgruppe	9
1.4	Geltungsbereich	9
1.5	Abgrenzung des Dokuments	9
1.6	Methodik.....	9
1.6.1	Anforderungen.....	9
1.6.2	Diagramme.....	9
1.6.3	Hinweis auf offene Punkte	10
2	Systemüberblick	11
2.1	Einführung	11
2.2	Übergeordnete Ziele	12
2.2.1	Sicherheit und Datenschutz	12
2.2.2	Berechtigungserhalt.....	12
2.2.3	Zugang zur Fachanwendung	13
2.2.4	Skalierung	13
2.2.5	Interoperabilität.....	13
2.2.6	Erweiterbarkeit interoperabler Dokumente.....	13
2.3	Zonenmodell	13
2.4	Akteure und Rollen.....	14
2.4.1	Fachliche Rollen	15
2.4.1.1	Nutzer.....	16
2.4.1.2	Versicherter	16
2.4.1.3	Vertreter	17
2.4.1.4	Leistungserbringer.....	17
2.4.1.5	Leistungserbringerinstitution	17
2.4.1.6	Anbieter.....	17
2.4.2	Technische Rollen	17
2.5	Funktionale Zerlegung	17
2.5.1	Konzept Dokumentenverwaltung	20
2.5.1.1	Funktionsweise.....	20
2.5.1.2	Realisierungskonzept	21
2.5.1.3	Metadaten	22
2.5.1.4	Formatspezifische Metadaten.....	22
2.5.2	Konzept Berechtigung	23
2.5.2.1	Funktionsweise.....	23
2.5.2.2	Realisierungskonzept	25
2.5.2.3	Geräteprüfung	26

2.5.2.4	Berechtigungserhalt.....	26
2.5.3	Konzept Lokalisierung	27
2.5.4	Konzept Protokollierung.....	27
2.5.5	Konzept Verschlüsselung	29
3	Anwendungsfälle	31
3.1	Übersicht der Anwendungsfälle	31
3.2	Übergreifende Vorbedingungen	32
3.3	Übergreifende Nachbedingungen.....	32
3.4	Nutzerzugang ePA.....	33
3.4.1	Login durch einen Versicherten	33
3.4.2	Login durch einen Leistungserbringer	36
3.4.3	Logout durch einen Nutzer.....	37
3.4.4	Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren	40
3.4.5	Eigene Stammdaten im Verzeichnisdienst durch einen Leistungserbringer verwalten	42
3.5	Aktenkontoverwaltung	43
3.5.1	Aktenkonto einrichten	43
3.5.2	Vertragsdaten ändern	49
3.5.3	Aktenkonto schließen	49
3.5.4	Anbieter wechseln	50
3.6	Berechtigungsverwaltung.....	53
3.6.1	Berechtigung durch einen Versicherten vergeben	53
3.6.2	Vertretung durch einen Versicherten einrichten	55
3.6.3	Neue eGK über alte eGK bekannt machen	57
3.6.4	Neue eGK über Vertreter bekannt machen	60
3.6.5	Berechtigungen durch einen Versicherten auflisten	61
3.6.6	Bestehende Berechtigungen durch einen Versicherten verwalten	63
3.6.7	Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern	66
3.6.8	Einlesen von sicher verwahrtm Schlüsselmaterial.....	68
3.7	Dokumentenverwaltung	70
3.7.1	Dokumente durch einen Leistungserbringer einstellen.....	70
3.7.2	Dokumente durch einen Versicherten einstellen	71
3.7.3	Dokumente durch einen Leistungserbringer suchen	73
3.7.4	Dokumente durch einen Versicherten suchen.....	75
3.7.5	Ändern einer Dokumentenklassifizierung durch einen Leistungserbringer	76
3.7.6	Dokumente durch einen Leistungserbringer löschen	78
3.7.7	Dokumente durch einen Versicherten löschen.....	80
3.7.8	Dokumente durch einen Leistungserbringer anzeigen	81
3.7.9	Dokumente durch einen Versicherten anzeigen.....	83
3.8	Benachrichtigungsverwaltung.....	84
3.8.1	Benachrichtigungen durch einen Leistungserbringer verwalten	84
3.8.2	Benachrichtigungen durch einen Versicherten verwalten.....	85
3.9	Protokollverwaltung	85
3.9.1	Protokolldaten durch einen Versicherten einsehen	85
3.9.2	Übertragungsprotokoll einsehen Leistungserbringer	86
4	Systemzerlegung (Deployment)	88

4.1	Produkttypen der Fachanwendung	88
4.1.1	Produkttyp Fachmodul ePA	89
4.1.2	Produkttyp ePA-Aktensystem	89
4.1.2.1	Komponente „Autorisierung“	90
4.1.2.2	Komponente „Dokumentenverwaltung“	91
4.1.2.3	Komponente „Zugangsgateway“	93
4.1.3	Produkttyp ePA-Frontend des Versicherten	94
4.1.4	Primärsystem.....	96
4.2	Schnittstellen der Fachanwendung ePA.....	97
4.2.1	Schnittstelle zwischen Primärsystem und Fachmodul ePA	98
4.2.1.1	Schnittstelle I_PHR_Management	98
4.2.1.2	Schnittstelle I_Authorization_Administration	100
4.2.1.3	Schnittstelle I_Account_Administration	101
4.2.2	Schnittstelle zwischen Fachmodul ePA und ePA-Aktensystem.....	102
4.2.2.1	Schnittstelle I_Authorization.....	103
4.2.2.2	Schnittstelle I_Authorization_Management.....	103
4.2.2.3	Schnittstelle I_Document_Management_Connect	105
4.2.2.4	Schnittstelle I_Account_Management.....	106
4.2.2.5	Schnittstelle I_Document_Management.....	107
4.2.3	Schnittstelle zwischen ePA-Aktensystem und ePA-Frontend des Versicherten	110
4.2.3.1	Schnittstelle I_Authentication_Insurant	110
4.2.3.2	Schnittstelle I_Authorization_Insurant.....	111
4.2.3.3	Schnittstelle I_Authorization_Management_Insurant	112
4.2.3.4	Schnittstelle I_Document_Management_Connect	115
4.2.3.5	Schnittstelle I_Account_Management_Insurant	115
4.2.3.6	Schnittstelle I_Document_Management_Insurant.....	116
4.2.4	Weitere Schnittstellen	119
5	Datenschutz- und Sicherheitsaspekte sowie vertrauenswürdige Umgebung.....	121
5.1	Spezielle Anforderungen an das Fachmodul ePA.....	122
5.2	Anforderungen an das ePA-Frontend des Versicherten.....	123
5.3	Anforderungen an das ePA-Aktensystem.....	123
5.3.1	Anforderungen an die Komponente Zugangsgateway	126
5.3.2	Anforderungen an die Komponente Autorisierung	126
5.3.3	Anforderungen an die Komponente Dokumentenverwaltung	127
5.4	Anforderungen an die vertrauenswürdige Ausführungsumgebung (VAU) 128	
5.4.1	Isolation	129
5.4.2	Wartung.....	129
5.4.3	Integrität der VAU	129
5.4.4	Vertrauenswürdigkeit aus Sicht des Nutzers.....	130
5.4.5	Skalierbarkeit.....	130
5.4.6	Anforderungen an die Komponente Dokumentenverwaltung	130
6	Informationsmodell	132
7	Anhang A – Verzeichnisse	135
7.1	Abkürzungen.....	135

7.2	Glossar	136
7.3	Abbildungsverzeichnis.....	140
7.4	Tabellenverzeichnis.....	141
7.5	Referenzierte Dokumente.....	143
7.5.1	Dokumente der gematik.....	143
7.5.2	A5.2. – Weitere Dokumente.....	144

1 Einführung

1.1 Zielsetzung

Das vorliegende Dokument beschreibt die systemspezifische Lösung der Fachanwendung ePA. Die Umsetzung der Funktionalität der Anwendung ePA wird in Stufen erfolgen. Dieses Dokument beschreibt die Lösung für die erste Stufe.

In diesem systemspezifischen Konzept werden insbesondere die Komponenten der Lösung von ePA sowie ihre Schnittstellen untereinander und mit der Telematikinfrastruktur-Plattform beschrieben. Dieses Dokument bildet somit die Grundlage für die Spezifikationen und Produkttypsteckbriefe der Komponenten der Fachanwendung ePA.

Das Dokument ist in unterschiedliche Abschnitte gegliedert, um die verschiedenen Aspekte der konzeptionellen Beschreibung der Fachanwendung abzudecken:

- Im Kapitel „Systemüberblick“ erfolgt eine inhaltliche Beschreibung der Fachanwendung, der verschiedenen Rollen und der Rahmenbedingungen für die Fachanwendung und deren Konzeption.
- Das Kapitel „Anwendungsfälle“ beschreibt alle Anwendungsfälle der Fachanwendung als „Außen-“ und „Innensicht“, um sowohl die Perspektive der Nutzer darzustellen, als auch die Abhängigkeiten und Verantwortlichkeiten der einzelnen Produkttypen in einem Anwendungsfall festzulegen.
- Im Kapitel „Systemzerlegung“ erfolgt der Systemschnitt in die einzelnen Produkttypen und Komponenten der Fachanwendung und es werden die Schnittstellen mit ihren Operationen und deren Signaturen auf Ebene der Konzeption festgelegt. Die ausgewiesenen Parameter der Operationen beschränken sich dabei auf ein für die Konzeption notwendiges Maß.
- Im Kapitel „Datenschutz- und Sicherheitsaspekte sowie vertrauenswürdige Umgebung“ werden die speziellen Aspekte des Datenschutzes und der Informationssicherheit der Fachanwendung behandelt und der Rahmen für die „vertrauenswürdige Ausführungsumgebung (VAU)“ gesetzt.
- Das Kapitel „Informationsmodell“ stellt die Semantik der verwendeten Datentypen und deren Verhältnis zueinander dar.

1.2 Dokumentenlandschaft

Die Abbildung Dokumentenlandkarte ePA zeigt schematisch die Dokumentenlandschaft, in welche sich das systemspezifische Konzept ePA und alle weiteren Dokumente, die die Fachanwendung beschreiben, eingliedern. Parallel dazu sind die Dokumente der TI-Plattform aufgeführt, die im Rahmen des Projektes ePA angepasst werden müssen.

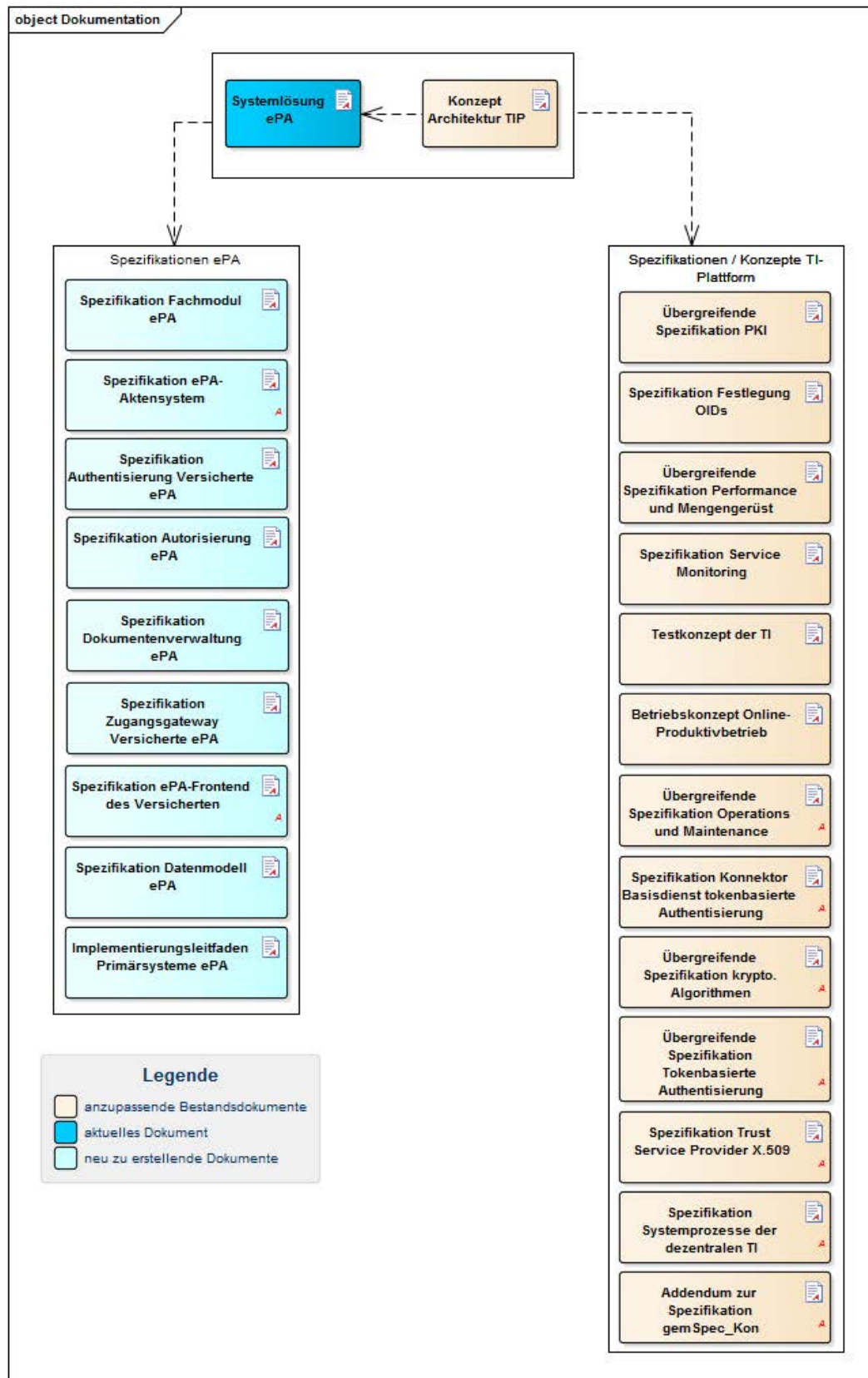


Abbildung 1 : Dokumentenlandschaft ePA

1.3 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter der Produkttypen der Fachanwendung ePA.

1.4 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.

Wichtiger Schutzrechts-/Patentrechtshinweis

Das nachfolgende Konzept ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass das Konzept 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.

1.5 Abgrenzung des Dokuments

Nicht Bestandteil des vorliegenden Dokumentes bzw. der vorliegenden Version sind die Festlegungen zu Folgestufen der Fachanwendung ePA.

1.6 Methodik

1.6.1 Anforderungen

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 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.

1.6.2 Diagramme

Die Darstellung der Facharchitektur erfolgt prinzipiell auf der Grundlage einer durchgängigen UML-Modellierung unter Nutzung der folgenden Diagrammtypen:

- Komponentendiagramme (CMP) zur Darstellung der beteiligten Komponenten und ihrer Schnittstellen
- Verteilungsdiagramme zur Darstellung der Verteilung von Komponenten auf Systeme
- Use-Case-Diagramme (UC) zur Darstellung der Beziehungen der Anwendungsfälle zueinander
- Sequenzdiagramme (SD) zur Abbildung von Reihenfolgen und Abläufen zwischen den Komponenten innerhalb eines Anwendungsfalls. Die Sequenzdiagramme werden durch Tabellen ergänzt, die die funktionalen Ergänzungen des Anwendungsfalls beinhalten.
- Klassendiagramm zur Abbildung des Informationsmodells

1.6.3 Hinweis auf offene Punkte

Themen, die noch intern geklärt werden müssen oder eine Entscheidung seitens der Gesellschafter erfordern, sind wie folgt im Dokument gekennzeichnet:

Beispiel für einen offenen Punkt.

2 Systemüberblick

2.1 Einführung

Die Fachanwendung ePA ermöglicht die wechselseitige Bereitstellung von Dokumenten für Leistungserbringer und gesetzlich Versicherte auf Basis einer Dokumentenverwaltung. Aufgrund der Vernetzung der Versicherten mit der Telematikinfrastruktur (TI) über ein Dokumentenmanagementsystem entstehen neue Schnittstellen zwischen verteilten, heterogenen Systemumgebungen und Technologien. Dabei muss die Syntax dieser technischen Schnittstellen zwischen den beteiligten Komponenten interoperabel gestaltet werden. Die Anforderungen an Datenschutz und Datensicherheit begegnen dem Anspruch einer potentiell lebenslangen Akte, die die medizinische Dokumentation eines Versicherten sammelt.

Die Fachanwendung ePA setzt sich aus den in Abbildung 2: Übersicht der Fachanwendung ePA dargestellten Bestandteilen zusammen.

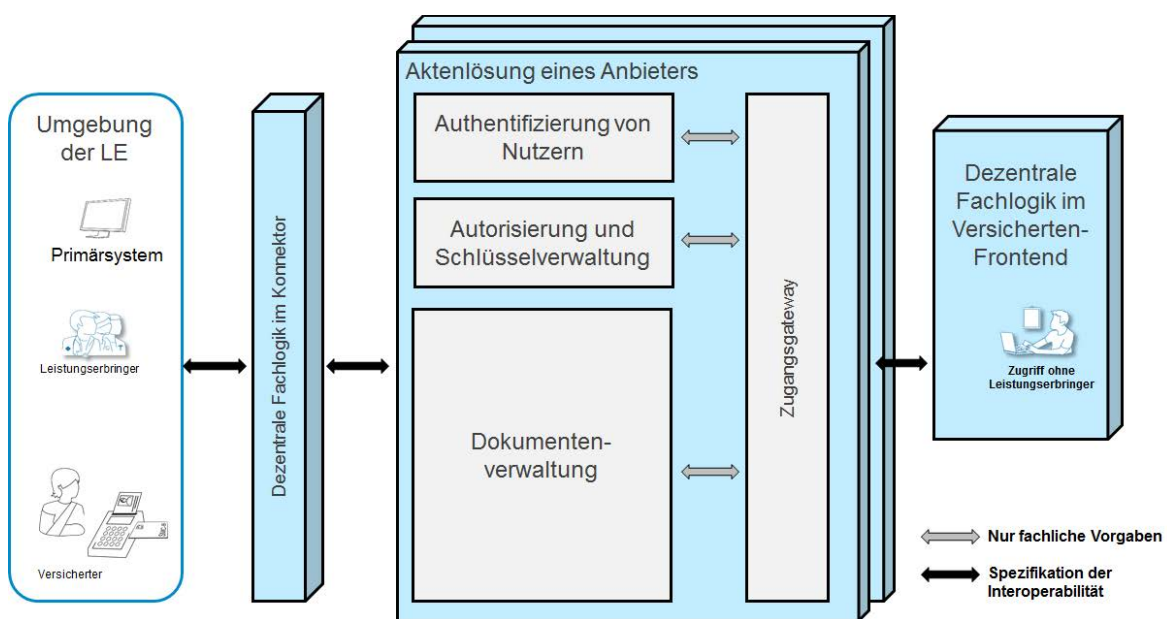


Abbildung 2: Übersicht der Fachanwendung ePA

In der Umgebung der Leistungserbringer wird die Fachanwendung über die Primärsysteme der Leistungserbringer genutzt. Der Versicherte hingegen nutzt die Anwendung in seiner Umgebung über ein Frontend mit grafischem Benutzerinterface.

Die dezentrale Fachlogik ePA im Konnektor bietet dem Primärsystem des Leistungserbringers eine Schnittstelle für die Verwaltung der Dokumente eines Versicherten an.

Die dezentrale ePA-Fachlogik in der Umgebung des Versicherten ermöglicht dem Versicherten den Zugriff auf seine Daten über ein Zugangsgateway zum ePA-Aktensystem eines Anbieters.

Das ePA-Aktensystem eines Anbieters setzt sich aus den logischen Bestandteilen Authentifizierung von Nutzern, Autorisierung und Schlüsselverwaltung, Dokumentenverwaltung und dem Zugangsgateway zusammen (siehe auch Abbildung 2). Die Umsetzung der Produkttypen Fachmodul ePA, ePA-Frontend des Versicherten und ePA-Aktensystem wird durch die jeweiligen Hersteller verantwortet.

In der TI kann es mehrere Anbieter für ePA-Frontends und ePA-Aktensysteme geben; ein Versicherter hat dabei immer nur ein aktives Aktenkonto eine elektronische Patientenakte bei einem Anbieter seiner Wahl.

Die ePA-Aktensysteme stellen sicher, dass nur authentifizierte und autorisierte Nutzer mit dem System interagieren. Die Authentifizierung von Nutzern erfolgt auf Basis der Karten der TI. Die Vergabe von Zugriffsberechtigungen für Leistungserbringer erfolgt durch den Versicherten oder einen berechtigten Vertreter.

2.2 Übergeordnete Ziele

2.2.1 Sicherheit und Datenschutz

Die Fachanwendung ePA stellt sicher, dass die Daten der Fachanwendung ePA beim Anbieter beteiligter Komponenten nicht für Zwecke der Profilbildung und Auswertung verarbeitet werden, da nur Personen, die in § 291a Abs. 4 Satz 1 Nr. 2 und Satz 2 SGB V genannt sind, auf medizinische personenbezogene Daten von ePA zugreifen dürfen. Die Fachanwendung ePA stellt ferner sicher, dass die Sicherheit der TI durch die Nutzung der Fachanwendung ePA nicht beeinträchtigt wird. Die Zugriffsbedingungen des § 291a Abs. 5 SGB V (Zwei-Schlüssel-Prinzip) werden umgesetzt.

Die Fachanwendung verarbeitet Metadaten über Dokumente des Versicherten in der Dokumentenverwaltung im Klartext in einer vertrauenswürdigen Verarbeitungsumgebung (VAU). Dies ermöglicht die fachdienstseitige Durchsetzung von Zugriffsregeln für Berechtigte auf ePA-Dokumente des Versicherten und erleichtert die Suchfunktion für Dokumente. Zusätzlich muss eine sicherheitstechnische Validierung im Sinne einer starken Eingabevalidierung sowie eine Schemavalidierung der Metadaten zur Sicherstellung der Interoperabilität durchgeführt werden.

2.2.2 Berechtigungserhalt

Die Fachanwendung ePA stellt den Berechtigungserhalt bei Wechsel oder Verlust einer Karte eines Nutzers (SMC-B oder eGK) sicher, indem die für eine Karte verschlüsselte Berechtigung über verschiedene Anwendungsfälle auf eine neue Karte umgeschlüsselt werden kann. Die kartenübergreifende Identifikation anhand eindeutiger Merkmale (z.B. Krankenversicherungsnummer (KVNR)) stellt sicher, dass die Umschlüsselung nur für den Berechtigten erfolgt. Auf der eGK gespeicherte Daten, die in ePA gesichert wurden, können im Fall des Kartenwechsels durch einen Leistungserbringer wieder auf die eGK geschrieben werden.

Der Berechtigungserhalt stellt somit sicher, dass der Versicherte weiterhin auf seine Daten zugreifen kann. Dem Versicherten stehen die folgenden Anwendungsfälle zur Verfügung, die für seine eGK verschlüsselten Berechtigungen zu erhalten:

- UC 3.3 - Neue eGK über alte eGK bekannt machen
- UC 3.4 - Neue eGK über Vertreter bekannt machen
- UC 3.8 - Umschlüsselung mit sicher verwahrtem Schlüsselmaterial

2.2.3 Zugang zur Fachanwendung

Die Fachanwendung ePA stellt keine Sicherheitsanforderungen an die Umgebung des Versicherten. Sie schafft einen Zugang zur Telematikinfrastuktur für Versicherte, der gleichzeitig das Sicherheitsniveau der TI wahrt. Der Zugang für Leistungserbringer erfolgt mittels Konnektor. Dabei stellt die Fachanwendung ePA sicher, dass die fachlichen Anwendungsfälle mit der vorhandenen Konnektor-Hardware des Online-Produktivbetriebs (Stufe 1) umgesetzt werden können.

2.2.4 Skalierung

Die Fachanwendung ePA stellt sicher, dass die Lösung über die Anzahl der Nutzer (gesetzlich Versicherte, Leistungserbringerinstitutionen), über die Anzahl der verwalteten Dokumente innerhalb eines Aktenkontos und über die Anzahl der angebotenen ePA-Aktensysteme verschiedener Anbieter skaliert.

2.2.5 Interoperabilität

Die Fachanwendung ePA stellt zum einen über das Fachmodul des Konnektors die Interoperabilität jedes ePA-Aktensystems zum Konnektor sicher. Zum anderen ermöglicht sie die Interoperabilität zwischen den Primärsystemen und dem Fachmodul des Konnektors sowie zwischen den ePA-Frontends der Versicherten und den angebotenen ePA-Aktensystemen.

Die Metadaten der über die Fachanwendung transportierten Inhalte jedes ePA-Aktensystems werden interoperabel gestaltet. Die widerspruchsfreie Semantik der transportierten Informationen innerhalb der verschlüsselten Dokumente wird dabei aber nicht sichergestellt.

2.2.6 Erweiterbarkeit interoperabler Dokumente

Die Lösung ePA stellt sicher, dass die Anwendung funktional erweiterbar ist. Neue Dokumentenformate sollen konfigurativ auch nach dem Rollout eingebracht werden können.

Dokumentenformate stellen definierte Inhalte von Dokumenten in Verbindung mit definierten Dateitypen dar. Ein Beispiel ist der Notfalldatensatz (Inhalt) im XML-Format (Dateityp). Alle weiteren ePA-Dokumente definieren sich lediglich durch die erlaubten Dateitypen.

2.3 Zonenmodell

ePA ist eine Fachanwendung der Telematikinfrastuktur. Ein Merkmal dieser Fachanwendung ist die Anbindung der Umgebung des Versicherten. Die Fachanwendung ePA erweitert das Zonenmodell des Architekturkonzepts der TI-Plattform [gemKPT_Arch_TIP] um die Personal Zone, in der der Versicherte seine Geräte betreibt. Diese Zone steht

unter der Kontrolle des Versicherten und der Versicherte nutzt seine Geräte und seine eGK in seiner persönlichen Verantwortung. Die Nutzung dieser Geräte erfolgt via ePA-Frontend des Versicherten. Die Personal Zone hat dabei keinen direkten Zugriff auf die zentrale Zone der TI.

2.4 Akteure und Rollen

Im folgenden Abschnitt werden die an ePA beteiligten Akteure/Rollen betrachtet. Ein Akteur ist eine Person oder ein technisches System, die/das mit der Fachanwendung ePA interagiert. Diese Interaktion wird durch einen Anwendungsfall ausgelöst.

Akteure innerhalb der Fachanwendung ePA sind jedoch keine konkreten beteiligten Personen oder Systeme, sondern Rollen, die jene im Rahmen des Anwendungsfalles einnehmen. Insofern kann eine Person oder ein technisches System in mehreren Rollen mit dem ePA-System interagieren. Im weiteren Abschnitt werden die im ePA-Kontext beteiligten fachlichen und technischen Rollen beschrieben.

Die folgende Tabelle listet die in ePA verwendeten kryptografischen Identitäten auf und ordnet sie den verschiedenen Akteuren mit ihrer jeweiligen Rolle zu.

Tabelle 1: Kryptografische Identitäten der Akteure und ihre jeweilige Rolle

Komponente	Identität	Verwendungszweck	Prüfende Komponente
SMC-B	ID.HCI.OSIG	Signatur des Authentisierungstokens der authentisierenden SMC-B	Autorisierung, Dokumentenverwaltung
	ID.HCI.ENC	Entschlüsselung der Ende-zu-Ende gesicherten kryptografischen Berechtigung	Fachmodul, Frontend des Versicherten
eGK	ID.CH.AUT	Anmeldung am ePA-Aktensystem	Authentisierung Versicherter
	ID.CH.ENC	Entschlüsselung der Ende-zu-Ende gesicherten kryptografischen Berechtigung	Fachmodul, Frontend des Versicherten
Aktensystem	ID.FD.TLSC	TLS-Cientauthentisierung des ePA-Aktensystems bei Abruf Exportpaket für Aktenumzug	bereitstellendes Aktensystem
	ID.FD.TLSS	TLS-Serverauthentisierung	abrufendes Aktensystem

		rung des ePA-Aktensystems bei Abruf Exportpaket für Aktenumzug	
Authentisierung Versicherter	ID.FD.TLS-S	TLS-Serverauthentisierung der Komponente innerhalb der TI	Fachmodul
	ID.FD.SIG	Signatur des Authentisierungstoken für Versicherte	Authentisierung Versicherter, Autorisierung, Dokumentenverwaltung
Autorisierung	ID.FD.TLS-S	TLS-Serverauthentisierung der Komponente innerhalb der TI	Fachmodul
	ID.FD.SIG	Signatur des Autorisierungstokens	Dokumentenverwaltung, VAU
Dokumentenverwaltung	ID.FD.TLS-S	TLS-Serverauthentisierung der Komponente innerhalb der TI	Fachmodul
VAU	ID.FD.AUT	Authentisierung der vertrauenswürdigen Ausführungsumgebung auf dem sicheren Kommunikationskanal	Fachmodul, Frontend des Versicherten
Zugangsgateway	Internet PKI	TLS-Serverauthentisierung im Internet	Frontend des Versicherten

2.4.1 Fachliche Rollen

Für eine bessere Übersicht sind in Abbildung 3 die im ePA-Kontext beteiligten Rollen in einem UML-Klassendiagramm dargestellt, die über kryptografische Identitäten als Nutzer mit der Fachanwendung interagieren. Die Rollen werden im Weiteren kurz beschrieben.

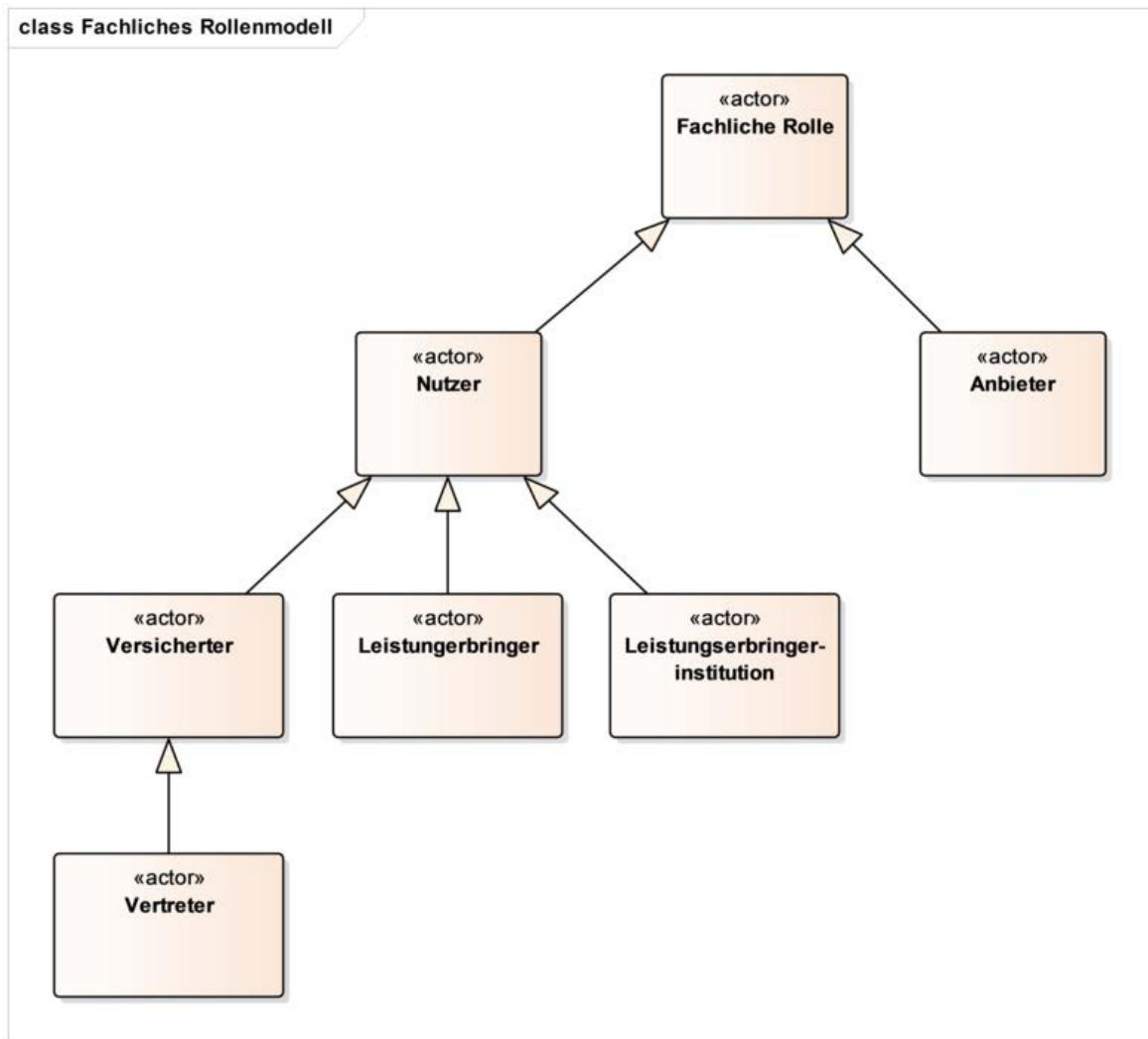


Abbildung 3: Fachliches Rollenmodell

2.4.1.1 Nutzer

Nutzer der ePA sind Personen, die mit der Fachanwendung fachlich agieren. Versicherte, Vertreter, Leistungserbringer und Leistungserbringerinstitutionen können im ePA-Kontext die Rolle eines Nutzers einnehmen.

2.4.1.2 Versicherter

Im ePA-Kontext ist ein Versicherter eine Person, die in einem Versichertenverhältnis mit einer gesetzlichen Krankenversicherung steht. Der Versicherte wird in diesem Zusammenhang durch seine eGK repräsentiert. Die eindeutige Identifikation des Versicherten im ePA-Kontext erfolgt über seine KVNR. Für die Anwendungen nach § 291a SGB V kann die KVNR verwendet werden.

Die medizinischen Daten des Versicherten werden in einer mit seinem ePA-Aktenkonto verknüpften Patientenakte bereitgestellt. Nur der Versicherte besitzt die Hoheit über die gespeicherten Daten. Der Versicherte kann andere Nutzer berechtigen, auf seine Patientenakte zuzugreifen (s. „Vertreter“).

2.4.1.3 Vertreter

Ein Vertreter ist ebenfalls eine Person, die in einem Versichertenverhältnis mit einer gesetzlichen Krankenversicherung steht. Auch ein Vertreter muss über eine eigene eGK verfügen. Um allerdings die Vertreter-Rolle einzunehmen, muss ein anderer gesetzlich Versicherter diese Person erst als Vertreter berechtigen.

Ein Vertreter hat zwar alle Rechte im Zusammenhang mit der Dokumenten- und Berechtigungsverwaltung in einem ePA-Aktenkonto, er kann aber selbst keinen weiteren Vertreter für den Vertretenen berechtigen.

2.4.1.4 Leistungserbringer

Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 291a Abs. 4 Satz 1 Nr. 2 SGB V und wird im ePA-Kontext über einen HBA repräsentiert. Er wird vom Versicherten für den Zugriff auf die Patientenakte explizit berechtigt.

Hinweis: In der aktuellen Ausbaustufe wird dies durch die Berechtigung der Leistungserbringerinstitution umgesetzt.

2.4.1.5 Leistungserbringerinstitution

Eine Leistungserbringerinstitution (LEI) ist eine organisatorische Einheit oder juristische Person zusammengefasster Leistungserbringer (z. B. Arztpraxen, Apotheken, Krankenhäuser) sowie deren berufsmäßige Gehilfen und wird im ePA-Kontext durch eine oder mehrere SMC-Bs repräsentiert. Ein Versicherter kann eine Leistungserbringerinstitution nur als Ganzes berechtigen.

2.4.1.6 Anbieter

Der Anbieter ePA-Aktensystem ist ein Dienstleister, der die Patientenakte für Versicherte bereitstellt. Der Anbieter hat auch die Betriebsverantwortung über das ePA-Aktensystem. Der Anbieter ePA-Aktensystem ist nicht zugriffsberechtigt auf die medizinischen Daten des Versicherten.

2.4.2 Technische Rollen

Neben den fachlichen Rollen existieren technische Rollen. Diese technischen Rollen kommen zum Tragen, wenn nicht eine Person mit dem System interagiert, sondern eine technische Komponente, ein Produkttyp der Fachanwendung ePA oder das Primärsystem der Leistungserbringerumgebung. Die entsprechenden Produkttypen und Komponenten der Fachanwendung werden im Kapitel „Systemzerlegung“ dargestellt.

2.5 Funktionale Zerlegung

Der Kern der Fachanwendung ePA besteht in der Bereitstellung von Daten durch Versicherte und Leistungserbringerinstitutionen. Diese Daten werden in einer Dokumentenverwaltung organisiert. Um diese Dokumentenverwaltung werden Funktionsblöcke herum gruppiert, um dem Versicherten und den Leistungserbringerinstitutionen Zugang zu dieser Dokumentenverwaltung zu ermöglichen. Der Zugriff der jeweiligen Nutzer muss autorisiert sein, d.h. es muss eine Berechtigung zum Zugriff vorliegen. Um eine

Berechtigung prüfen zu können, muss ein Nutzer als ein bekannter Nutzer authentifiziert worden sein.

Die drei wesentlichen Funktionsblöcke sind demnach die Authentifizierung von Nutzern, die Prüfung auf Autorisierung eines Zugriffs und die Verwaltung der Daten eines Versicherten in einer Dokumentenverwaltung.

Das folgende Bild zeigt eine detaillierte Zerlegung der Funktionen der Fachanwendung in Funktionsblöcke sowie die logischen, funktionalen Schnittstellen zwischen diesen. Diese funktionale Zerlegung dient der Verdeutlichung der funktionalen Zusammenhänge der Fachanwendung. Normativ für den Schnitt von Produkttypen und Komponenten ist die Systemzerlegung in Kapitel 4.1.

Hinweis: es empfiehlt sich der Ausdruck der Abbildung im A3-Format.

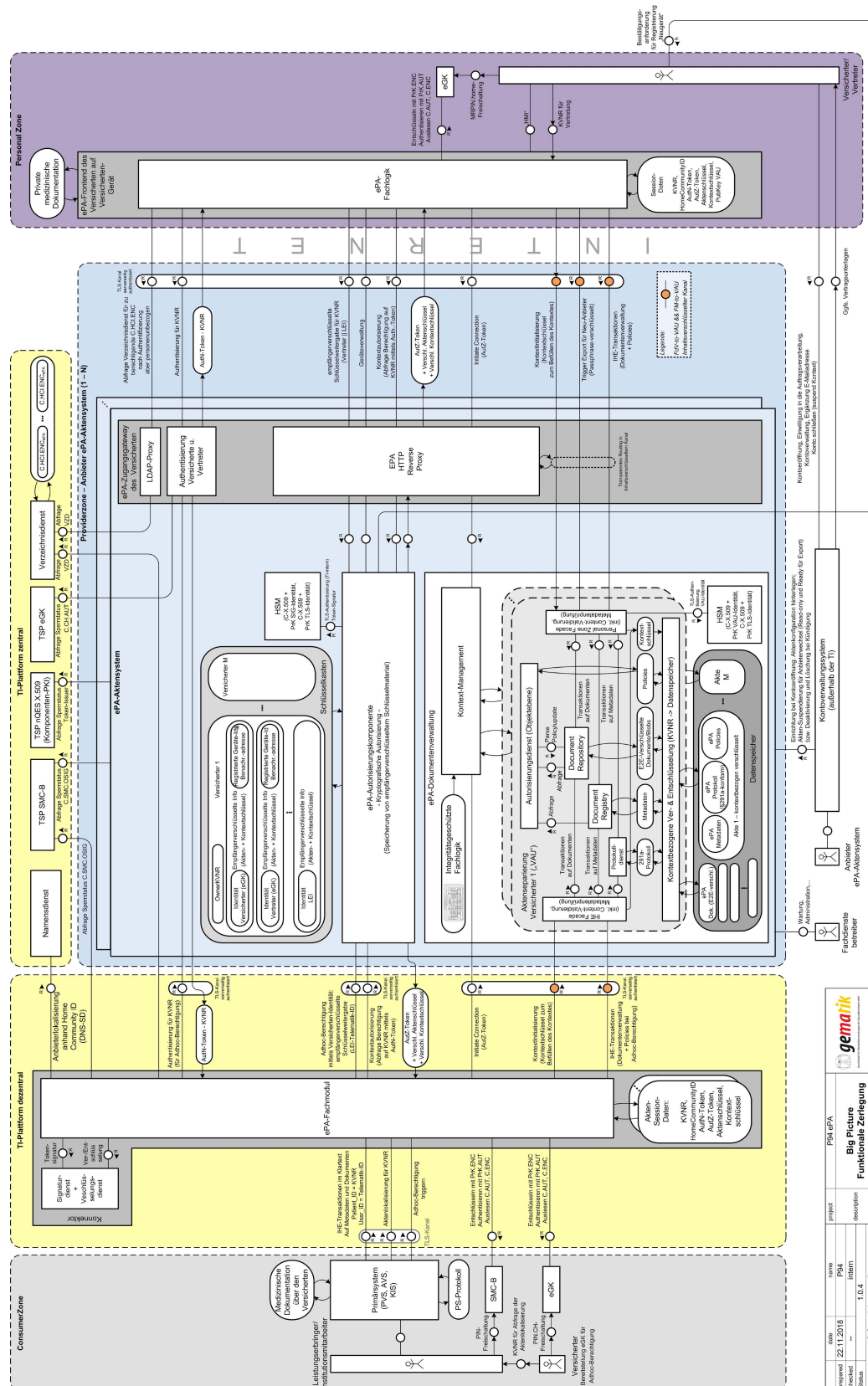


Abbildung 4: Funktionale Zerlegung

Im Zentrum der Anwendung steht das ePA-Aktensystem. Dieses wird zerlegt in die Komponenten zur Authentisierung für Versicherte (im Zugangsgateway), zur Autorisierung und die Dokumentenverwaltung. Das Primärsystem des Leistungserbringers und das ePA-Frontend des Versicherten bilden die Schnittstellen zum Benutzer mittels grafischer Oberflächen. In der Umgebung der Leistungserbringer realisiert das Fachmodul des Konnektors die dezentrale Fachlogik, die auf Seiten des Versicherten im ePA-Frontend des Versicherten umgesetzt wird. Die dezentrale Fachlogik steuert die Aufrufe an die verschiedenen Komponenten des ePA-Aktensystems in den Anwendungsfällen, realisiert die Ver- und Entschlüsselung von Dokumenten und kapselt das Sessionhandling.

Aktenzugriffe funktionieren aus der Umgebung der Leistungserbringer und der Versicherten immer nach dem gleichen, folgenden Schema:

1. Ein Nutzer muss sich mit seiner Karte authentisieren. Die Leistungserbringer und Versicherte in der Leistungserbringerumgebung authentifizierende Komponente ist das Fachmodul. Versicherte außerhalb der Leistungserbringerumgebung werden durch das Zugangsgateway authentifiziert. Für eine erfolgreiche Authentifizierung erhält er eine Authentifizierungsbestätigung.
2. Mit einer gültigen Authentifizierungsbestätigung authentisiert sich der Nutzer gegenüber der Komponente Autorisierung. Anhand der bestätigten Merkmale des Nutzers (Telematik-ID der LEI, oder KVNR des Versicherten) in der Authentifizierungsbestätigung kann die Komponente Autorisierung die kryptografische Berechtigung des Nutzers prüfen. Liegt für diesen authentifizierten Nutzer verschlüsseltes kryptografisches Schlüsselmaterial vor, wird ihm dieses ausgehändigt. Ist in dieser Berechtigung zusätzlich die Erlaubnis zum Zugriff auf Daten des Versicherten hinterlegt, stellt die Komponente Autorisierung für diesen Nutzer eine Autorisierungsbestätigung aus.
3. Mit einer gültigen Autorisierungsbestätigung authentisiert sich der Nutzer gegenüber der Komponente Dokumentenverwaltung. Anhand der bestätigten Merkmale des Nutzers (RecordIdentifier, Telematik-ID der LEI, KVNR des Versicherten) in der Autorisierungsbestätigung kann die Komponente Dokumentenverwaltung die Berechtigung des Nutzers für den Zugriff auf Daten des Versicherten in den hinterlegten Zugriffsregeln prüfen. Liegt für diesen autorisierten Nutzer eine Zugriffsregel vor, die den gewünschten Zugriff auf Daten gestattet (Lesen, Schreiben, Löschen von Dokumenten), wird die Operation entsprechend ausgeführt.

Das Ausstellen von Authentifizierungs- und Autorisierungsbestätigungen erfolgt im Rahmen des Anwendungsfalls „Login“. Diese können im Rahmen der internen Session-Verwaltung der Fachanwendung für die Dauer ihrer Gültigkeit und bis zu einem möglichen Logout wiederverwendet werden.

2.5.1 Konzept Dokumentenverwaltung

Die Dokumentenverwaltung setzt den Kern der Fachanwendung ePA um. Sie speichert und organisiert den Zugriff auf *„Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation“* sowie die *„durch von Versicherten selbst oder für sie zur Verfügung gestellte Daten“* gemäß § 291a SGB V Abs. 3.

2.5.1.1 Funktionsweise

Die Dokumente werden vom Versicherten als Eigentümer der Daten sowie von berechtigten Leistungserbringern und Vertretern über folgende Anwendungsfälle verwaltet:

- Dokumente durch einen Leistungserbringer einstellen, suchen, anzeigen/herunterladen, löschen
- Dokumente durch einen Versicherten einstellen, suchen, anzeigen/herunterladen, löschen
- Ändern einer Dokumentklassifizierung durch einen Leistungserbringer
- Hinzufügen einer Dokumentklassifizierung durch den Versicherten.

Leistungserbringer und Versicherte führen diese Anwendungsfälle über ihr jeweiliges Frontend (Primärsystem des Leistungserbringers bzw. ePA-Frontend des Versicherten) aus, das einen Datenspeicher zur Auswahl einzustellender und Ablage herunterzuladen der Dokumente einbindet. Das aus dem Klinikumfeld bekannte IT Infrastructure Technical Framework von IHE (Integrating the Healthcare Enterprise) wird als Stand der Technik angenommen. Auf Basis der von IHE definierten Transaktionen des XDS.b-Integrationsprofils werden die oben genannten Anwendungsfälle über Schnittstellen zwischen den beteiligten Produkttypen und Komponenten umgesetzt. Eine Umsetzung der von IHE geforderten internen Komponenten einer Dokumentenverwaltung wie Document Repository, Document Registry oder Audit Repository wird nicht explizit gefordert, solange das geforderte Sicherheitsniveau und die Funktionalität erhalten bleiben.

2.5.1.2 Realisierungskonzept

Beim Einstellen eines Dokuments muss dieses gemäß IHE mit Metadaten (Autor, eindeutige Dokumentenkennung, Dateiformat etc.) versehen werden, die zusammen mit dem Dokument in der Dokumentenverwaltung gespeichert werden. Die Akte eines Versicherten wird eindeutig über den RecordIdentifier identifiziert, d.h., das XDS.b-Metadatum patientId ist äquivalent zum RecordIdentifier. Ein oder mehrere Dokumente werden in IHE immer als Paket (sog. SubmissionSet) übertragen. Die Zugehörigkeit eines Dokuments zu einem SubmissionSet wird auch in der Dokumentenverwaltung gespeichert, d.h., es ist ersichtlich, welche Dokumente zusammen eingestellt wurden. Für die Anwendungsfälle zum Herunterladen und Löschen von Dokumenten muss zunächst eine Abfrage der Metadaten erfolgen, da in den Metadaten eine Referenz auf die Dokumente enthalten ist. Über diese Referenz können ein oder mehrere Dokumente heruntergeladen oder gelöscht werden.

Für einen Zugriff auf einmal eingestellte Dokumente stellt ein Client eine Suchanfrage ("Stored Query" gemäß IHE), die sich immer auf einen gewählten Versicherten und die Metadaten seiner Dokumente bezieht. Versichertenübergreifende Suchen ("alle Versicherten mit den Eigenschaften...") sind nicht möglich. Die Dokumentenverwaltung liefert auf Wunsch pro Treffer den vollen Satz der zum Dokument zugehörigen Metadaten zurück. Die Ergebnismenge kann vom Client nach den Wünschen des Nutzers nachgefiltert und sortiert werden. Das verschlüsselte Dokument kann in einem weiteren Schritt durch Angabe des Dokumentenidentifikators aus den Metadaten aus der Dokumentenverwaltung heruntergeladen werden. Den Klartext des Dokuments erhält man durch Entschlüsselung mit dem jeweiligen Dokumentenschlüssel im Fachmodul oder im ePA-Frontend des Versicherten.

Um die Vertraulichkeit der medizinischen Informationen in den Dokumenten des Versicherten sicherzustellen, werden diese Ende-zu-Ende verschlüsselt in der Dokumentenverwaltung gespeichert. Das heißt, vor dem Hochladen werden die Dokumente von der ePA-Fachlogik im ePA-Fachmodul des Konnektors bzw. im ePA-Frontend des Versicherten verschlüsselt und nach dem Herunterladen in diesen Komponenten entschlüsselt. Die beschreibenden Metadaten werden transportverschlüsselt gesichert und werden im Arbeitsspeicher der Dokumentenverwaltung im Klartext verarbeitet. Die persistente Spei-

Cherung der Metadaten in der Dokumentenverwaltung erfolgt ebenfalls verschlüsselt, mit kryptografischem Schlüsselmaterial, das der Versicherte beim Login in die vertrauenswürdige Ausführungsumgebung der Dokumentenverwaltung einbringt.

2.5.1.3 Metadaten

Die Dokumentenverwaltung führt zu jedem gespeicherten Dokument beschreibende Metadaten. Diese Metadaten umfassen zum einen technische Attribute zur Dateiverwaltung und der Durchsetzung von Zugriffsregeln. Zusätzlich werden medizinische Metadaten gespeichert, um eine fachliche Suche auf dem Datensatz eines Versicherten zu ermöglichen, damit Leistungserbringer und auch der Versicherte selbst umfangreiche Möglichkeiten haben, sich in den Daten zurechtzufinden und diese bedarfsgerecht organisieren können.

Die Festlegung der konkreten Metadaten erfolgt in der Spezifikation der Schnittstellen des Produkttyps zur Realisierung der Dokumentenverwaltung. Fachlich und funktional werden die Metadaten mindestens die folgenden Attribute enthalten:

Tabelle 2 : Metadaten für die Dokumentenverwaltung

Metadatum	Beschreibung
Autor	Name des einstellenden Akteurs, bei LEI weitere, detaillierende Angaben
Zeitstempel	der Erstellung/Speicherung
ID	eindeutige Dokumentenkennung
Dateiformat	zur Formatprüfung
Dokumentenformat	für die Detaillierung medizinischer Formate
Hashwert	
UserID	des Versicherten bzw. Aktenkennung
Dokumentengröße	
Dateiname	

Die angegebenen Attribute werden mittels IHE-Metadatensets realisiert.

2.5.1.4 Formatspezifische Metadaten

IHE XDS-basierte Patientenakten können unter Beachtung der im XDS-Profil festgesetzten Metadatenregelungen beliebige Dokumente speichern; XDS ist "content agnostic". Allerdings ist es sinnvoll, für einige Metadatenfelder bei bestimmten Inhalten weitere Einschränkungen vorzunehmen.

IHE tut dies, indem es für einige Inhalte, z. B. medizinische Bilder im DICOM-Format oder Laborberichte im HL7 CDA-Format, sogenannte "Content Profiles" definiert (z. B. XD-LAB für verschiedene Laborberichte). Diese machen Vorgaben zu Format und Inhalt des Dokuments aber auch zur Belegung von Metadaten für Dokument und SubmissionSet (s.o.).

ePA verwendet in der ersten Ausbaustufe keinerlei IHE Content Profiles, da die dort ausgetauschten Dokumentenformate ("Allzweckformate" und den Formaten der Fachanwendung des § 291a SGB V in ePA) nicht durch IHE abgedeckt werden. Allerdings ist es in IHE üblich, bei HL7 CDA-basierten Dokumenten auf einige grundlegende Regelungen zurückzugreifen (siehe [IHE_PCC_TF], Kapitel 4). Da ePA mit dem eArztBrief über das generische HL7_CDA_R2-Format HL7 CDA-basierte Dokumente verwendet, sollen die Anforderungen aus [IHE_PCC_TF] auch für diese Dokumente gelten.

2.5.2 Konzept Berechtigung

Die Fachanwendung ePA setzt ein zweistufiges Berechtigungskonzept um. Es erlaubt das Vergeben und Entziehen von Zugriffsrechten im Aktenkonto eines Versicherten innerhalb des ePA-Aktensystems durch den Versicherten bzw. einen berechtigten Vertreter. Ein Benutzer wird in der Dokumentenverwaltung über Zugriffsregeln berechtigt, auf Dokumente des Versicherten zugreifen zu dürfen. Zusätzlich muss dieser im Besitz kryptografischen Schlüsselmaterials sein, um autorisierte Inhalte entschlüsseln zu können. Es ist jedoch auch möglich, eine kryptografische Berechtigung, d.h. für einen Nutzer verschlüsseltes Schlüsselmaterial, zu hinterlegen und den Zugriff auf Dokumente der Dokumentenverwaltung explizit auszuschließen. Dieses Szenario kann für den Berechtigungserhalt genutzt werden, in dem das Schlüsselmaterial eines Aktenkontos bei Kartenverlust von einem kryptografisch Berechtigten oder mittels exportiertem Schlüsselmaterial auf eine neue Karte umgeschlüsselt werden kann. Das Szenario ist vergleichbar mit der Einrichtung einer Vertretungsberechtigung für einen anderen eGK-Inhaber als Vertreter, der im Fall eines Kartenverlusts das Schlüsselmaterial für die neue eGK eines Versicherten neu verschlüsseln kann.

2.5.2.1 Funktionsweise

Die kryptografische Autorisierung erfolgt auf Basis kartenbezogener, kryptografischer Identitäten der Benutzer, in dem das kryptografische Schlüsselmaterial des Aktenkontos eines Versicherten für die Karte des Empfängers verschlüsselt weitergegeben wird. Die verschlüsselte Weitergabe des kryptografischen Schlüsselmaterials erfolgt über die Dienstkomponekte "Autorisierung" des ePA-Aktensystems, die die Funktionalität eines Schlüsselkastens abbildet.

Beim Aktivieren des Aktenkontos sowie beim Berechtigen eines Benutzers (Leistungserbringer, Vertreter, Drittanwendung) erfolgt zum einen die Aktivierung von Zugriffsregeln im Dokumentenmanagementsystem und zum anderen wird das kryptografische Akten-schlüsselmaterial empfängerindividuell verschlüsselt hinterlegt. Eine Hinterlegung für Vertreter oder Wiederherstellungsfunktionen (siehe Daten- und Berechtigungserhalt) mit speziellen, eingeschränkten Nutzungsrechten kann hier ebenfalls erfolgen.

Die Vergabe von Zugriffsberechtigungen erfolgt initial durch den Versicherten als Eigentümer seiner Akte. Seine Zugriffsrechte können durch keinen anderen Nutzer entzogen werden. Der Versicherte kann Leistungserbringerinstitutionen und Vertreter für den Zugriff in seines Aktenkontos berechtigen, indem er das kryptografische Schlüsselmaterial seines Aktenkontos für die Karte des Berechtigten (SMC-B der LEI, eGK des Vertreters) verschlüsselt und zusammen mit entsprechenden Zugriffsregeln im ePA-Aktensystem hinterlegt.

In diesen Zugriffsregeln legt der Versicherte fest, auf welche Dokumente der Berechtigte zugreifen darf (nur auf von Leistungserbringerinstitutionen eingestellte Dokumente, oder zusätzlich auf vom Versicherten eingestellte Dokumente). Für Leistungserbringerinstituti-

onen muss zusätzlich der Gültigkeitszeitraum der Berechtigung (1 Tag, 28 Tage, 18 Monate oder frei wählbar bis max. 18 Monate) angegeben werden.

In der Umgebung der Leistungserbringer erfolgt die Vergabe der Berechtigung über den Anwendungsfall "Ad-hoc-Berechtigung anfordern", den ein Mitarbeiter der Leistungserbringerinstitution über das Primärsystem startet. Mittels eGK und PIN-Eingabe des Versicherten oder eines von ihm berechtigten Vertreter werden im ePA-Aktensystem Zugriffsregeln für diese LEI und für die SMC-Bs der LEI verschlüsseltes Schlüsselmaterial hinterlegt.

In der Umgebung des Versicherten können Versicherte und Vertreter mit dem Anwendungsfall "Berechtigung durch einen Versicherten vergeben" Leistungserbringerinstitutionen berechtigen, deren Zertifikatsinformationen der zu berechtigenden SMC-Bs im Verzeichnisdienst der TI-Plattform hinterlegt sind. Der Versicherte kann Vertretungen mittels Anwendungsfall "Vertretung durch einen Versicherten einrichten" einrichten, die Einrichtung von weiteren Vertretungen durch einen Vertreter ist jedoch nicht zulässig.

Die nachfolgende Tabelle zeigt die Zulässigkeit von Anwendungsfällen im Zusammenhang des Berechtigungskonzepts in den jeweiligen Umgebungen.

Tabelle 3: Berechtigungsmaske

UseCase	Versicherter	Vertreter	Leistungserbringerinstitution	Wiederherstellung/Identität/Schlüsselmaterial
Berechtigung an eine LEI vergeben	Umgebung des Versicherten, ad hoc in LE-Umgebung	Umgebung des Versicherten ad hoc in LE-Umgebung	-	-
Vertretung einrichten	Umgebung des Versicherten	-	-	-
Berechtigungen auflisten, ändern, löschen	Umgebung des Versicherten	Umgebung des Versicherten	-	-
Neue eGK bekannt machen	Umgebung des Versicherten mittels alter eGK	Umgebung des Versicherten mittels Vertreter-eGK	-	-
Zugriff auf Schlüsselmaterial	Für Berechtigungsvergabe Für Datenzugriff Für Umschlüsselung	Für Berechtigungsvergabe Für Datenzugriff Für Umschlüsselung	Für Datenzugriff	Für Umschlüsselung
Zugriff auf	Metadaten:	Metadaten:	Metadaten:	-

Daten und Dokumente	Lesen, Schreiben, Löschen (per Löschen Dokument) Dokument: Lesen, Schreiben, Löschen	Lesen, Schreiben, Löschen (per Löschen Dokument) Dokument: Lesen, Schreiben, Löschen	<i>Lesen, Schreiben, Löschen (per Löschen Dokument)</i> Dokument: <i>Lesen, Schreiben, Löschen</i>	
---------------------	--	--	--	--

2.5.2.2 Realisierungskonzept

Die Realisierung des Berechtigungskonzepts setzt auf die erfolgreiche Authentifizierung aller Nutzer auf. Hierfür wird eine Komponente angenommen, die in der Lage ist, jeden Benutzer anhand seiner Authentisierungsmerkmale (z.B. eGK, SMC-B und ggfs. später auch alternativer Authentisierungsmerkmale) eindeutig zu authentifizieren.

Die Idee eines „Schlüsselkastens“ sieht einen separaten, neben der Dokumentenverwaltung stehenden Autorisierungsdienst vor. Dieser speichert und verwaltet das empfängerbezogene verschlüsselte Schlüsselmaterial eines Aktenkontos und gibt den Datensatz eines Nutzers auf Anforderung des authentifizierten Nutzers heraus. Die Authentifizierungsbestätigung stellt eine Authentisierungskomponente aus, wenn der Nutzer von dieser erfolgreich authentifiziert wurde (z.B. mittels Karte + PIN).

Ist im Autorisierungsdienst neben dem empfängerbezogenen verschlüsselten Schlüsselmaterial jedes Nutzers im Aktenkonto eines Versicherten zusätzlich die Erlaubnis hinterlegt worden, mit diesem Schlüsselmaterial auf Daten des Versicherten zugreifen zu dürfen, stellt der Autorisierungsdienst eine Autorisierungsbestätigung aus, die ihn gegenüber der Komponente Dokumentenverwaltung als autorisierten Nutzer im Aktenkonto eines Versicherten ausweist.

Das für die Schnittstelle zur Dokumentenverwaltung vorgesehene IHE-Framework legt die Nutzung des IHE APPC-Profiles mit dem OASIS XACML-Standard für die Autorisierung auf Dokumentenebene nahe. Mittels XACML lassen sich Zugriffsregeln definieren, die aus Gründen der Handhabbarkeit für Versicherte auf einen vordefinierten Satz an Regeln beschränkt werden. Umgesetzt werden vordefinierte Regeln für die Berechtigung von Leistungserbringern, befristete Ad-hoc-Berechtigungen sowie die Autorisierung des Zugriffs für Vertreter auf der Basis von Dokumenteneigenschaften. Dabei soll gelten, dass ein Zugriff nur gewährt wird, wenn eine Zugriffsregel dies explizit erlaubt. Für die Prüfung der Zugriffsregeln eines Nutzers, muss dieser für jeden Zugriff eine Autorisierungsbestätigung vorlegen.

Für die Realisierung der Authentifizierungs- und Autorisierungsbestätigung zur Durchsetzung von Zugriffsregeln auf Schlüsselmaterial für Berechtigte und Daten des Versicherten kommen Standardtechniken aus dem WS-Trust-Kontext (z.B. SAML) zum Einsatz, da diese der bestehenden Webservice-Infrastruktur der TI am nächsten stehen.

Die Vergabe von Berechtigungen erfolgt bezogen auf reale Identitäten. Der Versicherte sowie der berechtigte Vertreter werden anhand des unveränderlichen Teils der KVNR identifiziert, auch über einen möglichen Kartenwechsel hinweg. Die Leistungserbringereinstitution wird anhand der Telematik-ID identifiziert, zu der es eine oder mehrere SMC-Bs im Praxisbetrieb geben kann.

Die Hinterlegung des kryptografischen Schlüsselmaterials des Aktenkontos erfolgt im Autorisierungsdienst, verschlüsselt mit dem öffentlichen Schlüssel des ENC-Zertifikats der jeweiligen Karte des Berechtigten. Die Hinterlegung der Zugriffsregeln in der Doku-

mentenverwaltung erfolgt auf Basis der KVNR des Versicherten bzw. seines Vertreters und für Leistungserbringerinstitutionen für die Telematik-ID der Institution.

2.5.2.3 Geräteprüfung

Um einen möglichen Missbrauch und Identitätsdiebstahl erkennen zu können, wird eine weitere Berechtigungsprüfung auf Geräteebeane auf Seiten der Versicherten umgesetzt. Der Zugriff durch Versicherte und deren Vertreter auf Daten und Dokumente in einem Aktenkonto ist zulässig, wenn das Gerät, auf dem der Versicherte bzw. ein berechtigter Vertreter das ePA-Frontend des Versicherten für den Zugriff auf das Aktenkonto nutzt, über einen separaten Benachrichtigungskanal (E-Mail mit Freischalt-Link, SMS-TAN o.ä.) zur Benutzung autorisiert wurde. Die Prüfung auf die Verwendung eines registrierten Geräts ergänzt um die Benachrichtigung zur Neuregistrierung ist Stand der Technik und wird u.a. bei Anbietern von E-Mail-Accounts verwendet, deren Benutzerinteraktion primär über Webbrowser erfolgt.

2.5.2.4 Berechtigungserhalt

Die Fachanwendung ePA bietet mehrere Möglichkeiten des Berechtigungserhalts an, die mit unterschiedlichen Voraussetzungen durchgeführt werden können.

Tabelle 4 : Übersicht über die Verfahren des Berechtigungserhalts für Versicherte

Anlass Verfahren des Berechtigungs- erhalts für Versicherte	Karten- wechsel			Ablauf der Gül- tigkeit/ Sperrung			Verlust/ Diebstahl		
Umgebung	pU m. KT	pU o. KT	LEI	pU m. KT	pU o. KT	LEI	pU m. KT	pU o. KT	LEI
UC 3.3 - Neue eGK über alte eGK bekannt machen	X	-	-	X	-	-	-	-	-
UC 3.4 - Neue eGK über Vertreter bekannt machen	X	-	-	X	-	-	X	-	-
UC 3.8 - Umschlüsse- lung mit sicher verwahr- tem Schlüsselmaterial	X	-	-	X	-	-	X	-	-

pU m. KT = persönliche Umgebung (Personal Zone) mit Kartenterminal

pU o. KT = persönliche Umgebung (Personal Zone) ohne Kartenterminal

LEI = Leistungserbringerinstitution

Der Autorisierungsdienst für ePA unterstützt das Leistungsmerkmal „Daten- und Berechtigungserhalt“, indem eine für eine Wiederherstellungsidentität verschlüsselte Kopie des kryptografischen Schlüsselmaterials hinterlegt werden kann. Diese Wiederherstellungsidentität ist die eGK eines Vertreters oder auch das für eine Umschlüsselungsfunktion sicher verwahrte kryptografische Schlüsselmaterial. Der Autorisierungsdienst wird dabei so gestaltet, dass er diese Kopie nur an eine zur Umschlüsselung berechnigte, authentifizierte Identität (Umschlüsselungsfunktion, Vertreter) herausgibt. Für diese Identität wird

keine Autorisierungsbestätigung ausgestellt, womit der missbräuchliche Zugriff auf Daten des Versicherten in der Komponente Dokumentenverwaltung ausgeschlossen werden kann.

2.5.3 Konzept Lokalisierung

Für Leistungserbringer und Versicherte muss ein Aktenkonto lokalisiert werden können. Dies muss aus allen dezentralen Einsatzumgebungen heraus möglich sein. Insbesondere berechnete Leistungserbringerinstitutionen und Vertreter benötigen einen Mechanismus, das Aktenkonto des Versicherten zu lokalisieren, das bei einem beliebigen Anbieter ePA-Aktensystem geführt werden kann.

Die Lokalisierung der Zielakte erfolgt über den `RecordIdentifier`, der im Rahmen der Kontoeröffnung für jedes Aktenkonto bei jedem Anbieter ePA-Aktensystem eindeutig vergeben wird. Dieser besteht aus einer Anbieterkennung und dem 10-stelligen unveränderlichen Teil der KVN-R des Versicherten (Versicherten-ID). Die Anbieterkennung wird als Home Community ID gemäß IHE-Framework als OID dargestellt.

Mit Hilfe der Anbieterkennung und des Namensdienstes der zentralen TI-Plattform wird die Adresse des ePA-Aktensystems mit seinen Komponenten Authentisierung, Autorisierung und Dokumentenverwaltung ermittelt. Mit der Versicherten-ID wird dann das konkrete Aktenkonto eines Versicherten in diesem ePA-Aktensystem adressiert.

Mittels Auswahl zwischen zwei oder mehr ihm bekannten Versicherten-ID kann ein Versicherter aus seinem eigenen Aktenkonto in ein Aktenkonto eines Vertretenen wechseln, um eine Vertretung wahrnehmen zu können. Die Versicherten-ID des Versicherten-Kontos hat ihm der Versicherte im Rahmen der Einrichtung der Vertretung zur Nutzung im ePA-Frontend mitgeteilt. Mit der Auflistung der Versicherten-ID (10-stelliger, unveränderlicher Teil der KVN-R) im ePA-Frontend erhält ein Versicherter die Übersicht, für welche Aktenkonten er eine Vertretung eingeräumt bekommen hat.

Verschiedene ePA Aktensysteme prüfen untereinander die Existenz eines bestehenden Aktenkontos auf Basis der Versicherten-ID, um das mehrfache Anlegen eines Aktenkontos durch einen Versicherten zu unterbinden. Die Schnittstelle ist nur innerhalb der TI (nicht im Internet) verfügbar.

Zur Vereinfachung der Abläufe im Praxisbetrieb besteht für die Systeme der Leistungserbringerumgebung die Möglichkeit der Abfrage der `RecordIdentifier` auf Basis der Versicherten-ID des Versicherten. Diese Schnittstelle steht aus Sicherheitsgründen nicht zur Abfrage durch ePA-Frontends der Versicherten aus dessen Umgebung zur Verfügung.

Hinweis: Wenn im Folgenden die KVN-R als Parameter benannt wird, ist jeweils der 10-stellige, unveränderliche Anteil der KVN-R gemeint.

2.5.4 Konzept Protokollierung

Gemäß § 291a SGB V Abs. 6 müssen wenigstens die letzten 50 Zugriffe auf medizinische Daten eines Versicherten für Zwecke der Datenschutzkontrolle protokolliert werden. Zeitpunkt und Art des Zugriffs sowie das medizinische Datum, auf welches zugegriffen wurde, muss für den Versicherten nachvollziehbar sein. Es gelten die Anforderungen des § 291a SGB V zur Protokollierung des Zugriffs auf medizinische Daten eines Versicherten. Da alle Anwendungsfälle mit einem Bezug zu Dokumenten oder deren Metadaten in der Komponente Dokumentenmanagement des ePA-Aktensystems abgearbeitet werden, werden diese Zugriffe auch in dieser Komponente protokolliert.

Zudem sind insbesondere die Regelungen der Artikel 25, 32 DSGVO i.V.m. § 22 BDSG bei der Ausgestaltung der Protokolle zu berücksichtigen. Protokolliert werden in diesem Zusammenhang alle Anwendungsfälle, die nicht direkt ein Dokument oder dessen Metadaten betreffen und eher administrativen Charakter haben (z.B. Login, Berechtigungsvergabe, neue eGK mit alter eGK bekannt machen etc.). Diese Art von Zugriffen wird innerhalb des ePA-Aktensystems in den Komponenten „Zugangsgateway“ und „Autorisierer“ als Verwaltungsprotokoll protokolliert.

Die Einsicht in das Protokoll ist nur dem Versicherten oder einem von ihm autorisierten Vertreter gestattet. Durch das ePA-Frontend des Versicherten werden hierzu die Protokolleinträge der drei protokollierenden Systeme abgeholt und in einer für den Versicherten lesbaren und verständlichen Form aufbereitet. Die Protokolldaten sind gegen zweckfremde Verwendung und gegen sonstigen Missbrauch zu schützen. Das Zugriffsprotokoll enthält personenbezogene medizinische Informationen. Der Schutzbedarf für Vertraulichkeit und Integrität ist daher sehr hoch. Auf eine zusätzliche Protokollierung für den Versicherten im Fachmodul oder im ePA-Frontend des Versicherten wird verzichtet.

Für die Protokollierung der Zugriffe auf medizinische Daten eines Versicherten besteht kein Grund, die auf die Speicherkapazität der eGK ausgelegte Beschränkung auf die letzten 50 Protokolleinträge auch für dienstbasierte Fachanwendungen aufrecht zu erhalten. Insbesondere stellen Suchoperationen ebenfalls einen Zugriff auf medizinische (Meta-)daten über Dokumente des Versicherten dar. Daher ist eine Beschränkung auf 50 Einträge aus technischer Sicht nicht notwendig. Im Sinne der Nachvollziehbarkeit für den Versicherten wird eine Einschränkung der Anzahl von Protokolleinträgen auch von der BfDI und dem BSI nicht empfohlen.

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.

Da die Dokumentenverwaltung als einzige Komponente im ePA-Aktensystem mit IHE-Schnittstellen realisiert wird, wird auf die Verwendung des IHE ATNA-Profiles für die Protokollierung verzichtet und ein separates Protokoll spezifiziert.

Auf Versichertenseite ist der Versicherte bzw. sein Vertreter durch seine Authentisierung identifizierbar. Alle Zugriffe des Versicherten bzw. seines Vertreters sind im Zugriffsprotokoll klar erkennbar.

Auf Seite des Leistungserbringers wird die Authentisierung durch den Konnektor auf Ebene der SMC-B durchgeführt. Um es für den Versicherten nachvollziehbar zu gestalten, welche Leistungserbringerinstitution auf seine Daten zugegriffen hat, muss das Primärsystem den Klarnamen der Leistungserbringerinstitution bei der Authentisierung mitliefern.

Im Falle eines Anbieterwechsels werden beim Datentransfer vom Aktenkonto des alten Anbieters zu dem des neuen Anbieters die Einträge des §291a-konformen Zugriffsprotokolls (Zugriff auf medizinische Daten) übernommen. Für die Einträge des Verwaltungsprotokolls hat der Versicherte die Möglichkeit, die Protokolleinträge vor dem Wechsel lokal abzuspeichern.

Eine Protokollierung der Tätigkeiten der Leistungserbringer für den Leistungserbringer ist in § 291a SGB V nicht gefordert.

Eine technische Protokollierung der Prozesse und Transaktionen innerhalb und zwischen verschiedener/n Komponenten ohne Personenbezug ist für den sicheren Betrieb geboten. Zu diesen technischen Protokollen wird in diesem Abschnitt keine Aussage getroffen. Die Ausgestaltung von Art und Umfang technischer Protokolle obliegt einem Anbieter ePA-Aktensystem, soweit diese nicht den berechtigten Datenschutzinteressen aller Nut-

zer (Versicherte, Vertreter, Leistungserbringerinstitutionen) entgegenstehen. In den nachfolgenden Spezifikationen wird allerdings in Abhängigkeit zum Verhalten im Fehlerfall eine genauere Festlegung getroffen. Die grundsätzliche Prämisse, dass medizinische und personenbezogene Daten in technischen Protokollen nicht gespeichert werden dürfen, kann maximal durch die Speicherung personenbezogener Daten im Falle eines schwerwiegenden Fehlers durchbrochen werden.

2.5.5 Konzept Verschlüsselung

Zur Erreichung der Schutzziele wird das folgende kryptografische Schlüsselmaterial verwendet:

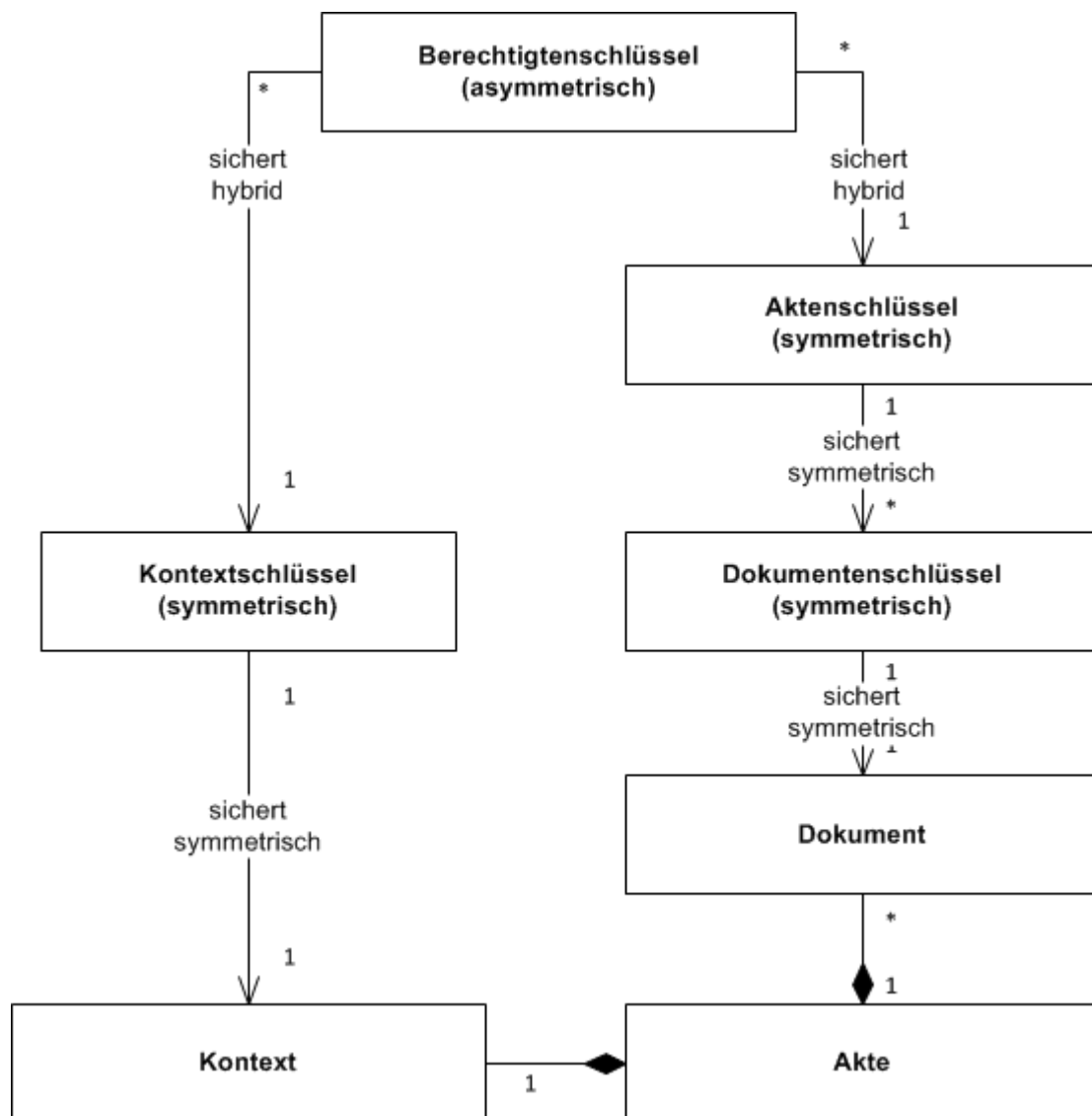


Abbildung 5 : Kryptografisches Schlüsselmaterial

Die „Akte“ als medizinische Dokumentation eines Versicherten besteht aus der Summe der für diesen Versicherten gespeicherten Dokumente und dem Kontext des Aktenkontos zur vertraulichen, geschützten Verarbeitung von Meta- und Protokolldaten sowie der Policies der Zugriffsberechtigung auf Objektebene der Dokumentenverwaltung.

Die medizinischen Dokumente der Patientenakte eines Versicherten werden Ende-zu-Ende-verschlüsselt gesichert, d. h., die Ver- und Entschlüsselung findet in den Produkttypen der dezentralen Umgebungen statt (ePA-Fachmodul, ePA-Frontend des Versicherten). Dazu wird für jedes Dokument in der dezentralen Umgebung ein zufälliger, symmetrischer Dokumentenschlüssel generiert, mit dem das Dokument verschlüsselt wird. Dieser Dokumentenschlüssel wiederum wird mit dem Aktenschlüssel eines Aktenkontos verschlüsselt und dem verschlüsselten Dokument beigelegt. Dieses Verschlüsselungspaket stellt dasjenige Datenobjekt dar, das als „Dokument“ in der Komponente „Dokumentenverwaltung“ gespeichert wird.

Die Metadaten über Dokumente in der Komponente „Dokumentenverwaltung“ enthalten Klartextinformationen über den Versicherten und den das Dokument einstellenden Nutzer. Dies ermöglicht unter anderem eine serverseitige, komfortable Suche in allen gespeicherten Metadaten der Dokumente, sowie die serverseitige Durchsetzung von Zugriffsrechten auf Objektebene. Gleiches gilt für das Zugriffsprotokoll für den Versicherten, in dem er über eine komfortable Suche detailliert die Zugriffe auf seine medizinischen Daten nachvollziehen kann. Um dem Anbieter ePA-Aktensystem keine Einsicht in diese Daten zu gewähren, werden diese in einer vertrauenswürdigen Umgebung verarbeitet und ausschließlich verschlüsselt persistiert. Die Ver- und Entschlüsselung dieser Daten erfolgt mit dem Kontextschlüssel, der in der vertrauenswürdigen Ausführungsumgebung beim Start einer Session im Aktenkonto des Versicherten eingebracht wird und beim Beenden der Sitzung aus dem Arbeitsspeicher der vertrauenswürdigen Ausführungsumgebung gelöscht wird. Das Prinzip ist mit einer virtuellen Festplattenverschlüsselung vergleichbar.

Der Aktenschlüssel und der Kontextschlüssel sind aus Sicht der Fachanwendung ePA die zentralen kryptografischen Elemente, die den Zugriff auf Daten und Dokumente ermöglichen. Somit stellen sie die kryptografische Zugriffsberechtigung dar, die vom Versicherten in verschlüsselter Form an Berechtigte weitergegeben wird. Die Erzeugung des Akten- und Kontextschlüssels wird initial beim Anlegen eines Aktenkontos durchgeführt. Beim Anlegen eines Aktenkontos in der Leistungserbringerumgebung werden diese dezentral im Konnektor und in der Versichertenumgebung im ePA-Frontend des Versicherten erzeugt.

Der Aktenschlüssel und der Kontextschlüssel werden für jeden Zugriffsberechtigten durch den jeweiligen Berechtigtenschlüssel (C.CH.ENC Zertifikat der eGK des Versicherten sowie das C.HCI.ENC Zertifikat der SMC-B einer Leistungserbringerinstitution) hybrid verschlüsselt. Diese Verschlüsselung findet im Rahmen der Berechtigungsvergabe statt, das verschlüsselte Paket wird in der Komponente Autorisierung für jeden berechtigten Nutzer hinterlegt und wird dort vom Versicherten bzw. einem berechtigten Vertreter des Versicherten verwaltet.

3 Anwendungsfälle

3.1 Übersicht der Anwendungsfälle

Das folgende in der Abbildung 6 dargestellte UML-Diagramm gibt eine Übersicht über die Anwendungsfälle der Fachanwendung ePA.

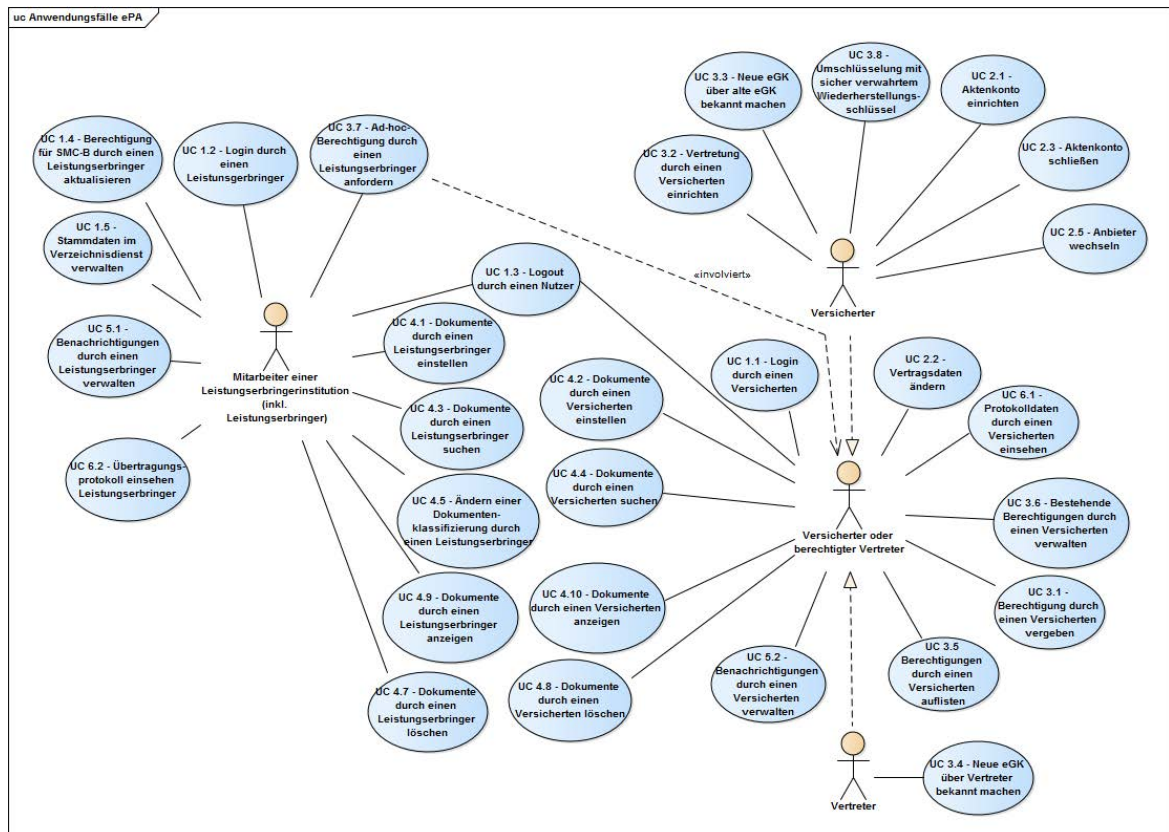


Abbildung 6: Übersicht der Anwendungsfälle ePA

Die Anwendungsfälle „Aktenkonto einrichten“ und „Aktenkonto schließen“ können nur vom Versicherten als Inhaber des Aktenkontos ausgelöst werden. Die Anwendungsfälle zur Berechtigungsverwaltung hingegen können nicht nur von Versicherten, sondern auch von Vertretern ausgeführt werden. Das Einrichten von Vertretungen durch einen Vertreter ist, wie zuvor erwähnt, nicht zulässig. Trigger der Anforderung einer Ad-hoc-Berechtigung ist ein Mitarbeiter der Leistungserbringereinstitution. Die Anwendungsfälle zur Dokumenten- und Protokollverwaltung werden sowohl Versicherten bzw. ihren Vertretern als auch den Leistungserbringern zugeordnet. Für Leistungserbringer erfolgt die Protokollverwaltung im Primärsystem.

Die Anwendungsfälle für den Nutzerzugang sowie den Berechtigungserhalt werden nicht direkt von Nutzern des Aktenkontos ausgeführt. Sie werden stattdessen in fachlichen Anwendungsfällen genutzt, um notwendige Vor- bzw. Nachbedingungen der übrigen Anwendungsfälle sicherzustellen. Die Transportfunktionalität des Zugangsgateways für Versicherte ist aus Gründen der Vereinfachung in den Anwendungsfällen nicht dargestellt.

3.2 Übergreifende Vorbedingungen

Die nachfolgenden Vorbedingungen müssen für alle Anwendungsfälle erfüllt sein, damit sie erfolgreich ausgeführt werden können. Wenn diese Vorbedingungen nicht erfüllt sind, so muss die Operation mit einer Fehlermeldung abbrechen.

EPA-EPF-A_0001 - Übergreifende Vorbedingung: Aufrufparameter gültig

Jeder Produkttyp und jede Komponente der Fachanwendung ePA MÜSSEN bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn notwendige Aufrufparameter unvollständig, ungültig oder inkonsistent sind.

[<=]

Hinweis: Sofern in den folgenden fachlichen Anwendungsfällen ein Login für den benannten Nutzer nicht explizit angegeben ist, wird davon ausgegangen, dass dieser implizit durch die Session-Verwaltung des entsprechenden Produkttyps vorgenommen wird.

EPA-EPF-A_0002 - Übergreifende Vorbedingung: Login nach Notwendigkeit

Jeder Produkttyp und jede Komponente der Fachanwendung ePA MÜSSEN den Anwendungsfall „Login durch einen Versicherten“ oder „Login durch einen Leistungserbringer“ vor der Ausführung einer weiteren fachlichen Operation starten, wenn im Rahmen der internen Session-Verwaltung keine aktuellen Session-Daten vorhanden sind.

[<=]

EPA-EPF-A_0003 - Übergreifende Vorbedingung: Veröffentlichung von Dienstendpunkten

Das ePA-Aktensystem MUSS die Endpunkte der Komponente „Autorisierung“ im Namensdienst der TI-Plattform registrieren.

[<=]

EPA-EPF-A_0004 - Übergreifende Vorbedingung: Anbieterlokalisierung

Das Fachmodul ePA MUSS den Namensdienst der TI-Plattform für die Lokalisierung der Komponente der Autorisierung verwenden.

[<=]

3.3 Übergreifende Nachbedingungen

Der folgende Abschnitt beschreibt übergreifende Nachbedingungen, die für den erfolgreichen Abschluss fachlicher Anwendungsfälle gelten.

Jeder Zugriff auf medizinische Daten des Versicherten muss gemäß § 291a Abs. 6 Satz 3 SGB V für den Versicherten nachvollziehbar dokumentiert werden. Hierzu führt die Fachanwendung ePA ein Zugriffsprotokoll im Aktenkonto des Versicherten, in dem jeder Zugriff auf Daten des Versicherten im ePA-Aktensystem mit Datum, Uhrzeit und dem Namen des Zugreifenden eingetragen wird.

EPA-EPF-A_0005 - Protokollierung der Zugriffe auf medizinische Daten

Die Komponente „Dokumentenverwaltung“ MUSS für jeden Aufruf einer Operation mit Zugriff auf Metadaten oder Dokumente des Versicherten einen Protokolleintrag im Aktenkonto des Versicherten hinzufügen. Der Eintrag MUSS dabei das aktuelle Datum, die aktuelle Uhrzeit und die Art des Zugriffs, einen lesbaren Namen des Zugreifenden sowie einen Bezeichner des zugegriffenen Datenobjekts enthalten.

[<=]

EPA-EPF-A_0006 - Für den Nutzer verständliche Fehlermeldungen

Alle an den Anwendungsfällen der Fachanwendung ePA beteiligten Produkttypen und Komponenten MÜSSEN interoperable Fehlermeldungen bereitstellen, die es den Versicherten bzw. den Mitarbeitern der Leistungserbringerinstitution ermöglichen, die Ursache des Fehlers über ihr jeweiliges Frontend zu identifizieren und mögliche Gegenmaßnahmen zu ergreifen. [≤=]

3.4 Nutzerzugang ePA

Die in diesem Abschnitt vorgestellten Anwendungsfälle beschreiben die technischen Aktionen zur Herstellung und Aufrechterhaltung des Zugangs eines Nutzers zur Fachanwendung ePA.

3.4.1 Login durch einen Versicherten

Mit dem Anwendungsfall „Login durch einen Versicherten“ meldet sich der Versicherte am ePA-Aktensystem an. Zunächst wird er durch die Komponente Zugangsgateway über seine eGK authentifiziert, anschließend erfolgt die Autorisierungsprüfung über die Komponente Autorisierung. Unter Verwendung der Autorisierungsbestätigung baut das ePA-Frontend des Versicherten einen auf Anwendungsebene verschlüsselten Kommunikationskanal zum Aktenkontext der ePA-Dokumentenverwaltung auf. Abgeschlossen wird der Anwendungsfall durch das erfolgreiche Öffnen des Aktenkontextes in der Komponente Dokumentenverwaltung.

Der Anwendungsfall kann implizit im Zusammenhang mit einer Fachoperation (z.B. Suche und Anzeige der Metadaten zu Dokumenten, die seit dem letzten Login eingestellt wurden) erfolgen oder explizit durch Starten des Anwendungsfalls durch den Versicherten.

EPA-EPF-A_0007 - Anwendungsfall „Login durch einen Versicherten“

Alle am Anwendungsfall „Login durch einen Versicherten“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 5: Login durch einen Versicherten

Name	UC 1.1 - Login durch einen Versicherten
Vorbedingung	Für die Ausführung einer Fachoperation liegt für die aktuelle Session keine gültige Authentifizierungsbestätigung vor. Alternativ kann der Anwendungsfall durch den Versicherten explizit gestartet werden.
Kurzbeschreibung (Außensicht)	Ein Versicherter oder ein Vertreter meldet sich zur Benutzung der Fachanwendung ePA explizit an. Dazu verwendet er das zugelassene 2-Faktor-Authentisierungsmerkmal (eGK + PIN). Der Anwendungsfall „Login durch einen Versicherten“ wird im Kontext eines fachlichen Anwendungsfalls (Ausführung einer Fachoperation) ausgeführt. Mit der Authentifizierungsbestätigung wird die Autorisierung in der Komponente „Autorisierung“ geprüft und je nach Gültigkeit und Umfang der Berechtigung des Nutzers das empfängerverschlüsselte Schlüs-

	selmaterial heruntergeladen. Ist eine Berechtigung für den Zugriff auf Dokumente des Versicherten hinterlegt, wird mittels Autorisierungsbestätigung das Öffnen des Aktenkontextes in der te „Dokumentenverwaltung“ für das Aktenkonto des Versicherten durchgeführt.
Nachbedingung	-

sd UC 1.1 - Login durch einen Versicherten

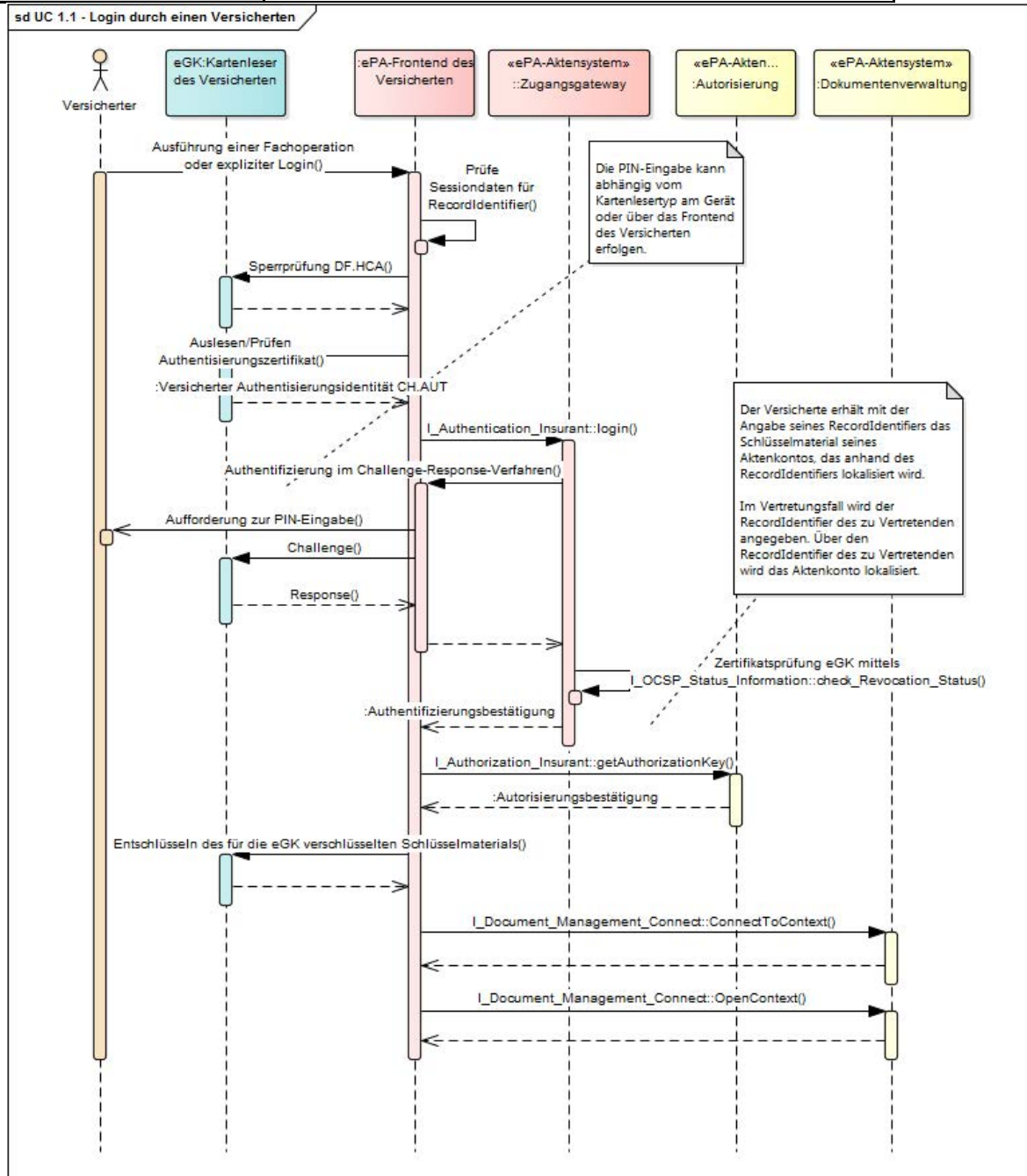


Abbildung 7: Login durch einen Versicherten

[<=]

Um einen Versicherten zu vertreten, meldet sich der Vertreter mit seiner eigenen eGK an. Dazu verwendet er sein persönliches 2-Faktor-Authentisierungsmerkmal (eGK + PIN) und benennt im Rahmen der Autorisierung das Aktenkonto des Vertretenden mittels RecordIdentifier. Den RecordIdentifier erhält er vom Versicherten, der ihn zuvor als Vertreter berechtigt hat. Über diese ID wird das Aktenkonto des Versicherten lokalisiert.

Die Anwendungsfälle zur Vertretung innerhalb des Aktenkontos zur Dokumentenverwaltung, Berechtigungsverwaltung etc. werden in gleicher Weise ausgeführt wie durch den Versicherten.

EPA-EPF-A_0008 - Vertretung für einen Versicherten wahrnehmen

Das Frontend des Versicherten MUSS zur Wahrnehmung der Vertretung eines anderen Versicherten im Anwendungsfall „Login durch einen Versicherten“ den RecordIdentifier des zu Vertretenden verwenden.

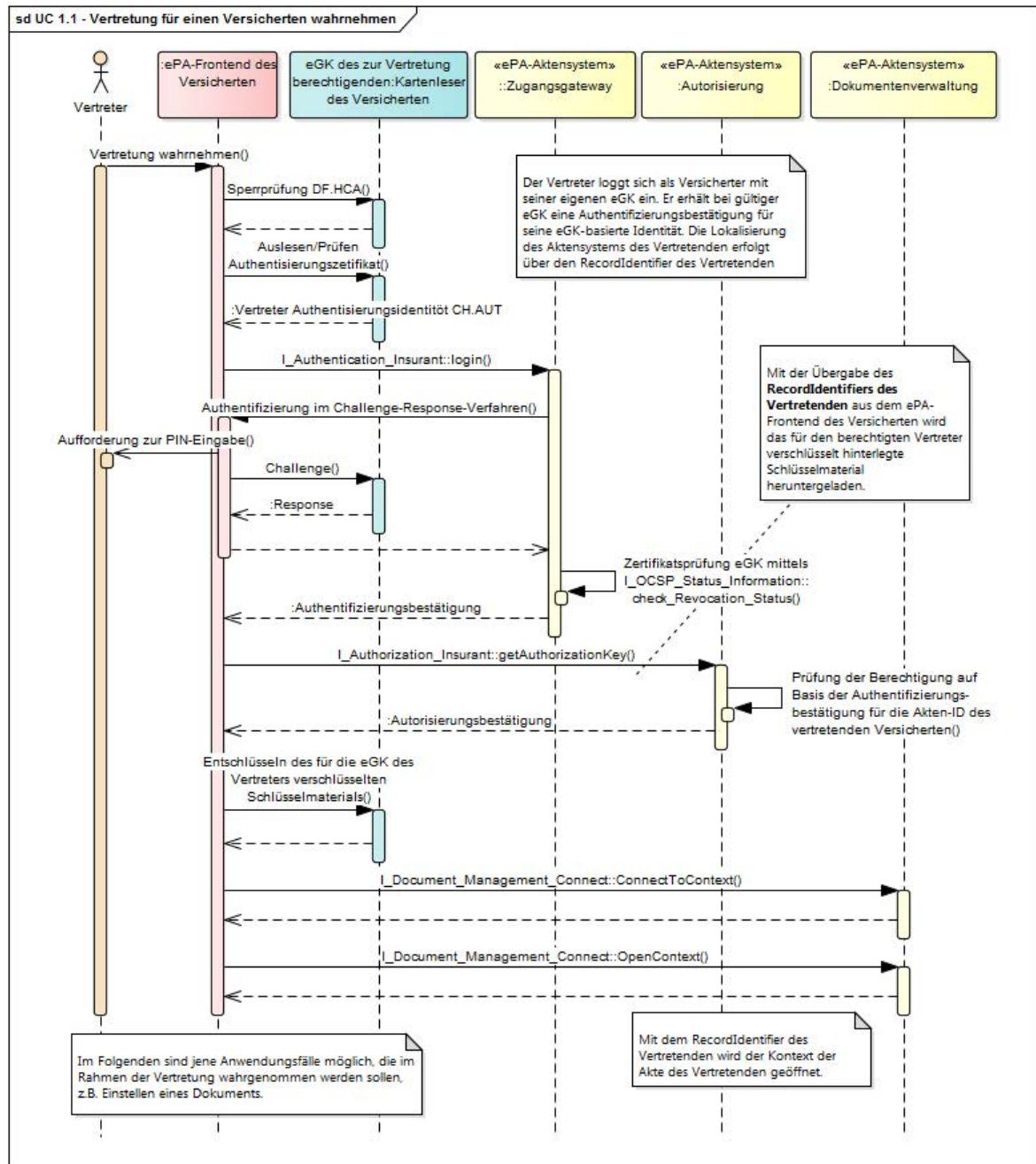


Abbildung 8: Vertretung für einen Versicherten wahrnehmen

[<=]

3.4.2 Login durch einen Leistungserbringer

Der Login in der Umgebung der Leistungserbringer wird durch das Fachmodul ePA gekapselt und erfolgt bei Bedarf. Fordert das Primärsystem die Ausführung einer Fachoperation vom Fachmodul ePA für ein konkretes über den RecordIdentifier adressiertes Aktenkonto eines Versicherten an, prüft das Fachmodul die Anmeldung in diesem Aktenkonto über die interne Sessionverwaltung. Liegen keine Sessiondaten für diesen RecordIdentifier vor (Aktenschlüssel, Authentifizierungs- und Autorisierungsbestätigung), erfolgt automatisch eine Anmeldung im ePA-Aktensystem für diesen RecordIdentifier und eine im Aufrufkontext des Konnektors referenzierte SMC-B. Unter Verwendung der Autorisierungsbestätigung baut das Fachmodul ePA einen auf Anwendungsebene verschlüsselten Kommunikationskanal zum Aktenkontext der ePA-Dokumentenverwaltung auf. Anschließend erfolgt die Ausführung der Fachoperation im Aktenkonto des Versicherten.

EPA-EPF-A_0009 - Anwendungsfall „Login durch einen Leistungserbringer“

Alle am Anwendungsfall „Login durch einen Leistungserbringer“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 6: Login durch einen Leistungserbringer

Name	UC 1.2 - Login durch einen Leistungserbringer
Vorbedingung	Für die Ausführung einer Fachoperation liegt für die aktuelle Session keine gültige Authentifizierungsbestätigung vor. Für die Leistungserbringerinstitution wurde eine Berechtigung im Aktenkonto des Versicherten hinterlegt bzw. aktualisiert.
Kurzbeschreibung (Außensicht)	In der Leistungserbringerumgebung führt das Fachmodul ePA einen Login gegenüber dem ePA-Aktensystem durch. Über eine Verwaltung der Session-Daten je ePA-Aktensystem und Aktenkonto innerhalb eines ePA-Aktensystems stellt das Fachmodul ePA sicher, dass Logins nur für jene ePA-Aktensysteme durchgeführt und für die Zeitdauer der Gültigkeit gespeichert werden, zu denen ein Nutzer explizite Aktionen der Dokumentenverwaltung über das Primärsystem triggert. Mit der Authentifizierungsbestätigung wird die Autorisierung in der Komponente „Autorisierung“ geprüft und bei Gültigkeit der Berechtigung der Leistungserbringerinstitution das empfängerverschlüsselte Schlüsselmaterial heruntergeladen. Anschließend wird mittels Autorisierungsbestätigung das Öffnen des Aktenkontextes in der Komponente „Dokumentenverwaltung“ für das Aktenkonto des Versicherten durchgeführt.
Nachbedingung	-

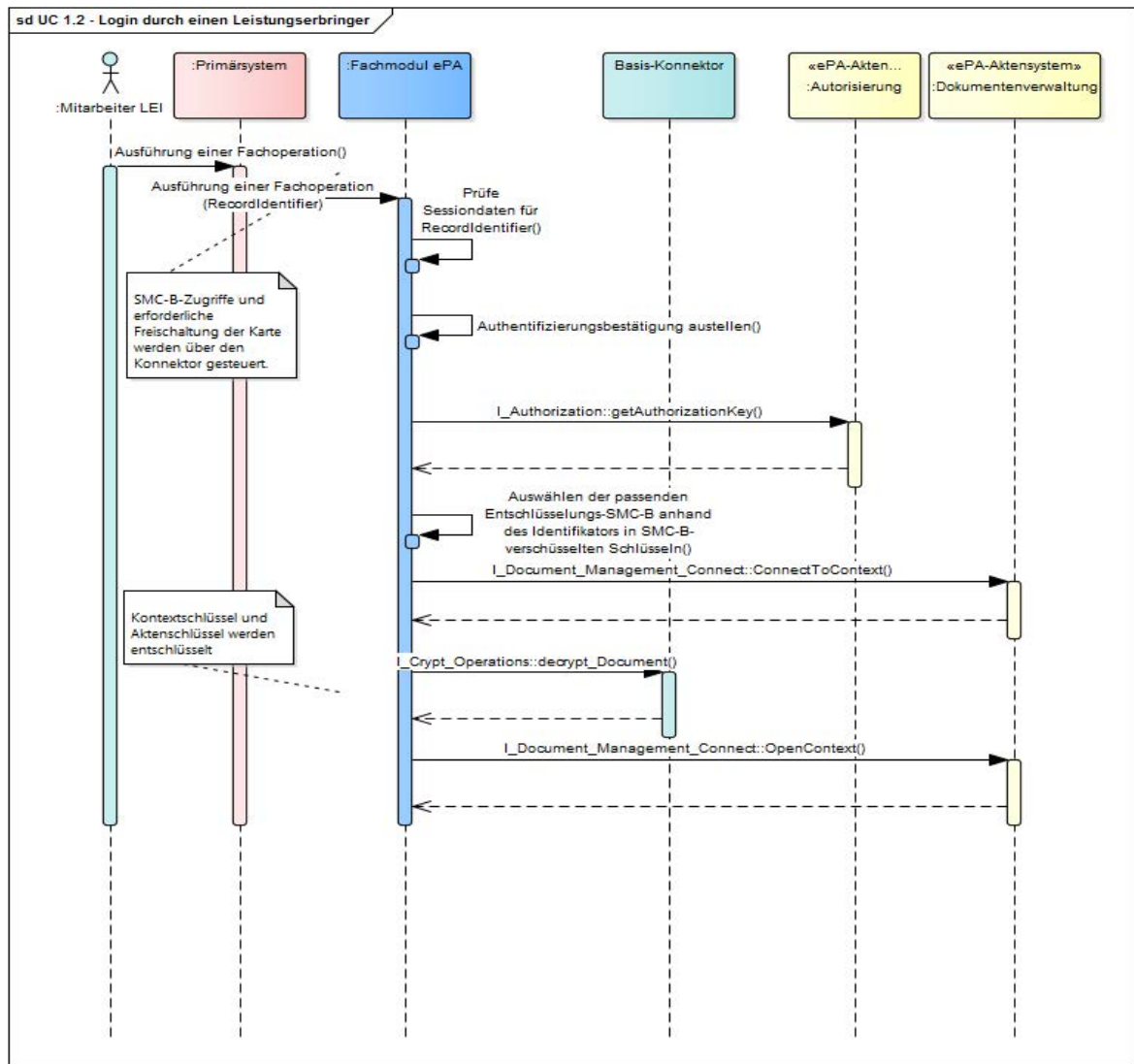


Abbildung 9: Login durch einen Leistungserbringer

[<=]

3.4.3 Logout durch einen Nutzer

Mit einem Logout wird eine Session eines Nutzers beendet. Dies kann explizit auf Nutzerwunsch oder implizit mittels Timeout erfolgen. Im ePA-Aktenystem werden die Sessondaten des Nutzers gelöscht, insbesondere in der Komponente Dokumentenverwaltung werden alle temporär entschlüsselten Metadaten, Protokolle und Policydateien kontextverschlüsselt gespeichert und zusammen mit dem Kontextschlüssel aus dem Arbeitsspeicher gelöscht, womit der Aktenkontext für ein Aktenkonto eines Versicherten geschlossen wird. Das Schließen des Aktenkontextes erfolgt dabei nur, wenn kein weiterer Nutzer über eine aktive Session in diesem Aktenkontext verfügt.

EPA-EPF-A_0010 - Impliziter Logout nach Inaktivität eines Nutzers

Das Fachmodul ePA, das Frontend des Versicherten, die Komponente Zugangsgateway und die Komponente „Dokumentenverwaltung“ MÜSSEN einen impliziten Logout für ein Aktenkonto nach einem Timeout bei Inaktivität in diesem Aktenkonto starten.

[<=]

EPA-EPF-A_0011 - Expliziter Logout auf Anforderung eines Nutzers

Das Frontend des Versicherten MUSS einen expliziten Logout auf Anforderung eines Versicherten starten.

[<=]

EPA-EPF-A_0012 - Anwendungsfall „Logout durch einen Nutzer“

Alle am Anwendungsfall „Logout durch einen Nutzer“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 7: Logout durch einen Nutzer

Name	UC 1.3 - Logout durch einen Nutzer
Vorbedingung	Ein Nutzer verfügt über eine aktive Session in einem geöffneten Aktenkontext eines Aktenkontos eines Versicherten in der Komponente Dokumentenverwaltung.
Kurzbeschreibung (Außensicht)	Mit der Beendigung einer Session in einem Aktenkonto werden der Kontext eines Aktenkontos geschlossen und alle lokalen Sessiondaten inkl. der ausgestellten Authentifizierungs- und Autorisierungsbestätigung in den beteiligten Produkttypen und Komponenten gelöscht.
Nachbedingung	Ein Nutzer, dessen Sessiondaten im Zuge des impliziten oder expliziten Logouts gelöscht wurden, ist nicht mehr in der Lage, Daten, Dokumente und verschlüsseltes Schlüsselmaterial aus dem System abzurufen, da er vom System abgewiesen wird.

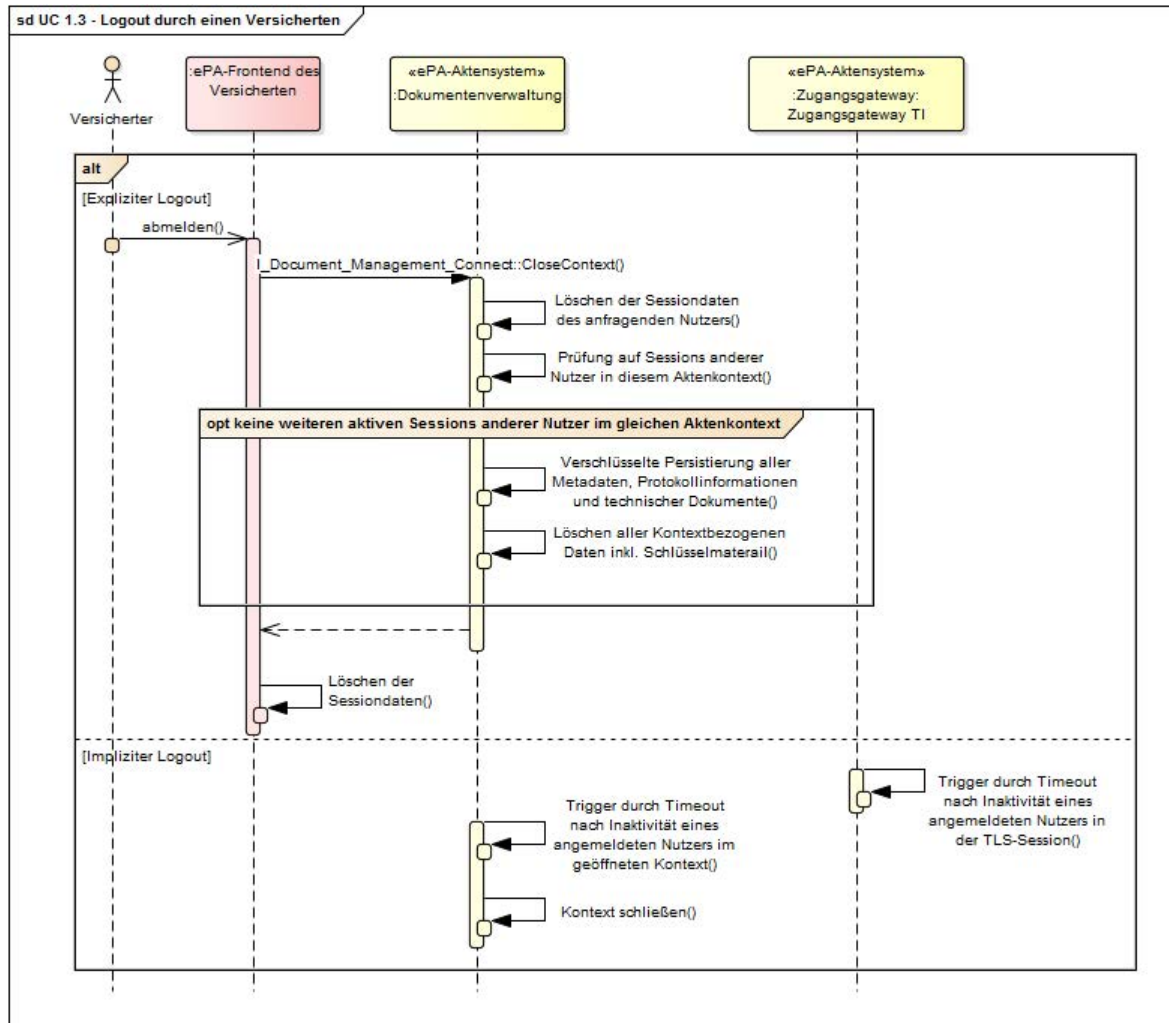


Abbildung 10: Logout durch einen Versicherten

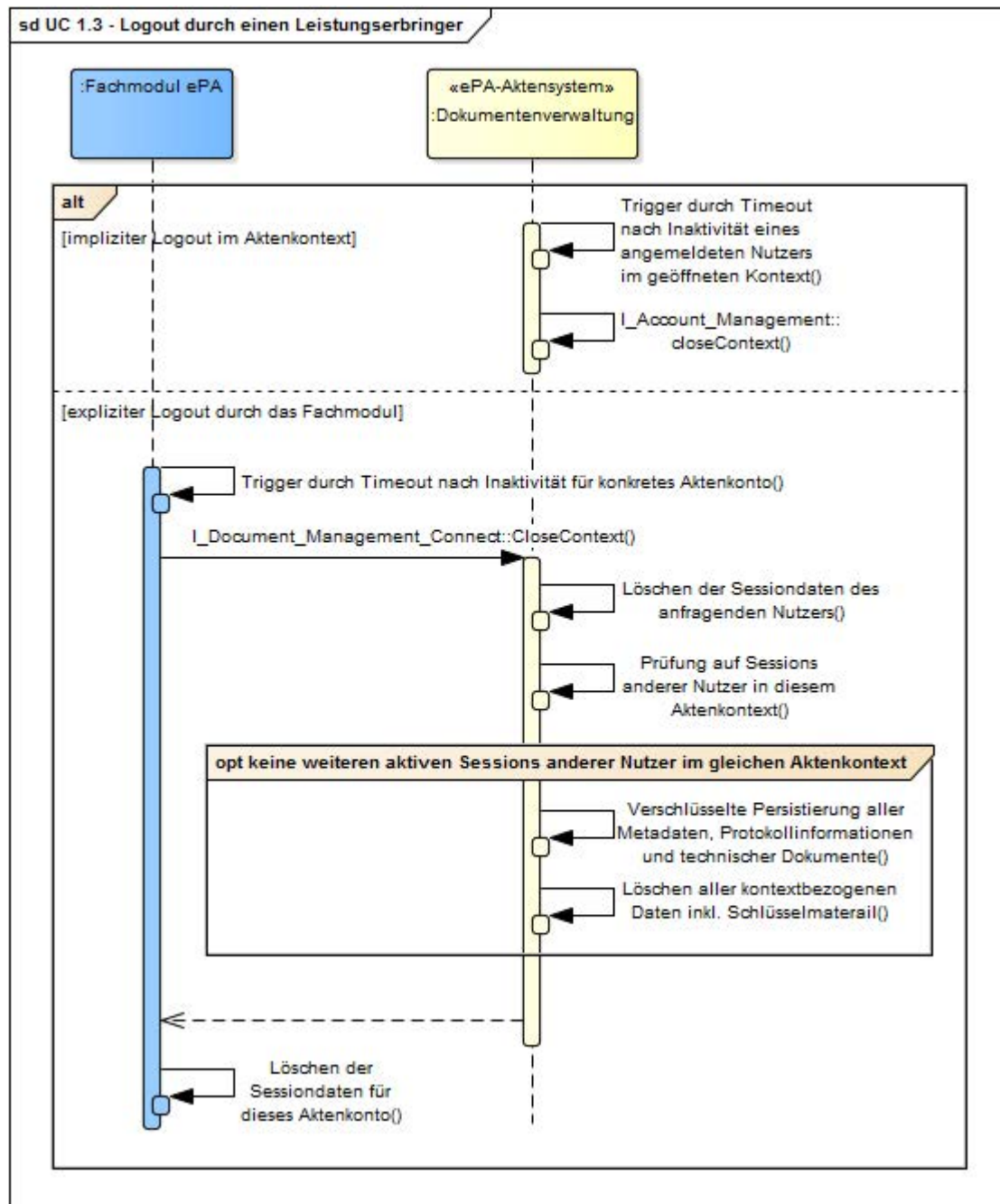


Abbildung 11: Logout in der Leistungserbringerumgebung

[<=]

3.4.4 Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren

Mit diesem Anwendungsfall aktualisiert eine Leistungserbringerorganisation unabhängig von der Anwesenheit von Versicherten ihre eigenen, bestehenden Berechtigungen in den Aktenkonten von Versicherten. Die Aktualisierung besteht in der Aktualisierung des hinterlegten, für eine oder mehrere SMC-Bs verschlüsselten Schlüsselmaterials für den Zugriff je Aktenkonto eines Versicherten.

Eine Leistungserbringereinrichtung kann über mehrere SMC-Bs verfügen. Mit diesem Anwendungsfall erfolgt pro Aktenkonto eines Versicherten eine Umschlüsselung des kryptografischen Schlüsselmaterials von einer vorhandenen, zur Entschlüsselung eingesetzten SMC-B für alle öffentlichen Schlüssel der für die Telematik-ID im VZD hinterlegten ENC-Zertifikate der SMC-Bs der Leistungserbringereinrichtung.

Sollte die Leistungserbringereinrichtung bestehende Berechtigungen für SMC-Bs mit unterschiedlichen Telematik-IDs besitzen, so muss dieser Anwendungsfall separat für die SMC-Bs der einzelnen Telematik-IDs durchgeführt werden. Bei einem Wechsel der SMC-B mit gleichzeitigem Wechsel der Telematik-ID muss eine neue Berechtigung durch den Versicherten erteilt werden (siehe UC 3.7 - Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern oder UC 3.1 - Berechtigung durch einen Versicherten vergeben).

Die Vergabe von Zugriffsberechtigungen an eine Leistungserbringereinrichtung kann ohne Einbeziehung des VZD immer erfolgen, in dem der Versicherte in der Umgebung der Leistungserbringer eine Ad-hoc-Berechtigung vergibt (siehe UC 3.7 - Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern).

EPA-EPF-A_0013 - Anwendungsfall „Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren“

Alle am Anwendungsfall „Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 8: Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren

Name	UC 1.4 - Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren
Vorbedingung	Im Verzeichnisdienst (VZD) müssen alle gültigen, zu verwendenden Zertifikate der Leistungserbringereinrichtung der betrachteten Telematik-ID registriert sein. Auch SMC-Bs der Leistungserbringereinrichtung, die bisher nicht in Berechtigungen ePA hinterlegt wurden, nun aber zu registrieren sind, müssen dem VZD bekannt sein. Die Telematik-ID der Leistungserbringereinrichtung hat sich nicht geändert. Zudem ist dem Primärsystem (PS) bekannt, bei welchen ePA-Aktensystemen eine Autorisierung für die eigene(n) SMC-B(s) hinterlegt ist. Dies kann bspw. bei der erstmaligen Ermittlung eines RecordIdentifiers im Rahmen einer Ad-hoc-Berechtigung abgeleitet werden.
Kurzbeschreibung (Außensicht)	Ein Mitarbeiter der Leistungserbringereinrichtung fordert über das PS das Aktualisieren der kryptografischen Berechtigungen in den Aktenkonten der Versicherten an. Da eine Leistungserbringereinrichtung über mehrere SMC-Bs zu einer Telematik-ID verfügen kann, erfolgt eine Identifizierung der je Karten-Identität verschlüsselten Schlüssel über einen Identifikator des ENC-Zertifikats der jeweiligen SMC-B.
Nachbedingung	Alle bestehenden Berechtigungen der Leistungserbringereinrichtung in Aktenkonten der Versicherten bei ihren jeweiligen Anbietern sind für alle gültigen SMC-

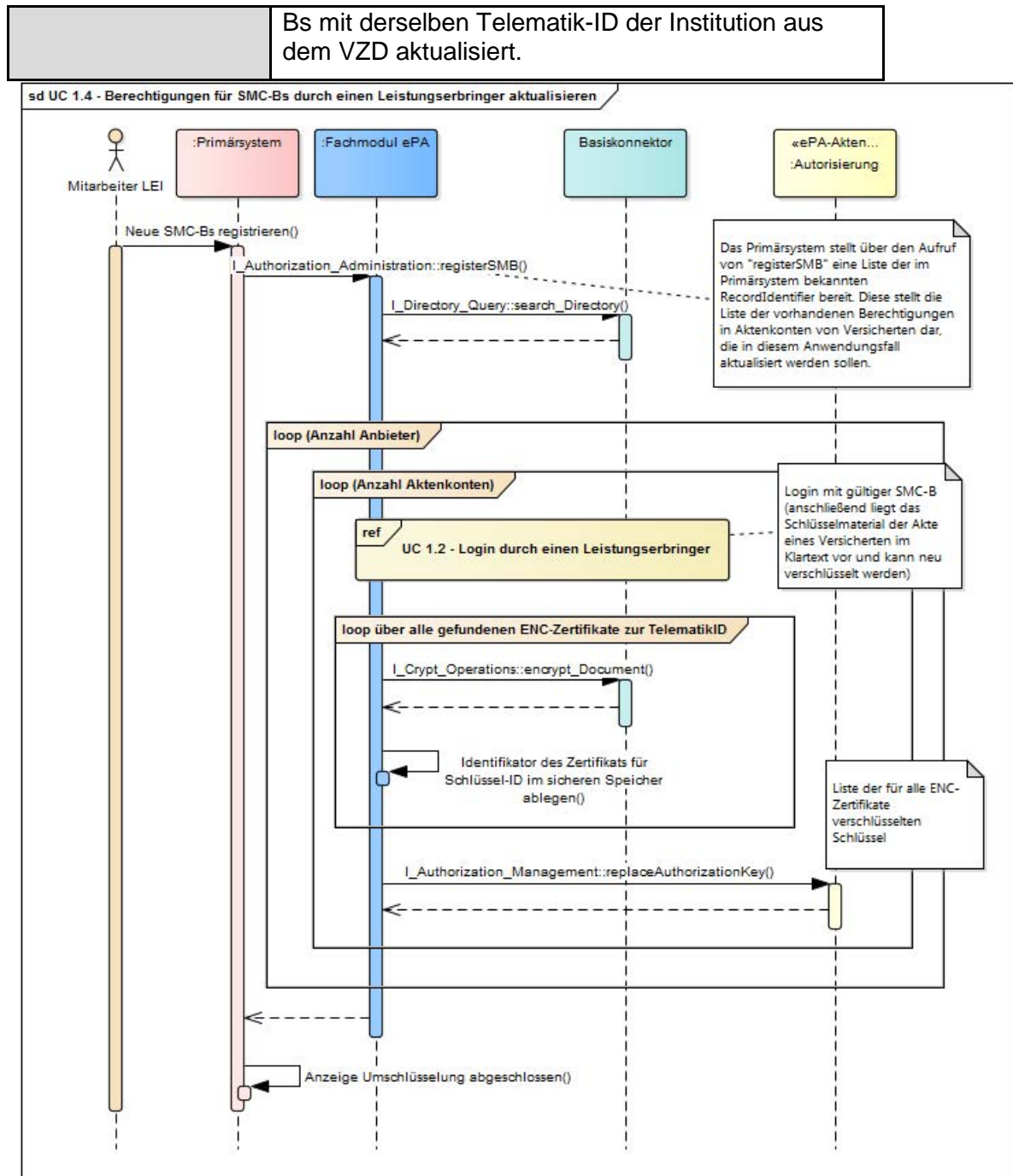


Abbildung 12: Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren

[<=]

3.4.5 Eigene Stammdaten im Verzeichnisdienst durch einen Leistungserbringer verwalten

Dieser fachliche Anwendungsfall „UC 1.5 Stammdaten im Verzeichnisdienst verwalten“ ist kein Betrachtungsgegenstand der Anwendung ePA, da die Pflege der Stammdaten einer Leistungserbringerinstitution im Verzeichnisdienst bereits über die TI-Plattform geregelt wird.

Die Pflege gewährleistet, dass bei Ausführung der Anwendungsfälle

- UC 3.1 - Berechtigung durch einen Versicherten vergeben
- UC 3.7 - Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern
- UC 1.4 - Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren

stets die aktuellen ENC-Zertifikate der im Einsatz befindlichen SMC-Bs einer zu berechtigenden Leistungserbringerinstitution gefunden werden.

Die Fachanwendung ePA geht davon aus, dass die im Verzeichnisdienst hinterlegten SMC-B-ENC-Zertifikate einer Leistungserbringerinstitution alle aktuell gültigen und im Einsatz befindlichen SMC-Bs umfassen.

3.5 Aktenkontoverwaltung

Die folgenden Anwendungsfälle beschreiben, wie ein Versicherter oder ein von ihm berechtigter Vertreter sein Aktenkonto verwalten kann. Das folgende Zustandsdiagramm verdeutlicht die möglichen Zustände eines Aktenkontos bei einem Anbieter und zeigt die möglichen Zustandsübergänge, insbesondere im Zusammenhang mit dem Umzug der Daten des Versicherten beim Wechsel des Anbieters durch den Versicherten.

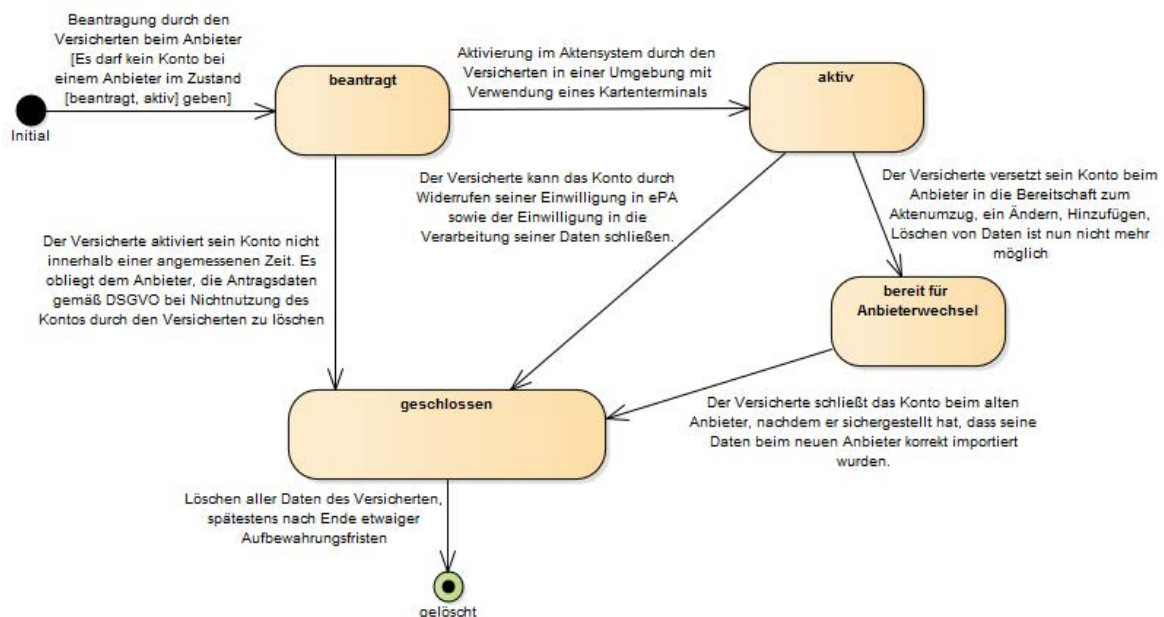


Abbildung 13: Lebenszyklus eines Kontos bei einem Anbieter

3.5.1 Aktenkonto einrichten

Die Einrichtung eines Aktenkontos erfolgt in zwei Schritten. Zunächst beantragt der Versicherte bei einem Anbieter seiner Wahl ein Aktenkonto. Art, Umfang und Wahl des Transportmediums der transportierten Informationen (Vertragsdaten, KVNR des Versicherten etc.) wählt der Anbieter ePA-Akten-System. Möglich sind z.B. webbasierte Lösungen oder auch der Postweg.

Im zweiten Schritt erfolgt die Aktivierung des Aktenkontos durch den Versicherten. In diesem Schritt ist der Einsatz der eGK des Versicherten zwingend erforderlich, um die kryptografischen Identitäten für die Authentisierung und zur Ver- und Entschlüsselung im ePA-Aktensystem bekannt zu machen.

EPA-EPF-A_0014 - Anwendungsfall „Aktenkonto einrichten“

Alle am Anwendungsfall beteiligten Produkttypen und Komponenten **MÜSSEN** die nachfolgenden Festlegungen umsetzen.

Tabelle 9: Aktenkonto einrichten

Name	UC 2.1 - Aktenkonto einrichten
Vorbedingung	Der Versicherte verfügt über eine gültige eGK und eine eindeutige KVNR.

Kurzbeschreibung (Außensicht)	<p>Die Einrichtung des Aktenkontos erfolgt in zwei Schritten.</p> <p><u>Schritt 1:</u> Der Versicherte eröffnet ein Aktenkonto bei einem Anbieter ePA-Aktensystem in einem Initialisierungsschritt mittels Eingabe seiner Vertragsdaten, Einwilligungserklärung ePA und Zustimmung zur Datenverarbeitung gegenüber dem Anbieter. Der Anbieter informiert den Versicherten über die Anwendungen ePA entsprechend den Anforderungen der DSGVO. Nach erfolgreicher Initialisierung und Prüfung auf ein bereits bestehendes Aktenkonto zur KVNR des Versicherten und der optionalen Verwendung des Benachrichtigungskanals (E-Mail) erhält der Versicherte den RecordIdentifier und alle notwendigen Vertragsunterlagen.</p> <p><u>Schritt 2 (LE-Umgebung):</u> Der Aktivierungsschritt kann in der Leistungserbringenumgebung erfolgen, wo der Leistungserbringer eine Identitätsprüfung für eGK und Versicherten vornimmt und den Aktivierungsprozess über das Primärsystem anstößt. Dazu übermittelt er das Primärsystem den RecordIdentifier des Versicherten aus dem unveränderlichen Teil der KVNR des Versicherten sowie über die Operation <code>PHRManagementService::GetHomeCommunityID</code> suchen lassen. Der Versicherte bzw. sein bevollmächtigter Vertreter bestätigt die Einwilligung und Aktivierung mittels PIN-Eingabe für die eGK des Versicherten am eHealth-Kartenterminal. Alle konfigurierbaren Parameter werden durch die Komponenten des ePA-Aktensystems mit Standardwerten belegt.</p> <p><u>Schritt 2 (Umgebung des Versicherten mit Kartenlesegerät):</u> Verfügt der Versicherte über ein Kartenlesegerät, kann er den Schritt der Kontoaktivierung in seiner privaten Umgebung vornehmen. Das Schlüsselmaterial des Aktenkontos wird lokal erzeugt. Alle konfigurierbaren Parameter werden durch die Komponenten des ePA-Aktensystems mit Standardwerten belegt.</p>
Nachbedingung	<p>Der Versicherte ist in der Lage Dokumente in ePA zu suchen und kann Leistungserbringern in seiner Umgebung Berechtigungen einrichten sowie diese ad hoc in der Praxis berechtigen.</p>

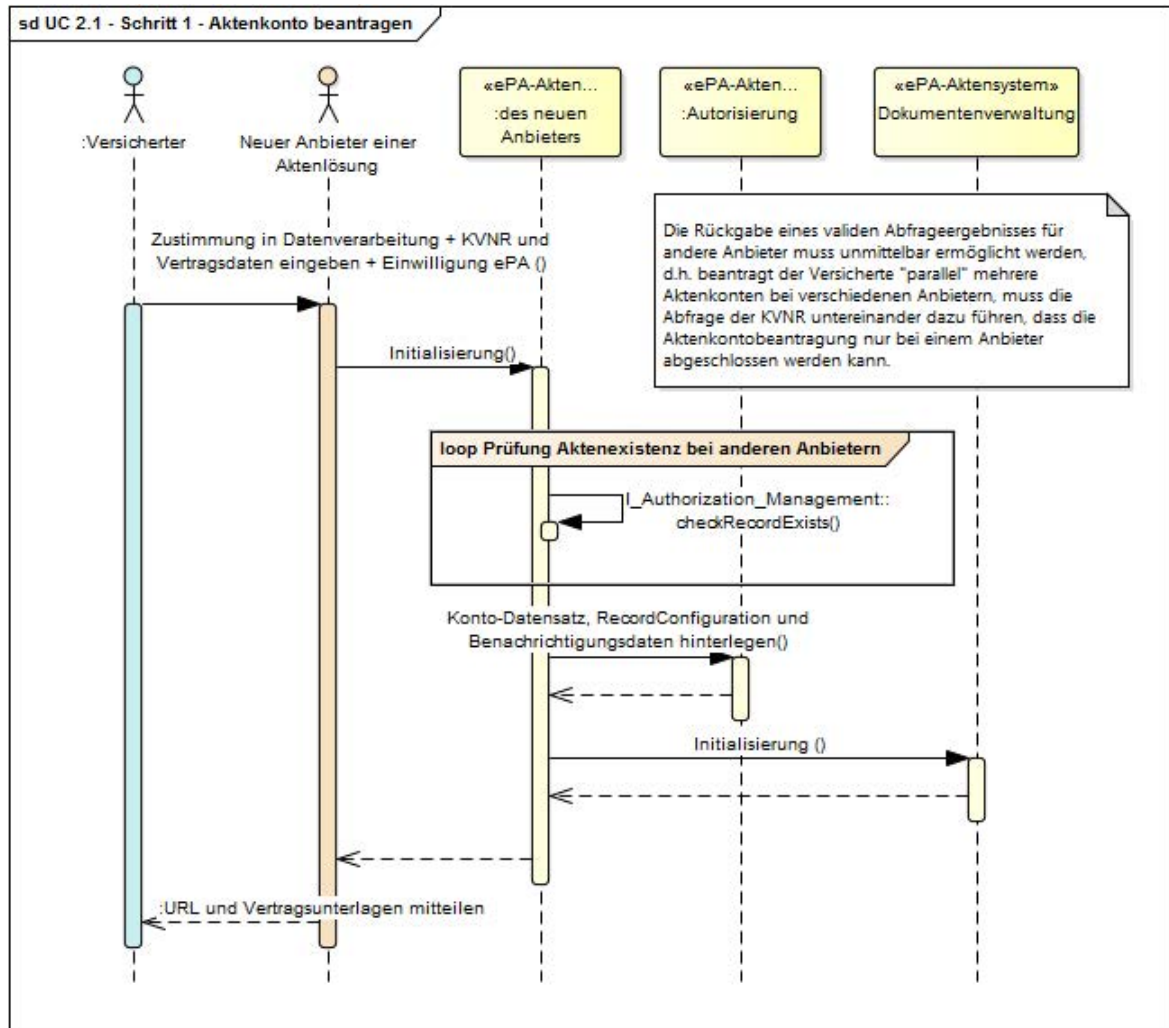


Abbildung 14: Schritt 1 – Aktenkonto beantragen

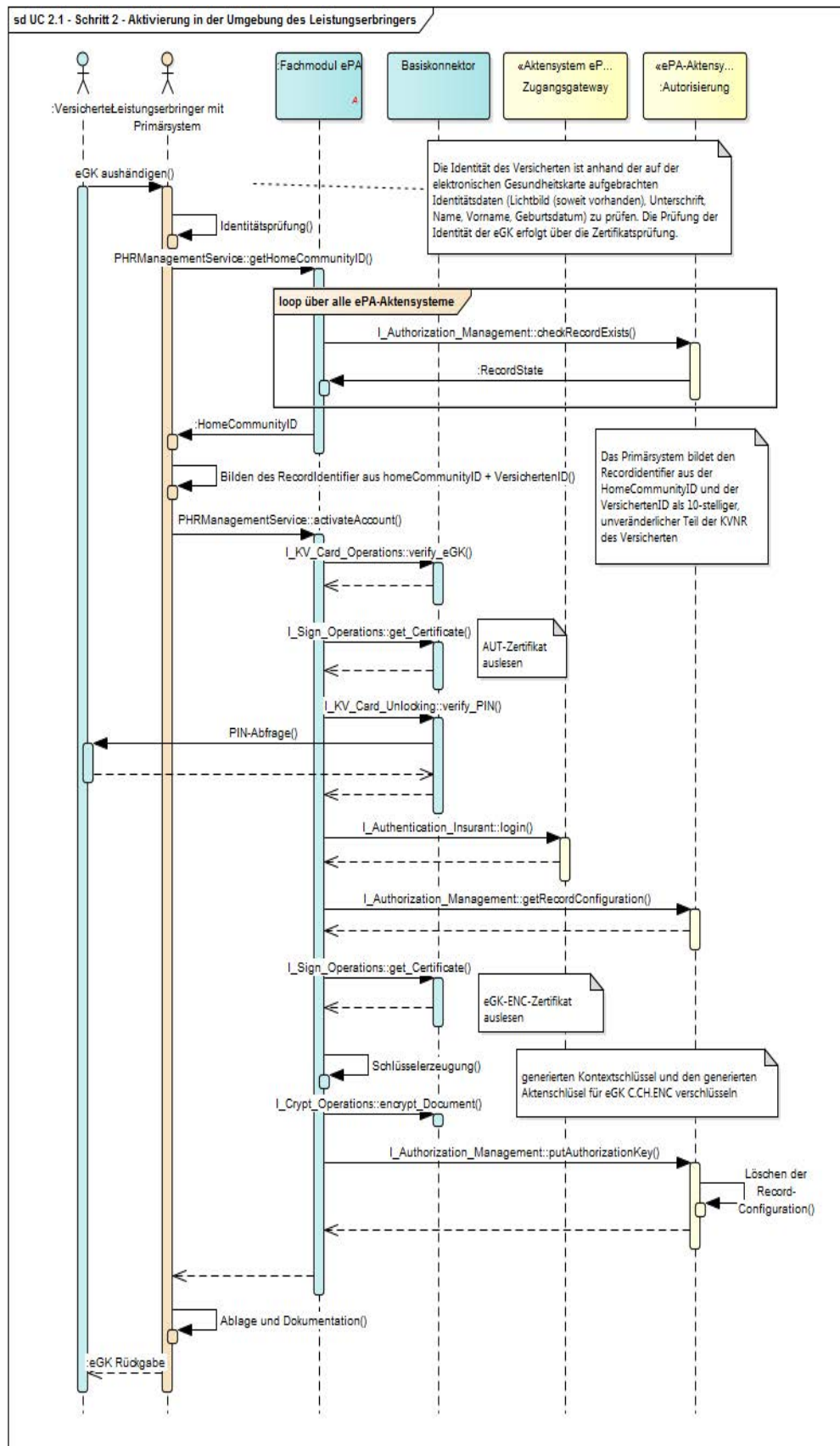


Abbildung 15: Schritt 2 – Aktivierung in der Umgebung des Leistungserbringers

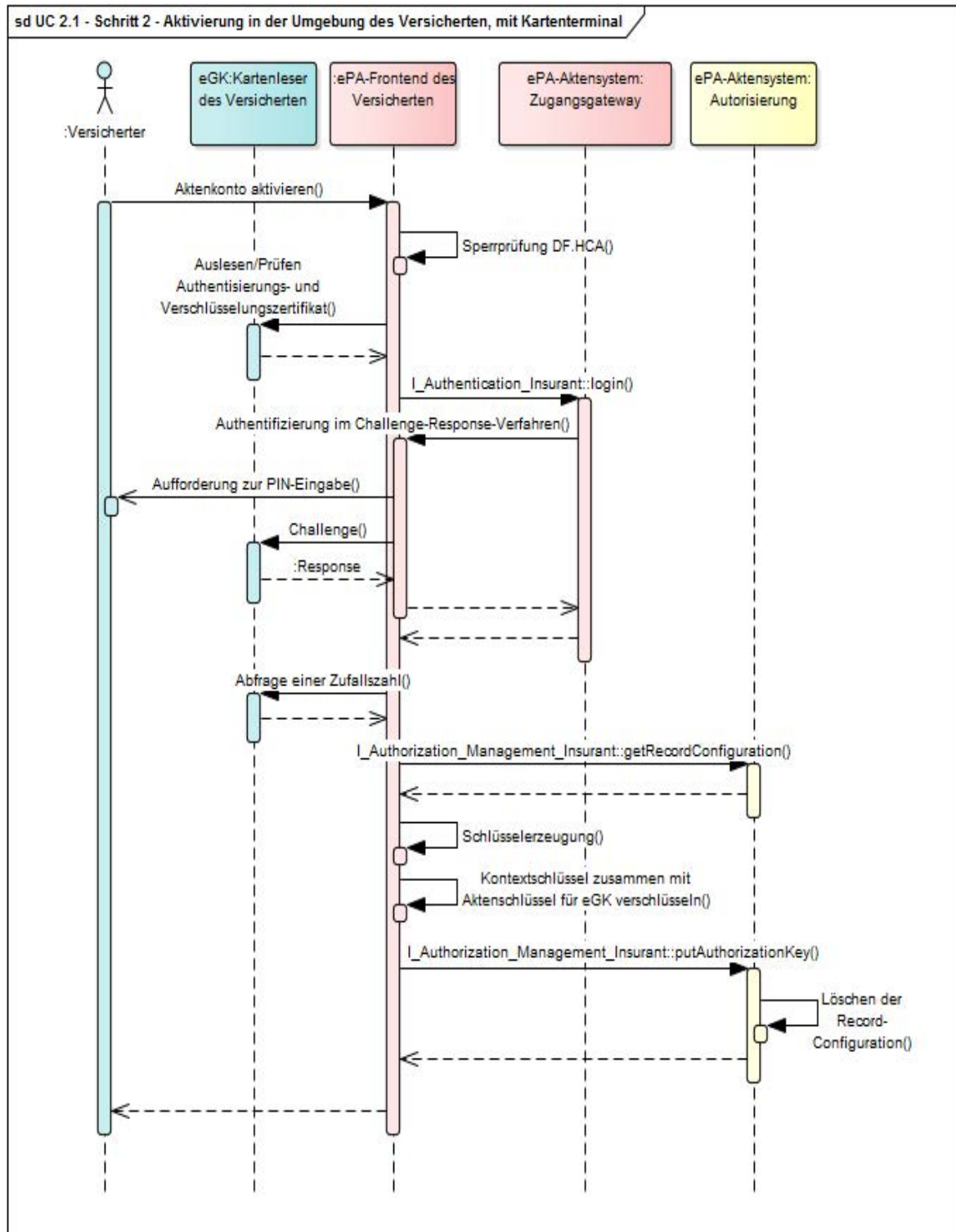


Abbildung 16: Schritt 2 – Aktivierung in der Umgebung des Versicherten, mit Kartenterminal

[<=]

Ein Schriftformerfordernis für die Einwilligung in ePA besteht weder durch die DSGVO i.V.m. BDSG (neue Fassung) noch durch den § 291a SGB V.

EPA-EPF-A_0015 - Schlüsselmaterial für Berechtigungserhalt

Das ePA-Frontend des Versicherten MUSS ein Verfahren bereitstellen, mit dem ein Versicherter das kryptografische Schlüsselmaterial des AuthorizationKey seines Aktenkontos exportieren und sicher verwahren, sowie im Wiederherstellungsfall für einen Berechtigungserhalt nutzen kann.

[<=]

Es obliegt dem Hersteller des ePA-Frontends des Versicherten, dem Versicherten geeignete Exportformate anzubieten, die der Versicherte über die Peripherie des Geräts des Versicherten in das ePA-Frontend des Versicherten wieder einbringen kann.

EPA-EPF-A_0016 - Zustimmungseinholung

Der Anbieter ePA-Aktensystem MUSS im Rahmen der Eröffnung des Aktenkontos die Zustimmung zur Datenverarbeitung vom Versicherten einholen.

[<=]

3.5.2 Vertragsdaten ändern

Dem Anbieter ePA-Aktensystem obliegt es, Abrechnungsdaten o. Ä. über separate, selbst gewählte Schnittstellen vom Versicherten oder von einem von ihm berechtigten Vertreter ändern zu lassen, z.B. via Webformular, per Post oder Telefon-Hotline.

EPA-EPF-A_0317 - Vertragsdaten ändern

Der Anbieter ePA-Aktensystem MUSS es dem Versicherten ermöglichen, seine Vertragsdaten zu ändern. Hierzu gehört auch der Widerruf der Einwilligung.

[<=]

A_13803 - Ausschluss einer Änderung der KVNR im Aktenkonto

Der Anbieter ePA-Aktensystem MUSS verhindern, dass die KVNR des Versicherten im ePA-Aktensystem geändert werden kann.[<=]

3.5.3 Aktenkonto schließen

Mit diesem Anwendungsfall schließt der Versicherte sein Aktenkonto bei seinem Anbieter. Nach Abschluss des Anwendungsfalls kann der Versicherte sich nicht mehr in seinem Aktenkonto anmelden, ebenso keine der ehemals berechtigten Leistungserbringerinstitutionen. Der Anbieter des ePA-Aktensystems, bei dem der Versicherte sein Konto geführt hat, löscht alle Daten und Dokumente des Aktenkontos des Versicherten gemäß DSGVO und abhängig von etwaigen Aufbewahrungsfristen für nachweispflichtige Informationen.

Der Versicherte hat vor dem Schließen seines Aktenkontos die Möglichkeit der Sicherung aller Dokumente seines Aktenkontos auf einem lokalen Datenträger, in dem er folgende Anwendungsfälle vor dem Schließen ausführt.

1. UC 1.1 - Login durch einen Versicherten
2. UC 4.4 - Dokumente durch einen Versicherten suchen
3. UC 4.10 - Dokumente durch einen Versicherten anzeigen

A_15680 - Anwendungsfall „Aktenkonto schließen“

Der Anbieter eines ePA-Aktensystems MUSS es dem Versicherten auf geeignetem Weg ermöglichen, sein Konto auf Verlangen zu kündigen und zu schließen.[<=]

EPA-EPF-A_0318 - Vertragsdaten löschen beim Schließen des Kontos

Der Anbieter ePA-Aktensystem MUSS sicherstellen, dass beim Schließen des Aktenkontos durch den Versicherten alle Daten über das Vertragsverhältnis nach Ablauf etwaiger Aufbewahrungsfristen ebenfalls gelöscht werden.

[<=]

3.5.4 Anbieter wechseln

Ein Versicherter kann mit diesem Anwendungsfall den Anbieter seines Aktenkontos wechseln und alle Inhalte zu einem neuen Anbieter übertragen. Hierfür wird das bestehende Aktenkonto suspendiert, zu einem neuen Anbieter migriert und anschließend gelöscht.

EPA-EPF-A_0019 - Anwendungsfall „Anbieter wechseln“

Alle am Anwendungsfall beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 10: Anbieter wechseln

Name	UC 2.5 - Anbieter wechseln
Vorbedingung	-
Kurzbeschreibung (Außensicht)	<p>Der Versicherte möchte den Anbieter ePA-Aktensystem für sein Aktenkonto wechseln. Hierzu versetzt er das Aktenkonto beim alten Anbieter in den Zustand „bereit für Anbieterwechsel“. Sämtliche Daten werden in ein Exportpaket verpackt, das mit dem Kontextschlüssel verschlüsselt und zum Download durch den neuen Anbieter bereitgestellt wird.</p> <p>Der Versicherte eröffnet anschließend ein neues Konto beim neuen Anbieter gemäß Use Case „Aktenkonto einrichten“ und lässt seine Daten inkl. der bestehenden Berechtigungen vom neuen Anbieter importieren. Sollte der Anbieterwechsel im Zusammenhang mit einem Kassenwechsel und einem damit verbundenen eGK-Wechsel stehen, kann der Versicherte wahlweise die neue eGK bereits bei seinem bisherigen Aktenkonto bekannt machen oder die alte eGK einmalig zur Entschlüsselung des bisherigen Schlüsselmaterials beim neuen Aktenkonto einsetzen.</p>
Nachbedingung	<p>Ein bisher berechtigter Leistungserbringer kann auf Daten und Dokumente des Versicherten beim neuen Anbieter zugreifen, wenn er das Aktenkonto des Versicherten vor dem Zugriff beim neuen Anbieter (über Abfrage des neuen Anbieters im Primärsystem via KVNR mittels <code>PHRManagementService::GetHomeCommunityID</code>) lokalisiert.</p> <p>Dem Vertreter oder den Vertretern des Versicherten muss der Versicherte den Namen (bzw. URL) des neuen Anbieters mitteilen. Sowohl Versicherte als auch Vertreter müssen ihre jeweils genutzten Geräte</p>

	im Rahmen des Logins erneut am Aktensystem bekannt machen.
--	--

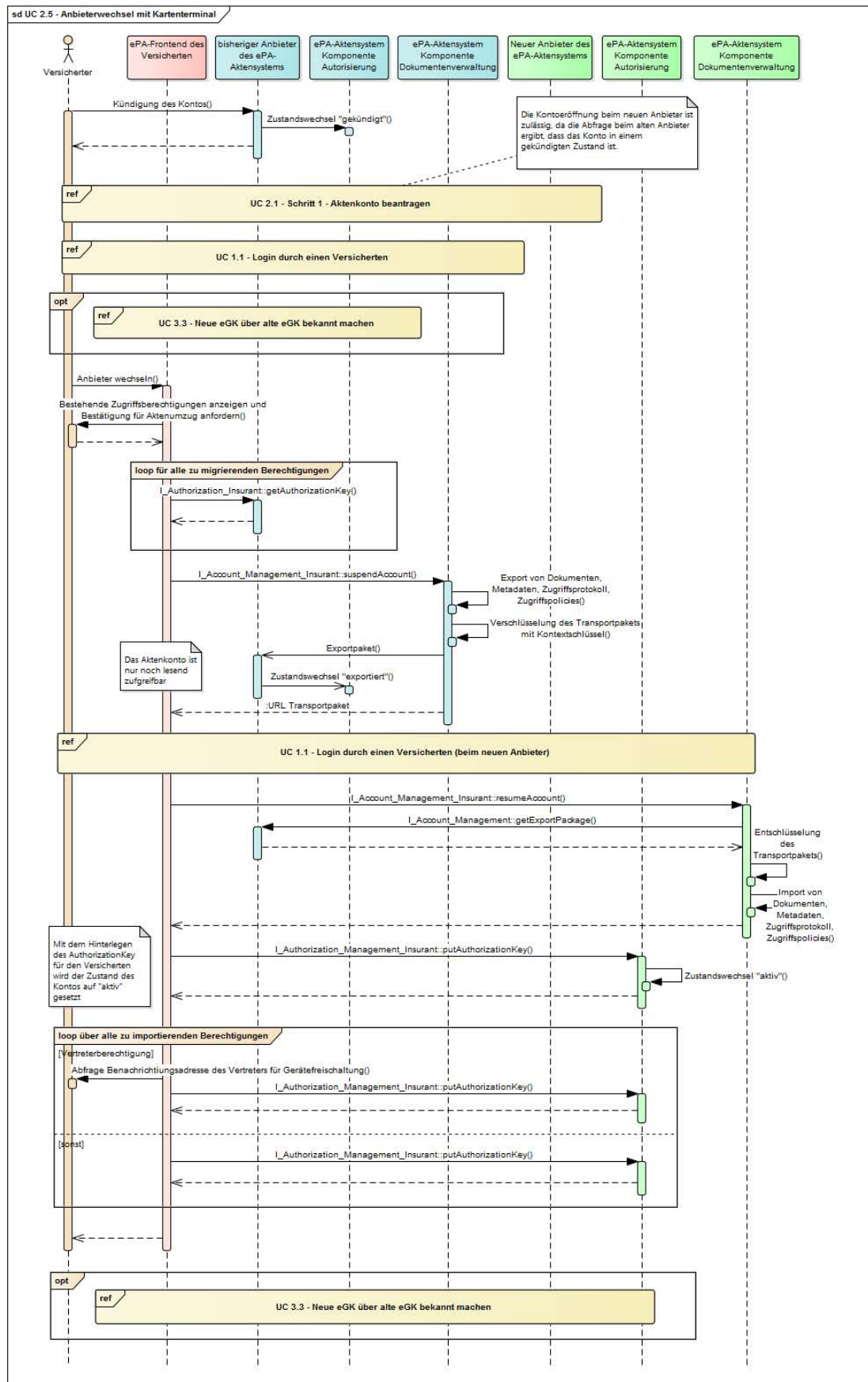


Abbildung 17 : Anbieter wechseln

[<=]

3.6 Berechtigungsverwaltung

3.6.1 Berechtigung durch einen Versicherten vergeben

Mit diesem Anwendungsfall richtet ein Versicherter oder ein von ihm berechtigter Vertreter Zugriffsberechtigungen für Leistungserbringerinstitutionen ein. Bei der Berechtigungsvergabe kann der Versicherte oder ein von ihm berechtigter Vertreter auswählen, ob die Leistungserbringerinstitution nur Zugriff auf Dokumente erhalten soll, die von Leistungserbringerinstitutionen eingestellt wurden (LE-Dok) oder zusätzlich auch auf Dokumente, die vom Versicherten oder einem von ihm berechtigten Vertreter eingestellt wurden (Vers-Dok). Auch die Dauer der Berechtigung wird an dieser Stelle festgelegt. Die Verwaltung der Berechtigungen (Ändern, Zeitraum verlängern, Berechtigung entziehen) erfolgt über den Anwendungsfall UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten.

EPA-EPF-A_0020 - Anwendungsfall „Berechtigung durch einen Versicherten vergeben“

Alle am Anwendungsfall „Berechtigung durch einen Versicherten vergeben“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 11: Berechtigung durch einen Versicherten vergeben

Name	UC 3.1 - Berechtigung durch einen Versicherten vergeben
Vorbedingung	Die zu berechtigende Leistungserbringerinstitution ist im VZD angelegt und gepflegt, d.h., verfügt über Attribute (Name, Adresse etc.), die der Versicherte durchsuchen kann.
Kurzbeschreibung (Außensicht)	Ein Versicherter bzw. sein Vertreter wählt eine zu berechtigende Leistungserbringerinstitution aus dem Verzeichnisdienst der TI-Plattform aus. Der Versicherte bzw. sein Vertreter wählt die gewünschte Berechtigungsregel aus (LE-Dok LE-Dok + Vers-Dok) und -dauer (1 Tag, 28 Tage [default], 18 Monate oder flexibel 1 bis 540 Tage) aus. Der Versicherte bzw. sein Vertreter bestätigt die Hinterlegung der Zugriffsberechtigung im System.
Nachbedingung	Die vom Versicherten berechnete LEI kann gemäß Konfiguration des Versicherten Dokumente in ePA einstellen und sofern vorhanden, Dokumente suchen, sich anzeigen lassen und auf Wunsch oder Verlangen des Versicherten löschen.

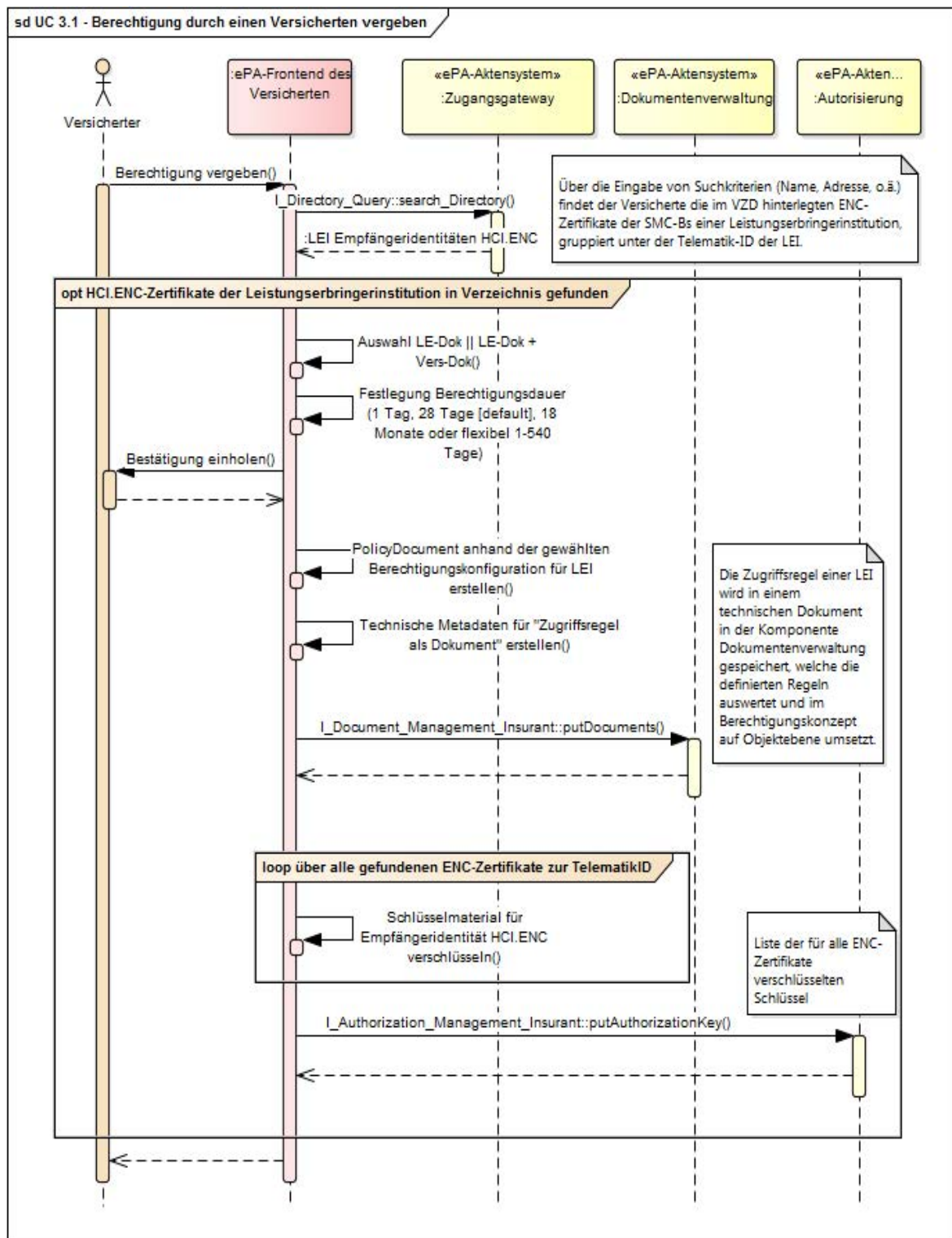


Abbildung 18: Berechtigung durch einen Versicherten vergeben

[<=]

3.6.2 Vertretung durch einen Versicherten einrichten

Mit diesem Anwendungsfall richtet ein Versicherter eine Zugriffsberechtigung für einen Vertreter ein. Dieser Vertreter muss über eine eigene eGK und PIN verfügen. Die Verwaltung der Berechtigungen (Ändern, Berechtigung entziehen) erfolgt über den Anwendungsfall *UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten*.

EPA-EPF-A_0021 - Anwendungsfall „Vertretung durch einen Versicherten einrichten“

Alle am Anwendungsfall „Vertretung durch einen Versicherten einrichten“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 12: Vertretung durch einen Versicherten einrichten

Name	UC 3.2 - Vertretung durch einen Versicherten einrichten
Vorbedingung	Vertreter und Versicherter befinden sich gemeinsam an einem ePA-Frontend des Versicherten Der Vertreter kann über ein Aktenkonto bei einem beliebigen Anbieter verfügen, es ist jedoch keine Voraussetzung für diesen Anwendungsfall und es wird mit diesem Anwendungsfall auch kein Aktenkonto für den Vertreter eingerichtet.
Kurzbeschreibung (Außensicht)	Ein Versicherter richtet eine Vertretung durch Stecken der eGK des Vertreters in das Kartenlesegerät ein. Der Vertreter bestätigt seine Anwesenheit mit der Eingabe seiner PIN. Der Versicherte wählt aus, ob der Vertreter nur für den Berechtigungserhalt oder auch für den Zugriff auf die Dokumente berechtigt werden soll und bestätigt die Hinterlegung der Zugriffsberechtigung im System. Der Versicherte teilt dem Vertreter den zu verwendenden RecordIdentifier mit, für den sich der Vertreter zur Wahrnehmung der Vertretung anmelden muss. Der Versicherte hinterlegt für den berechtigten Vertreter, dessen E-Mail-Adresse für die Gerätefreischaltung als Benachrichtigungskanal.

Nachbedingung	<p>Der berechtigte Vertreter ist, wenn der Zugriff auf die Dokumente erlaubt wurde, über sein ePA-Frontend des Versicherten und mittels seines Kartenlesers in der Lage, in Abwesenheit des Versicherten die nachfolgenden Anwendungsfälle auszuführen:</p> <ul style="list-style-type: none"> • Vertretung für einen Versicherten wahrnehmen • Protokolle einsehen • Benachrichtigungen innerhalb der Fachanwendung verwalten • Berechtigung für LEI vergeben • Ad-hoc-Berechtigung für LEI einholen • Liste der Zugriffsberechtigten anzeigen • Berechtigung entziehen • Dokument einstellen – Versicherter • Dokumente suchen – Versicherter • Dokumente anzeigen Versicherter • Dokumente herunterladen – Versicherter • Dokumente löschen – Versicherter • Neue eGK des zu vertretenden Versicherten über Vertreter bekannt machen • Liste der Vertretungen anzeigen (ich bin Vertreter für) <p>Wenn der Vertreter nur für den Berechtigungserhalt berechtigt wurde, dann ist der Vertreter über sein ePA-Frontend des Versicherten und mittels seines Kartenlesers in der Lage, den folgenden Anwendungsfall auszuführen:</p> <ul style="list-style-type: none"> • Neue eGK des zu vertretenden Versicherten über Vertreter bekannt machen
----------------------	---

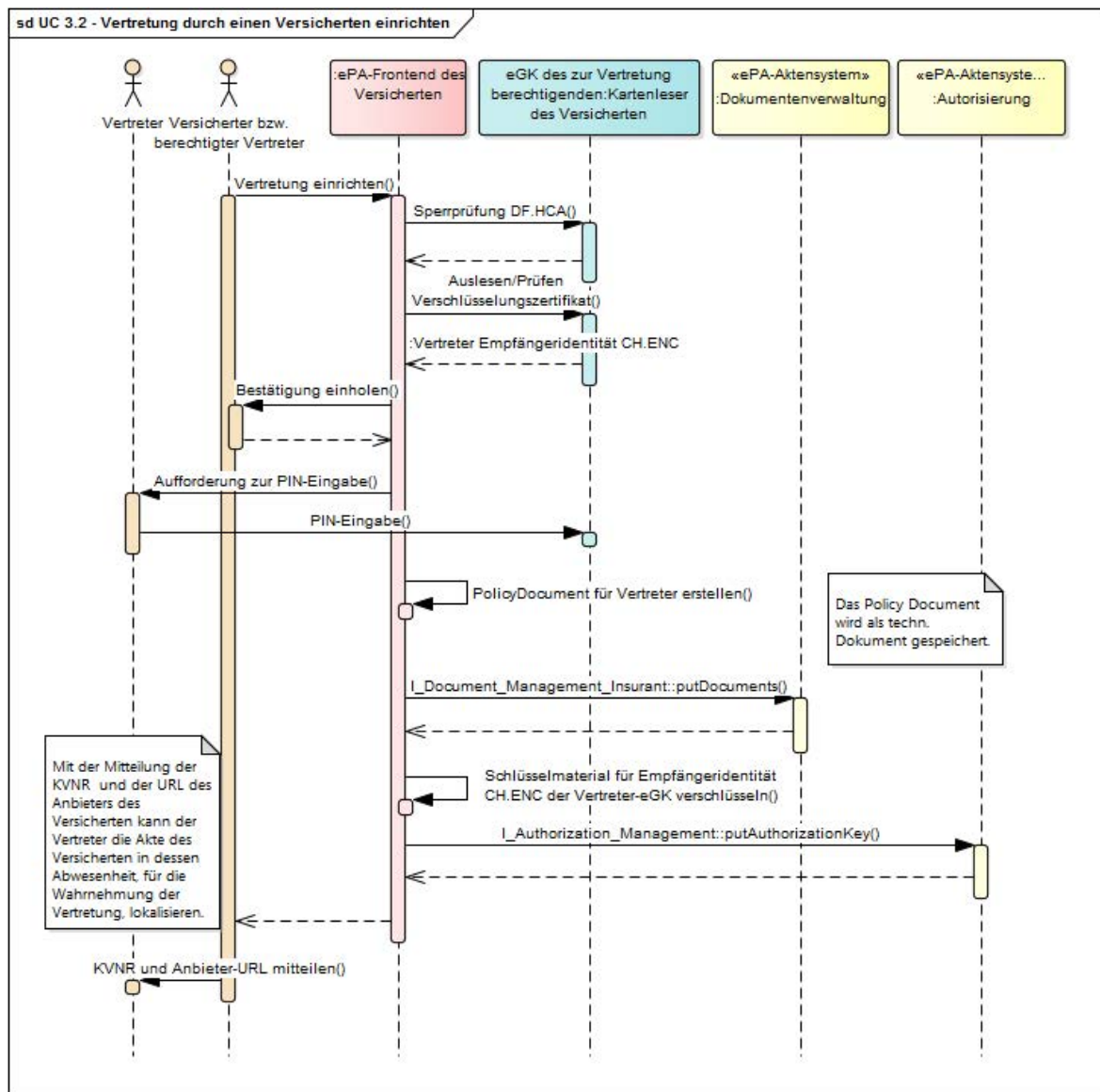


Abbildung 19: Vertretung durch einen Versicherten einrichten

[<=]

3.6.3 Neue eGK über alte eGK bekannt machen

Mit diesem Anwendungsfall wird eine neue eGK mit Hilfe einer alten eGK im System registriert. Hierbei werden auch kryptografisch gesicherte Informationen für die neue eGK erneut verschlüsselt.

EPA-EPF-A_0022 - Anwendungsfall „Neue eGK über alte eGK bekannt machen“

Alle am Anwendungsfall „Neue eGK über alte eGK bekannt machen“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 13: Neue eGK über alte eGK bekannt machen

Name	UC 3.3 - Neue eGK über alte eGK bekannt machen
Vorbedingung	<p>Die PUK der alten eGK des Versicherten ist nicht gesperrt, d. h., das kryptografische Schlüsselmaterial der alten eGK kann genutzt werden.</p> <p>Für den Fall, dass ein Vertreter kein eigenes Aktenkonto führt, muss der UC im Frontend des Versicherten ohne spezifisches Login in ein eigenes Aktenkonto erreichbar sein. Ein Durchlaufen des Prozess erfolgt dann lediglich für die Aktenkonten der zu vertretenden Versicherten.</p>
Kurzbeschreibung (Außensicht)	<p>Ein mittels neuer eGK authentifizierter Versicherter wählt das Wechseln seiner eGK als Anwendungsfall aus. Dazu steckt er seine alte eGK in das Kartenlesegerät, um das für die alte eGK verschlüsselte Schlüsselmaterial zu entschlüsseln. Der Versicherte bestätigt den Wunsch zum Kartenwechsel. Das für die neue eGK verschlüsselte Schlüsselmaterial ersetzt die kryptografische Berechtigung der alten eGK im ePA-Aktensystem.</p> <p>Ist der Prozess für das eigene Aktenkonto abgeschlossen, prüft das Frontend des Versicherten, ob für den Versicherten Vertretungen eingetragen sind. Ist dies der Fall, wird der UC für jedes einzelne Vertretungskonto erneut durchlaufen.</p>
Nachbedingung	Berechtigung für die neue eGK im Aktenkonto des Versicherten ist eingerichtet.

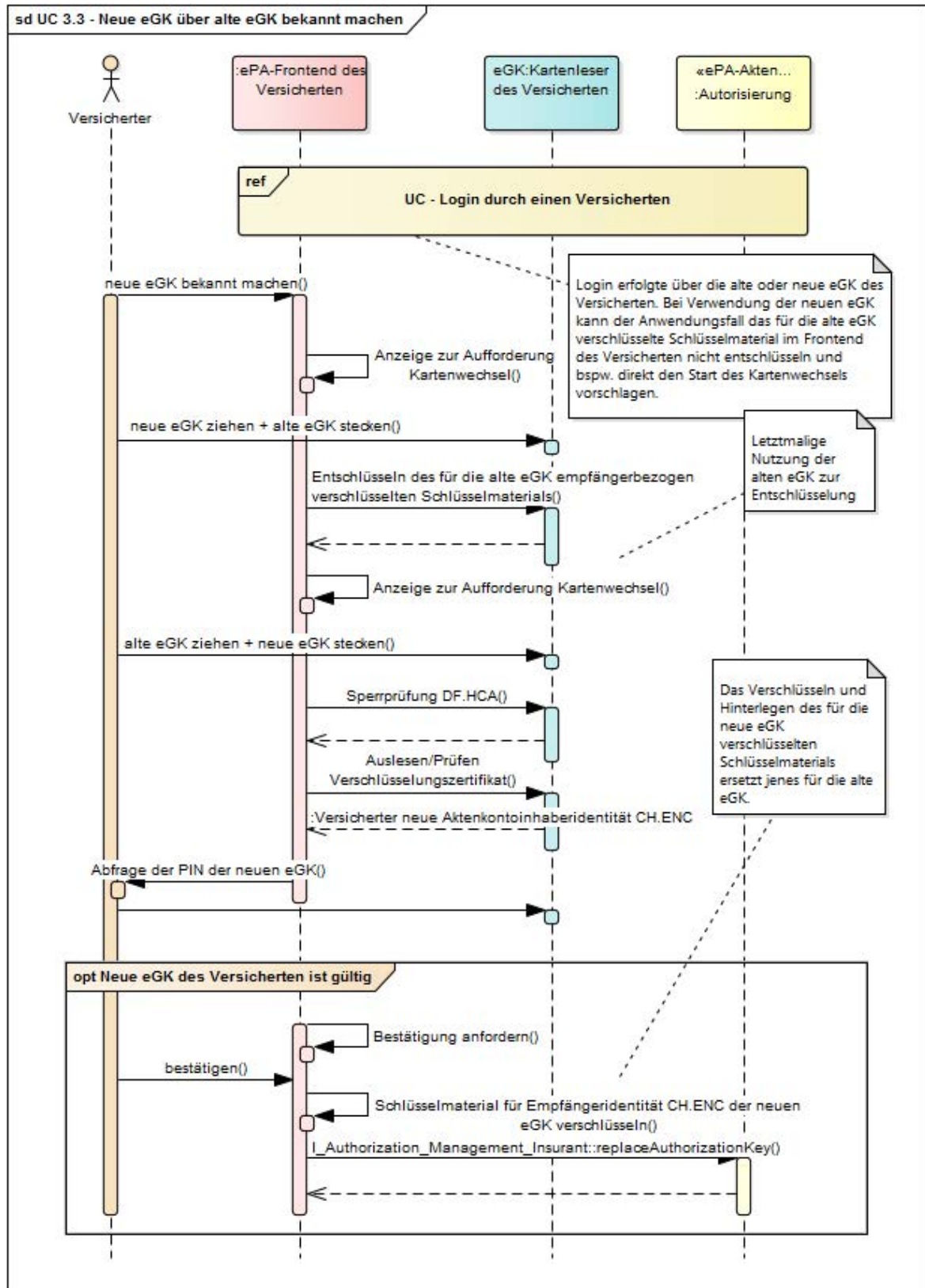


Abbildung 20: Neue eGK über alte eGK bekannt machen

[<=]

3.6.4 Neue eGK über Vertreter bekannt machen

Mit diesem Anwendungsfall unterstützt ein berechtigter Vertreter den Berechtigungserhalt des Versicherten, in dem er dem Versicherten bei dessen eGK-Verlust seine kryptografische Berechtigung durch Umschlüsselung auf die neue eGK des Versicherten wiederherstellt. Der berechtigte Vertreter meldet sich im Aktenkonto des Versicherten an und entschlüsselt das für den Vertreter hinterlegte kryptografische Schlüsselmaterial des Aktenkontos des Versicherten mit der eGK des Vertreters. Anschließend erfolgt die Verschlüsselung für die neue eGK des Versicherten, das neue verschlüsselte Schlüsselmaterial ersetzt dabei das für eine alte eGK des Versicherten verschlüsselte Schlüsselmaterial in der Komponente Autorisierung.

EPA-EPF-A_0023 - Anwendungsfall „Neue eGK über Vertreter bekannt machen“

Alle am Anwendungsfall beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 14: Neue eGK über Vertreter bekannt machen

Name	UC 3.4 - Neue eGK über Vertreter bekannt machen
Vorbedingung	Der Versicherte ist während des Anwendungsfalls zugegen, trägt seine neue eGK bei sich.
Kurzbeschreibung (Außensicht)	Ein Vertreter wählt das Wechseln der eGK als Authentisierungsmerkmal des Versicherten, dazu steckt er die neue eGK des Versicherten in den Kartenleser. Der Versicherte autorisiert die Umschlüsselung mittels PIN-Eingabe, der Vertreter bestätigt den Wunsch zum Kartenwechsel.
Nachbedingung	Berechtigung für die neue eGK des Versicherten im Aktenkonto des Versicherten ist eingerichtet. Die alte eGK wird vom System nicht mehr akzeptiert.

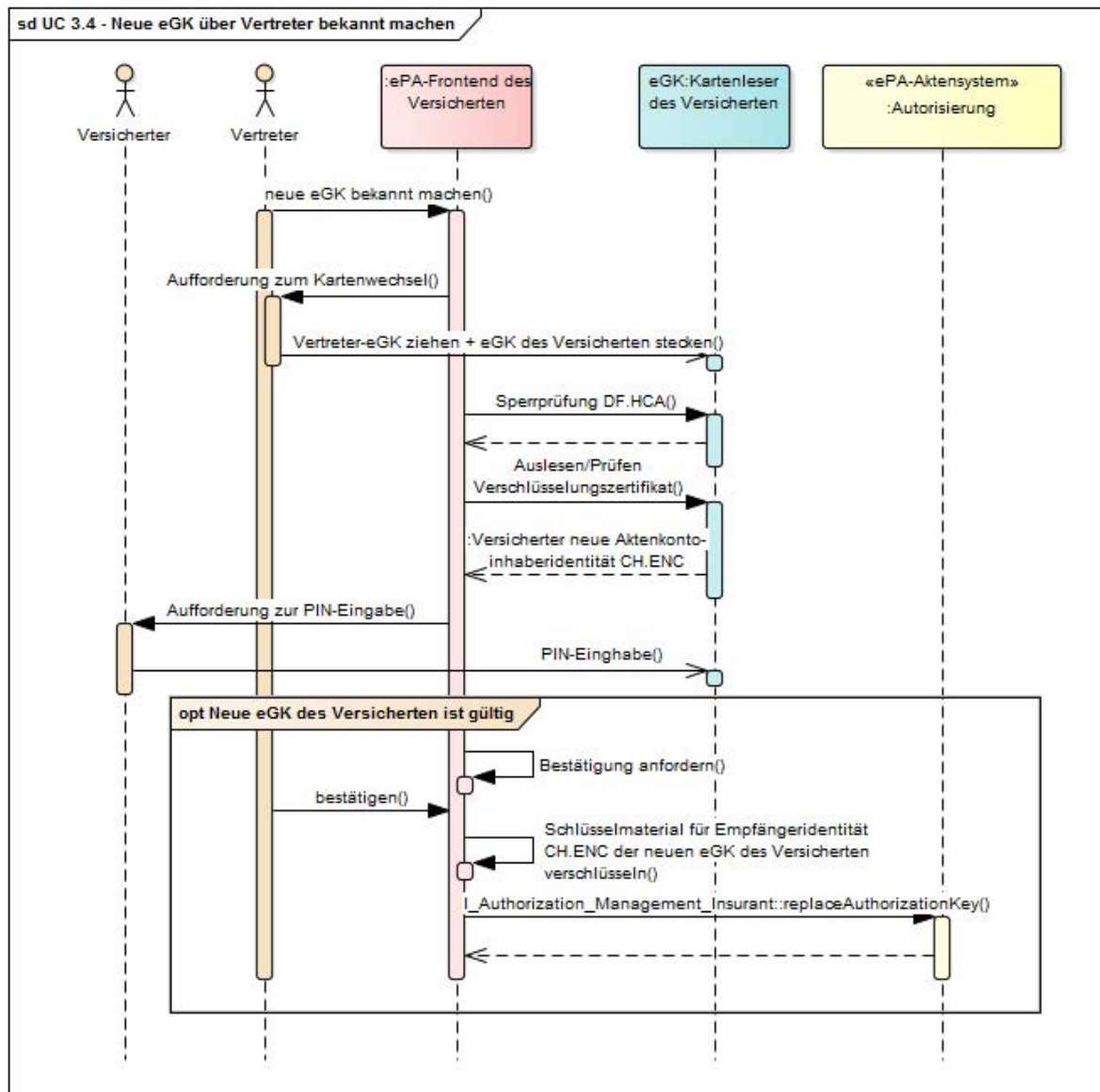


Abbildung 21: Neue eGK über Vertreter bekannt machen

 $[<=]$

3.6.5 Berechtigungen durch einen Versicherten auflisten

Die Berechtigungen für Vertreter und Leistungserbringerinstitutionen sind in Zugriffsregeln in technischen Dokumenten in der Komponente Dokumentenverwaltung hinterlegt. In diesen Zugriffsregeln ist für jeden Benutzer (d.h. Leistungserbringerinstitution, Versicherter, Vertreter) u.a. auch der Klurname hinterlegt, um dem Versicherten die Liste der Berechtigten in lesbarer Form aufzubereiten.

Der Anwendungsfall zum Auflisten aller Berechtigungen bezieht sich auf die Anzeige der Zugriffsberechtigten innerhalb eines Aktenkontos. Ein Auflisten aller (Vertretungs-) Berechtigungen in fremden Aktenkonten für den Anwendungsfall „*ich bin Vertreter für*“ muss frontendseitig über die Auflistung der verwendeten Versicherten-ID der Vertretenen (jeweils 10-stelliger, unveränderlicher Anteil der KVNR) realisiert werden.

EPA-EPF-A_0024 - Auflisten der eingerichteten Vertretungen

Das ePA-Frontend des Versicherten MUSS eine Liste aller vom Versicherten in der Anwendung im Rahmen einer Vertretung verwendeten Versicherten-ID (10-stelliger, unveränderlicher Anteil der KVNR) anderer Versicherter führen und im Rahmen einer Abfrage „ich bin Vertreter für“ zur Anzeige bringen.

[<=]

EPA-EPF-A_0025 - Sortieren der Liste der zugriffsberechtigten LEI

Das ePA-Frontend des Versicherten MUSS für den Versicherten die Liste der zugriffsberechtigten LEI so generieren, dass der Versicherte bei der Sortierung und Darstellung der Liste mindestens folgende Informationen verwenden kann: Name der Leistungserbringerinstitution, Berechtigung (LE-Dok || LE-Dok + Vers-Dok), eingestellte und verbleibende Berechtigungsdauer (analog der Suchkriterien).

[<=]

EPA-EPF-A_0026 - Anwendungsfall „Berechtigungen durch einen Versicherten auflisten“

Alle am Anwendungsfall beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 15: Berechtigungen durch einen Versicherten auflisten

Name	UC 3.5 - Berechtigungen durch einen Versicherten auflisten
Vorbedingung	-
Kurzbeschreibung (Außensicht)	<p>Der Versicherte bzw. sein Vertreter wählt das Auflisten aller vergebenen Berechtigungen aus. Der Versicherte bzw. sein Vertreter erhält eine Auflistung aller zum aktuellen Zeitpunkt in seinem Aktenkonto zugriffsberechtigten Leistungserbringerinstitutionen und Vertreter.</p> <p>Das Policy Document enthält die Zugriffsregeln für jeden Berechtigten in der Komponente Dokumentenverwaltung auf Basis einer Benutzer-ID (d.h. Telematik-ID, KVNR des Versicherten, KVNR des Vertreters). An jeder Berechtigungsregel ist zusätzlich der Klurname hinterlegt. Dieser wird für die Darstellung im ePA-Frontend des Versicherten verwendet.</p>
Nachbedingung	Der Versicherte bzw. berechtigte Vertreter kann die aufgelisteten Berechtigungen über den UC 3.6 bearbeiten.

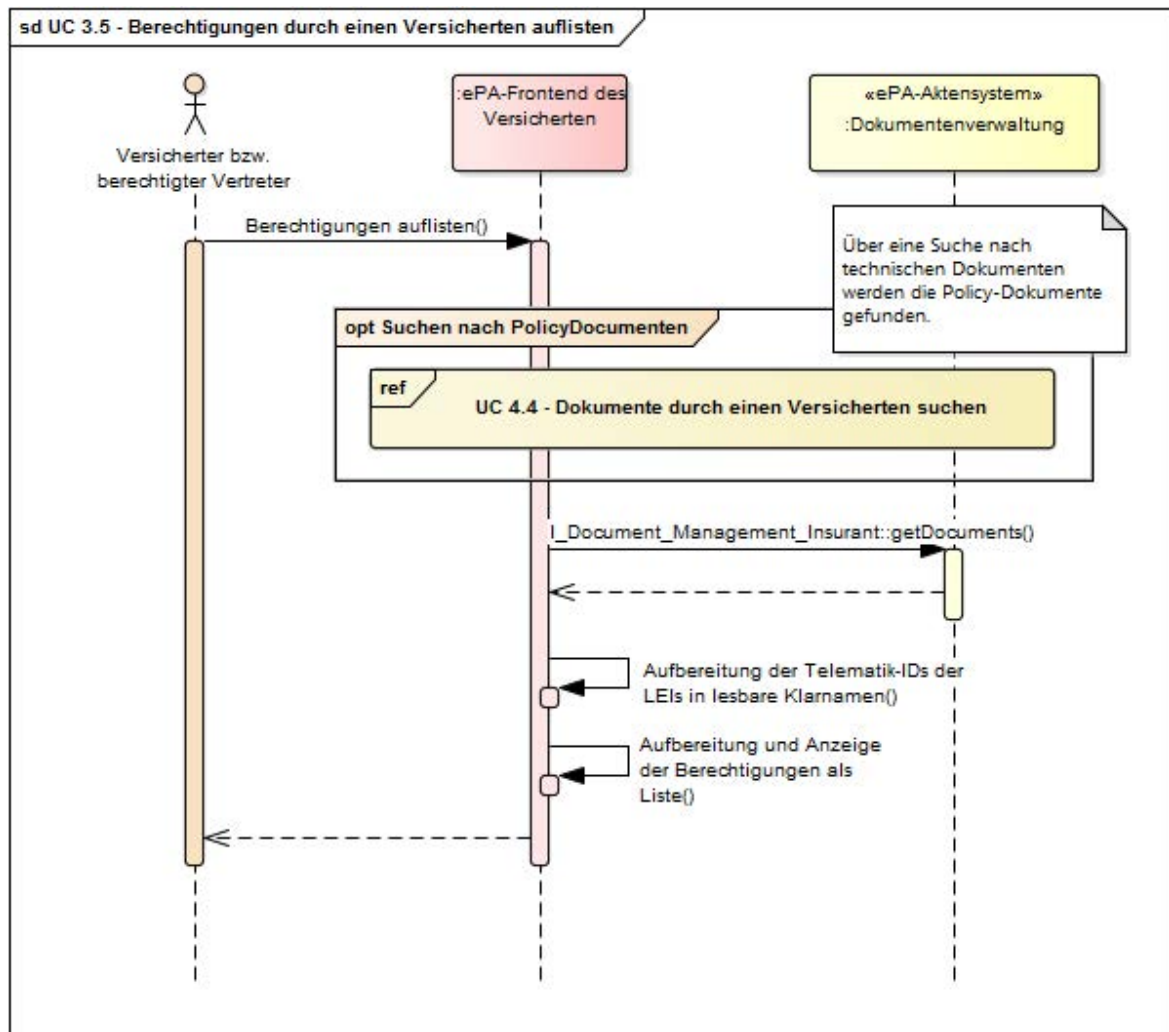


Abbildung 22: Berechtigungen durch einen Versicherten auflisten

[<=]

3.6.6 Bestehende Berechtigungen durch einen Versicherten verwalten

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter die im Aktenkonto eines Versicherten hinterlegten Zugriffsberechtigungen verwalten.

Der Versicherte oder ein berechtigter Vertreter kann die Berechtigung einer Leistungserbringerinstitution über die Änderung der Berechtigungsregel (LE-Dok|| LE-Dok + Vers-Dok) löschen bzw. ändern. Ferner kann auf diesem Weg die Dauer der Berechtigung für Leistungserbringerinstitutionen gekürzt oder verlängert werden.

Zusätzlich kann der Versicherte einen oder mehrere Vertreter löschen.

EPA-EPF-A_0027 - Anwendungsfall „Bestehende Berechtigungen durch einen Versicherten verwalten“

Alle am Anwendungsfall „Bestehende Berechtigungen durch einen Versicherten verwalten“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 16: Bestehende Berechtigungen durch einen Versicherten verwalten

Name	UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten
Vorbedingung	
Kurzbeschreibung (Außensicht)	Der Versicherte bzw. sein Vertreter wählt aus der angezeigten Liste aller vergebenen Berechtigungen diejenige Berechtigung einer Leistungserbringerinstitution , die angepasst werden soll. Der Versicherte bearbeitet die Berechtigungsregel (LE-Dok LE-Dok + Vers-Dok) und -dauer (1 Tag, 28 Tage [default], 18 Monate oder flexibel 1 bis 540 Tage) für Leistungserbringerinstitutionen oder er entzieht die Berechtigung. Der Versicherte bzw. sein Vertreter bestätigt das Löschen bzw. die Hinterlegung der angepassten Zugriffsberechtigungen im System. Ebenso kann der Versicherte aus der angezeigten Liste Vertreter markieren und diese löschen.
Nachbedingung	Modifizierte Berechtigungen sind für alle aktuell und ehemals Berechtigten wirksam.

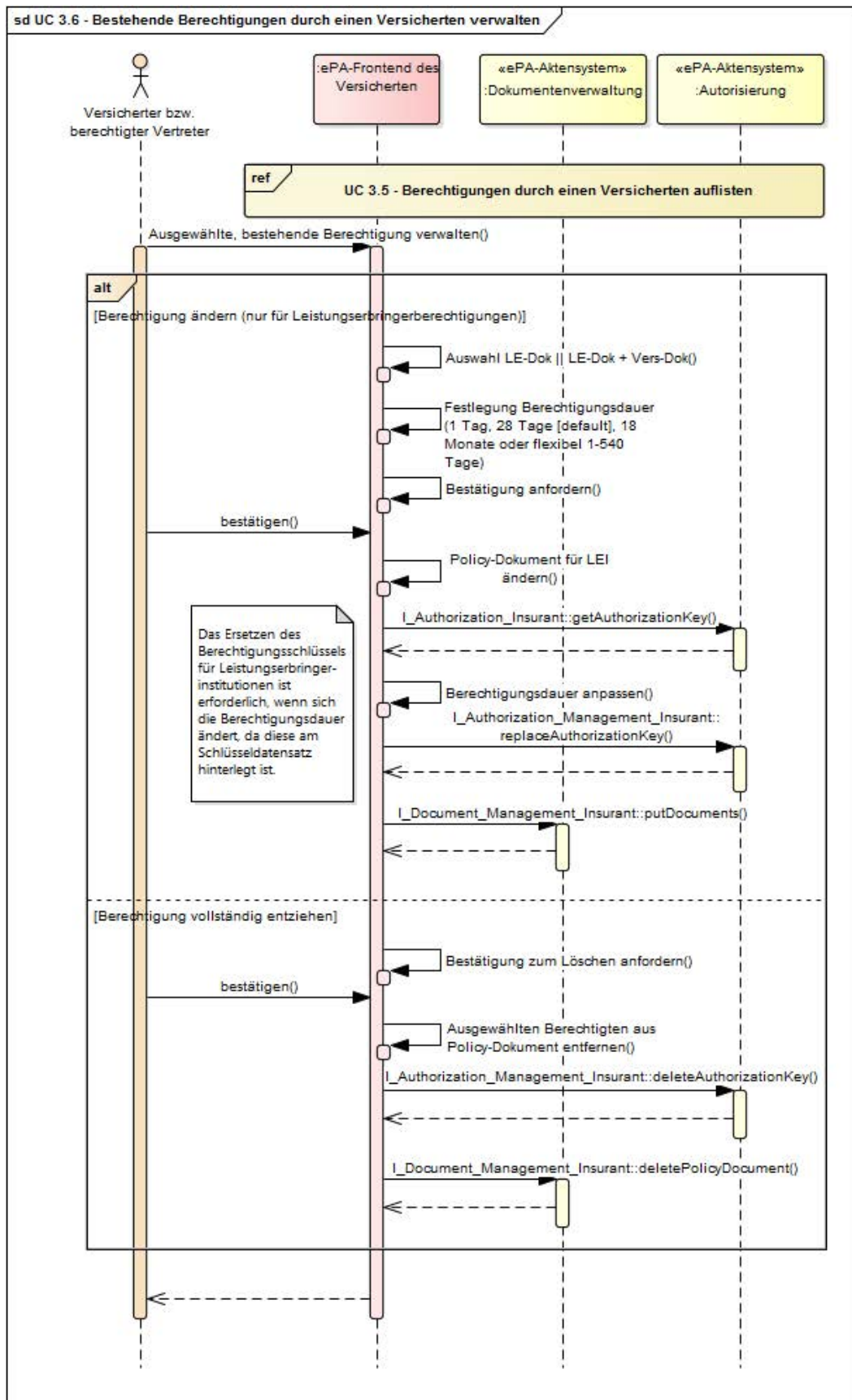


Abbildung 23: Bestehende Berechtigungen durch einen Versicherten verwalten

[<=]

3.6.7 Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern

Mit diesem Anwendungsfall erteilt ein Versicherter einer Leistungserbringerinstitution eine Zugriffsberechtigung in seiner Akte. Der Anwendungsfall wird durch einen Mitarbeiter der LEI über das Primärsystem getriggert. Sämtliche Operationen und Zugriffe im ePA-Aktensystem für die Einrichtung der Berechtigung (Hinterlegung von Zugriffsregeln und für die LEI verschlüsseltes Schlüsselmaterial) erfolgen jedoch mit der Kartenidentität AUT der eGK des Versicherten.

EPA-EPF-A_0028 - Anwendungsfall „Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern“

Alle am Anwendungsfall „Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 17: Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern

Name	UC 3.7 - Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern
Vorbedingung	Die PIN.CH der eGK ist nicht gesperrt.
Kurzbeschreibung (Außensicht)	Ein Mitarbeiter der Leistungserbringerinstitution fordert über das PS am Konnektor eine Zugriffsberechtigung auf das Aktenkonto des Versicherten an. Dem Versicherten oder einem von ihm berechtigten Vertreter wird über das Kartenterminal angezeigt, wofür (LE-Dok LE-Dok und Vers-Dok) und für welche Dauer (1 Tag, 28 Tage [default], 18 Monate oder flexibel 1 bis 540 Tage) er eine Berechtigung erteilt. Der Versicherte oder ein von ihm berechtigter Vertreter stimmt der Berechtigung durch PIN-Eingabe zu.
Nachbedingung	Ein Mitarbeiter der Leistungserbringerinstitution ist in Abwesenheit des Versicherten in der Lage, Dokumente für den Versicherten einzustellen und herunterzuladen.

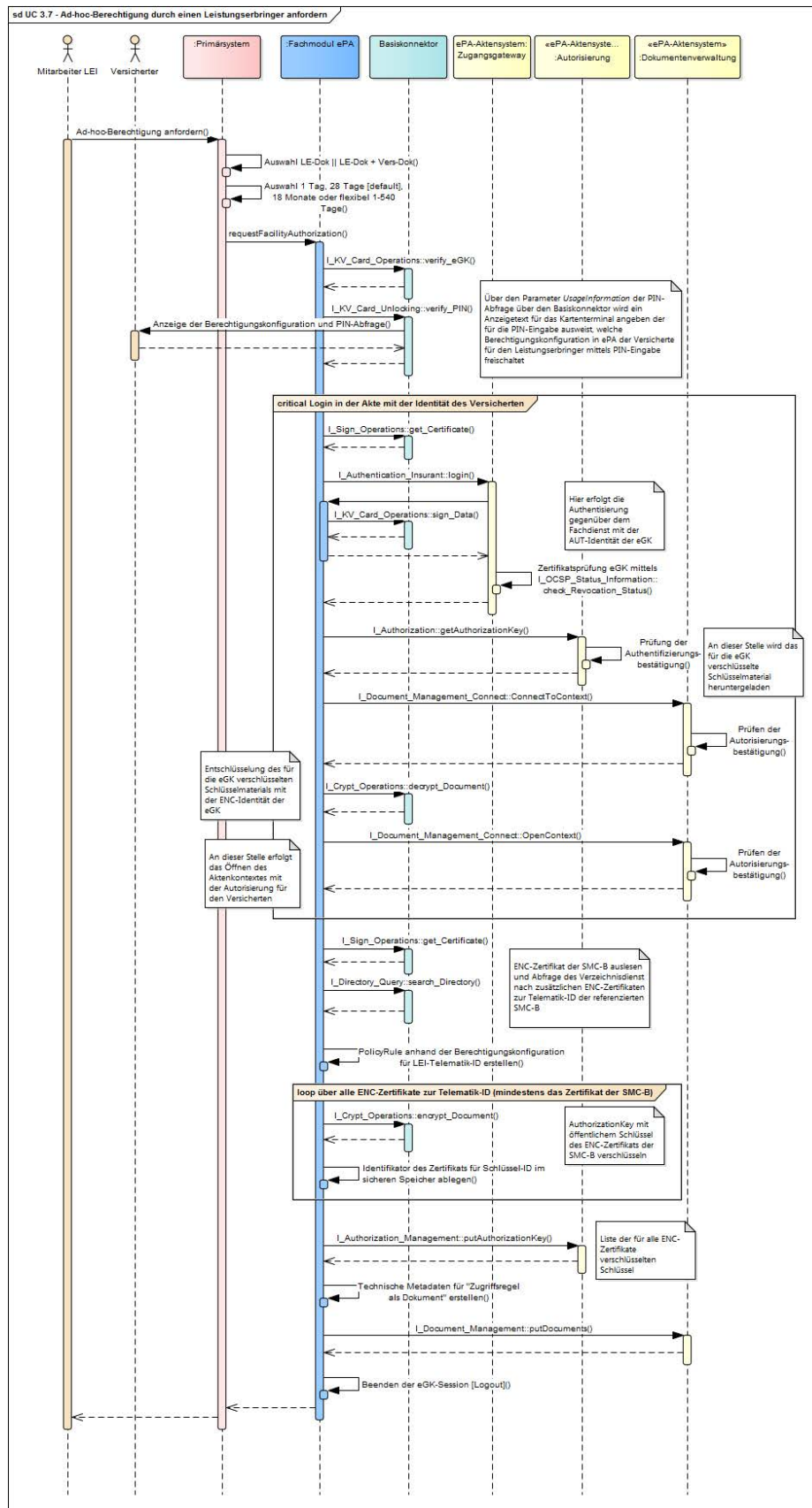


Abbildung 24: Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern

[<=]

3.6.8 Einlesen von sicher verwahrtem Schlüsselmaterial

Mit diesem Anwendungsfall wird das vom Versicherten sicher verwahrte exportierte Schlüsselmaterial für einen Berechtigungserhalt eingelesen und im ePA-Frontend des Versicherten zur Umschlüsselung des verschlüsselt hinterlegten Schlüsselmaterials im ePA-Aktensystem genutzt.

A_13822 - Das ePA-Frontend des Versicherten - Einlesen von sicher verwahrtem Schlüsselmaterial für Berechtigungserhalt

Das ePA-Frontend des Versicherten MUSS das durch sein Produkt exportierte Schlüsselmaterial einlesen, sodass das Schlüsselmaterial des Aktenkontos des Versicherten im ePA-Frontend des Versicherten im Anschluss in der Form verfügbar ist, wie es für den Export in den Sitzungsdaten eines aktiven Logins im ePA-Frontend des Versicherten verfügbar war.[<=]

Diese Anforderung bezieht sich ausschließlich auf den bspw. durch die eGK des Versicherten entschlüsselten Akten- und Kontextschlüssel.

A_13823 - Anwendungsfall Umschlüsselung mit sicher verwahrtem Schlüsselmaterial

Alle am Anwendungsfall "Umschlüsselung mit sicher verwahrtem Schlüsselmaterial" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 18: Umschlüsselung mit sicher verwahrtem Schlüsselmaterial

Name	UC 3.8 - Umschlüsselung mit sicher verwahrtem Schlüsselmaterial
Vorbedingung	Der Versicherte verfügt über das sicher verwahrte Schlüsselmaterial. Der Versicherte nutzt das Frontend des Versicherten desselben Herstellers, mit dem er das Schlüsselmaterial exportiert hat.
Kurzbeschreibung (Außensicht)	Der Versicherte erhält eine neue eGK, die bisher verwendete alte eGK kann nicht genutzt werden. Für diese alte eGK ist das kryptografische Schlüsselmaterial des Aktenkontos des Versicherten im ePA-Aktensystem verschlüsselt hinterlegt. Der Versicherte authentisiert sich gegenüber dem ePA-Aktensystem mit seiner neuen eGK. Anschließend importiert er den exportierten Schlüsselmaterial in das ePA-Frontend des Versicherten. Das damit im ePA-Frontend des Versicherten im Klartext vorhandene Schlüsselmaterial wird für die neue eGK verschlüsselt und im ePA-Aktensystem hinterlegt.
Nachbedingung	Der Versicherte ist in der Lage mit seiner aktuell gültigen eGK in der Umgebung der Leistungser-

bringer eine Ad-hoc-Berechtigung zu vergeben und mit dem ePA-Frontend des Versicherten auf die Daten in seinem Aktenkonto zuzugreifen.

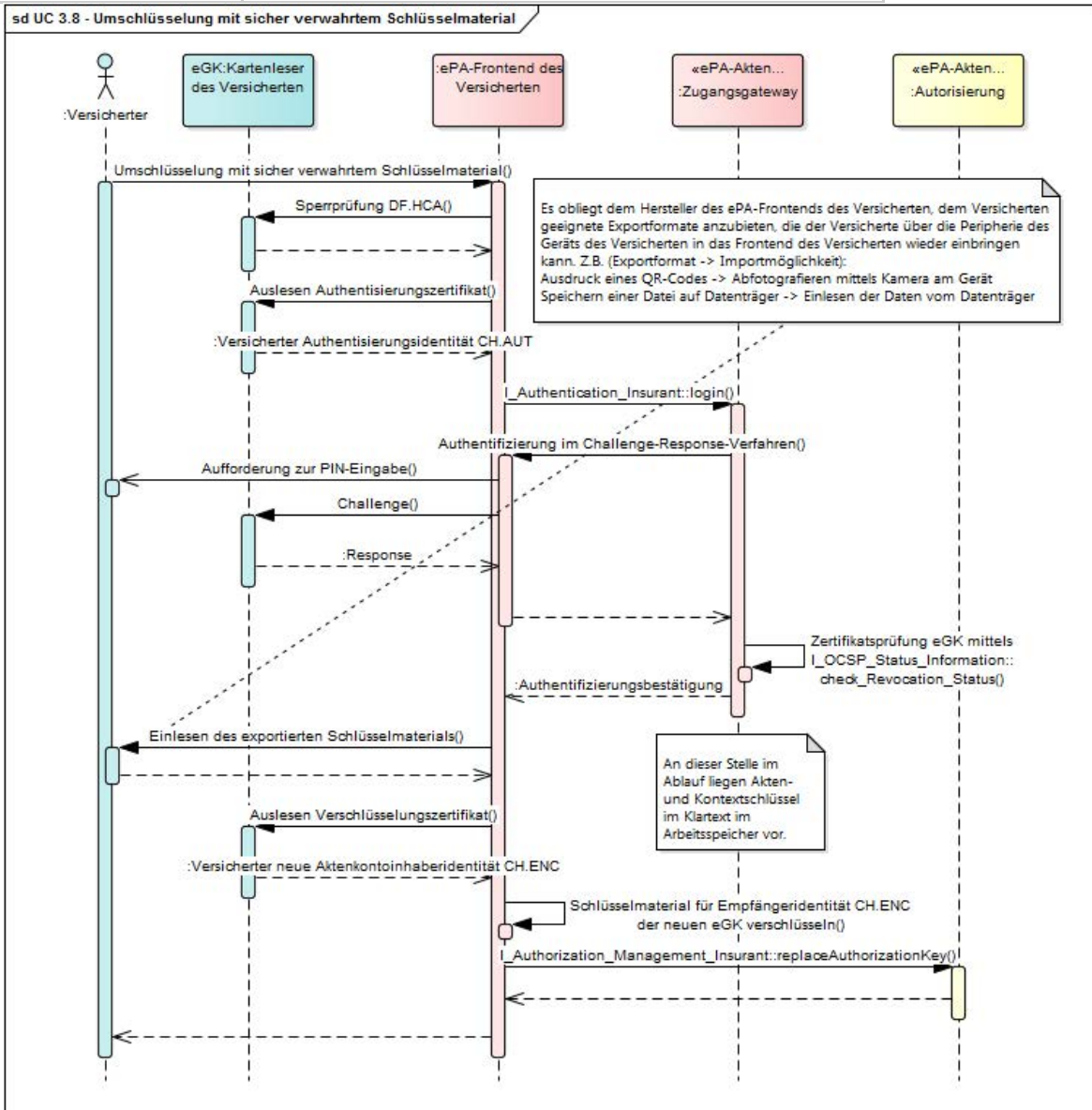


Abbildung 25: Umschlüsselung mit sicher verwahrtm Schlüsselmaterial

[<=]

3.7 Dokumentenverwaltung

3.7.1 Dokumente durch einen Leistungserbringer einstellen

EPA-EPF-A_0029 - Anwendungsfall „Dokumente durch einen Leistungserbringer einstellen“

Alle am Anwendungsfall „Dokumente durch einen Leistungserbringer einstellen“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 19: Dokumente durch einen Leistungserbringer einstellen

Name	UC 4.1 - Dokumente durch einen Leistungserbringer einstellen
Vorbedingung	Dem Leistungserbringer ist die Existenz des Aktenkontos des Versicherten durch Hinterlegung des RecordIdentifiers im Primärsystem bekannt. Der Leistungserbringerinstitution wurde eine Zugriffsberechtigung eingeräumt.
Kurzbeschreibung (Außensicht)	Ein Mitarbeiter der Leistungserbringerinstitution registriert über das PS am Konnektor ein neues Dokument für die elektronische Patientenakte des Versicherten. Dazu gibt er inhaltsbeschreibende Metadaten zum ausgewählten Dokument ein. Es muss dem Mitarbeiter der Leistungserbringerinstitution durch die Nutzung der Metadaten möglich sein, Dokumente mit Relevanz für die Versorgung von Dokumenten zur Information des Versicherten zu unterscheiden.
Nachbedingung	Die vom Leistungserbringer eingestellten Dokumente sind vom Versicherten und alle vom Versicherten dazu berechtigten Nutzer abrufbar.

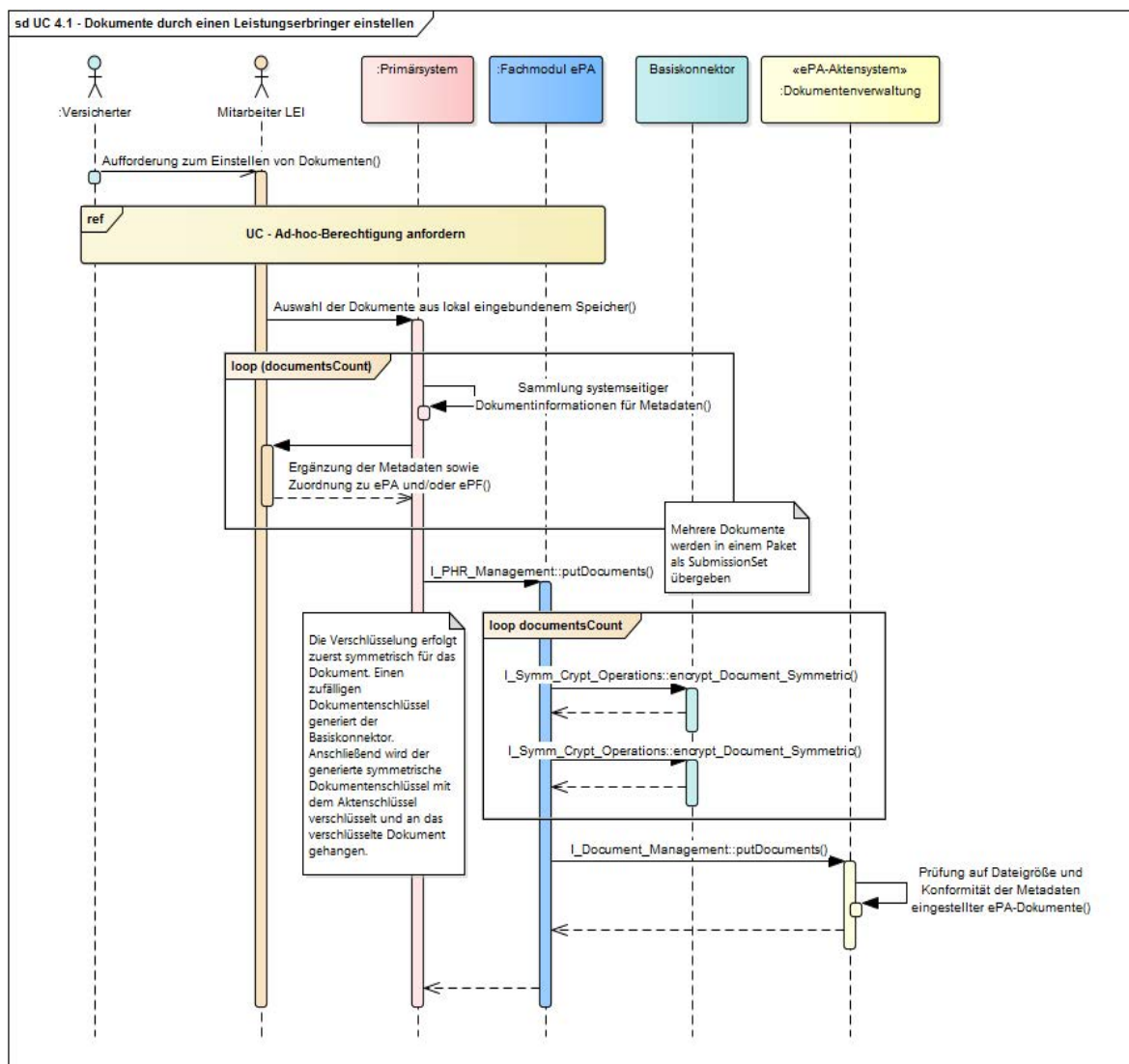


Abbildung 26: Dokumente durch einen Leistungserbringer einstellen

[<=]

3.7.2 Dokumente durch einen Versicherten einstellen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter Dokumente in die Komponente Dokumentenverwaltung hochladen. Diese sind dann durch andere Nutzer abrufbar, sofern der Versicherte ihnen Zugriffsrechte eingeräumt hat. Zur Kontrolle der vergebenen Berechtigungen wird vor dem Hochladen die Liste der potentiell zugriffsberechtigten Nutzer angezeigt und dem Versicherten die Möglichkeit gegeben, das Hochladen abubrechen, wenn er mit der genau diesen aufgelisteten Nutzern das Dokument nicht zur Verfügung stellen möchte. In diesem Fall muss der Versicherte die Zugriffsberechtigungen mittels des Anwendungsfalls "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" anpassen oder auf das Einstellen des Dokuments verzichten.

EPA-EPF-A_0030 - Anwendungsfall „Dokumente durch einen Versicherten einstellen“

Alle am Anwendungsfall „Dokumente durch einen Versicherten einstellen“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 20: Dokumente durch einen Versicherten einstellen

Name	UC 4.2 - Dokumente durch einen Versicherten einstellen
Vorbedingung	Die Liste der vergebenen Berechtigungen (Policy Document) wurde nach dem Login aus der Dokumentenverwaltung automatisch geladen.
Kurzbeschreibung (Außensicht)	<p>Ein Versicherter oder ein von ihm berechtigter Vertreter wählt am ePA-Frontend des Versicherten ein oder mehrere Dokumente aus, die er in die Patientenakte hochladen möchte.</p> <p>Der Versicherte ergänzt die notwendigen Metadaten zu den gewählten Dokumenten und erhält eine Übersicht der Nutzer, die dieses Dokument auf Basis der vergebenen Berechtigungen einsehen dürfen.</p> <p>Nach der Bestätigung durch den Versicherten überträgt das Frontend des Versicherten die Dokumente in das ePA-Aktensystem.</p> <p>Ist der Versicherte mit der Liste der potentiell zugriffsberechtigten Nutzer nicht einverstanden, kann er den Anwendungsfall abbrechen und die Vergebenen Berechtigungen über die Anwendungsfälle "UC 3.6 Berechtigungen verwalten" und "UC 3.1 Berechtigungen vergeben" bearbeiten.</p>
Nachbedingung	Die vom Versicherten eingestellten Dokumente sind durch genau die in der Auflistung potentiell berechtigter Nutzer angezeigten Berechtigten abrufbar.

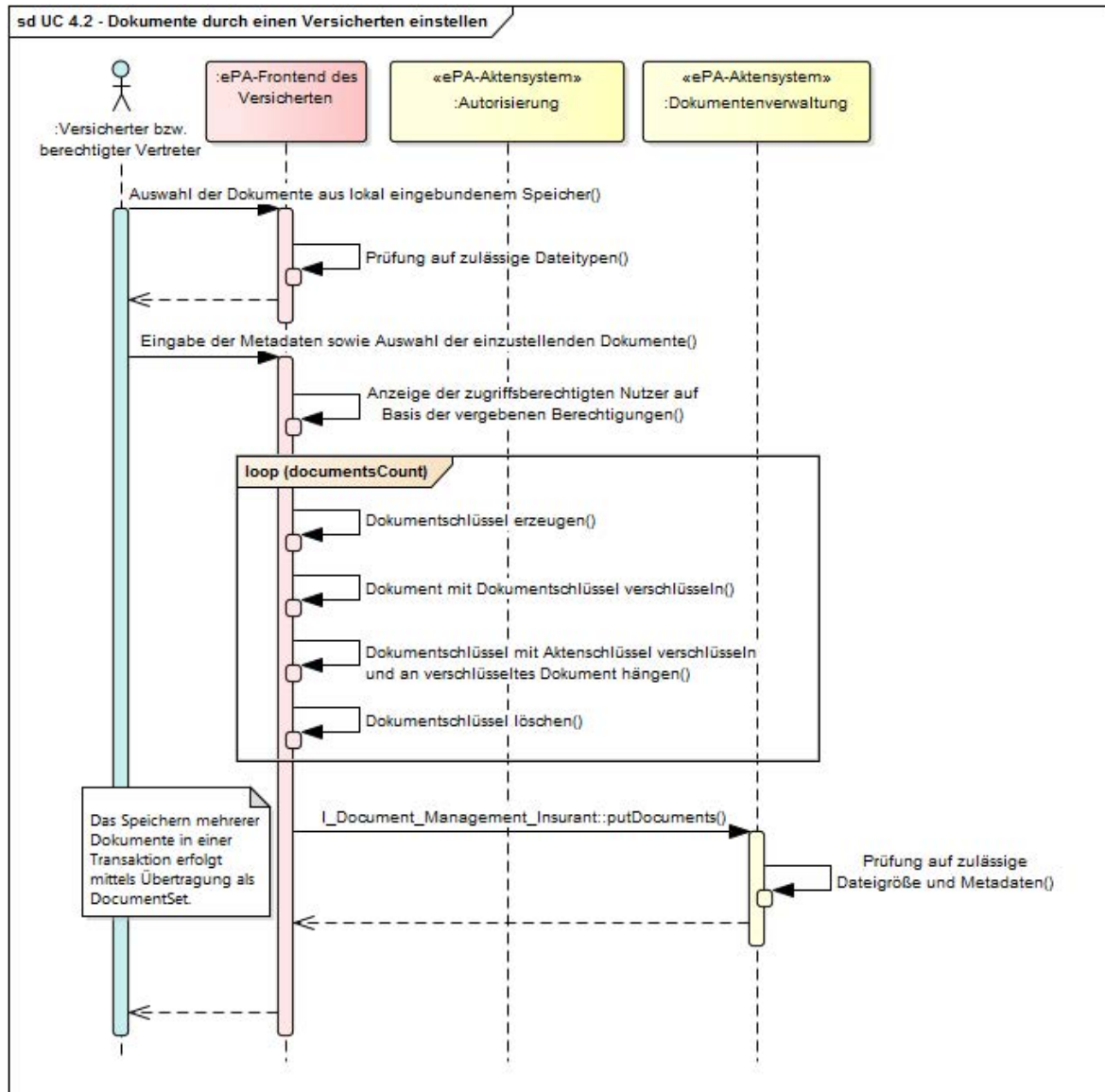


Abbildung 27: Dokumente durch einen Versicherten einstellen

[<=]

EPA-EPF-A_0031 - Potentielle Berechtigte ermitteln

Das ePA-Frontend des Versicherten SOLL vor dem Hochladen der Dokumente anzeigen, welche Leistungserbringerinstitutionen auf dieses Dokument Zugriff haben werden. Die Funktion MUSS für den Versicherten abschaltbar umgesetzt werden.

[<=]

3.7.3 Dokumente durch einen Leistungserbringer suchen

Mit diesem Anwendungsfall kann ein Leistungserbringer in einem Aktenkonto eines Versicherten nach Dokumenten suchen. Für die Suche stehen ihm die pro Dokument hinterlegten Metadaten zur Verfügung. Daraus kann der Leistungserbringer über das Primärsystem Suchanfragen zusammenstellen, die eine beliebige Kombination aus technischen und personenbezogenen Werten umfassen kann. Das Ergebnis der Suche besteht aus

einer Liste von Metadatensätzen der zur Suchanfrage passenden Dokumente und wird vom ePA-Aktensystem zurückgegeben.

EPA-EPF-A_0032 - Anwendungsfall „Dokumente durch einen Leistungserbringer suchen“

Alle am Anwendungsfall „Dokumente durch einen Leistungserbringer suchen“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 21: Dokumente durch einen Leistungserbringer suchen

Name	UC 4.3 - Dokumente durch einen Leistungserbringer suchen
Vorbedingung	-
Kurzbeschreibung (Außensicht)	Ein Mitarbeiter der Leistungserbringerinstitution führt über das PS am Konnektor eine Dokumentensuche über das Aktenkonto des Versicherten durch. Dazu gibt er Filterkriterien in eine Suchmaske des PS ein. Die auf dem ePA-Aktensystem erzeugte Suchergebnisliste mit Dokumentmetadaten, die den Filterkriterien entsprechen, wird auf dem PS angezeigt.
Nachbedingung	Aus der nicht-leeren Ergebnismenge einer Suchanfrage kann ein Leistungserbringer ein gewähltes Dokument mittels UC 4.9 "Dokumente durch einen Leistungserbringer anzeigen" herunterladen und anzeigen lassen.

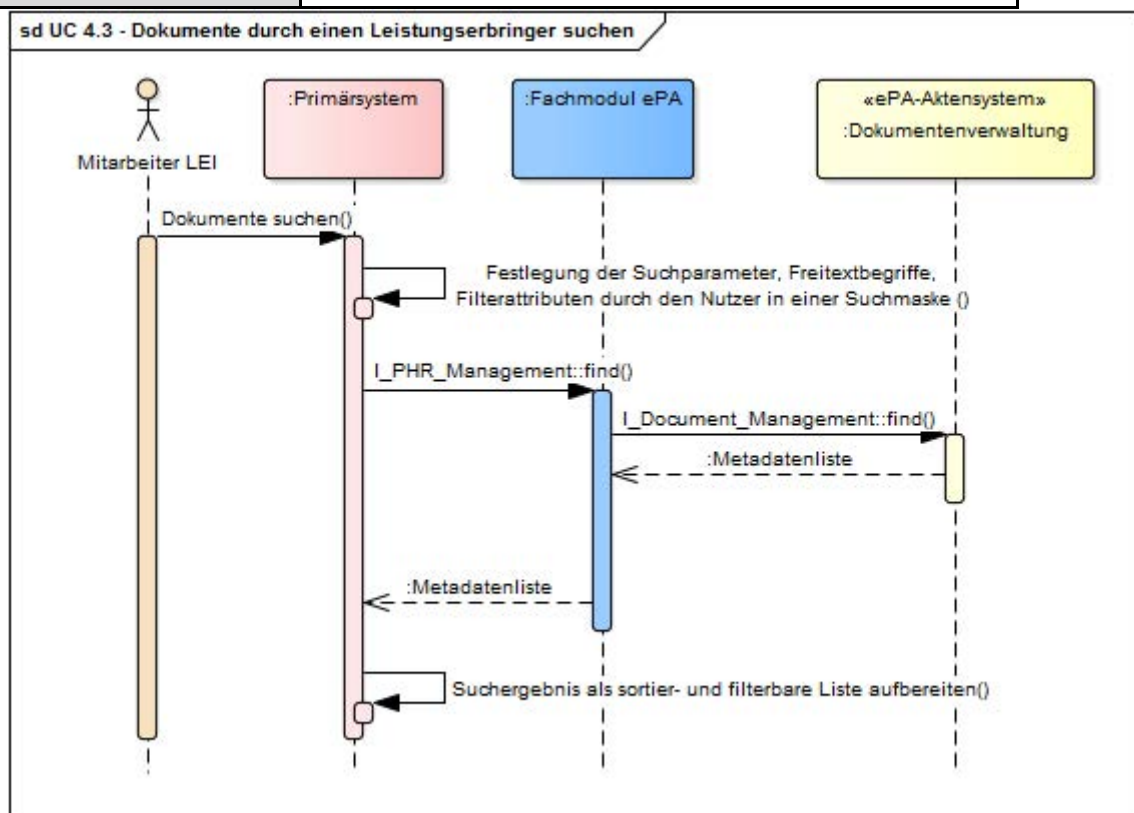


Abbildung 28: Dokumente durch einen Leistungserbringer suchen

[<=]

3.7.4 Dokumente durch einen Versicherten suchen

Mit diesem Anwendungsfall kann ein Versicherter nach Dokumenten in der Komponente Dokumentenverwaltung suchen. Als mögliche Suchparameter stehen ihm die technischen und personenbezogenen Dokument-Metadaten zur Verfügung. Eine Verfeinerung der Suche erfolgt durch mehrmaliges Ausführen dieses Anwendungsfalls über angepasste Suchanfragen.

EPA-EPF-A_0033 - Anwendungsfall „Dokumente durch einen Versicherten suchen“

Alle am Anwendungsfall „Dokumente durch einen Versicherten suchen“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 22: Dokumente durch einen Versicherten suchen

Name	UC 4.4 - Dokumente durch einen Versicherten suchen
Vorbedingung	-
Kurzbeschreibung (Außensicht)	Ein Versicherter oder ein von ihm berechtigter Vertreter führt über das Frontend des Versicherten eine Dokumentensuche im Aktenkonto des Versicherten durch. Dazu können die Ergebnisse über eine Suchmaske des Frontends eingeschränkt werden. Die vom ePA-Aktensystem erzeugte Trefferliste mit passenden Dokumentmetadaten wird auf dem Frontend des Versicherten angezeigt.
Nachbedingung	Aus der nicht-leeren Ergebnismenge einer Suchanfrage kann ein Versicherter bzw. berechtigter Vertreter ein gewähltes Dokument mittels UC 4.10 „Dokumente durch einen Versicherten anzeigen“ herunterladen und anzeigen lassen.

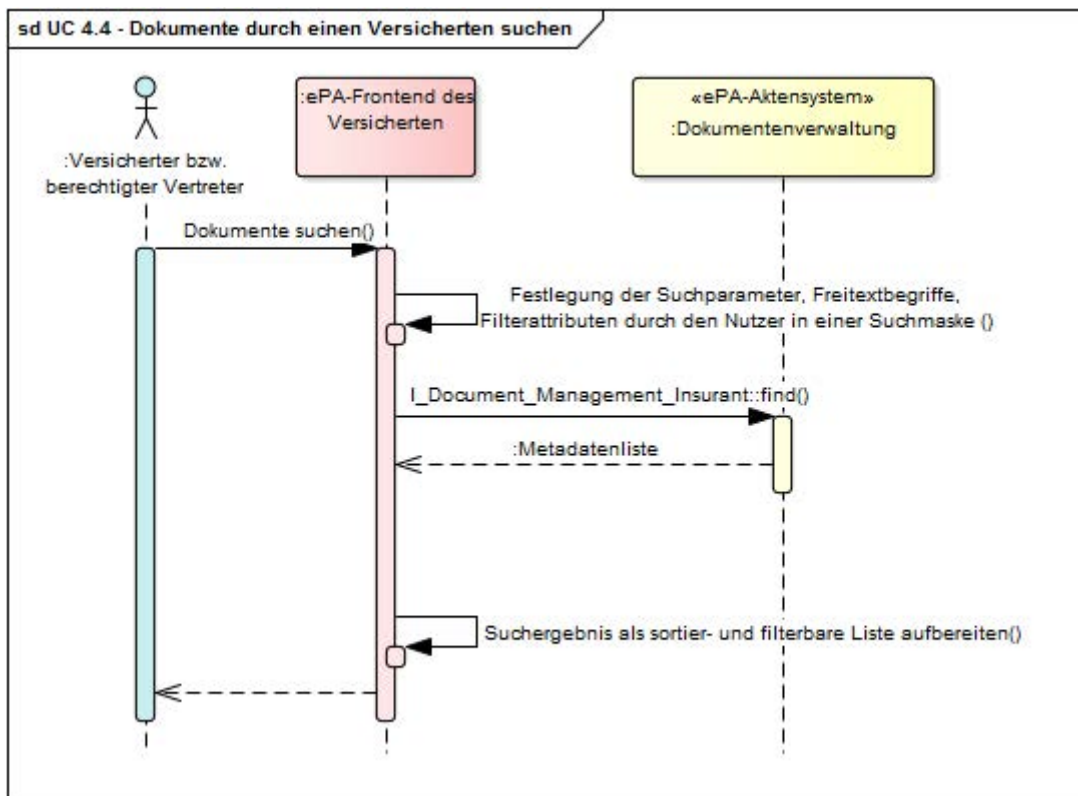


Abbildung 29: Dokumente durch einen Versicherten suchen

[<=]

3.7.5 Ändern einer Dokumentenklassifizierung durch einen Leistungserbringer

Mit diesem Anwendungsfall bekommt ein Mitarbeiter einer Leistungserbringerinstitution die Möglichkeit, ein vom Versicherten im Aktenkonto des Versicherten abgelegtes Dokument als Leistungserbringer-Äquivalent zu kennzeichnen. Zur Durchführung des Anwendungsfalls muss die Leistungserbringerinstitution berechtigt sein, auf Dokumente zuzugreifen, die vom Versicherten in das Aktenkonto des Versicherten eingestellt wurden. Die Kennzeichnung eines Dokuments als Leistungserbringer-Äquivalent führt dazu, dass dieses Dokument, obwohl es ursprünglich von einem Versicherten eingestellt wurde, von Leistungserbringerinstitutionen eingesehen werden kann, die nur eine Berechtigung für Dokumente besitzen, die von Leistungserbringerinstitutionen eingestellt wurden.

EPA-EPF-A_0034 - I_Authentication_Insurant Anwendungsfall „Ändern einer Dokumentenklassifizierung durch einen Leistungserbringer“

Alle am Anwendungsfall „Ändern einer Dokumentenklassifizierung durch einen Leistungserbringer“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 23: Ändern einer Dokumentenklassifizierung durch einen Leistungserbringer

Name	UC 4.5 - Ändern einer Dokumentenklassifizierung durch einen Leistungserbringer
Vorbedingung	Der Versicherte hat die Leistungserbringerinstitution, die diesen Anwendungsfall durchführen soll, berechtigt, auf Dokumente zuzugreifen, die der Versicherte oder ein von ihm berechtigter Vertreter eingestellt hat. Der Leistungserbringer hat die medizinische Relevanz eines Dokuments festgestellt und möchte die Dokumentenklassifizierung an einem Dokument ändern.
Kurzbeschreibung (Außensicht)	Ein Mitarbeiter der Leistungserbringerinstitution ändert über das PS am Konnektor die Klassifizierung eines Versichertendokuments. Dabei muss in den Metadaten eines Dokuments das Kennzeichen geändert werden, mit dessen Hilfe die Unterscheidung der Zugriffsberechtigung auf von Leistungserbringerinstitutionen bzw. auf von Versicherten eingestellte Dokumente erfolgt. Das Entfernen dieses Kennzeichens ist möglich. Der Mitarbeiter initiiert das Hochladen der geänderten Dokument-Metadaten über sein PS.
Nachbedingung	Ein Dokument ist als Leistungserbringer-Äquivalent gekennzeichnet. In der Folge bleibt es sichtbar für LE, die generell nur eine Berechtigung auf vom Versicherten eingestellte Dokumente haben und wird zusätzlich sichtbar für LE, die nur eine Berechtigung auf von LEI eingestellte Dokumente haben.

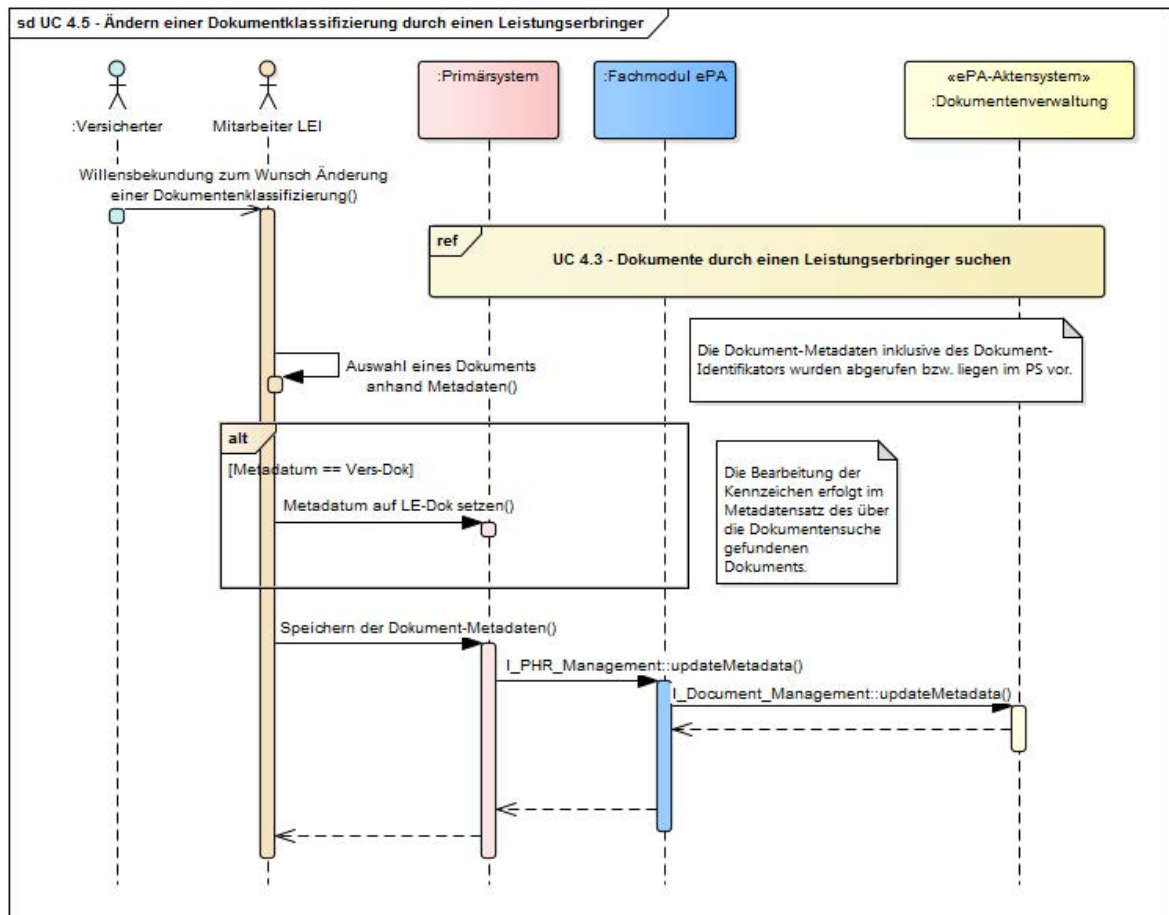


Abbildung 30: Ändern einer Dokumentenklassifizierung durch einen Leistungserbringer

[<=]

3.7.6 Dokumente durch einen Leistungserbringer löschen

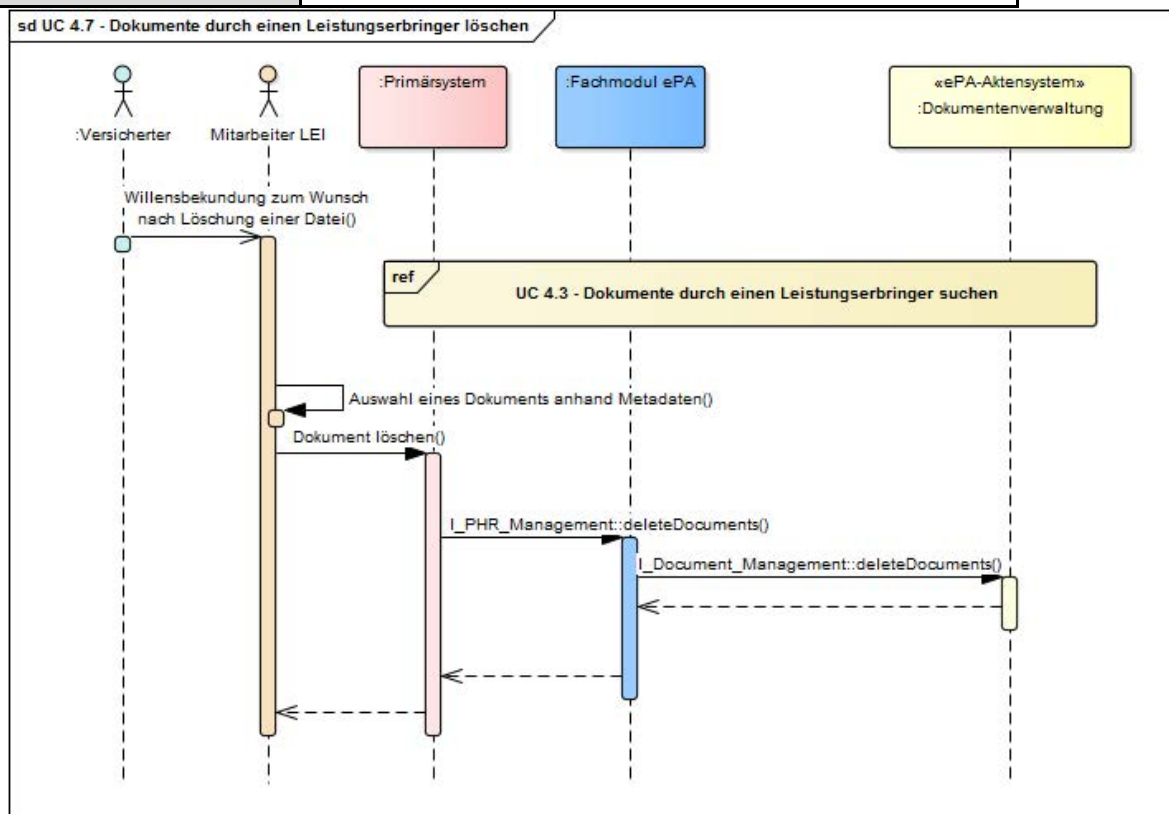
Eine für den Zugriff berechtigte Leistungserbringerinstitution kann im Aktenkonto eines Versicherten Dokumente löschen. Das Löschen von Dokumenten unternimmt der Leistungserbringer bzw. ein Mitarbeiter der LEI auf Anforderung durch den Versicherten. Die Auswahl des zu löschenden Dokuments erfolgt in der Ergebnismenge der Dokumentensuche mittels UC 4.3 - *Dokumente durch einen Leistungserbringer suchen*. Das ePA-Aktensystem entfernt das Dokument in der Komponente Dokumentenverwaltung.

EPA-EPF-A_0036 - Anwendungsfall „Dokumente durch einen Leistungserbringer löschen“

Alle am Anwendungsfall „Dokumente durch einen Leistungserbringer löschen“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 24: Dokumente durch einen Leistungserbringer löschen

Name	UC 4.7 - Dokumente durch einen Leistungserbringer löschen
Vorbedingung	Der Versicherte äußert den Wunsch (ggf. auch auf Anraten des LE), dass ein Dokument (oder mehrere) gelöscht werden soll. Ein Dokument kann vom Versicherten auch ohne Hilfe eines Mitarbeiters der Leistungserbringerinstitution gelöscht werden.
Kurzbeschreibung (Außensicht)	Ein Mitarbeiter der Leistungserbringerinstitution fordert über das PS am Konnektor das Löschen eines über den Dokument-Identifikator identifizierten Dokuments im Aktenkonto des Versicherten an. Der Dokument-Identifikator wird entweder einer vorangegangenen Dokumentsuche entnommen oder ist im PS bereits bekannt. Der Löschwunsch des Versicherten bzw. die erforderliche Zustimmung zur Löschung durch den Versicherten bildet dabei die Berechtigung für diesen Leistungserbringer.
Nachbedingung	Das identifizierte Dokument ist mitsamt zugehöriger Metadaten aus der Fachanwendung ePA gelöscht.


Abbildung 31: Dokumente durch einen Leistungserbringer löschen

[<=]

3.7.7 Dokumente durch einen Versicherten löschen

Der Versicherte kann mit diesem Anwendungsfall Dokumente löschen. Die Liste zur Auswahl der zu löschenden Dokumente erhält der Versicherte über den Anwendungsfall "UC 4.4 - Dokumente durch einen Versicherten suchen". Das eigentliche Entfernen aus dem System erfolgt durch die Komponente Dokumentenverwaltung für alle nicht-technischen Dokumente.

EPA-EPF-A_0037 - Anwendungsfall „Dokumente durch einen Versicherten löschen“

Alle am Anwendungsfall „Dokumente durch einen Versicherten löschen“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 25: Dokumente durch einen Versicherten löschen

Name	UC 4.8 - Dokumente durch einen Versicherten löschen
Vorbedingung	Ein Versicherter oder ein von ihm berechtigter Vertreter hat ein oder mehrere Dokumente identifiziert (z. B. über eine vorhergehende Suche), die gelöscht werden sollen.
Kurzbeschreibung (Außensicht)	Ein Versicherter oder ein von ihm berechtigter Vertreter wählt am Frontend des Versicherten ein oder mehrere Dokumente aus, die gelöscht werden sollen. Das Frontend überträgt die Anforderung an das ePA-Aktensystem, welches das Dokument löscht.
Nachbedingung	Jedes betroffene Dokument wird vom ePA-Aktensystem unwiderruflich gelöscht.

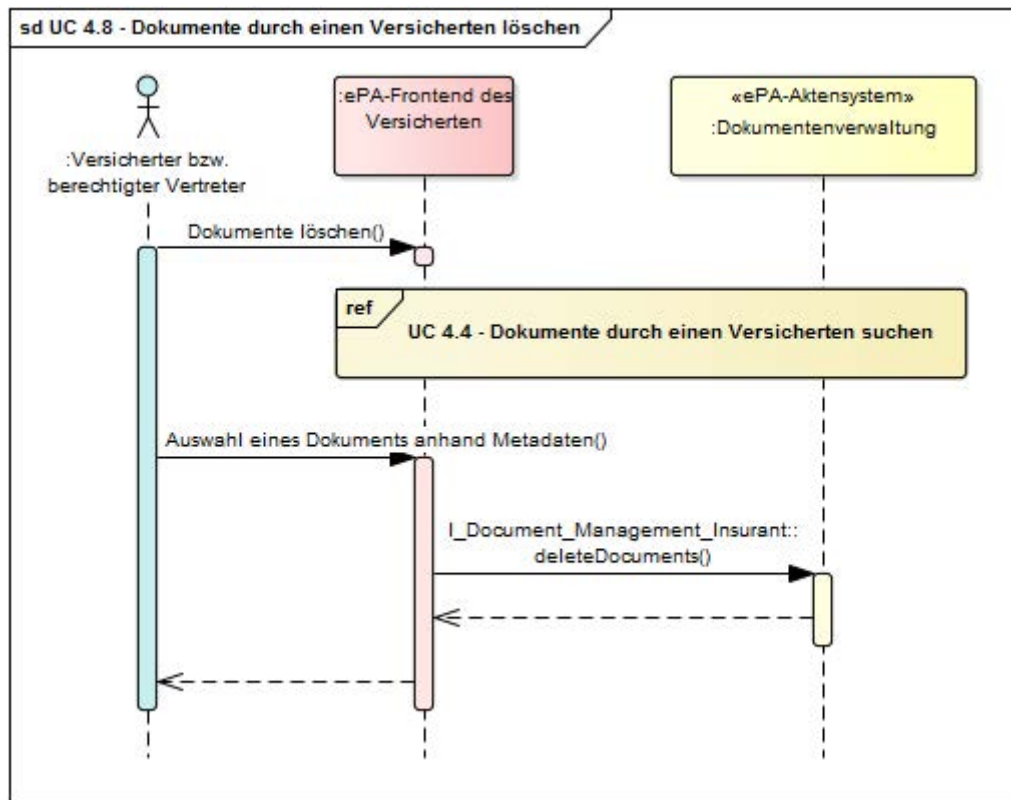


Abbildung 32: Dokumente durch einen Versicherten löschen

[<=]

3.7.8 Dokumente durch einen Leistungserbringer anzeigen

Mit diesem Anwendungsfall werden ein Dokument oder mehrere ausgewählte Dokumente aus der Komponente Dokumentenverwaltung heruntergeladen und entschlüsselt. Nach der Entschlüsselung liegen diese temporär oder persistent in einem Speicher im bzw. am Primärsystem des Leistungserbringers vor und können mit dem Standardprogramm für einen gegebenen Dateitypen geöffnet werden. Eine Ablage in einen persistenten Speicher ist möglich. Die Übernahme eines Dokuments in die Primärdokumentation des Leistungserbringers ist jedoch kein Betrachtungsgegenstand der Fachanwendung ePA.

EPA-EPF-A_0038 - Anwendungsfall „Dokumente durch einen Leistungserbringer anzeigen“

Alle am Anwendungsfall „Dokumente durch einen Leistungserbringer anzeigen“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 26: Dokumente durch einen Leistungserbringer anzeigen

Name	UC 4.9 - Dokumente durch einen Leistungserbringer anzeigen
Vorbedingung	Der Mitarbeiter der Leistungserbringerinstitution hat ein oder mehrere Dokumente identifiziert (z. B. über eine vorhergehende Suche), die gelöscht werden sollen.

Kurzbeschreibung (Außensicht)	Ein Mitarbeiter der Leistungserbringerinstitution fordert über das PS am Konnektor den Download eines über den Dokument-Identifikator identifizierten Dokuments an. Der Dokument-Identifikator wird entweder einer vorangegangenen Dokumentsuche entnommen oder ist im PS bereits bekannt. Das Dokument kann in das PS übernommen werden.
Nachbedingung	Im PS liegt das angeforderte Dokument aus der Fachanwendung ePA vor.

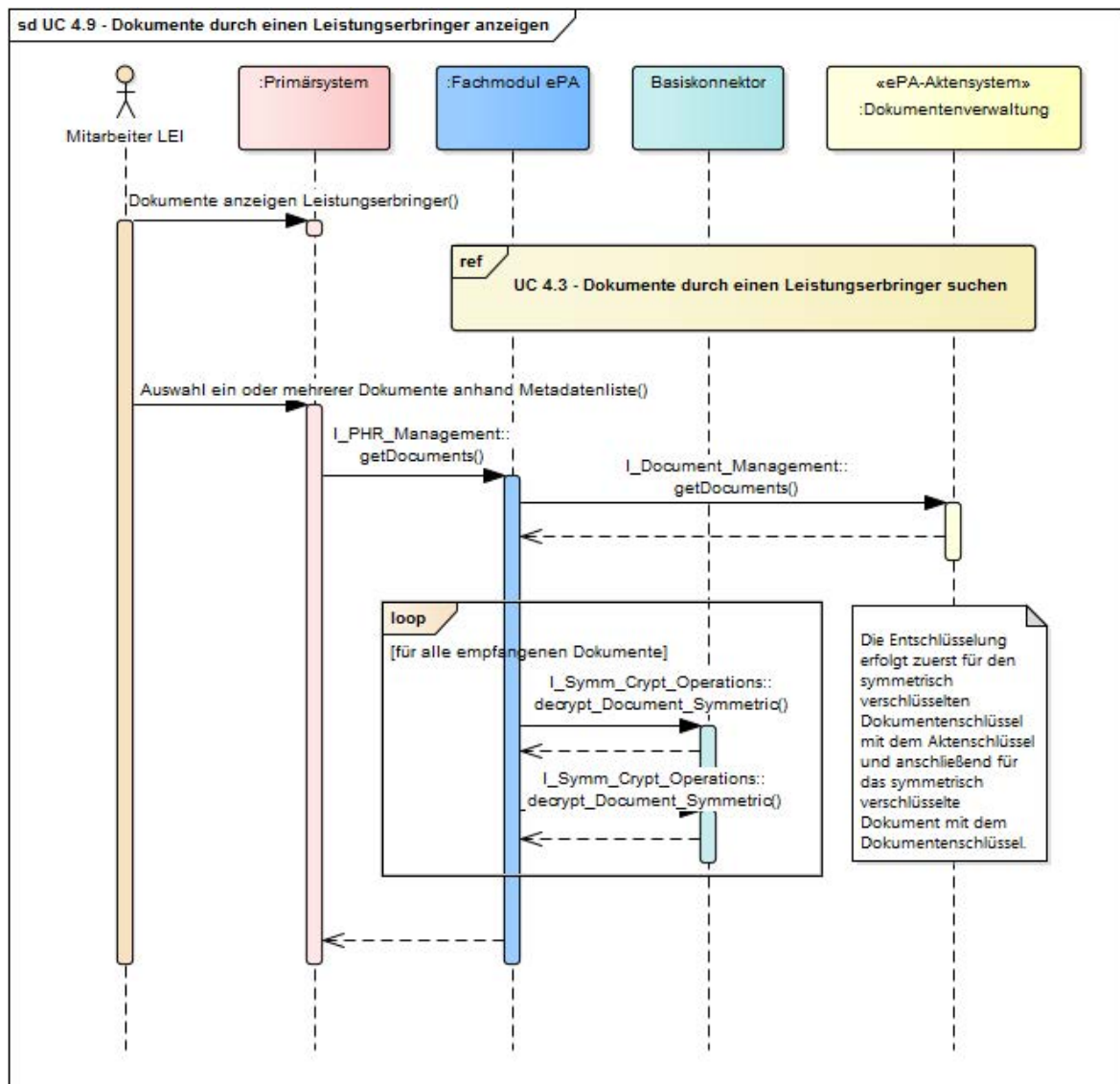


Abbildung 33: Dokumente durch einen Leistungserbringer anzeigen

[<=]

3.7.9 Dokumente durch einen Versicherten anzeigen

Mit diesem Anwendungsfall werden ein Dokument oder mehrere ausgewählte Dokumente aus der Komponente Dokumentenverwaltung heruntergeladen und entschlüsselt. Nach der Entschlüsselung liegen diese temporär oder persistent in einem Speicher im bzw. am Gerät des Versicherten vor und können mit dem Standardprogramm für einen gegebenen Dateitypen geöffnet werden. Eine Ablage in einen persistenten Speicher durch den Versicherten bzw. einen berechtigten Vertreter ist möglich. Die Eigenorganisation von Dokumenten des Versicherten durch den Versicherten ist jedoch kein Betrachtungsgegenstand der Fachanwendung ePA.

EPA-EPF-A_0039 - Anwendungsfall „Dokumente durch einen Versicherten anzeigen“

Alle am Anwendungsfall „Dokumente durch einen Versicherten anzeigen“ beteiligten Produkttypen und Komponenten **MÜSSEN** die nachfolgenden Festlegungen umsetzen.

Tabelle 27: Dokumente durch einen Versicherten anzeigen

Name	UC 4.10 - Dokumente durch einen Versicherten anzeigen
Vorbedingung	-
Kurzbeschreibung (Außensicht)	Ein Versicherter oder ein von ihm berechtigter Vertreter wählt am Frontend des Versicherten ein oder mehrere Dokumente aus, die heruntergeladen werden sollen. Das Frontend des Versicherten überträgt die Anforderung an das ePA-Aktensystem, das die gewünschten Dokumente an das Frontend des Versicherten zurückliefert.
Nachbedingung	Die zur Anzeige gewählten Dokumente sind auf einem lokal eingebundenen Speicher am Gerät des Versicherten heruntergeladen.

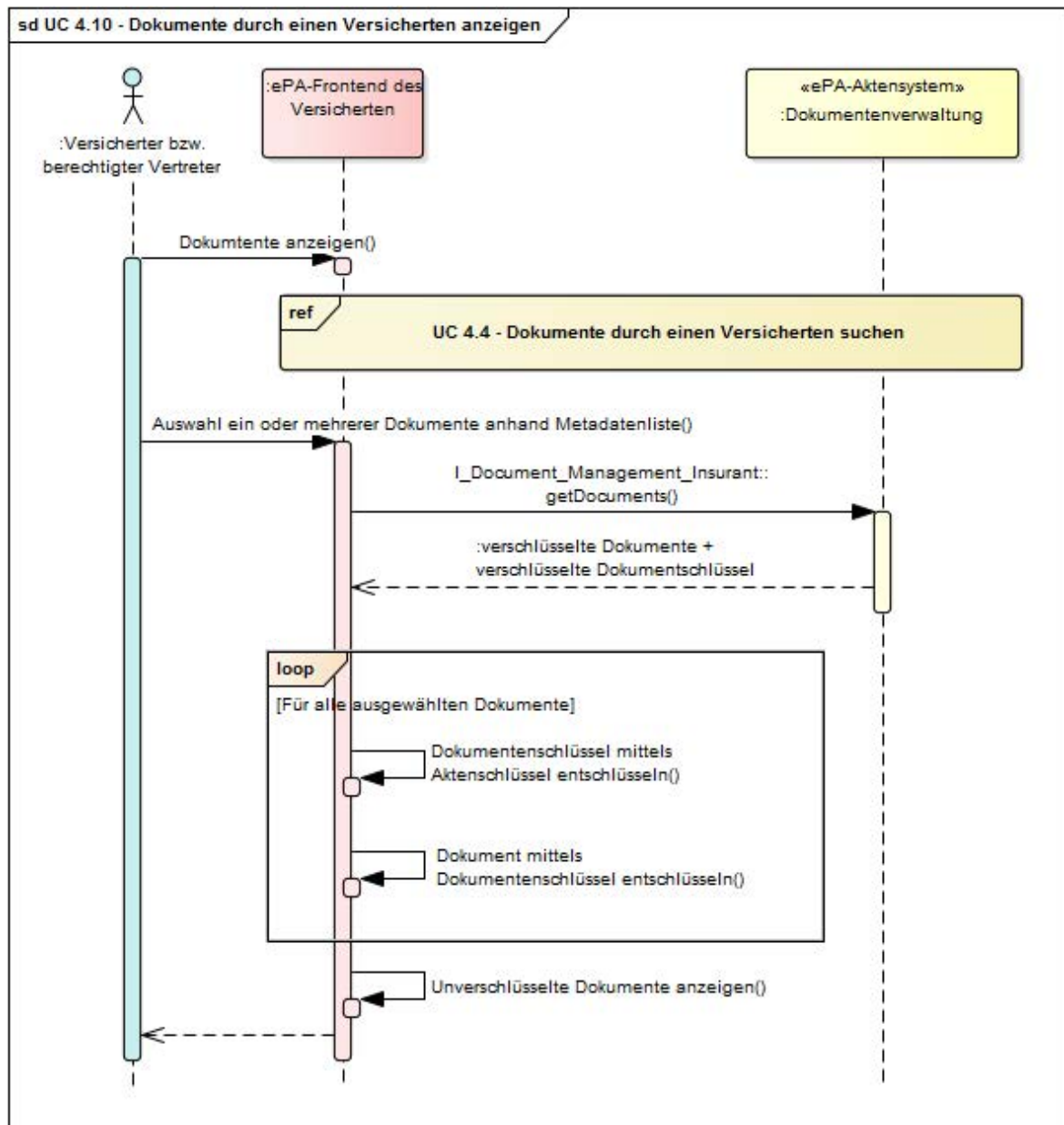


Abbildung 34: Dokumente durch einen Versicherten anzeigen

[<=]

3.8 Benachrichtigungsverwaltung

3.8.1 Benachrichtigungen durch einen Leistungserbringer verwalten

Die Fachanwendung ePA realisiert den Anwendungsfall „UC 5.1 - Benachrichtigungen durch einen Leistungserbringer verwalten“ über das Primärsystem. Hierfür ist kein „Push“-Mechanismus vorgesehen. Es bietet sich daher an, über den Abruf von aktuellen Metadaten Veränderungen über geänderte oder neue Dokumente auf Basis lokal vor-

handener Metadaten als Benachrichtigung aufzubereiten und diese dem Mitarbeiter der Leistungserbringerinstitution in der Ansicht hervorzuheben. Die Verwaltung der Benachrichtigung (Inhalt, Aktivierung/Deaktivierung, Benachrichtigungszeiträume) erfolgt über das Primärsystem.

3.8.2 Benachrichtigungen durch einen Versicherten verwalten

Eine Benachrichtigung über neue oder geänderte ePA-Dokumente erleichtert die Handhabung der Anwendung für Versicherte. Dafür ist im ePA-Frontend des Versicherten ein Benachrichtigungsmechanismus vorgesehen, der nach dem Start der Anwendung auf Wunsch über entsprechende Änderungen informiert. Das ePA-Frontend des Versicherten bietet dem Versicherten die Verwaltung der Benachrichtigungseinstellungen im Anwendungsfall "UC 5.2 - Benachrichtigungen durch einen Versicherten verwalten" für die interne Konfigurationsanpassung der Auswahlparameter für Benachrichtigungen im ePA-Frontend des Versicherten intern an.

EPA-EPF-A_0041 - Anwendungsfall „Benachrichtigung durch einen Versicherten verwalten“

Das ePA-Frontend des Versicherten MUSS eine Benachrichtigung für Versicherte auf Basis der Metadaten eingestellter Dokumente und Protokolldaten zu gelöschten Dokumenten umsetzen. Einstellungsparameter für Benachrichtigungen sind:

- Benachrichtigungszeitraum (seit der letzten Anmeldung; durch den Versicherten einstellbarer, flexibel zurückliegender Zeitraum; zurückliegender Zeitraum beginnend mit einem konkreten Datum (durch den Versicherten einstellbar) (X Wochen, X Monate)
- Benachrichtigungen aktivieren/deaktivieren.

[<=]

EPA-EPF-A_0042 - Anwendungsfall „Benachrichtigung nach einem Login“

Das ePA-Frontend des Versicherten MUSS nach dem Login eines Versicherten eine Benachrichtigung über neue und gelöschte Dokumente anzeigen, sofern diese Benachrichtigung aktiviert wurde.

[<=]

3.9 Protokollverwaltung

3.9.1 Protokolldaten durch einen Versicherten einsehen

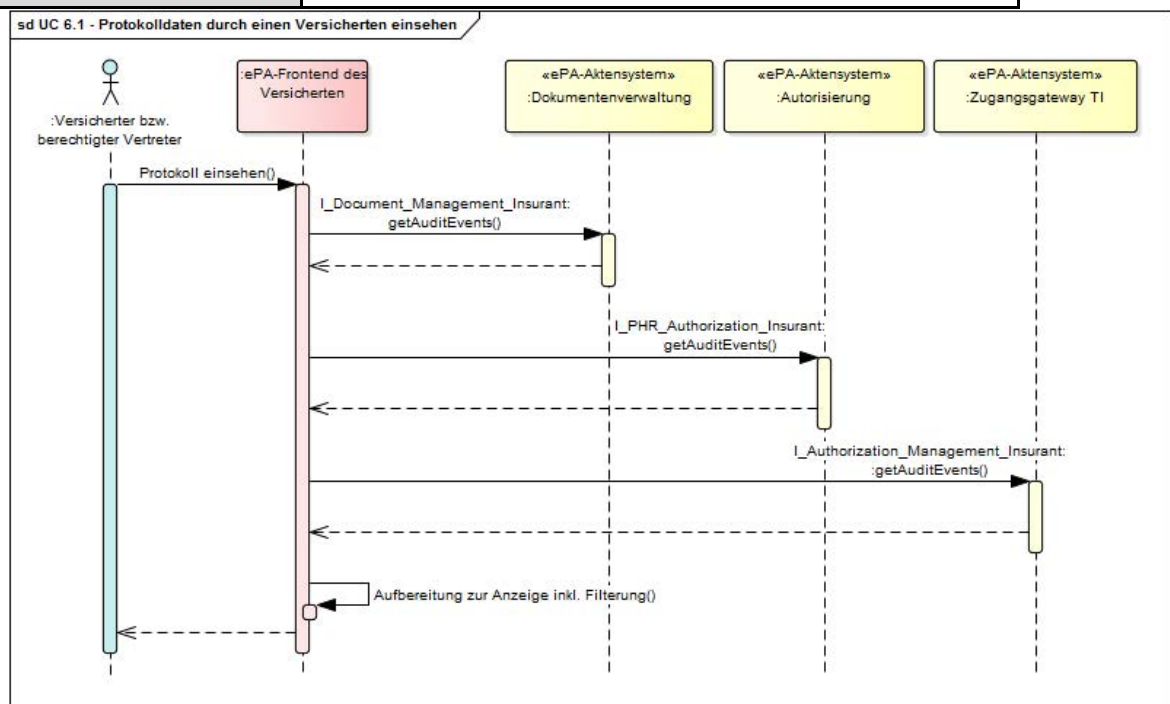
Mit diesem Anwendungsfall nimmt der Versicherte Einsicht in das §291a-konforme Zugriffsprotokoll und die Einträge aus dem Verwaltungsprotokoll. Darin ersichtlich sind die dokumentierten Zugriffe aller Nutzer auf seine im ePA-Aktensystem gespeicherten Dokumente.

EPA-EPF-A_0043 - Anwendungsfall „Protokolldaten durch einen Versicherten einsehen“

Alle am Anwendungsfall „Protokolldaten durch einen Versicherten einsehen“ beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 28: Protokolldaten durch einen Versicherten einsehen

Name	UC 6.1 - Protokolldaten durch einen Versicherten einsehen
Vorbedingung	Der Versicherte ist am ePA-Aktensystem angemeldet.
Kurzbeschreibung (Außensicht)	Ein Versicherter oder ein von ihm berechtigter Vertreter ruft über das ePA-Frontend des Versicherten Protokolleinträge zur Anzeige ab, welche die vergangenen Zugriffe auf sein Aktenkonto dokumentieren. Die Fachanwendung ePA bietet ihm dabei geeignete Filterungsfunktionen an, welche die Anzahl der anzuzeigenden Protokolleinträge nach wählbaren Kriterien (z. B. Zeiträume oder Attribute von Dokumenten) einschränken.
Nachbedingung	-



[<=]

Abbildung 35: Protokolldaten durch einen Versicherten einsehen

3.9.2 Übertragungsprotokoll einsehen Leistungserbringer

Zur Nachvollziehbarkeit der getätigten Dokumententransfers für Leistungserbringer ist ein Übertragungsprotokoll vorgesehen, welches vom Primärsystem der berechtigten Leistungserbringerinstitution geführt wird.

Die Umsetzung des Anwendungsfalls zur "UC 6.2 - Übertragungsprotokoll einsehen Leistungserbringer" zur Nachvollziehbarkeit getätigter ePA-Zugriffe einer Leistungserbringereinstitution in den Aktenkonten der Versicherten obliegt dem Primärsystem.

4 Systemzerlegung (Deployment)

4.1 Produkttypen der Fachanwendung

Die Fachanwendung ePA realisiert die fachlichen Anwendungsfälle über das Zusammenspiel mehrerer Produkttypen in verschiedenen Zonen der Telematikinfrastruktur. Die Systemzerlegung der Fachanwendung ist in der nachfolgenden Abbildung 42: „Systemzerlegung ePA“ dargestellt. Sie ordnet die Produkttypen (blau dargestellt) und ihre Komponenten (gelb dargestellt) den Zonen gemäß Zonenmodell der TI-Plattform aus [gemKPT_Arch_TIP] ergänzt um die Personal Zone zu.

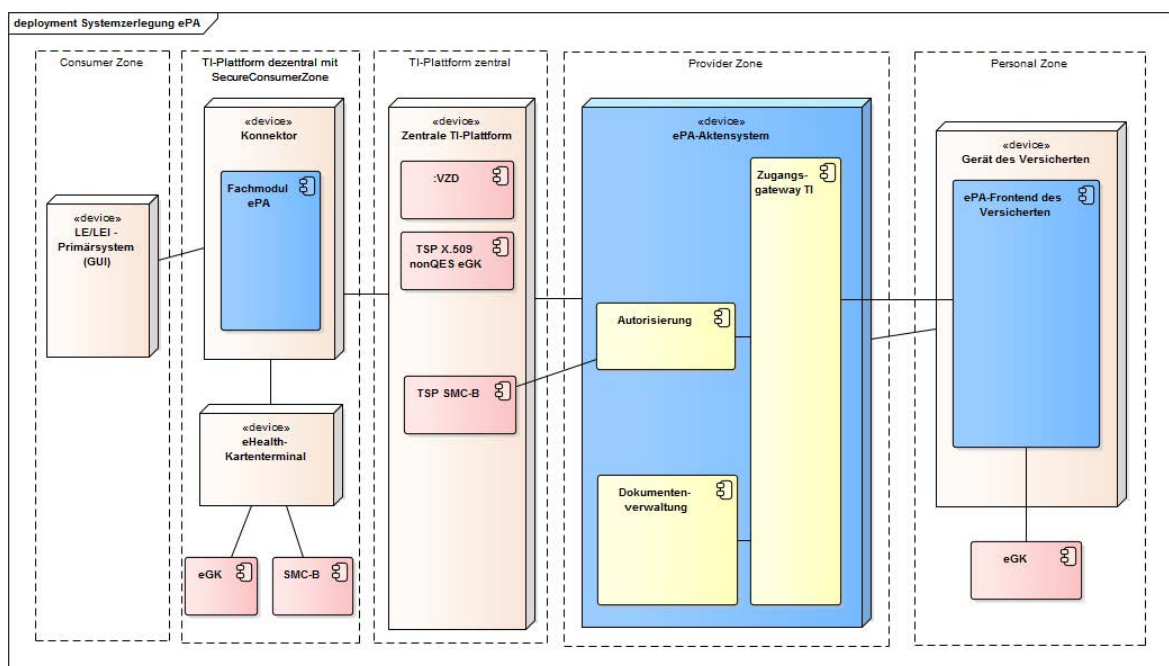


Abbildung 36: Systemzerlegung ePA

In der Umgebung der Leistungserbringer erweitert das Fachmodul ePA im Konnektor die Funktionalität des Konnektors um die Funktionen zur Realisierung der fachlichen Anwendungsfälle für Leistungserbringer. Das Primärsystem stellt dabei das Frontend des Leistungserbringers dar.

Der Produkttyp ePA-Aktensystem wird durch den jeweiligen Anbieter verantwortet und setzt sich aus den Komponenten für die Autorisierung, die Dokumentenverwaltung und dem Zugangsgateway (inkl. Authentifizierung für Versicherten und Vertreter) zusammen.

In der Umgebung des Versicherten (Personal Zone) kapselt der Produkttyp „ePA-Frontend des Versicherten“ die funktionalen Abläufe der fachlichen Anwendungsfälle der Fachanwendung auf einem Gerät des Versicherten. Das ePA-Frontend stellt dem Versicherten die Anwendungsfälle über eine grafische Benutzeroberfläche zur Verfügung und bindet die eGK des Versicherten über einen Kartenleser ein. Dabei wird ein Kartenleser der Klasse 1 angenommen, der über keine Sicherheitsmerkmale wie Display und PIN-Pad verfügt.

4.1.1 Produkttyp Fachmodul ePA

Das Fachmodul ePA ist in der Secure Consumer Zone im Konnektor angesiedelt, kapselt die Fachlogik gegenüber den Primärsystemen der Leistungserbringer und führt die sicherheitsrelevanten Anteile der Fachlogik (z. B. die Verschlüsselung der Dokumente) aus.

EPA-EPF-A_0045 - Fachmodul ePA Schnittstellen zum Primärsystem

Das Fachmodul ePA MUSS die im Folgenden benannten Schnittstellen bereitstellen.

Tabelle 29: Schnittstellen Fachmodul ePA

Bereitgestellte Schnittstelle	Nutzer	Bedingung
I_PHR_Management	Primärsystem	-
I_Authorization_Administration	Primärsystem	-
I_Account_Administration	Primärsystem	-

[<=]

EPA-EPF-A_0046 - Fachmodul ePA – Session-Trennung

Das Fachmodul ePA MUSS eine Separierung zwischen den sessionbezogenen Daten je Aktenkonto eines Versicherten umsetzen.

[<=]

EPA-EPF-A_0047 - Fachmodul ePA – Authentifizierungsbestätigung der LEI

Das Fachmodul ePA MUSS sicherstellen, dass eine mit einer SMC-B signierte Authentifizierungsbestätigung ausgestellt wird.

[<=]

EPA-EPF-A_0048 - Fachmodul ePA – IHE-Framework

Das Fachmodul ePA MUSS die Operationen der Schnittstellen I_PHR_Management mit Techniken des IHE-Frameworks umsetzen.

[<=]

EPA-EPF-A_0050 - Fachmodul ePA – Ungültige Kartenversion

Das Fachmodul ePA DARF Karten der TI der Version kleiner Generation 2 NICHT verwenden.

[<=]

A_13766 - Fachmodul ePA - Skalierbarkeit

Das Fachmodul ePA MUSS in der Lage sein, parallele Anfragen zu Operationen in verschiedenen Akten unterschiedlicher Versicherter gleichzeitig zu bearbeiten.[<=]

A_13826 - Fachmodul ePA - Minimierung von PIN-Eingaben

Das Fachmodul ePA MUSS die Anforderung von PIN-Eingaben für eGK und SMC-B auf die technisch erforderlichen Eingaben beschränken.[<=]

4.1.2 Produkttyp ePA-Aktensystem

Das ePA-Aktensystem vereint die im Folgenden benannten Teilkomponenten in einem Produkttyp. Es stellt sicher, dass nur authentifizierte und autorisierte Nutzer mit dem ePA-Aktensystem interagieren. In einer Komponente zur Dokumentenverwaltung verwaltet das ePA-Aktensystem die Dokumente zu einem Aktenkonto eines Versicherten.

EPA-EPF-A_0051 - Produkttyp ePA-Aktensystem

Das ePA-Aktensystem MUSS die Komponenten

- Autorisierung,
- Dokumentenverwaltung und
- Zugangsgateway (inkl. Authentifizierung Vers./Vertreter) bereitstellen.

[<=]

EPA-EPF-A_0052 - Produkttyp ePA-Aktensystem – Zugriff auf Verzeichnisdienst

Das ePA-Aktensystem MUSS sicherstellen, dass systeminterne Zugriffe auf den Verzeichnisdienst der TI-Plattform nur über die Komponente „Zugangsgateway“ erfolgen.

[<=]

A_16435 - Produkttyp ePA-Aktensystem - konzeptionelle Operation Download Exportpaket

Das ePA-Aktensystem MUSS für den Download des Exportpakets beim Anbieterwechsel über eine URL die konzeptionelle Operation

I_Account_Management::GetExportPackage zur Verfügung stellen.[<=]

4.1.2.1 Komponente „Autorisierung“

Die Komponente „Autorisierung“ stellt authentifizierten Nutzern eines Aktenkontos bei gegebener Autorisierung das für sie jeweils empfängerverschlüsselte Schlüsselmaterial bereit. Neben der zentralen Verwaltung des empfängerbezogenen verschlüsselten Schlüsselmaterials erfolgt hierbei auch ein Berechtigungserhalt für Versicherte.

EPA-EPF-A_0057 - Komponente Autorisierung – Schnittstellen

Die Komponente „Autorisierung“ MUSS die im Folgenden benannten Schnittstellen bereitstellen.

Tabelle 30: Schnittstellen-Autorisierung

Bereitgestellte Schnittstelle	Nutzer	Bedingung
I_Authorization	Fachmodul ePA	-
I_Authorization_Management	Fachmodul ePA	-
I_Authorization_Insurant	ePA-Frontend des Versicherten	-
I_Authorization_Management_Insurant	ePA-Frontend des Versicherten	-

[<=]

EPA-EPF-A_0058 - Komponente Autorisierung, Berechtigungssystem

Die Komponente „Autorisierung“ MUSS für die Verwaltung und den Zugriff auf das gespeicherte, verschlüsselte Schlüsselmaterial ein Berechtigungssystem auf Basis der Authentifizierungsbestätigung authentifizierter Nutzer umsetzen.

[<=]

A_16199 - Komponente Autorisierung - Rollenprüfung §291a

Die Komponente Autorisierung MUSS vor dem Ausstellen einer Autorisierungsbestätigung für den Zugriff auf medizinische Daten prüfen, ob der authentifizierte Nutzer als Versicherter oder gemäß einer Berufsgruppe nach § 291a Abs. 4 Satz 1 Nr. 2 SGB V für den Zugriff berechtigt ist.[<=]

EPA-EPF-A_0059 - Komponente Autorisierung – Ausstellung Autorisierungsbestätigung

Die Komponente „Autorisierung“ MUSS nach erfolgreicher Prüfung der Berechtigung eines Nutzers eine Autorisierungsbestätigung erzeugen.

[<=]

EPA-EPF-A_0060 - Komponente Autorisierung – Wiederherstellungsidentität

Die Komponente „Autorisierung“ MUSS den privaten Schlüssel einer Wiederherstellungsidentität in einem HSM sicher speichern.

[<=]

EPA-EPF-A_0061 - Komponente Autorisierung – Geräteprüfung

Die Komponente „Autorisierung“ MUSS bei Autorisierungsanfragen über I_Authorization_Insurant prüfen, ob das anfragende Gerät in der Liste der freigeschalteten Geräte des Versicherten bzw. seines Vertreters in diesem Aktenkonto enthalten ist. Ist das Gerät nicht enthalten, MUSS die Autorisierung abgebrochen und ein Freischaltprozess über den hinterlegten Benachrichtigungskanal gestartet werden. Für Autorisierungsanfragen aus der Leistungserbringerumgebung entfällt die Geräteprüfung.

[<=]

EPA-EPF-A_0062 - Komponente Autorisierung – Geräteverwaltung

Die Komponente „Autorisierung“ MUSS dem authentifizierten Versicherten über eine grafische Oberfläche das Verwalten derjenigen Gerätekennungen anbieten, die der Versicherte bzw. sein Vertreter nutzen, um auf das Aktenkonto zuzugreifen.

[<=]

A_13768 - Komponente Autorisierung – Skalierbarkeit

Die Komponente „Autorisierung“ MUSS in der Lage sein, nebenläufige Operationen in verschiedene Akten gleichzeitig zu bearbeiten.[<=]

4.1.2.2 Komponente „Dokumentenverwaltung“

Die Komponente „Dokumentenverwaltung“ stellt ein Dokumentenmanagementsystem der medizinischen Dokumentation des Versicherten dar.

EPA-EPF-A_0063 - Komponente Dokumentenverwaltung – Schnittstellen

Die Komponente „Dokumentenverwaltung“ MUSS die im Folgenden benannten Schnittstellen bereitstellen.

Tabelle 31: Schnittstellen Dokumentenverwaltung

Bereitgestellte Schnittstelle	Nutzer	Bedingung
I_Document_Management	Fachmodul ePA	-
I_Document_Management_Insurant	ePA-Frontend des Versicherten	-
I_Account_Management_Insurant	ePA-Frontend des Versicherten	-
I_Document_Management_Connect	ePA-Frontend des Versicherten, Fachmodul ePA	-

[<=]

EPA-EPF-A_0064 - Komponente Dokumentenverwaltung – Berechtigungssystem

Die Komponente „Dokumentenverwaltung“ MUSS für die Verwaltung und den Zugriff der gespeicherten, verschlüsselten Daten ein Berechtigungssystem auf Basis der Authentifizierungs- und Autorisierungsbestätigung authentifizierter Nutzer umsetzen.

[<=]

EPA-EPF-A_0065 - Komponente Dokumentenverwaltung – Datenverarbeitung

Die Komponente „Dokumentenverwaltung“ MUSS die folgenden Daten zum Aktenkonto des Versicherten in einer vertrauenswürdigen Ausführungsumgebung („VAU“) verarbeiten, da die darin transportierten Informationen in der Komponente Dokumentenverwaltung im Klartext verarbeitet werden sollen:

- Metadaten zu verschlüsselten Dokumenten
- Inhalte des Zugriffsprotokolls zum Aktenkonto des Versicherten
- Policy-Dokumente für alle vom Versicherten vergebenen Zugriffsberechtigungen auf Datenobjekte in der Komponente „Dokumentenverwaltung“.

[<=]

EPA-EPF-A_0066 - Komponente Dokumentenverwaltung – Datenpersistierung

Die Komponente „Dokumentenverwaltung“ MUSS die folgenden Daten zum Aktenkonto des Versicherten mit einem zur Laufzeit temporär übergebenen Kontextschlüssel verschlüsselt persistieren und diesen nach Abschluss sicher löschen:

- Metadaten zu verschlüsselten Dokumenten
- Inhalte des Zugriffsprotokolls zum Aktenkonto des Versicherten
- Policy Document als Summe aller vom Versicherten vergebenen Zugriffsberechtigungen auf Datenobjekte in der Komponente Dokumentenverwaltung.

[<=]

EPA-EPF-A_0067 - Komponente Dokumentenverwaltung – IHE-Framework

Die Komponente „Dokumentenverwaltung“ MUSS die Operationen der Schnittstellen I_Document_Management und I_Document_Management_Insurant mit Technologien des IHE-Frameworks umsetzen.

[<=]

EPA-EPF-A_0068 - Komponente Dokumentenverwaltung – Dateityppprüfung

Die Komponente „Dokumentenverwaltung“ MUSS Dokumente, die eingestellt werden sollen, ablehnen, wenn sie gemäß der Angaben in den Metadaten nicht einem der folgenden Dateitypen PDF, JPG, TIFF, TXT, RTF, DOCX, XLSX, ODT, ODS, XML, HL7 CDA/R2 XML entsprechen. Diese Liste gilt nur initial.

[<=]

EPA-EPF-A_0069 - Komponente Dokumentenverwaltung – Konfigurationsänderung der Dokumententypen

Die Komponente „Dokumentenverwaltung“ MUSS die Liste der zulässigen Dateitypen durch eine Konfigurationsanpassung verändern können.

[<=]

EPA-EPF-A_0072 - Komponente Dokumentenverwaltung – Dokumentengrößenprüfung

Die Komponente „Dokumentenverwaltung“ MUSS Dokumente, die eingestellt werden sollen, ablehnen, wenn sie die Maximaldateigröße überschreitet, die der Konnektor ge-

mäß aktuell freigegebener und veröffentlichter Spezifikation mindestens in der Lage ist, zu verarbeiten. [≤]

Dies dient der Interoperabilität zwischen den Systemen verschiedener Leistungserbringer, die unabhängig voneinander mit Dokumenten eines Versicherten in ePA arbeiten. Die Spezifikation des Konnektors fordert im Performancemodell eine Mindestdateigröße für zu verarbeitende Dokumente. Somit ist nicht sichergestellt, dass alle zugelassenen Produkte des Produkttyps Konnektor in der Lage sind, Dokumente größer als die Mindestdateigröße zu verarbeiten. Daraus ergibt sich eine maximal verarbeitbare Dateigröße in der Komponente „Dokumentenverwaltung“, auf welche die Systeme der Leistungserbringer über den Konnektor zugreifen. In der aktuell veröffentlichten Spezifikation des Konnektors wird eine verarbeitbare Mindestdateigröße von 25 MByte gefordert.

EPA-EPF-A_0073 - Komponente Dokumentenverwaltung – automatische Befüllung von Attributen

Die Komponente „Dokumentenverwaltung“ MUSS die folgenden Attribute beim Einstellen von neuen Dokumenten automatisch befüllen:

- Einstelldatum und -uhrzeit
- Dateigröße.

[≤]

4.1.2.3 Komponente „Zugangsgateway“

Die Komponente „Zugangsgateway“ ermöglicht dem ePA-Frontend des Versicherten über das Internet die sichere Nutzung des ePA-Aktensystems. Versicherte und Vertreter werden am Zugangsdienst authentifiziert. Außerdem sorgt das Zugangsgateway für die Abwehr gegen Angriffe auf das ePA-Aktensystem und die TI im Allgemeinen. Eine weitere Aufgabe des Zugangsgateways ist die sichere Weiterleitung der Client Requests auf nachgelagerte ePA-Komponenten. Auch unterstützt das Zugangsgateway die Suche nach ENC-Zertifikaten im Verzeichnisdienst.

EPA-EPF-A_0074 - Komponente Zugangsgateway – Schnittstellen

Die Komponente „Zugangsgateway“ MUSS die im Folgenden benannten Schnittstellen bereitstellen.

Tabelle 32: Schnittstellen Authentisierung Versicherter

Bereitgestellte Schnittstelle	Nutzer	Bedingung
I_Authentication_Insurant	Fachmodul ePA, ePA-Frontend des Versicherten	

[≤]

Die Authentifizierungsfunktionalität der Schnittstelle I_Authentication_Insurant der Komponente Zugangsgateway wird standardmäßig für die Authentifizierung des Versicherten aus der Umgebung des Versicherten mittels eGK und PIN verwendet. Im Anwendungsfall *UC 3.7 - Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern* erfolgt die Anmeldung im ePA-Aktensystem aus der Umgebung der Leistungserbringer mittels eGK. Für diesen Zweck muss die Komponente Zugangsgateway diese Schnittstelle zusätzlich für Fachmodule bereitstellen.

EPA-EPF-A_0075 - Komponente Zugangsgateway – Authentifizierung des Versicherten

Die Komponente „Zugangsgateway“ MUSS Versicherte oder Vertreter über ihre eGK authentifizieren.[<=]

Durch die Nutzung der kryptografischen Identitäten der eGK und den Einsatz des privaten Schlüsselmaterials auf der eGK wird in diesem Zusammenhang eine PIN-Eingabe auf Seiten des Versicherten erzwungen (2-Faktor-Authentifizierung: Karte + PIN).

EPA-EPF-A_0076 - Komponente Zugangsgateway – Ausstellung Authentifizierungsbestätigung

Die Komponente „Zugangsgateway“ MUSS nach erfolgreicher Authentifizierung eines Versicherten oder Vertreters eine Authentifizierungsbestätigung erzeugen.

[<=]

EPA-EPF-A_0077 - Komponente Zugangsgateway – Kartenversionen eGK

Die Komponente „Zugangsgateway“ DARF eGKs der Versionen kleiner G2 NICHT akzeptieren.

[<=]

EPA-EPF-A_0078 - Komponente Zugangsgateway – Erreichbarkeit im Internet

Die Komponente „Zugangsgateway“ MUSS im Internet erreichbar sein.

[<=]

EPA-EPF-A_0079 - Komponente Zugangsgateway – Sicherung der TI

Die Komponente „Zugangsgateway“ MUSS die TI gegenüber dem Internet absichern.

[<=]

EPA-EPF-A_0080 - Komponente Zugangsgateway – Zugang zur TI

Die Komponente „Zugangsgateway“ MUSS sicherstellen, dass nur nach erfolgreicher Authentifizierung der Zugang zur TI gewährt wird.

[<=]

A_13769 - Komponente Zugangsgateway - Skalierbarkeit

Die Komponente Zugangsgateway MUSS in der Lage sein, nebenläufige Operationen in verschiedene Akten gleichzeitig zu bearbeiten.[<=]

4.1.3 Produkttyp ePA-Frontend des Versicherten

Das ePA-Frontend des Versicherten wird in der Versichertenumgebung genutzt und ermöglicht dem Versicherten die Nutzung des ePA-Aktensystems. Das ePA-Frontend des Versicherten führt die dezentrale Fachlogik der Fachanwendung ePA in der persönlichen Umgebung des Versicherten aus.

EPA-EPF-A_0081 - Produkttyp ePA-Frontend des Versicherten – GUI

Das ePA-Frontend des Versicherten MUSS über eine grafische Oberfläche (GUI) als Frontend bedienbar sein.

[<=]

A_13761 - Umsetzung von Renderingvorgaben

Das ePA-Frontend des Versicherten KANN die Visualisierungsvorgaben für Daten und Dokumente in ePA umsetzen, wenn diese in den Daten bzw. Dokumenten enthalten sind oder diese über eine Verlinkung eingebunden werden.[<=]

EPA-EPF-A_0082 - Produkttyp ePA-Frontend des Versicherten – Barrierefreiheit

Das ePA-Frontend des Versicherten SOLL Bedienungselemente der Barrierefreiheit umsetzen.

[<=]

EPA-EPF-A_0083 - Produkttyp ePA-Frontend des Versicherten – eGK-Anbindung

Das ePA-Frontend des Versicherten MUSS die eGK des Versicherten über eine lokale Schnittstelle zu einem Kartenlesegerät der Klasse 1 am Gerät des Versicherten in die Ausführung von Anwendungsfällen einbeziehen.

[<=]

EPA-EPF-A_0084 - Produkttyp ePA-Frontend des Versicherten – eGK-PIN

Das ePA-Frontend des Versicherten MUSS dem Versicherten über eine grafische Oberfläche das Ändern und Entsperren der MRPIN.home auf der eGK anbieten.

[<=]

A_13827 - Produkttyp ePA-Frontend des Versicherten - Reduzierung von PIN-Eingaben

Das ePA-Frontend des Versicherten MUSS die Anforderung von PIN-Eingaben für die eGK auf die technisch erforderlichen Eingaben beschränken.[<=]

EPA-EPF-A_0085 - Produkttyp ePA-Frontend des Versicherten – eGK-Version

Das ePA-Frontend des Versicherten DARF eine eGK der Version kleiner Generation 2 NICHT verwenden.

[<=]

A_13825 - Produkttyp ePA-Frontend des Versicherten – Interoperabilität ePA-Aktensysteme

Das ePA-Frontend des Versicherten MUSS durch die Nutzung der interoperablen Schnittstellen eines ePA-Aktensystems

- I_Authentication_Insurant
- I_Authorization_Insurant
- I_Authorization_Management_Insurant
- I_Document_Management_Insurant
- I_Account_Management_Insurant
- I_Document_Management_Connect

die Verwendung von ePA in verschiedenen Aktenkonten verschiedener Anbieter eines ePA-Aktensystems erlauben.[<=]

EPA-EPF-A_0086 - Produkttyp ePA-Frontend des Versicherten - Drucken und Speichern von Listen

Das ePA-Frontend des Versicherten MUSS dem Versicherten über eine grafische Oberfläche das Drucken und Speichern von Listen (z. B. Liste der Vertreter, Liste der Vertretenden, Protokolle, Suchergebnisse etc.) anbieten.[<=]

A_13841 - Produkttyp ePA-Frontend des Versicherten - Filtern und Sortieren von Listen

Das ePA-Frontend des Versicherten MUSS dem Versicherten über eine grafische Oberfläche das lokale Filtern und Sortieren von Listen (z.B. Ergebnisliste einer Dokumentensuche, Protokolleinträge) ermöglichen.[<=]

A_13817 - Produkttyp ePA-Frontend des Versicherten - Wechsel in Vertretungsmodus

Das ePA-Frontend des Versicherten MUSS dem Versicherten die wechselnde Verwendung verschiedener RecordIdentifier für die Arbeit im eigenen Aktenkonto und ggfs. zur Wahrnehmung von Vertretungen in anderen Aktenkonten erlauben.[<=]

Die dezentrale Fachlogik der Fachanwendung ePA im ePA-Frontend des Versicherten kann als Softwarekomponente in Anwendungen umgesetzt werden, die dem Versicherten weitere Funktionalitäten anbieten. Die Anwendung, welche die dezentrale Fachlogik des

Versicherten umsetzt, wird weiterhin als Produkttyp „ePA-Frontend des Versicherten“ betrachtet. Die darin enthaltene zusätzliche Funktionalität ist jedoch im Rahmen der Zulassung nicht geprüft.

A_13658 - Zusätzliche Funktionalität im ePA-Frontend des Versicherten

Das ePA-Frontend des Versicherten KANN zusätzliche Funktionalität enthalten, sofern diese nicht den Schutz der personenbezogenen und medizinischen Daten des Versicherten in ePA gefährdet.

[<=]

A_15671 - Produkttyp ePA-Frontend des Versicherten - Automatisches Setzen von Metadaten

Das ePA-Frontend des Versicherten MUSS die folgenden Attribute beim Einstellen von neuen Dokumenten automatisch befüllen:

- einstellender Akteur
- Dateiformat.

[<=]

4.1.4 Primärsystem

Das Primärsystem stellt das Frontend für Leistungserbringer dar. Hier greift der Leistungserbringer auf die Fachanwendung ePA zu.

Zur Sicherstellung der Interoperabilität kommen vorrangig standardisierte Schnittstellen der IHE XDS-Familie zum Einsatz (siehe Schnittstellenbeschreibung zu `I_PHR_Management`). Funktionalitäten der Berechtigungsverwaltung werden über eine separate Schnittstelle (`I_Authorization_Administration`) realisiert. Operationen im Zusammenhang mit der Kontoeröffnung des Versicherten werden in der Schnittstelle `I_Account_Administration` zusammengefasst.

Die Primärsysteme verwalten in einer lokalen Datenbasis notwendige Informationen zu Aktenkonten der Versicherten und der in der Fachanwendung ePA eingesetzten SMC-Bs.

A_13659 - Primärsystem - Interoperable Dokumentenformate

Das Primärsystem MUSS interoperable Dokumente, die eingestellt werden sollen, durch eine geeignete Kombination von Metadaten eindeutig erkennbar machen.[<=]

Hinweis: Die Liste gültiger Inhalts- und Dateitypen enthält initial (Notfalldaten, XML), (eMP/AMTS, XML), (eArztbrief, HL7 CDA XML).

A_16292 - Primärsystem - Interoperables Dateiformat eArztbrief

Das Primärsystem MUSS eine XML-Container-Datei erzeugen. Die Datei muss die XML- und PDF-Anteile gemäß der jeweils gültigen Fassung der Richtlinie zu § 291f SGB V enthalten.[<=]

Hinweis: Die Fachanwendungen eMP/AMTS und NFDM definieren das jeweilige Format in der vorhandenen Fachanwendungsspezifikation. Für den eArztbrief wird das Format entsprechend der jeweils gültigen Fassung der Richtlinie zu § 291f SGB V festgelegt. In der elektronischen Patientenakte wird je Arztbrief nur eine Datei abgelegt.

4.2 Schnittstellen der Fachanwendung ePA

Der folgende Abschnitt beschreibt die interoperablen Schnittstellen der Fachanwendung ePA, die zwischen Primärsystem und Konnektor mit Fachmodul ePA, zwischen Fachmodul ePA und ePA-Aktensystem sowie zwischen ePA-Aktensystem und des ePA-Frontends in der Umgebung des Versicherten genutzt werden.

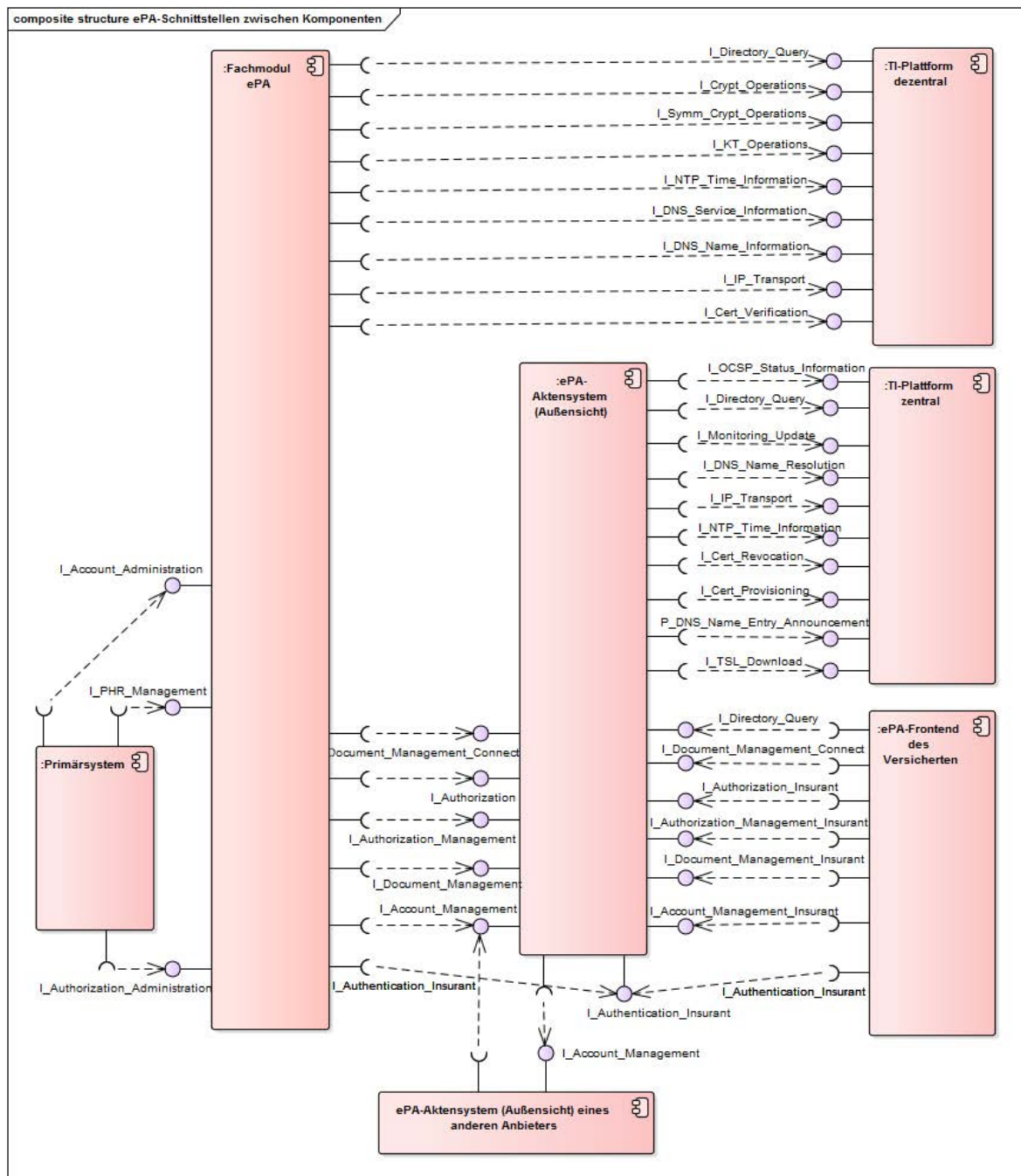


Abbildung 37: Übersicht über die Schnittstellen der Fachanwendung ePA

4.2.1 Schnittstelle zwischen Primärsystem und Fachmodul ePA

Die interoperable Nutzung des Fachmoduls ePA in unterschiedlichen Konnektoren mit verschiedenen Primärsystemen in der Umgebung der Leistungserbringer wird durch die gemeinsame Umsetzung der

Schnittstellen `I_PHR_Management`, `I_Authorization_Administration` und `I_Account_Administration` realisiert.

EPA-EPF-A_0088 - Interoperabilität zwischen Primärsystem und Fachmodul ePA

Das Fachmodul ePA MUSS die Interoperabilität zwischen Primärsystem und dem Fachmodul ePA über die Schnittstellen

`I_PHR_Management`, `I_Authorization_Administration` und `I_Account_Administration` sicherstellen.

[<=]

4.2.1.1 Schnittstelle `I_PHR_Management`

Die Schnittstelle `I_PHR_Management` stellt Operationen zur Verwaltung von Dokumenten eines Versicherten in einem ePA-Aktensystem über das Fachmodul ePA zur Verfügung.

EPA-EPF-A_0089 - Logische Operation `I_PHR_Management::find`

Die Schnittstelle `I_PHR_Management` MUSS die logische Operation `find` implementieren.

Tabelle 33: Logische Operation `find`

Kategorie	Name	Typ
Schnittstelle	<code>I_PHR_Management</code>	-
Operation	<code>find</code>	-
Param-In	<code>RecordIdentifier</code>	<code>RecordIdentifier</code>
Param-In	<code>Query</code>	<code>Query</code>
Param-Out	<code>ResultSet</code>	<code>ResultSet</code>

Diese Operation leitet die übergebenen Suchparameter (`Query`) an ein ePA-Aktensystem weiter, in dem serverseitig nach Dokumenten in dem in `RecordIdentifier` benannten ePA-Aktenkonto gesucht wird. Das Ergebnis der Suche auf dem Server wird als `ResultSet` als Liste der Metadaten der Dokumente passend zur Suchabfrage zurückgegeben. Es muss möglich sein, dass in allen Metadaten der Dokumente und auch der Dokumenten-ID nach freiem Text gesucht werden kann.

[<=]

EPA-EPF-A_0090 - Logische Operation `I_PHR_Management::getDocuments`

Die Schnittstelle `I_PHR_Management` MUSS die logische Operation `getDocuments` implementieren.

Tabelle 34: Logische Operation `getDocuments`

Kategorie	Name	Typ
Schnittstelle	<code>I_PHR_Management</code>	-
Operation	<code>getDocuments</code>	-
Param-In	<code>RecordIdentifier</code>	<code>RecordIdentifier</code>

Param-In	DocumentIdentifiers	DocumentIdentifier[1..*]
Param-Out	Documents	Document[0..*]

Mit dieser Operation werden die über die `DocumentIdentifiers` referenzierten Dokumente aus einem Repository des in `RecordIdentifier` benannten Aktenkontos des ePA-Aktensystems heruntergeladen. Die Identifier wurden zuvor über eine Metadaten-suche aus einer Registry an das Primärsystem übertragen geladen. Vor der Rückgabe der Dokumente als `Documents` entschlüsselt das Fachmodul alle Dokumente mit dem jeweiligen durch den Aktenschlüssel entschlüsselten Dokumentenschlüssel.

[<=]

EPA-EPF-A_0091 - Logische Operation `I_PHR_Management::putDocuments`

Die Schnittstelle `I_PHR_Management` MUSS die logische Operation `putDocuments` implementieren.

Tabelle 35: Logische Operation `putDocuments`

Kategorie	Name	Typ
Schnittstelle	<code>I_PHR_Management</code>	-
Operation	<code>putDocuments</code>	-
Param-In	<code>RecordIdentifier</code>	<code>RecordIdentifier</code>
Param-In	<code>DocumentSet</code>	<code>Document[1..*]</code>

Mit dieser Operation werden Dokumente (`DocumentSet`) über das Fachmodul in das im `RecordIdentifier` benannten Aktenkonto in das ePA-Aktensystem hochgeladen. Jedes Dokument wird vom Fachmodul vor dem Hochladen mit einem zufälligen Dokumentenschlüssel verschlüsselt, welcher wiederum mit dem Aktenschlüssel verschlüsselt wird. Zum einen werden die im `DocumentSet` enthaltenen Dokumente gespeichert, zum anderen werden die zu den Dokumenten zusätzlich mitgelieferten Metadaten registriert. Vor dem Verschlüsseln und Hochladen werden folgende Prüfungen vorgenommen:

- die Dokumentengröße,
- Korrektheit und Vollständigkeit der Metadaten,
- der Dokumententyp basierend auf den in den Metadaten übergebenen ePA- bzw. ePF-Kennzeichen.

[<=]

EPA-EPF-A_0092 - Logische Operation `I_PHR_Management::updateMetadata`

Die Schnittstelle `I_PHR_Management` MUSS die logische Operation `updateMetadata` implementieren.

Tabelle 36: Logische Operation `updateMetadata`

Kategorie	Name	Typ
Schnittstelle	<code>I_PHR_Management</code>	-
Operation	<code>updateMetadata</code>	-
Param-In	<code>RecordIdentifier</code>	<code>RecordIdentifier</code>
Param-In	<code>NewMetadata</code>	<code>DocumentEntry[1..*]</code>

Mit dieser Operation werden Metadaten von einem oder mehreren Dokumenten des in `RecordIdentifier` benannten Aktenkontos aktualisiert (`NewMetadata`). Die aktuellen Metadaten, in denen eine Änderung durchgeführt wird, wurden über eine zuvor durchge-

führte Metadaten-suche (find) an das Primärsystem übertragen.

[<=]

EPA-EPF-A_0093 - Logische Operation I_PHR_Management::deleteDocuments

Die Schnittstelle I_PHR_Management MUSS die logische Operation deleteDocuments implementieren.

Tabelle 37: Logische Operation deleteDocuments

Kategorie	Name	Typ
Schnittstelle	I_PHR_Management	-
Operation	deleteDocuments	-
Param-In	RecordIdentifier	RecordIdentifier
Param-In	DocumentIdentifiers	DocumentIdentifier[1..*]

Mit dieser Operation werden die über die DocumentIdentifiers referenzierten Dokumente aus dem im RecordIdentifier benannten Aktenkonto inklusive ihrer Metadaten aus einem Document Repository und einer Document Registry gelöscht.

[<=]

4.2.1.2 Schnittstelle I_Authorization_Administration

Die Schnittstelle I_Authorization_Administration stellt Operationen zum Einholen und Aktualisieren von Berechtigungen in Akten von Versicherten bei verschiedenen Anbietern bereit.

EPA-EPF-A_0094 - Logische Operation

I_Authorization_Administration::requestFacilityAuthorization

Die Schnittstelle I_Authorization_Administration MUSS die logische Operation requestFacilityAuthorization implementieren.

Tabelle 38: Logische Operation requestFacilityAuthorization

Kategorie	Name	Typ
Schnittstelle	I_Authorization_Administration	-
Operation	requestFacilityAuthorization	-
Param-In	RecordIdentifier	RecordIdentifier
Param-In	AuthorizationConfiguration	String
Param-In	userName	String
Param-In	registerSMB	String

Die Operation startet den Autorisierungsprozess zur Berechtigungsvergabe für die Leistungserbringerinstitution in dem über den RecordIdentifier referenzierten Aktenkonto des Versicherten. Das Fachmodul stellt die Auswahl des Primärsystems als AuthorizationConfiguration am Kartenterminal dar und lässt sie vom Versicherten mittels PIN-Eingabe bestätigen.

Für die im Aufruf referenzierte SMC-B (registerSMB) und alle weiteren im Verzeichnisdienst hinterlegten ENC-Zertifikate zu zusätzlichen SMC-Bs der entsprechenden Telematik-ID wird das mittels eGK heruntergeladene und entschlüsselte Schlüsselmaterial ver-

schlüsselt und im Autorisierungssystem hinterlegt. Das in der Dokumentenverwaltung hinterlegte Policy Document wird vom Fachmodul heruntergeladen, um eine Zugriffsregel entsprechend der `AuthorizationConfiguration` erweitert und zurückgespielt. Der Name der Leistungserbringerinstitution wird in dem Parameter `userName` gemäß einer hinterlegten Konfiguration im Fachmodul übergeben.

[<=]

EPA-EPF-A_0096 - Logische Operation

I_Authorization_Administration::registerSMB

Die Schnittstelle `I_Authorization_Administration` MUSS die logische Operation `registerSMB` implementieren.

Tabelle 39: Logische Operation registerSMB

Kategorie	Name	Typ
Schnittstelle	<code>I_Authorization_Administration</code>	-
Operation	<code>registerSMB</code>	-
Param-In	<code>knownRecords</code>	<code>RecordIdentifier[0..*]</code>

Die Operation aktualisiert die Berechtigungen der Leistungserbringerinstitution für ePA. Das Fachmodul iteriert dabei über alle dem Primärsystem bekannten `RecordIdentifiers` der Akten von Versicherten (`knownRecords`) und ersetzt das in jedem Aktenkonto hinterlegte Schlüsselmaterial mit dem für alle aktuellen SMC-B-Einträge des Verzeichnisses im Fachmodul neu verschlüsselte Schlüsselmaterial.

[<=]

4.2.1.3 Schnittstelle I_Account_Administration

Die Schnittstelle `I_Account_Administration` stellt Operationen zur Verwendung im Rahmen der Kontoeröffnung eines Versicherten bereit.

EPA-EPF-A_0095 - Logische Operation PHRManagementService::getHomeCommunityID

Die Schnittstelle `PHRManagementService` MUSS die logische Operation `getHomeCommunityID` implementieren.

Tabelle 40: Logische Operation getHomeCommunityID

Kategorie	Name	Typ
Schnittstelle	<code>PHRManagementService</code>	-
Operation	<code>getHomeCommunityID</code>	-
Param-In	<code>KVNR</code>	<code>PatientIdentifier</code>
Param-Out	<code>HomeCommunityID</code>	<code>OID</code>

Mit dieser Operation erhält das Primärsystem die Anbieterkennung HomeCommunityID für eine gegebene KVNR eines Versicherten. Das Fachmodul iteriert dafür über alle bekannten Anbieter ePA-Aktensystems und ruft die Operation `I_Authorization_Management::checkRecordExists` des ePA-Aktensystems auf. Existiert für einen über die KVNR bekannten Versicherten ein aktives Aktenkonto, kennt das Fachmodul dessen HomCommunityID aus der Netzwerkennung des ePA-Aktensystems. Diese gibt das Fachmodul an das Primärsystem zurück, welches mit dieser OID den RecordIdentifier bilden kann. Ein Login des Fachmoduls ist für diese Abfrage nicht erforderlich.

[<=]

A_13665 - Logische Operation PHRManagementService::activateAccount

Die Schnittstelle PHRManagementService MUSS die logische Operation `activateAccount` implementieren.

Tabelle 41 : Logische Operation activateAccount

Kategorie	Name	Typ
Schnittstelle	PHRManagementService	-
Operation	activateAccount	-
Param-In	RecordIdentifier	RecordIdentifier

Mit dieser Operation startet das Primärsystem die Aktivierung des beantragten Aktenkontos des Versicherten bei seinem Anbieter. Mit dem `RecordIdentifier` wird das Aktenkonto lokalisiert. Diese ermittelt der Leistungserbringer per Abfrage über die KVNR des Versicherten bei den ePA-Aktensystemen verschiedener Anbieter. Das Fachmodul prüft die Echtheit und Gültigkeit der eGK, authentifiziert den Versicherten über die Abfrage seiner PIN.CH. Gegenüber dem ePA-Aktensystem meldet sich das Fachmodul ePA mit der AUT-Identität des Versicherten an. Der symmetrische Akten-schlüssel und der symmetrische Kontextschlüssel werden lokal im Konnektor erzeugt. Diese werden hybrid für die ENC-Identität der eGK des Versicherten verschlüsselt und in der Komponente Autorisierung hinterlegt.

[<=]

4.2.2 Schnittstelle zwischen Fachmodul ePA und ePA-Aktensystem

Das Fachmodul ePA ist dafür verantwortlich, IHE-Anfragen von Primärsystemen an die Schnittstellen des ePA-Aktensystems umzusetzen. Da Fachmodul ePA und ePA-Aktensystem potentiell von unterschiedlichen Anbietern stammen, aber dennoch interoperabel sein müssen, müssen beide die vier Schnittstellen

`I_Document_Management`, `I_Document_Management_Connect`, `I_Account_Management` und `I_Authorization` unterstützen.

Im Rahmen der Aktenkonto-Aktivierung in Leistungserbringerinstitutionen und der Vergabe von Ad-hoc-Berechtigungen an Leistungserbringerinstitutionen wird beim Stecken der eGK des Versicherten vom Fachmodul auch die Schnittstelle `I_Authentication_Insurant` für die Authentisierung des Versicherten benutzt. Die Beschreibung dieser Schnittstelle befindet sich in Kapitel 4.2.3.

EPA-EPF-A_0097 - Interoperabilität zwischen Fachmodul und ePA-Aktensystem

Das ePA-Aktensystem MUSS die Interoperabilität zwischen Fachmodul ePA und ePA-Aktensystem über die Schnittstellen `I_Document_Management`, `I_Document_Management_Connect`, `I_Account_Management`, `I_Authentication_Insurant` und `I_Authorization` sicherstellen.

[<=]

Die Separierung der interoperablen Schnittstelle in verschiedene Interfaces folgt aus der funktionalen Zerlegung der Fachanwendung. Die Interoperabilität wird sichergestellt, indem eine Komponente alle fünf `I_*`-Schnittstellen nutzt bzw. implementiert.

4.2.2.1 Schnittstelle `I_Authorization`

Die Schnittstelle dient dem Fachmodul dazu, eine Autorisierung in Form eines Tokens für einen bereits authentifizierten Leistungserbringer zu erhalten, um damit dann das ePA-Aktensystem verwenden zu können. Zudem werden einige zusätzliche Operationen zur Berechtigungsverwaltung unterstützt.

EPA-EPF-A_0099 - Logische Operation `I_Authorization::getAuthorizationKey`

Die Schnittstelle `I_Authorization` MUSS die logische Operation `getAuthorizationKey` implementieren.

Tabelle 42: Logische Operation `getAuthorizationKey`

Kategorie	Name	Typ
Schnittstelle	<code>I_Authorization</code>	-
Operation	<code>getAuthorizationKey</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>RecordIdentifier</code>	<code>RecordIdentifier</code>
Param-In	<code>PublicTargetKey (opt.)</code>	<code>CertificateX.509</code>
Param-Out	<code>AuthorizationKey</code>	<code>AuthorizationKey</code>
Param-Out	<code>AuthorizationAssertion</code>	<code>AuthorizationToken</code>

Mit der Operation `getAuthorizationKey` wird das für einen Berechtigten verschlüsselte Schlüsselmaterial (kryptografische Berechtigung) für ein konkretes Aktenkonto (`RecordIdentifier`) eines Versicherten heruntergeladen. Zur Prüfung auf Vorhandensein und der Berechtigung zum Download des hinterlegten Schlüsselmaterials (`AuthorizationKey`) muss eine gültige `AuthenticationAssertion` übergeben werden. Im Ergebnis wird, je nach am Schlüsselmaterial gespeicherten `AuthorizationType`, neben dem Schlüsselmaterial eine Autorisierungsbestätigung (`AuthorizationAssertion`) ausgegeben, die die zur Berechtigungsprüfung relevanten Informationen `UserID` (Telematik-ID) und `RecordIdentifier` zur Prüfung in der Komponente Dokumentenverwaltung des ePA-Aktensystems enthält.[<=]

4.2.2.2 Schnittstelle `I_Authorization_Management`

Die Schnittstelle dient dazu, kryptografische Berechtigungen im Autorisierungsdienst eines ePA-Aktensystems zu verwalten.

EPA-EPF-A_0100 - Logische Operation**I_Authorization_Management::putAuthorizationKey**

Die Schnittstelle I_Authorization_Management MUSS die logische Operation putAuthorizationKey implementieren.

Tabelle 43: Logische Operation putAuthorizationKey

Kategorie	Name	Typ
Schnittstelle	I_Authorization_Management	-
Operation	putAuthorizationKey	-
Param-In	AuthenticationAssertion	AuthenticationToken
Param-In	RecordIdentifier	RecordIdentifier
Param-In	AuthorizationKey	AuthorizationKey

Mit der Operation putAuthorizationKey wird das für einen Berechtigten (hier: die Leistungserbringerinstitution) verschlüsselte Schlüsselmateriale (AuthorizationKey) für ein konkretes Aktenkonto (RecordIdentifier) eines Versicherten im ePA-Aktensystem gespeichert. Das Speichern darf nur von einem dazu berechtigten und mittels gültiger AuthenticationAssertion ausgewiesenen Nutzer (dem Versicherten im Rahmen der Ad-hoc-Berechtigung in der Umgebung der Leistungserbringer) erfolgen. Im Fall des Aktivieren des Aktenkontos wird das im Fachmodul des Konnektors erzeugte und verschlüsselte Schlüsselmateriale (AuthorizationKey) für den Versicherten hinterlegt.

[<=]

EPA-EPF-A_0101 - Logische Operation**I_Authorization_Management::replaceAuthorizationKey**

Die Schnittstelle I_Authorization_Management MUSS die logische Operation replaceAuthorizationKey implementieren.

Tabelle 44: Logische Operation replaceAuthorizationKey

Kategorie	Name	Typ
Schnittstelle	I_Authorization_Management	-
Operation	replaceAuthorizationKey	-
Param-In	AuthenticationAssertion	AuthenticationToken
Param-In	RecordIdentifier	RecordIdentifier
Param-In	NewAuthorizationKey	AuthorizationKey

Mit dieser Operation kann eine ausgewiesene (AuthenticationAssertion) Leistungserbringerorganisation das für ihre eigenen aktuellen SMC-Bs verschlüsselte Schlüsselmateriale (NewAuthorizationKey) ersetzen. Das Einsetzen eines NewAuthoriza-

tionKey ist nur zulässig, wenn bereits ein AuthorizationKey im Aktenkonto des Versicherten hinterlegt ist, welcher mit dem Ersetzen überschrieben wird. RecordIdentifier identifiziert das Aktenkonto eines Versicherten, in dem das Schlüsselmaterial für die berechnete Leistungserbringerinstitution ersetzt werden soll.

[<=]

A_15679 - Logische Operation I_Authorization_Management::checkRecordExists

Die Schnittstelle I_Authorization_Management MUSS die logische Operation checkRecordExists implementieren.

Tabelle 45 Logische Operation checkRecordExists

Kategorie	Name	Typ
Schnittstelle	I_Authorization_Management	-
Operation	checkRecordExists	-
Param-In	KVNR	PatientIdentifier
Param-Out	RecordState	Boolean String

Mit dieser Operation kann das Fachmodul ePA oder ein ePA-Aktensystem A eines Anbieters A bei einem anderen ePA-Aktensystem B die Existenz eines Aktenkontos auf Basis der KVNR eines Versicherten abfragen. Ist dem Anbieter B die angefragte KVNR bekannt und wird zu dieser KVNR ein Aktenkonto geführt, so liefert der Rückgabeparameter RecordState den Status zurück.

Ein ePA-Aktensystem MUSS anderen ePA-Aktensystemen diese Information bereits während des Beantragungsvorgangs im Rahmen der Kontoeröffnung durch einen Versicherten zur Verfügung stellen.[<=]

4.2.2.3 Schnittstelle I_Document_Management_Connect

Die Schnittstelle I_Document_Management_Connect ermöglicht den Aufbau eines sicheren Kommunikationskanals auf Anwendungsebene zwischen Clients und dem Verarbeitungskontext des Aktenkontos eines Versicherten sowie die Aktivierung und das Schließen des Verarbeitungskontextes.

EPA-EPF-A_0102 - Logische Operation

I_Document_Management_Connect::connectToContext

Die Schnittstelle Document_Management_Connect MUSS die logische Operation connectToContext implementieren.

Tabelle 46: Logische Operation ConnectToContext

Kategorie	Name	Typ
Schnittstelle	I_Document_Management_Connect	-
Operation	connectToContext	-
Param-In	AuthorizationAssertion	AuthorizationToken

Diese logische Operation stellt eine sichere Verbindung zwischen Client und dem bedarfsgesteuert instanziierten Aktenkontext eines Versicherten im ePA-Aktensystem her. Mittels `AuthorizationAssertion` zeigt ein Nutzer an, dass er autorisiert ist, diesen Kontext aufzubauen. Das ePA-Aktensystem prüft anhand der in der `AuthorizationAssertion` enthaltenen Informationen des Nutzers (`UserID` und `RecordIdentifier`) die Zulässigkeit des Verbindungsaufbaus.

[<=]

EPA-EPF-A_0103 - Logische Operation

I_Document_Management_Connect::openContext

Die Schnittstelle `I_Document_Management_Connect` MUSS die logische Operation `openContext` implementieren.

Tabelle 47: Logische Operation openContext

Kategorie	Name	Typ
Schnittstelle	<code>I_Document_Management_Connect</code>	-
Operation	<code>openContext</code>	-
Param-In	<code>ContextInformation</code>	<code>ContextInformation</code>

Diese Operation initialisiert den Aktenkontext eines Versicherten im ePA-Aktensystem. Im Übergabeparameter `ContextInformation` ist der Kontextschlüssel des Aktenkontos des Versicherten enthalten, mit dem die Ausführungsumgebung den Kontext des Aktenkontos eines Versicherten (Metadaten, Policy-Dokumente, Protokoll etc.) entschlüsseln und initialisieren kann.[<=]

EPA-EPF-A_0104 - Logische Operation

I_Document_Management_Connect::closeContext

Die Schnittstelle `I_Document_Management_Connect` MUSS die logische Operation `closeContext` implementieren.

Tabelle 48: Logische Operation closeContext

Kategorie	Name	Typ
Schnittstelle	<code>I_Document_Management_Connect</code>	-
Operation	<code>closeContext</code>	-

Diese Operation entfernt die Sessiondaten des Nutzers und schließt den Aktenkontext eines Versicherten im ePA-Aktensystem, wenn für keinen Nutzer eine aktive Session vermerkt ist. Die im Klartext im Arbeitsspeicher vorliegenden Daten des Versicherten werden vor dem Schließen des Aktenkontextes mit dem beim Starten des Kontextes übergebenen Schlüsselmaterial (`ContextInformation`) verschlüsselt persistiert. Alle Session- und in der Session entschlüsselten Daten werden gelöscht.

[<=]

4.2.2.4 Schnittstelle I_Account_Management

Die Schnittstelle `I_Account_Management` stellt anderen Anbietern die logische Operation zum Download eines Exportpakets zu Verfügung.

A_13652 - Logische Operation I_Account_Management::getExportPackage

Die Schnittstelle `I_Account_Management` MUSS die logische Operation `getExportPackage` implementieren.

Tabelle 49 Logische Operation getExportPackage

Kategorie	Name	Typ
Schnittstelle	<code>I_Account_Management</code>	-
Operation	<code>getExportPackage</code>	-
Param-In	<code>URI</code>	<code>String</code>
Param-Out	<code>ExportPackage</code>	<code>ExportPackageType</code>

Mit dieser Operation lädt ein Anbieter eines ePA-Aktensystems ein ExportPaket (`ExportPackage`) aus dem ePA-Aktensystem des Anbieters eines ePA-Aktensystems, bei dem der Versicherte bisher sein Konto geführt hatte, herüber. Das ExportPaket wurde vom Versicherten zuvor durch Signalisierung eines Aktenumzugs erstellt und das Aktenkonto beim bisherigen Anbieter in den Zustand "bereit für Anbieterwechsel" versetzt. Die Abrufadresse (`URI`) zur Lokalisierung des ExportPakets für die Datenmigration zum neuen Anbieter transportiert der Versicherte vom Altsystem zum Neusystem, z.B. durch Copy-Paste oder Weiterverwendung des bisherigen Frontends.

[<=]

4.2.2.5 Schnittstelle I_Document_Management

Die Schnittstelle `I_Document_Management` stellt dem Fachmodul ePA Operationen zur Dokumentenverwaltung der Inhalte eines Aktenkontos eines Versicherten in der Komponente Dokumentenverwaltung eines ePA-Aktensystems eines Aktenanbieters bereit.

EPA-EPF-A_0107 - Logische Operation I_Document_Management::find

Die Schnittstelle `I_Document_Management` MUSS die logische Operation `find` implementieren.

Tabelle 50: Logische Operation find

Kategorie	Name	Typ
Schnittstelle	<code>I_Document_Management</code>	-
Operation	<code>find</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>Query</code>	<code>Query</code>
Param-Out	<code>ResultSet</code>	<code>ResultSet</code>

Diese Operation lässt ein ePA-Aktensystem serverseitig in den Metadaten der gespeicherten Dokument gemäß dem übergebenen Suchparameter (`Query`) suchen. Mittels `AuthenticationAssertion` zeigt ein Nutzer an, dass er autorisiert ist, auf Daten des Versicherten zuzugreifen. Das ePA-Aktensystem prüft anhand der in der `AuthenticationAssertion` enthaltenen Informationen des Nutzers (`UserID=Telematik-ID` und `RecordIdentifier`) konkrete Zugriffsregeln auf Objekte, die von der Suche betroffen sind. Das Ergebnis der Suche auf dem Server wird als `ResultSet` als Liste der Metadaten der Dokumente passend zur Suchabfrage, reduziert auf die für den Nutzer gemäß

Zugriffsregeln zulässigen Einträge, zurückgegeben.
 [≤]

EPA-EPF-A_0108 - Logische Operation I_Document_Management::putDocuments

Die Schnittstelle `I_Document_Management` MUSS die logische Operation `putDocuments` implementieren.

Tabelle 51: Logische Operation putDocuments

Kategorie	Name	Typ
Schnittstelle	<code>I_Document_Management</code>	-
Operation	<code>putDocuments</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>DocumentSet</code>	<code>Document[1..*]</code>

Mit dieser Operation werden Dokumente in das ePA-Aktensystem hochgeladen. Zum einen werden die im `DocumentSet` enthaltenen Dokumente gespeichert, zum anderen werden die zu den Dokumenten zusätzlich mitgelieferten Metadaten registriert. Mittels `AuthenticationAssertion` zeigt ein Nutzer an, dass er autorisiert ist, auf Daten des Versicherten zu operieren. Das ePA-Aktensystem prüft anhand der in der `AuthenticationAssertion` enthaltenen Informationen des Nutzers (`UserID=Telematik-ID` und `RecordIdentifier`) die Zulässigkeit der Operation und konkrete Zugriffsregeln auf Objekte, die vom Speichern betroffen sind.

Medizinische Dokumente (`MedicalDocument` im `DocumentSet`) werden vom Nutzer Ende-zu-Ende-verschlüsselt übertragen. Diese werden vom ePA-Aktensystem direkt persistiert.

Technische Dokumente (`TechnicalDocument` im `DocumentSet`) werden transportverschlüsselt übertragen, müssen vom ePA-Aktensystem jedoch vor dem Speichern verarbeitet werden. Das Policy Document als konkretes `TechnicalDocument` MUSS vom System nach dem Hochladen eingelesen und geprüft werden. Ein valides, passend formatiertes, widerspruchsfreies Policy Document wird vom ePA-Aktensystem akzeptiert und bildet die aktualisierte Definition der Zugriffsregeln für den Zugriff auf die Daten des Versicherten.

Vor dem Verschlüsseln und Hochladen werden die Metadaten auf Korrektheit und Vollständigkeit geprüft.

[≤]

EPA-EPF-A_0109 - Logische Operation I_Document_Management::getDocuments

Die Schnittstelle `I_Document_Management` MUSS die logische Operation `getDocuments` implementieren.

Tabelle 52: Logische Operation getDocuments

Kategorie	Name	Typ
Schnittstelle	<code>I_Document_Management</code>	-
Operation	<code>getDocuments</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>DocumentIdentifiers</code>	<code>DocumentIdentifier[1..*]</code>
Param-Out	<code>DocumentSet</code>	<code>Document[0..*]</code>

Mit dieser Operation werden die über die `DocumentIdentifiers` referenzierten Dokumente als `DocumentSet`, reduziert auf die für den Nutzer gemäß Zugriffsregeln zulässig-

gen Einträge; aus einem Repository heruntergeladen. Diese Identifier wurden zuvor über eine Metadatenuche aus einer Registry an das Fachmodul übertragen. Mittels `AuthenticationAssertion` zeigt ein Nutzer an, dass er autorisiert ist, auf Daten des Versicherten zu operieren. Das ePA-Aktensystem prüft anhand der in der `AuthenticationAssertion` enthaltenen Informationen des Nutzers (`UserID=Telematik-ID` und `RecordIdentifier`) die Zulässigkeit der Operation und konkrete Zugriffsregeln auf Objekte, die vom Dokumentenabruf betroffen sind.

[<=]

EPA-EPF-A_0110 - Logische Operation `I_Document_Management::updateMetadata`

Die Schnittstelle `I_Document_Management` MUSS die logische Operation `updateMetadata` implementieren.

Tabelle 53: Logische Operation `updateMetadata`

Kategorie	Name	Typ
Schnittstelle	<code>I_Document_Management</code>	-
Operation	<code>updateMetadata</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>NewMetadata</code>	<code>DocumentEntry[1..*]</code>

Mit dieser Operation werden Metadaten von einem oder mehreren Dokumenten aktualisiert (`NewMetadata`). Die aktuellen Metadaten, in denen eine Änderung durchgeführt wird, wurden über eine zuvor durchgeführte Metadatenuche (`find`) an das Fachmodul übertrage. Mittels `AuthenticationAssertion` zeigt ein Nutzer an, dass er autorisiert ist, auf Daten des Versicherten zu operieren. Das ePA-Aktensystem prüft anhand der in der `AuthenticationAssertion` enthaltenen Informationen des Nutzers (`UserID=Telematik-ID` und `RecordIdentifier`) die Zulässigkeit der Operation und konkrete Zugriffsregeln auf Objekte, die vom Speichern betroffen sind.

[<=]

EPA-EPF-A_0111 - Logische Operation `I_Document_Management::deleteDocuments`

Die Schnittstelle `I_Document_Management` MUSS die logische Operation `deleteDocuments` implementieren.

Tabelle 54: Logische Operation `deleteDocuments`

Kategorie	Name	Typ
Schnittstelle	<code>I_Document_Management</code>	-
Operation	<code>deleteDocuments</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>DocumentIdentifiers</code>	<code>DocumentIdentifier[1..*]</code>

Mit dieser Operation werden die über die `DocumentIdentifiers` referenzierten Dokumente inklusive der Metadaten aus Repository und Registry gelöscht. Mittels `AuthenticationAssertion` zeigt ein Nutzer an, dass er autorisiert ist, auf Daten des Versicherten zu operieren. Das ePA-Aktensystem prüft anhand der in der `AuthenticationAssertion` enthaltenen Informationen des Nutzers (`UserID=Telematik-ID` und `RecordIdentifier`) die Zulässigkeit der Operation und konkrete Zugriffsregeln auf Objekte, die vom Löschen betroffen sind.

[<=]

4.2.3 Schnittstelle zwischen ePA-Aktensystem und ePA-Frontend des Versicherten

Die interoperable Nutzung unterschiedlicher ePA-Anwendungen auf Geräten des Versicherten in der Umgebung des Versicherten zur Anbindung der ePA-Backend-Komponenten wird durch die gemeinsame Umsetzung der Schnittstellen

`I_Authentication_Insurant`, `I_Authorization_Insurant`,
`I_Account_Management_Insurant` und `I_Document_Management_Insurant` realisiert.

EPA-EPF-A_0113 - Interoperabilität zwischen ePA-Aktensystem und ePA-Frontend des Versicherten

Das ePA-Aktensystem MUSS die Interoperabilität zwischen ePA-Aktensystem und der dezentralen Fachlogik im ePA-Frontend des Versicherten über die Schnittstellen

`I_Authentication_Insurant`, `I_Authorization_Insurant`,
`I_Account_Management_Insurant`, `I_Document_Management_Connect` und
`I_Document_Management_Insurant` sicherstellen.

[<=]

Die Separierung der Interoperablen Schnittstelle in die genannten Interfaces folgt aus der funktionalen Zerlegung der Fachanwendung. Die Interoperabilität wird sichergestellt, indem eine Komponente alle vier `I_*`-Schnittstellen nutzt bzw. implementiert.

4.2.3.1 Schnittstelle `I_Authentication_Insurant`

Die Schnittstelle `I_Authentication_Insurant` stellt Operationen zur Authentisierung von Versicherten im ePA-Aktensystem bereit. Die Schnittstelle ist aus der Umgebung des Versicherten erreichbar, damit diese sich im ePA-Aktensystem anmelden können. Die Schnittstelle wird außerdem vom Fachmodul aus der Umgebung der Leistungserbringer aufgerufen, im Anwendungsfall der Ad-hoc-Berechtigung, in der ein Versicherter durch das Fachmodul gesteuert für einen Leistungserbringer eine Berechtigung im ePA-Aktensystem hinterlegt.

EPA-EPF-A_0114 - Logische Operation `I_Authentication_Insurant::login`

Die Schnittstelle `I_Authentication_Insurant` MUSS die logische Operation `login` implementieren.

Tabelle 55: Logische Operation `login`

Kategorie	Name	Typ
Schnittstelle	<code>I_Authentication_Insurant</code>	-
Operation	<code>login</code>	-
Param-In	2-Factor-Authentication	Credential
Param-Out	AuthenticationAssertion	AuthenticationToken

Das ePA-Frontend des Versicherten ruft diese Operation auf. Der Versicherte authentisiert sich gegenüber der Komponente „Zugangsgateway“ des ePA-Aktensystems ePA mit dem Authentisierungsmerkmal `2-Factor-Authentication` (eGK + PIN). Das Zugangsgateway prüft die Echtheit und Gültigkeit inkl. Sperrstatus des Zertifikates der eingesetzten eGK.

Bei erfolgreicher Authentifizierung mittels echter und gültiger eGK erhält das ePA-Frontend des Versicherten eine Authentifizierungsbestätigung (`AuthenticationAssertion`), die die Prüfung der Identität bestätigt und erforderliche Identitätsmerkmale des Versicherten enthält (CH.AUT-Zertifikat).

[<=]

A_14224 - Logische Operation I_Authentication_Insurant::getAuditEvents

Die Schnittstelle I_Authentication_Insurant MUSS die logische Operation getAuditEvents implementieren.

Tabelle 56: Logische Operation getAuditEvents

Kategorie	Name	Typ
Schnittstelle	I_Authentication_Insurant	-
Operation	getAuditEvents	-
Param-In	AuthenticationAssertion	AuthenticationToken
Param-In	RecordIdentifier	RecordIdentifier
Param-Out	ResultSet	LogEntry[0..*]

Mit dieser Operation kann ein authentifizierter Versicherter bzw. ein berechtigter Vertreter (AuthenticationAssertion) das Verwaltungsprotokoll der Authentisierungskomponente auslesen. Es werden nur Protokolleinträge zurückgegeben, die eindeutig diesem Nutzer zu einem Aktenkonto (RecordIdentifier) zugeordnet werden können. [≤=]

4.2.3.2 Schnittstelle I_Authorization_Insurant

Die Schnittstelle I_Authorization_Insurant stellt Operationen zur Autorisierungsprüfung auf das Vorhandensein von kryptografischem Schlüsselmaterial für einen Nutzer des Aktenkontos eines Versicherten bereit.

EPA-EPF-A_0115 - Logische Operation**I_Authorization_Insurant::getAuthorizationKey**

Die Schnittstelle I_Authorization_Insurant MUSS die logische Operation getAuthorizationKey implementieren.

Tabelle 57: Logische Operation getAuthorizationKey

Kategorie	Name	Typ
Schnittstelle	I_Authorization_Insurant Consumer	-
Operation	getAuthorizationKey	-
Param-In	AuthenticationAssertion	AuthenticationToken
Param-In	RecordIdentifier	RecordIdentifier
Param-In	ActorID	String
Param-In	DeviceID	String
Param-Out	AuthorizationKey	AuthorizationKey
Param-Out	AuthorizationAssertion	AuthorizationToken

Mit der Operation getAuthorizationKey wird das für einen Berechtigten (ActorID) verschlüsselte Schlüsselmaterial (kryptografische Berechtigung) für ein konkretes Akten-

konto (`RecordIdentifier`) eines Versicherten heruntergeladen. Bei Aufruf der Operation muss eine Prüfung mittels der Geräteerkennung (`DeviceID`) stattfinden. Zur Prüfung auf Vorhandensein und der Berechtigung zum Download des hinterlegten Schlüsselmaterials (`AuthorizationKey`) muss eine gültige `AuthenticationAssertion` übergeben werden. Im Ergebnis wird, je nach am Schlüsselmaterial hinterlegtem `AuthorizationType`, neben dem Schlüsselmaterial eine Autorisierungsbestätigung (`AuthorizationAssertion`) ausgegeben, die die zur Berechtigungsprüfung relevanten Informationen `UserID=KVN` und `RecordIdentifier` zur Prüfung in der Komponente Dokumentenverwaltung des ePA-Aktensystems enthält.

[<=]

4.2.3.3 Schnittstelle `I_Authorization_Management_Insurant`

Die Schnittstelle `I_Authorization_Management_Insurant` stellt Operationen zur Verwaltung von kryptografischen Berechtigungen im Autorisierungsdienst eines ePA-Aktensystems bereit.

EPA-EPF-A_0118 - Logische Operation

`I_Authorization_Management_Insurant::putAuthorizationKey`

Die Schnittstelle `I_Authorization_Management_Insurant` MUSS die logische Operation `putAuthorizationKey` implementieren.

Tabelle 58: Logische Operation `putAuthorizationKey`

Kategorie	Name	Typ
Schnittstelle	<code>I_Authorization_Management_Insurant</code>	-
Operation	<code>putAuthorizationKey</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>RecordIdentifier</code>	<code>RecordIdentifier</code>
Param-In	<code>AuthorizationKey</code>	<code>AuthorizationKey</code>
Param-In	<code>DeviceID</code>	<code>String</code>
Param-In	<code>NotificationInfoRepresentative</code> (opt.)	<code>String</code>

Mit der Operation `putAuthorizationKey` wird das für einen Berechtigten verschlüsselte Schlüsselmaterial (kryptografische Berechtigung) `AuthorizationKey` für ein konkretes Aktenkonto (`RecordIdentifier`) eines Versicherten im ePA-Aktensystem gespeichert. Bei Aufruf der Operation muss eine Prüfung mittels der Geräteerkennung (`DeviceID`) stattfinden. Mit der Angabe des Berechtigungstyps `AuthorizationType` im Schlüsseldatensatz `AuthorizationKey` steuert der Versicherte die Verwendung des Schlüsselmaterials. Das Schlüsselmaterial kann einerseits über die Ausstellung eines Autorisierungstokens beim `getAuthorizationKey` für den Abruf von Dokumenten über die IHE-Schnittstelle verwendet werden. Andererseits möchte ein Versicherter evtl. nur die Verwendung zum Umschlüsseln gestatten und daher die Ausstellung einer Autorisierungsbestätigung für einen Berechtigten verweigern. Der zur Schlüssel hinterlegung be-

rechtigte Nutzer authentisiert sich mittels `AuthenticationAssertion`. Optional kann ein Vertreter seine der Versicherte für die Einrichtung einer Vertretung für die Gerätefreischaltung eine E-Mail-Adresse als Benachrichtigungskanal (`NotificationInfoRepresentative`) hinterlegen.

[<=]

EPA-EPF-A_0119 - Logische Operation

`I_Authorization_Management_Insurant::deleteAuthorizationKey`

Die Schnittstelle `I_Authorization_Management_Insurant` MUSS die logische Operation `deleteAuthorizationKey` implementieren.

Tabelle 59: Logische Operation `deleteAuthorizationKey`

Kategorie	Name	Typ
Schnittstelle	<code>I_Authorization_Management_Insurant</code>	-
Operation	<code>deleteAuthorizationKey</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>RecordIdentifier</code>	<code>RecordIdentifier</code>
Param-In	<code>ActorID</code>	<code>String</code>
Param-In	<code>DeviceID</code>	<code>String</code>

Mit dieser Operation kann ein authentifizierter Versicherter bzw. ein berechtigter Vertreter (`AuthenticationAssertion`) die kryptografische Berechtigung (`AuthorizationKey`) für einen via `ActorID` identifizierten Nutzer (unveränderlicher Teil der KVNR oder Telematik-ID) innerhalb seines Aktenkontos löschen. Bei Aufruf der Operation muss eine Prüfung mittels der Geräteerkennung (`DeviceID`) stattfinden. `RecordIdentifier` identifiziert das Aktenkonto eines Versicherten, in dem das Schlüsselmaterial gelöscht werden soll. Das Löschen des für die eGK des Versicherten als Eigentümer des Aktenkontos verschlüsselten Schlüsselmaterials ist nicht zulässig.

[<=]

EPA-EPF-A_0121 - Logische Operation

`I_Authorization_Management_Insurant::replaceAuthorizationKey`

Die Schnittstelle `I_Authorization_Management_Insurant` MUSS die logische Operation `replaceAuthorizationKey` implementieren.

Tabelle 60: Logische Operation `replaceAuthorizationKey`

Kategorie	Name	Typ
Schnittstelle	<code>I_Authorization_Management_Insurant</code>	-
Operation	<code>replaceAuthorizationKey</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>RecordIdentifier</code>	<code>RecordIdentifier</code>
Param-In	<code>NewAuthorizationKey</code>	<code>AuthorizationKey</code>
Param-In	<code>DeviceID</code>	<code>String</code>

Mit dieser Operation kann ein authentifizierter Versicherter bzw. ein berechtigter Vertreter (`AuthenticationAssertion`) das für eine alte eGK verschlüsselte Schlüsselmaterial durch neues für eine Folgekarte verschlüsseltes Schlüsselmaterial (`NewAuthorizationKey`) ersetzen. Bei Aufruf der Operation muss eine Prüfung mittels der Geräteken-

nung (DeviceID) stattfinden. RecordIdentifier identifiziert das Aktenkonto eines Versicherten, in der das Schlüsselmaterial ersetzt werden soll. Das Prüfkriterium zur Sicherstellung, dass das Schlüsselmaterial zum gleichen Versicherten gehört ist der unveränderliche Teil der KVN des Versicherten entsprechend der AuthenticationAssertion. Das Schlüsselmaterial NewAuthorizationKey muss für eine neuere als die aktuell verwendete und eine nicht schon einmal verwendete eGK verschlüsselt sein.

[<=]

A_14225 - Logische Operation

I_Authorization_Management_Insurant::getAuditEvents

Die Schnittstelle I_Authorization_Management_Insurant MUSS die logische Operation getAuditEvents implementieren.

Tabelle 61 Logische Operation getAuditEvents

Kategorie	Name	Typ
Schnittstelle	I_Authentication_Insurant	-
Operation	getAuditEvents	-
Param-In	AuthenticationAssertion	AuthorizationToken
Param-In	RecordIdentifier	RecordIdentifier
Param-In	DeviceID	String
Param-Out	ResultSet	LogEntry[0..*]

Mit dieser Operation kann ein authentisierter Versicherter bzw. ein berechtigter Vertreter (AuthenticationAssertion) das Verwaltungsprotokoll der Autorisierungskomponente auslesen. Bei Aufruf der Operation muss eine Prüfung der Geräteerkennung (DeviceID) stattfinden. Es werden nur Protokolleinträge zurückgegeben, die eindeutig diesem Nutzer zu einem Aktenkonto (RecordIdentifier) zugeordnet werden können.

[<=]

A_14226 - Logische Operation

I_Authorization_Management_Insurant::putNotificationInfo

Die Schnittstelle I_Authorization_Management_Insurant MUSS die logische Operation putNotificationInfo implementieren.

Tabelle 62: Logische Operation putNotificationInfo

Kategorie	Name	Typ
Schnittstelle	I_Authorization_Management_Insurant	-
Operation	putNotificationInfo	-
Param-In	AuthenticationAssertion	AuthenticationToken
Param-In	RecordIdentifier	RecordIdentifier
Param-In	DeviceID	String
Param-In	NotificationInfo	String

Mit dieser Operation kann ein autorisierter Versicherter bzw. ein berechtigter Vertreter (`AuthorizationAssertion`) die im Benachrichtigungskanal hinterlegten Daten für sich selbst aktualisieren. Bei Aufruf der Operation muss eine Prüfung mittels der Gerätekennung (`DeviceID`) stattfinden. Das ePA-Aktensystem prüft anhand der `AuthenticationAssertion` und dem `RecordIdentifier` die Zulässigkeit der Operation. [`<=`]

4.2.3.4 Schnittstelle `I_Document_Management_Connect`

Das ePA-Frontend des Versicherten nutzt die in Kapitel 4.2.2.3 beschriebene Schnittstelle, die auch das Fachmodul ePA nutzt.

4.2.3.5 Schnittstelle `I_Account_Management_Insurant`

Die Schnittstelle `I_Account_Management_Insurant` stellt administrative Operationen zur Verwaltung des Aktenkontos eines Versicherten bereit.

EPA-EPF-A_0132 - Logische Operation

`I_Account_Management_Insurant::suspendAccount`

Die Schnittstelle `I_Account_Management_Insurant` MUSS die logische Operation `suspendAccount` implementieren.

Tabelle 63: Logische Operation `suspendAccount`

Kategorie	Name	Typ
Schnittstelle	<code>I_Account_Management_Insurant</code>	-
Operation	<code>suspendAccount</code>	-
Param-In	<code>AuthorizationAssertion</code>	<code>AuthorizationToken</code>
Param-Out	<code>URI</code>	<code>string</code>

Mit dieser Operation kann ein Aktenkonto eines Versicherten in den Exportzustand versetzen. Das ePA-Aktensystem erstellt dafür ein `ExportPackage` mit folgendem Inhalt:

- alle entschlüsselten Daten (Metadaten, Zugriffsprotokoll) und Dokumente (`PolicyDocumente`), die mit `I_Account_Management_Insurant::openContext` geladen werden,
- alle Dokumente (`MedicalDocument`, `TechnicalDocument`) die über die Operationen `I_Document_Management_Insurant::putDocuments` und `I_Document_Management::putDocuments` in das ePA-Aktensystem übertragen wurden.

Das `ExportPackage` wird mit dem Kontextschlüssel symmetrisch verschlüsselt. Als Rückgabeparameter erhält der Aufrufer mittels `URI` einen Link auf das `ExportPackage`, über das ein berechtigter Anbieter eines ePA-Aktensystems das Paket herunterladen kann.

[`<=`]

EPA-EPF-A_0133 - Logische Operation**I_Account_Management_Insurant::resumeAccount**

Die Schnittstelle `I_Account_Management_Insurant` MUSS die logische Operation `resumeAccount` implementieren.

Tabelle 64: Logische Operation resumeAccount

Kategorie	Name	Typ
Schnittstelle	<code>I_Account_Management_Insurant</code>	-
Operation	<code>resumeAccount</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>URI</code>	<code>string</code>

Mit dieser Operation erfolgt der Import der Daten eines Aktenkontos eines Versicherten, welche im ePA-Aktensystem eines anderen Anbieters exportiert wurden.

Die Inhalte des mittels `ContextKey` entschlüsselten `ExportPakets` werden in die Komponente "Dokumentenverwaltung" importiert (Dokumente, Metadaten, Zugriffsprotokoll). Anschließend wird das `ExportPaket` gelöscht.[<=]

EPA-EPF-A_0139 - Logische Operation**I_Account_Management_Insurant::getAuditEvents**

Die Schnittstelle `I_Account_Management_Insurant` MUSS die logische Operation `getAuditEvents` implementieren.

Tabelle 65: Logische Operation getAuditEvents

Kategorie	Name	Typ
Schnittstelle	<code>I_Account_Management_Insurant</code>	-
Operation	<code>getAuditEvents</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-Out	<code>ResultSet</code>	<code>LogEntry[0..*]</code>

Mit dieser Operation kann der gemäß gültiger `AuthenticationAssertion` autorisierte Versicherte bzw. ein berechtigter Vertreter das Zugriffsprotokoll eines Aktenkontos auslesen. Es werden nur Protokolleinträge zurückgegeben, die eindeutig diesem Nutzer, d. h. dem konkreten Versicherten, dem dieses Aktenkonto (`RecordIdentifier` in `AuthenticationAssertion`) gehört, zugeordnet werden können.

[<=]

4.2.3.6 Schnittstelle I_Document_Management_Insurant

Die Schnittstelle `I_Document_Management_Insurant` stellt dem ePA-Frontend des Versicherten Operationen zur Dokumentenverwaltung der Inhalte des Aktenkontos des Versicherten in der Komponente Dokumentenverwaltung eines ePA-Aktensystems eines Aktenanbieters bereit.

EPA-EPF-A_0134 - Logische Operation I_Document_Management_Insurant::find
 Die Schnittstelle I_Document_Management_Insurant MUSS die logische Operation find implementieren.

Tabelle 66: Logische Operation find

Kategorie	Name	Typ
Schnittstelle	I_Document_Management_Insurant	-
Operation	find	-
Param-In	AuthenticationAssertion	AuthenticationToken
Param-In	Query	Query
Param-Out	ResultSet	ResultSet

Diese Operation lässt ein ePA-Aktensystem serverseitig in den Metadaten der gespeicherten Dokument gemäß dem übergebenen Suchparameter (Query) suchen. Mittels AuthenticationAssertion zeigt ein Nutzer an, dass er autorisiert ist, auf Daten des Versicherten zuzugreifen. Das ePA-Aktensystem prüft anhand der in der AuthenticationAssertion enthaltenen Informationen des Nutzers (UserID=KVNR und RecordIdentifier) konkrete Zugriffsregeln auf Objekte, die von der Suche betroffen sind. Das Ergebnis der Suche auf dem Server wird als ResultSet als Liste der Metadaten der Dokumente passend zur Suchabfrage, reduziert auf die für den Nutzer gemäß Zugriffsregeln zulässigen Einträge, zurückgegeben.

Es muss möglich sein, dass in allen Metadaten der Dokumente und auch der Dokumenten-ID nach freiem Text gesucht werden kann.

[<=]

EPA-EPF-A_0135 - Logische Operation I_Document_Management_Insurant::putDocuments

Die Schnittstelle I_Document_Management_Insurant MUSS die logische Operation putDocuments implementieren.

Tabelle 67: Logische Operation putDocuments

Kategorie	Name	Typ
Schnittstelle	I_Document_Management_Insurant	-
Operation	putDocuments	-
Param-In	AuthenticationAssertion	AuthenticationToken
Param-In	DocumentSet	Document[1..*]

Mit dieser Operation werden Dokumente in das ePA-Aktensystem hochgeladen. Zum einen werden die im DocumentSet enthaltenen Dokumente gespeichert, zum anderen werden die zu den Dokumenten zusätzlich mitgelieferten Metadaten registriert. Mittels AuthenticationAssertion zeigt ein Nutzer an, dass er autorisiert ist, auf Daten des Versicherten zu operieren. Das ePA-Aktensystem prüft anhand der in der AuthenticationAssertion enthaltenen Informationen des Nutzers (UserID=KVNR und RecordIdentifier) die Zulässigkeit der Operation und konkrete Zugriffsregeln auf Objekte, die vom Speichern betroffen sind.

Medizinische Dokumente (MedicalDocument im DocumentSet) werden vom Nutzer Ende-zu-Ende-verschlüsselt übertragen. Diese werden vom ePA-Aktensystem direkt persistiert.

Technische Dokumente (TechnicalDocument im DocumentSet) werden transportver-

schlüsselt übertragen, müssen vom ePA-Aktensystem jedoch vor dem Speichern verarbeitet werden. Das Policy Document als konkretes `TechnicalDocument` enthält die Zugriffsregeln aller Berechtigten im Aktenkonto des Versicherten in der Komponente „Dokumentenverwaltung“ und MUSS vom System nach dem Hochladen eingelesen und geprüft werden. Ein valides, passend formatiertes, widerspruchsfreies Policy Document wird vom ePA-Aktensystem akzeptiert und bildet die aktualisierte Definition der Zugriffsregeln für den Zugriff auf die Daten des Versicherten.

Vor dem Verschlüsseln und Hochladen werden folgende Prüfungen vorgenommen:

- die Dokumentengröße,
- Korrektheit und Vollständigkeit der Metadaten,
- der Dokumententyp basierend auf den in den Metadaten übergebenen ePF-Kennzeichen. [\leq]

EPA-EPF-A_0136 - Logische Operation

I_Document_Management_Insurant::getDocuments

Die Schnittstelle `I_Document_Management_Insurant` MUSS die logische Operation `getDocuments` implementieren.

Tabelle 68: Logische Operation getDocuments

Kategorie	Name	Typ
Schnittstelle	<code>I_Document_Management_Insurant</code>	-
Operation	<code>getDocuments</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>DocumentIdentifiers</code>	<code>DocumentIdentifier[1..*]</code>
Param-Out	<code>DocumentSet</code>	<code>Document[0..*]</code>

Mit dieser Operation werden die über die `DocumentIdentifiers` referenzierten Dokumente als `DocumentSet`, reduziert auf die für den Nutzer gemäß Zugriffsregeln zulässigen Einträge, aus einem Repository heruntergeladen. Diese Identifier wurden zuvor über eine Metadatensuche aus einer Registry an das ePA-Frontend übertragen. Mittels `AuthenticationAssertion` zeigt ein Nutzer an, dass er autorisiert ist, auf Daten des Versicherten zu operieren. Das ePA-Aktensystem prüft anhand der in der `AuthenticationAssertion` enthaltenen Informationen des Nutzers (`UserID=KVNR` und `RecordIdentifier`) die Zulässigkeit der Operation und konkrete Zugriffsregeln auf Objekte, die vom Dokumentenabruf betroffen sind.[\leq]

EPA-EPF-A_0138 - Logische Operation

I_Document_Management_Insurant::deleteDocuments

Die Schnittstelle `I_Document_Management_Insurant` MUSS die logische Operation `deleteDocuments` implementieren.

Tabelle 69: Logische Operation deleteDocuments

Kategorie	Name	Typ
Schnittstelle	<code>I_Document_Management_Insurant</code>	-
Operation	<code>deleteDocuments</code>	-
Param-In	<code>AuthenticationAssertion</code>	<code>AuthenticationToken</code>
Param-In	<code>DocumentIdentifiers</code>	<code>DocumentIdentifier[1..*]</code>

Mit dieser Operation werden die über die `DocumentIdentifiers` referenzierten Dokumente inklusive der Metadaten aus Repository und Registry gelöscht. Mittels `AuthenticationAssertion` zeigt ein Nutzer an, dass er autorisiert ist, auf Daten des Versicherten zu operieren. Das ePA-Aktensystem prüft anhand der in der `AuthenticationAssertion` enthaltenen Informationen des Nutzers (`UserID=KVNR` und `RecordIdentifier`) die Zulässigkeit der Operation und konkrete Zugriffsregeln auf Objekte, die vom Löschen betroffen sind.

[<=]

4.2.4 Weitere Schnittstellen

Die Fachanwendung ePA nutzt Leistungen der TI-Plattform nach, um ihre Anwendungsfälle zu realisieren.

EPA-EPF-A_0141 - Nutzung von Schnittstellen der TI-Plattform durch das Fachmodul

Das Fachmodul ePA MUSS für die Erbringung seiner Leistungen folgende Schnittstellen der TI-Plattform nutzen:

- `I_Cert_Verification`
- `I_IP_Transport`
- `I_Crypt_Operations`
- `I_Symm_Crypt_Operations`
- `I_DNS_Name_Information`
- `I_DNS_Service_Information`
- `I_NTP_Time_Information`
- `I_KT_Operations`
- `I_Directory_Query`
- `I_Sign_Operations`

[<=]

EPA-EPF-A_0142 - Nutzung von Schnittstellen der TI-Plattform durch das ePA-Aktensystem

Das ePA-Aktensystem MUSS für die Erbringung seiner Leistungen folgende Schnittstellen der TI-Plattform nutzen:

- `I_Directory_Query`
- `I_DNS_Name_Resolution`
- `P_DNS_Name_Entry_Announcement`
- `I_TSL_Download`
- `I_OCSP_Status_Information`
- `I_Cert_Provisioning`
- `I_Cert_Revocation`
- `I_NTP_Time_Information`
- `I_IP_Transport`
- `I_Monitoring_Update`

[<=]

Das ePA-Frontend des Versicherten greift nicht direkt auf Leistungen der TI-Plattform zu.

Für die Umsetzung des Anwendungsfalls „3.5.5 Anbieter wechseln“ wird beim alten Anbieter aus dem Aktenkonto ein ExportPackage erstellt, welches dann vom neuen Anbieter heruntergeladen – `I_Account_Management::getExportPackage()` – und dann importiert werden kann.

EPA-EPF-A_0143 - ExportPackage zum Herunterladen bereitstellen

Das ePA-Aktensystem MUSS es einem anderen ePA-Aktensystem ermöglichen, ein ExportPackage, welches durch die Operation

`I_Account_Management_Insurant::suspendAccount` erstellt wurde, für die Ausführung der Operation `I_Account_Management::getExportPackage()` über eine TLS-Verbindung herunterzuladen.

[<=]

EPA-EPF-A_0343 - Abfrage Aktenexistenz zwischen ePA-Aktensystemen

Das ePA-Aktensystem MUSS es einem anderen ePA-Aktensystem ermöglichen, mit der Operation `I_Authorization_Management::checkRecordExists` die Existenz eines Aktenkontos zu einer KVNR eines Versicherten abzufragen.

[<=]

5 Datenschutz- und Sicherheitsaspekte sowie vertrauenswürdige Umgebung

Für die Akzeptanz der Fachanwendung ePA durch die Nutzer ist die Gewährleistung des Datenschutzes und damit verbunden der Sicherheit der personenbezogenen medizinischen Daten ein unabdingbares Merkmal. Die Fachanwendung ePA erreicht dies durch das Aufstellen von Anforderungen an den Datenschutz und die Informationssicherheit, das Prüfen der Einhaltung dieser Anforderungen in der Zulassung und die Überprüfung der Einhaltung der Anforderungen im laufenden Betrieb durch den Anbieter ePA-Aktensystem selbst, aber auch durch Audits der gematik.

Die aufgestellten Anforderungen des Datenschutzes und der Informationssicherheit entsprechen dem Gebot der Angemessenheit dadurch, dass sie einerseits den Schutzbedarf der zu verarbeitenden Daten und andererseits die Umsetzungsfähigkeit durch die Anbieter ePA-Aktensystem berücksichtigen. Die Angemessenheit der Anforderungen hinsichtlich des Schutzbedarfs wird durch die Nutzung der Methoden zur Informationssicherheit und des Datenschutzes der TI unter Beachtung der Risiko-Policy der TI erreicht. Die Angemessenheit hinsichtlich der Umsetzbarkeit wird in den spezifizierten Technologien berücksichtigt.

Für die Aufrechterhaltung des Datenschutz- und Informationssicherheitsniveaus der TI ist es erforderlich, dass die TI durch die Nutzung der Fachanwendung ePA/ePF nicht negativ beeinflusst wird. Eine Beeinträchtigung kann insbesondere über den Anschluss des ePA-Aktensystems erfolgen. Um dies zu verhindern, werden dem Anbieter ePA-Aktensystem entsprechend dem Modularisierungskonzept in [gemSpec_DS_Anbieter] Module der Informationssicherheit und des Datenschutzes zugeordnet. Über diese Module bzw. die zugehörigen Anforderungen wird der Anbieter auch verpflichtet, Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzurichten.

Hinzu kommen spezifische Anforderungen an das ePA-Aktensystem zur Umsetzung der unten genannten ePA spezifischen Aspekte.

In Bezug auf das ePA-Fachmodul muss der Hersteller des ePA-Fachmoduls die übergreifenden Sicherheitsanforderungen an Hersteller erfüllen. Das ePA-Fachmodul wird im Konnektor ausgeführt und kann daher von einer sicheren Ausführungsumgebung ausgehen. Es kann davon ausgegangen werden, dass die von außen von den Primärsystemen der Leistungserbringer nutzbaren Schnittstellen des Fachmoduls in der vorgesehenen Weise genutzt werden. Ferner muss das Fachmodul ePA/ePF nachweisen, dass es das Datenschutz- und Informationssicherheitsniveau des Konnektors nicht negativ beeinflusst.

Die Erfüllung der Anforderungen an das ePA-Frontend des Versicherten sind von einem Anbieter im Sinne des Herstellers des ePA-Frontends in Rahmen der Zulassung nachzuweisen. In Bezug auf das ePA-Frontend muss der Hersteller die übergreifenden Sicherheitsanforderungen an Hersteller erfüllen. Das ePA-Frontend des Versicherten kann über die Sicherheit der Client-Systeme der Versicherten auf denen es läuft, keine Aussagen treffen. Deshalb müssen dem Nutzer die vom Anbieter des ePA-Frontends getroffenen Annahmen an die Einsatzumgebung des ePA-Frontends in Form von Empfehlungen zu Sicherheitsmaßnahmen mitgeteilt werden.

Durch den Zulassungsprozess der gematik wird sichergestellt, dass die Einhaltung der Anforderungen vor einem produktiven Einsatz der Fachanwendung ePA nachgewiesen werden muss.

Nur Personen, die in § 291a Abs. 4 SGB V genannt sind, dürfen auf medizinische personenbezogene Daten von ePA zugreifen können. Es muss daher technisch ausgeschlossen werden, dass ein Anbieter (oder ein von ihm beauftragter Betreiber) Zugriff auf im Klartext vorliegende personenbezogene medizinische Daten erhält. Diese Anforderung ist vom Anbieter (oder von seinem Betreiber) durch technische Maßnahmen umzusetzen, deren Wirksamkeit nicht von organisatorischen Maßnahmen des Anbieters (Betreibers) abhängen darf.

Für die Dokumente in der Komponente Dokumentenverwaltung wird dies durch eine Verschlüsselung erreicht, die für den Versicherten und für durch ihn autorisierte Leistungserbringer bzw. Vertreter erfolgt. Für die Metadaten, die im ePA-Aktensystem verarbeitet werden sollen, wird dies durch eine vertrauenswürdige Ausführungsumgebung (VAU) umgesetzt.

Folgende produkttypübergreifende Anforderungen müssen erfüllt werden:

EPA-EPF-A_0144 - Schutz der Kommunikation

Alle Produkttypen der Fachanwendung ePA und alle Komponente des ePA-Aktensystems MÜSSEN vertraulich miteinander kommunizieren.

[<=]

EPA-EPF-A_0145 - Informationstechnische Trennung

Alle Produkttypen der Fachanwendung ePA, die nicht miteinander kommunizieren, MÜSSEN informationstechnisch voneinander getrennt sein.

[<=]

EPA-EPF-A_0146 - Schutzmaßnahmen gegen die OWASP Top 10 Risiken

Alle Produkttypen der Fachanwendung ePA MÜSSEN Maßnahmen zum Schutz vor der aktuellsten Version der OWASP-Top-10-Risiken umsetzen.

[<=]

5.1 Spezielle Anforderungen an das Fachmodul ePA

EPA-EPF-A_0147 - Keine Speicherung von privaten Schlüsseln im Fachmodul

Das Fachmodul ePA DARF symmetrische und private asymmetrische Schlüssel (z.B. Dokumentenschlüssel, Aktenschlüssel) NICHT persistent speichern.

[<=]

EPA-EPF-A_0148 - Keine Speicherung von personenbezogenen Daten im Fachmodul

Das Fachmodul ePA DARF personenbezogenen Daten NICHT persistent speichern.

[<=]

EPA-EPF-A_0149 - Keine Weitergabe vertraulicher Informationsobjekte an das PS

Das Fachmodul ePA DARF vertrauliches Schlüsselmaterial und Daten der Sessionverwaltung im Konnektor NICHT an das PS weitergeben.

[<=]

5.2 Anforderungen an das ePA-Frontend des Versicherten

EPA-EPF-A_0150 - Information zur Einsatzumgebung

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass der Nutzer über die Annahmen und Anforderungen an die Einsatzumgebung des ePA-Frontends informiert wird. [≤]

EPA-EPF-A_0152 - Anzeige von Protokolldaten

Das ePA-Frontend des Versicherten MUSS es den Versicherten ermöglichen, alle in der Fachanwendung für ihn erzeugten Verwaltungsprotokoll- und 291a-Protokolleinträge anzeigen zu können. Hierzu holt das ePA-Frontend die Protokolle aus allen Komponenten des ePA-Aktensystems ab und fasst technische Einzelschritte, die zu einem Anwendungsfall gehören, für den Versicherten verständlich zusammen.

[≤]

Hinweis: Die beiden Protokolltypen werden im Abschnitt 5.3 bei den einzelnen Komponenten des ePA-Aktensystems eingeführt. Das Verwaltungsprotokoll enthält Einträge für den Versicherten, die nicht im § 291a-Protokoll aufgenommen werden (z.B. Logins, Berechtigungsvergabe).

EPA-EPF-A_0153 - Schutz der sensiblen Daten im ePA-Frontend des Versicherten

Das ePA-Frontend des Versicherten MUSS die im ePA-Frontend des Versicherten verarbeiteten Daten mit Best-Practices-Sicherheitsmaßnahmen schützen. [≤]

Hinweis: Die Best-Practice-Sicherheitsmaßnahmen sind abhängig von der Technologie, mit der das ePA-Frontend vom Hersteller umgesetzt wird. Ein Beispiel von Best-Practices-Sicherheitsmaßnahmen für SAML sind die OWASP Cheat Sheet Series: https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series. Mehrere von diesen Cheat Sheets könnten für ePA relevant werden, z.B. das SAML Security Cheat Sheet oder das Input Validation Cheat Sheet.

EPA-EPF-A_0154 - Keine Speicherung von symmetrischen und privaten asymmetrischen Schlüsseln im ePA-Frontend des Versicherten

Das ePA-Frontend des Versicherten DARF symmetrische und private asymmetrische Schlüssel NICHT im Klartext persistent speichern.

[≤]

A_17076 - Verhindern von Session Hijacking im ePA-Frontend des Versicherten

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass eine ePA-Session nicht von anderen Anwendungen auf dem Gerät übernommen werden kann.

[≤]

A_14230 - Identität von autorisierten Geräten

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass jedes autorisierte Gerät eine eindeutige Kennung hat.

[≤]

5.3 Anforderungen an das ePA-Aktensystem

EPA-EPF-A_0157 - Zusammenführung von Vertragsdaten und Aktendaten verhindern

Das ePA-Aktensystem MUSS verhindern, dass eine missbräuchliche Profilbildung von Vertragsdaten und Daten der Fachanwendung ePA möglich ist.

[≤]

EPA-EPF-A_0158 - Verbot der Auswertung von Beziehungen zwischen LE, LEI und Versicherten

Das ePA-Aktensystem MUSS verhindern, dass eine Auswertung von Beziehungen zwischen LE, LEI und Versicherten möglich ist.

[<=]

EPA-EPF-A_0159 - Verbot der Profilbildung

Das ePA-Aktensystem MUSS verhindern, dass eine missbräuchliche Profilbildung möglich ist.

[<=]

EPA-EPF-A_0161 - Privacy by Default im ePA-Aktensystem

Das ePA-Aktensystem MUSS sicherstellen, dass bei Konfigurationsmöglichkeiten die datenschutzfreundlichere Option vorausgewählt ist.

[<=]

EPA-EPF-A_0163 - Serverseitige Authentisierung erforderlich

Das ePA-Aktensystem MUSS sich gegenüber dem ePA-Frontend des Versicherten und dem Fachmodul authentisieren.

[<=]

Hinweis: Die Authentisierung kann auf Transport- oder Anwendungsebene umgesetzt werden.

EPA-EPF-A_0164 - Zugriff eines Versicherten über registrierte Geräte

Das ePA-Aktensystem MUSS sicherstellen, dass einen Zugriff eines Versicherten auf das ePA-Aktensystem nur von einem vom Versicherten registrierten Gerät möglich ist.

[<=]

Hinweis: Zugriffe auf das ePA-Aktensystem von Konnektoren werden grundsätzlich erlaubt, da diese Geräte ein „vertrauenswürdiger“ Bestandteil der TI sind.

EPA-EPF-A_0165 - Autorisiertes Gerät ist im Besitz des Versicherten

Das ePA-Aktensystem MUSS während der Gerätregistrierung einen zusätzlichen Authentifizierungsschritt über einen separaten Benachrichtigungskanal durchführen.

[<=]

Hinweis: Als separater Benachrichtigungskanal kann eine E-Mail dienen.

EPA-EPF-A_0167 - Sperrung von autorisierten Geräten

Das ePA-Aktensystem MUSS umsetzen, dass einen Zugriff auf das ePA-Aktensystem für ein autorisiertes Gerät gesperrt werden kann.

[<=]

EPA-EPF-A_0168 - Verhindern von Session Hijacking

Das ePA-Aktensystem MUSS sicherstellen, dass eine ePA-Session nicht von anderen Anwendungen auf dem Gerät übernommen werden kann.

[<=]

EPA-EPF-A_0169 - Zusätzliche Autorisierung von sensiblen Anwendungsfällen

Das ePA-Aktensystem MUSS sicherstellen, dass für folgende Anwendungsfälle eine nochmalige Authentifizierung erfolgt, wenn die Authentifizierung zulange zurück liegt.

- Vertretung einrichten
- Vertragsdaten ändern
- Aktenkonto schließen.

[<=]

EPA-EPF-A_0170 - Informationstechnische Trennung der Komponenten des ePA-Aktensystems

Das ePA-Aktensystem muss sicherstellen, dass alle Komponenten des ePA-Aktensystems informationstechnisch voneinander getrennt sind.

[<=]

EPA-EPF-A_0171 - Schutzmaßnahmen gegen Angriffe aus der Umgebung des Versicherten

Das ePA-Aktensystem MUSS sicherstellen, dass Angriffe aus der Umgebung des Versicherten abgewehrt werden.

[<=]

EPA-EPF-A_0172 - Angriffen entgegenwirken

Das ePA-Aktensystem MUSS Maßnahmen zur Erkennung und zur Schadensreduzierung und -verhinderung von Angriffen umsetzen.

[<=]

EPA-EPF-A_0173 - Standardaktennutzung

Das ePA-Aktensystem MUSS eine Standardaktennutzung definieren.[<=]

Hinweis: Standardaktennutzung dient zur Abgrenzung von Angriffen und bedeutet die Definition eines Nutzungsprofils für einen Standardnutzer des ePA-Aktensystems z.B. über

- das erwartete Laufzeitverhalten von Anwendungsfällen und Transaktionen
- die Anzahl ausgeführter Anwendungsfälle pro Stunde
- die Anzahl parallel genutzter Geräte
- Geofencing von IP-Adressen auf Client-Geräten

Die Standard-Aktennutzung wird in der Spezifikation erörtert.

EPA-EPF-A_0174 - Abweichung von Standardaktennutzung

Das ePA-Aktensystem MUSS bei einer erkannten Abweichung von der Standardnutzung darauf reagieren.[<=]

Hinweis: Wie das ePA-Aktensystem reagieren soll, wird in der Spezifikation dargelegt.

EPA-EPF-A_0175 - Integritätsschutz für Bestätigungen

Das ePA-Aktensystem MUSS sicherstellen, dass die Authentifizierungsbestätigung und Autorisierungsbestätigung integritätsgeschützt sind und eine begrenzte Gültigkeitsdauer haben.

[<=]

EPA-EPF-A_0176 - Akzeptanz nur von eigenen Autorisierungsbestätigungen

Das ePA-Aktensystem MUSS sicherstellen, dass nur die vom ePA-Aktensystem selbst ausgestellten Autorisierungsbestätigungen akzeptiert werden.

[<=]

EPA-EPF-A_0178 - Nutzung von Bestätigungen nur auf genau einem Gerät

Das ePA-Aktensystem MUSS sicherstellen, dass die Authentifizierungs- und Autorisierungsbestätigung nur auf jeweils genau einem Gerät nutzbar sind.[<=]

A_14239 - Einsatz zertifizierter HSM

Das ePA-Aktensystem MUSS beim Einsatz eines HSM sicherstellen, dass deren Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria, ITSEC oder Federal Information Processing Standard (FIPS) in Frage.

Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3,
2. Common Criteria EAL 4+ mit hohem Angriffspotenzial oder
3. ITSEC E3 der Stärke „hoch“ entsprechen

[<=]

A_14240 - Sicherer Betrieb und Nutzung eines HSMs

Das ePA-Aktensystem MUSS sicherstellen, dass die im HSM verarbeiteten privaten Schlüssel nicht unautorisiert ausgelesen, unautorisiert verändert, unautorisiert ersetzt oder in anderer Weise unautorisiert benutzt werden können.

[<=]

5.3.1 Anforderungen an die Komponente Zugangsgateway

EPA-EPF-A_0179 - Kein direkter Zugriff auf Dienste der zentralen TI-Plattform

Die Komponente Zugangsgateway des ePA-Aktensystems DARF einen direkten Zugriff auf Dienste der zentralen TI-Plattform NICHT aus der Personal Zone erlauben.

[<=]

EPA-EPF-A_0180 - Verwaltungsprotokollierung im Zugangsgateway

Die Komponente Zugangsgateway des ePA-Aktensystems MUSS für den folgenden Anwendungsfall Einträge in einem Verwaltungsprotokoll für den Versicherten bzw. seine Vertreter vornehmen:

- Login.

[<=]

A_13810 - Verwaltungsprotokollierung im Zugangsgateway Löschen von Protokolleinträgen

Die Komponente Zugangsgateway MUSS sicherstellen, dass Protokolleinträge am Ende des auf ihre Generierung folgenden Kalenderjahres gelöscht werden. Ausnahme: Die 50 jüngsten Protokolleinträge DÜRFEN auch dann NICHT gelöscht werden, wenn die o. g. Frist erreicht bzw. überschritten ist.[<=]

5.3.2 Anforderungen an die Komponente Autorisierung

EPA-EPF-A_0182 - Verwaltungsprotokollierung in der Komponente Autorisierung

Die Komponente Autorisierung des ePA-Aktensystems MUSS für die folgenden Anwendungsfälle Einträge in einem Verwaltungsprotokoll für den Versicherten bzw. seine Vertreter vornehmen.

- Berechtigung vergeben
- Vertretung einrichten
- Neue eGK über Vertreter bekannt machen
- Neue eGK über alte eGK bekannt machen
- Bestehende Berechtigungen verwalten
- Vertretung für einen Versicherten wahrnehmen
- Aktenkonto schließen
- Geräte verwalten

[<=]

A_13812 - Verwaltungsprotokollierung in der Komponente Autorisierung Löschen von Protokolleinträgen

Die Komponente Autorisierung MUSS sicherstellen, dass Protokolleinträge am Ende des auf ihre Generierung folgenden Kalenderjahres gelöscht werden. Ausnahme: Die 50 jüngsten Protokolleinträge DÜRFEN auch dann NICHT gelöscht werden, wenn die o. g. Frist erreicht bzw. überschritten ist.[<=]

5.3.3 Anforderungen an die Komponente Dokumentenverwaltung

EPA-EPF-A_0183 - Umsetzung der Dokumentenverwaltung in einer VAU

Die Komponente Dokumentenverwaltung DARF die Nutzdaten eines Aktenkontos NICHT außerhalb einer VAU verarbeiten.

[<=]

EPA-EPF-A_0184 - Verschlüsselung der Nutzdaten eines Aktenkontos außerhalb der VAU

Die Komponente Dokumentenverwaltung MUSS sicherstellen, dass alle Nutzdaten eines Aktenkontos außerhalb der VAU nur in verschlüsselter Form vorliegen.

[<=]

EPA-EPF-A_0185 - Kommunikationsendpunkt zu der Komponente Dokumentenverwaltung

Die Komponente „Dokumentenverwaltung“ des ePA-Aktensystems MUSS den verschlüsselten Benachrichtigungskanal zum Frontend des Versicherten bzw. zum Fachmodul im Aktenkontext des Versicherten innerhalb der VAU terminieren.

[<=]

EPA-EPF-A_0186 - Verifikation des Versichertenkontextes

Das ePA-Frontend des Versicherten MUSS die Authentizität des Aktenkontextes innerhalb der VAU verifizieren, bevor die Übergabe von personenbezogenen, medizinischen Daten und kryptografischem Schlüsselmaterial stattfindet.

[<=]

EPA-EPF-A_0187 - Keine Beeinflussung der Sicherheit zwischen Akten

Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS sicherstellen, dass die Beeinträchtigung der Sicherheit eines Aktenkontos nicht die Sicherheit eines anderen Aktenkontos beeinträchtigt.

[<=]

EPA-EPF-A_0188 - Sichere Session-Verwaltung

Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS eine sichere Session-Verwaltung umsetzen.

[<=]

A_13679 - Sicherheitstechnische Validierung in der Dokumentenverwaltung

Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS eine Sicherheitsprüfung von allen übergebenen Daten durchführen, bevor die Datenverarbeitung stattfindet.

[<=]

EPA-EPF-A_0189 - 291a Protokollierung von Anwendungsfällen

Die Komponente Dokumentenverwaltung des ePA-Aktensystem MUSS für die folgenden Anwendungsfälle Einträge in das §291a-konforme Protokoll für den Versicherten bzw. seine Vertreter vornehmen:

- Dokumente einstellen
- Dokumente suchen
- Hinzufügen einer Dokumentenklassifizierung
- Metadaten ändern
- Dokument löschen
- Dokument anzeigen
- Dokumente herunterladen

[<=]

EPA-EPF-A_0190 - Verwaltungsprotokollierung in der Komponente Dokumentenverwaltung

Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS für die folgenden Anwendungsfälle Einträge in einem Verwaltungsprotokoll für den Versicherten bzw. seine Vertreter vornehmen.

- Berechtigung vergeben
- Vertretung einrichten
- Bestehende Berechtigungen verwalten
- Login
- Vertretung für einen Versicherten wahrnehmen
- Aktenkonto schließen

[<=]

A_13813 - Verwaltungsprotokollierung in der Komponente Dokumentenverwaltung Löschen von Protokolleinträgen

Die Komponente Dokumentenverwaltung MUSS sicherstellen, dass Protokolleinträge am Ende des auf ihre Generierung folgenden Kalenderjahres gelöscht werden. Ausnahme: Die 50 jüngsten Protokolleinträge DÜRFEN auch dann NICHT gelöscht werden, wenn die o. g. Frist erreicht bzw. überschritten ist.[<=]

5.4 Anforderungen an die vertrauenswürdige Ausführungsumgebung (VAU)

Die Vertrauenswürdige Ausführungsumgebung (VAU) weist die folgenden zentralen Datenschutz- und Informationssicherheitseigenschaften auf:

- Erkennung und Schadensreduzierung und -verhinderung von Angriffen,
- Ausschluss der schadhafte Einwirkung der Verarbeitung von Daten eines Versicherten auf die Verarbeitung von Daten eines anderen Versicherten,
- Ausschluss des Betreibers vom Zugriff auf die personenbezogenen medizinischen Daten sowie
- Überprüfbarkeit des Sicherheitszustands des Systems aus Sicht des sich verbindenden Systems.

Die VAU setzt eine durch die Mechanismen für den sicheren Betrieb von Fachdiensten im Rechenzentrum spezifizierte Umgebung voraus. Sie definiert die technischen Mechanismen zur Gewährleistung der genannten Datenschutz- und Informationssicherheitseigenschaften.

5.4.1 Isolation

Um zu verhindern, dass Verarbeitungsvorgänge eines Aktenkontos eines Versicherten schadhaft auf Verarbeitungsvorgänge anderer Versicherter einwirken können, werden Mechanismen zur Trennung der Verarbeitungskontexte gefordert.

EPA-EPF-A_0191 - Isolation zwischen Aktendatenverarbeitungsprozessen

Die VAU MUSS die in ihr ablaufenden Verarbeitungsprozesse für die Daten eines Aktenkontos von den Verarbeitungsprozessen für die Daten anderer Aktenkonten trennen.

[<=]

Die VAU stellt den technischen Mechanismus bereit, der auch den Betreiber des Fachdienstes vom Zugriff auf schützenswerte Aktendaten ausschließt.

EPA-EPF-A_0192 - Isolation von Datenverarbeitungsprozessen des Anbieters

Die VAU MUSS die in ihr ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters ePA-Aktensystem trennen.

[<=]

Neben dem Zugriff des Anbieters auf die in der VAU ablaufenden Datenverarbeitungsprozesse mittels anderer Datenverarbeitungsprozesse muss auch der physische Zugriff des Anbieters auf Systeme der VAU ausgeschlossen werden, um dem Anbieter die Möglichkeit zum Missbrauch von physikalischen Seitenkanälen zu nehmen. Dies erfordert einen technischen Zutrittsschutz.

EPA-EPF-A_0193 - Kein physischer Zugang des Anbieters zu Systemen der VAU

Die VAU MUSS technisch sicherstellen, dass der Anbieter ePA-Aktensystem während der Verarbeitung personenbezogener und medizinischer Daten keinen Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.

[<=]

5.4.2 Wartung

Der Austausch von Hardware-Komponenten bedingt den physischen Zugang zu Systemen.

EPA-EPF-A_0194 - Nutzdatenbereinigung vor physischem Zugang

Die VAU MUSS mit technischen Mitteln sicherstellen, dass physischer Zugang zu Hardware-Komponenten der VAU nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten mehr extrahiert werden können. [<=]

5.4.3 Integrität der VAU

EPA-EPF-A_0195 - Nur geprüfte Software in der VAU

Die VAU MUSS sicherstellen, dass ausschließlich integritätsgeprüfte Software in der VAU ausgeführt wird. [<=]

EPA-EPF-A_0196 - Eine für ein Aktenkonto initialisierte VAU verarbeitet Daten genau zu diesem Aktenkonto

Die VAU MUSS sicherstellen, dass sie ausschließlich Daten des Aktenkontextes verarbeitet, für den sie initialisiert wurde. [<=]

Sämtliche Aktendaten, die ein Speicherdienst vorhält, sind verschlüsselt. Für Daten aus dem Speicherdienst, die in der VAU im Klartext verarbeitet werden sollen, wird daher zunächst das entsprechende Schlüsselmaterial benötigt.

5.4.4 Vertrauenswürdigkeit aus Sicht des Nutzers

Ein Element für die Vertrauenswürdigkeit eines außerhalb der Umgebung des Nutzers (im Rechenzentrum) betriebenen Dienstes besteht darin, dass sich der Nutzer selbst davon überzeugen kann, dass er tatsächlich mit dem gewünschten Dienst verbunden ist und dass die Integrität der Datenverarbeitung durch den Dienst nicht kompromittiert ist.

Die Umsetzung einer vertrauenswürdigen Ausführungsumgebung besteht darin, Angriffe aus dem „Inneren“ des Betreibers mit primär technischen Mitteln zu verhindern. Eine Integritätsprüfung der VAU macht es für den Endbenutzer, wenn er mit einem System verbunden wird, erkennbar, ob dieses manipuliert wurde.

A_15704 - Nachweis der Integrität des Verarbeitungskontextes über sichere Verbindung

Die VAU MUSS für Client-Verbindungen einen sicheren Kommunikationskanal erzwingen und sich gegenüber Clients mit kryptographischen Identitäten authentisieren, deren Verwendung durch Aktenkontexte nur unter der Voraussetzung der Integrität der Aktenkontexte möglich ist. [≤]

5.4.5 Skalierbarkeit

Der Betrieb der ePA-Fachdienste verteilt sich voraussichtlich über mehrere Anbieter. Trotzdem fallen dem einzelnen Anbieter bis zu mehrere Millionen Aktenkonten zu. Der Fachdienst muss eine entsprechende Skalierbarkeit mitbringen und diese Forderung bildet sich auch auf die VAU ab.

EPA-EPF-A_0200 - Skalierbarkeit

Die VAU MUSS eine Skalierung auf bis zu mehrere Millionen Aktenkonten und eine entsprechende Anzahl gleichzeitiger Aktenkontexte ermöglichen. [≤]

5.4.6 Anforderungen an die Komponente Dokumentenverwaltung

Auf das Aktenkonto eines Versicherten greifen neben dem Versicherten (und Vertretern) die berechtigten Leistungserbringer zu. Es kann dazu kommen, dass mehrere Zugriffe auf ein Aktenkonto parallel erfolgen.

Die Meta- und Steuerungsdaten liegen außerhalb des Aktenkontos niemals unverschlüsselt vor. Da konkurrierende Zugriffe außerhalb des Aktenkontos daher weder erkannt noch gelöst werden können, muss die Dokumentenverwaltung alle erforderlichen Mechanismen zur Gewährleistung der transaktionalen Integrität der Daten umsetzen.

EPA-EPF-A_0201 - Parallele Zugriffe

Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS parallele Zugriffe auf das Aktenkonto eines Versicherten ermöglichen und dabei die transaktionale Integrität der gespeicherten Daten gewährleisten. [≤]

Der Schutz der transaktionalen Integrität der gespeicherten Daten erfordert einen Verarbeitungskontext, in dem alle parallelen Zugriffe zusammen kommen. Aus diesem Grund darf es zu einem Zeitpunkt maximal eine Instanz der Dokumentenverwaltung für das Aktenkonto eines Versicherten geben.

EPA-EPF-A_0202 - Eindeutige Dokumentenverwaltungsinstanz für ein Aktenkonto

Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS sicherstellen, dass parallele Zugriffe auf das Aktenkonto eines Versicherten immer in derselben Instanz

der Dokumentenverwaltung verarbeitet werden.

[<=]

Die Skalierbarkeit im Sinne des Supports einer vertraulichen Datenverarbeitung erfordert technische Mechanismen zur Erhaltung eines konsistenten Zustands der Lösung.

EPA-EPF-A_0203 - Konsistenter Systemzustand

Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS sicherstellen, dass ein konsistenter Zustand des Aktenkontos auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw. wiederhergestellt werden kann.

[<=]

Die für den Betrieb des Fachdienstes für den Anbieter erforderlichen technischen Log-Informationen über Verarbeitungsvorgänge innerhalb der Dokumentenverwaltung werden aus der Dokumentenverwaltung heraus bereitgestellt. Die für den Betrieb des ePA-Aktensystems für den Anbieter erforderlichen Monitoring-Informationen werden durch Komponenten außerhalb der VAU erhoben. In beiden Fällen muss sichergestellt werden, dass der Anbieter weder in Kenntnis vertraulicher Daten der Versicherten gelangt, noch Möglichkeiten zur Profilbildung (im Sinne von Rückschlüssen auf Beziehungen zwischen bestimmten Versicherten und bestimmten Leistungserbringern sowie im Sinne von Aktivitätsprofilen über Leistungserbringer) erhält.

EPA-EPF-A_0204 - Datenschutzkonformes Logging und Monitoring

Die Dokumentenverwaltung MUSS die für den Betrieb des Fachdienstes erforderlichen Log- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass dem Anbieter keine vertraulichen oder zur Profilbildung geeigneten Daten zur Kenntnis gelangen.

[<=]

6 Informationsmodell

Im Folgenden wird ein Ausschnitt aller verwendeten Datentypen erläutert.

Die Datentypen der Fachanwendung ePA gruppieren sich um die drei zentralen Datentypen:

- Document
- Record
- User

Ein berechtigter Nutzer (*User*) hat Zugriff auf ein Aktenkonto (*Record*), in dem Dokumente (*Document*) gespeichert werden. Zu einem Dokument gehört der Dokumenteninhalte selbst – z. B. ein Brief als PDF-Datei oder eine XML-Datei mit Laborwerten etc. – sowie Metadaten (*DocumentEntry*). Diese kategorisieren zum einen den Inhalt des Dokuments und stellen zum anderen den Personenbezug zu einem Versicherten bzw. Patienten her. Um die Dokumente in einer Dokumentenverwaltung zu organisieren, werden zusätzliche technische Attribute wie Dateigröße und kryptographischer Hash ergänzt. Die Metadaten eines Dokuments verfügen demnach sowohl über technische als auch personenbezogene medizinische Informationen. Um ein oder mehrere Dokumente in eine Akte einzustellen, müssen diese für jeden Aufruf der dazugehörigen Operation in einem Paket (*SubmissionSet*) zusammengefasst werden. Ein *SubmissionSet* verfügt seinerseits über Metadaten (z. B. Einstellungszeitpunkt, einstellende Organisation) und wird zusammen mit dem von ihm gebündelten Dokumenten in die Akte eingestellt. Metadaten zu Dokumenten und *SubmissionSets* können mittels einer Suchanfrage (*Query*) in einer Suchoperation im ePA-Aktensystem durchsucht werden. Die Suche nach *SubmissionSets* erlaubt auch im Nachhinein festzustellen, welche Dokumente zusammen in die Akte eingestellt wurden. Dokumente sind entweder technisch (*TechnicalDocument*) oder medizinisch (*MedicalDocument*).

Hinweis: Der konzeptionelle Parameter Query meint eine Formulierung einer Suchbedingung auf Attributen eines Dokuments. Query ist dabei nicht im IHE-Sinne zu verstehen.

Das Aktenkonto eines Versicherten (*Patient*) wird von genau einem Anbieter (*Provider*) zur Verfügung gestellt, der das dazugehörige Benutzerkonto (*Account*) des Versicherten verwaltet. Jedes Aktenkonto verfügt über eine eindeutige Kennung (*RecordIdentifier*), über die es beim Zugriff identifiziert werden kann und die auch zur Vergabe und Durchsetzung von Berechtigungen verwendet wird. Für jeden Aktenzugriff wird ein Kontext (*ContextInformation*) benötigt, der das Aktenkonto vor unberechtigtem Zugriff durch den Anbieter schützt.

Damit ein Nutzer auf ein Aktenkonto zugreifen kann, muss er sich zunächst authentisieren. Hierfür präsentiert er seine Zugangsdaten (*Credential*) und erhält für seine digitale Identität (*Identity*) eine Authentifizierungsbestätigung (*AuthenticationToken*). Mit der Authentifizierungsbestätigung und der Aktenkennung können die Berechtigungen geprüft werden. Ein Versicherter kann andere Nutzer für den Zugriff auf sein Aktenkonto berechtigen, indem er einen Autorisierungsschlüssel (*AuthorizationKey*) für den Berechtigten hinterlegt, welcher das kryptografische Schlüsselmaterial zu seinem Aktenkonto enthält. Ergänzend zum Autorisierungsschlüssel werden Benachrichtigungsinformationen zur Geräteverwaltung hinterlegt sowie eine Liste der verwendeten Geräte des Nutzers geführt. In der Komponente Dokumentenverwaltung wird eine Zugriffsregel

(PolicyDocument) für jeden zu berechtigenden Nutzer hinterlegt, mit der der Versicherte festlegt, auf welche Dokumente der Nutzer mit welchen Operationen (lesen, schreiben) in welchem Zeitraum zugreifen darf. Ein berechtigter Nutzer kann, analog zum Versicherten, über Authentifizierungs- und Autorisierungsbestätigung (AuthorizationToken) auf das Aktenkonto des Versicherten zugreifen.

Das Informationsmodell wird in der nachstehenden Abbildung dargestellt.

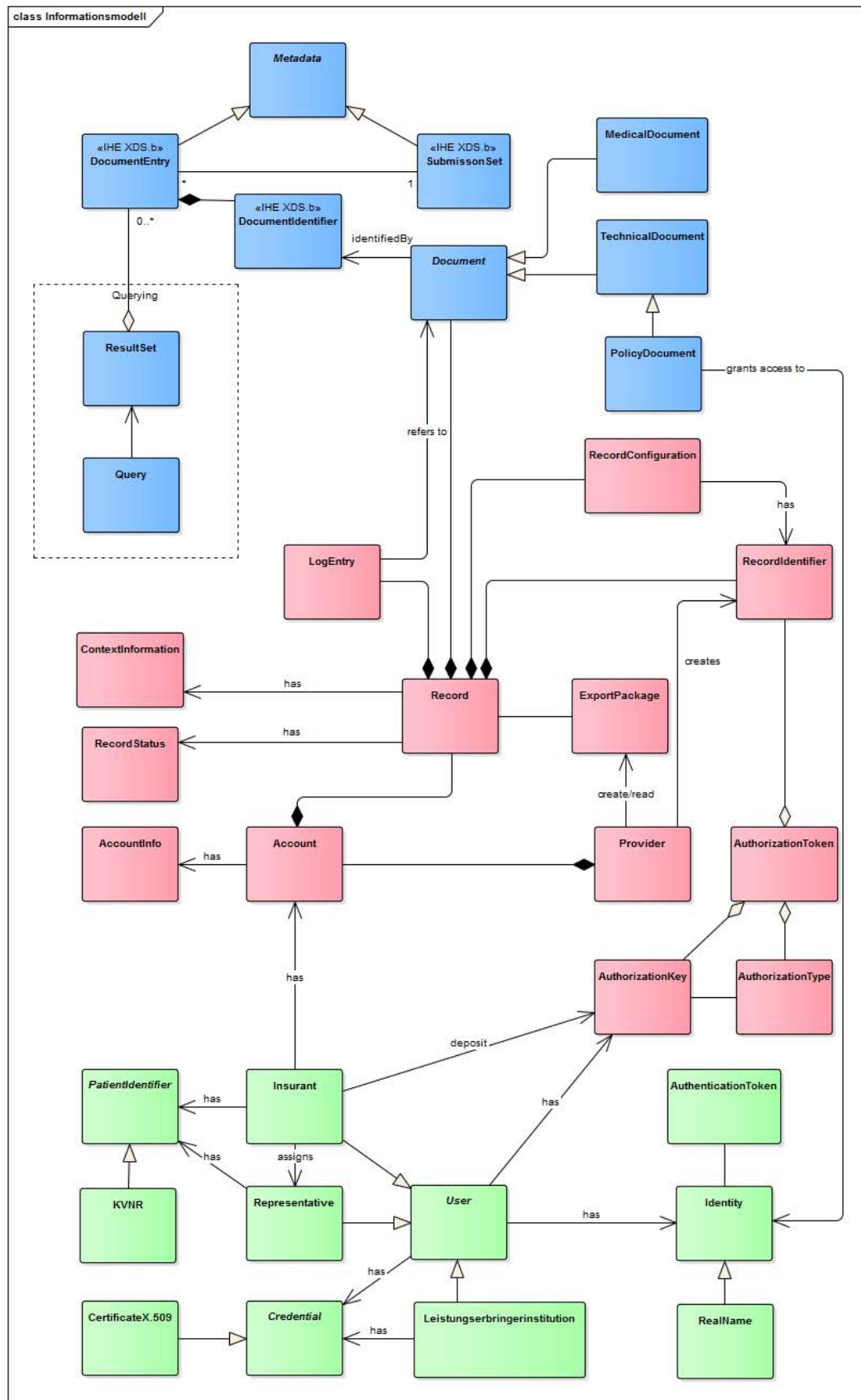


Abbildung 38: Informationsmodell

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

Abkürzung	Bedeutung
ATNA	Audit Trail and Node Authentication
CMP	Komponentendiagramm
DSGVO	Datenschutz-Grundverordnung
eGK	Elektronische Gesundheitskarte
ENC	Encryption – bezogen auf C.CH.ENC bzw. C.HCI.ENC meint „ENC“ das Zertifikat für die Verschlüsselung des Schlüsselmaterials einer Akte
ePA	Elektronische Patientenakte
GUI	Graphical User Interface
HBA	Heilberufsausweis
IHE	Integrating the Healthcare Enterprise
ITI	IHE IT Infrastructure
KVNR	Krankenversichertennummer
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
OID	Object Identifiers
PHR	Personal Health Record („Patientenakte“)
PS	Primärsystem
SD	Sequenzdiagramm
SGB	Sozialgesetzbuch
SMC-B	Security Modul Card Typ B

UC	Use Case Diagramm
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
VAU	Vertrauenswürde Ausführungsumgebung
VZD	Verzeichnisdienst
XDS	Cross-Enterprise Document Sharing

7.2 Glossar

Begriff	Erläuterung
Akte	Der Begriff „Akte“ ist in diesem Dokument gleichbedeutend mit „Aktenkonto“
Aktenkonto	Ein Aktenkonto wird durch die Gesamtheit der Daten eines Versicherten im ePA-Aktensystem eines Anbieters gebildet.
Aktensystem	Das ePA-Aktensystem ist ein Produkttyp der Fachanwendung ePA. Es stellt sicher, dass nur authentifizierte und autorisierte Nutzer mit dem ePA-Aktensystem interagieren. In einer Komponente zur Dokumentenverwaltung verwaltet das ePA-Aktensystem die Dokumente zu einem Aktenkonto eines Versicherten.
Ad-hoc-Berechtigung	Der Begriff beschreibt ein Prozess, indem ein Versicherter einen Mitarbeiter einer Leistungserbringerumgebung eine zeitlich eingeschränkte Zugriffsberechtigung auf sein Aktenkonto vergibt.
Aktenkontext	Separierung der Konten verschiedener Versicherter sowohl auf Ebene verschlüsselter Speicherung als auch auf Separierung der Ausführung von Fachlogik (Contentvalidierung, Dokumente suchen) innerhalb der Akte.

Aktenschlüssel	Der Aktenschlüssel ist ein symmetrischer Schlüssel, der alle Dokumente eines Versicherten schützt, indem der Aktenschlüssel die dazugehörigen Dokumentenschlüssel verschlüsselt.
Authentifizierung	Prüfen einer behaupteten Eigenschaft einer Entität, die beispielsweise ein Mensch bzw. seiner digitalen Identität, z.B. über ein Challenge-Response-Verfahren.
Authentisierung	Nachweisen der eigenen Identität, z. B. durch Präsentation einer glaubwürdigen Eigenschaft
Authentisierungsmerkmal	Im ePA-Kontext wird unter diesen Begriff der Einsatz der eGK + PIN bei der Authentisierung am ePA-Aktensystem verstanden.
Autorisierung	Gewähren von Zugriffsberechtigungen für sich authentisierende Nutzer.
berufsmäßige Gehilfen	Personen, die in einer Leistungserbringerinstitution als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind, jedoch nicht die Gehilfen der nichtärztlichen Psychotherapeuten.
BLOB	Unter dem Begriff wird ein großes binäres Datenobjekt verstanden.
Dokumentenschlüssel	Der Dokumentenschlüssel ist ein symmetrischer Schlüssel zur Verschlüsselung von Dokumenten in der dezentralen Umgebung.
Fachanwendung ePA	Die Fachanwendung ist die Summe aller Komponenten und Dienste, die zu ePA gehören und von ePA genutzt werden. Dazu gehören auch ePA-Frontends und Primärsysteme.

Fachmodul ePA	Das Fachmodul ePA wird im Konnektor ausgeführt. Es kapselt die Fachlogik gegenüber den Primärsystemen der Leistungserbringer und führt die sicherheitsrelevanten Anteile der Fachlogik (z. B. die Verschlüsselung der Dokumente) aus.
Frontend	Softwareprogramm mit grafischer Benutzeroberfläche zum Starten fachlicher Anwendungsfälle und Darstellung des Ergebnisses eines Anwendungsfalls.
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
HSM	Hardware Security Module, sicherer Speicher für kryptografisches Schlüsselmaterial
Kontextschlüssel	Der Kontextschlüssel ist ein symmetrischer Schlüssel, der Meta- und technische Daten einer Versichertenakte vor dem Zugriff eines Aktenanbieters schützt.
KVNR	Die Krankenversichertennummer wird von einer Krankenkasse für einen Versicherten vergeben. Die Nummer besteht aus einem unveränderlichen Teil (Krankenversicherten-ID) und einem veränderlichen Teil. In diesem Dokument wird die KVNR immer im Sinne der Krankenversicherten-ID verwendet.
Metadaten	Beschreibende Daten zu einem Dateinobjekt, z.B. beschreibende Daten zu einer Datei wie Dateigröße, Änderungsdatum usw.

OWASP	Open Web Application Security Project Organisation zur Verbesserung der Sicherheit von Anwendungen und Diensten im Internet
Record	Englische Bezeichnung für allgemein „Akte“, RecordIdentifier ist dem folgend der Parameter für die Akten-ID.
RecordIdentifier	Ein eindeutiger Bezeichner - synonym mit Akten-ID - für genau eine spezifische Akte.
Schlüsselmateriale	Das Schlüsselmateriale wird für die Erzeugung eines kryptografischen Schlüssels benötigt. Das Schlüsselmateriale kann zum Beispiel durch einen kryptografischen Zufallsgenerator erzeugt werden.
Session	Bezeichnet die Sitzung eines Nutzers, in dieser führt der Nutzer fachliche Anwendungsfälle der Fachanwendung ePA im Aktenkonto eines Versicherten aus.
Session-Daten	Temporäre Daten zur Sitzung eines Nutzers. In dezentralen Produkttypen zählen dazu der im Klartext vorhandene Aktenschlüssel, die Authentifizierungsbestätigung und ggfs. Autorisierungsbestätigung. Im ePA-Aktenystem zählen zu den Sessiondaten die ausgestellten Authentifizierungsbestätigung, Autorisierungsbestätigung sowie die in der vertrauenswürdigen Ausführungsumgebung der Komponente Dokumentenverwaltung verarbeiteten Daten eines Aktenkontos. Zum Ende der Sitzung werden die Session-Daten gelöscht.
Standardaktennutzung	Erwartetes Nutzungsprofil eines Standardnutzers

TCDP	Trusted Cloud Data Protection Profile for Cloud Services
Token	z.B. im Rahmen einer Authentisierung eines Nutzers signierte Bestätigung einer korrekten Authentifizierung durch einen Dritten
XACML	eXtensible Access Control Markup Language, das Policy Document mit den Zugriffsregeln in der Komponente Dokumentenverwaltung des ePA-Aktensystems ist gemäß XACML strukturiert

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

7.3 Abbildungsverzeichnis

Abbildung 1 : Dokumentenlandschaft ePA	8
Abbildung 2: Übersicht der Fachanwendung ePA	11
Abbildung 3: Fachliches Rollenmodell	16
Abbildung 4: Funktionale Zerlegung.....	19
Abbildung 5 : Kryptografisches Schlüsselmaterial.....	29
Abbildung 6: Übersicht der Anwendungsfälle ePA	31
Abbildung 7: Login durch einen Versicherten.....	34
Abbildung 8: Vertretung für einen Versicherten wahrnehmen	35
Abbildung 9: Login durch einen Leistungserbringer	37
Abbildung 10: Logout durch einen Versicherten.....	39
Abbildung 11: Logout in der Leistungserbringerumgebung	40
Abbildung 12: Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren	42
Abbildung 13: Lebenszyklus eines Kontos bei einem Anbieter.....	43
Abbildung 14: Schritt 1 – Aktenkonto beantragen	46
Abbildung 15: Schritt 2 – Aktivierung in der Umgebung des Leistungserbringers.....	47
Abbildung 16: Schritt 2 – Aktivierung in der Umgebung des Versicherten, mit Kartenterminal	48
Abbildung 17 : Anbieter wechseln	52
Abbildung 18: Berechtigung durch einen Versicherten vergeben	54
Abbildung 19: Vertretung durch einen Versicherten einrichten.....	57
Abbildung 20: Neue eGK über alte eGK bekannt machen	59

Abbildung 21: Neue eGK über Vertreter bekannt machen	61
Abbildung 22: Berechtigungen durch einen Versicherten auflisten.....	63
Abbildung 23: Bestehende Berechtigungen durch einen Versicherten verwalten	65
Abbildung 24: Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern	67
Abbildung 25: Umschlüsselung mit sicher verwahrtm Schlüsselmaterial.....	69
Abbildung 26: Dokumente durch einen Leistungserbringer einstellen	71
Abbildung 27: Dokumente durch einen Versicherten einstellen.....	73
Abbildung 28: Dokumente durch einen Leistungserbringer suchen.....	74
Abbildung 29: Dokumente durch einen Versicherten suchen	76
Abbildung 30: Ändern einer Dokumentenklassifizierung durch einen Leistungserbringer	78
Abbildung 31: Dokumente durch einen Leistungserbringer löschen	79
Abbildung 32: Dokumente durch einen Versicherten löschen	81
Abbildung 33: Dokumente durch einen Leistungserbringer anzeigen.....	82
Abbildung 34: Dokumente durch einen Versicherten anzeigen	84
Abbildung 35: Protokolldaten durch einen Versicherten einsehen.....	86
Abbildung 36: Systemzerlegung ePA.....	88
Abbildung 37: Übersicht über die Schnittstellen der Fachanwendung ePA	97
Abbildung 38: Informationsmodell	134

7.4 Tabellenverzeichnis

Tabelle 1: Kryptografische Identitäten der Akteure und ihre jeweilige Rolle	14
Tabelle 2 : Metadaten für die Dokumentenverwaltung	22
Tabelle 3: Berechtigungsmaske	24
Tabelle 4 : Übersicht über die Verfahren des Berechtigungserhalts für Versicherte	26
Tabelle 5: Login durch einen Versicherten	33
Tabelle 6: Login durch einen Leistungserbringer.....	36
Tabelle 7: Logout durch einen Nutzer	38
Tabelle 8: Berechtigungen für SMC-Bs durch einen Leistungserbringer aktualisieren....	41
Tabelle 9: Aktenkonto einrichten	44
Tabelle 10: Anbieter wechseln	50
Tabelle 11: Berechtigung durch einen Versicherten vergeben	53
Tabelle 12: Vertretung durch einen Versicherten einrichten	55
Tabelle 13: Neue eGK über alte eGK bekannt machen.....	58
Tabelle 14: Neue eGK über Vertreter bekannt machen.....	60

Tabelle 15: Berechtigungen durch einen Versicherten auflisten	62
Tabelle 16: Bestehende Berechtigungen durch einen Versicherten verwalten	64
Tabelle 17: Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern	66
Tabelle 18: Umschlüsselung mit sicher verwahrtem Schlüsselmaterial	68
Tabelle 19: Dokumente durch einen Leistungserbringer einstellen	70
Tabelle 20: Dokumente durch einen Versicherten einstellen	72
Tabelle 21: Dokumente durch einen Leistungserbringer suchen	74
Tabelle 22: Dokumente durch einen Versicherten suchen	75
Tabelle 23: Ändern einer Dokumentenklassifizierung durch einen Leistungserbringer	77
Tabelle 24: Dokumente durch einen Leistungserbringer löschen	79
Tabelle 25: Dokumente durch einen Versicherten löschen.....	80
Tabelle 26: Dokumente durch einen Leistungserbringer anzeigen	81
Tabelle 27: Dokumente durch einen Versicherten anzeigen	83
Tabelle 28: Protokolldaten durch einen Versicherten einsehen	86
Tabelle 29: Schnittstellen Fachmodul ePA.....	89
Tabelle 30: Schnittstellen-Autorisierung.....	90
Tabelle 31: Schnittstellen Dokumentenverwaltung	91
Tabelle 32: Schnittstellen Authentisierung Versicherter	93
Tabelle 33: Logische Operation find.....	98
Tabelle 34: Logische Operation getDocuments.....	98
Tabelle 35: Logische Operation putDocuments.....	99
Tabelle 36: Logische Operation updateMetadata	99
Tabelle 37: Logische Operation deleteDocuments	100
Tabelle 38: Logische Operation requestFacilityAuthorization	100
Tabelle 39: Logische Operation registerSMB	101
Tabelle 40: Logische Operation getHomeCommunityID	101
Tabelle 41 : Logische Operation activateAccount	102
Tabelle 42: Logische Operation getAuthorizationKey	103
Tabelle 43: Logische Operation putAuthorizationKey	104
Tabelle 44: Logische Operation replaceAuthorizationKey	104
Tabelle 45 Logische Operation checkRecordExists	105
Tabelle 46: Logische Operation ConnectToContext	105
Tabelle 47: Logische Operation openContext	106
Tabelle 48: Logische Operation closeContext	106
Tabelle 49 Logische Operation getExportPackage	107
Tabelle 50: Logische Operation find.....	107

Tabelle 51: Logische Operation putDocuments.....	108
Tabelle 52: Logische Operation getDocuments.....	108
Tabelle 53: Logische Operation updateMetadata.....	109
Tabelle 54: Logische Operation deleteDocuments.....	109
Tabelle 55: Logische Operation login.....	110
Tabelle 56: Logische Operation getAuditEvents.....	111
Tabelle 57: Logische Operation getAuthorizationKey.....	111
Tabelle 58: Logische Operation putAuthorizationKey.....	112
Tabelle 59: Logische Operation deleteAuthorizationKey	113
Tabelle 60: Logische Operation replaceAuthorizationKey	113
Tabelle 61 Logische Operation getAuditEvents.....	114
Tabelle 62: Logische Operation putNotificationInfo	114
Tabelle 63: Logische Operation suspendAccount	115
Tabelle 64: Logische Operation resumeAccount.....	116
Tabelle 65: Logische Operation getAuditEvents.....	116
Tabelle 66: Logische Operation find.....	117
Tabelle 67: Logische Operation putDocuments.....	117
Tabelle 68: Logische Operation getDocuments.....	118
Tabelle 69: Logische Operation deleteDocuments.....	118

7.5 Referenzierte Dokumente

7.5.1 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 entnehmen Sie bitte der aktuellsten, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemGlossar]	gematik: Glossar
[gemKPT_Arch_TIP]	gematik: Architekturkonzept der TI-Plattform

7.5.2 A5.2. – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt (zuletzt geprüft am 02.05.2018)
[XACML-V2.0]	OASIS Standard eXtensible Access Control Markup Language (XACML) Version 2.0, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf (zuletzt geprüft 02.05.2018)
[IHE_ITI_14.0]	IHE – Integrating the Healthcare Enterprise (Final Text, Revision 14.0 vom 21.07.2017): IHE IT Infrastructure (ITI) Technical Framework, http://ihe.net/Technical_Frameworks/#IT (zuletzt geprüft am 02.05.2018)
TCDP	Trusted Cloud Data Protection Profile for Cloud Services, https://www.tcdp.de/index.php/dokumente (zuletzt geprüft am 02.05.2018)
[IHE-ITI-VS]	IHE Deutschland (2016): Value Sets für Aktenprojekte im deutschen Gesundheitswesen, Implementierungsleitfaden, Version 2.0, http://www.ihe-d.de/download/ihe-valuesets-v2-0/ (zuletzt geprüft am 30.10.2018)
[IHE_PCC_TF]	IHE International (2016): IHE Patient Care Coordination (PCC) Technical Framework, Volume 2, IHE PCC TF-2, Transactions and Content Modules, Revision 11.0 - Final Text, http://www.ihe.net/uploadedFiles/Documents/PCC/IHE_PCC_TF_Vol2.pdf (zuletzt geprüft am 18.07.2018)