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

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation ePA-Frontend des Versicherten

ENTWURF

Version:	1.~~7~~8.0 CC
Revision:	~~294783~~304775
Stand:	09.12.~~11.~~2020
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_ Entwurf
Referenzierung:	gemSpec_ePA_FdV

Dokumenteninformation

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	18.12.18		Erstversion	gematik
1.1.0	15.05.19		Einarbeitung P18.1	gematik
1.2.0	28.06.19		Einarbeitung P19.1	gematik
1.3.0	02.10.19		Einarbeitung P20.1/2	gematik
1.4.0	02.03.20		Einarbeitung P21.1	gematik
1.5.0	27.03.20		Einarbeitung P21.2	gematik
1.5.1	26.06.20		Einarbeitung P21.3	gematik
1.6.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
1.7.0	12.11.20		Einarbeitung Scope-Themen, PDSG-Änderungen	gematik
1.8.0 CC	09.12.20		Einarbeitung Änderungsliste P22.5	gematik

ENTWURF

Inhaltsverzeichnis

ENTWURF

ENTWURF

ENTWURF

ENTWURF

ENTWURF

ENTWURF

1 Einordnung des Dokumentes

1.1 Zielsetzung

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

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller von Produkten des Frontend des Versicherten sowie an Hersteller und Anbieter von weiteren Produkttypen der Fachanwendung ePA.

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

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

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

ENTWURF

1.5 Methodik

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

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

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

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

ENTWURF

2 Systemüberblick

Das ePA-Frontend des Versicherten (FdV) ist eine Anwendung, welche die für die Nutzung der ePA notwendigen Funktionalitäten bündelt und dezentrale Fachlogik der Fachanwendung ePA ausführt. Das FdV ermöglicht es Versicherten, ePA-Anwendungsfälle auszuführen.

Ausführungsumgebung des FdV ist ein Gerät des Versicherten (GdV), bspw. ein stationäres Gerät oder ein mobiles Endgerät. Es steht unter alleiniger Kontrolle des Versicherten. Dem Versicherten obliegt es, durch geeignete Maßnahmen die Sicherheit der Daten zu stärken.

Das FdV kann zusätzliche Funktionalitäten anbieten, die nicht der Fachanwendung ePA zugeordnet werden und somit nicht der Regelungshoheit der gematik unterliegen.

ENTWURF

3 Systemkontext

3.1 Akteure und Rollen

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

Tabelle 1: TAB_FdV_101 – Akteure und Rollen

Akteur	Rolle	Beschreibung
~~Nutzer der~~Nutzerder FdV	Versicherter (als Aktenkontoinhaber) oder Vertreter eines Versicherten	Primärer Anwender, Ausführen von fachlichen Anwendungsfällen mit Zugriff auf ein ePA-Aktensystem
Ausführungsumgebung	Gerät des Versicherten	Betriebs-/Ablaufumgebung des FdV
Kartenleser	Gerät des Versicherten	Ermöglicht dem ePA-Frontend des Versicherten den Zugriff auf die eGK des Nutzers. Es kann die kontaktbehaftete oder die kontaktlose Schnittstelle der eGK genutzt werden.
Anbieter ePA-Aktensystem	Organisatorisch, kein Akteur in der Ausführung von ePA-Anwendungsfällen	Der Anbieter stellt Informationen bereit, um sich via FdV am ePA-Aktensystem anzumelden.
Hersteller ePA-Frontend des Versicherten	Organisatorisch, kein Akteur in der Ausführung von ePA-Anwendungsfällen	Der Hersteller FdV stellt im Handbuch Informationen bereit bezüglich • Anforderungen an die Ausführungsumgebung • Möglichkeiten zur Anbindung der eGK Der Hersteller FdV erfüllt sicherheitstechnische Anforderungen zum

ENTWURF

		Herstellungsprozess.

3.2 Nachbarsysteme

Die vom FdV direkt erreichbaren Produkttypen der TI sind

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

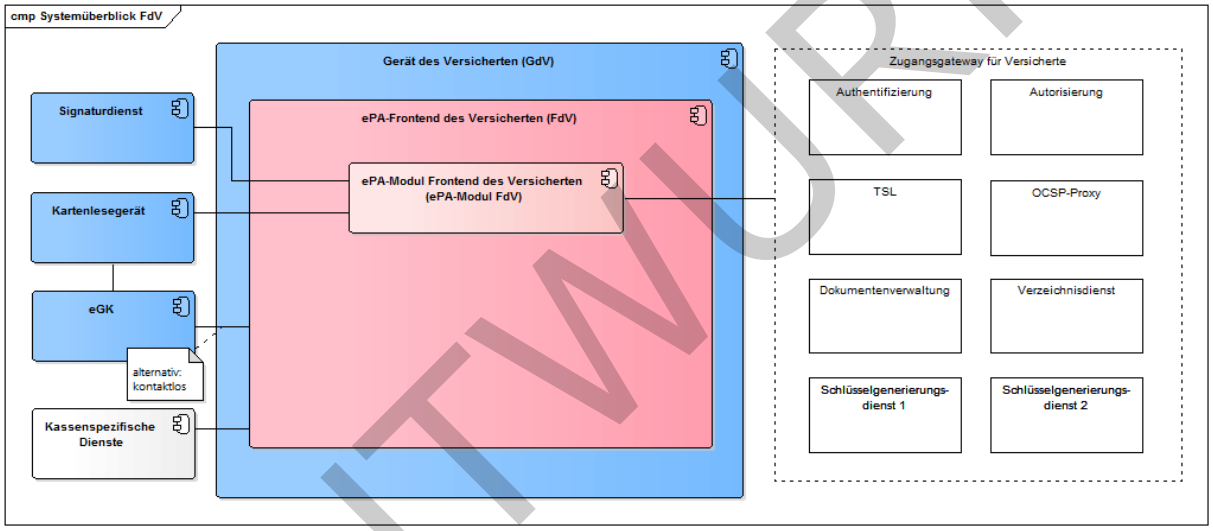


Abbildung 1: Systemüberblick FdV

Der Signaturdienst bietet die Schnittstelle `I_Remote_Sign_Operations` für Signaturen mittels der alternativen kryptographischen Versichertenidentität an. Siehe [gemSpec_SigD].

In TAB_FdV_102 sind die Schnittstellen des ePA-Aktensystems gelistet, welche durch das ePA-Frontend des Versicherten

genutzt werden.

Tabelle 2: TAB_FdV_102 – Schnittstellen des ePA-Aktensystems

Schnittstelle	Operationen	Bemerkung
I_Authentication_Insurant	getAuditEvents LoginCreateChallenge LoginCreateToken LogoutToken RenewToken	Definition in [gemSpec_Authentisierung_Vers]

ENTWURF

I_Authorization_Insurant	getAuthorizationKey	Definition in [gemSpec_Autorisierung]
I_Authorization_Management_Insurant	deleteAuthorizationKey getAuditEvents getAuthorizationList putAuthorizationKey putNotificationInfo replaceAuthorizationKey	Definition in [gemSpec_Autorisierung]
I_Account_Management_Insurant	GetAuditEvents SuspendAccount ResumeAccount	Definition in [gemSpec_Dokumentenverwaltung]
I_Proxy_Directory_Query	Search	Definition in [gemSpec_Zugangsgateway_Vers]
I_Document_Management_Connect	CloseContext OpenContext	Definition in [gemSpec_Dokumentenverwaltung]
I_Document_Management_Insurant	ProvideAndRegisterDocumentSet-b RegistryStoredQuery RemoveMetadata RetrieveDocumentSet RestrictedUpdateDocumentSet	Definition in [gemSpec_Dokumentenverwaltung]
Status-Proxy		Definition in [gemSpec_Zugangsgateway_Vers]
TSL-Proxy		Definition in [gemSpec_Zugangsgateway_Vers]
Schlüsselgenerierungsdienst Typ 1 und Typ 2		Definition in [gemSpec_SGD_ePA]

344

345 Für die Authentisierung mittels eGK und kryptographischer Operationen greift das ePA-
346 Frontend des Versicherten über ein Kartenlesegerät oder über die kontaktlose
347 Schnittstelle auf die eGK zu.

ENTWURF

3.2.1 Identität des Nutzers

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

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

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

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

ENTWURF

4 Zerlegung des Produkttyps

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

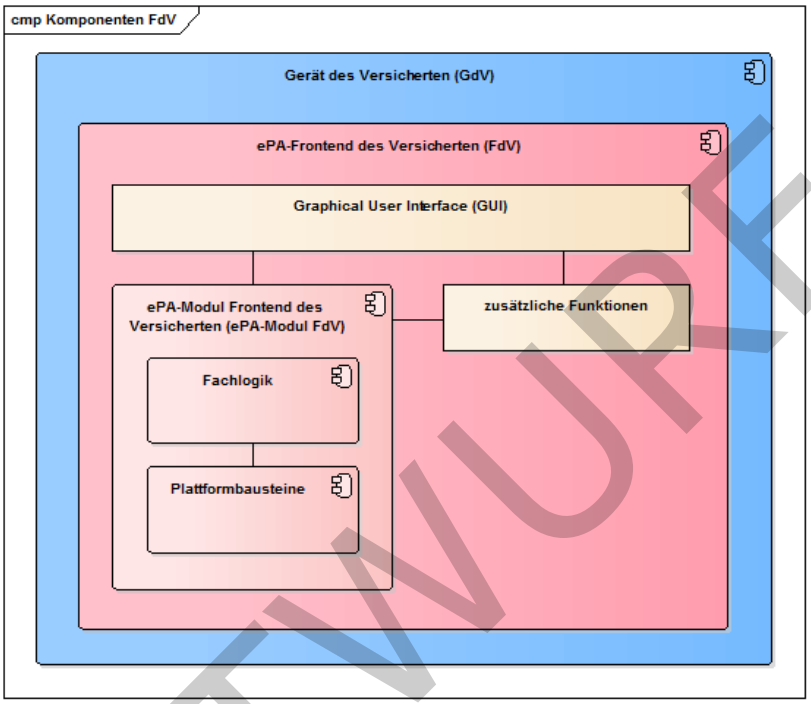


Abbildung 2: Komponenten ePA-Frontend des Versicherten

Tabelle 3: TAB_FdV_167 – Komponenten des FdV

Komponente	Verantwortung und Funktionalität	Spezifiziert in
Fachlogik	Die Komponente steuert die Anwendungsfälle entsprechend den fachanwendungsspezifischen Festlegungen.	Kap. 6.2
Plattformbausteine	Diese Komponente enthält Plattformbausteine, welche Funktionalitäten der TI-Plattform zur Verfügung stellen: • Zugriff auf die eGK für kryptografische Operationen, PIN-Management, ... • Kryptografische Operationen Die Plattformbausteine werden durch die Fachlogik angesteuert.	Kap. 6.3

ENTWURF

Das für die Nutzung des ePA-Frontend des Versicherten notwendige GUI ist Teil des FdV und wird nicht normativ durch die Spezifikation des FdV vorgegeben.

Das FdV kann zusätzliche Funktionen beinhalten, bspw. kassenspezifische Funktionen, welche Schnittstellen zu kassenspezifischen Diensten außerhalb der TI nutzen.

Das ePA-Frontend des Versicherten besitzt eine produktspezifische anwendungsinterne Schnittstelle, welche durch das GUI oder die zusätzlichen Funktionalitäten der integrierenden Anwendung genutzt werden kann, um ePA-Anwendungsfälle auszuführen.

ENTWURF

5 Übergreifende Festlegungen

Das ehemalige ePA-Modul FdV wurde als eigenständiges Objekt der Produktzulassung vollständig abgelöst vom ePA-Frontend des Versicherten (also der Gesamt-App). Das sollte durch die Verfahrensbeschreibung und den Aufbau sowie die Bezeichnung des Produkttypsteckbriefs eindeutig und normativ dargestellt sein. Das heißt, prinzipiell richten sich alle Anforderungen des Produkttypsteckbriefs an die gesamte ePA-App bzw. an deren Entwicklungsprozess. Der Nachweis zur Erfüllung der Anforderungen erfolgt dabei im Einzelnen folgendermaßen:

- Die Menge der Anforderungen zur funktionalen Eignung, deren Erfüllung im Produkttest bzw. Produktübergreifenden Test nachzuweisen ist, entspricht weitgehend der die ursprünglich dem ehemaligen ePA-Modul zugeordnet war. Es handelt sich um die Vorgaben an die Funktionalität für den Zugriff auf die ePA (die Komponenten der TI). Der Test erfolgt, unverändert zum bisher geplanten Vorgehen, unter Einsatz des AKTORs und der Testtreiberschnittstelle.
- Die Menge der Anforderungen zur funktionalen Eignung, deren Erfüllung durch Herstellererklärung zu belegen ist, umfasst nunmehr auch Anforderungen, die bisher nur mittelbar durch das Verfahren der Bestätigung der Entwicklungsprozesse an die gesamte App gestellt wurden. Dabei handelt es sich beispielsweise um elementare Anforderungen an die Nutzerinteraktion (Anzeige etc.), die nicht unter Nutzung des AKTORs geprüft werden können/sollen.
- Die Anforderungen der sicherheitstechnischen Eignung, deren Erfüllung im Produktgutachten bzw. in der CC-Evaluierung nachzuweisen ist, richten sich an die gesamt App – der Betrachtungsgegenstand der Prüfung ist die gesamte App einschließlich der von der gematik nicht spezifizierten Funktionalität.
- Die Herstellererklärung zur sicherheitstechnischen Eignung bezieht sich auf die Erfüllung von Anforderungen an die gesamte App.
- Die Anforderungen zur Sicherheitsbegutachtung entsprechen denen, die nach dem bisherigen Verfahren in der Bestätigung der sicheren Entwicklungsprozesse des Herstellers nachgewiesen wurden.

Die Gesamtmenge der Anforderungen, die sich aus der Zusammenführung der Produktzulassung und der Bestätigung der Entwicklungsprozesse des Herstellers ergibt, ist im Wesentlichen unverändert geblieben.

Die Darstellung in der Systemlösung hat keinen normativen Charakter, was den Schnitt der Zulassungsobjekte und deren inneren Aufbau betrifft.

5.1 Datenschutz und Sicherheit

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

A_16973-01 - ePA-Frontend des Versicherten: lokale Ausführung
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass alle ePA-fachanwendungsspezifischen Anteile lokal auf dem Gerät des Versicherten ausgeführt werden.**[<=]**

ENTWURF

A_15251 - ePA-Frontend des Versicherten: Anforderungen an Ausführungsumgebung
Der Hersteller des ePA-Frontends des Versicherten MUSS den Nutzer über die Annahmen und Anforderungen an die Ausführungsumgebung seines Produktes informieren.**[<=]**

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

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

A_17723 - ePA-Frontend des Versicherten: Über mögliche Schadsoftware informieren
Der Hersteller des ePA-Frontends des Versicherten MUSS den Nutzer darüber informieren, dass Dokumente Schadsoftware enthalten können und welche Maßnahmen der Nutzer zum Selbstschutz vornehmen kann.**[<=]**

A_15252-02 - ePA-Frontend des Versicherten: Schlüsselmaterial nicht persistent speichern
Das ePA-Frontend des Versicherten DARF alle verwendeten symmetrischen und privaten asymmetrischen Schlüssel NICHT persistent speichern, sofern es sich nicht um Authentisierungsmerkmale handelt.**[<=]**

Hinweis: Die Anforderung A_20211 legt die Bedingungen für die persistente Speicherung von Authentisierungsmerkmalen fest.

A_15253-01 - ePA-Frontend des Versicherten: Schutz Session-Daten
Das ePA-Frontend des Versicherten DARF Session-Daten NICHT an Dritte, außer im Rahmen der in den Anwendungsfällen spezifizierten Kommunikation, weitergeben.**[<=]**

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

A_15254-01 - ePA-Frontend des Versicherten: Session-Daten nicht persistent speichern
Das ePA-Frontend des Versicherten DARF Session-Daten NICHT persistent speichern.**[<=]**

A_17625-01 - ePA-Frontend des Versicherten: Keine Speicherung der PIN der eGK
Das ePA-Frontend des Versicherten DARF die PIN der eGK NICHT speichern.**[<=]**

A_20211-01 - ePA-Frontend des Versicherten: Schutz von gespeicherten Authentisierungsmerkmalen
Das ePA-Frontend des Versicherten DARF Authentisierungsmerkmale NICHT speichern, außer wenn

- der Versicherte sich hierfür bewusst entscheidet (Opt-in),
- die Speicherung des Authentisierungsmerkmals auf dem Endgerät gemäß den Anforderungen O.Data_2 und O.Data_3 der BSI TR-03161 erfolgt,
- auf das gespeicherte Authentisierungsmerkmal ausschließlich durch das ePA-Frontend des Versicherten nach erfolgreicher Authentifizierung des Versicherten über die Biometrie des Endgeräts oder die PIN bzw. das Passwort des Endgerätes zugegriffen werden kann,

ENTWURF

- die biometrischen Sensoren des Endgerätes die Anforderungen O.Biom_x der BSI TR-03161 mit Ausnahme der O.Biom_2 erfüllen,
- die Forderung O.Biom_3 der BSI TR-03161 mit einer Whitelist umgesetzt wird (d.h. eine Blacklist ist nicht möglich) und
- die Qualität und Eigenschaften des biometrischen Sensors die spezifischen Anforderungen zur Biometrie des BSI-Dokumentes „Bewertung von Authentisierungslösungen gemäß TR-03107" für das Vertrauensniveau von mindestens „substanziell" erfüllen.

Die oben beschriebene Ausnahme vom Verbot der Speicherung von Authentisierungsmerkmalen gilt nicht für die PIN der eGK, die niemals gespeichert werden darf.
[<=]

A_20746 - ePA-Frontend des Versicherten: Authentifizierung des Nutzers am ePA-FdV
Das ePA Frontend des Versicherten MUSS den Nutzer beim Starten des ePA Frontends des Versicherten am ePA Frontend des Versicherten authentisieren. **[<=]**

Hinweis: Für die Authentifizierung des Nutzers am ePA-FdV können die Authentifizierungsfunktionen des Betriebssystems des Endgerätes (z.B. Logscreen-Credentials, Biometrie) genutzt werden. Bei der Authentifizierung der oberen Anforderung ist nicht die Anmeldung an Backendsystemen (z.B. ePA-Aktensystem) gemeint, sondern die Authentifizierung am ePA-Frontend des Versicherten.

A_20747 - ePA-Frontend des Versicherten: Hinweis auf Verwendung eines sicheren PINs/Passworts bei Erstnutzung
Das ePA Frontend des Versicherten MUSS den Versicherten bei Erstverwendung des ePA-Frontend des Versicherten darauf hinweisen, dass dieser bei Wahl einer PIN oder eines Passworts zur Freischaltung seines Endgerätes, die bzw. das auch zur Authentisierung am ePA-Frontend des Versicherten genutzt wird, eine sichere PIN bzw. ein sicheres Passwort nutzen sollte inkl. Hinweisen, wie eine sichere PIN bzw. ein sicheres Passwort zu wählen sind.**[<=]**

A_15255-01 - ePA-Frontend des Versicherten: Schutzmaßnahmen gegen die OWASP-Mobile-Top-10-Risiken
Das ePA-Frontend des Versicherten MUSS Maßnahmen zum Schutz vor den in der aktuellen Version genannten OWASP-Top-10-Mobile-Risiken [OWASPMobileTop10] umsetzen.**[<=]**

Dies betrifft bspw. die folgenden Aspekte:

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

Für mobile Anwendungen sind OWASP Top Ten Mobile Controls [OWASP TTMC] und OWASP MASVS – L2 + R [OWASP MASVS] zu beachten. Anforderung A_15255-01 ist sowohl für Lösungen auf mobilen als auch Desktop-Plattformen umzusetzen.

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

ENTWURF

A_17660 - ePA-Frontend des Versicherten: Schutzmaßnahmen gegen Schadsoftware aus Dokumenten
Das ePA-Frontend des Versicherten MUSS, wenn es Dokumentinhalte direkt anzeigt, Maßnahmen zum Schutz vor Schadsoftware in den Dokumenten umsetzen.**[<=]**

Folgende Maßnahmen sind sinnvoll:

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

A_15256-02 - ePA-Frontend des Versicherten: Verbot von Werbe-Tracking
Das ePA-Frontend des Versicherten DARF ein Werbe-Tracking NICHT verwenden.**[<=]**

Im Folgenden wird unter Tracking Usability-Tracking sowie Crash-Reporting verstanden.

A_18767 - Tracking-Funktionen – Keine Weitergabe von Sicherheitsmerkmalen
Das ePA-Frontend des Versicherten MUSS sicherstellen, falls es Tracking-Funktionen implementiert, dass in den übermittelten Tracking-Informationen keine Sicherheitsmerkmale enthalten sind.**[<=]**

Hinweis: Sicherheitsmerkmale sind die Gerätekennung (DeviceID) und Session-Daten wie z.B. geheime oder private Schlüssel, Authentifzierungs- oder Autorisierungsbestätigungen.

A_18768 - Tracking-Funktionen – Verarbeitung und Auswertung der Tracking-Daten
Der Hersteller des ePA-Frontend des Versicherten MUSS die Verarbeitung und Auswertung der gesammelten Tracking-Daten des ePA-Frontends des Versicherten selbst durchführen und nicht von einem Drittanbieter durchführen lassen.**[<=]**

A_18769 - Tracking-Funktionen – Keine direkt identifizierenden personenbezogenen Daten
Das ePA-Frontend des Versicherten MUSS sicherstellen, falls es Tracking-Funktionen nutzt, dass die Tracking-Daten keine Daten enthalten, die natürliche Personen direkt identifizieren.**[<=]**

Hinweis: Personenbezogene Daten mit direktem Personenbezug sind bspw. Namen von natürlichen Personen, Geräte-IDs, Nutzerkennungen oder ein „Fingerabdruck" auf Basis von Geräteeigenschaften und Einstellungen.

Tracking Anforderungen für Trackingdaten ohne Einwilligung

A_18770 - Tracking-Funktionen – Ohne Einwilligung des Nutzers
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen ohne Einwilligung des Versicherten nutzt, sicherstellen, dass die Tracking-Daten

- sich nur auf eine Nutzersession (von der ersten Interaktion des Nutzers mit dem FdV bis zum Schließen des FdVs bzw. bis zum Inaktivitätstimeout) beziehen und nicht mit anderen Sessions des Nutzers verknüpft werden,
- weder personenbezogene noch pseudonymisierte personenbezogene Daten enthalten,

ENTWURF

- keine nutzerbezogenen IDs oder gerätespezifischen IDs der Nutzergeräte enthalten,
- keinen Rückschluss auf Versicherte, deren Vertreter, Leistungserbringer oder Kostenträger ermöglichen, insbesondere Rückschlüsse anhand des Nutzerverhaltens über die Zeit oder über Nutzersessions hinweg,
- nicht durch die Verknüpfung mit personenbezogenen Daten aus anderen Quellen de-anonymisiert werden können.

[<=]

Hinweis: Andere Quellen sind z.B. Webtracker, Tracker von anderen Apps oder Trackingmerkmale des Betriebssystems (z.B. Hardware IDs, Network IDs oder Advertising IDs).

A_19061 - Tracking-Funktionen – Nutzer Informieren
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen ohne Einwilligung des Versicherten nutzt, den Nutzer über das Tracking im ePA-FdV in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache informieren, bevor die Trackingdaten erhoben werden.
[<=]

Hinweis: Diese Anforderung ist nicht durch einen alleinigen Verweis auf die AGB oder Nutzungsbedingungen des FdVs erfüllbar. Verständliche Form bedeutet eine kurze nicht juristische Erklärung zum Zweck des Trackings. Leicht zugängliche Form bedeutet direkt im FdV.

A_18771 - Tracking-Funktionen – Generierung von Nutzersession basierte Trackingmerkmale
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen ohne Einwilligung des Versicherten nutzt, beim Start einer Nutzersession die Nutzersession-ID zufällig neu generieren.**[<=]**

Anforderungen zur Einwilligung zum Session-übergreifenden Tracking

A_18772 - Tracking-Funktionen - Opt-in
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass diese Tracking-Funktionen bei der Installation des FdV standardmäßig deaktiviert sind und nur nach expliziter Einwilligung durch den Versicherten als Nutzer des FdV aktiviert werden (Opt-in).**[<=]**

A_18773 - Tracking-Funktionen – Kopplungsverbot
Das ePA-Frontend des Versicherten DARF, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpft, die Nutzung des FdVs NICHT an die Aktivierung dieser Trackingfunktion koppeln. **[<=]**

Hinweis: Das FdV muss voll-funktional ohne aktiviertes Tracking nutzbar sein.

A_18774 - Tracking-Funktionen - Einwilligungsinformation des Nutzers
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, den Versicherten vor der Einwilligung in die Aktivierung dieser Tracking-Funktionen in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache folgende Einwilligungsinformationen anzeigen:

- welche Daten durch die Tracking-Funktionen erhoben werden,

ENTWURF

- zu welchen Zwecken die Daten erhoben werden,
- welche Informationen durch die Auswertung der erhobenen Daten gewonnen werden und ob Rückschlüsse auf den Gesundheitszustand des Nutzers möglich wären,
- wer die Empfänger der Daten sind,
- wie lange die Daten gespeichert werden.

[<=]

Hinweis: Diese Anforderung ist nicht durch einen alleinigen Verweis auf die AGB oder Nutzungsbedingungen des FdVs erfüllbar. Verständliche Form bedeutet eine kurze nicht juristische Erklärung zum Zweck des Trackings. Leicht zugängliche Form bedeutet direkt im FdV.

A_18775 - Tracking-Funktionen – Aktivierung erst nach Lesebestätigung der Einwilligungsinformationen
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, sicherstellen, dass die Einwilligung des Nutzers in die Aktivierung der Tracking-Funktionen erst erfolgt, wenn der Nutzer bestätigt, die angezeigten Einwilligungsinformationen gelesen zu haben.**[<=]**

A_18776 - Tracking-Funktionen – Deaktivierung ist jederzeit möglich
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass aktivierte Tracking-Funktionen jederzeit durch den Nutzer des FdVs deaktiviert werden können.**[<=]**

A_18777 - Tracking-Funktionen – Neue Generierung der Pseudonyme ist jederzeit möglich
Das ePA-Frontend des Versicherten SOLL, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass eine neue Generierung der pseudonymen Identifier jederzeit durch den Nutzer des FdVs veranlasst werden kann.**[<=]**

A_18778 - Tracking-Funktionen – Verbot von mehrmaligen Einwilligungsabfragen
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass der Benutzer der App maximal einmal eine Abfrage zur Einwilligung des Trackings angezeigt bekommt.**[<=]**

Hinweis: Wenn der Benutzer seine Einwilligung zum Tracking nicht erteilt, darf das FdV den Nutzer nicht solange nach seiner Einwilligung fragen, bis der Nutzer diese erteilt.

A_15257-01 - ePA-Frontend des Versicherten: Qualität verwendeter Schlüssel
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass die von ihm erzeugten Schlüssel die Qualität nach [gemSpec_Krypt#GS-A_4368] besitzen.**[<=]**

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

ENTWURF

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

A_15258-01 - ePA-Frontend des Versicherten: Dynamische Inhalte von Drittanbieter
Das ePA-Frontend des Versicherten DARF dynamische Inhalte von Drittanbietern NICHT herunterladen oder verwenden.**[<=]**

A_15259-01 - ePA-Frontend des Versicherten: Privacy bei default
Das ePA-Frontend des Versicherten MUSS bei Konfigurationsmöglichkeiten die sichere, datenschutzfreundlichere Option vorauswählen.**[<=]**

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

A_15261-01 - ePA-Frontend des Versicherten: Sicherheitsrisiken von Software Bibliotheken minimieren
Das ePA-Frontend des Versicherten MUSS Maßnahmen umsetzen, um die Auswirkung von unentdeckten Schwachstellen in benutzten Software-Bibliotheken zu minimieren.**[<=]**

Hinweis: Beispielmaßnahmen sind in [OWASP Proactive Control#C2] zu finden. Das gewählte Verfahren muss die gleiche Wirksamkeit aufweisen, wie die Kapselung gemäß [OWASP Proactive Control#C2 Punkt 4].

Das ePA-Frontend des Versicherten bietet nur Funktionalitäten an, welche sich aus den Anwendungsfällen der Fachanwendung ePA ergeben.

Zusätzliche Funktionalitäten können durch das FdV angeboten werden. Folgende Anforderungen gelten für die Abgrenzung der zusätzlichen Funktionalitäten zu denen der Fachanwendung ePA.

A_16438 - ePA-Frontend des Versicherten: Unterscheidbarkeit zusätzlicher Funktionalitäten
Das ePA-Frontend des Versicherten MUSS sicherstellen, falls es zusätzliche Funktionalitäten enthält, dass der Nutzer diese zusätzlichen Funktionalitäten von den Funktionalitäten für die ePA unterscheiden kann.**[<=]**

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

A_18401 - ePA-Frontend des Versicherten: Verarbeiten von ePA-Daten in zusätzlichen Funktionalitäten - Zustimmung
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass der Nutzer dem Verarbeiten der ePA-Daten in zusätzlichen Funktionalitäten des ePA-Frontends des Versicherten bezüglich Umfang, Art und Dauer der Verarbeitung vor dem Zugriff der Zusatzfunktionen auf die ePA-Daten zustimmen muss.**[<=]**

A_18402 - ePA-Frontend des Versicherten: Verarbeiten von ePA-Daten in zusätzlichen Funktionalitäten - Opt-In
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass die Zustimmung zur Verarbeitung der ePA-Daten in zusätzlichen Funktionalitäten des ePA-Frontends des Versicherten optional (Opt-In) und jederzeit widerrufbar ist.**[<=]**

ENTWURF

A_16439 - ePA-Frontend des Versicherten: Weiterleiten von Daten - Zustimmung
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass Daten, die aus der ePA ins FdV geladen werden, nur mit Zustimmung des Versicherten unter Nutzung von expliziten Opt-in-Lösungen weitergeleitet werden können, wobei sich das Opt-In nur genau auf die Weiterleitung beziehen und nicht mit anderen Zustimmungen kombiniert werden darf.**[<=]**

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

A_20721 - Weiterleiten von Daten an Krankenkassen erst nach Einwilligung
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass Daten, die aus der ePA ins FdV geladen werden, nur an von Krankenkassen angebotene Anwendungen weitergeleitet werden, falls der Versicherte zuvor gegenüber der Krankenkasse in die Verarbeitung dieser Daten eingewilligt hat.**[<=]**

Hinweis: Die A_20721 setzt die Forderung des § 345 Abs. 1 SGB V um. Die Einwilligung gegenüber der Krankenkasse kann elektronisch erfolgen. Dies betrifft insbesondere auch die Übermittlung des Nachweises, mit dem die Krankenkasse die Einwilligung des Versicherten in die Verarbeitung der Daten nachweisen kann (vgl. Art. 7 Abs. 1 DSGVO).

A_16440 - ePA-Frontend des Versicherten: Weiterleiten von Daten - Information
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass der Versicherte vor der Zustimmung zur Nutzung von aus der ePA ins FdV geladenen Daten durch Anwendungen oder Apps im oder außerhalb des Frontends in verständlicher Weise darüber informiert wird, welche Daten, wann und an wen weitergeleitet werden und zu welchem Zwecke die Anwendungen die Daten verarbeiten.**[<=]**

A_16441 - ePA-Frontend des Versicherten: Weiterleiten von Daten - Nachvollziehbarkeit
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass der Versicherte eine Weiterleitung der Daten im Nachhinein nachvollziehen kann (z.B. durch Protokollierung).**[<=]**

A_19110 - ePA-Frontend des Versicherten: – Unterbindung bei einer erheblichen Störung
Der Hersteller des ePA-Frontend des Versicherten MUSS bei Bekanntwerden einer erheblichen Störung (gemäß §291b Abs.6 S.3 SGB V) in einer Version des ePA-Frontend des Versicherten die Nutzung dieser Version unverzüglich unterbinden.
[<=]

5.1.1 Anforderungen zum Herstellungsprozess

A_19143 - ePA-Frontend des Versicherten: Mitwirkungspflicht bei der CC-Zertifizierung
Falls der Hersteller des ePA-Frontend des Versicherten entscheidet, eine CC-Zertifizierung statt eines Produktgutachtens durchzuführen, MUSS der Hersteller des ePA-Frontend des Versicherten bei der Einreichung eines CC-Zertifizierungsantrags sein Security Target Dokument der gematik zur Verfügung stellen.**[<=]**

ENTWURF

A_19144 - ePA-Frontend des Versicherten: Dokumentationspflicht bei der CC-Zertifizierung
Falls der Hersteller des ePA-Frontend des Versicherten entscheidet, eine CC-Zertifizierung statt eines Produktgutachtens durchzuführen, MUSS der Hersteller des ePA-Frontend des Versicherten

- die zusätzlichen Funktionen des ePA-Frontend des Versicherten,
- die in den zusätzlichen Funktionen verarbeiteten Daten,
- die Schnittstellen zwischen dem ePA-Frontend des Versicherten und den ggf. genutzten Backend-Diensten der zusätzlichen Funktionen inklusive ihrer Sicherheitsmaßnahmen und
- die Sicherheitsannahmen an das ePA-Frontend des Versicherten und die Ausführungsumgebung

im Security Target beschreiben.
[<=**]**

A_18208-01 - ePA-Frontend des Versicherten: Sicherheits- und Datenschutzkonzept
Der Hersteller des ePA-Frontend des Versicherten MUSS die Sicherheits- und Datenschutzmaßnahmen für sein Produkt in einem Sicherheits- und Datenschutzkonzept dokumentieren und auf Verlangen der gematik zur Verfügung stellen.**[**<=**]**

Hinweis: Das Sicherheitskonzept soll zwingend die folgenden Punkte umfassen:

- Beschreibung des ePA-Frontends des Versicherten und Einbindung zusätzlicher Funktionalitäten vom Hersteller bzgl. allgemeiner Informationssicherheitsaspekte und Sicherheitsanforderungen der gematik,
- Schutzbedarfsfeststellung,
- Bedrohungsanalyse,
- Sicherheitsanalyse (Verifikation der Wirksamkeit der Sicherheitsmaßnahmen),
- Erstellung einer Restrisikoabschätzung.

Hinweis: Das Datenschutzkonzept soll zwingend die folgenden Punkte umfassen:

- Beschreibung des ePA-Frontends des Versicherten (inklusiv zusätzliche Funktionalität vom Hersteller) bzgl. Datenschutzaspekte
- Identifikation der Randbedingungen des Datenschutzes
- Identifikation der personenbezogenen Daten und Anwendungsprozesse
- Umsetzung der Grundsätze für die Verarbeitung personenbezogener Daten - Datenschutz-Risiken und Datenschutz-Hinweise

A_18209 - ePA-Frontend des Versicherten: Sicherheitstestplan
Der Hersteller des ePA-Frontend des Versicherten MUSS einen Testplan für Sicherheitstests erstellen und auf Verlangen der gematik zur Verfügung stellen.**[**<=**]**

Hinweis: Der Testplan umfasst alle Sicherheitstests während den Phasen der Produktentwicklung sowie regelmäßige Sicherheitsprüfungen (Pentest) durch unabhängige Sicherheitsexperten. Der Umfang des Testplans hängt von der Zielplattform
sowie den Funktionalitäten des ePA-Frontends des Versicherten ab und muss zwingend das Testvorgehen zu den Sicherheitsvorgaben der gematik beinhalten.

ENTWURF

Orientierungen zu den Inhalten eines Testplanes sind im OWASP Mobile Security Testing Guide [MSTG] und im OWASP Mobile Application Security Verification Standard [MASVS] beschrieben. Der Testplan muss einen ähnlichen Detaillierungsgrad haben, wie in den beiden OWASP-Referenzen.

A_18210 - ePA-Frontend des Versicherten: Umsetzung Sicherheitstestplan
Der Hersteller des ePA-Frontends des Versicherten MUSS seinen Testplan für Sicherheitstests umsetzen und der gematik bei jeder Veröffentlichung einer neuen Produktversion einen Testbericht zur Verfügung stellen.**[<=]**

Hinweis: Der Testbericht muss zwingend Testauswertungen zu den Sicherheitsvorgaben der gematik beinhalten.

A_15262 - ePA-Frontend des Versicherten: Implementierungsspezifische Sicherheitsanforderungen
Der Hersteller des ePA-Frontends des Versicherten MUSS während der Entwicklung des Produktes implementierungsspezifische Sicherheitsanforderungen dokumentieren und umsetzen.**[<=]**

A_15263 - ePA-Frontend des Versicherten: Verwendung eines sicheren Produktlebenszyklus
Der Hersteller des ePA-Frontends des Versicherten MUSS innerhalb des Produktlebenszyklus (Entwicklung, Betrieb, Außerbetriebnahme) seines Produktes Sicherheitsaktivitäten integrieren und anwenden, d. h. in einschlägigen Fachkreisen anerkannte, erprobte und bewährte Regeln anwenden.**[<=]**

Ein Beispiel für Sicherheitsaktivitäten in einem Produktlebenszyklus ist der Microsoft Security Development Lifecycle. Für weitere Informationen siehe [OWASP SAMM Project] oder den durch das BSI bereitgestellte "Leitfaden zur Entwicklung sicherer Webanwendungen - Empfehlungen und Anforderungen an die Auftragnehmer" (insbesondere Kapitel 4). Als ein Hilfsmittel bietet die gematik eine informative SDL Orientierungshilfe an, die Hersteller sowie Sicherheitsgutachter unterstützt, um einen SDL zu etablieren oder zu Prüfen.

A_15443 - ePA-Frontend des Versicherten: Sicherheitsrelevante Softwarearchitektur-Review
Der Hersteller des ePA-Frontends des Versicherten MUSS einen sicherheitsrelevanten Softwarearchitektur-Review durchführen und identifizierte Architekturschwachstellen beheben.**[<=]**

A_15264-01 - ePA-Frontend des Versicherten: Durchführung einer Bedrohungsanalyse
Der Hersteller des ePA-Frontend des Versicherten MUSS eine Bedrohungsanalyse durchführen und Maßnahmen gegen die identifizierten Bedrohungen implementieren.**[<=]**

A_15265-01 - ePA-Frontend des Versicherten: Durchführung sicherheitsrelevanter Quellcode Review
Der Hersteller des ePA-Frontend des Versicherten MUSS während der Entwicklung des Produktes sicherheitsrelevante Quellcode-Reviews oder automatisierte sicherheitsrelevante Quellcode-Scans durchführen.**[<=]**

A_15266-01 - ePA-Frontend des Versicherten: Durchführung Sicherheitstests
Der Hersteller des ePA-Frontend des Versicherten MUSS während der Entwicklung des Produktes automatisierte Sicherheitstests durchführen.**[<=]**

ENTWURF

A_18193 - ePA-Frontend des Versicherten: Dokumentierter Plan zur Sicherheitsschulung für Entwickler
Der Hersteller des ePA-Frontend des Versicherten MUSS einen Schulungsplan zur regelmäßigen Schulung von Entwicklern in sicherer Entwicklung und Secure-Coding-Techniken dokumentieren und umsetzen.**[<=]**

A_15267-01 - ePA-Frontend des Versicherten: Sicherheitsschulung für Entwickler
Der Hersteller des ePA-Frontend des Versicherten MUSS alle Entwickler des Produktes in sicherer Entwicklung und Secure Coding Techniken schulen.**[<=]**

A_18191 - ePA-Frontend des Versicherten: Dokumentation des sicheren Produktlebenszyklus
Der Hersteller des ePA-Frontend des Versicherten MUSS den verwendeten sicheren Produktlebenszyklus und deren Teilprozesse dokumentieren und auf Nachfrage der gematik zur Verfügung stellen. Die Dokumentation soll mindestens die folgenden Sicherheitsaktivitäten beschreiben:

- Erfassen und Umsetzen von implementierungsspezifischen Sicherheitsanforderungen für das FdV und von Best Practice Sicherheitsanforderungen,
- Durchführen von sicherheitsrelevanten Architektur- und Design-Reviews,
- Durchführen von Bedrohungsanalyse,
- Durchführen von sicherheitsrelevanten Quellcode-Reviews,
- Durchführen von Sicherheitstests während der Qualitätssicherungsphase,
- Etablieren von Quality Gates, die eine Veröffentlichung des FdV mit 'Mittel' oder 'Hoch' bewerteten Sicherheitsfehlern verhindert,
- Änderungs- und Konfigurationsmanagement.
- Schwachstellen-Management.

[<=]

A_18192-02 - ePA-Frontend des Versicherten: Änderungs- und Konfigurationsmanagementprozess
Der Hersteller des ePA-Frontend des Versicherten MUSS während der Entwicklung des Produktes einen Änderungs- und Konfigurationsmanagementprozess verwenden. Das Änderungsmanagement umfasst mindestens den Entscheidungsprozess über vorgeschlagene Änderungen und die Autorisierung der Änderungen. Das Konfigurationsmanagement liefert mindestens zu jedem Zeitpunkt die eindeutige Zusammensetzung des Produktes bezüglich seiner eindeutigen Komponenten (Dritt-Software wie Bibliotheken und Frameworks) und den vorgenommenen Änderungen an eigenen Komponenten.**[<=]**

A_18253 - ePA-Frontend des Versicherten: Verifizierung der Einhaltung sicherheitstechnische Eignung durch Datenschutzbeauftragten
Der Hersteller des ePA-Frontends des Versicherten MUSS bei Veröffentlichung einer neuen Produktversion des Produktes die Einhaltung der Herstellererklärung sicherheitstechnische Eignung durch seinen Datenschutzbeauftragten verifizieren.**[<=]**

Falls es keinen Datenschutzbeauftragten bei dem Hersteller gibt, kann eine alternative Rolle die sicherheitstechnische Eignung verifizieren z.B. der Sicherheitsbeauftragte. Diese Rolle darf nicht in der Entwicklung des Produktes teilnehmen und muss direkt an die Geschäftsführung des Herstellers berichten.

ENTWURF

A_18194 - ePA-Frontend des Versicherten: Informationspflicht bei Veröffentlichung neue Produktversion
Der Hersteller des ePA-Frontend des Versicherten MUSS die gematik bei Veröffentlichung einer neuen Produktversion informieren und eine Erklärung sicherheitstechnische Eignung liefern.**[<=]**

5.1.2 Unterstützung von Audits

Die gematik kann für die Überprüfung der Umsetzung der Anforderungen zur sicherheitstechnischen Eignung Audits beim ePA- FdV durchführen. Für die Hersteller gelten Mitwirkungspflichten.

A_18254-01 - ePA-Frontend des Versicherten: Rechte der gematik zur sicherheitstechnischen Prüfung des Produktes
Der Hersteller des ePA-Frontends des Versicherten MUSS zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt sind,

- Sicherheitsprüfungen (z.B. Whitebox oder Blackbox Pentest) seines Produktes durchzuführen (Hiervon unbenommen ist das Recht der gematik, anlasslose Sicherheitsprüfung durchzuführen.),
- im Rahmen einer Sicherheitsprüfung die konkrete Umsetzung der an das Produkt gestellten Anforderungen zu überprüfen.

Der Hersteller muss dies im gleichen Maße für Unterauftragnehmer zusichern. Die Kosten, die dem Hersteller durch diese Mitwirkungspflichten entstehen, trägt der Hersteller selbst.
[<=]

A_18211-01 - ePA-Frontend des Versicherten: Mitwirkungspflicht bei Sicherheitsprüfung
Der Hersteller des ePA-Frontends des Versicherten MUSS Sicherheitsprüfungen (z.B. Pentest) der gematik unterstützen.**[<=]**

Hinweis: Unterstützen bedeutet beispielsweise das Bereitstellen einer Release oder Beta-Version des Produkts, das Bereitstellen eines Testsystems inkl. Test Accounts, kleine Anpassungen des Produktes, die ein Beschleunigung des Tests ermöglichen (z.B. Entfernung von Certificate Pinning, Code Obfuscation) und Unterstützung bei Rückfragen.

A_18246-01 - ePA-Frontend des Versicherten: Auditrechte der gematik zur Prüfung des Sicherheitsgutachtens
Der Hersteller des ePA-Frontends des Versicherten MUSS zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt sind,

- Audits durchzuführen (Hiervon unbenommen ist das Recht der gematik, anlasslose Audits durchzuführen.),
- im Rahmen eines Audits beim Hersteller die konkrete Umsetzung der an den Hersteller gestellten Anforderungen zu überprüfen,
- im Rahmen eines Audits während der üblichen Geschäftszeiten die Geschäftsräume des Herstellers zu betreten,
- im Rahmen eines Audits alle für das Audit benötigten Informationen zur Verfügung gestellt zu bekommen und insbesondere die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte zu erhalten.

ENTWURF

Der Hersteller muss dies im gleichen Maße für Unterauftragnehmer zusichern. Die Kosten, die dem Hersteller durch diese Mitwirkungspflichten entstehen, trägt der Hersteller selbst.**[<=]**

5.2 Verwendete Standards

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

A_15268-01 - ePA-Frontend des Versicherten: Konformität zu WS-I Basic Profil 2.0
Das ePA-Frontend des Versicherten MUSS SOAP-Nachrichten gemäß den Vorgaben aus WS-I Basic Profile V2.0 [WSIBP] unterstützen.**[<=]**

A_15269-01 - ePA-Frontend des Versicherten: Verwendung von WS-Trust 1.4
Das ePA-Frontend des Versicherten MUSS für die Authentisierung den Standard [WS-Trust1.4] unterstützen.**[<=]**

A_15270-01 - ePA-Frontend des Versicherten: Verwendung von DMSLv2
Das ePA-Frontend des Versicherten MUSS für die Abfrage des Verzeichnisdienstes die Standard Directory Services Markup Language v2.0 (DSMLv2) unterstützen.**[<=]**

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

5.3 Integrating the Healthcare Enterprise IHE

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

Das ePA-Frontend des Versicherten nutzt die folgenden Integrationsprofile des IHE ITI TF:

- Cross-Enterprise Document Sharing (XDS.b) Profile
- Remove Metadata and Documents (RMD) Profile
- Cross-Enterprise User Assertion (XUA) Profile
- Advanced Patient Privacy Consents (APPC) Profile

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

Tabelle 4: TAB_FdV_103 – IHE Akteure und Transaktionen

Aktion	Profile	IHE-Akteur	Transaktion	Referenz

ENTWURF

Suchanfrage auf Metadaten	XDS.b	Document Consumer	Registry Stored Query [ITI-18]	[IHE-ITI-TF2a]#3.18
Herunterladen von Dokumenten	XDS.b	Document Consumer	Retrieve Document Set [ITI-43]	[IHE-ITI-TF2b]#3.43
Einstellen von Dokumenten	XDS.b	Document Source	Provide & Register Document Set-b [ITI-41]	[IHE-ITI-TF2b]#3.41
Löschen von Dokumenten	RMD	Document Administrator	Remove Metadata [ITI-62]	[IHE-ITI-RMD]#3.62
AuthenticationAssertion übertragen	XUA	X-Service User	Provide X-User Assertion [ITI-40]	[IHE-ITI-TF2b]#3.40
Policy Document erstellen	APPC	APPC Content Creator	-	[IHE-ITI-APPC]
Interpretieren von Policy Documents	APPC	APPC Content Consumer	-	[IHE-ITI-APPC]

XDS-Option „Document Replacement" - Ersetzen eines existierenden Dokuments

Ein eingestelltes Dokument kann auch ein existierendes Dokument ersetzen. Dies erfolgt durch Verwendung der „Document Replacement"-Option (XDS.b Document Source). Dazu wird das gleiche Dokument (mit geändertem Inhalt und nebst ggf. geänderten DocumentEntry-Metadaten) erneut hochgeladen. Das neue Dokument erhält den Status „Approved". Das alte Dokument geht in den Status „Deprecated". Beide Dokumente werden über eine „Replace"-Association miteinander verbunden, sodass nach dem Einstellen erkennbar ist, dass das neue Dokument das alte ersetzt. Lädt man erneut eine neue Fassung hoch, erhält man zwei Dokumente im Status "Deprecated" und das neueste im Status "Approved".
Alle alten Dokumente (Status "Deprecated") können nach wie vor gefunden und heruntergeladen werden. Einige Suchen erlauben das Filtern nach Status bzw. zeigen per Default auch nur Dokumente im Status „Approved" an.

Eingestellt (im "Submission Set") wird zum einen das neue Dokument inkl. Metadaten und zum anderen eine Association vom Typ urn:ihe:iti:2007:AssociationType:RPLC, die auf das neue Dokument und das zu ersetzende, bestehende Dokument verweist und so die "Replace"-Beziehung herstellt.

XDS-Option „Document Addendum" - Verlinken von Dokumenten

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

ENTWURF

In ePA 2.0 ist die Nutzung von „Append"-Associations nicht erlaubt.

XDS-Option "Folder Management" - Verwendung von Ordnern

Ordner können durch die Option "Folder Management" (XDS.b Document Source) verwendet werden. Bei der mittelgranularen Berechtigungsverwaltung werden für die Dokumentenkategorie 1a* und die Kategorie eGA vom Aktensystem definierte Ordner genutzt. Für sogenannte Dokumentensammlungen vom Typ "mixed" (z. B. Kinderuntersuchungsheft und Mutterpass) werden Ordner durch das Frontend selbst angelegt. Durch die Assoziation eines Dokumentes zu einem dieser Ordner wird das Dokument dem Ordner der entsprechenden Dokumentenkategorie bzw. Dokumentensammlung zugeordnet. Die XDS-Option "Folder Management" ist nur für den geschilderten Verwendungszweck zugelassen; ein selbständiges Anlegen, Löschen oder Bearbeiten von Ordnern und ihrer Metadaten ist nicht möglich. Das Entfernen von Dokumenten aus einem Ordner durch Löschen der entsprechenden Assoziation ist jedoch vorgesehen.

Weitere Festlegungen

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

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

Im ePA-Frontend des Versicherten werden fachliche Dokumente (Versichertendokumente) und technische Dokumente (Policy Documents) unterschieden.

5.3.1 Policy Documents

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

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

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

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

ENTWURF

Das ePA-Frontend des Versicherten verarbeitet Policy Documents nur intern.

A_15271-02 - ePA-Frontend des Versicherten: Keine Anzeige von Policy Documents
Das ePA-Frontend des Versicherten DARF Policy Documents an der Schnittstelle zum FdV NICHT herausgeben.**[<=]**

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

A_15673-02 - ePA-Frontend des Versicherten: Policy Document für LEI erstellen
Das ePA-Frontend des Versicherten MUSS für zu berechtigende LEIs ein XACML 2.0 Policy Set als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in [gemSpec_Dokumentenverwaltung#9.3] erstellen. **[<=]**

Das Attribut der Base Policy mit der Attribut-ID "`urn:oasis:names:tc:xspa:1.0:subject:organization`" beinhaltet den Namen der LEI, welcher für die Anzeige der Berechtigung genutzt wird.

Das Attribut der Base Policy mit der Attribut-ID "`urn:gematik:subject:organization-id`" beinhaltet die Telematik-ID der LEI.

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

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

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

Das Attribut EnvironmentMatch/MatchID "`urn:oasis:names:tc:xacml:1.0:function:date-greater-than`" beinhaltet das Erstellungsdatum der Berechtigung. Das Erstellungsdatum entspricht bei der Neuerstellung eines Policy Documents dem aktuellen Datum.

Über `Policy`- und `PolicySetIdReference`-Einträge wird gesteuert, welche Zugriffsrechte der LEI eingeräumt werden, Details dazu finden sich in der entsprechenden Policy in [gemSpec_Dokumentenverwaltung#9.3].

A_15674-01 - ePA-Frontend des Versicherten: Policy Document für Vertreter erstellen
Das ePA-Frontend des Versicherten MUSS für zu berechtigende Vertreter ein XACML 2.0 Policy Set als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in [gemSpec_Dokumentenverwaltung#9.2] erstellen (Policy Set "`urn:gematik:policy-set-id:permissions-access-group-representative:base`").**[<=]**

Das Attribut der Policy mit der Attribut-ID "`urn:oasis:names:tc:xacml:1.0:subject:subject`" beinhaltet den Namen des Vertreters, welcher für die Anzeige der Berechtigung genutzt wird.

ENTWURF

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

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

A_17232-01 - ePA-Frontend des Versicherten: Policy Document für Kostenträger erstellen

Das ePA-Frontend des Versicherten MUSS für einen zu berechtigenden Kostenträger ein XACML 2.0 Policy Set als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in [gemSpec_Dokumentenverwaltung#9.4] erstellen (Policy Set "urn:gematik:policy-set-id:permissions-access-group-ktr:base"). **[<=]**

Das Attribut der Base Policy mit der Attribut-ID "urn:oasis:names:tc:xspa:1.0:subject:organization" beinhaltet den Namen des KTR, welcher für die Anzeige der Berechtigung genutzt wird.

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

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

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

Die Unterscheidung bei der Verarbeitung im FdV, ob es sich bei einer Base Policy um ein Policy Document für eine LEI, einen Vertreter oder einen Kostenträger handelt, erfolgt am einfachsten anhand der übergeordneten Id (PolicySetId bzw. PolicySetId).

5.3.2 Versichertendokumente

A_19830-01 - ePA-Frontend des Versicherten: Dokumente durch den Versicherten hochladen

Das ePA-Frontend des Versicherten MUSS für alle Dokumente, die der Versicherte in seine ePA einfügt, im submissionset.authorRole den Wert "102" setzen. **[<=]**

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

Für die XDS-Metadaten von Dokumenten des Versicherten gelten die Nutzungsvorgaben aus [gemSpec_DM_ePA#A_14760].

5.4 Benutzeroberfläche

Die Benutzeroberfläche, welche durch den Versicherten genutzt wird, um ePA-Anwendungsfälle auszuführen, ist Teil des FdV.

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

ENTWURF

5.4.1 Visuelle Darstellung

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

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

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

A_20968 - Unterstützung der ePA-Anwendungsfälle im Hintergrundmodus
Das ePA-Frontend des Versicherten MUSS den Hintergrundmodus unterstützen. [<=]

Wenn der Nutzer eine Aktion, wie etwa die Umschlüsselung, angestoßen hat, dann muss das FdV diese im Hintergrund weiterführen können.

A_20969 - Notwendige Permissions für den Hintergrundmodus
Das ePA-Frontend des Versicherten MUSS die notwendigen Permissions besitzen, die für eine fehlerfreie Funktion im Hintergrundmodus notwendig sind.[<=]

Sofern der Benutzer diese Permissions nicht schon bei der Installation freigegeben hat, ist die Freigabe beim Beginn längerer Aktionen einzuholen und zu aktivieren. Insbesondere ist dies bei der Umschlüsselung zu beachten, da sie länger dauern kann.

A_20970 - Hinweis zur Arbeitsweise im Hintergrundmodus
Das ePA-Frontend des Versicherten MUSS den Nutzer vor dem Beginn längerer Aktionen darauf hinweisen, dass die Aktion im Hintergrund weiter läuft und die Anwendung während dieser Zeit nicht beendet oder deinstalliert und dass das Gerät während dieser Zeit nicht ausgeschaltet oder rebootet werden darf.[<=]

5.4.2 Benutzerführung

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

DIN Normen und Verordnungen zur Beachtung:

Eine hohe Akzeptanz der Benutzerfreundlichkeit oder Usability wird durch eine einfache, selbsterklärende Bedienung der Oberfläche erreicht, die sich an gängigen Mustern des App-Designs orientiert.

Hierfür ist es auch erforderlich, die Erwartungshaltung der Zielgruppe zu kennen und zu berücksichtigen (z.B. auch Menschen mit körperlichen oder geistigen Einschränkungen).

Die Akzeptanz des Frontends für den Versicherten hängt in großem Maße von folgenden Faktoren ab:

- Anwendbarkeit auf verschiedenen Bildschirmgrößen und Auflösungen
- Intuitive und unkomplizierte Handhabung
- Anwendbarkeit auch im Offline-Modus
- Zielgruppenorientierung
- Leichte und verständliche Bereitstellung von Informationen
- Einhaltung ergonomischer Aspekte (z.B. kurze Touchwege)

ENTWURF

- Konsistente Gestaltung der Links, Buttons, etc.

5.4.2.1 Technische Normen und Verordnungen zur Beachtung

Die Entwicklung einer barrierearmen Anwendung unterliegt einem sich fortlaufend weiterentwickelnden Prozess. Die Umsetzung aller Anforderungen kann nicht mit der Ersteinführung der Anwendung sichergestellt werden.

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

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

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

- Teil 8: Anforderungen an Farbdarstellungen
- Teil 9: Anforderungen an Eingabegeräte – außer Tastaturen
- Teil 110: Grundsätze der Dialoggestaltung (ersetzt den bisherigen Teil 10)
- Teil 11: Anforderungen an die Gebrauchstauglichkeit – Leitsätze
- Teil 12: Informationsdarstellung
- Teil 13: Benutzerführung
- Teil 14: Dialogführung mittels Menüs
- Teil 15: Dialogführung mittels Kommandosprachen
- Teil 16: Dialogführung mittels direkter Manipulation
- Teil 17: Dialogführung mittels Bildschirmformularen
- Teil 171: Leitlinien für die Zugänglichkeit von Software BITV 2.0

Für die Entwicklung eines barrierefreien Frontend des Versicherten ist insbesondere die Verordnung zur barrierefreien Gestaltung von Informationstechnik zu beachten.

BITV 2.0 - Barrierefreie Informationstechnik-Verordnung

Hinweis: Die Versionsnummern der aufgeführten Normen und Richtlinien spiegeln den Stand zum Zeitpunkt der Erstellung dieses Dokumentes wider.

Die seit 2018 bestehende umfassende Forderung nach Umsetzung von Barrierefreiheit in der Informationstechnik erwächst aus der EU Richtlinie 2016/2102 zur „Barrierefreiheit von Webseiten und mobiler Anwendungen öffentlicher Stellen". Diese Richtlinie musste im Jahr 2018 in Bundes- und Landesrecht übertragen werden. – Diese Gesetze verweisen jeweils auf die Barrierefreie Informationstechnik-Verordnung mit Ausgabe vom 21. Mai 2019 (BITV 2.0).

Zur Erfüllung der BITV 2.0 § 3 Abs. 2 ist die durch die Veröffentlichung im europäischen Amtsblatt harmonisierte EN 301549 „Barrierefreiheitsanforderungen für IKT-Produkte und -Dienstleistungen" (V 2.1.2 von 2018-08) anzuwenden. Diese liegt in der Fassung von 2020-02 als DIN EN 301549 als deutsche Übersetzung vor. Die DIN EN 301549 ist

ENTWURF

eine Beschaffungsnorm. Die darin aufgeführten und für den Anwendungsfall des FdV des E-Rezepts anzuwendenden Erfolgskriterien sind in Kapitel 9 (Web mit 50 Erfolgskriterien), Kapitel 10 (Dokumente mit 46 Erfolgskriterien) und Kapitel 11 (Nicht webbasierte Software mit 44 Erfolgskriterien) aufgeführt. Sie entsprechen den Erfolgskriterien von Level AA der 2.1. WCAG 2.1 (Web Content Accessibility Guidelines).

Der sachliche Geltungsbereich der BITV 2.0 umfasst folgende relevanten Anwendungsbereiche für diese Spezifikation:

- Webseiten,
- nicht webbasierte Software mit mobilen Anwendungen.

Folgende Gestaltungsmerkmale der Anwendungen stellen die Barrierefreiheit sicher:

- wahrnehmbar,
- bedienbar,
- verständlich und
- robust.

In den genannten Normen und Standards werden nebeneinander die Belange von in der Handmotorik eingeschränkter, blinder, sehbehinderter, gehörloser, schwerhöriger, geistig und lernbehinderter Menschen berücksichtigt.

Nach BITV 2.0 müssen Dokumente, die über dem FdV angezeigt werden, die gleichen Anforderungen an die Barrierefreiheit erfüllen, wie sie an die Anwendung gestellt werden. Sämtliche bereitgestellten Dokumente müssen als barrierefreie Formate angeboten werden, die mit dem Screenreader lesbar und navigierbar sind. Hierbei müssen die behinderungsspezifischen Standardsoftwares zur Herstellung von Zugänglichkeit berücksichtigt werden.

Allgemeine Anforderungen an die Benutzerfreundlichkeit

A_20092 - ePA-Frontend des Versicherten: Intuitive Bedienung
Die Bedienung des ePA-Frontend des Versicherten SOLL für den Nutzer intuitiv gestaltet werden.**[<=]**

A_20094 - ePA Frontend des Versicherten: Bereitstellung Sprachen
Das ePA-Frontend des Versicherten SOLL dem Nutzer alle anzeigbaren Texte in der Sprache Deutsch bereitstellen.**[<=]**

Zusätzliche Sprachen können unterstützt werden.

A_20095 - ePA-Frontend des Versicherten: Abbruch Anwendungsfälle
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Anwendungsfälle auch vor dem Ende der Verarbeitung jederzeit abzubrechen.**[<=]**

A_20096 - ePA-Frontend des Versicherten: Arten der Verwaltung
Das ePA-Frontend des Versicherten SOLL dem Nutzer anzeigen, welche Arten von Dokumentenzugriffen und Verwaltungsfunktionen ausgeführt werden können.**[<=]**

A_20097 - ePA-Frontend des Versicherten: Bezeichnung der Anwendungsfälle
Das ePA-Frontend des Versicherten MUSS für die Inhalte und Anwendungsfälle eindeutige und verständliche Bezeichnungen verwenden.**[<=]**

Bezeichnungen sollen nach Möglichkeit vollständig ausgeschrieben sein, Abkürzungen sind zu vermeiden.

ENTWURF

A_20098 - ePA-Frontend des Versicherten: Navigierbarkeit bereitgestellter Inhalte
Das ePA-Frontend des Versicherten SOLL sicherstellen, dass bereitgestellte Inhalte maschinenlesbar und navigierbar sind, um dem Nutzer eine barrierefreie Bedienung zu ermöglichen.**[<=]**

A_20099 - ePA-Frontend des Versicherten: Nutzung Gerätefunktionalitäten
Das ePA-Frontend des Versicherten SOLL gerätespezifische Funktionalitäten (z.B. Lagebestimmung, Kamerafunktion, Multi-Touch-Gesten) sinnvoll nutzen und unterstützen.**[<=]**

A_20100 - ePA-Frontend des Versicherten: Nutzung Schnittstellen Bedienungsmöglichkeiten des Betriebssystems
Das ePA-Frontend des Versicherten SOLL die Schnittstellen für die Unterstützung der barrierefreien Bedienungsmöglichkeit, welche vom Betriebssystem zur Verfügung gestellt werden, nutzen.**[<=]**

A_20101 - ePA-Frontend des Versicherten: Nutzung Bedienhilfen des Betriebssystems
Das ePA-Frontend des Versicherten SOLL die Bedienhilfen der verwendeten Betriebssysteme zur barrierefreien Nutzung verwenden.**[<=]**

A_20102 - ePA-Frontend des Versicherten: Kontrastverhältnis
Das ePA-Frontend des Versicherten SOLL für das GUI ein Kontrastverhältnis verwenden, welches unter verschiedenen Bedingungen eine optimale Ablesbarkeit gewährleistet.**[<=]**

A_20103 - ePA-Frontend des Versicherten: Hinweise
Das ePA-Frontend des Versicherten SOLL dem Nutzer Hinweise anzeigen, die den Zweck sowie den inhaltlichen Ablauf eines Anwendungsfalls betreffen, um dem Nutzer die Bedienung zu vereinfachen.**[<=]**

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

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

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

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

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

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

5.4.3 Anzeige von Dokumenten

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

ENTWURF

A_18257 - ePA-Frontend des Versicherten: Dokumentengrösse an Aussenschnittstellen
Das ePA-Frontend des Versicherten MUSS für alle Außenschnittstellen, welche für Dokumente in ePA-Anwendungsfälle genutzt werden, Dokumente mit einer Größe von mindestens 25 MB unterstützen.**[<=]**

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

A_17226 - ePA-Frontend des Versicherten: Anzeige Metadaten von Dokumenten
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die zu einem Dokument zugehörigen Metadaten mit fachlichen Informationen einzusehen.**[<=]**

Technische Metadaten zu einem Dokument müssen nicht angezeigt werden.

A_15284 - ePA-Frontend des Versicherten: Anzeige von Dokumenten
Das ePA-Frontend des Versicherten SOLL Standardprogramme zur Anzeige von aus der ePA heruntergeladenen Dokumenten verwenden.**[<=]**

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

A_15285 - ePA-Frontend des Versicherten: Anzeige strukturierter Dokumente
Das ePA-Frontend des Versicherten MUSS für strukturierte Dokumente eine für den Nutzer lesbare Darstellung mit dem vollständigen Inhalt des Dokumentes generieren und dem Nutzer anzeigen können.**[<=]**

Für Informationen zu strukturierten Dokumenten siehe [A_14761-01].

Wenn ein Arztbrief Dokument mit xml und pdf Anteil vorliegt, muss nur das PDF angezeigt werden.

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

5.4.4 Sammlungen

Als Sammlung gemäß [gemSpec_DM_ePA#2.1.4.4.1] wird eine Zusammenstellung von Dokumenten verstanden, die in ihrer Gesamtheit betrachtet, berechtigt oder anderweitig besonders behandelt werden müssen. Zum Beispiel werden einzelne Einträge im Impfpass als separate Dokumente in ePA abgelegt. Als Sammlung "Impfpass" unterliegen sie jedoch bestimmten Verarbeitungsregeln. Beispiele für andere Sammlungen sind der Mutterpass oder das Kinderuntersuchungsheft. Je nach Verarbeitungsvorgaben für einzelne Sammlungen werden drei Sammlungstypen ("mixed", "uniform" und "atomic") eingeführt. Bestehende strukturierte Dokumente werden einem dieser Typen zugeordnet, weitere strukturierte Dokumente und ihre Sammlungstypen können konfiguriert werden. Weitere Details finden sich in [gemSpec_DM_ePA#2.1.4.4.1].

Für das Erteilen einer Berechtigung für eine LEI auf einen Pass gilt das analog, d.h., das ePA-Frontend des Versicherten muss die Erteilung einer Berechtigung zum Zugriff auf einen Pass in seiner Gesamtheit durch eine LEI unterstützen. Dies wird in Anforderung A_19686 geregelt.

ENTWURF

A_19897-01 - ePA-Frontend des Versicherten: Anzeige von Sammlungsinstanzen vom Typ "mixed" und "uniform"
Das ePA-Frontend des Versicherten MUSS für eine für den Nutzer lesbare Darstellung mit dem vollständigen Inhalt aller zur Sammlungsinstanz gehörenden Dokumente generieren und dem Nutzer anzeigen können.**[<=]**

A_19898-01 - ePA-Frontend des Versicherten: Sammlungsinstanzen drucken oder speichern
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine Sammlungsinstanz lokal zu drucken oder zu speichern.**[<=]**

Das lokale Speichern kann im PDF-Format angeboten werden.

A_19961-01 - ePA-Frontend des Versicherten: Löschen einer Sammlungsinstanz
Das ePA-Frontend des Versicherten MUSS einen Nutzer beim Löschen einer Sammlungsinstanz, insbesondere dem gesamtheitlichen Löschen bei Instanzen des Typs "mixed" und "uniform", unterstützen.**[<=]**

Das Löschen einer Sammlungsinstanz umfasst das Löschen aller zur Instanz gehörenden Dokumente.

A_20774 - ePA-Frontend des Versicherten: Berechtigung von Sammlungsinstanzen vom Typ "mixed" und "uniform"
Das ePA-Frontend des Versicherten MUSS eine Berechtigung für alle zu einer Sammlungsinstanz gehörenden Dokumente unterstützen.
[<=]

5.4.5 Eingabe Metadaten für einzustellende Dokumente

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

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

Tabelle 5: TAB_FdV_125 – Metadatenattribute

Metadatenattribut XDS.b	Dokument einstellen: Anzeige	Dokument einstellen: Defaultwert	Dokument einstellen: Änderbar	Bemerkung
Metadatenelement Document Entry				
author				

ENTWURF

	authorPerson	ja	leer	ja	
	authorInstitution	ja	leer	ja	
	authorRole	ja	leer	ja	value set authorRole
	authorSpecialty	ja	leer	ja	
	authorTelecommunication	ja	leer	ja	
availabilityStatus		nein			nicht genutzt
classCode		ja	"DOK" (Dokumente ohne besondere Form (Notizen))	ja	value set classCode
comments		ja	leer	ja	
confidentialityCode		ja		ja	Es MUSS einer der Codes • "N" (für Dokumente mit gewünschter Vertraulichkeitsstufe "normal"), • "R" (für Vertraulichkeitsstufe "vertraulich") oder • "V" (für Vertraulichkeitsstufe "streng vertraulich")

ENTWURF

				aus dem Code System 2.16.840.1.113883.5.25 (siehe auch [IHE-ITI-VS]) gesetzt werden.
creationTime	ja	aktuelle Systemzeit	ja	darf nicht in der Zukunft liegen.
entryUUID	nein	vom ePA-Frontend des Versicherten vergeben	nein	
eventCodeList	ja	"H1" (vom Patienten mitgebracht)	ja	value set eventCodeList
formatCode	ja	"urn:ihe:iti:xds:2017:mimeTypeSufficient"	ja	aus Dokument zu bestimmen value set formatCode
hash	nein	durch ePA-Frontend des Versicherten berechnet	nein	
healthcareFacilityTypeCode	ja	'PAT' (Patient außerhalb der Betreuung)	ja	value set healthcareFacilityTypeCode
homeCommunityId	nein	aus Session-Daten	nein	
languageCode	ja	"de-DE"	ja	
legalAuthenticator	nein		nein	
limitedMetadata	nein		nein	nicht verwendet
mimeType	ja	aus Eigenschaft der Datei (bspw. Dateiendung oder	nein	

ENTWURF

		Zuordnung einer XML-Datei zu einem XML-Schema)		
objectType	nein	"urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"	nein	
patientId	nein	aus Session-Daten	nein	
practiceSettingCode	ja	"PAT" (Patient außerhalb der Betreuung)	ja	value set practiceSettingCode
referenceIdList	nein			
repositoryUniqueId	nein	entspricht homeCommunityId	nein	
serviceStartTime	ja		ja	
serviceStopTime	ja		ja	
size	nein		nein	Wird durch die Dokumentenverwaltung gesetzt.
sourcePatientId	nein			nicht verwendet
sourcePatientInfo	nein			nicht verwendet
title	ja	leer	ja	
typeCode	ja	"PATD" (Patienteneigene Dokumente)	ja	value set typeCode

ENTWURF

uniqueId	nein	vom ePA-Frontend des Versicherten vergeben	nein	
URI	ja	Dateiname	nein	
Metadatenelement Submission Set				
author				
authorPerson	nein	Vorname, Nachname und Titel aus Authentisierungszertifikat des Nutzers	nein	
authorInstitution	nein	leer	nein	
authorRole	nein	"11" (Dokumentierender)	nein	value set authorRole
authorSpecialty	nein	leer	nein	
authorTelecommunication	nein	leer	nein	
availabilityStatus	nein			nicht verwendet
comments	nein			nicht verwendet
contentTypeCode	nein	8 (Veranlassung durch Patient)	nein	value set contentTypeCode
entryUUID	nein	vom ePA-Frontend des Versicherten vergeben	nein	

ENTWURF

homeCommunityId	nein	aus Session-Daten	nein	
intendedRecipient	nein			
limitedMetadata	nein		nein	nicht verwendet
patientId	nein	aus Session-Daten	nein	
sourceId	nein		nein	
submissionTime	nein	Systemzeit des ePA-Frontend des Versicherten	nein	
title	nein			nicht verwendet
uniqueId	nein	vom ePA-Frontend des Versicherten vergeben	nein	

Für value sets siehe [gemSpec_DM_ePA].

A_15287 - ePA-Frontend des Versicherten: Eingabe Metadaten für Dokument einstellen
Das ePA-Frontend des Versicherten MUSS dem Nutzer beim Einstellen von Dokumenten Metadatenattribute anzeigen und zum Editieren anbieten.**[<=]**

Es kann auf die Anzeige einzelner nutzbarer Metadatenattribute verzichtet werden, um eine übersichtliche Darstellung beim Einstellen der Dokumente zu erreichen. Die Tabelle Tab_FdV_125 gibt hierzu eine Empfehlung.

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

A_15563 - ePA-Frontend des Versicherten: Eingabe Metadaten - Defaultwerte
Das ePA-Frontend des Versicherten MUSS Felder für die Eingabe von Metadaten gemäß Tab_FdV_125 vorbelegen.**[<=]**

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

Entsprechend den Nutzungsvorgaben für die Verwendung von XDS-Metadaten sind für einzelne Attribute Value Sets zu verwenden. Für eine bessere Bedienbarkeit bei der Eingabe der Metadaten werden die in der GUI auswählbaren Werte defaultmäßig auf

ENTWURF

einen Teil des Value Sets gemäß [gemSpec_DM_ePA#Vorschläge zur verkürzten Ansicht der Auswahl von Werten aus Value Sets] eingeschränkt. Über die Konfiguration des FdV hat der Nutzer die Möglichkeit, die anzuzeigenden Werte zu ändern, d.h. nicht angezeigte Werte aus dem Value Set hinzuzunehmen oder angezeigte Werte zu verbergen.

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

Das Setzen der Metadaten für SubmissionSet und DocumentEntry ordnet ein Dokument automatisch bestimmten Kategorien zu (z. B. Kategorie "nfd" für Notfalldaten), auf die dann später Leistungserbringer gezieht berechtigt werden können. Andere Kategorien hingegen (category_1a* und eGA) müssen ausdrücklich für ein Dokument vergeben werden. Sie ermöglichen effektivere Suchen in der Akte, erlauben aber eben auch wie die "automatischen" Kategorien das gezielte Berechtigen von Leistungserbringern.

Das Frontend kann den Nutzer auch durch eine sinnvolle Vorauswahl bei der Kategorisierung unterstützen. Die genannten Kategorien unterscheiden sich von den restlichen Kategorien dahingehend, dass das jeweilige Dokument explizit in einen Ordner gelegt werden muss, während die restlichen Kategorien automatisch über Metadaten am Dokument erkannt werden können.

A_15291 - ePA-Frontend des Versicherten: Schlüsselwerte aus Value Sets decodieren
Das ePA-Frontend des Versicherten MUSS Schlüsselwerte aus Value Sets decodieren und in einem für den Nutzer verständlichen Text anzeigen.**[<=]**

Ggf. kann dazu bei unbekannten Codes der Anzeigename eines Codes (sofern mit übertragen bzw. verfügbar) angezeigt werden.

5.4.6 Konfiguration des ePA-Frontend des Versicherten

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

A_15292-04~~A_15292-03~~ - ePA-Frontend des Versicherten: Parameter speichern und laden
Das ePA-Frontend des Versicherten MUSS die Parameter aus TAB_FdV_104 persistent speichern und bei der Initialisierung laden.

Tabelle 6: TAB_FdV_104 – Parameter FdV

Parameter	Beschreibung	Wertebereich (Default Wert)
Aktenkontoinhaber: Akten-ID	Akten-ID (RecordIdentifier) des Aktenkontos für den Versicherten	siehe Bildungsvorschrift gemäß [gemSpec_DM_ePA#RecordIdentifier]
Aktenkontoinhaber: FQDN Anbieter ePA-Aktensystem	FQDN für den Zugriff auf das ePA-Aktensystem des	

ENTWURF

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

ENTWURF

	zu vertretenden Versicherten	
für jede Vertretung: FQDN Anbieter ePA-Aktensystem	FQDN für den Zugriff auf das ePA-Aktensystem des zugehörigen Anbieters für den zu vertretenden Versicherten	
für jede Vertretung: Anbieter-ID	"HomeCommunityId" des ePA-Aktensystems Der Parameter wird mittels Abfrage des Namensdienstes im Internet bestimmt. Er wird durch das ePA FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.	siehe [gemSpec_DM_ePA]
für jede Vertretung: Versicherten-ID des zu Vertretenden	unveränderlicher Teil der KVNR des zu Vertretenden	alphanummerisch, 10-stellig
für jede Vertretung: Geräteidentifikator	Von der Autorisierung einmalig übermittelte Zufallszahl. Wird durch das ePA-FdV übernommen und ist nicht durch den Nutzer konfigurierbar. Der Parameter wird nicht angezeigt.	base64Binary, 120 Zeichen
für jede Vertretung: letzte Anmeldung zum Aktenkonto	Zeitpunkt des letzten erfolgreichen Login des Nutzers in das Aktenkonto von dem Gerät. Dient der Auswahl der Benachrichtigungen. Der Parameter wird durch das ePA-FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.	Timestamp

ENTWURF

Benachrichtigungen aktivieren	Benachrichtigung über neue, geänderte oder gelöschte ePA-Dokumente	ja/nein Default: ja
Benachrichtigungszeitraum		Optionen: • seit der letzten Anmeldung • seit einem konkreten Datum • in einem durch den Versicherten einstellbarern, beliebigen zurückliegender Zeitraum (x Wochen, x Monate) bis zum aktuellen Datum • Default: seit der letzten Anmeldung
Dokumente einstellen: Berechtigte anzeigen	Gibt an, ob im Anwendungsfall Dokumente einstellen die Liste der für den Zugriff Berechtigten vor dem Hochladen angezeigt wird.	ja/nein Default: ja
Gerätenamen	Bezeichnung des GdV durch den Nutzer, um es im Freischaltprozess und während der Geräteverwaltung leichter wiedererkennen zu können. Bildet zusammen mit dem Geräteidentifikator die Gerätekennung (DeviceID). Die Gerätekennung wird für die Geräteautorisierung genutzt.	alphanumerisch, 64 Zeichen
eGK nutzen	Gibt an, ob zur Authentifizierung des Versicherten die eGK genutzt wird oder ein	ja/nein Default: ja

ENTWURF

	alternatives Verfahren.	
URL des Signaturdienstes	URL des Signaturdienstes	URL Default: nein

[<=]

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

A_15634-01 - ePA-Frontend des Versicherten: Anbieter-ID aus Namensdienst ermitteln
Das ePA-Frontend des Versicherten SOLL die Parameter "Aktenkontoinhaber: Anbieter-ID" und "Vertreter: Anbieter-ID" mittels DNS des Anbieters des ePA-Aktensystems im Internet auf Basis des FQDN des ePA-Aktensystems ermitteln.
Resource Record: ePA_FQDN, TXT Record: hcid**[<=]**

A_15293 - ePA-Frontend des Versicherten: Konfigurationsparameter verwalten
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, die nicht automatisch bestimmbaren Parameter aus TAB_FdV_104 zu verwalten (anzeigen, ändern, löschen).**[<=]**

A_17088-01 - ePA-Frontend des Versicherten: Kopplung an spezifisches ePA-Aktensystem
Der Hersteller des ePA-Frontend des Versicherten KANN den Wertebereich für die Parameter zur Identifikation des zu nutzenden ePA-Aktensystems fest vorgeben und eine Konfiguration durch den Nutzer einschränken.**[<=]**

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

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

Ein FdV kann an ein oder mehrere ePA-Aktensysteme gekoppelt werden.

ENTWURF

6 Funktionsmerkmale

6.1 Allgemein

6.1.1 Aktensession-Verwaltung

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

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

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

A_15294-01 - ePA-Frontend des Versicherten: Login nach Notwendigkeit
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "Login Aktensession" vor der Ausführung einer fachlichen Operation, welche eine Kommunikation mit dem ePA-Aktensystem beinhaltet, starten, wenn im Rahmen der internen Session-Verwaltung keine gültigen Session-Daten vorhanden sind.**[<=]**

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

A_17505-01 - ePA-Frontend des Versicherten: Auswahl kryptographische Versichertenidentität
Das ePA-Frontend des Versicherten MUSS dem Nutzer die Möglichkeit geben, für eine Aktensession anstelle der eGK eine von einem Signaturdienst erzeugte alternative kryptografische Identität des Versicherten zu verwenden, falls der Nutzer diese alternative kryptographische Versichertenidentität zuvor im ePA-Frontend des Versicherten bekannt gemacht hat.**[<=]**

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

A_15295-01 - ePA-Frontend des Versicherten: Beenden der Session
Das ePA-Frontend des Versicherten MUSS zum Beenden der Aktensession den Anwendungsfall "Logout Aktensession" ausführen.**[<=]**

A_15296-01 - ePA-Frontend des Versicherten: Abmeldung des Nutzers nach Inaktivität
Das ePA-Frontend des Versicherten MUSS den Nutzer nach spätestens 20 Minuten Inaktivität (Zeitspanne nach der letzten Nutzer-Aktivität) automatisch abmelden und die Aktensession beenden.**[<=]**

ENTWURF

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

Für die Dauer der Aktensession benötigt das ePA-Frontend des Versicherten einen gültigen Authentisierungstoken. Dieser wird in der Aktivität "Authentisieren des Nutzers" im Anwendungsfall "Login Aktensession" erstmalig ausgestellt. Der Authentisierungstoken hat eine Gültigkeitsdauer von 5 min und kann über einen Zeitraum von 120 min erneuert werden. Nach diesem Zeitraum muss sich der Nutzer neu authentisieren.

A_17543-01 - ePA-Frontend des Versicherten: periodisch Authentisierungstoken erneuern
Das ePA-Frontend des Versicherten MUSS vor Ablauf der Gültigkeit des Authentisierungstoken versuchen, mit der Aktivität "Authentisierungstoken erneuern" einen neuen Authentisierungstoken zu erhalten.**[<=]**

Der Zeitpunkt zum Erneuern soll so gewählt werden, dass bei einem Fehlschlagen der Operation je nach Fehlermeldung die Aktivität noch einmal ausgeführt werden kann, bzw. eine erneute Authentisierung gestartet werden kann.
Zu einer Aktensession im FdV gehören Session-Daten, welche für die Dauer der Aktensession vorzuhalten sind. Die Session-Daten beinhalten u.a. die in TAB_FdV_105 gelisteten Informationen. Eine vollständige Auflistung ist in "7- Informationsmodell" beschrieben.

Tabelle 7: TAB_FdV_105 – Session-Daten

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

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

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

6.1.2 Kommunikation mit dem ePA-Aktensystem

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

ENTWURF

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

A_15302-01 - ePA-Frontend des Versicherten: Lokalisierung Zugangsgateway für Versicherte
Das ePA-Frontend des Versicherten MUSS den Endpunkt für die Kommunikation mit dem Zugangsgateway für Versicherte mittels öffentlicher DNS-Dienste auf Basis des FQDN des ePA-Aktensystems ermitteln.**[<=]**

Falls für den FQDN mehrere IP-Adressen hinterlegt sind, wählt das ePA-Frontend des Versicherten zufällig eine der IP-Adressen als Endpunkt für den Verbindungsaufbau aus. Die Komponente Zugangsgateway des Versicherten weist bei Vollauslastung der Systemressourcen im ePA-Aktensystem die Verbindunganfrage ab. In diesem Fall kann das ePA-Frontend des Versicherten zufällig eine der weiteren IP-Adressen für einen neuen Verbindungsaufbau auswählen.
Jeder Anbieter eines ePA-Aktensystem verwaltet in den Nameservern Internet Resource Records zur Ermittlung der Aufruf-Schnittstellen seiner Module (siehe [gemSpec_Aktensystem#A_14128 - Anbieter ePA-Aktensystem - Resource Records FQDN ePA]). Die einzelnen Module werden mit Key/Value Paaren der TXT-Records mit den Kürzeln in TAB_FdV_106 identifiziert.

Tabelle 8: TAB_FdV_106 – DNS RR ePA-Aktensystem Komponenten

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

ENTWURF

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

A_15297-01 - ePA-Frontend des Versicherten: Kommunikation über TLS-Verbindung
Das ePA-Frontend des Versicherten MUSS mit dem Zugangsgateway des Versicherten ausschließlich über TLS kommunizieren.**[<=]**

A_15298-01 - ePA-Frontend des Versicherten: Unzulässige TLS-Verbindungen ablehnen
Das ePA-Frontend des Versicherten MUSS bei jedem Verbindungsaufbau das Zugangsgateway des Versicherten anhand seines TLS-Zertifikats authentifizieren und MUSS die Verbindungen ablehnen, falls die Authentifizierung fehlschlägt.**[<=]**

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

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

A_15299-01 - ePA-Frontend des Versicherten: eine TLS-Session pro Aktensession
Das ePA-Frontend des Versicherten MUSS für jede Aktensession - außer für die Kommunikation mit dem Schlüsselgenerierungsdienst - genau eine TLS-Session nutzen.**[<=]**

Für jede Aktensession wird eine separate TLS-Verbindung genutzt.

Für die Schlüsselgenerierung müssen der Schlüsselgenerierungsdienst (SGD) 1 und SGD 2 parallel angesprochen werden (siehe A_17994-01). Dafür baut das ePA-Frontend des Versicherten eine zweite TLS-Verbindung auf (siehe [gemSpec_SGD_ePA#A_17990]), welche nach Abschluss der Schlüsselgenerierung wieder geschlossen wird.

A_15300-01 - ePA-Frontend des Versicherten: TLS-Verbindungsaufbau nach Notwendigkeit
Das ePA-Frontend des Versicherten MUSS eine TLS-Verbindung zum Zugangsgateway des Versicherten aufbauen, wenn die ausgeführte Operation eine Kommunikation zum ePA-Aktensystem oder den zentralen Diensten der TI beinhaltet und keine TLS-Verbindung zum Zugangsgateway des Versicherten für die Aktensession besteht.**[<=]**

A_15301-01 - ePA-Frontend des Versicherten: TLS-Verbindung beenden
Das ePA-Frontend des Versicherten MUSS die für eine Aktensession aufgebaute TLS-Verbindung zum Zugangsgateway des Versicherten schließen, wenn die Aktensession beendet wird.**[<=]**

A_15303-01 - ePA-Frontend des Versicherten: SOAP-Responses valide
Das ePA-Frontend des Versicherten MUSS bei allen SOAP-Responses eine Schemaprüfung durchführen und mit einer qualifizierten Fehlermeldung abbrechen, wenn die Nachricht nicht valide ist.**[<=]**

6.1.3 Sicherer Kanal zur Dokumentenverwaltung

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

ENTWURF

- I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::RegistryStoredQuery
- I_Document_Management_Insurant::RemoveMetadata
- I_Document_Management_Insurant::RetrieveDocumentSet
- I_Document_Management_Insurant::RestrictedUpdateDocumentSet
- I_Account_Management_Insurant::GetAuditEvents
- I_Account_Management_Insurant::SuspendAccount
- I_Account_Management_Insurant::ResumeAccount
- I_Key_Management_Insurant::StartKeyChange
- I_Key_Management_Insurant::GetAllDocumentKeys
- I_Key_Management_Insurant::PutAllDocumentKeys
- I_Key_Management_Insurant::FinishKeyChange
- I_Document_Management_Connect::OpenContext
- I_Document_Management_Connect::CloseContext

A_15304-01 - ePA-Frontend des Versicherten: Umsetzung sicherer Kanal zur Dokumentenverwaltung
Das ePA-Frontend des Versicherten MUSS den im Rahmen des sicheren Verbindungsaufbaus mit der Dokumentenverwaltung ausgehandelten Sitzungsschlüssel verwenden, um den HTTP Body aller über den sicheren Kanal zu sendenden Requests an die Dokumentenverwaltung zu verschlüsseln und alle über den sicheren Kanal gesendeten Responses von der Dokumentenverwaltung zu entschlüsseln.**[<=]**

Für Informationen zum Kommunikationsprotokoll zwischen dem ePA-Frontend des Versicherten und einer VAU siehe [gemSpec_Krypt#3.15 ePA-spezifische Vorgaben] und [gemSpec_Krypt#6 Kommunikationsprotokoll zwischen VAU und ePA-Clients].

6.1.4 Geräteautorisierung

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

Das Gerät wird durch die Gerätekennung (DeviceID) identifiziert. Die Gerätekennung beinhaltet die Geräteidentität und den Gerätenamen. Die Geräteidentität ist eine Zufallszahl, welche dem ePA-Frontend des Versicherten von der Autorisierung übermittelt wird. Der Gerätename ist ein bis zur 64 Zeichen langer String, welcher durch den Nutzer in der Konfiguration des ePA-Frontend des Versicherten hinterlegt wird (siehe "A_15292-01").

Beim erstmaligen Login eines Nutzers von einem GdV wird die Gerätekennung mit leerem Geräteidentifikator (`phr:DeviceID::Device`) im Aufruf gesandt. Da noch kein bekannter Geräteidentifikator für dieses GdV in der Autorisierung registriert ist, antwortet die Autorisierung mit dem Fehler DEVICE_UNKNOWN und einer Zufallszahl im Fehlertext.

ENTWURF

Das ePA-Frontend des Versicherten speichert die Zufallszahl als Geräteidentifikator lokal und verwendet sie in allen Aufrufen gegenüber der Komponente Autorisierung.

A_15305-01 - ePA-Frontend des Versicherten: Geräteidentifikator abspeichern
Das ePA-Frontend des Versicherten MUSS einen von der Komponente Autorisierung übermittelten Geräteidentifikator nutzer- und aktenkontospezifisch abspeichern.**[<=]**

A_15306-01 - ePA-Frontend des Versicherten: DeviceID bilden
Das ePA-Frontend des Versicherten MUSS beim Start der Applikation nutzer- und aktenkontospezifisch die DeviceID aus der Geräteidentität und dem Gerätenamen aus der Konfiguration bilden und für Aufrufe an der Schnittstelle zur Komponente Autorisierung verwenden.**[<=]**

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

6.1.5 Zertifikatsprüfung

Das ePA-Frontend des Versicherten verwendet bei den in TAB_FdV_110 dargestellten Aktivitäten Zertifikate.

Tabelle 9: TAB_FdV_110 – Zertifikatsnutzung

Aktivität	Zertifikat der TI	Zertifikatstyp	Rollen-OID	Nutzung
Einlesen der eGK	ja	C.CH.AUT	oid_egk_aut	passiv
TLS-Verbindungsaufbau zum Zugangsgateway des Versicherten	nein	TLS Internet Zertifikat	n/a	aktiv
Authentisierung	ja	C.CH.AUT C.CH.AUT_ALT	oid_egk_aut oid_egk_aut_alt	passiv
Aufbau sicherer Kanal zur VAU	ja	C.FD.AUT	oid_epa_vau	aktiv
Berechtigung von LEI oder KTR erteilen Berechtigung von LEI ändern	ja	C.HCI.ENC	oid_smc_b_enc	aktiv
Verbindungsaufbau SGD	ja	C.SGD-HSM.AUT	oid_sgd1_hsm oid_sgd2_hsm	aktiv

ENTWURF

Es gelten folgende übergreifende Festlegungen für die Prüfung aktiv durch das ePA-Frontend des Versicherten genutzter Zertifikate.

A_15872-01 - ePA-Frontend des Versicherten: verpflichtende Zertifikatsprüfung
Das ePA-Frontend des Versicherten MUSS alle Zertifikate, die es aktiv verwendet (bspw. TLS-Verbindungsaufbau) auf Integrität und Authentizität prüfen. Falls die Prüfung kein positives Ergebnis ("gültig") liefert, so MUSS es die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen.
Das ePA-Frontend des Versicherten MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können.**[<=]**

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

6.1.5.1 Vertrauensanker des TI-Vertrauensraum

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

Die Initialisierung des TI-Vertrauensraums und der Wechsel des TI-Vertrauensankers wird beim ePA-Frontend des Versicherten

durch die Bereitstellung der FdV Applikation durchgeführt.

A_17667-01 - ePA-Frontend des Versicherten: Behandlung des Vertrauensankers
Das ePA-Frontend des Versicherten MUSS den aktuellen TI-Vertrauensanker (TSL-Signer-CA-Zertifikat) im Auslieferungszustand der Applikation integer und authentisch mit sich führen.
Dabei MUSS der TI-Vertrauensanker fest mit dem Code des ePA-Frontend des Versicherten verbunden sein, d.h. eine Manipulation des TI-Vertrauensankers MUSS durch das ePA-Frontend des Versicherten erkannt werden.
Das ePA-Frontend des Versicherten MUSS bei einem angekündigten Wechsel des TI-Vertrauensankers den neuen TI-Vertrauensanker zusätzlich zum aktuell gültigen Vertrauensanker mit sich führen.
Das ePA-Frontend des Versicherten MUSS eindeutig identifizierte und während der Erstellung der Applikation mittels Fingerprint validierte TSL-Signer-CA-Zertifikate mit sich führen und ausschließlich diese als Vertrauensanker verwenden.
[<=]

6.1.5.2 TSL-Behandlung

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

A_15874-01 - ePA-Frontend des Versicherten: Periodische Aktualisierung TI-Vertrauensraum
Das ePA-Frontend des Versicherten MUSS zur periodischen Aktualisierung des TI-Vertrauensraums den TUC_PKI_001 mit folgenden Anpassungen umsetzen:

- Der Offline-Modus ist nicht zu berücksichtigen

ENTWURF

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

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

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

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

A_16489-01 - ePA-Frontend des Versicherten: TSL - Prüfung Integrität und Authentizität
Das ePA-Frontend des Versicherten MUSS die Integrität und Authentizität der heruntergeladenen TSL prüfen. Falls die Prüfung kein positives Ergebnis liefert, so MUSS die gerade heruntergeladene TSL verworfen werden.**[<=]**

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

A_17732-01 - ePA-Frontend des Versicherten: TSL - Truststore für Zertifikatsprüfung
Das ePA-Frontend des Versicherten MUSS die TSL auswerten, um aus den Inhalten einen Truststore für die durchzuführenden Zertifikatsprüfungen zu bilden.**[<=]**

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

A_16490-01 - ePA-Frontend des Versicherten: TSL nicht verfügbar
Das ePA-Frontend des Versicherten MUSS, falls keine nach A_16489 erfolgreich geprüfte TSL zur Verfügung steht oder das aktuelle Datum nach dem Datum nextUpdate der TSL liegt, den Vertrauensraum als ungültig betrachten und sicherstellen, dass alle Zertifikatsprüfungen für TI-Zertifikate mit "ungültig" bewertet werden.**[<=]**

Hinweis: Es ist in Bezug auf die CC-Evaluierung hilfreich, wenn die TSL-Signaturprüfung mit einer speziell dafür geschriebenen (und gehärteten) Programmkomponente durchgeführt wird. Bei einer anschließenden XML-Auswertung der TSL mit einer Standard-XML-Bibliothek können die verarbeiteten XML-Daten dann als vertrauenswürdig angesehen werden.

ENTWURF

6.1.5.3 Zertifikatsprüfung von Zertifikaten der TI

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

A_15873-01 - ePA-Frontend des Versicherten: Prüfung TI-Zertifikate (ausser SGD-Zertifikate)
Das ePA-Frontend des Versicherten MUSS bei der Prüfung von X.509-Zertifikaten der TI (ausser X.509-Zertifikaten eines Schlüsselgenerierungsdienstes) folgende Prüfschritte durchlaufen.

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

Führt einer der Prüfschritte nicht zu einen positiven Prüfergebnis, so MUSS das Zertifikat abgelehnt werden und die weitere Verarbeitung des Zertifikats oder der Attribute darin abgelehnt werden.
Das ePA-Frontend des Versicherten muss die referenzierten gemSpec_PKI#TUC_PKI_* im Rahmen dieser Anforderung nicht normativ umsetzen.**[<=]**

Für die Prüfung des Online-Status von Zertifikaten der TI wird die Schnittstelle I_OCSP_Status_Information genutzt. Siehe [gemSpec_PKI#9]. Die Schnittstelle wird durch den Status-Proxy der Komponente Zugangsgateway des Versicherten angeboten. Siehe auch [gemSpec_Zugangsgateway_Vers#A_15869 - Zugangsgateway des Versicherten, Bereitstellung OCSP-Forwarder].

ENTWURF

A_18177-01 - ePA-Frontend des Versicherten: Prüfung TI-Zertifikate (SGD-Zertifikate)
Das ePA-Frontend des Versicherten MUSS X.509-Zertifikate eines Schlüsselgenerierungsdienstes der TI gemäß PL_TUC_PKI_VERIFY_CERTIFICATE prüfen.

PL_TUC_PKI_VERIFY_CERTIFICATE nutzen	Eingangsdaten: • Zu prüfendes Zertifikat: vom SGD übermitteltes Zertifikat • EECertificateContainedInTSL: true • Referenzzeitpunkt: aktuelle Systemzeit Rückgabedaten: • Gültigkeit zu Referenzzeitpunkt • Rolle des Zertifikates

[<=]

6.1.5.4 Zertifikatsprüfung von Internet-Zertifikaten

Folgende Vorgaben gelten für die Prüfung von Internet-Zertifikaten.

A_15887-01 - ePA-Frontend des Versicherten: Prüfung Internet-Zertifikate
Das ePA-Frontend des Versicherten MUSS für die Prüfung des internetseitigen Zertifikats des Zugangsgateways des Versicherten das Zertifikat auf ein CA-Zertifikat einer CA, die die "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (https://cabforum.org/baseline-requirements-documents/) erfüllt, kryptographisch (Signaturprüfung) zurückführen können. Ansonsten MUSS es das Zertifikat als "ungültig" bewerten.
Es MUSS die zeitliche Gültigkeit des Zertifikats prüfen. Falls diese Prüfung negativ ausfällt, muss es das Zertifikat als "ungültig" bewerten. **[<=]**

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

6.1.6 Dokumente

Das ePA-Aktensystem unterstützt die einzelne Dokumente bis zu einer Größe von 25 MB.

A_15283-01 - ePA-Frontend des Versicherten: Dokumentgrößen von 25 MB
Das ePA-Frontend des Versicherten MUSS für alle Außenschnittstellen, in denen ein Dokument verarbeitet wird, Dokumente mit einer Größe von mindestens 25 MB unterstützen.**[<=]**

6.1.7 Umschlüsselung der Dokumente

Die Dokumente der elektronischen Patientenakte sind mit ePA-spezifischen kryptographischen Schlüsseln gesichert. Ab der ePA Version 2.0 ist es möglich, dass der Versicherte zu jedem Zeitpunkt eine Umschlüsselung starten kann. Dadurch kann bei Verdacht oder bei tatsächlicher Kompromittierung eine missbräuchliche Nutzung der Dokumente verhindert werden.

ENTWURF

Die Umschlüsselung kann über das FdV vom Versicherten gestartet werden.

6.1.7.1 Kryptographische Architektur der Dokumentenverschlüsselung

Die Dokumente der elektronischen Patientenakte werden verschlüsselt im Aktensystem abgelegt. Der Betreiber hat keinen Zugriff auf die Klartext-Daten der Dokumente. Die Versicherten können jederzeit alle Dokumente entschlüsseln und die Leistungserbringer dürfen im Rahmen ihrer von den Versicherten festgelegten Berechtigungen für sie freigegebene Dokumente über ihr Primärsystem entschlüsseln. Um diese Funktionalität umzusetzen sind verschiedene Verschlüsselungen mit unterschiedlichen Schlüsseln notwendig. Diese müssen bei der Umschlüsselung ausgetauscht werden. In der folgenden Abbildung sind die verschiedenen Schlüssel aufgeführt.

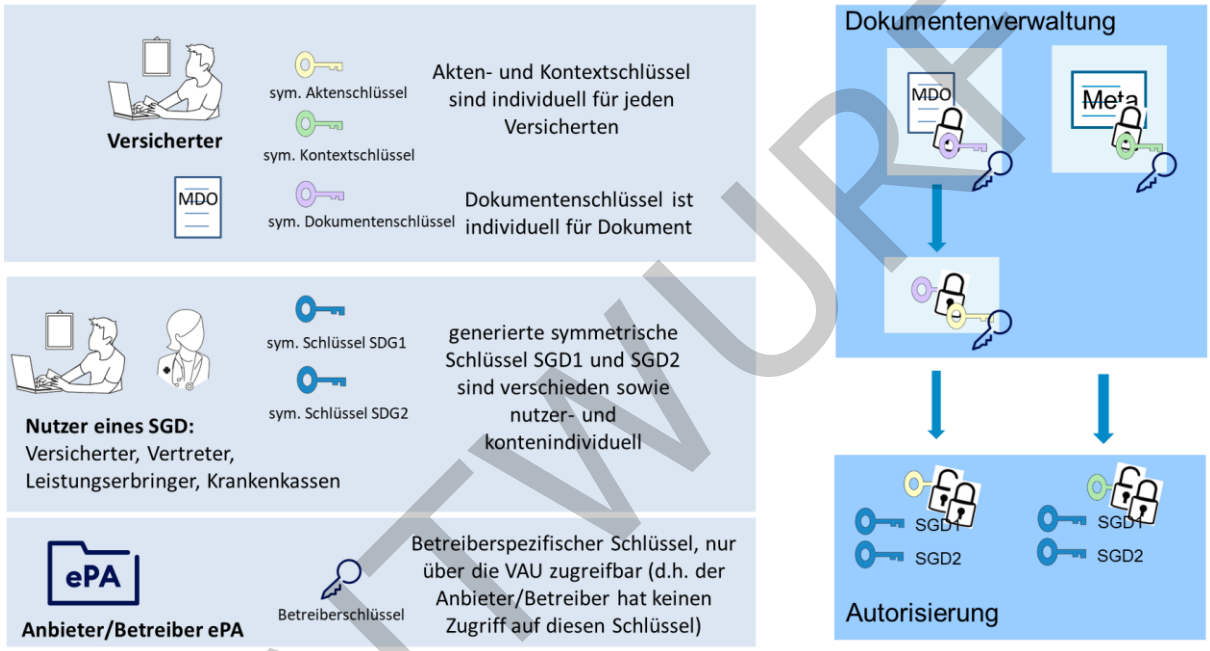


Abbildung 3: Kryptographische Schlüssel der ePA

Für die Verschlüsselung eines Dokumentes wird ein dokumentenindividueller symmetrischer Dokumentenschlüssel verwendet. Dieser wird mit einem versichertenindividuellen Aktenschlüssel verschlüsselt. Der Aktenschlüssel wird mit nutzerindividuellen Schlüsseln des SGD1 und SGD2 verschlüsselt und anschließend in der Komponente Autorisierung abgelegt. Nutzer sind berechtigte LEI, Kassen und Vertreter des Versicherten.

Die mit dem Dokumentenschlüssel gesicherten Dokumente und die mit dem Aktenschlüssel verschlüsselten Dokumentenschlüssel werden mit einem aus einem betreiberspezifischen Schlüssel abgeleiteten aktenspezifischen Schlüssel nochmals verschlüsselt und anschließend im Aktensystem abgelegt.

Die Metadaten werden mit dem versichertenindividuellen Kontextschlüssel verschlüsselt. Die verschlüsselten Metadaten werden nochmals mit dem aus dem betreiberspezifischen Schlüssel abgeleiteten aktenspezifischen Schlüssel verschlüsselt und im Aktensystem abgelegt. Die Kontextschlüssel werden mit den nutzerindividuellen Schlüsseln des Schlüsselgenerierungsdienstes 1 und 2 (SGD1 und SGD2) symmetrisch verschlüsselt und anschließend in der Komponente Autorisierung abgelegt.

ENTWURF

Ab Release 4.0.1 ist die explizite, vom Versicherten angestoßene, Erneuerung der Akten-, Kontext- und SGD1- und SGD2 Schlüssel umgesetzt. Der Betreiber kann unabhängig davon regelmäßig den betreiberspezifischen Schlüssel erneuern.

Einzelne Rückgabewerte bei der Kommunikation zwischen dem FdV und der Autorisierungskomponente und der Dokumentenverwaltung sind vom jeweiligen Absender signiert, damit beim Weiterleiten von Argumenten (z.B. bei der Übermittlung der von der Autorisierung ausgestellten rollbackTime) der Empfänger diese über eine Signaturprüfung validieren kann. Es werden sowohl die Herkunft als auch der Signaturerstellungszeitpunkt vom Empfänger geprüft. Das Frontend des Versicherten prüft die Signaturen der Rückgabewerte nicht.

A_20477 - ePA-Frontend des Versicherten: Unterstützung der Umschlüsselungsfunktion
Das ePA-Frontend des Versicherten MUSS dem Nutzer eine Umschlüsselungsfunktion anbieten, die auf Wunsch des Versicherten einen Wechsel der Akten- und Kontextschlüssel sowie der SGD1- und SGD2-Schlüssel durch die Komponenten, die diese Schlüssel verwalten, einleitet.
[<=]

6.2 Implementation ePA-Anwendungsfälle im FdV

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

6.2.1 Übergreifende Festlegungen

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

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

A_15567-04~~A_15567-03~~ - ePA-Frontend des Versicherten: Zulässigkeit der Anwendungsfälle
Das ePA-Frontend des Versicherten MUSS die Zulässigkeit des Anwendungsfalls in Abhängigkeit von folgenden Kriterien sicherstellen:
VerificationResult

- K1: Rolle des Nutzers (Aktenkontoinhaber, Vertreter)
- K2: Status Aktenkonto
- K3: falls eGK zur Authentisierung genutzt wird: Status PIN (MRPIN.home) der eGK: `[OK (PasswordEnabledVerified) / BLOCKED (PasswordBlocked) / VERIFYABLE (PasswordEnabledNotVerified.X)]`

ENTWURF

1857 **Tabelle 10: TAB_FdV_161 – Zulässigkeit von Anwendungsfällen**

Anwendungsfall	K1	K2	K3
Login Aktensession	Aktenkontoinhaber Vertreter	immer	OK VERIFYABLE
Logout Aktensession	Aktenkontoinhaber Vertreter	immer	immer
Aktenkonto aktivieren	Aktenkontoinhaber	Registered	OK VERIFYABLE
Anbieter wechseln	Aktenkontoinhaber	~~Activated~~Dismissed	OK VERIFYABLE
Dokumente umschlüsseln	Aktenkontoinhaber	vor und nach der Umschlüsselung: Activated , während der Umschlüsselung: KEY_CHANGE	OK VERIFYABLE
Berechtigung für LEI vergeben	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
Vertretung einrichten	Aktenkontoinhaber	Activated Dismissed	OK VERIFYABLE
Berechtigung für Kostenträger vergeben	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
Vergebene Berechtigungen anzeigen	Aktenkontoinhaber Vertreter	Activated Dismissed Suspended	OK VERIFYABLE
Eingerichtete Vertretungen auflisten	Aktenkontoinhaber Vertreter	n/a	immer
Berechtigung für LEI ändern	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
Berechtigung für LEI löschen	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
Berechtigung für Vertreter löschen	Aktenkontoinhaber	Activated Dismissed	OK VERIFYABLE
Berechtigung für Kostenträger löschen	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE

ENTWURF

Dokumente einstellen	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
Dokumente suchen	Aktenkontoinhaber Vertreter	Activated Dismissed Suspended	OK VERIFYABLE
Dokumente löschen	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
Dokumente herunterladen	Aktenkontoinhaber Vertreter	Activated Dismissed Suspended	OK VERIFYABLE
Protokolldaten einsehen	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
PIN der eGK ändern	Aktenkontoinhaber Vertreter	n/a	OK VERIFYABLE
PIN der eGK mit PUK entsperren	Aktenkontoinhaber Vertreter	n/a	BLOCKED OK VERIFYABLE
Benachrichtigungsadresse für Geräteautorisierung aktualisieren	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE

[<=]

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

6.2.2 Fehlerbehandlung

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

A_15307-01 - ePA-Frontend des Versicherten: Abbruch bei Fehler im Anwendungsfall
Das ePA-Frontend des Versicherten MUSS, wenn bei der Abarbeitung der Aktivitäten eines Anwendungsfalls ein Fehler auftritt und keine Fehlerbehandlung beschrieben ist, den Anwendungsfall abbrechen.**[<=]**

Das FdV soll dem Nutzer nach einem Abbruch eine verständliche Fehlermeldung anzeigen.

Wenn die Möglichkeit besteht, dass der Nutzer das fehlerverursachende Problem selbst beheben kann, kann das FdV den Nutzer auf die Lösung hinweisen. Bspw. kann dem

ENTWURF

Nutzer bei einer gesperrten PIN der Anwendungsfall "PIN der eGK entsperren" angeboten werden.

A_15308 - ePA-Frontend des Versicherten: Anzeige von Handlungsmöglichkeiten im Fehlerfall
Das ePA-Frontend des Versicherten SOLL dem Nutzer im Fehlerfall einen Hinweis geben, wenn es für den Nutzer Handlungsmöglichkeiten dazu gibt.**[<=]**

A_15309-02~~A_15309-01~~ - ePA-Frontend des Versicherten: Anzeige im Fehlerfall
Das ePA-Frontend des Versicherten MUSS bei Auftreten der Fehlercodes aus TAB_FdV_107 und TAB_FdV_108 dem Nutzer den entsprechenden Fehlertext anzeigen und die spezifische Aktion durchführen.

Tabelle 11: TAB_FdV_107 – Behandlung von Fehlercodes von Plattformbausteinen

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

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

Fehlercode	Fehlertext	Spezifische Aktion durch ePA-Frontend des Versicherten

ENTWURF

ASSERTION_INVALID		Das ePA-Frontend des Versicherten kann versuchen die Authentisierung mittels der übergreifenden Aktivität "Authentisieren des Nutzers" zu aktualisieren und den Operationsaufruf wiederholen.
DEVICE_UNKNOWN	~~Das Gerät ist nicht für die Nutzung des Aktensystems registriert. Bitte führen Sie eine Geräteautorisierung durch, indem Sie den Link zur Freischaltung aufrufen, welcher Ihnen über eine E-Mail zugesendet wird.~~Sie haben noch nie mit diesem Gerät auf Ihre ePA zugegriffen. Aus Sicherheitsgründen bitten wir Sie Ihren Zugriff zu autorisieren. Ihre Registrierung mit diesem Gerät ist fast abgeschlossen. In Kürze erhalten Sie den Bestätigungslink für Ihre Autorisierung an die hinterlegte E-Mail Adresse. Falls Sie diese E-Mail nicht erhalten haben, prüfen Sie bitte Ihren Spam-Ordner. Falls Sie keinen Zugriff mehr auf Ihre hinterlegte E-Mail Adresse haben, können Sie uns gerne kontaktieren.	Der Anwendungsfall wird abgebrochen.
wst:InvalidSecurityToken	Ihre Gesundheitskarte ist ungültig, bitte wenden Sie sich an Ihre Krankenkasse.	

[<=]

A_15310-01 - ePA-Frontend des Versicherten: Fehlerbehandlung ungültiger Token

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

ENTWURF

A_15311-01 - ePA-Frontend des Versicherten: Aufrufparameter ungültig
Das ePA-Frontend des Versicherten MUSS bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn notwendige Aufrufparameter unvollständig, ungültig oder inkonsistent sind.**[<=]**

6.2.3 Aktivitäten

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

6.2.3.1 Authentisieren des Nutzers

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

A_15312-02 - ePA-Frontend des Versicherten: Authentisieren des Nutzers
Das ePA-Frontend des Versicherten MUSS die Aktivität "Authentisieren des Nutzers" gemäß TAB_FdV_109 umsetzen.

Tabelle 13: TAB_FdV_109 – Authentisieren des Nutzers

`I_Authentication_Insurant::LoginCreateChallenge` Request erstellen	RequestSecurityToken (RST) erstellen
`I_Authentication_Insurant::LoginCreateChallenge` Response verarbeiten	RequestSecurityTokenResponse (RSTR) verarbeiten Rückgabedaten: • `st:Challenge` = Challenge
`I_Authentication_Insurant::LoginCreateToken` Request erstellen	RequestSecurityTokenResponse (RSTR) erstellen Eingangsdaten: • `wst:Challenge` = Challenge aus RSTR Der Request wird signiert und die Signatur im SOAP Header eingefügt. • wsse:BinarySecurityToken = C.CH.AUT des Nutzers • ds:SignatureValue = signierter Hashwert

ENTWURF

wenn Authentisierung mittels eGK: Plattformbaustein PL_TUC_SIGN_HASH_nonQES zum Signieren nutzen	Eingangsdaten: • `Identifikator` = für eGK G2: PrK.CH.AUT.R2048 für eGK höhere Generation: PrK.CH.AUT.E256 • `Signaturverfahren` = für eGK G2: signPSS für eGK höhere Generation: signECDSA • Hashwert = soap:Body Der Body der SOAP-Nachricht wird gemäß [gemSpec_Authentisierung_Vers] durch Übergabe dessen Hashwerts mittels des Karten-Kommandos PSO Compute Digital Signature von der eGK signiert. Für den Aufruf der Operation wird der Nutzer zur PIN-Eingabe (MRPIN.home) für seine eGK aufgefordert, falls der notwendige Sicherheitszustand der eGK noch nicht erreicht ist. Rückgabedaten: 1. OK + Hashsignatur oder 2. Fehler
wenn Authentisierung mittels alternativer kryptographischer Versichertenidentität:	Aufruf der signaturdienstspezifischen Schnittstelle `I_Remote_Sign_Operations::sign_Data` Eine Beschreibung der konkreten Ausgestaltung der Schnittstelle befindet sich in [vesta]. Der Response liefert u.a. das C.CH.AUT_ALT Zertifikat. Dieses wird in die Session-Daten übernommen.
`I_Authentication_Insurant::LoginCreateToken` Response verarbeiten	RequestSecurityTokenResponse Collection (RSTRC) verarbeiten Rückgabedaten: • `saml2:Assertion` = AuthenticationAssertion AuthenticationAssertion (Authentisierungstoken) in Session-Daten übernehmen

ENTWURF

Fehlerbehandlung	Wenn der Response von LoginCreateToken den WS-Trust Fehler wst:InvalidSecurityToken liefert, dann ist das C.CH.AUT bzw. C.CH.AUT_ALT Zertifikat des Nutzers ungültig. Der Anwendungsfall wird abgebrochen. Falls die Authentisierung mittels eGK erfolgte, muss der Nutzer aufgefordert werden, seine aktuell gültige eGK zu stecken oder sich an seine Krankenkasse zu wenden.

[<=]

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

6.2.3.2 Authentisierungstoken erneuern

Mit dieser Operation kann das ePA-Frontend des Versicherten den Authentisierungstoken am ePA-Aktensystem verlängern.

A_17541-01 - ePA-Frontend des Versicherten: Authentisierungstoken erneuern
Das ePA-Frontend des Versicherten MUSS die Aktivität "Authentisierungstoken erneuern" gemäß TAB_FdV_173 umsetzen.

Tabelle 14: TAB_FdV_173 – Logout - Authentisierungstoken abmelden

Vorbedingung	AuthenticationAssertion in Session-Daten
`I_Authentication_Insurant::RenewToken` Request erstellen	Eingangsdaten: • RenewTarget: `AuthenticationAssertion` aus Session-Daten
`I_Authentication_Insurant::RenewToken` Response verarbeiten	RequestSecurityTokenResponse (RSTR) verarbeiten Rückgabedaten: • `RequestedSecurityToken` = AuthenticationAssertion AuthenticationAssertion (Authentisierungstoken) in Session-Daten ersetzen.

[<=]

Der vorher genutzte Authentisierungstoken wird gelöscht.

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

ENTWURF

6.2.3.3 Dokumentenset in Dokumentenverwaltung hochladen

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

A_15314-01 - ePA-Frontend des Versicherten: Dokumentenset in Dokumentenverwaltung hochladen
Das ePA-Frontend des Versicherten MUSS die Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" gemäß TAB_FdV_111 umsetzen.

Tabelle 15: TAB_FdV_111 – Dokumentenset in Dokumentenverwaltung hochladen

`I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b` Request erstellen	Eingangsparameter: • `Provide And Register Document Set-b` Message gemäß IHE XDS-Transaktion [ITI-41] • `AuthenticationAssertion` aus Session-Daten
`I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b` Response verarbeiten	Rückgabedaten: • `Provide And Register Document Set-b` Response Message gemäß IHE XDS-Transaktion [ITI-41]

[<=]

A_15315-01 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-41]
Das ePA-Frontend des Versicherten MUSS für die Nutzung der Operation `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b` gemäß der in [IHE-ITI-TF] definierten IHE XDS-Transaktion [ITI-41] "Provide & Register Document Set-b" als Akteur "Document Source" umsetzen.**[<=]**

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

A_15316-01 - ePA-Frontend des Versicherten: Upload verschlüsselter Versichertendokumente
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass Dokumente des Versicherten, welche in das ePA-Aktensystem eingestellt werden, verschlüsselt sind.**[<=]**

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

A_17772-01 - ePA-Frontend des Versicherten: Upload unverschlüsselter technischer Dokumente
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass technische Dokumente (Policy Documents) unverschlüsselt, d.h. nicht mit dem Aktenschlüssel verschlüsselt, in das ePA-Aktensystem eingestellt werden. **[<=]**

ENTWURF

A_15972-01 - ePA-Frontend des Versicherten: Trennung fachlicher und technischer Dokumente beim Upload
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass eine Provide And Register Document Set-b Message entweder ein oder mehrere Versichertendokumente oder genau ein technisches Dokument enthält.**[<=]**

A_16221-01 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-41] - Unterstützung MTOM/XOP
Das ePA-Frontend des Versicherten MUSS bei der Umsetzung der IHE XDS-Transaktion [ITI-41] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] gemäß [IHE-ITI-TF2x#V.3.6.] verwenden.**[<=]**

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

6.2.3.4 Dokumentenset aus Dokumentenverwaltung herunterladen

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

A_15317-01 - ePA-Frontend des Versicherten: Dokumentenset aus Dokumentenverwaltung herunterladen
Das ePA-Frontend des Versicherten MUSS die Aktivität "Dokumentenset aus Dokumentenverwaltung herunterladen" gemäß TAB_FdV_112 umsetzen.

Tabelle 16: TAB_FdV_112 – Dokumentenset aus Dokumentenverwaltung herunterladen

`I_Document_Management_Insurant::RetrieveDocumentSet` Request erstellen	Eingangsparameter: • `RetrieveDocumentSet_Message` gemäß IHE XDS-Transaktion [ITI-43] • `AuthenticationAssertion` aus Session-Daten
`I_Document_Management_Insurant::RetrieveDocumentSet` Response verarbeiten	Rückgabedaten: • RetrieveDocumentSetResponse_Message gemäß IHE XDS-Transaktion [ITI-43] RetrieveDocumentSetResponse_Message beinhaltet ein oder mehrere Dokumente. Jedes medizinisches Dokument ist mit einem individuellen Dokumentenschlüssel verschlüsselt. Der Dokumentenschlüssel ist mit dem Aktenschlüssel verschlüsselt.

ENTWURF

für jedes medizinische Dokument aus RetrieveDocumentSetResponse_Message: Plattformbaustein PL_TUC_SYMM_DECIPHER nutzen Hinweis: Der Begriff "medizinische Dokumente" umfasst alle Dokumente, welche durch LEI, KTR oder Versicherte in das ePA-Aktensystem eingestellt wurden. Davon abgegrenzt werden die technischen Dokumente (Policy Documents). Sie werden unverschlüsselt übertragen.	Für Vorgaben zum Entschlüsseln eines Dokumentes aus dem ePA-Aktensystem siehe [gemSpec_DM_ePA#2.4.2 Entschlüsselung]. Dokumentenschlüssel mit PL_TUC_SYMM_DECIPHER entschlüsseln Eingangsdaten: • verschlüsselter Dokumentenschlüssel aus EncryptedData\EncryptedKey\CipherData • Aktenschlüssel (`RecordKey`) aus Session-Daten • Der optionale Parameter AD wird nicht verwendet. Rückgabedaten: • entschlüsselter Dokumentenschlüssel Dokument mit PL_TUC_SYMM_DECIPHER entschlüsseln Eingangsdaten: • verschlüsseltes Dokument aus EncryptedData\CipherData • entschlüsselter Dokumentenschlüssel • Der optionale Parameter AD wird nicht verwendet. Rückgabedaten: • entschlüsseltes Dokument

[<=]

A_15318-01 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-43]
Das ePA-Frontend des Versicherten MUSS für die Nutzung der Operation `I_Document_Management_Insurant::RetrieveDocumentSet` gemäß der in [IHE-ITI-TF] definierten IHE XDS-Transaktion [ITI-43] "Retrieve Document Set" als Akteur "Document Consumer" umsetzen.**[<=]**

A_16222-02 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-43] - MTOM unterstützen
Das ePA-Frontend des Versicherten MUSS bei der Umsetzung der IHE XDS-Transaktion [ITI-43] die Übertragung von Dokumenten mit MTOM/XOP [MTOM] unterstützen.**[<=]**

ENTWURF

6.2.3.5 Dokumentenset in Dokumentenverwaltung löschen

Mit dieser Operation werden ein oder mehrere Dokumente anhand ihrere entryUUIDs aus der Dokumentenverwaltung gelöscht. Die XDS-Metadaten wurden vorab mit einer Suche nach Dokumenten im ePA-Aktensystem ermittelt.

A_15319-02 - ePA-Frontend des Versicherten: Dokumentenset in Dokumentenverwaltung löschen
Das ePA-Frontend des Versicherten MUSS die Aktivität "Dokumentenset in Dokumentenverwaltung löschen" gemäß TAB_FdV_113 umsetzen.

Tabelle 17: TAB_FdV_113 – Dokumentenset in Dokumentenverwaltung löschen

`I_Document_Management_Insurant::RemoveMetadata` Request erstellen	Eingangsdaten: • `AuthenticationAssertion` aus Session-Daten • `xds:DeleteDocumentSet_Message` gemäß IHE RMD-Transaktion [ITI-62]
`I_Document_Management_Insurant::RemoveMetadata` Response verarbeiten	Rückgabedaten: • `xds:DeleteDocumentSetResponse_Message` gemäß IHE RMD-Transaktion [ITI-62]

[<=]

A_15320-02 - ePA-Frontend des Versicherten: IHE RMD-Transaktion [ITI-62]
Das ePA-Frontend des Versicherten MUSS die Nutzung der Operation `I_Document_Management_Insurant::RemoveMetadata` gemäß der in [IHE-ITI-RMD] definierten IHE RMD-Transaktion [ITI-62] "Remove Metadata" als Akteur "Document Administrator" umsetzen.**[<=]**

6.2.3.6 Suche nach Dokumenten in Dokumentenverwaltung

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

A_15321-01 - ePA-Frontend des Versicherten: Suche nach Dokumenten in Dokumentenverwaltung
Das ePA-Frontend des Versicherten MUSS die Aktivität "Suche nach Dokumenten in Dokumentenverwaltung" gemäß TAB_FdV_114 umsetzen.

Tabelle 18: TAB_FdV_114 – Suche nach Dokumenten in Dokumentenverwaltung

`I_Document_Management_Insurant::RegistryStoredQuery` Request erstellen	Eingangsparameter: • `query:AdhocQueryRequest_Message` gemäß IHE XDS-Transaktion [ITI-18] • `AuthenticationAssertion` aus Session-Daten

ENTWURF

I_Document_Management_Insurant::RegistryStoredQuery Response verarbeiten	Rückgabedaten: • query:AdhocQueryResponse_Message gemäß IHE XDS-Transaktion [ITI-18]

[<=]

A_15322-01 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-18]
Das ePA-Frontend des Versicherten MUSS für die Nutzung der Operation I_Document_Management_Insurant::RegistryStoredQuery gemäß der in [IHE-ITI-TF] definierten IHE XDS-Transaktion [ITI-18] "Registry Stored Query" als Akteur "Document Consumer" umsetzen.**[<=]**

A_17854-01 - ePA-Frontend des Versicherten: Nutzung des Anfragetyps "FindDocumentsByTitle"
Das ePA-Frontend des Versicherten MUSS den in [ITI-18] nicht enthaltenen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.1] in Verbindung mit dem zusätzlich zu [ITI-18] eingeführten Suchparameter$XDSDocumentEntryTitle sowie dem optionalen Parameter $XDSDocumentEntryAuthorInstitution nutzen können.**[<=]**

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

Der optionale Parameter "$XDSDocumentEntryAuthorInstitution" filtert die Suchergebnismenge über das AttributXDSDocumentEntry.authorInstitution.

6.2.3.7 Vergebene Berechtigungen bestimmen

Mit dieser Operation werden die für das Aktenkonto vergebenen Berechtigungen ermittelt. Für jeden Berechtigten ist in der Komponente Autorisierung ein AuthorizationKey und in der Komponente Dokumentenverwaltung ein technisches Dokument (Policy Document) hinterlegt. Letzteres beinhaltet die Parameter der Berechtigung.

A_15323-01 - ePA-Frontend des Versicherten: Vergebene Berechtigungen bestimmen
Das ePA-Frontend des Versicherten MUSS die Aktivität "Vergebene Berechtigungen bestimmen" gemäß TAB_FdV_115 umsetzen.

Tabelle 19: TAB_FdV_115 – Vergebene Berechtigungen bestimmen

Standardablauf	Aktivitäten im Standardablauf 1. Schlüsselmaterial aller Berechtigten laden 2. Policy Documents suchen 3. Policy Documents herunterladen 4. Berechtigungen aus Policy Documents extrahieren

ENTWURF

[<=]

A_17129-01 - ePA-Frontend des Versicherten: Berechtigung bestimmen - Schlüsselmaterial aller Berechtigten laden
Das ePA-Frontend des Versicherten MUSS für die Aktivität "Vergebene Berechtigungen bestimmen" die übergreifende Aktivität "Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden" ausführen.**[<=]**

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

A_15324-01 - ePA-Frontend des Versicherten: Berechtigung bestimmen - Policy Documents suchen
Das ePA-Frontend des Versicherten MUSS für die Aktivität "Vergebene Berechtigungen bestimmen" zur Suche der Policy Documents die übergreifende Aktivität "Suche nach Dokumenten in Dokumentenverwaltung" mit einer query:AdhocQueryRequest_Message für Policy Documents ausführen.**[<=]**

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

A_15325-01 - ePA-Frontend des Versicherten: Berechtigung auflisten - Policy Dokuments herunterladen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vergebene Berechtigungen anzeigen" zum Herunterladen der Policy Documents die übergreifende Aktivität "Dokumentenset aus Dokumentenverwaltung herunterladen" mit einer RetrieveDocumentSet_Message für alle über die XDS-Metadaten ermittelten Kennungen (`DocumentEntry.uniqueId`) von Policy Documents ausführen.**[<=]**

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

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

Berechtigung für LEI: Telematik-ID, Name der LEI, Berechtigung "erteilt am", Berechtigung "gültig bis", Zugriffsrecht der LEI (normal, erweitert), berechtigte Dokumentenkategorien, einzeln freigeschaltete oder geblockte Dokumente (Whitelist, Blacklist)

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

Berechtigung für Vertreter: Versicherten-ID, Name des Vertreters

Berechtigung für KTR: Telematik-ID, Name des KTR

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

6.2.3.8 AuthorizationKey

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

ENTWURF

6.2.3.8.1 Struktur AuthorizationKeyType

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

Das Attribut `validTo` beinhaltet die Gültigkeit des AuthorizationKey, d.h. den Zeitpunkt bis zu dem die Berechtigung erteilt wird. Für eine Berechtigung ohne zeitliche Begrenzung wird ein technisches Datum heute + 100 Jahre verwendet.

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

Das Element `DisplayName` beinhaltet den Klartextnamen des Berechtigten.

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

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

Die Datenstruktur für EncryptedKeyContainer und die Klartextpräsentation für Akten- und Kontextschlüssel ist in [gemSpec_SGD_ePA#8 Interoperables Austauschformat] beschrieben.

6.2.3.8.2 Schlüsselableitung für Ver- und Entschlüsselung

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

A_17842-01 - ePA-Frontend des Versicherten: Symmetrische Schlüssel für Akten- und Kontextschlüssel ermitteln
Das ePA-Frontend des Versicherten MUSS zur Schlüsselableitung den in [gemSpec_SGD_ePA#2.3 Basisablauf Kommunikation SGD-Client und SGD] festgelegten Ablauf in der Rolle Client durchführen.**[<=]**

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

Anwendungsfall im FdV	Akteur	Zweck	Anwendungsfall für SGD
Aktenkonto aktivieren Anbieter wechseln	Versicherter	Verschlüsseln	[gemSpec_SGD_ePA#2.4 Initiale Schlüsselableitung für den Kontoinhaber]
Berechtigung für LEI vergeben Vertretung einrichten Berechtigung für Kostenträger vergeben	Versicherter	Verschlüsseln	[gemSpec_SGD_ePA#2.6 Schlüsselableitung für einen Berechtigungsempfänger]

ENTWURF

Berechtigung für LEI ändern			
Berechtigung für LEI vergeben Berechtigung für Kostenträger vergeben Berechtigung für LEI ändern	Vertreter	Verschlüsseln	[gemSpec_SGD_ePA#2.8 Schlüsselableitung für einen Berechtigungsempfänger durch einen Vertreter]
Login	Versicherter Vertreter	Entschlüsseln	Für das Entschlüsseln müssen keine Anwendungsfälle für SGD unterschieden werden. Es wird das Element AssociatedData des ermittelten AuthorizationKey für den Aufruf der Operation KeyDerivation beim SGD wie folgt verwenden: `KeyDerivation <Teilstring aus AssociatedData für den entsprechenden SGD>`

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

`Key` ist der für die Verschlüsselung zu verwendende symmetrische Schlüssel und `a` entspricht AssociatedData für den entsprechenden SGD.

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

A_17994-01 - ePA-Frontend des Versicherten: Aufrufe zur Schlüsselableitung parallelisieren
Das ePA-Frontend des Versicherten MUSS die Schlüsselableitung mit SGD 1 und SGD 2 sowie das Erzeugen des ephemeren ECDH-Schlüsselpaares parallelisieren.**[<=]**

Siehe auch [gemSpec_SGD_ePA#A_17990].

ENTWURF

6.2.3.8.3 AuthorizationKey erstellen

Für den Aktenkontoinhaber, Vertreter und KTR wird die Berechtigung ohne zeitliche Begrenzung vergeben. Für LEI ist das Enddatum entsprechend der vom Nutzer gewählten Berechtigungsdauer zu setzen. Der für `DisplayName` zu verwendende Name einer LEI oder eines KTR und die Telematik-ID werden aus dem Eintrag der zu berechtigenden Institution im VZD bestimmt (siehe "6.2.3.15- Suchanfrage Verzeichnisdienst der TI").

A_18248-01 - ePA-Frontend des Versicherten: AuthorizationKey erstellen - Verschlüsselungszertifikate für Telematik-ID verwenden
Das ePA-Frontend des Versicherten MUSS beim Erstellen eines AuthorizationKeys für das Ermitteln der Telematik-ID einer Leistungserbringerinstitution oder eines Kostenträger ein Verschlüsselungszertifikat der Institution verwenden.**[<=]**

A_16204-01 - ePA-Frontend des Versicherten: AuthorizationKey erstellen - Verschlüsselungszertifikate Gültigkeit online prüfen
Das ePA-Frontend des Versicherten MUSS beim Erstellen eines AuthorizationKey alle verwendeten Verschlüsselungszertifikate prüfen und den Anwendungsfall abbrechen, wenn das Zertifikat in der Prüfung abgelehnt wurde oder der Sperrstatus nicht ermittelt werden konnte.**[<=]**

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

A_15328-01 - ePA-Frontend des Versicherten: AuthorizationKey erstellen - Berechtigungstyp DOCUMENT_AUTHORIZATION
Das ePA-Frontend des Versicherten MUSS beim Erstellen eines AuthorizationKey den `AuthorizationType` = DOCUMENT_AUTHORIZATION setzen, wenn dem zu Berechtigenden Zugriff auf Dokumente in der Dokumentenverwaltung gewährt werden soll.**[<=]**

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

A_17995-02 - ePA-Frontend des Versicherten: AuthorizationKey erstellen - Akten- und Kontextschlüssel verschlüsseln
Das ePA-Frontend des Versicherten MUSS beim Erstellen eines AuthorizationKeys den Akten- und Kontextschlüssel mit den von der Schlüsselableitung mit SGD 1 und SGD 2 erhaltenen symmetrischen Schlüssel gemäß [gemSpec_SGD_ePA] und [gemSpec_Krypt] verschlüsseln.

ENTWURF

Tabelle 20: TAB_FdV_179 – Akten- und Kontextschlüssel verschlüsseln

Plattformbaustein PL_TUC_SYMM_ENCIPHER nutzen	Eingangsdaten: • Doc: Klartextpräsentation von Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel) • Cert: aus SGD1 abgeleiteter symmetrischer Schlüssel • AD: Berechnung siehe gemSpec_SGD_ePA A_17930 Rückgabedaten: • Doc_{enc} Mit Doc_{enc} und AD_{SGD1} wird eine Struktur gemäß [gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht] gebildet -> $Doc_{enc}1$
Plattformbaustein PL_TUC_SYMM_ENCIPHER nutzen	Eingangsdaten: • Doc: $Doc_{enc}1$ • Cert: aus SGD2 abgeleiteter symmetrischer Schlüssel • AD: Berechnung siehe gemSpec_SGD_ePA A_17930 Rückgabedaten: • Doc_{enc} Mit Doc_{enc}, AD_{SGD1} und AD_{SGD2} wird der EncryptedKeyContainer des AuthorizationKey gebildet.

[<=]

6.2.3.8.4 AuthorizationKey entschlüsseln

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

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

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

ENTWURF

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

A_17843 - ePA-Frontend des Versicherten: Akten- und Kontextschlüssel entschlüsseln
Das ePA-Frontend des Versicherten MUSS beim Entschlüsseln des Akten- und Kontextschlüssel die bei der Schlüsselableitung mit SGD 1 und SGD 2 erhaltenen symmetrischen Schlüssel gemäß [gemSpec_SGD_ePA] und [gemSpec_Krypt] nutzen.

Tabelle 21: TAB_FdV_180 – Akten- und Kontextschlüssel entschlüsseln

Plattformbaustein PL_TUC_SYMM_DECIPHER nutzen	Eingangsdaten: • Doc_{enc}: EncryptedKeyContainer\Ciphertext aus AuthorizationKey • Cert: aus SGD2 abgeleiteter symmetrischer Schlüssel • AD: SGD2 Anteil aus EncryptedKeyContainer\AssociatedData aus AuthorizationKey Rückgabedaten: • Doc: $Doc_{enc}1$ = einfach symmetrisch verschlüsselter Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht)
Plattformbaustein PL_TUC_SYMM_DECIPHER nutzen	Eingangsdaten: • Doc_{enc}: EncryptedKeyContainer\Ciphertext aus $Doc_{enc}1$ • Cert: aus SGD1 abgeleiteter symmetrischer Schlüssel • AD: EncryptedKeyContainer\AssociatedData aus $Doc_{enc}1$ Rückgabedaten: • Doc: Klartextpräsentation von Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel)

[<=]

6.2.3.9 Schlüsselmaterial aus ePA-Aktensystem laden

Mit dieser Operation wird die Autorisierung eines Nutzers des FdV für ein Aktenkonto geprüft und die Schlüssel eines berechtigten Nutzers (bspw. Aktenkontoinhaber, berechtigter Vertreter, LEI) für den Zugriff auf die Dokumentenverwaltung heruntergeladen.

ENTWURF

A_15330-01 - ePA-Frontend des Versicherten: Schlüsselmaterial aus ePA-Aktensystem laden

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

Tabelle 22: TAB_FdV_116 – Schlüsselmaterial aus ePA-Aktensystem laden

Vorbedingung	AuthenticationAssertion liegt in Session-Daten vor
`I_Authorization_Insurant::getAuthorizationKey` Request erstellen	Eingangsparameter: • `AuthenticationAssertion` aus Session-Daten • `RecordIdentifier` aus Session-Daten • `DeviceID` aus Gerät-Daten
`I_Authorization_Insurant::getAuthorizationKey` Response verarbeiten	Rückgabedaten: • AuthorizationKey • AuthorizationAssertion Beinhaltet der Response keinen AuthorizationKey und keine AuthorizationAssertion, wird die Aktivität abgebrochen. Beinhaltet der Response einen AuthorizationKey und eine AuthorizationAssertion wird versucht, das Element (verschlüsseltes Schlüsselpaar) aus `EncryptedKeyBackup` zu entschlüsseln. (siehe Kapitel "6.2.3.8.4-AuthorizationKey entschlüsseln ") Liefert das Entschlüsseln einen Fehler, dann stehen die Informationen RecordKey und ContextKey nicht für die weitere Verarbeitung zur Verfügung. Die Aktivität wird nicht abgebrochen.

ENTWURF

Nachbedingung	Nach Abarbeitung der Aktivität stehen folgende Informationen bereit: • AuthorizationKey (optional) • AuthorizationAssertion (optional) • RecordKey (optional) • ContextKey (optional) • Status der Entschlüsselung Authorization Key (erfolgreich/nicht erfolgreich)

[<=]

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

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

6.2.3.10 Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden

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

A_17130-01 - ePA-Frontend des Versicherten: Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden
Das ePA-Frontend des Versicherten MUSS die Aktivität "Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden" gemäß TAB_FdV_163 umsetzen.

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

`I_Authorization_Management_Insurant::getAuthorizationList` Request erstellen	Eingangsparameter: • `AuthenticationAssertion` aus Session-Daten • `RecordIdentifier` aus Session-Daten • `DeviceID` aus Geräte-Daten
`I_Authorization_Management_Insurant::getAuthorizationList` Response verarbeiten	Rückgabedaten: • Liste von AuthorizationKeys

[<=]

ENTWURF

6.2.3.11 Schlüsselmaterial im ePA-Aktensystem speichern

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

A_15331-01 - ePA-Frontend des Versicherten: Schlüsselmaterial im ePA-Aktensystem speichern
Das ePA-Frontend des Versicherten MUSS die Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" gemäß TAB_FdV_117 umsetzen.

Tabelle 24: TAB_FdV_117 – Schlüsselmaterial im ePA-Aktensystem speichern

`I_Authorization_Management_Insurant::putAuthorizationKey` Request erstellen	Eingangsparameter: • `AuthenticationAssertion` aus Session-Daten • `RecordIdentifier` aus Session-Daten • `AuthorizationKey` • `DeviceID` aus Geräte-Daten • optional: `NotificationInfoRepresentative`
`I_Authorization_Management_Insurant::putAuthorizationKey` Response verarbeiten	HTTP OK ohne SOAP-Response oder gematik Fehlermeldung Für Fehler KEY_ERROR siehe A_15874-01

[<=]

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

A_15332-01 - ePA-Frontend des Versicherten: Schlüsselmaterial im ePA-Aktensystem speichern KEY_ERROR
Das ePA-Frontend des Versicherten MUSS, wenn die Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" den Fehler KEY_ERROR liefert, einmalig den Anwendungsfall nicht abbrechen, das bereits hinterlegte Schlüsselmaterial mit der Aktivität "Schlüsselmaterial im ePA-Aktensystem löschen" löschen und die Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" wiederholen.**[<=]**

ENTWURF

6.2.3.12 Schlüsselmaterial im ePA-Aktensystem ersetzen

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

A_15333-01 - ePA-Frontend des Versicherten: Schlüsselmaterial im ePA-Aktensystem ersetzen
Das ePA-Frontend des Versicherten MUSS die Aktivität "Schlüsselmaterial im ePA-Aktensystem ersetzen" gemäß TAB_FdV_118 umsetzen.

Tabelle 25: TAB_FdV_118 – Schlüsselmaterial im ePA-Aktensystem ersetzen

`I_Authorization_Management_Insurant::replaceAuthorizationKey` Request erstellen	Eingangsparameter: • `AuthenticationAssertion` aus Session-Daten • `RecordIdentifier` aus Session-Daten • `NewAuthorizationKey` • `DeviceID` aus Gerät-Daten
`I_Authorization_Management_Insurant::replaceAuthorizationKey` Response verarbeiten	HTTP OK ohne SOAP-Response oder gematik Fehlermeldung

[<=]

6.2.3.13 Schlüsselmaterial im ePA-Aktensystem löschen

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

A_15334-01 - ePA-Frontend des Versicherten: Schlüsselmaterial im ePA-Aktensystem löschen
Das ePA-Frontend des Versicherten MUSS die Aktivität "Schlüsselmaterial im ePA-Aktensystem löschen" gemäß TAB_FdV_119 umsetzen.

Tabelle 26: TAB_FdV_119 – Schlüsselmaterial im ePA-Aktensystem löschen

`I_Authorization_Management_Insurant::deleteAuthorizationKey` Request erstellen	Eingangsparameter: • `AuthenticationAssertion` aus Session-Daten • `RecordIdentifier` aus Session-Daten • `ActorID` • `DeviceID` aus Gerät-Daten

ENTWURF

`I_Authorization_Management_Insurant::deleteAuthorizationKey` Response verarbeiten	HTTP OK ohne SOAP-Response oder gematik Fehlermeldung

[<=]

6.2.3.14 Leistungserbringerinstitution im Verzeichnisdienst der TI finden

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

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

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

A_15335 - ePA-Frontend des Versicherten: Search Operation mittels LDAP-Directory Basisdatensatz Attribut
Das ePA-Frontend des Versicherten MUSS es dem Versicherten ermöglichen, Leistungserbringerinstitutionen über Suchkriterien gemäß TAB_FdV_120 zu suchen.

Tabelle 27: TAB_FdV_120 – Suchkriterien LDAP Search

Suchkriterium	Beschreibung für die Suche nach Heilberuflern	Beschreibung der Suche nach Leistungserbringerinstitutionen	LDAP-Directory Basisdatensatz Attribut
Vollständiger Name	Der commonName enthält den vollständigen Namen des Inhabers, ohne akademischen Titel	Name der Institution (erste zwei Zeilen des Anschriftenfeldes)	cn
Vorname	Vorname Heilberufler		givenName
Nachname/Institutionsname	Nachname Heilberufler		sn
Anzeigename	Nachname, Vorname des Heilberuflers	Name der Organisation/Einrichtung des Gesundheitswesens	displayName

ENTWURF

Titel	Der Titel des LE (z.B. Dr. med)		title
Institutionsname	Die Bezeichnung der Organisation des Gesundheitswesens (z.B. Arztpraxis Dr. Mustermann)	Name der Organisation/Einrichtung des Gesundheitswesens	organization
Strasse, Hausnummer	Straße, Hausnummer	Straße, Hausnummer	streetAddress
Postleitzahl	Postleitzahl	Postleitzahl	postalCode
Ort	Ort	Ort	localityName
Bundesland	Bundesland	Bundesland	stateOrProvinceName
Langname	Für die Verwendung von überlangen Namen von Heilberuflern	Für die Verwendung von überlangen Namen von Institutionen, z.B. Praxisgemeinschaften unter Aufzählung aller beteiligten Ärzte	otherName
Institution/Berufsgruppe	Berufsgruppe	Institution	professionOID
Fachgebiet	medizinisches Fachgebiet	Fachabteilung	specialization
TelematikID	Eindeutige ID des Heilberuflers in der TI	Eindeutige ID der Institution in der TI	telematikID

[<=]

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

ENTWURF

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

A_17435-01 - ePA-Frontend des Versicherten: LEI in Verzeichnisdienst der TI finden
Das ePA-Frontend des Versicherten MUSS die Leistungserbringerinstitutionen mittels der Aktivität "Suchanfrage Verzeichnisdienst der TI" ermitteln, wobei mindestens als Suchkriterium (`professionOID aus {[gemSpec_VZD#Tab_VZD_Mapping_Eintragstyp Eingangstyp 3]}`) zu verwenden ist.**[<=]**

6.2.3.15 Suchanfrage Verzeichnisdienst der TI

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

A_18256-01 - ePA-Frontend des Versicherten: Search Operation mittels LDAP-Directory Basisdatensatz Attribut
Das ePA-Frontend des Versicherten MUSS für eine Suchanfrage im VZD der TI eine LDAP search Operation basierend auf dem VZD Datenmodell umsetzen.**[<=]**

Für das Datenmodell des LDAP-Verzeichnis siehe [gemSpec_VZD].

A_15336-01 - ePA-Frontend des Versicherten: Suchanfrage Verzeichnisdienst der TI
Das ePA-Frontend des Versicherten MUSS die Aktivität "Suchanfrage Verzeichnisdienst der TI" gemäß TAB_FdV_121 umsetzen.

Tabelle 28: TAB_FdV_121 – Abfrage Verzeichnisdienst

dsmlEnvelopeRequest mit searchRequest erstellen	
`I_Proxy_Directory_Query::Search` Request erstellen	Eingabedaten: • `searchRequest`: Suchanfrage formuliert in DSML
`I_Proxy_Directory_Query::Search` Response verarbeiten	Rückgabedaten: • `searchResponse` gemäß DSML mit Liste von `SearchResultEntry`

[<=]

Für ein Beispiel für eine Suchanfrage und ein Ergebnis siehe [gemSpec_Zugangsgateway_Vers#6.2.2.3 Nutzung].

Die Anzahl der Einträge im Ergebnis der Suchabfrage wird durch den VZD beschränkt. (siehe [gemSpec_VZD#TIP1-A_5552])

Die Anzahl der möglichen Anfragen an den Verzeichnisdienst ist begrenzt (default: 10 Anfragen pro Minute). Wird die Anzahl überschritten, beinhaltet der HTTP-Response des

ENTWURF

Zugangsgateway des Versicherten den HTTP-Statuscode 429 entsprechend RFC6585 Kapitel 4 "`429 Too Many Requests`". Der Response mit dem HTTP-Statuscode 429 stellt keinen Fehler dar. Der Anwendungsfall wird nicht abgebrochen. Das FdV muss den Nutzer informieren, dass der nächste Request erst nach einer Verzögerung möglich ist.

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

Der Name einer Institution wird aus dem Basisdatensatz Attribut `displayName` bestimmt. Die Telematik-ID einer Institution wird aus einem Verschlüsselungszertifikat des Datensatzes bestimmt (siehe [gemSpec_PKI]).

6.2.3.16 PIN-Eingabe für eGK durch Nutzer

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

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

A_15338-01 - ePA-Frontend des Versicherten: PIN-Eingabe für eGK durch Nutzer
Das ePA-Frontend des Versicherten MUSS die Aktivität "PIN-Eingabe durch Nutzer" gemäß TAB_FdV_122 umsetzen.

Tabelle 29: TAB_FdV_122 – PIN-Eingabe durch Nutzer

Plattformbaustein PL_TUC_CARD_VERIFY_PIN	Durch den Plattformbaustein PL_TUC_CARD_INFORMATION wird eine Nutzerverifikation durchgeführt.
Eingangsdaten	• Identifikator = MRPIN.home • Nutzerhinweis für PIN-Eingabe default: "EingabePIN:"
Beschreibung	Der Nutzerhinweis wird bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT im Nutzerinterface (GUI) bzw. bei Nutzung eines Kartenterminal Sicherheitsklasse 3 im Display des Kartenterminals angezeigt.
Rückgabedaten	• OK - PIN erfolgreich verifiziert Es wird mit der folgenden Aktivität fortgefahren

ENTWURF

Varianten/Alternati-ven	• WrongSecretWarning.X - PIN falsch, noch X Versuche Die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN wird dem Nutzer zurückgemeldet. Der Nutzer hat die Wahl die PIN erneut einzugeben oder den Anwendungsfall zu beenden. • PasswordBlocked - PIN ist durch Fehleingaben blockiert Dem Nutzer wird der Anwendungsfall "PIN der eGK entsperren" angeboten.

[<=]

A_15339-01 - ePA-Frontend des Versicherten: Abbruch Anwendungsfall nach fehlgeschlagener Nutzerverifikation
Das ePA-Frontend des Versicherten MUSS, wenn die Nutzerverifikation in der Operation "PIN-Eingabe durch Nutzer" fehlschlägt, den Anwendungsfall abbrechen, in dem die Operation aufgerufen wurde.**[<=]**

6.2.4 Nutzerzugang ePA

6.2.4.1 Login Aktensession

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

Für die Anmeldung des Nutzers mit seiner eGK wird eine 2-Faktor-Authentisierung (eGK + PIN) verwendet. Als weitere Möglichkeit kann die alternative kryptographische Versichertenidentität genutzt werden. Nach erfolgreicher Authentisierung inklusive Gültigkeitsprüfung der eGK und Autorisierung wird das empfängerverschlüsselte Schlüsselmaterial heruntergeladen und das Öffnen des Aktenkontextes in der Komponente "Dokumentenverwaltung" für das referenzierte Aktenkonto durchgeführt.

A_13695-02~~A_13695-01~~ - ePA-Frontend des Versicherten: Login Aktensession
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 1.1 - Login durch einen Versicherten" aus [gemSysL_ePA] gemäß TAB_FdV_123 umsetzen.

Tabelle 30: TAB_FdV_123 – Login Aktensession

Name	Login Aktensession

ENTWURF

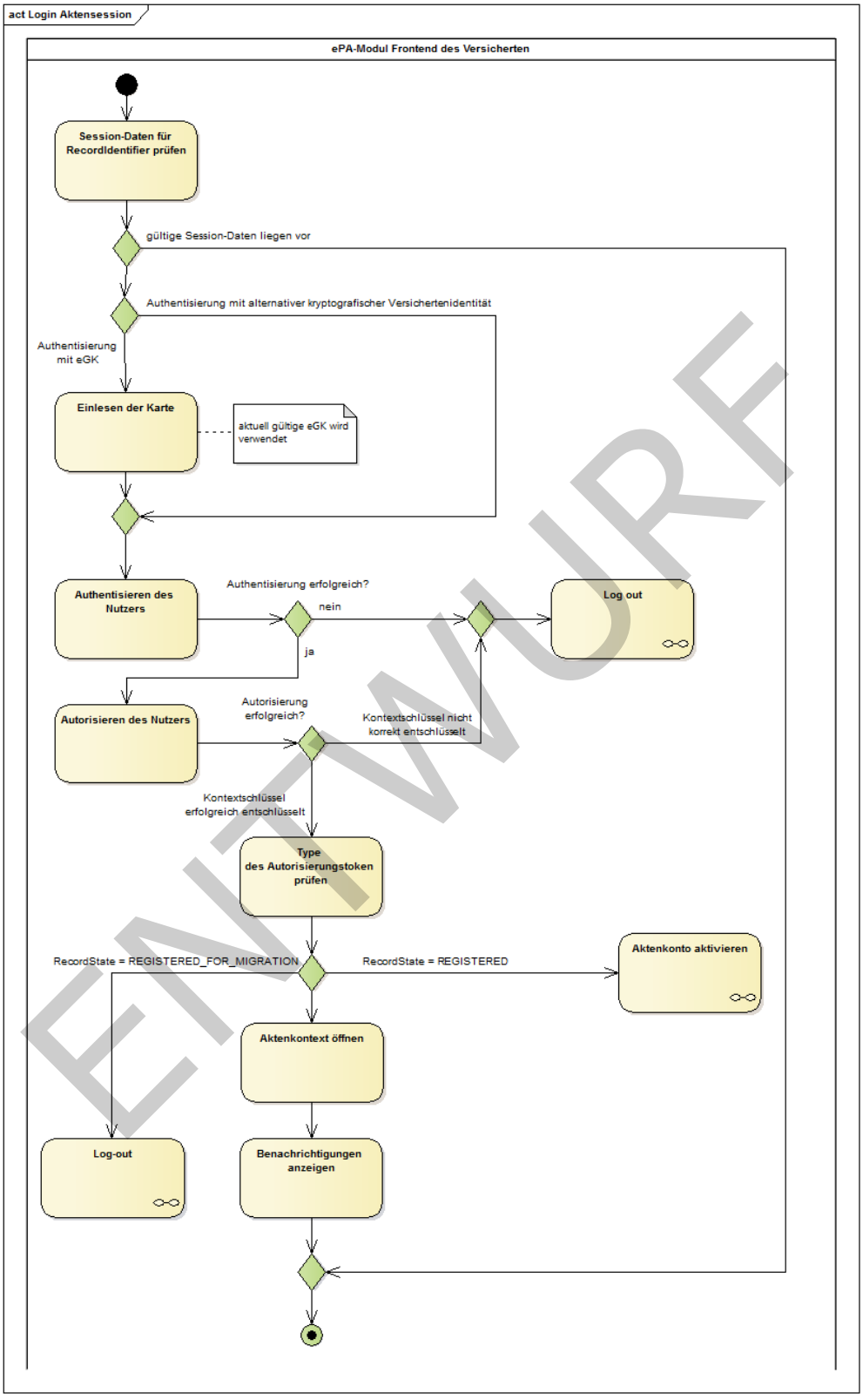
Auslöser	• Der Akteur möchte einen fachlichen Anwendungsfall mit Datenzugriff auf das ePA-Aktensystem ausführen. • optional: explizites Login im Verlauf des Starts des FdV
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	RecordIdentifier des Versicherten oder des zu Vertretenden ist im ePA-Frontend des Versicherten bekannt und ausgewählt. Falls Authentisierung mittels eGK: Die eGK des Nutzers steckt im Kartenleser. Falls Authentisierung mittels alternativer kryptographischer Versichertenidentität: es besteht eine freigeschaltete Verbindung zum Signaturdienst
Nachbedingung	Für die Aktensession liegen gültige Session-Daten im ePA-FdV vor.
Standardablauf	Aktivitäten im Standardablauf 1. Session-Daten für RecordIdentifier prüfen 2. optional: wenn Authentisieren mittels eGK a. Einlesen der Karte 3. Authentisieren des Nutzers 4. Autorisieren des Nutzers 5. Status des Aktenkontos prüfen 6. Aktenkontext öffnen 7. optional: Benachrichtigungen anzeigen
Varianten/Alternativen	Wenn nach der Aktivität "Autorisieren des Nutzers" ein Autorisierungstoken mit `RecordState` = REGISTERED vorliegt, dann wird der Anwendungsfall "Login Aktensession" ohne Fehler abgebrochen und der Anwendungsfall "Aktenkonto aktivieren" gestartet. ~~Wenn nach der Aktivität "Autorisieren des Nutzers" ein Autorisierungstoken mit `RecordState` = REGISTERED_FOR_MIGRATION vorliegt, dann wird der Anwendungsfall "Login Aktensession" abgebrochen, der Nutzer darauf hingewiesen, dass zuerst eine Datenmigration vom Aktenkonto des alten Anbieters durchzuführen ist und der Anwendungsfall "Logout Aktensession" gestartet.~~ In allen – nicht behebbaren – Fehlerfällen wird der Anwendungsfall abgebrochen und der Anwendungsfall "Logout Aktensession" gestartet.

2402 **[<=]**

ENTWURF

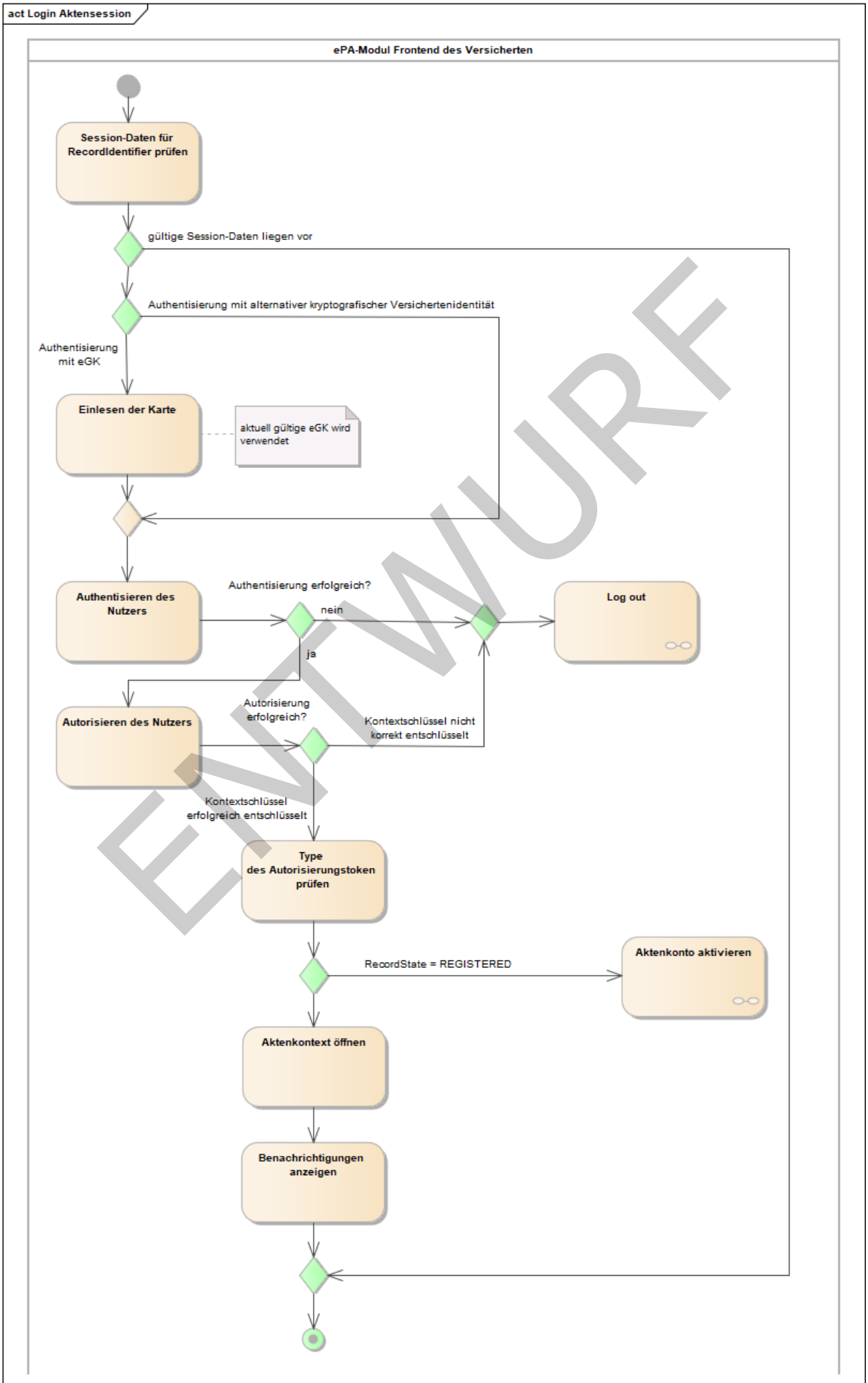
2403
2404

ENTWURF



ENTWURF

2405


act Login Aktensession
ePA-Modul Frontend des Versicherten
Session-Daten für RecordIdentifier prüfen
gültige Session-Daten liegen vor
Authentisierung mit alternativer kryptografischer Versichertenidentität
Authentisierung mit eGK
Einlesen der Karte
aktuell gültige eGK wird verwendet
Authentisieren des Nutzers
Authentisierung erfolgreich?
nein
ja
Log out
Autorisieren des Nutzers
Autorisierung erfolgreich?
Kontextschlüssel nicht korrekt entschlüsselt
Kontextschlüssel erfolgreich entschlüsselt
Type des Autorisierungstoken prüfen
RecordState = REGISTERED
Aktenkonto aktivieren
Aktenkontext öffnen
Benachrichtigungen anzeigen

ENTWURF

Abbildung 4: Aktivitätsdiagramm "Login Aktensession"

A_15340-01 - ePA-Frontend des Versicherten: Login - Session-Daten für RecordIdentifier prüfen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "Login Aktensession" ohne Fehler abbrechen, wenn gültige Session-Daten zu dem RecordIdentifier vorliegen.**[<=]**

Gültige Session-Daten liegen vor, wenn die Session-Daten einen Authentisierungstoken und einen Autorisierungstoken beinhalten. Auf eine Prüfung der zeitlichen Gültigkeit der Token wird verzichtet, da eine Synchronität der Systemzeit in der Ablaufumgebung des ePA-FdV mit der den Token ausstellenden Komponente nicht sichergestellt werden kann. Antwortet das ePA-Aktensystem auf einen Operationsaufruf mit dem Fehler, dass ein Token ungültig ist, dann löscht das ePA-FdV die Token aus den Session-Daten (siehe A_15310-01).

A_15341-01 - ePA-Frontend des Versicherten: Login - Einlesen der Karte
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession", wenn die Authentisierung mittels eGK erfolgt, die Aktivität "Einlesen der Karte" gemäß TAB_FdV_124 umsetzen.

Tabelle 31: TAB_FdV_124 – Login - Einlesen der Karte

Plattformbaustein PL_TUC_CARD_INFORMATION	Durch den Plattformbaustein PL_TUC_CARD_INFORMATION werden Statusinformationen der Karte bereitgestellt.
Eingangsdaten	eGK
Beschreibung	Das ePA-FdV MUSS die Karteninformationen in PL_TUC_CARD_INFORMATION auswerten hinsichtlich • Kartentyp = Typ eGK • Produkttypversion des Objektsystems = G2 oder höher und bei unpassenden Kartendaten den Anwendungsfall mit einem Fehler beenden. Die folgenden Informationen der Karte werden in die Session-Daten übernommen: • C.CH.AUT * • Versicherten-ID

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

A_15342 - ePA-Frontend des Versicherten: Login - Abbruch bei Karte lesen
Das ePA-Frontend des Versicherten MUSS, wenn der Anwendungsfall "Login Aktensession" aufgrund der Prüfungen beim Einlesen der Karte abbricht, den Nutzer darauf hinweisen, seine aktuell gültige eGK zu stecken. **[<=]**

ENTWURF

Authentisieren und Autorisieren

A_15343-01 - ePA-Frontend des Versicherten: Login - Authentisieren des Nutzers
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" die übergreifende Aktivität "Authentisieren des Nutzers" ausführen.**[**<=**]**

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

A_15344-01 - ePA-Frontend des Versicherten: Login - Autorisieren des Nutzers - Schlüsselmaterial aus ePA-Aktensystem laden
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" zum Autorisieren des Nutzers die übergreifende Aktivität "Schlüsselmaterial aus ePA-Aktensystem laden" ausführen. Wenn die Aktivität die Informationen AuthenticationAssertion, AuthorizationAssertion, RecordKey (Aktenschlüssel) oder ContextKey (Kontextschlüssel) liefert, dann werden diese in die Session-Daten übernommen.**[**<=**]**

Aktivieren und Migration

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

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

A_15346-01 - ePA-Frontend des Versicherten: Login - Autorisieren des Nutzers - Aktenkontostatus REGISTERED
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" den Aktenzustand aus dem Autorisierungstoken ermitteln und bei`RecordState = REGISTERED` den Anwendungsfall ohne Fehler abbrechen und den Anwendungsfall "Aktenkonto aktivieren" starten.**[**<=**]**

A_15681-02~~A_15681-01~~ - ePA-Frontend des Versicherten: Login - Autorisieren des Nutzers - Aktenkontostatus REGISTERED_FOR_MIGRATION
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" den Aktenzustand aus dem Autorisierungstoken prüfen und bei`RecordState = REGISTERED_FOR_MIGRATION` nur die Operation I_Account_Management_Insurant::ResumeAccount zum Import des Pakets mit den Daten aus der Akte des Versicherten beim alten Anbieter ermöglichen, alle anderen Anwendungsfällen sind mit einem Fehler abzubrechen. **[**<=~~ den Anwendungsfall mit Fehler abbrechen.~~**[**<=~~**]**

Dem Nutzer soll im Falle dieses Abbruchs ein Hinweis gegeben werden, dass vor der Nutzung des Aktenkontos beim neuen Anbieter eine Migration der Daten aus dem Aktenkonto des alten Anbieters durchgeführt werden muss.

Verbindung zur Dokumentenverwaltung

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

ENTWURF

A_15347-01 - ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Aufbau sicherer Kanal zu Dokumentenverwaltung
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" in der Aktivität "Aktenkontext öffnen" für die Schnittstellen zur Komponente Dokumentenverwaltung das Kommunikationsprotokoll gemäß den Vorgaben aus [gemSpec_Krypt#ePA-spezifische Vorgaben] und [gemSpec_Krypt#Kommunikationsprotokoll zwischen VAU und ePA-Clients] umsetzen. **[<=]**

A_15600-01 - ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Erweiterung des sicheren Verbindungsprotokolls
Das ePA-Frontend des Versicherten MUSS beim Aufbau des sicheren Kanals zur Dokumentenverwaltung die AuthorizationAssertion aus den Session-Daten der vom ePA-Frontend des Versicherten aufgerufenen Operation als Parameter gemäß [gemSpec_Dokumentenverwaltung#A_15592] übergeben.**[<=]**

Das ePA-FdV nutzt den abgeleiteten Sitzungsschlüssel, um alle fachlichen Eingangs- und Ausgangsnachrichten zur Dokumentenverwaltung zu ver- bzw. entschlüsseln. Siehe A_15304-01.

A_15348-01 - ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Operation OpenContext
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" in der Aktivität "Aktenkontext öffnen" das Übersenden des Kontextschlüssels gemäß TAB_FdV_126 umsetzen.

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

Vorbedingung	AuthorizationAssertion und entschlüsselter Kontextschlüssel liegen in Session-Daten vor.
`I_Document_Management_Connect::OpenContext` Request erstellen	Eingangsdaten: • Kontextschlüssel (`ContextKey`) aus Session-Daten
`I_Document_Management_Connect::OpenContext` Response verarbeiten	Rückgabedaten: • OK oder gematik Fehler

[<=]

Benachrichtigungen

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

ENTWURF

A_15350 - ePA-Frontend des Versicherten: Login - Benachrichtigungen anzeigen optional
Das ePA-Frontend des Versicherten MUSS, wenn die Konfiguration Benachrichtigungen aktivieren = nein gesetzt ist, die Aktivitäten zum Anzeigen von Benachrichtigungen ignorieren.**[<=]**

A_15351 - ePA-Frontend des Versicherten: Login - Benachrichtigungen anzeigen unterdrücken
Das ePA-Frontend des Versicherten MUSS, wenn die Konfiguration Benachrichtigungen aktivieren = ja gesetzt ist und der Anwendungsfall "Login Aktensession" nicht zum Start des FdV durchgeführt wird, sondern implizit durch einen anderen Anwendungsfall getriggert wird, beim Nutzer abfragen, ob die Benachrichtigungen angezeigt werden sollen.**[<=]**

A_15352-01 - ePA-Frontend des Versicherten: Login - Protokolldaten Dokumentenverwaltung abfragen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession", wenn die Konfiguration Benachrichtigungen aktivieren = ja gesetzt ist, die Protokolldaten der Komponente Dokumentenverwaltung gemäß A_15352-01 abfragen und das Ergebnis gemäß der Konfiguration Benachrichtigungszeitraum filtern.**[<=]**

A_15353 - ePA-Frontend des Versicherten: Login - Benachrichtigungen-Anzeige
Das ePA-Frontend des Versicherten MUSS eine Anzeige für Benachrichtigungen umsetzten, in der die Protokolleinträge für folgende Zugriffe übersichtlich dargestellt werden:

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

[<=]

Es gilt die folgende Anforderung aus dem Anwendungsfall "Protokolldaten einsehen" für die Darstellung der Benachrichtigung: "A_15495 - ePA-Frontend des Versicherten: Protokolldaten lokal speichern".

A_15354-01 - ePA-Frontend des Versicherten: Konfiguration letzte Anmeldung
Das ePA-Frontend des Versicherten MUSS nach erfolgreichem Login den Wert "Letzte Anmeldung zum Aktenkonto" für das Aktenkonto in den Konfigurationsdaten aktualisieren.**[<=]**

6.2.4.2 Logout Aktensession

Dieser Anwendungsfall beendet eine Aktensession.

A_15355-01 - ePA-Frontend des Versicherten: Logout Aktensession
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 1.3 - Logout durch einen Nutzer" aus [gemSysL_ePA] gemäß TAB_FdV_127 umsetzen.

ENTWURF

Tabelle 33: TAB_FdV_127 – Logout Aktensession

Name	Logout Aktensession
Auslöser	• Aufruf des Anwendungsfalls in der GUI • Der Akteur war innerhalb seiner Aktensession über einen maximalen Zeitraum hinaus inaktiv. • Fehler im Anwendungsfall "Login Aktensession"
Akteur	Versicherter, berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Die Session-Daten sind gelöscht.
Standardablauf	Aktivitäten im Standardablauf 1. Aktenkontext schließen 2. Authentisierungstoken abmelden 3. optional, wenn eine alternative kryptographische Versichertenidentität für die Authentisierung genutzt wurde: Freischaltung des Signaturdienstes beenden 4. Session-Daten löschen

[<=]

A_15356-01 - ePA-Frontend des Versicherten: Logout - Aktenkontext schließen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Logout Aktensession", wenn ein sicherer Kanal zur Dokumentenverwaltung aufgebaut und der Aktenkontext erfolgreich geöffnet wurde, die Aktivität "Aktenkontext schließen" gemäß TAB_FdV_128 umsetzen.

Tabelle 34: TAB_FdV_128 – Logout - Aktenkontext schließen

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

[<=]

ENTWURF

A_17542-01 - ePA-Frontend des Versicherten: Logout - Authentisierungstoken abmelden
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Logout Aktensession", wenn ein Authentisierungstoken in den Session-Daten gespeichert ist, die Aktivität "Authentisierungstoken abmelden" gemäß TAB_FdV_172 umsetzen.

Tabelle 35: TAB_FdV_172 – Logout - Authentisierungstoken abmelden

Vorbedingung	AuthenticationAssertion in Session-Daten
`I_Authentication_Insurant::LogoutToken` Request erstellen	Eingangsdaten: • CancelTarget: `AuthenticationAssertion` aus Session-Daten
`I_Authentication_Insurant::LogoutToken` Response verarbeiten	Keine Verarbeitung notwendig

[<=]

A_17766-01 - ePA-Frontend des Versicherten: Logout - Freischaltung des Signaturdienstes beenden
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Logout Aktensession", wenn für die Authentisierung eine alternative kryptographische Versichertenidentität genutzt wurde und die Schnittstelle`I_Remote_Sign_Operations::sign_Data` freigeschaltet wurde, den Signaturdienst aufrufen, um eine Freischaltung des Signaturdienstes für den Nutzer zu beenden.**[<=]**

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

A_15358-01 - ePA-Frontend des Versicherten: Logout - Session-Daten löschen
Das ePA-Frontend des Versicherten MUSS zum Abschluss des Anwendungsfall "Logout Aktensession" alle Session-Daten aus dem lokalen Speicher löschen.**[<=]**

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

6.2.5 Aktenkontoverwaltung

6.2.5.1 Aktenkonto aktivieren

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

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

A_15359 - ePA-Frontend des Versicherten: Aktenkonto aktivieren über GUI
Das ePA-Frontend des Versicherten MUSS, wenn der Versicherte den Anwendungsfall "Aktenkonto aktivieren" über die GUI auswählt, den Anwendungsfall "Login Aktensession" starten.**[<=]**

ENTWURF

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

A_15360-01 - ePA-Frontend des Versicherten: Aktenkonto aktivieren
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 2.1 - Aktenkonto einrichten" aus [gemSysL_ePA] gemäß TAB_FdV_130 umsetzen.

Tabelle 36: TAB_FdV_130 – Aktenkonto aktivieren

Name	Aktenkonto aktivieren
Auslöser	• über Anwendungsfall "Login Aktensession"
Akteur	Versicherter
Vorbedingung	In den Session-Daten liegt ein Authentisierungstoken und ein Autorisierungstoken mit `RecordState` = REGISTERED vor.
Nachbedingung	Das Aktenkonto ist aktiviert. Es können fachliche Anwendungsfälle mit dem Aktenkonto durchgeführt werden.
Standardablauf	Aktivitäten im Standardablauf 1. Aktenschlüssel erzeugen 2. Kontextschlüssel erzeugen 3. AuthorizationKey erzeugen 4. Schlüsselmaterial in ePA-Aktensystem laden 5. Schlüsselmaterial aus ePA-Aktensystem laden 6. Aktenkontext öffnen

[<=]

A_15362-01 - ePA-Frontend des Versicherten: Aktenkonto aktivieren - Aktenschlüssel erzeugen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Aktenkonto aktivieren" den Aktenschlüssel erzeugen.**[<=]**

A_15363-01 - ePA-Frontend des Versicherten: Aktenkonto aktivieren - Kontextschlüssel erzeugen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Aktenkonto aktivieren" den Kontextschlüssel erzeugen.**[<=]**

Für das Erzeugen von Schlüsseln ist [gemSpec_Krypt#GS-A_4368 - Schlüsselerzeugung] und [gemSpec_Krypt#A_15705 - Vorgaben Aktenschlüssel (RecordKey) und Kontextschlüssel (ContextKey)] zu beachten.

ENTWURF

A_15364-01 - ePA-Frontend des Versicherten: Aktenkonto aktivieren - AuthorizationKey erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Aktenkonto aktivieren" einen AuthorizationKey mit

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

für den Versicherten erstellen.**[<=]**

A_15365-01 - ePA-Frontend des Versicherten: Aktenkonto aktivieren - Schlüsselmaterial im ePA-Aktensystem speichern
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Aktenkonto aktivieren" für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey` = erstellter AuthorizationKey ausführen. Der optionale Parameter `NotificationInfoRepresentative` wird nicht belegt.**[<=]**

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

Das Laden des Schlüsselmaterial aus ePA-Aktensystem laden erfolgt gemäß A_15344-01.

Das Öffnen des Aktenkontext erfolgt gemäß A_15347-01 und A_15348-01.

6.2.5.2 Anbieter wechseln

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

- Kündigung des bestehenden Aktenkontos beim alten Anbieter
- Registrierung eines neuen Aktenkontos bei einem neuen Anbieter
- Bestätigung vom neuen Anbieter erhalten, dass das neue Aktenkonto zur Datenübernahme vorbereitet ist
- Übernahme der Daten vom Aktenkonto des alten Anbieters zum neuen Anbieter im FdV

A_15369 - ePA-Frontend des Versicherten: Anbieter wechseln - Hinweis Verwaltungsprotokoll
Das ePA-Frontend des Versicherten MUSS vor Start des Anwendungsfalls "Anbieter wechseln" den Versicherten darauf hinweisen, dass das Verwaltungsprotokoll nicht zum neuen Anbieter übertragen wird, der Versicherte sich das Verwaltungsprotokoll lokal speichern muss, falls es weiterhin verfügbar sein soll und dem Versicherten ermöglichen den Anwendungsfall "Protokolldaten einsehen" zu starten.**[<=]**

A_15371 - ePA-Frontend des Versicherten: Anbieter wechseln - Informationen zu neuen Anbieter
Das ePA-Frontend des Versicherten MUSS dem Versicherten ermöglichen, die folgenden Registrierungsinformationen des neuen Anbieters zu erfassen:

- Akten-ID
- FQDN des Anbieter

ENTWURF

[<=]

A_15372 - ePA-Frontend des Versicherten: Anbieter wechseln - Zugriffsberechtigungen anzeigen und Umzug bestätigen
Das ePA-Frontend des Versicherten MUSS dem Versicherten die zugriffsberechtigten Leistungserbringerinstitutionen, Vertreter und Kostenträger aus dem ePA-Aktensystem des alten Anbieters anzeigen und dem Versicherten die Möglichkeit geben, zu entscheiden, ob die bestehenden Berechtigungen in das ePA-Aktensystem des neuen Anbieters übernommen werden sollen.**[<=]**

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

A_15370-01 - ePA-Frontend des Versicherten: Anbieter wechseln
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 2.5 - Anbieter wechseln" aus [gemSysL_ePA] gemäß TAB_FdV_131 umsetzen.

Tabelle 37: TAB_FdV_131 – Anbieter wechseln

Name	Anbieter wechseln
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter
Vorbedingung	Der Versicherte hat ein neues Aktenkonto bei einem anderen Anbieter eröffnet. Das neue Aktenkonto ist bereit für den Datenimport. Der Versicherte ist im Aktenkonto des alten Anbieters angemeldet. Aktenschlüssel und Kontextschlüssel liegen unverschlüsselt in den Session-Daten vor. Der Versicherte hat die Registrierungsinformationen des neuen Anbieters erfasst. Der Versicherte hat eine Auswahl getroffen, ob die Zugriffsberechtigungen zum neuen Anbieter übernommen werden sollen.
Nachbedingung	Das Aktenkonto beim alten Anbieter befindet sich im Status „suspended". Es ist nur noch ein lesender Zugriff möglich. Der neue Anbieter ist informiert, dass zeitnah ein Transferpaket für den Import in das Aktenkonto vom alten Anbieter bereitgestellt wird. Die Berechtigungen sind ggf. vom Aktenkonto des alten in das des neuen Anbieters übernommen.

ENTWURF

Standardablauf	Aktivitäten im Standardablauf 1. Altes Aktenkonto in Exportzustand versetzen 2. Login beim Anbieter des neuen Aktenkontos 3. Daten in neues Aktenkonto importieren 4. Schlüsselmaterial für Versicherten in ePA-Aktensystem laden 5. Autorisierung aktualisieren 6. optional für jeden Berechtigten: Schlüsselmaterial im ePA-Aktensystem speichern

[<=]

ENTWURF

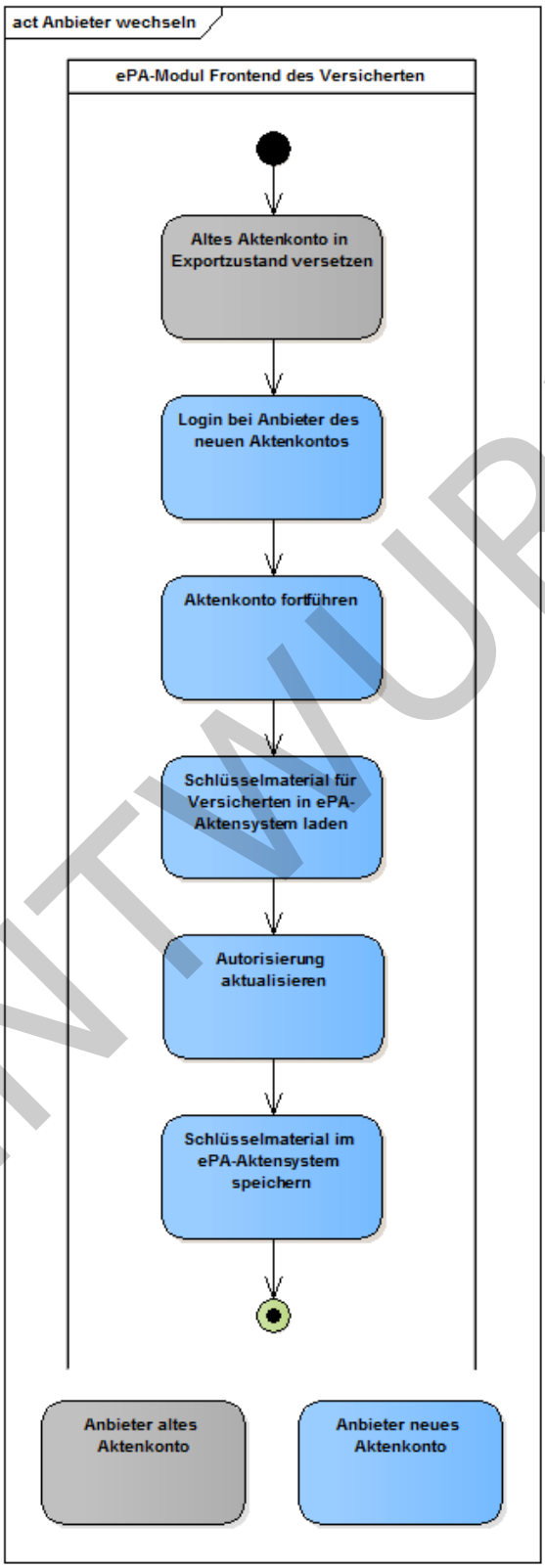


Abbildung 5: Aktivitätsdiagramm "Anbieter wechseln"

ENTWURF

A_15377-01 - ePA-Frontend des Versicherten: Anbieter wechseln - Aktenkonto in Exportzustand versetzen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" die Aktivität "Aktenkonto in Exportzustand versetzen" gemäß TAB_FdV_132 umsetzen.

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

`I_Account_Management_Insurant::SuspendAccount` Request erstellen	Eingangsparameter: • `AuthenticationAssertion` aus Session-Daten
`I_Account_Management_Insurant::SuspendAccount` Response verarbeiten	Rückgabedaten: • `PackageURL` Die URL ist ein Link auf ein Transportpaket, über den der Anbieter des neuen Aktenkontos ein Paket mit den Akteninhalten vom alten Anbieter herunterladen kann.

[<=]

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

A_15378-01 - ePA-Frontend des Versicherten: Anbieter wechseln - Login neues Aktenkonto
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" die folgenden Aktivitäten aus dem Anwendungsfall "Login Aktensession" mit den Daten des Aktenkontos beim neuen Anbieter ausführen, um sich beim neuen Aktenkonto einzuloggen:

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

[<=]

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

Die Autorisierung des Nutzers erfolgt gemäß A_15344-01. Die Operation getAuthorizationKeys liefert ein Autorisierungstoken mit `RecordState` = REGISTERED_FOR_MIGRATION und kein Schlüsselmaterial.

Der Aufbau des sicheren Kanals zur Dokumentenverwaltung erfolgt gemäß A_~~15374-01~~.15347-*.

ENTWURF

Das Öffnen des Aktenkontextes erfolgt gemäß A_15348-01 unter Nutzung des Autorisierungstoken mit `RecordState` = REGISTERED_FOR_MIGRATION und dem Kontextschlüssel des Aktenkontos des alten Anbieters.

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

A_15379-01 - ePA-Frontend des Versicherten: Anbieter wechseln - Aktenkonto fortführen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" die Aktivität "Aktenkonto fortführen" gemäß TAB_FdV_133 beim Aktenkonto des neuen Anbieters umsetzen.

Tabelle 39: TAB_FdV_133 – Anbieter wechseln - Aktenkonto fortführen

`I_Account_Management_Insurant::ResumeAccount` Request erstellen	Eingangsparameter: • `PackageURL` aus suspendAccount Operation • `AuthenticationAssertion` aus Session-Daten
`I_Account_Management_Insurant::ResumeAccount` Response verarbeiten	Rückgabedaten: • HTTP OK oder gematik SOAP-Fault

[<=]

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

A_15374-01 - ePA-Frontend des Versicherten: Anbieter wechseln - AuthorizationKey für Aktenkontoinhaber erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" einen AuthorizationKey mit dem für den Versicherten gesicherten Aktenschlüssel und Kontextschlüssel sowie`AuthorizationType` = DOCUMENT_AUTHORIZATION für den Versicherten erstellen.**[<=]**

A_15375-01 - ePA-Frontend des Versicherten: Anbieter wechseln - Schlüsselmaterial für Aktenkontoinhaber im ePA-Aktensystem speichern
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem des neuen Anbieters die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey` = erstellter AuthorizationKey ausführen. Der optionale Parameter `NotificationInfoRepresentative` wird nicht belegt.**[<=]**

Nach erfolgreichem Aufruf dieser Operation ist das Aktenkonto aktiviert.

Nach erfolgreichem Aktivieren des Aktenkontos wird der Autorisierungstoken aktualisiert. Dies erfolgt durch das Laden des Schlüsselmaterial aus ePA-Aktensystem gemäß A_15344-01.

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

ENTWURF

A_15598-01 - ePA-Frontend des Versicherten: Anbieter wechseln - Berechtigung LEI und KTR erteilen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln", wenn die Berechtigungen in das Aktenkonto des neuen Anbieters übernommen werden sollen, für jede aus dem Aktenkonto des alten Anbieters ermittelte Berechtigung einer LEI und KTR einen AuthorizationKey erstellen und das Schlüsselmaterial in das ePA-Aktensystem des neuen Anbieters laden. **[<=]**

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

A_15635 - ePA-Frontend des Versicherten: Anbieter wechseln - Benachrichtigungsadresse Vertreter erfassen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer im Anwendungsfall "Anbieter wechseln" ermöglichen, wenn die Berechtigungen in das Aktenkonto des neuen Anbieters übernommen werden sollen, für jeden Vertreter die Benachrichtigungsadresse für den Geräteautorisierung zu erfassen.**[<=]**

A_15636-01 - ePA-Frontend des Versicherten: Anbieter wechseln - Berechtigung Vertreter erteilen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall „Anbieter wechseln", wenn die Berechtigungen in das Aktenkonto des neuen Anbieters übernommen werden sollen und die Benachrichtigungsadresse des Vertreters für die Geräteautorisierung bekannt ist, für jede aus dem Aktenkonto des alten Anbieters heruntergeladene Berechtigung eines Vertreters das Schlüsselmaterial in das ePA-Aktensystem laden.**[<=]**

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

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

6.2.5.3 Schließen einer Akte

Der Versicherte hat jederzeit das Recht, seine ePA endgültig zu schließen.

A_21128 - Hinweis im FdV zur selbstständigen Sicherung der Protokolle bei Schließen der Akte
Falls das ePA-FdV dem Nutzer eine Funktion zum Schließen seiner Akte anbietet, MUSS das eA-FdV beim Schließen einer Akte über das ePA-FdV den Versicherten darauf hinweisen, seine Protokolldaten aus der Akte für eine weitere Verwendung selbstständig zu exportieren, da diese nach Schließen der Akte im Aktensystem nur noch eingeschränkt und nicht mehr vollständig für datenschutzrechtliche Auskünfte zur Verfügung stehen. Der Versicherte MUSS auf die Möglichkeit des signierten Exports der Protokolle hingewiesen werden.**[<=]**

A_21129 - Revisionssicherer Export der Protokolle
Das ePA-FdV MUSS dem Nutzer eine Funktion zum Export signierter Protokolldaten aus der Akte unter Nutzung der Operationen

ENTWURF

I_Authentication_Insurant::getSignedAuditEvents (nur wenn der Nutzer der Kontoinhaber ist), I_Authorization_Management_Insurant:: getSignedAuditEvents und I_Account_Management_Insurant::getSignedAuditEvents bereitstellen.[<=]

6.2.6 Umschlüsselung

Dieses Kapitel beschreibt den Anwendungsfall Umschlüsselung. In den folgenden Abbildungen ist in einem Sequenzdiagramm der Ablauf der Umschlüsselung mit den einzelnen Akteuren ePA-FdV, Autorisierung, Dokumentenverwaltung und SGD1/2 dargestellt. Grün eingefärbte Pfeile bezeichnen signierte Rückgabewerte. Die Signaturen werden bei der Weiterleitung der Rückgabewerte mit an den Empfänger geleitet. Dieser validiert nach Empfang des Wertes und der Signatur diese auf Gültigkeit und darauf, dass der Signaturerstellungszeitpunkt nicht zu weit in der Vergangenheit liegt.

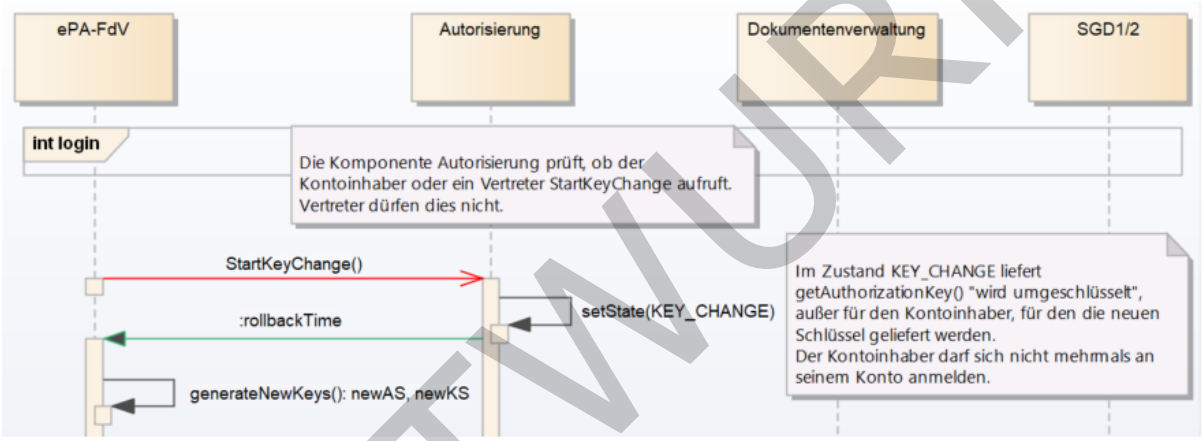


Abbildung 6: Umschlüsselung I

ENTWURF

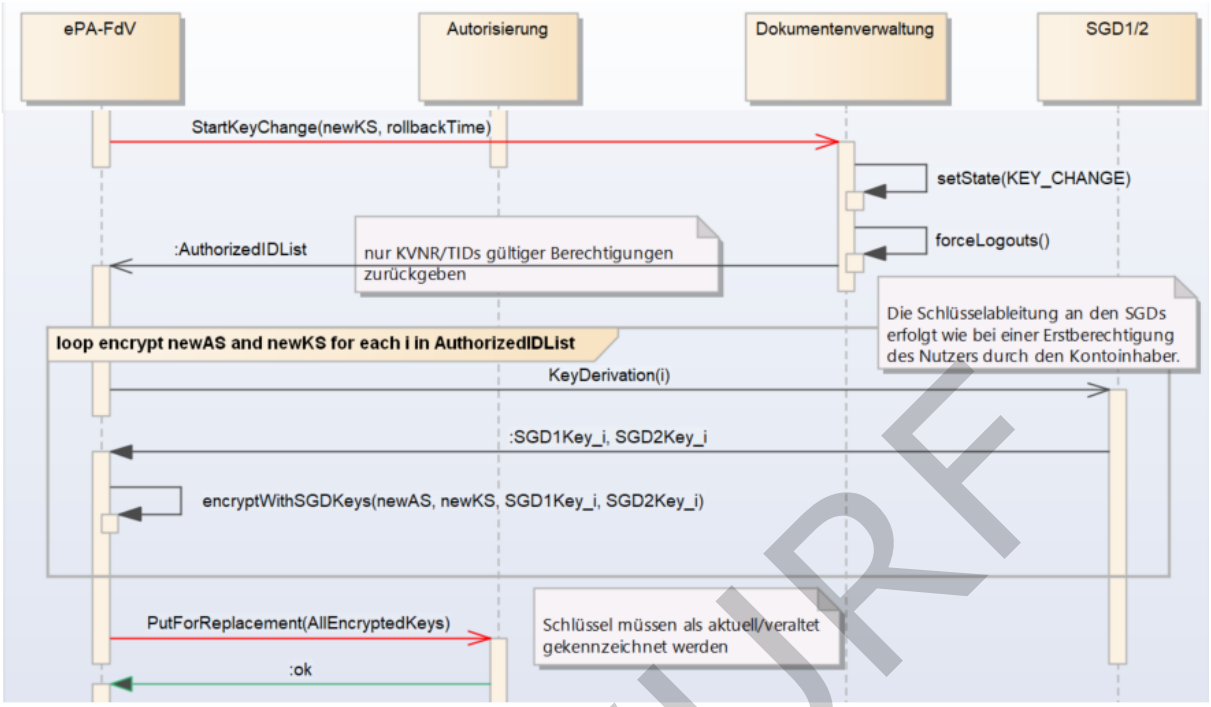


Abbildung 7: Umschlüsselung II

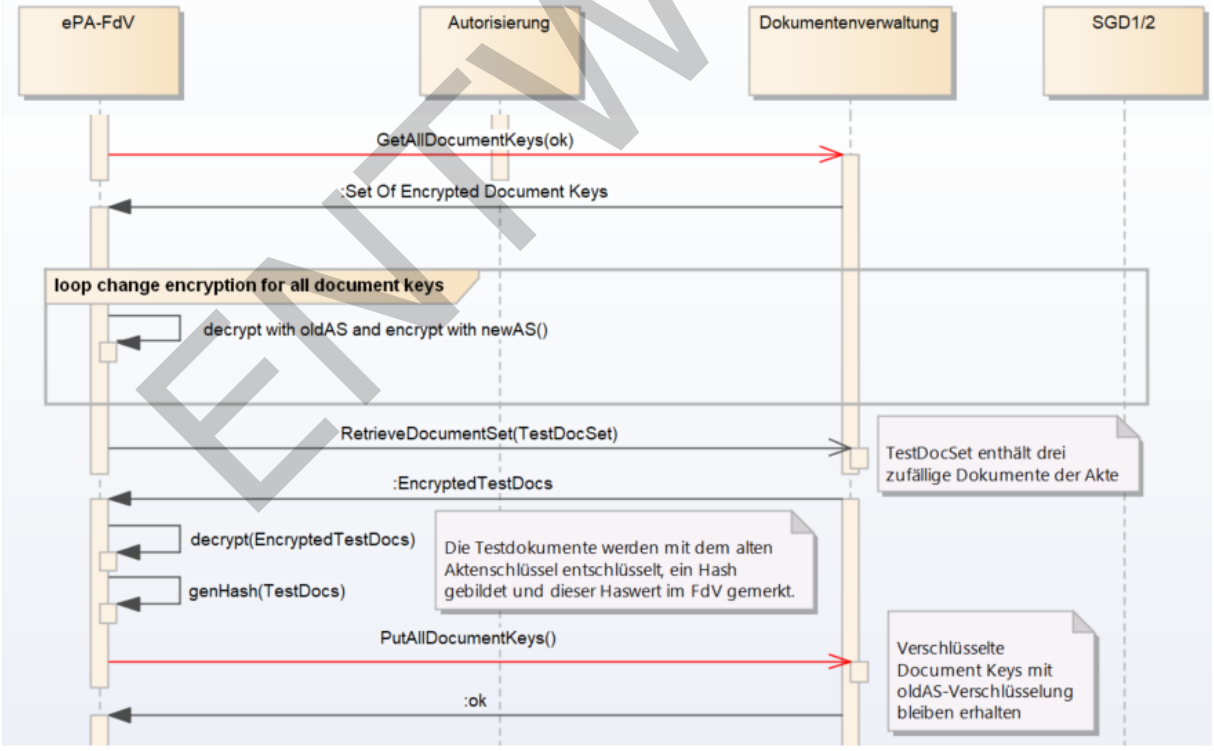
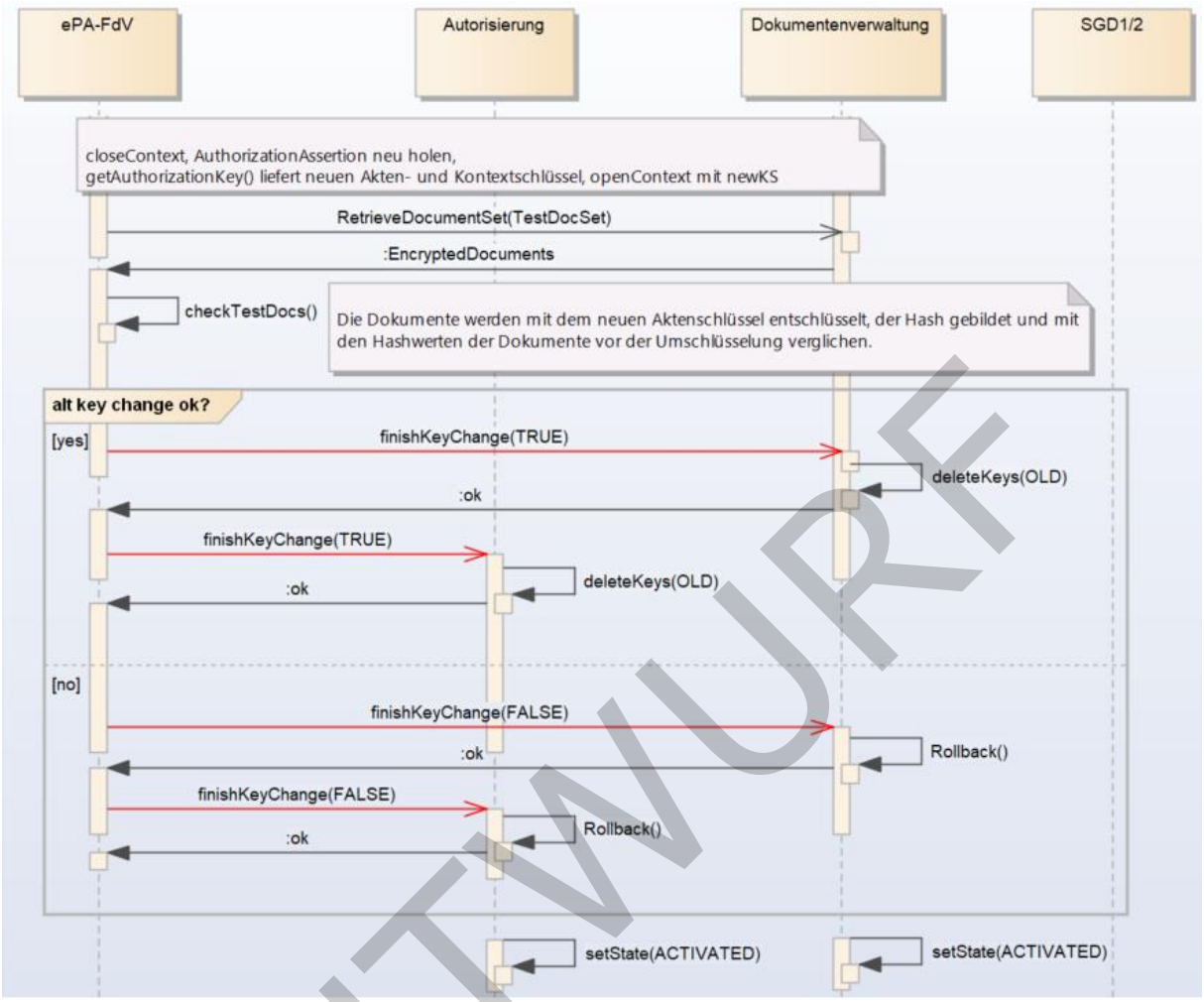


Abbildung 8: Umschlüsselung III

ENTWURF



2822

ENTWURF

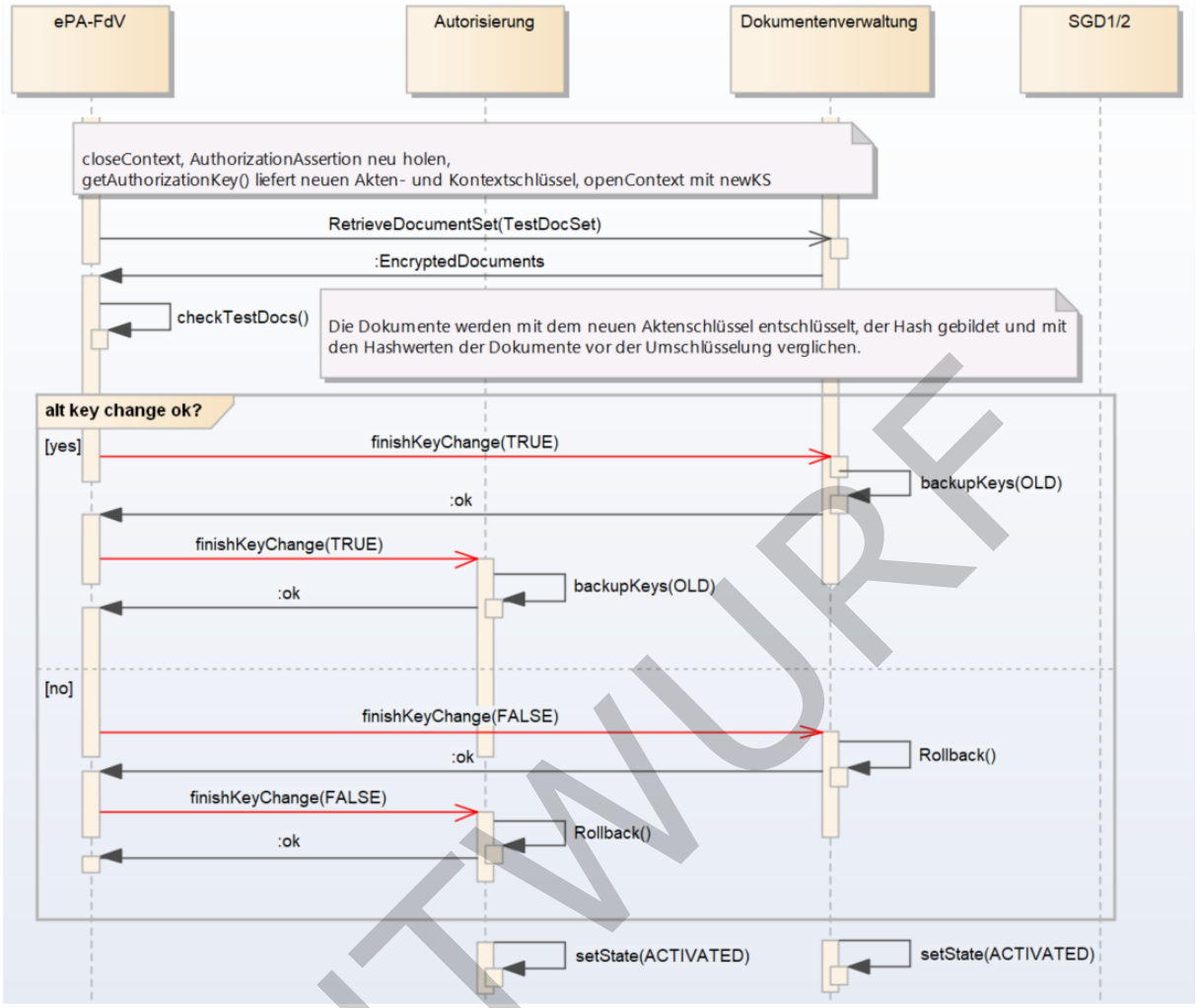


Abbildung 9: Umschlüsselung IV

A_20507 - ePA-Frontend des Versicherten: Funktions-Timeout für Aufrufe an das Aktensystem, die Autorisierungskomponente und die Schlüsselgenerierungsdienste SGD1 und SGD2

Das ePA-Frontend des Versicherten MUSS während der Umschlüsselung bei allen Funktionsaufrufen an das Aktensystem, die Autorisierungskomponente und die Schlüsselgenerierungsdienste nach Ablaufen der Timeout-Zeit von mindestens 60 Minuten die Umschlüsselung abbrechen und die Methode `finishKeyChange(FALSE)` sowohl bei der Komponente Autorisierung als auch bei der Komponente Dokumentenverwaltung aufrufen. **[<=]**

Wenn das Frontend des Versicherten auf einem Smartphone läuft, dann kann es durchaus die Verbindung in einem Funkloch verlieren und nach kurzer Zeit wieder herstellen. Weiterhin kann es sein, dass das Smartphone sich wegen erschöpften Akkumulators abschaltet und der Nutzer es innerhalb kurzer Zeit an das Ladegerät anschließt und die Umschlüsselung fortsetzen möchte. Diese Verbindungsabbrüche sollen nicht zum Abbrechen des Umschlüsselungsprozesses führen.

ENTWURF

A_20725 - ePA-Frontend des Versicherten: Abbruch der Umschlüsselung durch den Versicherten
Das ePA-Frontend des Versicherten MUSS während der Umschlüsselung dem Nutzer anbieten, die Umschlüsselung abzubrechen. Wenn der Nutzer die Umschlüsselung abbricht, dann sendet das FdV die Nachricht`finishKeyChange(FALSE)` sowohl an das Aktensystem als auch an die Dokumentenverwaltung.**[<=]**

Die Komponenten Aktensystem und Dokumentenverwaltung führen nach Erhalt der ~~Nachricht `finishKeyChange`~~Nachricht`finishKeyChange(FALSE)` die Methode `Rollback()` durch und stellen den Zustand von vor der Umschlüsselung wieder her.

A_20723 - ePA-Frontend des Versicherten: Anzeige des Aktenzustandes KEY_CHANGE
Das ePA-Frontend des Versicherten MUSS während der Umschlüsselung an der Oberfläche dem Nutzer anzeigen, dass die Akte im Zustand "KEY_CHANGE" ist.**[<=]**

A_20724 - ePA-Frontend des Versicherten: Verhindern aller sonstigen Aktivitäten während der Umschlüsselung
Das ePA-Frontend des Versicherten SOLL während der Umschlüsselung alle Aktivitäten verhindern, die nicht zum Umschlüsselungsprozess gehören.**[<=]**

Das Aktensystem lehnt im Zustand KEY_CHANGE alle sonstigen Aktivitäten vom FdV ab, daher sollte das FdV dem Benutzer auch keine weiteren Aktivitäten anbieten.

A_20479-01~~A_20479~~ - ePA-Frontend des Versicherten: Umschlüsselung durchführen
Das Frontend des Versicherten muss den Anwendungsfall "Umschlüsselung" für den Versicherten umsetzen.

Name	Umschlüsselung
Auslöser	Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Die Akte befindet sich im Zustand "ACTIVATED".
Nachbedingung	1. Neuer Aktenschlüssel ist erzeugt 2. Neuer Kontextschlüssel ist erzeugt. 3. Für jeden Berechtigten sind neue SGD1 und SGD2 Schlüssel erzeugt 4. Für alle Berechtigten sind der neue Akten- und der neue Kontextschlüssel mit den neuen SGD Schlüsseln geschützt in der Autorisierungskomponente hinterlegt. 5. Alle Dokumentenschlüssel in der Dokumentenverwaltungskomponente sind mit dem neuen Aktenschlüssel umgeschlüsselt. 6. Die Akte befindet sich im Zustand "ACTIVATED". ~~6.~~7. Der Versicherte kann innerhalb von 4 Wochen die Umschlüsselung rückgängig machen. Dazu werden von der

ENTWURF

	Dokumentenverwaltungskomponente und von der Autorisierungskomponente der alte Aktenschlüssel, der alte Kontext-Schlüssel und die alten chiffrierten Dokumentenschlüssel aufbewahrt und nach Ablauf der Frist, wenn die Umschlüsselung nicht rückgängig gemacht wurde, datenschutzkonform gelöscht.
Standardablauf	Aktivitäten im Standardablauf 1. Der Versicherte startet die Umschlüsselung mit dem Aufruf der Funktion `StartKeyChange()` (gemSpec_Autorisierung#6.2.4.13) an der Komponente Autorisierung. Als Rückgabewert liefert die Autorisierung die rollbackTime. Die Autorisierungkomponente setzt den Status der Akte auf den Zustand KEY_CHANGE. Wenn innerhalb der rollbackTime (z.B.24 h) die Umschlüsselung nicht abgeschlossen ist, werden sowohl die Autorisierung als auch das Aktensystem den Zustand einnehmen, den sie vor der Umschlüsselung hatten. Sollte die Autorisierungskomponente auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab. Das FdV muss dem Versicherten einen Hinweistext anzeigen, dass nach der Umschlüsselung die alten Kontext- und Aktenschlüssel sowie die alten verschlüsselten Dokumentenschlüssel vier Wochen aufbewahrt werden. Weiterhin muss explizit darauf hingewiesen werden, dass es sehr empfehlenswert ist, sich nach der erfolgreichen Umschlüsselung erneut anzumelden und Dokumente aus der ePA herunterzuladen und zu betrachten, um sich so von dem Erfolg der Umschlüsselung zu überzeugen. Der Hinweistext muss Informationen enthalten, wie man sich über einen anderen Weg als über das FdV an den Anbieter der Akte wenden kann. Dem Versicherten muss über diesen Weg die Möglichkeit geboten werden, die Umschlüsselung innerhalb von 4 Wochen rückgängig zu machen, wenn sie nicht erfolgreich verlaufen war. Weiterhin kann der Versicherte, wenn die Umschlüsselung erfolgreich war, die Aufbewahrung der alten Schlüssel und dem Schlüsselchiffrat verkürzen und sofort löschen lassen. Dies kann geboten sein, wenn der Grund für die Umschlüsselung eine Kompromittierung der alten Schlüssel war. 2. Das FdV ~~generiert~~ generiert einen neuen Akten- und einen neuen Kontextschlüssel wie in gemSpecFdv#6.2.5.1. beschrieben. 3. Das FdV ruft die Funktion `StartKeyChange(newKS,rollbackTime)` an der Dokumentenverwaltung (gemSpec_Dokumentenverwaltung#5.3.2.1) auf. Die Dokumentenverwaltung führt einen Logout aller angemeldeten anderen Instanzen (z.B. LEI oder Kassen) durch. Dieser Aufruf liefert als Rückgabewert eine Struktur mit KVNRs und / oder

ENTWURF

Telematik-IDs berechtigter LEIs, Kassen oder Vertretern zurück. Sollte die Dokumentenverwaltung auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab.

4. Das FdV ruft für den Versicherten, jede berechtigte LEI, für jede berechtigte Kasse und für jeden Vertreter die Funktion `KeyGeneration()` am SGD1 und am SGD2 (gemSpec_SGD_ePA#6.6) auf. Hierbei ist die Ableitungsregel für eine Erstableitung von Schlüsseln für den berechtigten Nutzer durch den Kontoinhaber zu verwenden. Als Rückgabewert vom SGD1 und vom SGD2 erhält das FdV jeweils einen neu generierten Schlüssel. Sollten die Schlüsselgenerierungsdienste auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab. Eine Ausnahme bildet der Fehlerfall, dass eine LEI nicht mehr im VZD gefunden wird. In diesem Fall ist der Nutzer des FdV darüber zu benachrichtigen, dass die Berechtigungen für diese LEI nicht mehr gültig sind, da die LEI nicht mehr im VZD verzeichnet ist. Anschließend wird die Umschlüsselung fortgesetzt.
5. Das FdV verschlüsselt für den Versicherten, für jede berechtigte LEI, jede berechtigte Kasse und jeden berechtigten Vertreter den neuen Aktenschlüssel mit den von den SGD1 und SGD2 generierten nutzerindividuellen ~~Schlüssel~~Schlüsseln.
6. Das FdV verschlüsselt für den Versicherten, für jede berechtigte LEI, jede berechtigte Kasse und jeden berechtigten Vertreter den neuen Kontextschlüssel mit den von den SGD1 und SGD2 generierten nutzerindividuellen ~~Schlüssel~~Schlüsseln.
7. Das FdV übermittelt mit dem Aufruf der Methode `PutForReplacement(SetOfEncryptedKeys)` die in (5 und 6) verschlüsselten Schlüssel an die Komponente Autorisierung, wo sie als neue Schlüssel gekennzeichnet, zunächst gespeichert werden. Nach erfolgreichem Abschluss der Umschlüsselung ersetzt die Autorisierungskomponente die alten Schlüssel durch die neuen. Sollte die Autorisierungskomponente auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab.
8. Das FdV ruft mit der Methode `GetAllDocumentKeys()` der Komponente Dokumentenverwaltung alle verschlüsselten Dokumentenschlüssel (Rückgabewert `DocumentKeyList`) vom Aktensystem ab. Dokumente werden dabei nicht übertragen. Sollte die Komponente Dokumentenverwaltung auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab.

ENTWURF

9. Das FdV entschlüsselt die verschlüsselten Dokumentenschlüssel mit dem alten Aktenschlüssel.
10. Das FdV verschlüsselt die entschlüsselten Dokumentenschlüssel mit dem neuen Aktenschlüssel.
11. Das FdV wählt aus den empfangenen DokumentenIDs einige aus und lädt zu diesen die verschlüsselten Dokumente aus der Dokumentenverwaltung, entschlüsselt sie und bildet über die einzelnen Dokumente mittels einer Hashfunktion eindeutige Hashwerte. Diese werden zusammen mit den Dokumenten-IDs gespeichert und benötigt, um später prüfen zu können, ob die Umschlüsselung erfolgreich war.
12. Das FdV übermittelt mit dem Aufruf der Methode `PutAllDocumentKeys()` die mit dem neuen Aktenschlüssel verschlüsselten Dokumentenschlüssel an die Komponente Dokumentenverwaltung. Sollte die Dokumentenverwaltung auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab.
13. Das FdV schließt die VAU in der Dokumentenverwaltung über `closeContext()`.
14. Um den Erfolg der Umschlüsselung zu überprüfen, holt sich das FdV von der Autorisierungskomponente den neuen Kontext-Schlüssel und öffnet dann damit die VAU in der Komponente Dokumentenverwaltung. Anschließend lädt es mit den in Schritt 11 gespeicherten Dokumenten-IDs die verschlüsselten Dokumente aus der Dokumentenverwaltung.
15. Das FdV entschlüsselt die in Schritt 14 heruntergeladenen Dokumente und bildet mit der in Schritt 11 verwendeten Hashfunktion erneut den Hashwert über jedes der entschlüsselten Dokumente.
16. Anschließend vergleicht das FdV die in Schritt 11 und Schritt 15 für jedes Dokument erzeugten Hashwerte, wenn sie identisch sind, dann ist die Umschlüsselung erfolgreich durchgeführt worden.
17. Wenn in Schritt 16 die erfolgreiche Umschlüsselung festgestellt worden ist, dann ruft das FdV an der Komponente Dokumentenverwaltung die Methode `finishKeyChange(true)` auf. Diese ersetzt die alten Schlüssel durch die neuen und ~~löscht~~sichert die alten Schlüssel für einen Zeitraum von 4 Wochen, bzw. sichert diese für eventuell vorhandene Backups verschlüsselter Dokumente im Rahmen eines Backup-Konzepts. Anschließend setzt die Dokumentenverwaltung den Status der Akte wieder auf ACTIVATED. Damit ist für die Dokumentenverwaltung die Umschlüsselung abgeschlossen.
18. Wenn Schritt 17 erfolgreich durchgeführt wurde, dann ruft das FdV an der Autorisierungskomponente die Methode `finishKeyChange(true)` auf. Diese ~~löscht~~sichert für einen

ENTWURF

	Zeitraum von vier Wochen die alten Schlüssel, bzw. sichert sie für eventuell vorhandene Backups verschlüsselter Dokumente im Rahmen eines Backup-Konzepts. Anschließend setzt die Autorisierungskomponente den Status der Akte wieder auf ACTIVATED. Damit ist für die Autorisierungskomponente die Umschlüsselung abgeschlossen. 19. Wenn in Schritt 16 die Umschlüsselung als fehlgeschlagen erkannt wurde (weil die verglichenen Hashwerte nicht gleich waren), dann ruft das FdV an der Komponente Dokumentenverwaltung die Methode `finishKeyChange(FALSE)` auf. Diese ruft die Rollback()- Methode auf, welche die alten gespeicherten Schlüssel wieder aktiviert und die neuen Schlüssel löscht. 20. Wenn der Schritt 19 durchgeführt wurde, dann ruft das FdV an der Autorisierungskomponente die Methode finishKeyChange(FALSE) auf. Diese ruft die Rollback()- Methode auf, welche die alten gespeicherten Schlüssel wieder aktiviert die neuen löscht. Anschließend setzt die Autorisierungskomponente den Status der Akte wieder auf ACTIVATED. Damit ist die Umschlüsselung abgeschlossen.

[<=]

6.2.7 Berechtigungsverwaltung

Dieses Kapitel beschreibt Anwendungsfälle zur Vergabe und Administration von Berechtigungen zum Zugriff auf das Aktenkonto.

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

Die zulässigen Berechtigungsvergaben für die verschiedenen Leistungserbringerinstitutionen, Kostenträger und Vertreter werden vom Aktensystem durchgesetzt. Das ePA-Frontend des Versicherten kann die grundsätzlich gesetzlich möglichen Berechtigungsvergaben nicht erweitern, sondern nur weiter einschränken.

A_15382 - ePA-Frontend des Versicherten: Bestätigung Berechtigungskonfiguration
Das ePA-Frontend des Versicherten MUSS, bevor es eine Berechtigung an eine LEI vergibt oder ändert, eine Bestätigung der gewählten Berechtigungskonfiguration vom Nutzer einholen.**[<=]**

A_20195 - ePA-Frontend des Versicherten: Anzeige der gesetzlichen Restriktionen für die Rechtevergabe in Abhängigkeit von der Berufsgruppe
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, sich die gesetzlichen Restriktionen für die Rechtevergabe in Abhängigkeit von der Berufsgruppe, die in [gemSpec_Dokumentenverwaltung#Tab_Dokv_030 - Zugriffsunterbindungsregeln] aufgeführt sind, anzeigen zu lassen.**[<=]**

Die Anzeige kann z.B. als Hilfetext vom Nutzer bei der Berechtigungsvergabe erreichbar sein.

ENTWURF

A_15380 - ePA-Frontend des Versicherten: Suche Leistungserbringerinstitution in Verzeichnisdienst
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine oder mehrere LEI im Verzeichnisdienst zu suchen und für die Vergabe von Berechtigungen auszuwählen.**[<=]**

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

A_20196 - ePA-Frontend des Versicherten: Anzeige der Berufsgruppe der Leistungserbringerinstitution bei der Berechtigungsvergabe
Das ePA-Frontend des Versicherten MUSS dem Nutzer die aus dem Zertifikat C.HCI.ENC aus GS-A_4601 über die professionOID aus GS-A_4442-01 ermittelte Berufsgruppe der Leistungserbringerinstitution bei der Berechtigungsvergabe anzeigen.**[<=]**

A_20254 - ePA-Frontend des Versicherten: Anzeige der Anzahl der Dokumente, auf die – in Abhängigkeit von der ausgewählten Berufsgruppe der zu berechtigenden Leistungserbringerinstitution – eine Berechtigung vergeben werden kann
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, sich die Anzahl der Dokumente anzeigen zu lassen, auf die ein konkrete LEI berechtigt werden kann. **[<=]**

Das FdV kann die Anzahl berechnen, indem es zunächst über die Suche mit simuliert Berechtigung (siehe [gemSpec_Dokumentenverwaltung#5.1.2.2.1.1 Suche mit simulierter Berechtigung]) das Aktensystem abfragt, auf welche Dokumente auf die konkrete LEI berechtigt werden kann.

A_15383-02 - ePA-Frontend des Versicherten: Berechtigung an LEI für Aktenkonto vergeben
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.1 - Berechtigung durch einen Versicherten vergeben" aus [gemSysL_ePA] für jede LEI, für die eine Berechtigung vergeben werden soll, gemäß TAB_FdV_134 umsetzen.

Tabelle 40: TAB_FdV_134 – Berechtigung an LEI für Aktenkonto vergeben

Name	Berechtigung an LEI für Aktenkonto vergeben
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Ein Verschlüsselungszertifikat, die Telematik-ID und der Name der LEI sind bekannt. Die Berechtigung widerspricht nicht [gemSpec_Dokumentenverwaltung#Tab_Dokv - Zugriffsunterbindungsregeln] Der Nutzer hat die Parameter für die Berechtigungen ausgewählt und die Vergabe der Berechtigung bestätigt.

ENTWURF

Nachbedingung	Die LEI ist zum Zugriff auf das Aktenkonto berechtigt. Das notwendige Schlüsselmaterial ist in der Autorisierung hinterlegt. Ein Policy Document für den LEI ist in der Dokumentenverwaltung hinterlegt.
Standardablauf	Aktivitäten im Standardablauf 1. AuthorizationKey für LEI erstellen 2. Schlüsselmaterial im ePA-Aktensystem speichern 3. Policy Document für LEI erstellen 4. Policy Document in Dokumentenverwaltung laden

[<=]

A_20198 - ePA-Frontend des Versicherten: Anzeige der auf ein Dokument berechtigten LEI

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "Anzeige der auf ein Dokument berechtigten LEI" gemäß TAB_FdV_178 umsetzen.

Tabelle 41: TAB_FdV_178 Anzeige der auf ein Dokument berechtigten LEI

Name	Anzeige der auf ein Dokument berechtigten LEI
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat ein Dokument ausgewählt
Nachbedingung	Der Nutzer hat Informationen darüber, welche Leistungserbringerinstitutionen auf das Dokument Zugriff haben.
Standardablauf	Aktivitäten im Standardablauf 1. Alle Policy Documents für LEI herunterladen 2. Für jede gefundene LEI-Policy werden folgende Unteraktivitäten durchgeführt: a. eine Dokumenten-Suchanfrage mit simulierter Berechtigung gemäß [gemSpec_Dokumentenverwaltung#5.1.2.2.1.1] als die ausgewählte LEI an das Aktensystem absenden b. Antwort des Aktensystems nach der DocumentEntry.uniqueId des ausgewählten Dokumentes durchsuchen.

ENTWURF

	c. Wenn die DocumentEntry.uniqueId enthalten ist, dann hat die LEI Zugriff auf das Dokument und die LEI wird der Liste der zugriffsberechtigten LEI hinzugefügt. 3. Liste mit den zugriffsberechtigten LEI dem Nutzer anzeigen.

[<=]

A_20199-01 - ePA-Frontend des Versicherten: Ändern der Vertraulichkeitsstufe eines Dokumentes
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "Ändern der Vertraulichkeitsstufe eines Dokumentes" gemäß TAB_FdV_179 umsetzen.

Tabelle 42: TAB_FdV_179: Ändern der Vertraulichkeitsstufe eines Dokumentes

Name	Ändern der Vertraulichkeitsstufe eines Dokumentes
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat ein Dokument ausgewählt
Nachbedingung	Im Aktensystem ist die neue Vertraulichkeitsstufe des Dokumentes gespeichert
Standardablauf	1. Der Nutzer wählt die neue Vertraulichkeitsstufe für das Dokument in einem Menü aus 2. Das FdV sendet die bestehenden Metadaten des Dokuments mit geänderter Vertraulichkeitsstufe an das Aktensystem. 3. Das FdV zeigt dem Versicherten die neue Vertraulichkeitsstufe des Dokumentes an.

[<=]

A_20201 - ePA-Frontend des Versicherten: Ändern der Zugriffsberechtigung einer LEI auf Dokumentenkategorien
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "Ändern der Zugriffsberechtigung einer LEI auf Dokumentenkategorien" gemäß TAB_FdV_180 umsetzen.

Name	Ändern der Zugriffsberechtigung einer LEI auf Dokumentenkategorien
Auslöser	Aufrufen des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter

ENTWURF

Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Im Aktensystem ist die geänderte Zugriffsberechtigung einer LEI auf Dokumentenkategorien gespeichert
Standardablauf	1. Der Nutzer wählt eine LEI aus, deren Policy Document schon heruntergeladen wurde oder er sucht über A_15336-01 eine neue LEI im Verzeichnisdienst und erzeugt für diese ein neues Policy Document 2. Wenn es eine neue LEI ist, dass wird dem Nutzer wird angezeigt, auf welche Dokumentenkategorien die LEI laut [gemSpec_Dokumentenverwaltung#Tab_Dokv_030 - Zugriffsunterbindungsregeln] zugreifen darf. Wenn es eine LEI ist, für die schon ein Policy Document im Aktensystem existiert, dann werden die dort gespeicherten Berechtigungen angezeigt. 3. Der Nutzer kann die Zugriffsberechtigungen auf die Dokumentenkategorien ändern, indem er in einem Menü den Zugriff auf entsprechende Kategorien auswählt oder abwählt. Er kann aber die Zugriffsunterbindungsregeln nur weiter einschränken, nicht aber erweitern. 4. Das FdV sendet das geänderte Policy Document an das Aktensystem.

[<=]

A_19306 - ePA-Frontend des Versicherten: Berechtigung konform mit Zugriffsunterbindungsregeln
Das ePA-Frontend des Versicherten MUSS verhindern, dass Nutzer Berechtigungen erteilen, die der Tabelle [gemSpec_Dokumentenverwaltung#Tab_Dokv_030 - Zugriffsunterbindungsregeln] widersprechen.**[<=]**

A_19119 - ePA-Frontend des Versicherten: Gesonderte Einwilligung bei jeder Zugriffsfreigabe
Das ePA-FdV MUSS sicherstellen, dass bei jeder Zugriffsfreigabe für Leistungserbringer eine gesonderte Einwilligung vom Versicherten eingeholt wird, nachdem er zuvor in verständlicher Art und Weise darüber informiert wurde, dass der Leistungserbringer für den Zugriff auf alle Dokumente der vom Versicherten ausgewählten Kategorie (LE-Dokumente, Versicherten-Dokumente, Kostenträger-Dokumente) berechtigt wird und die Berechtigung nicht auf einzelne spezifische Dokumente und Datensätze bzw. auf Gruppen von Dokumenten und Datensätzen beschränkt werden kann. **[<=]**

Hinweis: Die Einwilligung des Versicherten bei jeder Zugriffsfreigabe kann auf elektronischem Wege (z.B. durch das Klicken eines Einwilligungsbuttons nach Anzeige der genannten Informationen) erfolgen.

A_15384-01 - ePA-Frontend des Versicherten: Berechtigung an LEI vergeben - AuthorizationKey erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an LEI für Aktenkonto vergeben" einen AuthorizationKey mit `AuthorizationType` = DOCUMENT_AUTHORIZATION und `validTo` entsprechend der vom Nutzer festgelegten Berechtigungsdauer für die zu berechtigende LEI erstellen.**[<=]**

ENTWURF

A_15385-01 - ePA-Frontend des Versicherten: Berechtigung an LEI vergeben - Schlüsselmaterial im ePA-Aktensystem speichern
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an LEI für Aktenkonto vergeben" für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey` = erstellter AuthorizationKey ausführen. Der optionale Parameter `NotificationInfoRepresentative` wird nicht belegt.**[<=]**

A_15386-01 - ePA-Frontend des Versicherten: Berechtigung an LEI vergeben - Policy Document erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an LEI für Aktenkonto vergeben" ein Policy Document für den zu Berechtigenden entsprechend den für die Berechtigung ausgewählten Parametern erstellen.**[<=]**

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

A_15387-01 - ePA-Frontend des Versicherten: Berechtigung an LEI vergeben - Policy Document hochladen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an LEI für Aktenkonto vergeben" zum Hochladen des Policy Documents in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für Policy Documents ausführen.**[<=]**

A_20066 - ePA-Frontend des Versicherten: Vom Aktensystem durchgesetzte Zugriffsrechte der LEI auf ein einzelnes Dokument anzeigen
Das ePA-Frontend des Versicherten MUSS dem Nutzer anzeigen, in welcher Weise (z.B. nur Lesen, nur Schreiben, Lesen und Schreiben und Löschen) das Aktensystem für eine berechtigte LEI für ein konkretes Dokument den Zugriff ermöglicht.**[<=]**

Damit kann der Versicherte vor dem Besuch einer Leistungserbringerinstitution kontrollieren, auf welche Dokumente die Leistungserbringerinstitution lesenden bzw. löschenden Zugriff während der Behandlung hat.

A_20109-03~~A_20109-02~~ - ePA-Frontend des Versicherten: Konfiguration der zeitlichen Begrenzung der Berechtigungsdauer
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die zeitliche Begrenzung für eine Leistungserbringerinstitution ~~oder einen Kostenträger~~ für die erteilte Zugriffsberechtigung zu konfigurieren. Folgende Optionen MUSS das ePA-Frontend anbieten:

- 1 Tag
- 7 Tage [default]
- 18 Monate
- ~~flexibel (1-540 Tage)~~
- flexibles Enddatum (jedoch kleiner als heute + 100 Jahre)
- Unbefristet

Eine unbefristete Berechtigungsdauer MUSS über eine zeitliche Begrenzung auf 100 Jahre (heute+100 Jahre) umgesetzt werden.
[<=]

ENTWURF

6.2.7.1 Berechtigungsarten

A_19556 - ePA-Frontend des Versicherten: Auswahl der Berechtigungsart
Das ePA-Frontend des Versicherten MUSS für Dokumentenfreigaben alle drei Optionen unterstützen:

- Option Dokumentenfreigabe durch grobgranulare Berechtigung
- Option Dokumentenfreigabe durch mittelgranulare Berechtigung
- Option Dokumentenfreigabe durch feingranulare Berechtigung

[<=]

A_19701 - ePA-Frontend des Versicherten: Anzeige der berechtigten LEIs
Wenn sich ein Nutzer ein Dokument ansieht, MUSS das ePA-Frontend des Versicherten MUSS dem Nutzer anzeigen, welche LEIs für den Zugriff auf dieses Dokument berechtigt sind.**[<=]**

Das Aktensystem setzt folgende Regeln um:

- Die Regeln der mittelgranularen Berechtigung schränken die Regeln der grobgranularen Berechtigung weiter ein.
- Der Zugriff auf Dokumente kann feingranular unabhängig von grob- und mittelgranularer Berechtigung gewährt oder entzogen werden ("Whitelisting" und "Blacklisting).

6.2.7.2 Grobgranulare Berechtigungsverwaltung

Bei der grobgranularen Berechtigung wird der Zugriff auf die vorhandenen Dokumente der elektronischen Patientenakte in drei Vertraulichkeitsstufen unterteilt. Dabei werden die Vertraulichkeitsstufen **normal**, **vertraulich** und **streng vertraulich** verwendet. Eine einzelne Leistungserbringerinstitution kann entweder Zugriff auf alle Dokumente der Vertraulichkeitsstufe **normal** oder auf die Vertraulichkeitsstufen **normal** und **vertraulich** erhalten. Der Zugriff auf Dokumente der Vertraulichkeitsstufe **streng vertraulich** ist der Leistungserbringerinstitution nur möglich über eine explizite Freigabe über die Whitelist der feingranularen Berechtigungsverwaltung durch den Versicherten oder seinem Vertretern über das Frontend des Versicherten. Einmal getroffene Entscheidungen bezüglich der Zuordnung eines Dokumentes zu einer Vertraulichkeitsstufe und bezüglich des Zugriffs einer Leistungserbringerinstitution können vom Versicherten durch das ePA-Frontend des Versicherten jederzeit revidiert werden. Die Regeln der grobgranularen Berechtigungsverwaltung können von der mittelgranularen und der feingranularen Berechtigungsverwaltung ergänzt werden.

A_19566 - ePA-Frontend des Versicherten: Vertraulichkeitsstufen in der grobgranularen Berechtigungsverwaltung
Das ePA-Frontend des Versicherten MUSS dem Nutzer, der seine Dokumente mittels der grobgranularen Berechtigungsverwaltung freigeben möchte, folgende Vertraulichkeitsstufen zur Kennzeichnung jedes Dokuments anbieten:

- **normal**
- **vertraulich**
- **streng vertraulich**

[<=]

ENTWURF

A_20177-01 - ePA-Frontend des Versicherten: Verwendung der Operation RestrictedUpdateDocumentSet
Das ePA-Frontend des Versicherten MUSS die Operation I_Document_Management_Insurant::RestrictedUpdateDocumentSet ausschließlich dafür verwenden, um die Zugriffsberechtigungen für LEI auf Dokumente in der grobgranularen Berechtigungsverwaltung aufgrund einer Interaktion mit dem Versicherten zu verändern. Es darf ausschließlich der DocumentEntry.confidentialityCode am FdV durch ein Metadaten-Update geändert werden.
[<=]

Die Zugriffsberechtigungen von LEI auf Dokumente der ePA werden über Policy Dokumente im Aktensystem hinterlegt. Dies ist in Kapitel 6.2.7 in den Anforderungen A_15386-01 und A_15387-01 übergreifend für fein-/mittel-/grobgranulare Berechtigungen beschrieben.

A_20178 - ePA-Frontend des Versicherten:Vorauswahl der Vertrauensstufe
Das ePA-Frontend des Versicherten MUSS dem Nutzer als Vertrauensstufe normal vorschlagen.**[<=]**

A_19567 - ePA-Frontend des Versicherten: Kennzeichnung hochgeladener Dokumente in der grobgranularen Berechtigungsverwaltung
Das ePA-Frontend des Versicherten MUSS bei allen Dokumenten die vom Nutzer ausgewählte Vertraulichkeitsstufe in den Metadaten jedes Dokuments setzen.**[<=]**

A_19578 - ePA-Frontend des Versicherten: Abbildung der Vertraulichkeitsstufen auf confidentialityCodes
Das ePA-Frontend des Versicherten MUSS, wenn der Nutzer seine Dokumente mittels der grobgranularen Berechtigungsverwaltung freigeben möchte, bei diesen Dokumenten die vom Nutzer ausgewählte Vertraulichkeitsstufe über folgende confidentialityCodes abbilden:

- **normal** -> confidentialityCode**normal**
- **vertraulich** ->confidentialityCode**restricted**
- **streng vertraulich**-> confidentialityCode**very restricted**

Im Detail ist dies auch schon in Kapitel 6.2.6 in den AFOs A_15386-01 und A_15387-01 übergreifend für fein-/mittel-/grobgranulare Berechtigungen beschrieben.**[<=]**

A_19568 - ePA-Frontend des Versicherten: Auswahl der Leistungserbringerinstitution für das grobgranulare Berechtigungskonzept
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, einer oder mehreren LEI, die über die AFO A_15380 gefunden wurden, eines der folgenden Zugriffsrechte zu erteilen:

- einfaches Zugriffsrecht
- erweitertes Zugriffsrecht

[<=]

Eine Leistungserbringerinstitution, welche das einfache Zugriffsrecht erteilt wurde, hat nur Zugriff auf Dokumente in der ePA mit der Vertraulichkeitsstufe **normal**. Eine Leistungserbringerinstitution, welcher das erweitere Zugriffsrecht erteilt wurde, hat nur Zugriff auf Dokumente in der ePA mit den Vertraulichkeitsstufen **normal** und **vertraulich**.

ENTWURF

A_19577 - ePA-Frontend des Versicherten: Optische Anzeige der Vertraulichkeitsstufen
Das ePA-Frontend des Versicherten KANN dem Nutzer die Vertraulichkeitsstufe eines Dokumentes durch typografische Auszeichnung wie etwa Schriftfarbe, Hintergrundfarbe,Schriftart oder auch die Anordnung in Gruppen optisch kennzeichnen. **[<=]**

Mögliche Anzeigen wäre z. B: "LEI hat erweitertes Zugriffsrecht mit Freigabe der Kategorie Arztbrief und wurde nicht explizit einzeln ausgeschlossen.", "LEI hat explizite Einzelfreigabe für dieses Dokument.", "LEI hat kein Zugriffsrecht für dieses Dokument"

A_19580 - ePA-Frontend des Versicherten: Wechsel der Vertraulichkeitsstufe von normal nach vertraulich
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Vertraulichkeitsstufe eines Dokumentes von **normal** in **vertraulich** zu ändern. **[<=]**

A_19581 - ePA-Frontend des Versicherten: Wechsel der Vertraulichkeitsstufe von normal nach streng vertraulich
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Vertraulichkeitsstufe eines Dokumentes von **normal** in **streng vertraulich** zu ändern. **[<=]**

A_19582 - ePA-Frontend des Versicherten: Wechsel der Vertraulichkeitsstufe von vertraulich nach normal
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Vertraulichkeitsstufe eines Dokumentes von **vertraulich** in **normal** zu ändern. **[<=]**

A_19583 - ePA-Frontend des Versicherten: Wechsel der Vertraulichkeitsstufe von vertraulich nach streng vertraulich
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Vertraulichkeitsstufe eines Dokumentes von **vertraulich** in **streng vertraulich** zu ändern. **[<=]**

A_19584 - ePA-Frontend des Versicherten: Wechsel der Vertraulichkeitsstufe von streng vertraulich nach normal
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Vertraulichkeitsstufe eines Dokumentes von **streng vertraulich** in **normal** zu ändern. **[<=]**

A_19585 - ePA-Frontend des Versicherten: Wechsel der Vertraulichkeitsstufe von streng vertraulich nach vertraulich
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Vertraulichkeitsstufe eines Dokumentes von **streng vertraulich** in **vertraulich** zu ändern. **[<=]**

A_19588 - ePA-Frontend des Versicherten: Erstellen einer Leistungserbringer-Policy für das einfache Zugriffsrecht
Das ePA-Frontend des Versicherten MUSS beim Erteilen einer einfachen Zugriffsberechtigung für die Leistungserbringerinstitution in der APPC-Policy das einfache Zugriffsrecht über den confidentialityCode **normal** abbilden. **[<=]**

A_19589 - ePA-Frontend des Versicherten: Erstellen einer Leistungserbringer-Policy für das erweiterte Zugriffsrecht
Das ePA-Frontend des Versicherten MUSS beim Erteilen einer erweiterten Zugriffsberechtigung für die Leistungserbringerinstitution in der APPC-Policy das erweiterte Zugriffsrecht über die confidentialityCodes **normal** und **restricted** abbilden.**[<=]**

ENTWURF

6.2.7.3 Mittelgranulare Berechtigungsverwaltung

Bei der mittelgranularen Berechtigung wird der Zugriff auf die vorhandenen Dokumente der elektronischen Patientenakte in Dokumentenkategorien organisiert. Diese sind in der Spezifikation gemSpec_DM_ePA aufgeführt. Die Zuordnung eines einzelnen Dokumentes zu einer einzelnen Dokumentenart legt (mit Ausnahme der Dokumentenarten **Dokumente des Versicherten** und der **Kostenträgerdokumente**) die Leistungserbringerinstitution fest. Alle Dokumente, die der Versicherte selbst einstellt, sind immer der Kategorie **Dokumente des Versicherten** zugeordnet. Ein Kostenträger kann ausschließlich Kostenträgerdokumente einstellen. Der Versicherte kann über das ePA-Frontend des Versicherten eine einzelne Leistungserbringerinstitution den Zugriff auf einzelne **Dokumentenkategorien** erteilen oder entziehen.

A_19685 - ePA-Frontend des Versicherten: Anzeige der Dokumentenkategorien in der mittelgranularen Berechtigungsverwaltung
Das ePA-Frontend des Versicherten MUSS dem Nutzer die dem Dokument zugeordnete Dokumentenkategorie, die in der gemSpec_DM_ePA in den Anforderungen A_14761-01 und A_19388 aufgeführt sind, anzeigen können. **[<=]**

A_19686 - ePA-Frontend des Versicherten: Auswahl der Leistungserbringerinstitutionen in der mittelgranularen Berechtigungsverwaltung
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, eine oder mehrere LEI, die über die AFO A_15380 gefunden wurden, den Zugriff auf eine oder mehrere Dokumentenkategorien zu ermöglichen.**[<=]**

A_19989 - ePA-Frontend des Versicherten: Ermittlung der ProfessionOID in der mittelgranularen Berechtigungsverwaltung
Das ePA-Frontend des Versicherten MUSS bei der mittelgranularen Berechtigungsverwaltung die ProfessionOID der LEI aus dem Zertifikat C.HCI.ENC (Extension Admission) der LEI ermitteln.
[<=]

A_19687 - ePA-Frontend des Versicherten: Berücksichtigung der Zugriffsunterbindungsregeln bei der Anzeige der Dokumentenkategorien
Das ePA-Frontend des Versicherten MUSS bei der mittelgranularen Berechtigungsvergabe die Zugriffsunterbindungsregeln aus [gemSpec_Dokumentenverwaltung#Tab_Dokv_030 - Zugriffsunterbindungsregeln] beachten. Daraus folgt, dass dem Nutzer für eine ausgewählte Leistungserbringerinstitution nur diejenigen Dokumentenkategorien angezeigt werden, für die diese tatsächlich berechtigt werden kann.**[<=]**

Wenn die Nutzerin des ePA-Frontend des Versicherten als Leistungserbringerinstitution eine Hebamme auswählt, dann hat diese weniger mögliche Zugriffsrechte als zum Beispiel ein Hausarzt. Das ePA-Frontend des Versicherten darf dann für die Hebamme nur die nach [gemSpec_Dokumentenverwaltung#Tab_Dokv_030 - Zugriffsunterbindungsregeln] möglichen mittelgranularen Berechtigungen anzeigen.

A_19690 - ePA-Frontend des Versicherten: Optische Kennzeichnung der Dokumentenkategorien
Das ePA-Frontend des Versicherten KANN dem Nutzer die zugeordnete Dokumentenkategorie eines Dokumentes durch typografische Auszeichnung wie etwa Schriftfarbe, Hintergrundfarbe,Schriftart oder auch die Anordnung in Gruppen optisch kennzeichnen.**[<=]**

ENTWURF

A_19691 - ePA-Frontend des Versicherten: Anzeige der für den LEI sichtbaren Dokumentenkategorien
Das ePA-Frontend des Versicherten MUSS dem Nutzer anzeigen, auf welche Dokumentenkategorien eine einzelne Leistungserbringerinstitution zugreifen darf. **[<=]**

Damit kann der Nutzer vor dem Besuch einer Leistungserbringerinstitution sehen, welche Dokumentenkategorien der ePA bei der LEI sichtbar sind.

Ein Dokument kann sich in einer Dokumentenkategorie befinden, für die eine LEI zugriffsberechtigt ist, über das feingranulare Berechtigungskonzept wurde der LEI aber der Zugriff auf dieses Dokument entzogen. Im Resultat wird vom Aktensystem durchgesetzt, dass die LEI keinen Zugriff auf das Dokument hat.

A_19692 - ePA-Frontend des Versicherten: Anzeige der für den LEI geltenden Zugriffsregeln für die sichtbaren Dokumentenkategorien
Das ePA-Frontend des Versicherten MUSS dem Nutzer anzeigen, welche der vom Aktensystem durchgesetzten Zugriffsregeln bezüglich Lesen, Schreiben und Löschen für eine einzelne Dokumentenkategorie für eine einzelne Leistungserbringerinstitution gelten. **[<=]**

A_19693 - ePA-Frontend des Versicherten: Änderung der Dokumentenkategorie-Zugriffsberechtigung
Das ePA-Frontend des Versicherten MUSS dem Nutzer jederzeit ermöglichen, einmal getroffene Entscheidungen bezüglich der Zugriffsberechtigung für einzelne Dokumentenkategorien zurückzunehmen und neu zu vergeben.**[<=]**

A_19698 - ePA-Frontend des Versicherten: Erstellen einer APPC-Policy für die mittelgranulare Berechtigung
Das ePA-Frontend des Versicherten MUSS bei der Erteilung einer Berechtigung für den Zugriff auf eine Dokumentenkategorie nach dem mittelgranularen Berechtigungskonzept diese in der APPC-Policy der Leistungserbringerinstitution speichern. Diese muss in ihren Regeln die Freigabe der einzelnen Dokumentenkategorien enthalten. Wenn es für die LEI noch keine APPC-Policy gibt, dann muss das Frontend des Versicherten diese erstellen.**[<=]**

6.2.7.4 Feingranulare Berechtigungsverwaltung

Bei der feingranularen Berechtigung wird der Zugriff der LEI auf die vorhandenen Dokumente der elektronischen Patientenakte auf der Ebene der einzelnen Dokumente organisiert. Wenn der Nutzer einer LEI feingranular den Zugriff auf ein Dokument erteilt, dann erstellt das ePA Frontend des Versicherten für jedes freigegebene Dokument einen APPC-Policy-Eintrag mit den uniqueID des Dokuments. Die entsprechenden APPC-Policy-Einträge wirken als Whitelist. Wenn hingegen der Nutzer der LEI auf Dokumente, auf die z.B. über die mittelgranulare oder grobgranulare Berechtigung Zugriff erlaubt ist, den Zugriff entzieht, dann erstellt das ePA Frontend des Versicherten APPC-Policy-Einträge, die die uniqueIDs der Dokumente enthalten, auf die die LEI explizit nicht zugreifen darf. Diese APPC-Policy-Einträge wirken als Blacklist. Beim Aktualisieren der White- oder Black-List Policy-Einträge muss das Frontend des Versicherten sicherstellen, dass die Policy keine sich widersprüchlichen Einträge enthält.

A_19768 - ePA-Frontend des Versicherten: Zugriff auf ein einzelnes Dokument für eine Leistungserbringerinstitution erteilen
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, einer vorher ausgewählten LEI den Zugriff auf ein einzelnes Dokument ermöglichen.**[<=]**

ENTWURF

A_19770 - ePA-Frontend des Versicherten: Zugriff auf ein einzelnes Dokument für eine Leistungserbringerinstitution entziehen
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, einer vorher ausgewählten LEI den Zugriff auf ein einzelnes Dokument zu entziehen.**[<=]**

A_19771 - ePA-Frontend des Versicherten: Anzeige der freigegebenen Dokumente für eine einzelne Leistungserbringerinstitution
Das ePA-Frontend des Versicherten MUSS dem Nutzer in einer Liste anzeigen, welche Dokumente für eine einzelne LEI über die feingranulare Berechtigung freigegeben sind. Die Ansicht MUSS Angaben zu den vom Aktensystem durchgesetzten möglichen Zugriffsarten (Lesen, Schreiben und Löschen) der LEI enthalten.**[<=]**

A_19772 - ePA-Frontend des Versicherten: Anzeige der nicht freigegebenen Dokumente für eine einzelne Leistungserbringerinstitution
Das ePA-Frontend des Versicherten MUSS dem Nutzer in einer Liste anzeigen, welche Dokumente für eine einzelne LEI über die feingranulare Berechtigungsverwaltung der Zugriff entzogen wurde.**[<=]**

A_19773 - ePA-Frontend des Versicherten: Optische Kennzeichnung für eine LEI freigegebene Dokumente
Das ePA-Frontend des Versicherten KANN dem Nutzer die für eine LEI freigegebenen Dokumente durch typografische Auszeichnung wie etwa Schriftfarbe, Hintergrundfarbe, Schriftart oder auch die Anordnung in Gruppen optisch kennzeichnen.**[<=]**

A_19774 - ePA-Frontend des Versicherten: Optische Kennzeichnung der für eine LEI gesperrten Dokumente
Das ePA-Frontend des Versicherten KANN dem Nutzer die für eine LEI nicht freigegebene Dokumente durch typografische Auszeichnung wie etwa Schriftfarbe, Hintergrundfarbe,Schriftart oder auch die Anordnung in Gruppen optisch kennzeichnen.**[<=]**

A_19778 - ePA_Frontend des Versicherten: Abbilden eines erteilten Zugriffs in der APPC Policy
Das ePA-Frontend des Versicherten MUSS für jede zu einem Dokument für eine LEI erteilte Berechtigung einen Whitelist-Eintrag mit der DocumentEntry.uniqueID des Dokumentes in der APPC Policy der LEI vornehmen. **[<=]**

A_19866 - ePA_Frontend des Versicherten: Erzeugen einer neuen APPC Policy
Das ePA-Frontend des Versicherten MUSS für eine LEI eine neue APPC Policy anlegen, wenn der Versicherte eine Berechtigung auf ein Dokument für eine bestimmte LEI erteilt oder entzogen hat und es noch keine APPC Policy gibt.**[<=]**

A_19867 - ePA_Frontend des Versicherten: Kein Dokument gleichzeitig auf Whitelist und Blacklist
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass in einer APPC Policy kein Dokument gleichzeitig auf Black- und Whitelist gelistet ist.**[<=]**

A_19781 - ePA_Frontend des Versicherten: Abbilden eines entzogenen Zugriffs in der APPC Policy
Das ePA-Frontend des Versicherten MUSS einen einen Blacklist-Eintrag mit der DocumentEntry.uniqueID in der APPC-Policy LEI erstellen, wenn der Nutzer dieser LEI den Zugriff auf ein konkretes Dokument entzieht. **[<=]**

ENTWURF

6.2.7.5 Vertretung einrichten

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

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

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

A_15389 - ePA-Frontend des Versicherten: Daten des Vertreters
Das ePA-Frontend des Versicherten MUSS es dem Nutzer im Anwendungsfall "Vertretung einrichten" ermöglichen,den Namen, die Versicherten-ID und eine Benachrichtigungsadresse (E-Mail) für die Geräteautorisierung des Vertreters zu erfassen.**[<=]**

Die Berechtigungsdauer für Vertreter kann nicht zeitlich oder inhaltlich begrenzt werden. Wenn ein Vertreter berechtigt ist, auf die Dokumente zuzugreifen, dann kann der Vertreter dauerhaft auf alle Dokumente im Aktenkonto zugreifen, bis ihm die Berechtigung generell wieder entzogen wird.

A_15391-01 - ePA-Frontend des Versicherten: Vertretung einrichten
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.2 - Vertretung durch einen Versicherten einrichten" aus [gemSysL_ePA] gemäß TAB_FdV_135 umsetzen.

Tabelle 43: TAB_FdV_135 – Vertretung einrichten

Name	Vertretung einrichten
Auslöser	Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter
Vorbedingung	Die Versicherten-ID, der Name und die Benachrichtigungsadresse des Vertreters für die Geräteautorisierung sind bekannt. Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Der Vertreter ist zum Zugriff auf das Aktenkonto berechtigt. Das notwendige Schlüsselmaterial ist in der Autorisierung hinterlegt. Die Policy Document für den Vertreter ist in der Dokumentenverwaltung hinterlegt.
Standardablauf	Aktivitäten im Standardablauf 1. AuthorizationKey für Vertreter erstellen 2. Schlüsselmaterial im ePA-Aktensystem speichern 3. Policy Document für Vertreter erstellen 4. Policy Document in Dokumentenverwaltung laden

[<=]

ENTWURF

A_15396-01 - ePA-Frontend des Versicherten: Vertretung einrichten - AuthorizationKey erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung einrichten" einen AuthorizationKey für den Vertreter mit `AuthorizationType` = DOCUMENT_AUTHORIZATION erstellen.**[<=]**

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

A_15397-01 - ePA-Frontend des Versicherten: Vertretung einrichten - Schlüsselmaterial im ePA-Aktensystem speichern
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung einrichten" für das Hochladen des Schlüsselmaterials des Vertreters in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit den Eingangsparametern `AuthorizationKey` = erstellter AuthorizationKey und `NotificationInfoRepresentative` = Benachrichtigungsadresse für die Geräteautorisierung ausführen.**[<=]**

A_15398-01 - ePA-Frontend des Versicherten: Vertretung einrichten - Policy Document erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung einrichten", ein Policy Document für den zu berechtigenden Vertreter erstellen.**[<=]**

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

A_15399-01 - ePA-Frontend des Versicherten: Vertretung einrichten - Policy Document hochladen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung einrichten" zum Hochladen des Policy Documents in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für Policy Documents ausführen.**[<=]**

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

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

A_15400 - ePA-Frontend des Versicherten: PDF mit Information für Vertretung
Das ePA-Frontend des Versicherten MUSS dem Versicherten die Möglichkeit geben, ein druckbares PDF mit den Informationen für die Vertretung zu erzeugen. Das Dokument muss die folgenden Informationen des Versicherten, welcher vertreten wird, beinhalten:

- Versicherten-ID
- FQDN des Anbieter

[<=]

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

ENTWURF

6.2.7.6 Berechtigung für Kostenträger vergeben

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

A_17436 - ePA-Frontend des Versicherten: Kostenträger in Verzeichnisdienst der TI finden
Das ePA-Frontend des Versicherten SOLL es dem Nutzer mittels der Aktivität "Suchanfrage Verzeichnisdienst der TI" ermöglichen, einen Kostenträger im Verzeichnisdienst zu suchen und für die Vergabe von Berechtigungen auszuwählen.**[<=]**

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

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

Das Verschlüsselungszertifikat im Ergebnis der Abfrage beinhaltet die Telematik-ID (siehe [gemSpec_PKI#Tab_SMCB_TID_GKVSV]) des zu berechtigenden KTR.

A_17188 - ePA-Frontend des Versicherten: Bestätigung Berechtigung für Kostenträger
Das ePA-Frontend des Versicherten MUSS, bevor es eine Berechtigung an einen Kostenträger vergibt, eine Bestätigung vom Nutzer einholen. Hierbei ist der Name des zu berechtigenden Kostenträgers kenntlich zu machen.**[<=]**

A_17189-01 - ePA-Frontend des Versicherten: Berechtigung an Kostenträger für Aktenkonto vergeben
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.1 - Berechtigung durch einen Versicherten vergeben" aus [gemSysL_ePA] für den Kostenträger, für den eine Berechtigung vergeben werden soll, gemäß TAB_FdV_171 umsetzen.

Tabelle 44: TAB_FdV_171 – Berechtigung an Kostenträger für Aktenkonto vergeben

Name	Berechtigung an Kostenträger für Aktenkonto vergeben
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Ein Verschlüsselungszertifikat, die Telementik-ID und der Name des KTR sind bekannt. Der Nutzer hat die Vergabe der Berechtigung bestätigt.
Nachbedingung	Der Kostenträger ist zum Zugriff auf das Aktenkonto berechtigt. Das notwendige Schlüsselmaterial ist in der Autorisierung hinterlegt.

ENTWURF

	Ein Policy Document für den Kostenträger ist in der Dokumentenverwaltung hinterlegt.
Standardablauf	Aktivitäten im Standardablauf 1. AuthorizationKey für Kostenträger erstellen 2. Schlüsselmaterial im ePA-Aktensystem speichern 3. Policy Document für Kostenträger erstellen 4. Policy Document in Dokumentenverwaltung laden

[<=]

A_17190-01 - ePA-Frontend des Versicherten: Berechtigung Kostenträger vergeben - AuthorizationKey erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an Kostenträger für Aktenkonto vergeben" einen AuthorizationKey mit `AuthorizationType` = DOCUMENT_AUTHORIZATION für den zu berechtigenden Kostenträger erstellen.**[<=]**

A_17191-01 - ePA-Frontend des Versicherten: Berechtigung Kostenträger vergeben - Schlüsselmaterial im ePA-Aktensystem speichern
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an Kostenträger für Aktenkonto vergeben" für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey` = erstellter AuthorizationKey ausführen. Der optionale Parameter `NotificationInfoRepresentative` wird nicht belegt.**[<=]**

A_17192-01 - ePA-Frontend des Versicherten: Berechtigung Kostenträger vergeben - Policy Document erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an Kostenträger für Aktenkonto vergeben" ein Policy Document für den zu Berechtigenden erstellen.**[<=]**

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

A_17193-01 - ePA-Frontend des Versicherten: Berechtigung Kostenträger vergeben - Policy Document hochladen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an Kostenträger für Aktenkonto vergeben" zum Hochladen des Policy Documents in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für Policy Documents ausführen.
[<=]

6.2.7.7 Vergebene Berechtigungen anzeigen

Mit diesem Anwendungsfall kann ein Nutzer eine Liste der für das Aktenkonto vergebenen Berechtigungen anzeigen lassen. Diese Liste beinhaltet die

ENTWURF

zugriffsberechtigten Leistungserbringer, die berechtigten Vertreter und zugriffsberechtigte Kostenträger sowie die Details zu Berechtigungen (für LEI: Berechtigungsdauer, Zugriff auf durch den Versicherten eingestellte Dokumente).

A_15401-01 - ePA-Frontend des Versicherten: Vergebene Berechtigungen anzeigen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.5 - Berechtigungen durch einen Versicherten auflisten" aus [gemSysL_ePA] gemäß TAB_FdV_137 umsetzen.

Tabelle 45: TAB_FdV_137 – Vergebene Berechtigungen anzeigen

Name	Vergebene Berechtigungen anzeigen
Auslöser	• Aufruf des Anwendungsfalls in der GUI • Anwendungsfall "Anbieter wechseln"
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Die Liste der für das Aktenkonto vergebenen Berechtigungen kann angezeigt und durch den Nutzer bearbeitet werden.
Standardablauf	Aktivitäten im Standardablauf 1. Vergebene Berechtigungen bestimmen

[<=]

A_15402-01 - ePA-Frontend des Versicherten: Berechtigungen anzeigen - Berechtigungen bestimmen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vergebene Berechtigungen anzeigen" die übergreifende Aktivität "Vergebene Berechtigungen bestimmen" ausführen.**[<=]**

A_15403-02 - ePA-Frontend des Versicherten: Ergebnisliste Berechtigungen Felder
Das ePA-Frontend des Versicherten MUSS im Ergebnis der Suche nach Berechtigungen mindestens

- Name der Leistungserbringerinstitution, des Kostenträgers bzw. des Vertreters im Klartext,
- für LEI: Zugriffsrecht gemäß grobgranularer Berechtigung (normal vs. erweitert)
- für LEI: Berechtigte Kategorien gemäß mittelgranularer Berechtigung
- für LEI: Explizit erlaubte oder geblockte Dokumente gemäß feingranularer Berechtigung
- für LEI: eingestellte und verbleibende Berechtigungsdauer

anzeigen.
[<=]

ENTWURF

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

A_15405-01 - ePA-Frontend des Versicherten: Ergebnisliste Berechtigungen drucken und speichern
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, das Ergebnis der Suche nach Berechtigungen auszudrucken oder lokal zu speichern.**[**<=**]**

Das lokale Speichern kann im PDF-Format angeboten werden.

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

6.2.7.8 Eingerichtete Vertretungen anzeigen

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

A_15406 - ePA-Frontend des Versicherten: Liste "ich bin Vertreter für" anzeigen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine Liste mit den im ePA-Frontend des Versicherten für ihn konfigurierten Vertretungen anderer Versicherter anzuzeigen.**[**<=**]**

6.2.7.9 Bestehende Berechtigungen verwalten

6.2.7.9.1 Berechtigung für LEI ändern

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

A_15407-02 - ePA-Frontend des Versicherten: Bestehende Berechtigungen von LEI ändern
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, für bereits berechtigte LEI grob-, mittel- und feingranulare Berechtigungsvorgaben und die Berechtigungsdauer anzupassen.**[**<=**]**

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

Wenn die Berechtigungsdauer geändert wird, dann muss ein neuer AuthorizationKey auf Basis eines Verschlüsselungszertifikates der LEI erzeugt werden. Ein Verschlüsselungszertifikat kann mit der Aktivität "Suchanfrage Verzeichnisdienst der TI" mit dem Suchkriterium Telematik-ID ermittelt werden. Die Telematik-ID der LEI lässt sich aus dem Policy Document bestimmen.

A_15408-01 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" aus [gemSysL_ePA] für jede LEI, für die Konfiguration seiner Berechtigung geändert werden soll, gemäß TAB_FdV_138 umsetzen.

Tabelle 46: TAB_FdV_138 – Berechtigung für LEI ändern

Name	Berechtigung für LEI ändern

ENTWURF

Auslöser	• Aufruf der Aktion zum Ändern der Berechtigung in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat die Konfiguration für eine Berechtigung geändert und die Änderung der Einstellung bestätigt. Das Policy Document, der AuthorizationKey und ggf. ein Verschlüsselungszertifikat für die LEI stehen zur Verfügung.
Nachbedingung	Die geänderten Einstellungen für die Berechtigung der LEI sind als Policy Document in der Dokumentenverwaltung hinterlegt. Die Gültigkeitsdauer des Schlüsselmaterials in der Autorisierung ist ggf. aktualisiert.
Standardablauf	Aktivitäten im Standardablauf 1. Policy Document für LEI anpassen 2. Wenn die Berechtigungsdauer geändert wurde a. AuthorizationKey für LEI erstellen b. Schlüsselmaterial im ePA-Aktensystem ersetzen 3. Neues Policy Document in Dokumentenverwaltung laden

[<=]

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

A_15409-01 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern - Policy Document anpassen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI ändern" das Policy Document entsprechend der gewählten Einstellungen für Berechtigungsdauer und/oder Aktenanteil anpassen.**[<=]**

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

A_15412-01 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern - AuthorizationKey für LEI erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI ändern", wenn die Einstellung für Berechtigungsdauer geändert wurde, einen AuthorizationKey mit `AuthorizationType` = DOCUMENT_AUTHORIZATION und `validTo` entsprechend der vom Nutzer festgelegten Berechtigungsdauer für die zu berechtigende LEI erstellen.**[<=]**

A_15413-01 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern - Schlüsselmaterial im ePA-Aktensystem ersetzen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI ändern", wenn die Einstellung für Berechtigungsdauer geändert wurde, für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem ersetzen" mit den Eingangsparametern `NewAuthorizationKey` = geänderter AuthorizationKey ausführen.**[<=]**

ENTWURF

A_15414-01 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern - Policy Document in Dokumentenverwaltung laden
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI ändern" für das Hochladen des Policy Documents in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für das angepasste Policy Documents ausführen.**[<=]**

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

6.2.7.9.2 Berechtigung für LEI löschen

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

A_15415 - ePA-Frontend des Versicherten: LEI zum Entzug der Berechtigung markieren
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, berechtigte LEI für den Entzug der Berechtigung auszuwählen.**[<=]**

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

A_15416-01 - ePA-Frontend des Versicherten: Berechtigung für LEI löschen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" aus [gemSysL_ePA] für jeden berechtigten LEI, dessen Berechtigung entzogen werden soll, gemäß TAB_FdV_139 umsetzen.

Tabelle 47: TAB_FdV_139 – Berechtigung löschen

Name	Berechtigung für LEI löschen
Auslöser	• Aufruf der Aktion zum Löschen der Berechtigung in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat eine LEI zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt. Das Policy Document und Informationen zum AuthorizationKey der LEI stehen zur Verfügung.
Nachbedingung	Die LEI ist nicht mehr für den Zugriff auf das Aktenkonto autorisiert.
Standardablauf	Aktivitäten im Standardablauf 1. Policy Document in Dokumentenverwaltung löschen 2. Schlüsselmaterial in ePA-Aktensystem löschen

[<=]

ENTWURF

A_15417-02~~A_15417-01~~ - ePA-Frontend des Versicherten: Berechtigung für LEI löschen - Policy Document in Dokumentenverwaltung löschen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI löschen" für das Löschen des Policy Document in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung löschen" mit einer ~~RemoveDocuments~~RemoveMetadata Message für den über die XDS-Metadaten ermittelten Dokument Identifier des Policy Documents der LEI ausführen.**[<=]**

Die Telematik-ID der LEI kann aus dem Policy Document bestimmt werden.

A_15418-01 - ePA-Frontend des Versicherten: Berechtigung für LEI löschen - Schlüsselmaterial in ePA-Aktensystem löschen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI löschen" für das Löschen des Schlüsselmaterials die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem löschen" mit dem Eingangsparameter`ActorID` = Telematik-ID der LEI ausführen.**[<=]**

6.2.7.9.3 Berechtigung für Vertreter löschen

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

A_16044 - ePA-Frontend des Versicherten: Vertreter zum Entzug der Berechtigung markieren
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, berechtigte Vertreter für den Entzug der Berechtigung auszuwählen.**[<=]**

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

A_16045-01 - ePA-Frontend des Versicherten: Berechtigung für Vertreter löschen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" aus [gemSysL_ePA] für jeden berechtigten Vertreter, dessen Berechtigung entzogen werden soll, gemäß TAB_FdV_168 umsetzen.

Tabelle 48: TAB_FdV_168 – Berechtigung für Vertreter löschen

Name	Berechtigung für Vertreter löschen
Auslöser	• Aufruf der Aktion zum Löschen der Berechtigung in der GUI
Akteur	Versicherter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat einen Vertreter zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt. Informationen zum AuthorizationKey und das Policy Document des Vertreters stehen zur Verfügung.
Nachbedingung	Der Vertreter ist nicht mehr für den Zugriff auf das Aktenkonto autorisiert.

ENTWURF

Standardablauf	Aktivitäten im Standardablauf 1. Policy Document in Dokumentenverwaltung löschen 2. Schlüsselmaterial in ePA-Aktensystem löschen

[<=]

A_16046-02~~A_16046-01~~ - ePA-Frontend des Versicherten: Berechtigung für Vertreter löschen - Policy Document in Dokumentenverwaltung löschen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für Vertreter löschen" für das Löschen des Policy Document in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung löschen" mit einer ~~RemoveDocuments~~RemoveMetadata Message für den über die XDS-Metadaten ermittelten Dokument Identifier des Policy Documents des Vertreters ausführen.**[<=]**

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

A_16047-01 - ePA-Frontend des Versicherten: Berechtigung für Vertreter löschen - Schlüsselmaterial in ePA-Aktensystem löschen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für Vertreter löschen" für das Löschen des Schlüsselmaterials die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem löschen" mit dem Eingangsparameter`ActorID` = Versicherten-ID für Vertreter ausführen.**[<=]**

6.2.7.9.4 Berechtigung für Kostenträger löschen

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

A_17194 - ePA-Frontend des Versicherten: Kostenträger zum Entzug der Berechtigung markieren
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, berechtigte Kostenträger für den Entzug der Berechtigung auszuwählen.**[<=]**

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

A_17195-01 - ePA-Frontend des Versicherten: Berechtigung für Kostenträger löschen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" aus [gemSysL_ePA] für den Kostenträger, deren Berechtigung entzogen werden soll, gemäß TAB_FdV_166 umsetzen.

Tabelle 49: TAB_FdV_166 – Berechtigung für Kostenträger löschen

Name	Berechtigung für Kostenträger löschen
Auslöser	• Aufruf der Aktion zum Löschen der Berechtigung in der GUI
Akteur	Versicherter oder berechtigter Vertreter

ENTWURF

Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat einen Kostenträger zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt. Das Policy Document und Informationen zum AuthorizationKey des Kostenträgers stehen zur Verfügung.
Nachbedingung	Der Kostenträger ist nicht mehr für den Zugriff auf das Aktenkonto autorisiert.
Standardablauf	Aktivitäten im Standardablauf 1. Policy Document in Dokumentenverwaltung löschen 2. Schlüsselmaterial in ePA-Aktensystem löschen

[<=]

A_17196-02~~A_17196-01~~ - ePA-Frontend des Versicherten: Berechtigung für Kostenträger löschen - Policy Document in Dokumentenverwaltung löschen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für Kostenträger löschen" für das Löschen des Policy Document in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung löschen" mit einer ~~RemoveDocuments~~RemoveMetadata Message für den über die XDS-Metadaten ermittelten Dokument Identifier des Policy Documents des Kostenträgers ausführen.**[<=]**

Die Telematik-ID des Kostenträgers kann aus dem Policy Document bestimmt werden.

A_17197-01 - ePA-Frontend des Versicherten: Berechtigung für Kostenträger löschen - Schlüsselmaterial in ePA-Aktensystem löschen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für Kostenträger löschen" für das Löschen des Schlüsselmaterials die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem löschen" mit dem Eingangsparameter`ActorID` = Telematik-ID des Kostenträgers ausführen.**[<=]**

6.2.8 Dokumentenverwaltung

6.2.8.1 Dokumente einstellen

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

A_15464 - ePA-Frontend des Versicherten: Dokumente einstellen - Zugriffsberechtigungen anzeigen und bestätigen
Das ePA-Frontend des Versicherten MUSS, wenn die Option "Dokumente einstellen: Berechtigte anzeigen" aktiv ist, dem Nutzer vor dem Anwendungsfall "Dokumente einstellen" alle für die Dokumente potentiell zugriffsberechtigten Leistungserbringerinstitutionen anzeigen und eine Bestätigung vom Nutzer einholen.**[<=]**

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

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

ENTWURF

Zugriffsberechtigt sind alle Vertreter und alle LEI mit der Berechtigung für vom Versicherten eingestellte Dokumente.

A_15465 - ePA-Frontend des Versicherten: Dokumente einstellen - Hinweis Änderung Zugriffsberechtigungen
Das ePA-Frontend des Versicherten MUSS es ermöglichen, die Anwendungsfälle zum Verwalten von Berechtigungen auszuführen, wenn der Nutzer vor dem Anwendungsfall "Dokumente einstellen" die Zugriffsberechtigungen nicht bestätigt.**[<=]**

A_15286 - ePA-Frontend des Versicherten: Auswahl von Dokumenten
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, ein oder mehrere Dokumente aus lokal eingebundenem Speicher auszuwählen, um sie in die ePA einzustellen.**[<=]**

A_15462 - ePA-Frontend des Versicherten: Dokumente einstellen - Eingabe der Metadaten zu Dokumenten
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, zu jedem einzustellenden Dokument Metadaten einzugeben.**[<=]**

Für Festlegungen zur Eingabe von Metadaten siehe "5.4.5- Eingabe Metadaten für einzustellende Dokumente ".

Das ePA-Frontend des Versicherten kann eine Prüfung der Metadaten auf Vollständigkeit und Korrektheit durchführen und den Nutzer bei fehlenden oder falschen Werten zur Korrektur auffordern.

A_20223-01 - ePA-Frontend des Versicherten: Zusätzliche Auswahl der Kategorie "Dokumente der eGA"
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, zusätzlich die Dokumentenkategorie "ega" auszuwählen, wenn der Nutzer eGA-Dokumente hochladen möchte.**[<=]**

A_15458-01 - ePA-Frontend des Versicherten: Dokumente einstellen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 4.2 - Dokumente durch einen Versicherten einstellen" aus [gemSysL_ePA] gemäß TAB_FdV_146 umsetzen.

Tabelle 50: TAB_FdV_146 – Dokumente einstellen

Name	Dokumente einstellen
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Die hochzuladenden Dokumente sind im lokal eingebundenen Speicher verfügbar. Der Nutzer hat Metadaten zu den einzustellenden Dokumenten erfasst.
Nachbedingung	Die Dokumente sind in der ePA für alle Berechtigten verfügbar.

ENTWURF

Standardablauf	Aktivitäten im Standardablauf 1. Prüfung auf zulässige Dateigröße 2. Prüfung der Metadaten zu Dokumenten 3. für jedes Dokument: a. Dokument verschlüsseln b. Dokumentenschlüssel löschen 4. Dokumentenset in Dokumentenverwaltung hochladen

[<=]

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

A_15461-02 - ePA-Frontend des Versicherten: Dokumente einstellen - Prüfung Dateigröße
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" die Größe jedes durch den Nutzer ausgewählten Dokuments prüfen und ablehnen, wenn das Dokument die Größe von 25 MB überschreitet.**[<=]**

Das bedeutet, dass Dokumente bis zu einer Größe von 25 MB = 25 * (1024)^2 Byte in die ePA hochgeladen werden. Grundlage für die Berechnung der Dokumentengröße ist das Dokument ohne Verschlüsselung durch den Dokumentenschlüssel und ohne Transportcodierung. Größere Dokumente können nicht hochgeladen werden.

A_15463-01 - ePA-Frontend des Versicherten: Dokumente einstellen - Prüfung XDS-Metadaten
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" die XDS-Metadaten auf Vollständigkeit prüfen und bei fehlenden oder fehlerhaften Werten den Anwendungsfall abbrechen.**[<=]**

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

A_15466-01 - ePA-Frontend des Versicherten: Dokumente einstellen - Dokument verschlüsseln
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" für jedes zu übermittelnde Dokument die Aktivität "Dokument verschlüsseln" gemäß TAB_FdV_147 umsetzen.

ENTWURF

Tabelle 51: TAB_FdV_147 – Dokumente einstellen - Dokument verschlüsseln

Plattformbaustein PL_TUC_SYMM_ENCIPHER für Dokument nutzen	Dokument mit PL_TUC_SYMM_ENCIPHER verschlüsseln Eingangsdaten: • Dokument • Der optionalen Parameter Cert und AD werden nicht verwendet. Rückgabedaten: • verschlüsseltes Dokument • Dokumentenschlüssel Der Dokumentenschlüssel wird in der Aktivität erzeugt und an den Aufrufer zurückgegeben
Plattformbaustein PL_TUC_SYMM_ENCIPHER für Dokumentenschlüssel nutzen	Dokumentenschlüssel mit PL_TUC_SYMM_ENCIPHER verschlüsseln Eingangsdaten: • Dokument: Dokumentenschlüssel • Aktenschlüssel aus Session-Daten • Der optionale Parameter AD wird nicht verwendet. Rückgabedaten: • verschlüsselter Dokumentschlüssel

[<=]

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

A_15467-01 - ePA-Frontend des Versicherten: Dokumente einstellen - Dokumentenschlüssel löschen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" in der Aktivität "Dokument verschlüsseln" erstellte Dokumentenschlüssel nach dem Ende der Aktivität löschen.**[<=]**

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

Für Nutzungsvorgaben siehe Kapitel "Versichertendokumente".

A_15468-01 - ePA-Frontend des Versicherten: Dokumente einstellen - Dokumentenset in Dokumentenverwaltung hochladen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" zum Hochladen des Dokumentenset in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für Versichertendokumente ausführen.**[<=]**

ENTWURF

A_19050 - FdV-Warnhinweis grobgranulare Berechtigung
Das FdV MUSS dem Versicherten beim Hochladen von Dokumenten auf eine gegebenenfalls fehlende Möglichkeit hinweisen, die Einwilligung sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen der elektronischen Patientenakte zu beschränken.**[<=]**

6.2.8.2 Dokumente suchen

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

A_15469 - ePA-Frontend des Versicherten: Suchparameter für Dokumente
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Suchparameter auf Basis der XDS-Metadaten für eine Suchanfrage einzugeben. Für Suchparameter mit fest vorgegebenem Wertebereich muss der Nutzer eine Auswahlliste nutzen können.**[<=]**

Folgende Suchanfragen sollen mindestens möglich sein~~:~~ (ggf. mit zusätzlichem Nachfiltern auf dem FdV):

- Suche nach allen medizinischen Dokumenten im Aktenkonto
- Suche nach Ersteller bzw. Einstellendem ~~(XDSDocumentEntry.author)~~ ~~(für~~ XDSDocumentEntry.authorInstitution($XDSSubmissionSetAuthorPerson, $XDSDocumentEntryAuthorPerson, $XDSDocumentEntryAuthorInstitution siehe [gemSpec_Dokumentenverwaltung#A_18070] und A_17854~~-01~~)
- Suche nach in einem Zeitraum erstellten bzw. eingestellten Dokumenten ~~(XDSDocumentEntry.creationTime / XDSSubmissionSet.submissionTime~~($XDSDocumentEntryCeationTimeFrom/To / $XDSSubmissionSetSubmissionTimeFrom/To)
- Suche nach Dokumententitel (siehe [gemSpec_Dokumentenverwaltung#A_17185] und A_17854~~-01~~)
- Suche nach durch LEIs bereitgestellte Dokumente ~~(XDSDocumentEntry.confidentialityCode="LEI")~~
- Suche nach Dokumenten mit Kennzeichnung "Versicherteninformation"(siehe [gemSpec_DM_ePA#A_14986])
- Suche nach durch Krankenkassen bereitgestellte Informationen ~~(XDSDocumentEntry.confidentialityCode="KTR")~~

A_15470-01 - ePA-Frontend des Versicherten: Dokumente suchen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 4.4 - Dokumente durch einen Versicherten suchen" aus [gemSysL_ePA] gemäß TAB_FdV_148 umsetzen.

Tabelle 52: TAB_FdV_148 – Dokumente suchen

Name	Dokumente suchen
Auslöser	• Auswahl der Aktion zur Suche von Dokumenten in der GUI

ENTWURF

Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat Suchkriterien eingegeben.
Nachbedingung	Falls die Anfrage eine nicht-leere Ergebnismenge liefert, stehen die XDS-Metadaten der Dokumente zur Auflistung für den Nutzer bereit.
Standardablauf	Aktivitäten im Standardablauf 1. Suchanfrage ausführen

[<=]

A_15471-01 - ePA-Frontend des Versicherten: Dokumente suchen - Suchanfrage ausführen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente suchen" zum Ausführen der Suchanfrage die übergreifende Aktivität "Suche nach Dokumenten in Dokumentenverwaltung" mit einer query:AdhocQueryRequest_Message entsprechend der von Nutzer vorgegebenen Suchkriterien ausführen.**[<=]**

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

A_15472 - ePA-Frontend des Versicherten: Ergebnisliste Dokumente anzeigen
Das ePA-Frontend des Versicherten MUSS dem Nutzer das Ergebnis der Suche nach Dokumenten anzeigen.**[<=]**

A_21134 - ePA-Frontend des Versicherten: Unscharfe Ergebnisse in Ergebnisliste kennzeichnen
Das ePA-Frontend des Versicherten SOLL etwaige unscharfe Suchergebnisse (siehe gemSpec_Dokumentenverwaltung#A_21132) in der Ergebnismenge als solche kennzeichnen können.
[<=]

A_15473-01 - ePA-Frontend des Versicherten: Ergebnisliste Dokumente drucken oder speichern
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, das Ergebnis der Suche nach Dokumenten auszudrucken oder lokal zu speichern.**[<=]**

Das lokale Speichern kann im PDF Format angeboten werden.

A_15474 - ePA-Frontend des Versicherten: Suche verfeinern
Das ePA-Frontend des Versicherten MUSS die Ergebnisse einer Suchanfrage zusammen mit den zur Suche verwendeten Parameter anzeigen und es dem Nutzer ermöglichen, die Suchparameter anzupassen und die Suchanfrage erneut auszuführen.**[<=]**

6.2.8.3 Dokument herunterladen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter Dokumente aus dem Aktenkonto zum Anzeigen oder lokalen Speichern herunterladen.

ENTWURF

A_15475 - ePA-Frontend des Versicherten: Dokumente zum Herunterladen markieren
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Dokumente aus dem Ergebnis einer Suchanfrage zum Herunterladen (bspw. für die Anzeige oder lokales Speichern) zu markieren.**[<=]**

A_15476-01 - ePA-Frontend des Versicherten: Dokumente herunterladen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 4.10 - Dokumente durch einen Versicherten anzeigen" aus [gemSysL_ePA] gemäß TAB_FdV_149 umsetzen.

Tabelle 53: TAB_FdV_149 – Dokumente aus Aktenkonto herunterladen

Name	Dokumente herunterladen
Auslöser	• Auswahl der Aktion zum Herunterladen, Anzeigen oder lokalen Speichern für markierte Dokumente in einer Suchanfrage in der GUI
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Es wurde eine Suchanfrage nach Dokumenten in der Dokumentenverwaltung durchgeführt. Die Dokumente sind im Ergebnis einer Suchanfrage selektiert. Die Identifier der Dokumente (uniqueId) sind aus den Metadaten der Suchanfrage bekannt.
Nachbedingung	Die Dokumente liegen unverschlüsselt temporär in einem Speicher im Gerät des Versicherten vor.
Standardablauf	Aktivitäten im Standardablauf 1. markierte Dokumente herunterladen und entschlüsseln

[<=]

A_15477-01 - ePA-Frontend des Versicherten: Dokumente herunterladen - Herunterladen und Entschlüsseln
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente herunterladen" zum Herunterladen und Entschlüsseln der Dokumente die übergreifende Aktivität "Dokumentenset aus Dokumentenverwaltung herunterladen" mit einer RetrieveDocumentSet_Message für alle über die XDS-Metadaten ermittelten Dokument Identifier der ausgewählten Dokumente ausführen.**[<=]**

A_15478 - ePA-Frontend des Versicherten: Dokument lokal speichern
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, ein aus dem Aktenkonto heruntergeladenes Dokument im lokalen Speicher persistent abzulegen.**[<=]**

A_15479 - ePA-Frontend des Versicherten: Dokument mit Standardprogramm anzeigen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, wenn für einen gegebenen Dateitypen ein Standardprogramm verfügbar ist, ein aus dem Aktenkonto heruntergeladenes Dokument mit dem Standardprogramm anzuzeigen.**[<=]**

ENTWURF

6.2.8.4 Dokumente im Aktenkonto löschen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter Dokumente im Aktenkonto löschen. Die Dokumente sind damit unwiederbringlich aus dem ePA-Aktensystem entfernt.

A_15480 - ePA-Frontend des Versicherten: Dokumente zum Löschen markieren
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Dokumente aus dem Ergebnis einer Suchanfrage zum Löschen zu markieren.**[<=]**

A_15482 - ePA-Frontend des Versicherten: Dokumente löschen - Bestätigung
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente löschen" vom Nutzer eine Bestätigung einholen, dass die markierten Dokumente gelöscht werden sollen und die Möglichkeit geben, das Löschen abzubrechen.**[<=]**

A_15481-01 - ePA-Frontend des Versicherten: Dokumente löschen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 4.8 - Dokumente durch einen Versicherten löschen" aus [gemSysL_ePA] gemäß TAB_FdV_150 umsetzen.

Tabelle 54: TAB_FdV_150 – Dokumente löschen

Name	Dokumente löschen
Auslöser	• Auswahl der Aktion Löschen für zum Löschen markierte Dokument in einer Suchanfrage in der GUI
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Es wurde eine Suchanfrage nach Dokumenten in der Dokumentenverwaltung durchgeführt. Die zu löschenden Dokumente sind im Ergebnis einer Suchanfrage selektiert. Die Identifier für die Dokumente sind aus den Metadaten der Suchanfrage bekannt. Der Nutzer hat das Löschen bestätigt.
Nachbedingung	Die Dokumente sind im Aktenkonto unwiederbringlich gelöscht.
Standardablauf	Aktivitäten im Standardablauf 1. Dokumentenset in Dokumentenverwaltung löschen

[<=]

A_15483-03~~A_15483-02~~ - ePA-Frontend des Versicherten: Dokumente löschen - Löschnachricht Dokumentenverwaltung
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente löschen" zum Löschen der Dokumente die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung löschen" mit einer ~~RemoveDocuments~~RemoveMetadata Message für alle über die XDS-Metadaten ermittelten Dokument Identifier (entryUUIDs) der ausgewählten Dokumente ausführen.**[<=]**

ENTWURF

A_20722 - ePA-Frontend des Versicherten: Dokumente löschen – Hinweis auf mögliche versorgungsrelevante Folgen
Das ePA-Frontend des Versicherten MUSS dem Nutzer im Anwendungsfall "Dokumente löschen" vor dem Löschen von Dokumenten in der elektronischen Patientenakte auf die möglichen versorgungsrelevanten Folgen hinweisen.**[<=]**

6.2.9 Protokollverwaltung

6.2.9.1 Zugriffsprotokoll einsehen

Bei der Nutzung eines Aktenkontos durch LEI, durch berechtigte Vertreter oder den Aktenkontoinhaber werden Aktivitäten protokolliert, damit der Aktenkontoinhaber oder ein berechtigter Vertreter diese Aktivitäten nachvollziehen kann. Dazu zählen Zugriffe auf die Dokumente und seine Metadaten (§ 291a-konformes Zugriffsprotokoll) sowie auch Aktivitäten mit administrativem Charakter (Verwaltungsprotokoll).

Die verschiedenen Aktivitäten sind in [gemSpec_DM_ePA#A_14505 - Event Codes für Protokollereignisse] gelistet.

Die Protokolldaten des § 291a-konformen Zugriffsprotokolls werden im Aktenkonto (Komponente Dokumentenverwaltung) abgelegt. Die Protokolldaten des Verwaltungsprotokolls werden in verschiedenen Komponenten des ePA-Aktensystems vorgehalten. Die Daten müssen für eine Anzeige separat abgefragt werden.

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter die Protokolldaten über die Zugriffe auf das Aktenkonto des Versicherten einsehen.

A_15484-01 - ePA-Frontend des Versicherten: Protokoll einsehen - Hilfetext
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, den folgenden Text zur Erläuterung des Anwendungsfalls anzuzeigen.
"Sie können die Protokolldaten aller Zugriffe auf Ihr Aktenkonto einsehen. Dies umfasst

- Suche nach Dokumenten
- Einstellen, Herunterladen und Löschen von Dokumenten
- Vergabe, Ändern und Löschen von Berechtigungen
- Login"

[<=]

Die Protokolleinträge werden im Aktensystem nach Ablauf der in [gemSpec_ePA_FdV#A_19051] beschriebenen Frist gelöscht.

A_15485-01 - ePA-Frontend des Versicherten: Protokolldaten einsehen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 6.1 - Protokolldaten durch einen Versicherten einsehen" aus [gemSysL_ePA] gemäß TAB_FdV_151 umsetzen.

Tabelle 55: TAB_FdV_151 – Protokolldaten einsehen

Name	Protokolldaten einsehen
Auslöser	• Auswahl der Aktion zum Anzeigen der Protokolldaten in der GUI
Akteur	Versicherter bzw. ein berechtigter Vertreter

ENTWURF

Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Die Protokolldaten können dem Nutzer angezeigt werden.
Standardablauf	Aktivitäten im Standardablauf 1. Protokolldaten Dokumentenverwaltung abfragen 2. Protokolldaten Autorisierung abfragen 3. Protokolldaten Authentisierung abfragen

3868 **[<=]**

3869 **A_15486-01 - ePA-Frontend des Versicherten: Protokoll einsehen -**
3870 **Dokumentenverwaltung abfragen**
3871 Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Protokolldaten einsehen"
3872 die Aktivität "Protokolldaten Dokumentenverwaltung abfragen" gemäß TAB_FdV_152
3873 umsetzen.

3874
3875 **Tabelle 56: TAB_FdV_152 – Protokolldaten einsehen - Dokumentenverwaltung abfragen**

`I_Account_Management_Insurant::GetAuditEvents` Request erstellen	Eingangsdaten: • `AuthenticationAssertion` aus Session-Daten
`I_Account_Management_Insurant::GetAuditEvents` Response verarbeiten	Rückgabedaten: • Audit Event List

3876 **[<=]**

3877

3878 **A_15487-01 - ePA-Frontend des Versicherten: Protokoll einsehen -**
3879 **Autorisierung abfragen**
3880 Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Protokolldaten einsehen"
3881 die Aktivität "Protokolldaten Autorisierung abfragen" gemäß TAB_FdV_153 umsetzen.

3882
3883 **Tabelle 57: TAB_FdV_153 – Protokolldaten einsehen - Autorisierung abfragen**

`I_Authorization_Management_Insurant::getAuditEvents` Request erstellen	Eingangsdaten: • `AuthenticationAssertion` aus Session-Daten • `RecordIdentifier` aus Session-Daten • `DeviceID` aus Gerät-Daten

ENTWURF

`I_Authorization_Management_Insurant::getAuditEvents` Response verarbeiten	Rückgabedaten: • AuditMessage[0..*]

[<=]

A_15488-01 - ePA-Frontend des Versicherten: Protokoll einsehen - Authentisierung abfragen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Protokolldaten einsehen" die Aktivität "Protokolldaten Authentisierung abfragen" gemäß TAB_FdV_154 umsetzen.

Tabelle 58: TAB_FdV_154 – Protokolldaten einsehen - Zugangsgateway des Versicherten abfragen

`I_Authentication_Insurant::getAuditEvents` Request erstellen	Eingangsdaten: • `AuthenticationAssertion` aus Session-Daten
`I_Authentication_Insurant::getAuditEvents` Response verarbeiten	Rückgabedaten: • AuditMessage[0..*]
Varianten/Alternati-ven	Wenn in der Abarbeitung der Operation ein Fehler auftritt und kein Resultset vorliegt, kann der Anwendungsfall fortgesetzt werden, denn dieses Resultset ist nicht Teil der Standard-Anzeige. Der Nutzer ist darauf hinzuweisen, dass keine Protokolleinträge zur Authentisierung abgerufen werden konnten.

[<=]

Die Ergebnisse der Abfragen an die Komponenten des ePA-Aktensystems werden vereint.

Die Information eines Protokolleintrages sind in [gemSpec_DM_ePA#A_14471 - Objektstruktur Eintrag für Protokoll] beschrieben.

Tabelle 59: TAB_FdV_155 – Felder im Protokolleintrag

Protokolldatum	Bezeichnung in GUI	Hinweis zur Anzeige	optional in Standard-Anzeige
Aufgerufene Operation	Art des Zugriffs auf das Aktenkonto	DisplayName anzeigen	
Datum und Uhrzeit des Zugriffs	Zeitpunkt des Zugriffs		

ENTWURF

Ergebnis der aufgerufenen Operation	Ergebnis Zugriff	0 - erfolgreich 1 - nicht erfolgreich	
UserID	Identifier des Nutzers		x
UserName	Name des Nutzers		
ObjectID	Identifier des Objektes, auf das zugegriffen wurde		x
ObjectName	Bezeichner des Objektes, auf das zugegriffen wurde		
ObjectDetail	Details zum zugegriffenen Objekt		~~x~~
DeviceID	Gerätekennung		x
Home-CommunityID des ePA-Aktensystems	ID des Aktenanbieters		x
Name des Aktenanbieters	Name des Aktenanbieters		x

A_15489-05~~A_15489-04~~ - ePA-Frontend des Versicherten: Standard-Anzeige für Protokolldaten

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

- ~~Alle Anwendungsfälle des § 291a-konformen Zugriffsprotokolls der Dokumentenverwaltung~~
- PHR-220 (Login Versicherter/Vertreter (Abruf der Berechtigung)
- PHR-230 (Login aus der ärztlichen Umgebung oder eines Kostenträgers)
- PHR-451 (Änderung E-Mail-Adresse)
- PHR-470 (Geräteverwaltung)
- PHR-510 (Hinzufügen eines Dokuments aus der ärztlichen Umgebung)
- PHR-520 (Suchanfrage aus der ärztlichen Umgebung)
- PHR-530 (Löschen eines Dokuments aus der ärztlichen Umgebung)
- PHR-540 (Abruf eines Dokuments aus der ärztlichen Umgebung)
- PHR-560 (Löschen von Dokumenten~~,~~ oder Ordnern ~~oder deren Verbindungen~~ aus der ärztlichen Umgebung)

ENTWURF

- PHR-610 (Hinzufügen eines Dokuments aus der privaten Umgebung)
- PHR-620 (Suchanfrage aus der privaten Umgebung)
- PHR-630 (Löschen eines Dokuments aus der privaten Umgebung)
- PHR-640 (Abruf eines Dokuments aus der privaten Umgebung)
  - ~~PHR-670 (Abruf des §291a-Protokolls aus der privaten Umgebung)~~
- ~~PHR-810~~680 (Löschen von Dokumenten, Ordnern ~~oder deren Verbindungen~~aus der privaten Umgebung)
- PHT-690 (Änderungen der Vertraulichkeitsstufe von Dokumenten aus der privaten Umgebung)
- PHR-710 (Hinzufügen eines Dokuments aus der Kostenträger-Umgebung)
- PHR-810 (Start eines Umschlüsselungsvorgangs)
  - ~~PHR-820 (Herunterladen aller Dokumentenschlüssel)~~
  - ~~PHR-830 (Hochladen aller Dokumentenschlüssel)~~
- ~~PHR-840 (~~870 (Erfolgreicher Abschluss des Umschlüssungsvorgangs durch den Versicherten)
- PHR-860 (Abbruch des Umschlüsselungsvorgangs)
  - ~~PHR-860 (Rollback des Umschlüsselungsvorgangs in Dokumentenverwaltung (Wiederherstellung des alten Schlüsselmaterials)~~
  - ~~Folgende Anwendungsfälle aus dem Verwaltungsprotokoll der Autorisierung~~
    - ~~PHR-310 (Hinzufügen des Empfängerschlüssels aus der ärztlichen Umgebung)~~
    - ~~PHR-410 (Hinzufügen des Empfängerschlüssels aus der privaten Umgebung)~~
    - ~~PHR-420 (Löschen des Empfängerschlüssels aus der privaten Umgebung)~~
    - ~~PHR-430 (Ersetzen des Empfängerschlüssels aus der privaten Umgebung)~~
    - ~~PHR-850 (Rollback des Umschlüsselungsvorgangs in Autorisierung (Wiederherstellung des alten Schlüsselmaterials))~~

[<=]

A_15490 - ePA-Frontend des Versicherten: Erweiterte-Anzeige für Protokolldaten
Das ePA-Frontend des Versicherten MUSS eine Erweiterte-Anzeige für die Protokolldaten umsetzten, in der alle Protokolleinträge der vom ePA-Aktensystem erstellten Protokolle (§ 291a-konformes Zugriffsprotokoll und Verwaltungsprotokolle der Komponenten) übersichtlich dargestellt werden.**[<=]**

Das FdV kann in der Standard-Anzeige die gemäß TAB_FdV_155 optionalen Felder verbergen. Der Nutzer muss dann die Möglichkeit haben, sich die verborgenen Felder anzeigen zu lassen.

A_15491-01~~A_15491~~ - ePA-Frontend des Versicherten: Felder Protokolldaten
Das ePA-Frontend des Versicherten MUSS es dem Nutzer in der Standard-Anzeige und in der Erweiterte-Anzeige für die Protokolldaten ermöglichen, alle Felder aus TAB_FdV_155 darzustellen.**[<=]**

ENTWURF

Das FdV soll in der Standard-Anzeige und in der Erweiterte-Anzeige für die Protokolldaten die Bezeichnung der Felder sinngemäß zu TAB_FdV_155 verwenden.

Das FdV kann es dem Nutzer über einen Link in der Anzeige ermöglichen, das referenzierte Dokument direkt herunterzuladen.

Die Protokolldaten sollen für den Nutzer sortierbar und filterbar dargestellt werden. Der Nutzer soll die Protokolldaten durchsuchen können.

A_15495 - ePA-Frontend des Versicherten: Protokolldaten lokal speichern
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Protokolldaten lokal im Format AuditEventList aus der getAuditEvents Response abzuspeichern.**[<=]**

A_15496 - ePA-Frontend des Versicherten: lokal gespeicherte Protokolldaten anzeigen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die lokal abgespeicherten Protokolldaten einzulesen und in der Standard- und Erweiterte-Anzeige anzuzeigen.**[<=]**

6.2.10 Verwaltung eGK

6.2.10.1 PIN der eGK ändern

Mit diesem Anwendungsfall kann der Nutzer das Geheimnis der PIN einer eGK ändern.

A_15497-01 - ePA-Frontend des Versicherten: PIN der eGK ändern
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "PIN der eGK ändern" gemäß TAB_FdV_156 umsetzen.

Tabelle 60: TAB_FdV_156 – PIN der eGK ändern

Name	PIN der eGK ändern
Auslöser	• Auswahl des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Die eGK des Nutzers ist im Kartenleser gesteckt.
Nachbedingung	PIN wurde geändert
Standardablauf	Die Umsetzung ist in TAB_FdV_157 beschrieben 1. PL_TUC_CARD_CHANGE_PIN nutzen 2. PL_TUC_CARD_CHANGE_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen

ENTWURF

3980
3981 **Tabelle 61: TAB_FdV_157 – Ablaufaktivitäten – PIN der eGK ändern**

1. PL_TUC_CARD_CHANGE_PIN nutzen	
Plattformoperation	PL_TUC_CARD_CHANGE_PIN
Eingangsdaten	
Identifikator	MRPIN.home
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benuzterinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	Alte PIN: "Eingabe alte PIN: " bzw. Neue PIN: "Eingabe neue PIN: "
Beschreibung	Der Plattformbaustein wird zur Änderung den PIN genutzt.
2. Rückgabewert von PL_TUC_CARD_CHANGE_PIN verarbeiten	
Rückgabedaten	
`OK`	PIN erfolgreich geändert
Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_CHANGE_PIN
Beschreibung	Das Ändern einer PIN auf der eGK basiert auf der parametrierten Plattformbaustein PL_TUC_CARD_CHANGE_PIN. Diese liefert ein `Ergebnis` zurück. Zur Änderung muss zwingend die Eingabe der alten PIN erfolgen. Wird durch den Versicherten ein falsches altes PIN-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PINs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung entsprechenden Details zurückgegeben.
3. Ergebnis anzeigen	

ENTWURF

Hinweis an den Versicherten	Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen. Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt. Bei einer Fehleingabe der PIN des Versicherten wird dem Versicherten die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet.

[<=]

ENTWURF

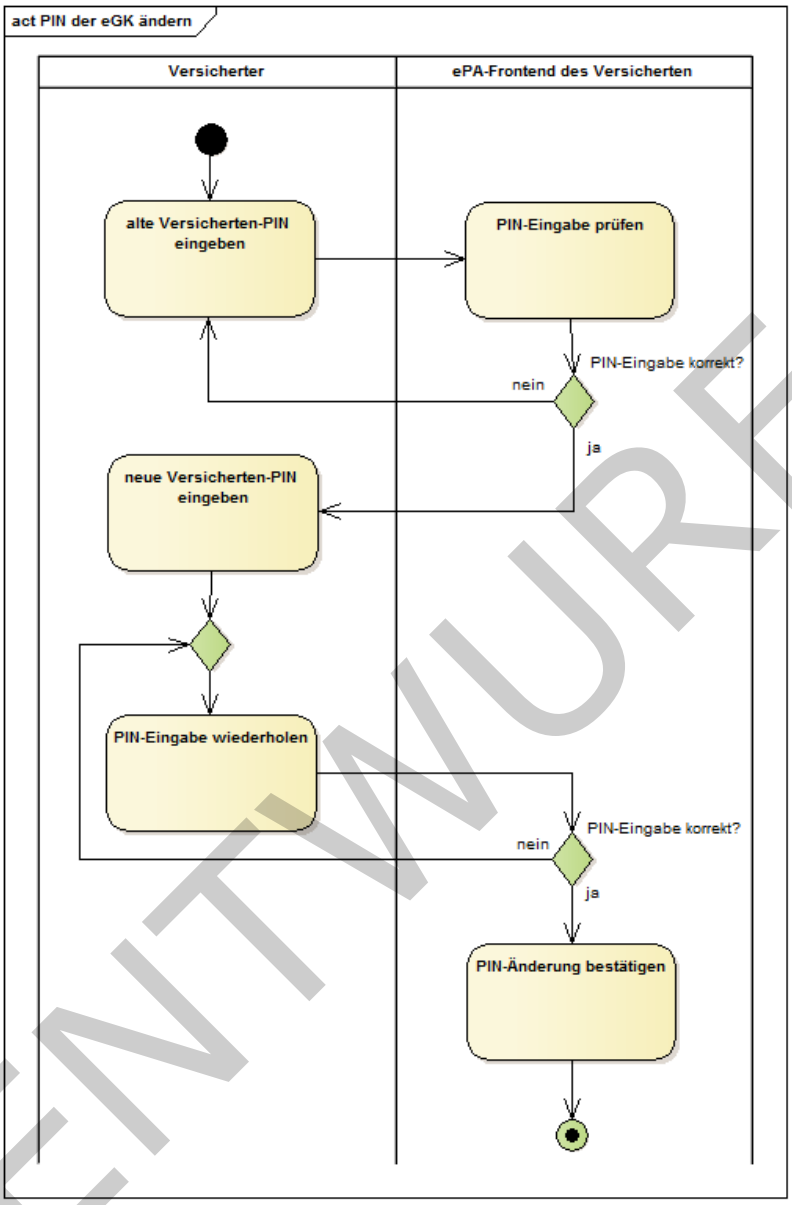


Abbildung 10: Aktivitätsdiagramm "PIN der eGK ändern"

ENTWURF

6.2.10.2 PIN der eGK entsperren

Mit diesem Anwendungsfall kann der Nutzer den gesperrten PIN einer eGK mit der PUK entsperren.

A_15498-01 - ePA-Frontend des Versicherten: PIN der eGK entsperren
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "PIN der eGK entsperren" gemäß TAB_FdV_158 umsetzen.

3994
3995 **Tabelle 62: TAB_FdV_158 – PIN der eGK entsperren**

Name	PIN der eGK entsperren
Auslöser	• Auswahl des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Die eGK des Nutzers ist im Kartenleser gesteckt. Die PIN der eGK (MRPIN.home) ist gesperrt.
Nachbedingung	PIN des Versicherten wurde entsperrt.
Standardablauf	Die Umsetzung ist in TAB_FdV_159 beschrieben 1. PL_TUC_CARD_UNBLOCK_PIN nutzen 2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen

3996
3997 **Tabelle 63: TAB_FdV_159 – Ablaufaktivitäten – PIN der eGK entsperren**

1. PL_TUC_CARD_UNBLOCK_PIN aufrufen	
Plattformbaustein	PL_TUC_CARD_UNBLOCK_PIN
Eingangsdaten	
Identifikator	MRPIN.home
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benuzterinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	PUK: "Eingabe PUK: " bzw. Neue PIN: "Eingabe neue PIN: "
Beschreibung	Für das Entsperren der PIN wird ein Plattformbaustein genutzt.
2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten	
Rückgabedaten	

ENTWURF

OK	PIN wurde entsperrt.
PasswordBlocked	Die PUK wurde wegen zu häufiger Nutzung gesperrt. Der Versicherte muss darüber in verständlicher Form informiert und auf die Notwendigkeit einer neuen eGK hingewiesen werden.
Weitere Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_UNBLOCK_PIN
Beschreibung	Das Entsperren einer PIN auf der eGK basiert auf dem parametrierten Plattformbaustein PL_TUC_CARD_UNBLOCK_PIN. Zum Entsperren muss zwingend die Eingabe einer PUK erfolgen. Wird durch den Versicherten ein falsches PUK-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PUKs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.
3. Ergebnis anzeigen	
Hinweis an den Versicherten	Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen. Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt.

[<=]

ENTWURF

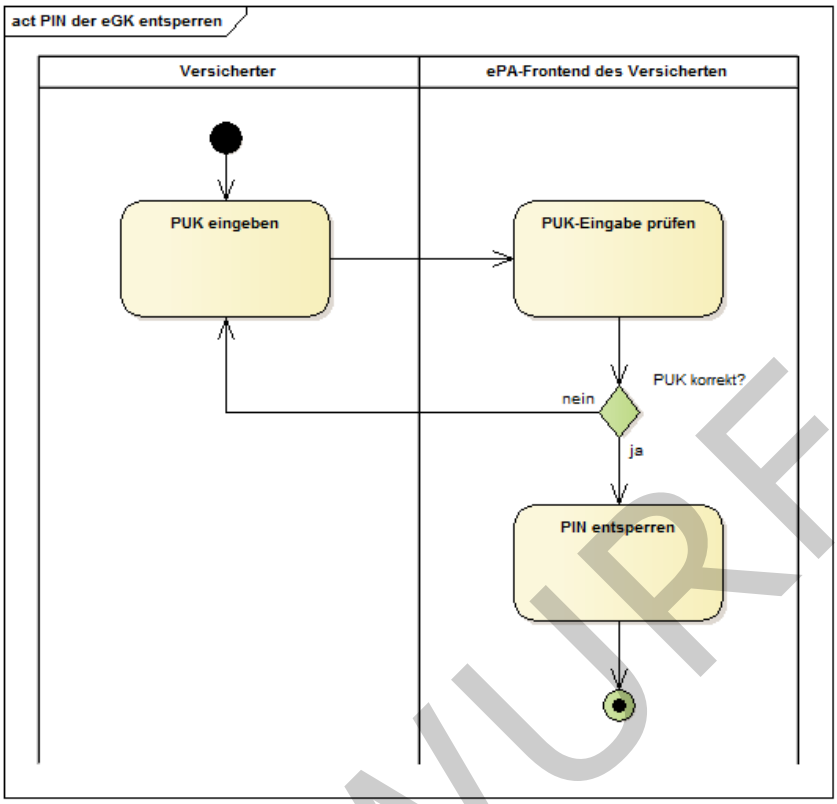


Abbildung 11: Aktivitätsdiagramm "PIN der eGK entsperren"

6.2.11 Geräteverwaltung

6.2.11.1 Benachrichtigungsadresse für Geräteautorisierung aktualisieren

Um ein Gerät mit dem FdV für den Zugriff auf ein Aktenkonto zu autorisieren, muss der Nutzer dieses über einen separaten Benachrichtigungskanal (E-Mail mit Freischalt-Link) bestätigen. Die E-Mail wird an die im Aktenkonto hinterlegte Benachrichtigungsadresse des Nutzers gesendet.

Für den Aktenkontoinhaber wird die Benachrichtigungsadresse initial im Rahmen der Kontoeröffnung hinterlegt. Für Vertreter erfolgt die initiale Hinterlegung der Benachrichtigungsadresse während der Vergabe der Zugriffsberechtigung.

Der Anwendungsfall "Benachrichtigungsadresse für Geräteautorisierung aktualisieren" gibt dem Nutzer die Möglichkeit eine neue Benachrichtigungsadresse im Aktenkonto zu hinterlegen.

A_15499 - ePA-Frontend des Versicherten: Benachrichtigungsadresse erfassen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine Benachrichtigungsadresse für die Geräteautorisierung einzugeben.**[<=]**

A_15500-01 - ePA-Frontend des Versicherten: Benachrichtigungsadresse aktualisieren
Das ePA-Frontend des Versicherten MUSS das Hinterlegen der Benachrichtigungsadresse im ePA-Aktensystem gemäß TAB_FdV_160 umsetzen.

ENTWURF

Tabelle 64: TAB_FdV_160 – Benachrichtigungsadresse aktualisieren

`I_Authorization_Management_Insurant::putNotificationInfo` Request erstellen	Eingangsparameter: • `AuthenticationAssertion` aus Session-Daten • `RecordIdentifier` aus Session-Daten • `DeviceID` aus Gerät-Daten • `NewNotificationInfo` = vom Nutzer eingegebene Benachrichtigungsadresse
`I_Authorization_Management_Insurant::putNotificationInfo` Response verarbeiten	Http OK ohne SOAP-Response oder gematik Fehlermeldung

[<=]

6.3 Realisierung der Leistungen der TI-Plattform

Der Produkttyp ePA-Frontend des Versicherten realisiert die von den Fachanwendungen benötigten Leistungen der TI-Plattform, die in den fachlichen Anwendungsfällen der ePA genutzt werden. Die durch die TI-Plattform bereitgestellten Leistungen umfassen einen für die Fachanwendungen einheitlichen Zugriff auf die eGK des Versicherten, Leistungen der PKI der Telematikinfrastruktur, kryptographische Operationen, etc. die in übergreifenden Spezifikationen der gematik festgelegt sind. Die Definition der Leistungen der TI-Plattform im ePA-Frontend des Versicherten finden sich in [gemSpec_Systemprozesse_dezTI].

Das ePA-Frontend des Versicherten verwendet u.a. die in der Tabelle TAB_FdV_177 dargestellten Plattformleistungen.

Tabelle 65: TAB_FdV_177 – Verwendete Plattformleistungen

Kürzel	Bezeichnung
PL_TUC_CARD_CHANGE_PIN	PIN ändern
PL_TUC_CARD_INFORMATION	Gesammelte Statusinformationen zu einer Karte
PL_TUC_CARD_UNBLOCK_PIN	PIN mit PUK entsperren
PL_TUC_CARD_VERIFY_PIN	Benutzer verifizieren
PL_TUC_GET_CHALLENGE	Auslesen einer Zufallszahl

ENTWURF

PL_TUC_PKI_VERIFY_CERTIFICATE	Prüfung eines Zertifikats der TI
PL_TUC_SIGN_HASH_nonQES	mit Karten-Identität signieren
PL_TUC_SYMM_DECIPHER	Symmetrisch entschlüsseln
PL_TUC_SYMM_ENCIPHER	Symmetrisch verschlüsseln

In den folgenden Abschnitten wird festgelegt, wie umgebungsspezifische Operationen an der Schnittstelle zu den Leistungen der TI-Plattform umgesetzt werden sollen.

6.3.1 Transportschnittstelle für Kartenkommandos

Der hier beschriebene Produkttyp ePA-Frontend des Versicherten ist als reines Softwareprodukt konzipiert. Als solches muss das ePA-Frontend des Versicherten eine Schnittstelle zur eGK über ein Kartenterminal herstellen. Diese Schnittstelle muss die von den Plattformprozessen erzeugten, kartenverständlichen APDUs an die Karte übertragen und wird im Folgenden als ENV_TUC_CARD_APDU_TRANSPORT bezeichnet. Neben proprietären Schnittstellentreibern von Kartenterminalherstellern existieren eine Reihe standardisierter Schnittstellen, die auch von verschiedenen Betriebssystemen zur Anbindung handelsüblicher Kartenterminals unterstützt werden.

A_15501-01 - ePA-Frontend des Versicherten: Transportschnittstelle für Kartenkommandos
Das ePA-Frontend des Versicherten SOLL eine Transportschnittstelle für die Übertragung von SmartCard-APDUs gegen die Standards CT-API und PCSC implementieren.**[<=]**

Von der Anforderung A_15501 darf abgewichen werden, wenn die Umsetzung technisch nicht möglich ist (bspw. durch die fehlende Unterstützung der NFC-Schnittstelle bei Herstellern mobiler Endgeräte).

Das ePA-Frontend des Versicherten kann ergänzend eine Transportschnittstelle für die Übertragung von SmartCard-APDUs auf Basis des SICCT-Protokolls, gegen den Standard CCID oder gegen proprietäre Hardwaretreiber eines Kartenterminalherstellers implementieren.

A_15502 - ePA-Frontend des Versicherten: Handbuch: Liste unterstützter Kartenterminals
Der Hersteller des ePA-Frontend des Versicherten MUSS im Handbuch ausweisen, welche Standards und Schnittstellen zu Kartenterminals sein Produkt unterstützt und MUSS eine Liste mit handelsüblichen Kartenterminals angeben, die mit seinem Produkt funktionieren.**[<=]**

Es sollen Kartenterminalvarianten der Sicherheitsklassen 1 (reine Kontaktiereinheit) zum Einsatz kommen. Zusätzlich können auch Kartenterminalvarianten der Sicherheitsklassen 2 (Kartenterminal mit eigenem PIN-Pad) oder 3 (PIN-Pad plus Display) unterstützt werden. Zusätzlich ist die Ausstattung des eingesetzten Kartenterminals (Klasse 1, 2 oder 3) mit einer NFC-Schnittstelle möglich. Das ePA-Frontend des Versicherten muss die von den Varianten gebotenen Features geeignet nutzen.

A_15503 - ePA-Frontend des Versicherten: PIN-Eingabe nicht speichern
Das ePA-Frontend des Versicherten DARF ein eingegebenes PIN-Geheimnis NICHT temporär und NICHT persistent speichern.**[<=]**

ENTWURF

A_15504-01 - ePA-Frontend des Versicherten: PIN-Geheimnis ausschließlich an Karte übermitteln
Das ePA-Frontend des Versicherten und das ePA-Frontend des Versicherten MÜSSEN sicherstellen, dass das eingegebene PIN-Geheimnis ausschließlich an die Karte und nicht an andere Adressaten übermittelt wird.**[<=]**

Das temporäre Speichern bezieht sich bei der Verwendung eines Kartenterminals der Sicherheitsklasse 1 auf das Verwenden der PIN über den Anwendungsfall hinaus, für den die PIN-Eingabe erfolgt ist, z.B. Caching während einer Sitzung. Gelangt das ePA-Frontend des Versicherten bei der Verwendung eines Kartenterminals der Sicherheitsklassen 2 und 3 ggfs. durch Fehlkonfiguration in Kenntnis der PIN, darf es diese ebenfalls weder temporär noch persistent speichern.

6.3.1.1 Kartenterminals der Sicherheitsklasse 1

Kartenterminals der Sicherheitsklasse 1 verfügen über keine Sicherheitsmerkmale, sie sind eine reine Kontaktiereinheit einer SmartCard. Sämtliche Geheimnis-Eingaben und Hinweistext-Ausgaben müssen über das FdV mittels Bildschirm und Tastatur/Maus erfolgen.

A_15505-01 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 1: PIN-Eingabe
Das ePA-Frontend des Versicherten MUSS, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird, die PIN-/PUK-Eingabe über ein angeschlossenes Eingabegerät entgegennehmen und in ein an die Karte adressiertes Kommando einbetten.**[<=]**

A_15506 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 1: PIN-Eingabe Geheimnis
Das ePA-Frontend des Versicherten DARF, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird, die eingegebene PIN/PUK Ziffernfolge NICHT im Klartext auf dem Bildschirm darstellen.**[<=]**

A_15507 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 1: PIN-Eingabe Eingabefeedback
Das ePA-Frontend des Versicherten MUSS, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird, ein eingegebenes Zeichen einer Geheimniseingabe mit dem Zeichen "*" (Wildcard) quittieren.**[<=]**

A_15508-01 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 1: PIN-Eingabe Validierung
Das ePA-Frontend des Versicherten MUSS, wenn das Geheimnis durch einen Anwendungsfall geändert werden soll und wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird, ein eingegebenes, neues PIN-Geheimnis durch eine erneute Abfrage des neuen PIN-Geheimnisses verifizieren.**[<=]**

6.3.1.2 Kartenterminals der Sicherheitsklasse 2

Kartenterminals der Sicherheitsklasse 2 verfügen über eine Eingabeschnittstelle zur Eingabe eines Benutzergeheimnisses. Typischerweise werden Kartenterminals der Sicherheitsklasse 2 in Anwendungsfällen mit Eingabe einer PIN bzw. PUK so angesteuert, dass das vorbereitete Kartenkommando mit einem Platzhalter des PIN-Geheimnisses an das Kartenterminal geschickt wird. Das Kartenterminal nimmt die PIN über die Eingabeschnittstelle entgegen, ersetzt den Platzhalter durch das eingegebene Geheimnis und leitet das Kartenkommando anschließend weiter an die Karte.

ENTWURF

A_15509-01 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 2: PIN-Eingabe
Das ePA-Frontend des Versicherten MUSS ein angeschlossenes Kartenterminal der Sicherheitsklasse 2 so ansteuern, dass ein Kartenkommando, das eine PIN-/PUK-Eingabe erfordert, an einem Kartenterminal um die Benutzereingabe ergänzt und anschließend direkt an die adressierte Karte weitergeleitet wird.**[<=]**

A_15510-01 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 2: PIN-Eingabe Fehlkonfiguration
Das ePA-Frontend des Versicherten MUSS alle Operationen mit einer eindeutigen Fehlermeldung abbrechen, in denen es die Kenntnis eines PIN/PUK-Geheimnisses erlangt, nachdem dieses an einem PIN-Pad eines Kartenterminals der Sicherheitsklasse 2 eingegeben wurde.**[<=]**

A_15511 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 2: PIN-Eingabe Eingabefeedback
Das ePA-Frontend des Versicherten MUSS während der Abfrage einer PIN/PUK an einem Kartenterminal der Sicherheitsklasse 2 einen Benutzerhinweis zur PIN-Eingabe am Kartenterminal an der Bildschirmausgabe ausgeben.**[<=]**

6.3.1.3 Kartenterminals der Sicherheitsklasse 3

Kartenterminals der Sicherheitsklasse 3 verfügen über eine Eingabeschnittstelle zur Eingabe eines Benutzergeheimnisses und Ausgabeschnittstelle zur Anzeige kurzer Textmeldungen. Typischerweise werden Kartenterminals der Sicherheitsklasse 3 in Anwendungsfällen mit Eingabe einer PIN bzw. PUK so angesteuert, dass das vorbereitete Kartenkommando mit einem Platzhalter des PIN-Geheimnisses an das Kartenterminal geschickt wird. Das Kartenterminal nimmt die PIN über die Eingabeschnittstelle entgegen, ersetzt den Platzhalter durch das eingegebene Geheimnis und leitet das Kartenkommando anschließend weiter an die Karte.

Während des Wartens auf eine Benutzereingabe kann ein an das Kartenterminal übergebener Text angezeigt werden. Einzelne Eingaben durch einen Benutzer werden in der Regel durch das Zeichen "*" quittiert. Ebenso besitzen Kartenterminals der Sicherheitsklasse 3 meist zusätzliche Logik, z.B. Eingaben zu verifizieren (siehe Anforderungen zum Ändern einer PIN mittels Klasse 1-Kartenterminal). Auf diese Logik soll hier nicht weiter eingegangen werden.

A_15512-01 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 3: PIN-Eingabe
Das ePA-Frontend des Versicherten MUSS ein angeschlossenes Kartenterminal der Sicherheitsklasse 3 so ansteuern, dass ein Kartenkommando, das eine PIN-/PUK-Eingabe erfordert, an einem Kartenterminal um die Benutzereingabe ergänzt und anschließend direkt an die adressierte Karte weitergeleitet wird.**[<=]**

A_15513-01 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 3: PIN-Eingabe Fehlkonfiguration
Das ePA-Frontend des Versicherten MUSS alle Operationen mit einer eindeutigen Fehlermeldung abbrechen, in denen es die Kenntnis eines PIN/PUK-Geheimnisses erlangt, nachdem dieses an einem PIN-Pad eines Kartenterminals der Sicherheitsklasse 3 eingegeben wurde.**[<=]**

A_15514-01 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 3: PIN-Eingabe Eingabefeedback
Das ePA-Frontend des Versicherten MUSS während der Abfrage einer PIN/PUK an einem Kartenterminal der Sicherheitsklasse 3 einen Benutzerhinweis zur PIN-Eingabe am Display des Kartenterminals ausgeben.**[<=]**

ENTWURF

Die Anzeige eines Benutzerhinweises soll den Nutzer informieren zu welchem Zweck eine Eingabe getätigt (z.B. alte PIN, neue PIN im Anwendungsfall PIN ändern) und welches konkrete Geheimnis abgefragt werden soll (PIN, PUK).

6.3.2 Schnittstelle für PIN-Operationen und Anbindung der eGK

Anwendungsfälle zur PIN-Verwaltung, das Login sowie weitere Anwendungsfälle können die Eingabe eines PIN- oder PUK-Geheimnisses durch den Versicherten erfordern. Der Zugriff auf die eGK erfolgt über die Systemprozesse PL_TUC_CARD_*. Das FdV als Realisierungsumgebung der Systemprozesse muss ihrerseits die von der Plattform geforderten Schnittstellen ENV_TUC_CARD_SECRET_INPUT implementieren, um die Kommunikation der Plattform mit dem Nutzer über die Außenschnittstelle des FdV zu ermöglichen. Die Außenschnittstelle ist in Kapitel "6.3.1 Transportschnittstelle für Kartenkommandos" beschrieben und umfasst das Kartenterminal, Eingabemedium und Hinweistexte an den Nutzer. Diese kann je nach Konfiguration an einem Gerät als Kartenterminal der Sicherheitsklasse 3 oder auch eine Kombination aus Bildschirmausgabe, Kartenterminal-PIN-Pad und/oder Tastatureingabe erfolgen.

A_15515-01 - ePA-Frontend des Versicherten: Übergabeschnittstelle PIN/PUK-Geheimnis
Das ePA-Frontend des Versicherten MUSS eine Operation ENV_TUC_SECRET_INPUT zur Eingabe eines PIN/PUK-Geheimnisses und Weiterleitung an eine SmartCard mit den Parametern

- Eingangsparameter:
  - `Identifikator`
  - `Aktion`
  - `minLength`
  - `maxLength`
  - `commandApduPart`
- Rückgabewerte:
  - responseApdu

implementieren.**[<=]**

A_15516-01 - ePA-Frontend des Versicherten: Umsetzung der Operation ENV_TUC_SECRET_INPUT
Das ePA-Frontend des Versicherten MUSS die Abbildung der Eingangsparameter auf die Rückgabewerte der Operation ENV_TUC_SECRET_INPUT derart umsetzen, dass

- die Eingangsparameter `Identifikator` und `Aktion` für einen Hinweistext an den Nutzer verwendet werden, welche Aktion auf welchem konkreten Kartenobjekt (z.B. Name einer PIN) durchgeführt wird
- wenn der Eingangsparameter `Aktion` die Eingabe eines Nutzerhinweises erfordert, der `commandApduPart` an der Eingabeschnittstelle um das Geheimnis des Nutzers ergänzt wird
- der `commandApduPart` über die Transportschnittstelle für Kartenkommandos an die Karte gesendet wird

ENTWURF

und die Antwortnachricht der Karte als `responseApdu` an den Aufrufer zur Auswertung zurückgegeben wird.**[<=]**

A_15517-01 - ePA-Frontend des Versicherten: Minimalprinzip Karteninteraktion
Das ePA-Frontend des Versicherten DARF ein Kartenkommando NICHT an eine angebundene Karte weiterleiten, dass nicht explizit im Kontext eines Anwendungsfalls (intendierte Kartenoperationen und Erhöhen des Sicherheitszustands der Karte falls erforderlich) erforderlich ist.**[<=]**

6.4 Test-App FdV

Für das Zulassungsverfahren des ePA-Frontend des Versicherten muss eine Anwendung (Test-App) mit integriertem ePA-Frontend des Versicherten bereitgestellt werden. Um einen automatisierten Test für das ePA-Frontend des Versicherten

zu ermöglichen, muss die Test-App zusätzlich ein Testtreiber-Modul beinhalten, welcher die Funktionalitäten der produktspezifischen Schnittstelle des ePA-Frontend des Versicherten über eine standardisierte Schnittstelle von außen zugänglich macht und einen Fernzugriff ermöglicht.

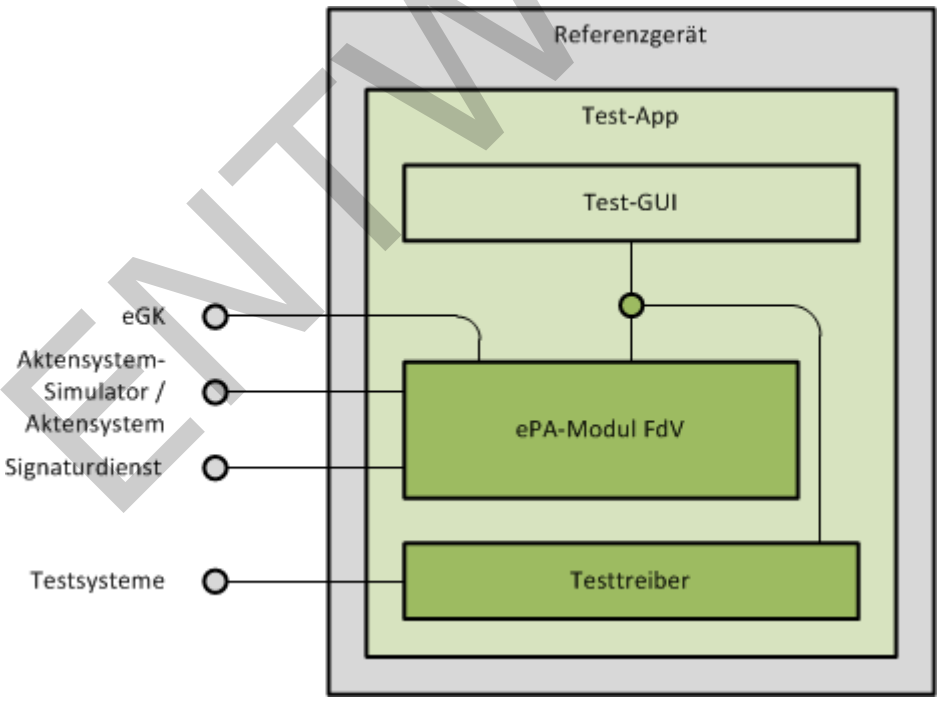


Abbildung 12: Test-App mit ePA-Frontend des Versicherten und Testtreiber

A_18044-01 - ePA-Frontend des Versicherten: Test-App mit ePA-Frontend des Versicherten und Testtreiber-Modul
Die Test-App des ePA-Frontend des Versicherten MUSS ein Testtreiber-Modul beinhalten, welches die Schnittstellen `I_FdV` und `I_FdV_Management` anbietet. Das Testtreiber-Modul

ENTWURF

MUSS die durch das ePA-Frontend des Versicherten – dem Zulassungsgegenstand – über eine produktspezifische Schnittstelle angebotene Funktionalität nutzen, um die Operationen der Schnittstellen umzusetzen.**[**<=**]**

Das Testtreiber-Modul darf die Ausgaben des ePA-Frontend des Versicherten gemäß der technischen Schnittstelle aufarbeiten, aber darf die Inhalte nicht verfälschen.

A_18171 - ePA-Frontend des Versicherten: Keine Fachlogik in Testtreiber-Modul
Das Testtreiber-Modul DARF NICHT die fachliche Logik des ePA-Frontend des Versicherten umsetzen.**[**<=**]**

Der Einsatz des Testtreiber-Moduls ist auf das Zulassungsverfahren in Test-Apps beschränkt und darf nicht in Wirkbetriebs-Apps genutzt werden.

A_18071 - ePA-Frontend des Versicherten: Beschränkung Einsatz Testtreiber-Modul
Das Frontend des Versicherten DARF ein Testtreiber-Modul NICHT enthalten.**[**<=**]**

Die Schnittstellen sind in den folgenden Abschnitten konzeptionell beschrieben. Die konkrete Ausgestaltung der Schnittstellen wird im gematik Fachportal veröffentlicht.

Die Test-App kann eine GUI anbieten. Diese kann bspw. für die Eingabe der PIN/PUK für die eGK oder die Authentifizierung gegenüber dem Signaturdienst genutzt werden.

Die Test-App muss Fehler, welche von aufgerufenen Systemen gemeldet werden oder bei der internen Verarbeitung auftreten, auf produktspezifische Fehler mappen. Der Hersteller muss die Fehler in der Betriebsdokumentation beschreiben und in einem strukturierten, maschinell verarbeitbarem Dokument übermitteln.

Wenn der Testtreiber einen Eingangsparameter an der Schnittstelle zum ePA-Frontend des Versicherten nicht benötigt, dann kann der Parameter ignoriert werden.

Alle Operationen beinhalten Parameter mit den notwendigen Informationen für ein Login. Diese sollen für ein implizites Login genutzt werden, wenn zu der insurantId noch keine Aktensession besteht.

Die Test-App muss bei Implementierung eines an ein ePA-Aktensystem gekoppeltes FdV sicherstellen, dass im Rahmen von gematik-Tests die Parameter für die Identifikation des zu nutzenden ePA-Aktensystems konfiguriert werden können.

Um Zugriffe aus einer Webanwendung, wie sie durch das AKTOR-Testfrontend zur Verfügung gestellt wird, auf die Testtreiberschnittstelle zu ermöglichen, werden folgende Schnittstelleneigenschaften benötigt:

Die Test-App kann die Testtreiberschnittstelle so über TLS zur Verfügung stellen, dass ein Zugriff aus Webanwendungen ermöglicht wird, die selbst über TLS geladen wurden.

Die Test-App kann den Zugriff auf die Testtreiberschnittstelle durch das Setzen von CORS-Headern für den Zugriff aus Webanwendungen öffnen, die aus einer anderen Origin geladen wurden.

6.4.1 Schnittstelle I_FdV

Die Schnittstelle `I_FdV` stellt Operationen zur Verfügung, um ePA-Anwendungsfälle im FdV auszuführen. Für eine technische Beschreibung der Schnittstelle siehe [testtreiber_fdv.yaml].

ENTWURF

A_18045-02~~A_18045-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::login

Die Schnittstelle `I_FdV` MUSS die Operation `login` implementieren.

Schnittstelle	I_FdV
Operation	login
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-Out	success
Parameter-Out	errorMessage
Parameter-Out	protocolEntries

Diese Operation führt ein explizites Login für ein Aktenkonto mit dem RecordIdenfier für `insurantId` aus.

Für die Verwendung einer eGK können die zu verwendende PIN sowie die CAN (für NFC) übergeben werden.
Für die Verwendung einer alvi-Identität kann der zu verwendende Authentisierungstoken übergeben werden.

[<=~~[<=~~]

Hinweis: Falls die insurantId übergeben wird, referenziert diese die Identität des Nutzers, welche über eine eGK oder einen Signaturdienst (entsprechend des Konfigurationsparameters UseEGK) verfügbar ist. Falls keine insurantID übergeben wird, dann wird eine PKCS12-Datei mit übergeben. Das C.CH.AUT-Zertifikat und der private Schlüssel aus der PKCS12-Datei werden im Testtreiber genutzt (bspw. Signatur bei der Authentisierung und der Schlüsselerzeugung mit SGD).

Für die Verwendung einer eGK kann die zu verwendende PIN übergeben werden (pin).

A_18046-01 - ePA-Frontend des Versicherten: Operation I_FdV::logout

Die Schnittstelle `I_FdV` MUSS die Operation `logout` implementieren.

Schnittstelle	I_FdV

ENTWURF

Operation	logout
Parameter-In	account
Parameter-In	insurantId
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt ein Logout für eine mit `insurantID` identifizierte Aktensession aus.**[<=]**

A_18047-02~~A_18047-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::changeProvider

Die Schnittstelle `I_FdV` MUSS die Operation `changeProvider` implementieren.

Schnittstelle	I_FdV
Operation	changeProvider
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	fqdnNewProvider
Parameter-In	transferPermission
Parameter-In	representativeNotificationInfo
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Anbieter wechseln" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

ENTWURF

A_18048-02~~A_18048-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::findHcpo

Die Schnittstelle `I_FdV` MUSS die Operation `findHcpo` implementieren.

Schnittstelle	I_FdV
Operation	findHcpo
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	directoryEntry
Parameter-Out	success
Parameter-Out	errorMessage
Parameter-Out	directoryEntries

Diese Operation führt eine Suchanfrage für Leistungserbringerinstitutionen im Verzeichnisdienst der TI in einer mit `insurantID` identifizierten Aktensession aus.**[<=]**

A_18049-03~~A_18049-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::grantPermissionHcpo

Die Schnittstelle `I_FdV` MUSS die Operation `grantPermissionHcpo` implementieren.

Schnittstelle	I_FdV
Operation	grantPermissionHcpo
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12

ENTWURF

Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	hcpoTelematikId
Parameter-In	hcpoName
Parameter-In	permissionAccessLevel
Parameter-In	permissionAccessCategories
Parameter-In	permissionAccessWhitelist
Parameter-In	permissionAccessBlacklist
Parameter-In	~~validity~~validFrom
Parameter-In	validThrough
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Berechtigung für LEI vergeben" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

~~A_18050-02A_18050-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::grantPermissionRepresentative

Die Schnittstelle `I_FdV` MUSS die Operation `grantPermissionRepresentative` implementieren.

Schnittstelle	I_FdV
Operation	grantPermissionRepresentative
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12

ENTWURF

Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	representativeInsurantId
Parameter-In	representativeName
Parameter-In	representativeNotificationInfo
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Vertretung einrichten" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

A_18051-02~~A_18051-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::findInsurance

Die Schnittstelle `I_FdV` MUSS die Operation `findInsurance` implementieren.

Schnittstelle	I_FdV
Operation	findInsurance
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	directoryEntry

ENTWURF

Parameter-Out	success
Parameter-Out	errorMessage
Parameter-Out	directoryEntries

Diese Operation führt eine Suchanfrage für Kostenträger im Verzeichnisdienst der TI in einer mit `insurantID` identifizierten Aktensession aus.
[<=]

A_18052-03~~A_18052~~ - ePA-Frontend des Versicherten: Operation I_FdV::grantPermissionInsurance
Die Schnittstelle `I_FdV` MUSS die Operation `grantPermissionInsurance` implementieren.

Schnittstelle	I_FdV
Operation	grantPermissionInsurance
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	insuranceTelematikId
Parameter-In	insuranceName
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Berechtigung für Kostenträger vergeben" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

ENTWURF

A_18053-02~~A_18053-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::getPermissions

Die Schnittstelle `I_FdV` MUSS die Operation `getPermissions` implementieren.

Schnittstelle	I_FdV
Operation	getPermissions
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-Out	success
Parameter-Out	permissions

Diese Operation führt den Anwendungsfall "Vergebene Berechtigungen auflisten" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

A_18054-02~~A_18054-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::changePermissionHcpo

Die Schnittstelle `I_FdV` MUSS die Operation `changePermissionHcpo` implementieren.

Schnittstelle	I_FdV
Operation	changePermissionHcpo
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore

ENTWURF

Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	hcpoTelematikId
Parameter-In	hcpoName
Parameter-In	permissionAccessLevel
Parameter-In	permissionAccessCategories
Parameter-In	permissionAccessWhitelist
Parameter-In	permissionAccessBlacklist
Parameter-In	~~validity~~validFrom
Parameter-In	validThrough
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Berechtigung für LEI ändern" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

A_18055-02~~A_18055-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::deletePermissionHcpo

Die Schnittstelle `I_FdV` MUSS die Operation `deletePermissionHcpo` implementieren.

Schnittstelle	I_FdV
Operation	deletePermissionHcpo
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin

ENTWURF

Parameter-In	can
Parameter-In	token
Parameter-In	hcpoTelematikId
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Berechtigung für LEI löschen" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

A_18056-02~~A_18056-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::deletePermissionRepresentative

Die Schnittstelle `I_FdV` MUSS die Operation `deletePermissionRepresentative` implementieren.

Schnittstelle	I_FdV
Operation	deletePermissionRepresentative
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	representativeInsurantId
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Berechtigung für Vertreter löschen" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

ENTWURF

A_18057-03~~A_18057-02~~ - ePA-Frontend des Versicherten: Operation I_FdV::deletePermissionInsurance

Die Schnittstelle `I_FdV` MUSS die Operation `deletePermissionInsurance` implementieren.

Schnittstelle	I_FdV
Operation	deletePermissionInsurance
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	insuranceTelematikId
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Berechtigung für Kostenträger löschen" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

A_18058-02~~A_18058-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::putDocuments

Die Schnittstelle `I_FdV` MUSS die Operation `putDocuments` implementieren.

Schnittstelle	I_FdV
Operation	putDocuments
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey

ENTWURF

Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	~~documents~~can
Parameter-In	token
Parameter-In	documentSets
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Dokumente einstellen" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

A_18059-02 - ePA-Frontend des Versicherten: Operation I_FdV::findObjects
~~A_18059-01 - ePA-Frontend des Versicherten: Operation I_FdV::findDocuments~~Die Schnittstelle `I_FdV` MUSS die Operation ~~`findDocuments`~~ findObjects implementieren.

Schnittstelle	I_FdV
Operation	~~findDocuments~~findObjects
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	~~doc~~can
Parameter-In	token
Parameter-In	queryMetadata
Parameter-In	query
Parameter-In	returnType
Parameter-In	startIndex

ENTWURF

Parameter-In	maxResults
Parameter-In	category
Parameter-Out	success
Parameter-Out	errorMessage
Parameter-Out	~~docs~~objectsMetadata

Diese Operation führt den Anwendungsfall "Dokumente suchen" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

Hinweis: Die für die Suchoperation zu verwendende Stored Query wird durch den Parameter query vorgegeben. Falls dieser nicht angegeben ist, muss eine geeignete Stored Query gewählt werden.

Die Parameter returnType (Werte sind „LeafClass" oder „ObjectRef"), startIndex und maxResults werden zum Gruppieren der Ergebnisse für das Blättern verwendet.

A_18060-02~~A_18060-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::getDocuments

Die Schnittstelle `I_FdV` MUSS die Operation `getDocuments` implementieren.

Schnittstelle	I_FdV
Operation	getDocuments
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	documentIds
Parameter-Out	success
Parameter-Out	errorMessage

ENTWURF

Parameter-Out	docs

Diese Operation führt den Anwendungsfall "Dokumente herunterladen" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

A_18061-02 - ePA-Frontend des Versicherten: Operation I_FdV::deleteObjects
~~**A_18061-01 - ePA-Frontend des Versicherten: Operation I_FdV::deleteDocuments**~~Die Schnittstelle `I_FdV` MUSS die Operation `deleteDocuments` implementieren.

Schnittstelle	I_FdV
Operation	~~deleteDocuments~~deleteObjects
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	~~documentIds~~can
Parameter-In	token
Parameter-In	objectIds
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Dokumente löschen" in einer mit`insurantID` identifizierten Aktensession aus.**[<=]**

Bei Passdokumenten enthält der Parameter `documentIds` die `uniqueID`s aller zum Pass gehörigen Dokumente.

A_21198 - ePA-Frontend des Versicherten: Operation I_FdV::changeFolder
~~**A_20760 - ePA-Frontend des Versicherten: Operation I_FdV::getDocAuthorized**~~Die Schnittstelle `I_FdV` MUSS die Operation ~~`getDocAuthorized`~~`changeFolder` implementieren.

Schnittstelle	I_FdV
Operation	~~getDocAuthorized~~changeFolder

ENTWURF

Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	documentId
Parameter-In	folders
Parameter-Out	success
Parameter-Out	errorMessage
~~Parameter-Out~~	~~authorizedList~~

~~Die Schnittstelle `getDocAuthorized` dient der Umsetzung von A_20198.[<=]~~

[<=]

A_21199 - ePA-Frontend des Versicherten: Operation I_FdV::replaceDocument
~~**A_20761 - ePA-Frontend des Versicherten: Operation I_FdV::updateDocument**~~Die ~~Die~~ Schnittstelle `I_FdV` MUSS die Operation ~~`updateDocument`~~`replaceDocument` implementieren.

Schnittstelle	I_FdV
Operation	~~updateDocument~~replaceDocument
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore

ENTWURF

Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	documentId
Parameter-In	documentSet
Parameter-~~In~~Out	~~value~~success
Parameter-Out	errorMessage

[<=]

A_20760-01 - ePA-Frontend des Versicherten: Operation I_FdV::permissionsForDocument

Die Schnittstelle `I_FdV` MUSS die Operation `permissionsForDocument` implementieren.

Schnittstelle	I_FdV
Operation	permissionsForDocument
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	documentId
Parameter-Out	success
Parameter-Out	errorMessage
Parameter-Out	permissions

[<=]

ENTWURF

A_20761-01 - ePA-Frontend des Versicherten: Operation I_FdV::updateMetadata

Die Schnittstelle `I_FdV` MUSS die Operation `updateMetadata` implementieren.

Schnittstelle	I_FdV
Operation	updateMetadata
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	documentId
Parameter-In	metadataSet
Parameter-Out	success
Parameter-Out	errorMessage

Die Operation wird für folgende Aktivitäten verwendet:

- Ersetzen / Ergänzen eines Dokuments
- Änderung der Vertraulichkeit
- Änderung der Kategorie

[<=]

A_20762-01~~A_20762~~ - ePA-Frontend des Versicherten: Operation I_FdV::updateKeys

Die Schnittstelle `I_FdV` MUSS die Operation `updateKeys` implementieren.

Schnittstelle	I_FdV
Operation	updateKeys

ENTWURF

Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-Out	success
Parameter-Out	errorMessage
Parameter-Out	rollbackTime

[<=]

Die Operation wird im Rahmen der Umschlüsselung verwendet.

A_18062-02~~A_18062-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::getProtocol

Die Schnittstelle `I_FdV` MUSS die Operation `getProtocol` implementieren.

Schnittstelle	I_FdV
Operation	getProtocol
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token

ENTWURF

Parameter-Out	success
Parameter-Out	errorMessage
Parameter-Out	protocolEntries

Diese Operation führt den Anwendungsfall "Zugriffsprotokoll einsehen" in einer mit`insurantID` identifizierten Aktensession aus. Die vom Aktensystem gelieferten Protokolleinträge werden aufgearbeitet und zurückgegeben.**[<=]**

A_21167 - ePA-Frontend des Versicherten: Operation I_FdV::getSignedProtocol
Die Schnittstelle `I_FdV` MUSS die Operation `getSignedProtocol` implementieren.

Schnittstelle	**I_FdV**
Operation	getSignedProtocol
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-Out	success
Parameter-Out	errorMessage
Parameter-Out	protocolEntries

Diese Operation führt den Anwendungsfall "signiertes Zugriffsprotokoll einsehen" in einer mit`insurantID` identifizierten Aktensession aus. Die vom Aktensystem gelieferten Protokolleinträge werden aufgearbeitet und zurückgegeben
[<=]

A_18063-02~~A_18063-01~~ - ePA-Frontend des Versicherten: Operation I_FdV::putNotificationInformation
Die Schnittstelle `I_FdV` MUSS die Operation `putNotificationInformation` implementieren.

Schnittstelle	I_FdV

ENTWURF

Operation	putNotificationInformation
Parameter-In	account
Parameter-In	insurantId
Parameter-In	pkcs12
Parameter-In	passwordPrivateKey
Parameter-In	passwordKeyStore
Parameter-In	pin
Parameter-In	can
Parameter-In	token
Parameter-In	notificationInformation
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation führt den Anwendungsfall "Benachrichtigungsadresse für Geräteautorisierung aktualisieren" in einer mit `insurantID` identifizierte Aktensession aus.**[<=]**

6.4.2 Schnittstelle I_FdV_Management

Die Schnittstelle `I_FdV_Management` stellt Operationen für die Konfiguration des FdV und die Abfrage der Selbstauskunft zur Verfügung.

A_20763 - ePA-Frontend des Versicherten: Operation I_FdV_Management::ping
Die Schnittstelle `I_FdV_Management` MUSS die Operation `ping` implementieren.

Schnittstelle	I_FdV_Management
Operation	ping
Parameter-Out	success
Parameter-Out	errorMessage
Parameter-Out	version

ENTWURF

Die Operation liefert die Schnittstellenversion.

Hinweis: Ping prüft die Erreichbarkeit der Testtreiber-Schnittstelle.**[<=]**

A_18066-01 - ePA-Frontend des Versicherten: Operation I_FdV_Management::setConfiguration

Die Schnittstelle `I_FdV_Management` MUSS die Operation `setConfiguration` implementieren.

Schnittstelle	I_FdV_Management
Operation	setConfiguration
Parameter-In	id
Parameter-In	value
Parameter-Out	success
Parameter-Out	errorMessage

Diese Operation setzt ein oder mehrere Werte für eine Liste von Konfigurationsparametern gemäß TAB_FdV_104 sowie für herstellerspezifische Konfigurationsparameter.**[<=]**

Die Liste der herstellerspezifischen Konfigurationsparameter sind in der Betriebsdokumentation zu beschreiben.

A_18067-01 - ePA-Frontend des Versicherten: Operation I_FdV_Management::getConfiguration

Die Schnittstelle `I_FdV_Management` MUSS die Operation `getConfiguration` implementieren.

Schnittstelle	I_FdV_Management
Operation	getConfiguration
Parameter-In	id
Parameter-Out	id
Parameter-Out	value

Die Operation liefert eine Liste aller Konfigurationsparameter des FdV mit den eingestellten Werten.**[<=]**

Hinweis: Liefert alle Konfigurationseinträge, die dem Filter entsprechen. Als Filter ist die Angabe einer configurationEntryId als id möglich. Wird kein Filter angegeben, dann werden alle Einträge aus der Konfiguration zurückgegeben.

ENTWURF

A_18068-01 - ePA-Frontend des Versicherten: Operation I_FdV_Management::getProductInformation

Die Schnittstelle `I_FdV_Management` MUSS die Operation `getProductInformation` implementieren.

Schnittstelle	I_FdV_Management
Operation	getProductInformation
Parameter-Out	producerId
Parameter-Out	code
Parameter-Out	version

Die Operation liefert eine Liste mit den Werten der Produktinformation.**[<=]**

ENTWURF

7 Informationsmodell

Aktenkonto:

Datenfeld	Herkunft	Beschreibung
Akten-ID (RecordIdentifier)	Konfiguration	beinhaltet Versicherten-ID und Anbieter-ID (homeCommunityId)
Name des Aktenkontoinhabers	Konfiguration	
FQDN des ePA-Aktensystem	Konfiguration	

Geräte-Daten:

Datenfeld	Herkunft	Beschreibung
Gerätekennung (DeviceID)	Konfiguration	beinhaltet Gerätenamen und Geräteidentität
Geräteidentität	Konfiguration	wird von der Autorisierung beim erstmaligen Aufruf zusammen mit dem DEVICE_UNKNOWN Fehler übermittelt
Gerätenamen	Konfiguration	durch Nutzer festgelegt

Session-Daten:

Datenfeld	Herkunft	Beschreibung
Akten-ID (RecordIdentifier)	Konfiguration	Kennung des Aktenkontos, auf das in der Aktensession zugegriffen wird, im Format von RecordIdentifier gemäß [gemSpec_DM_ePA#2.2] Die homeCommunityID muss bekannt sein.
Status Nutzer (Aktenkontoinhaber oder Vertreter)		Vergleich Versicherten-ID aus Akten-ID mit Versicherten-ID

ENTWURF

		aus Authentisierungszertifikat des Nutzers
Authentisierungstoken (AuthenticationAssertion)	Komponente Authentisierung (I_Authentication_Insurant::LoginCreateToken)	
Autorisierungstoken (AuthorizationAssertion)	Komponente Autorisierung (I_Authorization_Insurant::getAuthorizationKey)	
Aktenschlüssel (RecordKey)	AuthorizationKey	entschlüsselter Aktenschlüssel
Kontextschlüssel (ContextKey)	AuthorizationKey	entschlüsselter Kontextschlüssel
Zustand des Aktenkontos (RecordState)	Autorisierungstoken Attribut `Assertion/AttributeStatement/Attribute` mit dem Namen "Zustand des Kontos"	
Zeitpunkt der letzten Authentifizierung durch den Nutzer	Konfiguration	
Liste der vergebenen Berechtigungen	Aktivität "Vergebene Berechtigungen bestimmen"	Liste der für alle Berechtigungen ausgelesenen AuthorizationKeys und Policy Documents

4491

4492 Nutzer:

Datenfeld	**Herkunft**	**Beschreibung**
Authentisierungszertifikat des Nutzers	eGK für alternative kryptographische Versichertenidentität: Signaturdienst	falls eGK: C.CH.AUT falls alternative kryptographische Versichertenidentität: C.CH.AUT_ALT
Name des Nutzers	Authentisierungszertifikat des Nutzers	

ENTWURF

Versicherten-ID des Nutzers	Authentisierungszertifikat des Nutzers	
Benachrichtigungskanal für Geräteverwaltung (E-Mail)		durch den Nutzer während des Eröffnens des Aktenkontos angegeben.

4493

4494 Berechtigungen:

Datenfeld	**Herkunft**	**Beschreibung**
Name des Berechtigten	DisplayName aus AuthorizationKey	
Kategorie	Policy Document	LEI , KTR oder Vertreter
ID	AuthorizationKey / Policy Document	für LEI oder KTR: Telematik-ID für Vertreter: Versicherten-ID
Berechtigung ausgestellt am	Policy Document	nur LEI
Berechtigung gültig bis	Policy Document	nur LEI
Berechtigung für den Zugriff auf von LEI eingestellten Dokumenten	PolicyDocument mit "`urn:gematik:policy-set-id:permissions-access-group-hcp`"	nur LEI
Berechtigung für den Zugriff auf von Versicherten eingestellten Dokumenten	Policy Document mit "`urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents`"	nur LEI
Berechtigung für den Zugriff auf von KTR eingestellten Dokumenten	Policy Document mit "`urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents`"	nur LEI

ENTWURF

8 Verteilungssicht

Eine Darstellung der hardwareseitigen Verteilung des Produkttyps bzw. seiner Teilsysteme und der Einbettung in die physikalische Umgebung wird nicht benötigt.

ENTWURF

4498 # 9 Anhang A – Verzeichnisse

4499 ## 9.1 Abkürzungen

Kürzel	Erläuterung
DSMLv2	Directory Services Markup Language v2.0
eGK	Elektronische Gesundheitskarte
ePA	Elektronische Patientenakte
FdV	ePA-Frontend des Versicherten
FQDN	Fully-Qualified Domain Name
GdV	Gerät des Versicherten
IHE	Integrating the Healthcare Enterprise
KTR	Kostenträger, d.h. die gesetzlichen Krankenkassen
KVNR	Krankenversichertennummer
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
MTOM	Message Transmission Optimization Mechanism
NFC	Near Field Communication
OWASP	Open Web Application Security Project
PDF	Portable Document Format
PIN	Personal Identification Number
PUK	Personal Unblocking Key
SGD	Schlüsselgenerierungsdienst
SOAP	Simple Object Access Protocol

ENTWURF

TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust-service Status List
VZD	Verzeichnisdienst der TI

9.2 Glossar

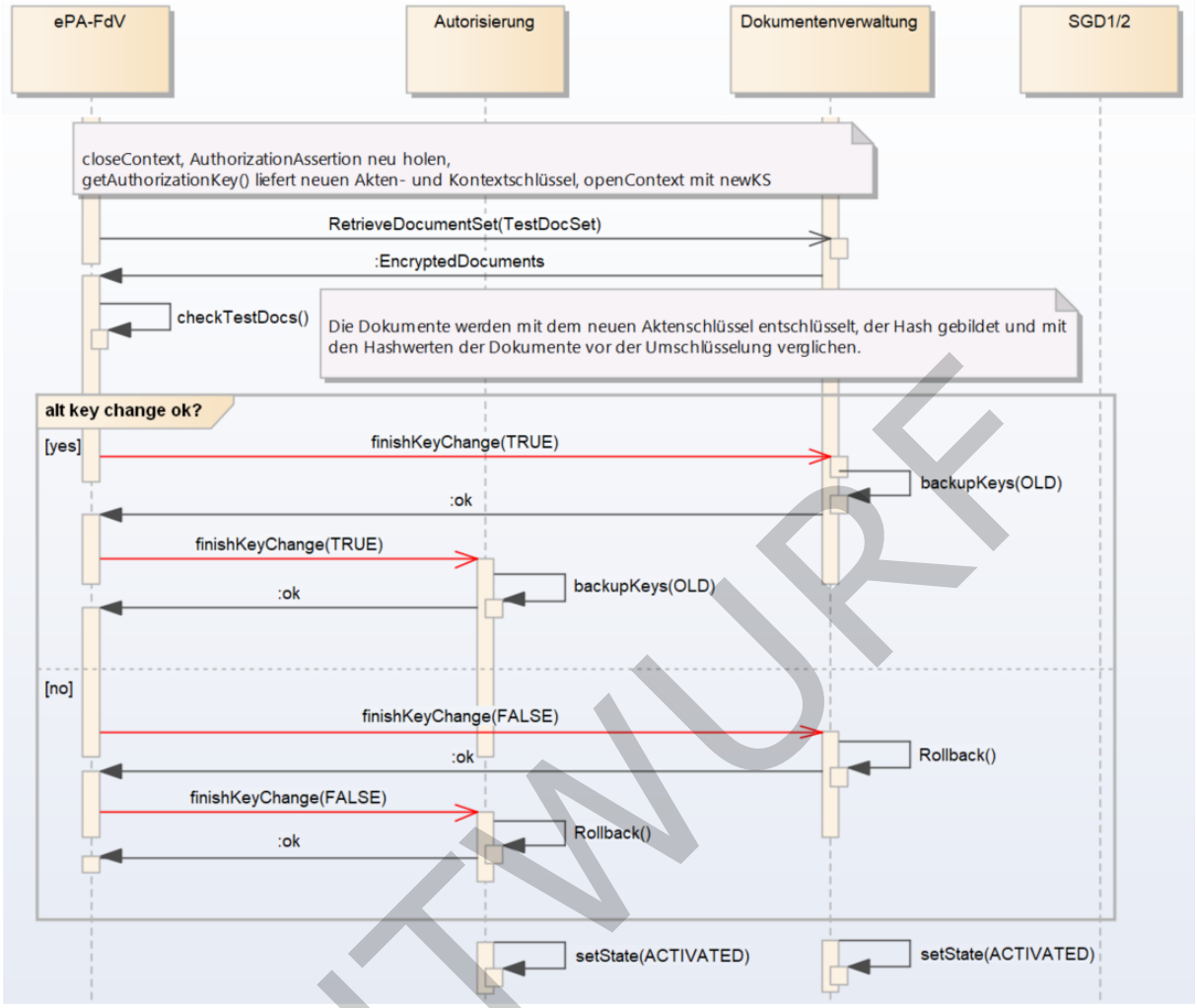
Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
Patienteninformation	Ist ein durch eine Leistungserbringerinstitution im Aktenkonto bereitgestelltes Dokument, welches vorrangig der Information von Versicherten dient. Das Dokument wird durch den Leistungserbringer als Versicherteninformation gekennzeichnet.
Policy Document	Das Policy Document ist ein technisches Dokument. Es enthält die Zugriffsregeln eines Berechtigten im Aktenkonto des Versicherten in der Komponente "Dokumentenverwaltung". Berechtige der Aktenkontoinhaber, Vertreter oder LEIs.
Versicherten-ID	Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen Krankenversichertennummer (KVNR).
Versichertendokument	Ist ein durch einen Versicherten (Aktenkontoinhaber oder Vertreter) im Aktenkonto bereitgestelltes Dokument
Versicherteninformation	siehe Patienteninformation

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

9.3 Abbildungsverzeichnis

ENTWURF

ENTWURF



9.4 Tabellenverzeichnis

ENTWURF

ENTWURF

ENTWURF

ENTWURF

9.5 Referenzierte Dokumente

9.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel

ENTWURF

[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemSpec_Aktensystem]	gematik: Spezifikation ePA-Aktensystem
[gemSpec_Authentisierung_Vers]	gematik: Spezifikation Authentisierung des Versicherten ePA
[gemSpec_Autorisierung]	gematik: Spezifikation Autorisierung ePA
[gemSpec_DM_ePA]	gematik: Datenmodell ePA
[gemSpec_Dokumentenverwaltung]	gematik: Spezifikation Dokumentenverwaltung ePA
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_PKI]	gematik: Übergreifende Spezifikation Spezifikation PKI
[gemSpec_SGD_ePA]	gematik: Spezifikation Schlüsselgenerierungsdienst ePA
[gemSpec_SigD]	gematik: Spezifikation Signaturdienst
[gemSpec_Systemprozesse_dezTI]	gematik: Spezifikation Systemprozesse der dezentralen TI
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
[gemSpec_X_509_TSP]	gematik: Spezifikation Trust Service Provider X.509
[gemSpec_Zugangsgateway_Vers]	gematik: Spezifikation Zugangsgateway des Versicherten ePA
[gemSysL_ ePA]	gematik: Systemspezifisches Konzept ePA

ENTWURF

9.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

[DSML2.0]	OASIS: Directory Services Markup Language v2.0 December 18, 2001 https://www.oasis-open.org/standards http://www.oasis-open.org/committees/dsml/docs/DSMLv2.doc http://oasis-open.org/committees/dsml/errata https://www.oasis-open.org/committees/dsml/docs/DSMLv2.xsd
[ETSI_TS_102_231_V3.1.2]	ETSI TS 102 231 V3.1.2 (2009-12) Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information
[IHE-ITI-APPC]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Advanced Patient Privacy Consents (APPC), Revision 1.2 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf
[IHE-ITI-TF]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Revision 15.0
[IHE-ITI-TF2a]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2a (ITI TF-2a) – Transactions Part A, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf
[IHE-ITI-TF2b]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf
[IHE-ITI-TF2x]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2x) – Volume 2 Appendices, Revision 15.1, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf
[IHE-ITI-RMD]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.2 – Trial Implementation https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/

ENTWURF

[OWASP Proactive Control]	OWASP Top Ten Proactive Controls Project OWASP Proactive Controls For Developers v3.0 https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf
[OWASP SAMM Project]	OWASP SAMM Project https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Browse_Online
[OWASPMobileTop10]	OWASP Mobile Security Project: Top 10 Mobile Risks https://owasp.org/www-project-mobile-top-10/
[OWASP MASVS]	OWASP Mobile Application Security Verification Service https://owasp.org/www-chapter-geneva/assets/slides/OWASP_Geneva-Chapter_Meeting-20161212_Jeremy_Matos-MASVS.pdf
[OWASP TTMC]	OWASP Mobile Security Project https://owasp.org/www-project-mobile-security/
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP https://tools.ietf.org/html/rfc6960
[vesta]	Zentrales Interoperabilitätsverzeichnis des deutschen Gesundheitswesens https://www.vesta-gematik.de/
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[XMLEnc-1.1]	XML Encryption Syntax and Processing, W3C Recommendation 11 April 2013, http://www.w3.org/TR/xmlenc-core1/

4684

ENTWURF