

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation ePA-Frontend des Versicherten

Version:	1.10. <del>01</del>
Revision:	<del>382375408480</del>
Stand:	30.09. <del>07</del> .2021
Status:	freigegeben
Klassifizierung:	öffentlich
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	19.02.21		Einarbeitung Änderungsliste P22.5	gematik
1.9.0	02.06.21		Einarbeitung ePA_Maintenance_21.1 und Featurspezifikation gemF_ePA_stat_FdV	gematik
1.10.0	09.07.21		Einarbeitung Anpassung IOP-WS (ePA_Maintenance_21.2)	gematik
1.10.1	30.09.21		Einarbeitung ePA_Maintenance_21.3	gematik

## Inhaltsverzeichnis

<b>1 Einordnung des Dokumentes</b>	<b>9</b>
1.1 Zielsetzung	9
1.2 Zielgruppe	9
1.3 Geltungsbereich	9
1.4 Abgrenzungen	9
1.5 Methodik	10
<b>2 Systemüberblick</b>	<b>11</b>
<b>3 Systemkontext</b>	<b>12</b>
3.1 Akteure und Rollen	12
3.2 Nachbarsysteme	13
3.2.1 Identität des Nutzers	15
<b>4 Zerlegung des Produkttyps</b>	<b>16</b>
<b>5 Übergreifende Festlegungen</b>	<b>18</b>
5.1 Datenschutz und Sicherheit	18
5.1.1 Anforderungen zum Herstellungsprozess	28
5.1.2 Unterstützung von Audits	31
5.2 Verwendete Standards	32
5.3 Integrating the Healthcare Enterprise IHE	32
5.3.1 Policy Documents	34
5.4 Benutzeroberfläche	35
5.4.1 Visuelle Darstellung	35
5.4.2 Benutzerführung	36
5.4.2.1 Technische Normen und Verordnungen zur Beachtung	37
5.4.3 Anzeige von Dokumenten	39
5.4.4 Sammlungen	40
5.4.5 Metadaten für einzustellende Dokumente	41
5.4.6 Konfiguration des ePA-Frontend des Versicherten	42
<b>6 Funktionsmerkmale</b>	<b>47</b>
6.1 Allgemein	47
6.1.1 Aktensession-Verwaltung	47
6.1.2 Kommunikation mit dem ePA-Aktensystem	49
6.1.3 Sicherer Kanal zur Dokumentenverwaltung	51
6.1.4 Geräteautorisierung	51
6.1.5 Zertifikatsprüfung	52
6.1.5.1 Vertrauensanker des TI-Vertrauensraum	53
6.1.5.2 TLS-Behandlung	53
6.1.5.3 Zertifikatsprüfung von Zertifikaten der TI	55

6.1.5.4 Zertifikatsprüfung von Internet-Zertifikaten .....	56
6.1.6 Dokumente .....	56
6.1.7 Umschlüsselung der Dokumente .....	57
6.1.7.1 Kryptographische Architektur der Dokumentenverschlüsselung .....	57
6.1.8 ePA FdV für Desktop-Plattformen .....	58
<b>6.2 Implementation ePA-Anwendungsfälle im FdV .....</b>	<b>58</b>
6.2.1 Übergreifende Festlegungen .....	59
6.2.2 Fehlerbehandlung .....	61
6.2.3 Aktivitäten .....	63
6.2.3.1 Authentisieren des Nutzers .....	63
6.2.3.2 Authentisierungstoken erneuern .....	65
6.2.3.3 Dokumentenset in Dokumentenverwaltung hochladen .....	66
6.2.3.4 Dokumentenset aus Dokumentenverwaltung herunterladen .....	67
6.2.3.5 Dokumentenset in Dokumentenverwaltung löschen .....	69
6.2.3.6 Suche nach Dokumenten in Dokumentenverwaltung .....	70
6.2.3.7 Vergebene Berechtigungen bestimmen .....	71
6.2.3.8 AuthorizationKey .....	72
6.2.3.8.1 Struktur AuthorizationKeyType .....	72
6.2.3.8.2 Schlüsselableitung für Ver- und Entschlüsselung .....	73
6.2.3.8.3 AuthorizationKey erstellen .....	74
6.2.3.8.4 AuthorizationKey entschlüsseln .....	76
6.2.3.9 Schlüsselmaterial aus ePA-Aktensystem laden .....	77
6.2.3.10 Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden .....	79
6.2.3.11 Schlüsselmaterial im ePA-Aktensystem speichern .....	80
6.2.3.12 Schlüsselmaterial im ePA-Aktensystem ersetzen .....	81
6.2.3.13 Schlüsselmaterial im ePA-Aktensystem löschen .....	81
6.2.3.14 Leistungserbringerinstitution im Verzeichnisdienst der TI finden .....	82
6.2.3.15 Suchanfrage Verzeichnisdienst der TI .....	83
6.2.3.16 PIN-Eingabe für eGK durch Nutzer .....	84
6.2.4 Nutzerzugang ePA .....	85
6.2.4.1 Login-Aktensession .....	85
6.2.4.2 Logout-Aktensession .....	93
6.2.5 Aktenkontoverwaltung .....	95
6.2.5.1 Aktenkonto aktivieren .....	95
6.2.5.2 Anbieter wechseln .....	97
6.2.5.3 Schließen einer Akte .....	104
6.2.6 Umschlüsselung .....	105
6.2.7 Berechtigungsverwaltung .....	111
6.2.7.1 Spezifische Zugriffsregeln .....	116
6.2.7.1.1 kategorienbasierte Berechtigung .....	116
6.2.7.1.2 Dokumentenspezifische Berechtigung .....	120
6.2.7.2 Vertretung einrichten .....	121
6.2.7.3 Berechtigung für Kostenträger vergeben .....	124
6.2.7.4 Vergebene Berechtigungen anzeigen .....	125
6.2.7.5 Eingerichtete Vertretungen anzeigen .....	127
6.2.7.6 Bestehende Berechtigungen verwalten .....	127
6.2.7.6.1 Berechtigung für LEI ändern .....	127
6.2.7.6.2 Berechtigung für LEI löschen .....	129
6.2.7.6.3 Berechtigung für Vertreter löschen .....	130

6.2.7.6.4 Berechtigung für Kostenträger löschen .....	131
6.2.8 Dokumentenverwaltung .....	133
6.2.8.1 Dokumente einstellen .....	133
6.2.8.2 Dokumente suchen .....	136
6.2.8.3 Dokument herunterladen .....	138
6.2.8.4 Dokumente im Aktenkonto löschen .....	139
6.2.9 Protokollverwaltung .....	140
6.2.9.1 Zugriffsprotokoll einsehen .....	140
6.2.10 Verwaltung eGK .....	145
6.2.10.1 PIN der eGK ändern .....	145
6.2.10.2 PIN der eGK entsperren .....	148
6.2.11 Geräteverwaltung .....	151
6.2.11.1 Benachrichtigungsadresse für Geräteautorisierung aktualisieren .....	151
6.2.11.2 Benachrichtigungsadressen abfragen .....	152
<b>6.3 Realisierung der Leistungen der TI-Plattform .....</b>	<b>153</b>
6.3.1 Transportschnittstelle für Kartenkommandos .....	153
6.3.1.1 Kartenterminals der Sicherheitsklasse 1 .....	155
6.3.1.2 Kartenterminals der Sicherheitsklasse 2 .....	156
6.3.1.3 Kartenterminals der Sicherheitsklasse 3 .....	156
6.3.2 Schnittstelle für PIN-Operationen und Anbindung der eGK .....	157
<b>6.4 Test-App-FdV .....</b>	<b>158</b>
<b>7 Informationsmodell .....</b>	<b>161</b>
<b>8 Verteilungssicht .....</b>	<b>164</b>
<b>9 Anhang A Verzeichnisse .....</b>	<b>165</b>
9.1 Abkürzungen .....	165
9.2 Glossar .....	166
9.3 Abbildungsverzeichnis .....	166
9.4 Tabellenverzeichnis .....	167
9.5 Referenzierte Dokumente .....	171
9.5.1 Dokumente der gematik .....	171
9.5.2 Weitere Dokumente .....	172
<b>1 Einordnung des Dokumentes .....</b>	<b>9</b>
1.1 Zielsetzung .....	9
1.2 Zielgruppe .....	9
1.3 Geltungsbereich .....	9
1.4 Abgrenzungen .....	9
1.5 Methodik .....	10
<b>2 Systemüberblick .....</b>	<b>11</b>
<b>3 Systemkontext .....</b>	<b>12</b>
3.1 Akteure und Rollen .....	12

<b>3.2 Nachbarsysteme .....</b>	<b>13</b>
3.2.1 Identität des Nutzers .....	15
<b>4 Zerlegung des Produkttyps .....</b>	<b>16</b>
<b>5 Übergreifende Festlegungen .....</b>	<b>18</b>
<b>5.1 Datenschutz und Sicherheit.....</b>	<b>18</b>
5.1.1 Anforderungen zum Herstellungsprozess .....	28
5.1.2 Unterstützung von Audits .....	31
<b>5.2 Verwendete Standards .....</b>	<b>32</b>
<b>5.3 Integrating the Healthcare Enterprise IHE .....</b>	<b>32</b>
5.3.1 Policy Documents .....	34
<b>5.4 Benutzeroberfläche .....</b>	<b>35</b>
5.4.1 Visuelle Darstellung .....	35
5.4.2 Benutzerführung .....	36
5.4.2.1 Technische Normen und Verordnungen zur Beachtung .....	37
5.4.3 Anzeige von Dokumenten .....	39
5.4.4 Sammlungen .....	40
5.4.5 Metadaten für einzustellende Dokumente .....	41
5.4.6 Konfiguration des ePA-Frontend des Versicherten .....	42
<b>6 Funktionsmerkmale .....</b>	<b>47</b>
<b>6.1 Allgemein .....</b>	<b>47</b>
6.1.1 Aktensession-Verwaltung .....	47
6.1.2 Kommunikation mit dem ePA-Aktensystem .....	49
6.1.3 Sicherer Kanal zur Dokumentenverwaltung .....	51
6.1.4 Geräteautorisierung .....	51
6.1.5 Zertifikatsprüfung .....	52
6.1.5.1 Vertrauensanker des TI-Vertrauensraum .....	53
6.1.5.2 TSL-Behandlung .....	53
6.1.5.3 Zertifikatsprüfung von Zertifikaten der TI .....	55
6.1.5.4 Zertifikatsprüfung von Internet-Zertifikaten .....	56
6.1.6 Dokumente .....	56
6.1.7 Umschlüsselung der Dokumente .....	57
6.1.7.1 Kryptographische Architektur der Dokumentenverschlüsselung .....	57
6.1.8 ePA-FdV für Desktop-Plattformen .....	58
<b>6.2 Implementation ePA-Anwendungsfälle im FdV .....</b>	<b>58</b>
6.2.1 Übergreifende Festlegungen .....	59
6.2.2 Fehlerbehandlung .....	61
6.2.3 Aktivitäten .....	63
6.2.3.1 Authentisieren des Nutzers .....	63
6.2.3.2 Authentisierungstoken erneuern .....	65
6.2.3.3 Dokumentenset in Dokumentenverwaltung hochladen .....	66
6.2.3.4 Dokumentenset aus Dokumentenverwaltung herunterladen .....	67
6.2.3.5 Dokumentenset in Dokumentenverwaltung löschen .....	69
6.2.3.6 Suche nach Dokumenten in Dokumentenverwaltung .....	70
6.2.3.7 Vergebene Berechtigungen bestimmen .....	71
6.2.3.8 AuthorizationKey .....	72
6.2.3.8.1 Struktur AuthorizationKeyType .....	72
6.2.3.8.2 Schlüsselableitung für Ver- und Entschlüsselung .....	73

6.2.3.8.3 AuthorizationKey erstellen .....	74
6.2.3.8.4 AuthorizationKey entschlüsseln .....	76
6.2.3.9 Schlüsselmateriale aus ePA-Aktensystem laden .....	77
6.2.3.10 Schlüsselmateriale aller Berechtigten aus ePA-Aktensystem laden .....	79
6.2.3.11 Schlüsselmateriale im ePA-Aktensystem speichern .....	80
6.2.3.12 Schlüsselmateriale im ePA-Aktensystem ersetzen .....	81
6.2.3.13 Schlüsselmateriale im ePA-Aktensystem löschen .....	81
6.2.3.14 Leistungserbringerinstitution im Verzeichnisdienst der TI finden .....	82
6.2.3.15 Suchanfrage Verzeichnisdienst der TI .....	83
6.2.3.16 PIN-Eingabe für eGK durch Nutzer .....	84
6.2.4 Nutzerzugang ePA .....	85
6.2.4.1 Login Aktensession .....	85
6.2.4.2 Logout Aktensession .....	93
6.2.5 Aktenkontoverwaltung .....	95
6.2.5.1 Aktenkonto aktivieren .....	95
6.2.5.2 Anbieter wechseln .....	97
6.2.5.3 Schließen einer Akte .....	104
6.2.6 Umschlüsselung .....	105
6.2.7 Berechtigungsverwaltung .....	111
6.2.7.1 Spezifische Zugriffsregeln .....	116
6.2.7.1.1 kategorienbasierte Berechtigung .....	116
6.2.7.1.2 Dokumentenspezifische Berechtigung .....	120
6.2.7.2 Vertretung einrichten .....	121
6.2.7.3 Berechtigung für Kostenträger vergeben .....	124
6.2.7.4 Vergebene Berechtigungen anzeigen .....	125
6.2.7.5 Eingerichtete Vertretungen anzeigen .....	127
6.2.7.6 Bestehende Berechtigungen verwalten .....	127
6.2.7.6.1 Berechtigung für LEI ändern .....	127
6.2.7.6.2 Berechtigung für LEI löschen .....	129
6.2.7.6.3 Berechtigung für Vertreter löschen .....	130
6.2.7.6.4 Berechtigung für Kostenträger löschen .....	131
6.2.8 Dokumentenverwaltung .....	133
6.2.8.1 Dokumente einstellen .....	133
6.2.8.2 Dokumente suchen .....	136
6.2.8.3 Dokument herunterladen .....	138
6.2.8.4 Dokumente im Aktenkonto löschen .....	139
6.2.9 Protokollverwaltung .....	140
6.2.9.1 Zugriffsprotokoll einsehen .....	140
6.2.10 Verwaltung eGK .....	145
6.2.10.1 PIN der eGK ändern .....	145
6.2.10.2 PIN der eGK entsperren .....	148
6.2.11 Geräteverwaltung .....	151
6.2.11.1 Benachrichtigungsadresse für Geräteautorisierung aktualisieren .....	151
6.2.11.2 Benachrichtigungsadressen abfragen .....	152
<b>6.3 Realisierung der Leistungen der TI-Plattform .....</b>	<b>153</b>
6.3.1 Transportschnittstelle für Kartenkommandos .....	153
6.3.1.1 Kartenterminals der Sicherheitsklasse 1 .....	155
6.3.1.2 Kartenterminals der Sicherheitsklasse 2 .....	156
6.3.1.3 Kartenterminals der Sicherheitsklasse 3 .....	156

6.3.2 Schnittstelle für PIN-Operationen und Anbindung der eGK.....	157
<b>6.4 Test-App FdV .....</b>	<b>158</b>
<b>7 Informationsmodell .....</b>	<b>161</b>
<b>8 Verteilungssicht .....</b>	<b>164</b>
<b>9 Anhang A – Verzeichnisse .....</b>	<b>165</b>
9.1 Abkürzungen .....	165
9.2 Glossar .....	166
9.3 Abbildungsverzeichnis .....	166
9.4 Tabellenverzeichnis .....	167
<b>9.5 Referenzierte Dokumente .....</b>	<b>171</b>
9.5.1 Dokumente der gematik.....	171
9.5.2 Weitere Dokumente.....	172



---

## 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.

## 1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

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

Text / Beschreibung

[<=]

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

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

---

## 2 Systemüberblick

---

Das ePA-Frontend des Versicherten (FdV) 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.

---

## 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**

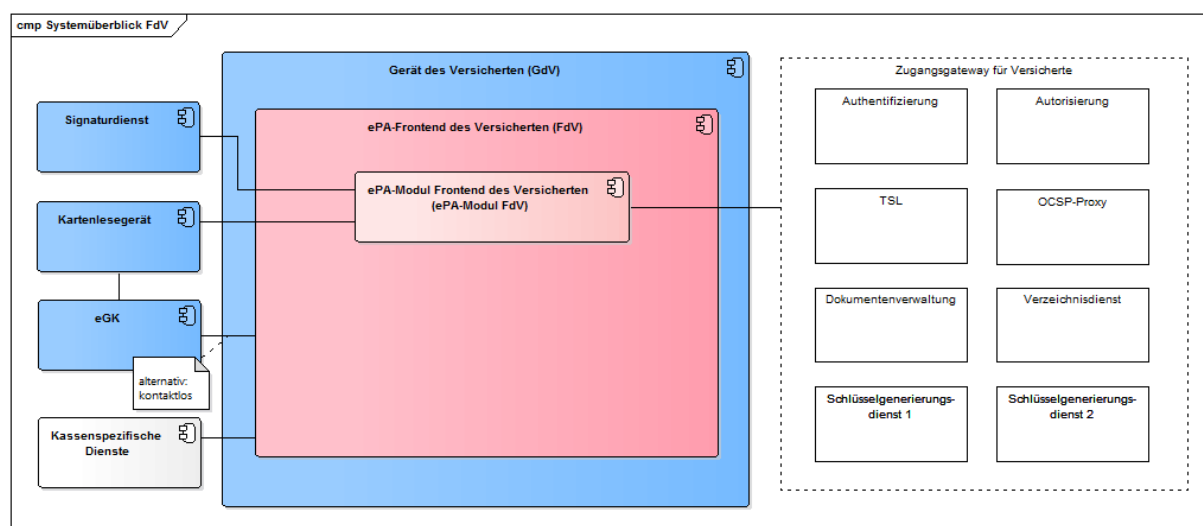
Akteur	Rolle	Beschreibung
Nutzer der FdV	Versicherter (als Aktenkontoinhaber) oder Vertreter eines Versicherten	Primärer Anwender, Ausführen von fachlichen Anwendungsfällen mit Zugriff auf ein ePA-Aktensystem
Ausführungsumgebung	Gerät des Versicherten	Betriebs-/Ablaufumgebung des FdV
Kartenleser	Gerät 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	<p>Der Hersteller FdV stellt im Handbuch Informationen bereit bezüglich</p> <ul style="list-style-type: none"><li>• Anforderungen an die Ausführungsumgebung</li><li>• Möglichkeiten zur Anbindung der eGK</li></ul> <p>Der Hersteller FdV erfüllt sicherheitstechnische Anforderungen zum</p>

		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]

I_Authorization_Insurant	getAuthorizationKey	Definition in [gemSpec_Autorisierung]
I_Authorization_Management_Insurant	deleteAuthorizationKey getAuditEvents getAuthorizationList putAuthorizationKey putNotificationInfo getNotificationInfo 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]

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

### 3.2.1 Identität des Nutzers

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

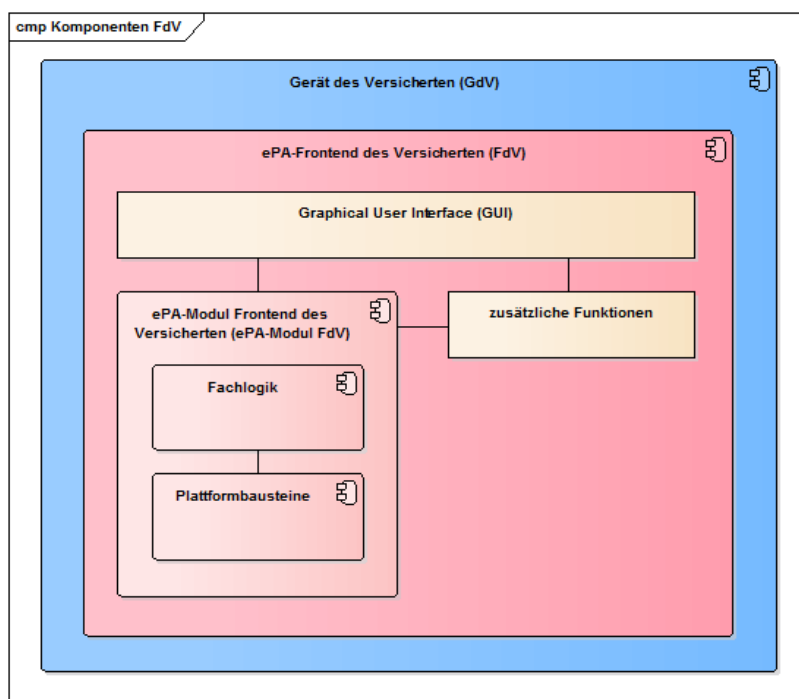
Voraussetzung ist die Nutzung einer eGK G2 oder höher, wobei eine eGK G2 nur den RSA-2048-Algorithmenkatalog unterstützt. Eine eGK G2.1 unterstützt den RSA-2048 und ECC-256-Algorithmenkatalog. Die normierenden Organisationen haben das Ende der Zulässigkeit für den RSA-2048 festgelegt. Aus diesem Grund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

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

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

## 4 Zerlegung des Produkttyps

Im Folgenden wird die Zerlegung des Produkttyps 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	<p>Diese Komponente enthält Plattformbausteine, welche Funktionalitäten der TI-Plattform zur Verfügung stellen:</p> <ul style="list-style-type: none"> <li>Zugriff auf die eGK für kryptografische Operationen, PIN-Management, ...</li> <li>Kryptografische Operationen</li> </ul> <p>Die Plattformbausteine werden durch die Fachlogik angesteuert.</p>	Kap. 6.3



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.

---

## 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 gesamte 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. [ <= ]

*Hinweis:* Der auszuführende Code für die ePA-Funktionen des ePA-FdV muss lokal vorliegen und ausgeführt werden, so dass insbesondere alle ePA-Daten (medizinische Daten, sicherheitskritische Daten wie Schlüssel) ausschließlich lokal verarbeitet werden. Zudem erschwert es Administratoren von Servern, auf denen der Code liegen könnte, den Code zu manipulieren.

Dies bedeutet insbesondere, dass eine Auslagerung von ePA-Funktionen auf Webserver nicht erlaubt ist. Dies verhindert jedoch nicht, das ePA-FdV mithilfe von Webtechnologien umzusetzen, um eine Plattformunabhängigkeit zu erreichen. Mithilfe des Frameworks *Electron* können beispielsweise in HTML, CSS und JavaScript entwickelte Anwendungen lokal unabhängig vom verwendeten Betriebssystem (Windows, MacOS, Linux) ausgeführt werden. *Electron* bietet auch die Möglichkeit der Nutzung von *WebAssembly*.

## **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. [ $\leq$ ]

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

## **A\_21235 - ePA-Frontend des Versicherten: Versicherten über Konsequenzen der Datenfreigabe informieren**

Der Hersteller des ePA-Frontends des Versicherten MUSS den Nutzer darüber informieren, dass das Erteilen einer Zugriffsberechtigung auf Daten für Leistungserbringer mit einem Speichern dieser Daten in der Umgebung des Leistungserbringers verbunden sein kann. [ $\leq$ ]

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. [ $\leq$ ]

## **A\_15252-02 - ePA-Frontend des Versicherten: Schlüsselmateriale 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. [ $\leq$ ]

Hinweis: Die Anforderung A\_20211 und A\_21354 legen 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. [ $\leq$ ]

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\_20211-02 - ePA-Frontend des Versicherten für mobile Plattformen: 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 Endgeräts zugegriffen werden kann,
- die biometrischen Sensoren des Endgeräts 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\_21354 - ePA-FdV für Desktop-Plattformen: Schutz von gespeicherten Authentisierungsmerkmalen**

Das ePA-FdV für Desktop-Plattformen MUSS sicherstellen, dass Authentisierungsmerkmale ausschließlich unter folgenden Bedingungen gespeichert werden:

- der Versicherte entscheidet sich hierfür bewusst (Opt-in),
- die Speicherung des Authentisierungsmerkmals auf dem Endgerät des Versicherten erfolgt ausschließlich verschlüsselt,
- auf das verschlüsselte gespeicherte Authentisierungsmerkmal kann ausschließlich nach erfolgreicher Authentifizierung des Versicherten über ein Passwort bzw. eine Passphrase zugegriffen werden.

[<=]

*Hinweis:* Dies ist die analoge Anforderung zu A\_20211 bei mobilen Endgeräten.

*Hinweis:* Eine explizite Authentifizierung des Versicherten durch das ePA-FdV wird empfohlen.

## **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. [ $\leq$ ]

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. [ $\leq$ ]

## **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. [ $\leq$ ]

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.

## **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. [ $\leq$ ]

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 Gerätekenung (DeviceID) und Session-Daten wie z.B. geheime oder private Schlüssel, Authentifizierungs- 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,
- 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,
- 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.

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. [ <= ]

## **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.

[<=]

#### **A\_21342 - ePA-FdV für Desktop-Plattformen: Anzeige eines Hinweistextes zum Betrieb auf Hardware, die nicht unter der Kontrolle des Versicherten steht**

Das ePA-FdV MUSS den Versicherten in einem Hinweistext auf die Gefahren hinweisen, die bei einem Betrieb des ePA-FdV auf Hardware, die nicht unter der Kontrolle des Versicherten steht, gegeben sind.[<=]

*Hinweis:* Im Gegensatz zu Betriebssystem für Smartphones und Tablets wie etwa Android und iOS sind Betriebssysteme für stationäre Geräte wie etwa PCs durchaus im öffentlichen Raum verfügbar. So läuft etwa auf den meisten Geräten in Internet-Cafes Windows. Würde hier das ePA-FdV ausgeführt werden und der Versicherte sich Dokumente aus seiner Akte herunterladen, dann müsste der Versicherte dafür sorgen, dass keine Daten von ihm auf der Hardware verbleiben, wenn er den Zugriff auf die Hardware beendet. Es wird empfohlen, die Nutzung des ePA-FdV auf öffentlich zugänglicher Hardware zu unterlassen.

Hinweis: Die einmalige Anzeige des Hinweises mit Bestätigung pro Versicherten ist ausreichend. Es muss dabei sichergestellt sein, dass jedem Nutzer (Mehrbenutzerbetrieb) dieser Hinweis zur Bestätigung angezeigt wird. Dieses könnte etwa durch Anzeige im Anschluss an die Authentisierung gegenüber dem ePA-FdV erfolgen.

#### **A\_21343 - ePA-FdV für Desktop-Plattformen: Ausführen von begutachtetem Code**

Der Hersteller des ePA-FdV MUSS technisch sicherstellen, dass nur im Rahmen eines Produktgutachtens begutachteter Code ausgeführt wird oder Code-Änderungen nach Vorgaben der gematik durch den Hersteller des ePA-FdV als nicht zulassungsrelevant bewertet wurden.[<=]

*Hinweis:* Die Anforderung soll das Einschleusen von Schadcode verhindern. Dies kann beispielsweise durch Signieren des ePA-FdV durch den Hersteller erfolgen, um

Manipulationen am ePA-FdV vor der Ausführung erkennen zu können. Das Verbot des dynamischen Nachladens von ungeprüftem Code soll insbesondere auch sicherstellen, dass zum Zeitpunkt der Prüfung des ePA-FdV durch den Produktgutachter der gesamte Anwendungscode vorliegt und dieser nicht später durch ungeprüften Code ersetzt bzw. ergänzt werden kann.

Im Zulassungsverfahren für das ePA-FdV ist festgelegt, wann Änderungen durch die gematik als zulassungsrelevant betrachtet werden. Zulassungsrelevante Änderungen sind z.B. Änderungen von Sicherheitsfunktionen oder deren Implementierung (z.B. Wechsel der TLS-Implementierung). Nicht-zulassungsrelevante Änderungen sind z.B. Sicherheitsupdates für von anderen Herstellern bezogenen Software-Komponenten der Plattform (z.B. Bibliotheken), die aus einer vertrauenswürdigen Quelle bezogen werden.

#### **A\_21344 - ePA-FdV für Desktop-Plattformen: Code von Drittanbietern aus vertrauenswürdigen Quellen**

Der Hersteller des ePA-FdV MUSS die Software-Komponenten des ePA-FdV, die nicht vom Hersteller des ePA-FdV selbst entwickelt oder zur Entwicklung beauftragt werden (z.B. TLS-Bibliotheken), aus bekannten und vertrauenswürdigen Quellen beziehen. [ $\leq$ ]

#### **A\_21355 - ePA-FdV für Desktop-Plattformen: Zugriff auf den Geräteidentifikator durch Zusatzfunktionen**

Das ePA-FdV DARF Zusatzfunktionen des FdV (d.h. kassenspezifische Dienste) NICHT auf den Geräteidentifikator (die von der Autorisierung übermittelte Zufallszahl bei der Gerätebindung) zugreifen lassen. [ $\leq$ ]

#### **A\_21356 - ePA-FdV für Desktop-Plattformen: Speicherung des Geräteidentifikators**

Das ePA-FdV MUSS sicherstellen, dass die Speicherung des Geräteidentifikators (die von der Autorisierung übermittelte Zufallszahl bei der Gerätebindung) ausschließlich verschlüsselt erfolgt. [ $\leq$ ]

#### **A\_21357 - ePA-FdV für Desktop-Plattformen: Zugriff auf den Geräteidentifikator**

Das ePA-FdV MUSS sicherstellen, dass auf den verschlüsselten gespeicherten Geräteidentifikator ausschließlich nach erfolgreicher Authentifizierung des Versicherten beim Start des ePA-FdV zugegriffen werden kann. [ $\leq$ ]

*Hinweis:* Nach A\_20746 muss sich der Nutzer beim Starten des ePA-FdV am ePA-FdV authentisieren.

#### **A\_21350 - ePA-FdV für Desktop-Plattformen: Informieren des Versicherten über sichere Bezugsquellen für die Verteilung des FdV**

Der Hersteller des ePA-FdV MUSS Versicherte über die vertrauenswürdigen Quellen informieren, von denen Versicherte das ePA-FdV beziehen können und wie sie die Vertrauenswürdigkeit der Quelle erkennen können. [ $\leq$ ]

*Hinweis:* Krankenkassen (als Anbieter eines ePA-Aktensystems) können zur Umsetzung dieser Anforderung z.B. den Versicherten hierzu entsprechendes Informationsmaterial zur Verfügung stellen, wo die Download-Punkte aufgelistet sind.

#### **A\_21351 - ePA-FdV für Desktop-Plattformen: Sicherstellung der Authentifizierung der Bezugsquelle bei Erstbezug**

Der Hersteller des ePA-FdV MUSS sicherstellen, dass der Versicherte bei Erstbezug eines ePA-FdV die Authentizität der vertrauenswürdigen Bezugsquelle verifizieren kann. [ $\leq$ ]

*Hinweis:* Beim Erstbezug des ePA-FdV kann die Prüfung der Authentizität der Quelle noch nicht durch das ePA-FdV selbst erfolgen. Dies kann z.B. über eine TLS-Server-Authentifizierung der Bezugsquelle erreicht werden. Bei ePA-FdVs in den Stores der mobilen Plattformen kann der Versicherte die Vertrauenswürdigkeit daran erkennen, dass

er den offiziellen Store nutzt. Auch unter Windows und Mac OS und Linux/Debian gibt es einen offiziellen Store.

### **A\_21352 - ePA-FdV für Desktop-Plattformen: Technische Authentifizierung der Update-Bezugsquellen für die sichere Verteilung der ePA-FdV-Anwendung**

Das ePA-FdV MUSS sicherstellen, dass Updates nur von bekannten und vertrauenswürdigen Quellen bezogen werden, nach dem die Authentizität der Quelle technisch erfolgreich verifiziert wurde. [ $\leq$ ]

## **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. [ $\leq$ ]

### **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.

[ $\leq$ ]

### **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. [ $\leq$ ]

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 (inklusive 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.

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. [ <= ]

**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.

**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 eine 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.

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
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 geänderten 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**

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 kategorienbasierten Berechtigungsverwaltung werden vom Aktensystem definierte Ordner genutzt. Nur für dynamische Dokumentensammlungen (z. B. Kinderuntersuchungsheft und Mutterpass) werden Ordner durch Primärsysteme erstellt und vom Frontend ggf. ausgewertet. 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 oder Bearbeiten von Ordnern und ihrer Metadaten ist durch das FdV nicht möglich. Das Entfernen von Dokumenten aus einem Ordner durch Löschen der entsprechenden Assoziation ist nicht vorgesehen, da dies die direkte Zuordnung gemäß einer Zugriffsunterbindungsregel verletzen könnte.

### **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 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

der ePA-Dokumentenverwaltung herunter (IHE-Akteur Content Consumer), bearbeitet es und lädt die veränderte Fassung als neu zu registrierendes Policy Document in die ePA-Dokumentenverwaltung hoch (IHE APPC-Akteur Content Creator). Beim Hochladen einer veränderten Version eines Policy Document wird die vorherige Version infolge des Hochladens des neuen Policy Document automatisch durch die ePA-Dokumentenverwaltung gelöscht. Beim Entzug einer Berechtigung löscht das ePA-Frontend des Versicherten das entsprechende Policy Document aus der ePA-Dokumentenverwaltung.

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

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\_15673-03 - ePA-Frontend des Versicherten: Policy Document für LEI erstellen**

Das ePA-Frontend des Versicherten MUSS für eine zu berechtigende LEI ein Policy Document unter Berücksichtigung der Anforderungen an deren Inhalt in A\_15442 erstellen. [ $\leq$ ]

#### **A\_15674-03 - ePA-Frontend des Versicherten: Policy Document für Vertreter erstellen**

Das ePA-Frontend des Versicherten MUSS für einen zu berechtigenden Vertreter ein Policy Document unter Berücksichtigung der Anforderungen an deren Inhalt in A\_15440 erstellen. [ $\leq$ ]

#### **A\_17232-03 - ePA-Frontend des Versicherten: Policy Document für Kostenträger erstellen**

Das ePA-Frontend des Versicherten MUSS für einen zu berechtigenden Kostenträger ein Policy Document unter Berücksichtigung der Anforderungen an deren Inhalt in A\_17460 erstellen. [ $\leq$ ]

## **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.

### **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. [ $\leq$ ]

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. [ $\leq$ ]

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. [ $\leq$ ]

## **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)
- 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 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.

## **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.



**A\_18257 - ePA-Frontend des Versicherten: Dokumentengröße an Ausschnittstellen**

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.



**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.

## 5.4.5 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] beschrieben. Es kann auf die Anzeige einzelner nutzbarer Metadatenattribute verzichtet werden, um eine übersichtliche Darstellung beim Einstellen der Dokumente zu erreichen.

Das FdV soll für die Eingabe von Metadaten required-Attribute als Pflichtfelder kennzeichnen. Dabei soll unterschieden werden zwischen einer einfachen Ansicht für das Einstellen von Dokumenten des Versicherten und einer erweiterten Ansicht für das Einstellen von LE-Dokumenten durch den Versicherten. Vorgaben dazu werden in [gemSpec\_DM\_ePA] getroffen.

Defaultmäßig wird der Nutzer als Submission Set author (Einstellender) gesetzt. Die Werte für den author werden mindestens 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 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 gezielt 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\_15292-05 - 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 5: TAB\_FdV\_104 – Parameter FdV**

Parameter	Beschreibung	Wertebereich (Default Wert)
Aktenkontoinhaber: Akten-ID	Akten-ID (RecordIdentifier) des Aktenkontos für den Versicherten	siehe Bildungsvorschrift gemäß <a href="#">[gemSpec_DM_ePA#Record Identifier]</a>
Aktenkontoinhaber: FQDN Anbieter ePA-Aktensystem	FQDN für den Zugriff auf das ePA- Aktensystem des zugehörigen Anbieters für den Versicherten	
Aktenkontoinhaber: Anbieter-ID	"HomeCommunityId" des ePA-Aktensystems Der Parameter wird mittels Abfrage des Namensdienstes im Internet bestimmt. Er wird durch das FdV automatisch gesetzt	siehe [gemSpec_DM_ePA]

	und ist nicht durch den Nutzer konfigurierbar.	
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 zu vertretenden Versicherten	siehe Bildungsvorschrift gemäß <a href="#">[gemSpec_DM_ePA#RecordIdentifier]</a>
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
Benachrichtigungen aktivieren	Benachrichtigung über neue, geänderte oder gelöschte ePA-Dokumente	ja/nein Default: ja

Benachrichtigungszeitraum		<p>Optionen:</p> <ul style="list-style-type: none"> <li>• seit der letzten Anmeldung</li> <li>• seit einem konkreten Datum</li> <li>• in einem durch den Versicherten einstellbaren, beliebigen zurückliegender Zeitraum (x Wochen, x Monate) bis zum aktuellen Datum</li> <li>• Default: seit der letzten Anmeldung</li> </ul>
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 Geräteerkennung (DeviceID). Die Geräteerkennung wird für die Geräteautorisierung genutzt.	string, 64 Zeichen
eGK nutzen	Gibt an, ob zur Authentifizierung des Versicherten die eGK genutzt wird oder ein alternatives Verfahren.	ja/nein Default: ja

URL des Signaturdienstes	URL des Signaturdienstes	URL Default: nein
Defaultwert der Vertraulichkeitsstufe beim Einstellen von Dokumenten		normal/vertraulich/streng vertraulich Default: gemäß A_20178*

[<=]

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 bestimmbar 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.

---

## 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. [ $\leq$ ]

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

##### **A\_17505-02 - ePA-Frontend des Versicherten für mobile Plattformen: 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. [ $\leq$ ]

##### **A\_21830 - ePA-FdV für Desktop-Plattformen: optionale Auswahl kryptographische Versichertenidentität**

Das ePA-Frontend des Versicherten für Desktop-Plattformen KANN 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 für Desktop-Plattformen bekannt gemacht hat. [ $\leq$ ]

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. [ <= ]

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 6: 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].

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 Vollausslastung der Systemressourcen im ePA-Aktensystem die Verbindungsanfrage 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 7: 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	

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. [ $\leq$ ]

#### **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. [ $\leq$ ]

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\_15299-03 - ePA-Frontend des Versicherten: eine TLS-Session pro Aktensession**

Das ePA-Frontend des Versicherten MUSS für jede Aktensession genau eine TLS-Session nutzen. [ $\leq$ ]

Für jede Aktensession kann eine separate TLS-Verbindung genutzt werden.

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. [ $\leq$ ]

#### **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. [ $\leq$ ]

#### **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. [ $\leq$ ]

### 6.1.3 Sicherer Kanal zur Dokumentenverwaltung

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

- `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b`
- `I_Document_Management_Insurant::RegistryStoredQuery`
- `I_Document_Management_Insurant::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. [ $\leq$ ]

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 Geräteebeane auf Seiten der Versicherten umgesetzt. Der Zugriff auf ein Aktenkonto ist zulässig, wenn das Gerät, auf dem das FdV genutzt wird, durch den Nutzer über einen separaten Benachrichtigungskanal (E-Mail mit Freischalt-Link) zur Benutzung eines Aktenkontos autorisiert wurde. Siehe auch [\[gemSpec\\_Autorisierung#Freischaltprozess neuer Geräte\]](#).

Das Gerät wird durch die Geräteerkennung (DeviceID) identifiziert. Die Geräteerkennung beinhaltet die Geräteidentität und den Gerätenamen. Die Geräteidentität ist eine Zufallszahl, welche dem ePA-Frontend des Versicherten von der Autorisierung übermittelt wird. Der Gerätenamen 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 Geräteerkennung mit leerem Geräteidentifikator (`phr:DeviceID::Device`) im Aufruf gesandt. Da noch kein bekannter Geräteidentifikator für dieses GdV in der Autorisierung registriert ist, antwortet die Autorisierung mit dem Fehler `DEVICE_UNKNOWN` und einer Zufallszahl im Fehlertext. Das 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 8: 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	ja	C.HCI.ENC	oid_smc_b_enc	aktiv

Berechtigung von LEI ändern				
Verbindungsaufbau SGD	ja	C.SGD-HSM.AUT	oid_sgd1_hsm oid_sgd2_hsm	aktiv

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. [ $\leq$ ]

"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.

[ $\leq$ ]

#### **6.1.5.2 TSL-Behandlung**

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

**A\_15874-02 - ePA-Frontend des Versicherten: Periodische Aktualisierung TI-Vertrauensraum**

Das ePA-Frontend des Versicherten MUSS zur periodischen Aktualisierung des TI-Vertrauensraums den TUC\_PKI\_001 mit folgenden Anpassungen umsetzen:

- Der Offline-Modus ist nicht zu berücksichtigen
- Auslöser: keine TSL lokal gespeichert oder die gespeicherte TSL ist zu alt (die in der TSL selbst kodierte Gültigkeitsdauer NextUpdate ist abgelaufen).
- Sofern nur eine abgelaufene TSL vorliegt, soll abweichend von TUC\_PKI\_006 in Schritt 5 die Prüfung des OCSP-Signer-Zertifikats des TSL-Signer OCSP-Responders nicht mittels der TSL, sondern gegen die TSL-Signer-CA erfolgen.
- 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.

### 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 [\[gemSpec\\_Zugangsgateway\\_Vers#A\\_15869 - Zugangsgateway des Versicherten, Bereitstellung OCSP-Forwarder\]](#).



#### 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	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• Zu prüfendes Zertifikat: vom SGD übermitteltes Zertifikat</li> <li>• EECertificateContainedInTSL: true</li> <li>• Referenzzeitpunkt: aktuelle Systemzeit</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• Gültigkeit zu Referenzzeitpunkt</li> <li>• Rolle des Zertifikates</li> </ul>
--------------------------------------	--

[<=]

#### 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 Webrowsers 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. [<=]

##### A\_21301 - ePA-FdV für Desktop-Plattformen: Kein Ausführen von aktiven Inhalten bei der Anzeige

Das ePA-FdV DARF bei der Anzeige von Dokumenten aktive Elemente NICHT ausführen. [<=]

*Hinweis:* Aktive Elemente sind alle code-ausführenden Anteile eines Dokuments, also etwa Makros oder Skripte. Diese dürfen im Kontext des FdV nicht ausgeführt werden, etwa indem auch bei zugelierten Bibliotheken diese Funktionalität deaktiviert wird. Die Verwendung explizit externer Applikationen wird dabei nicht betrachtet, da hier aus



Sicht des ePA-FdV der Vorgang mit dem Herunterladen des Dokuments als abgeschlossen angesehen wird.

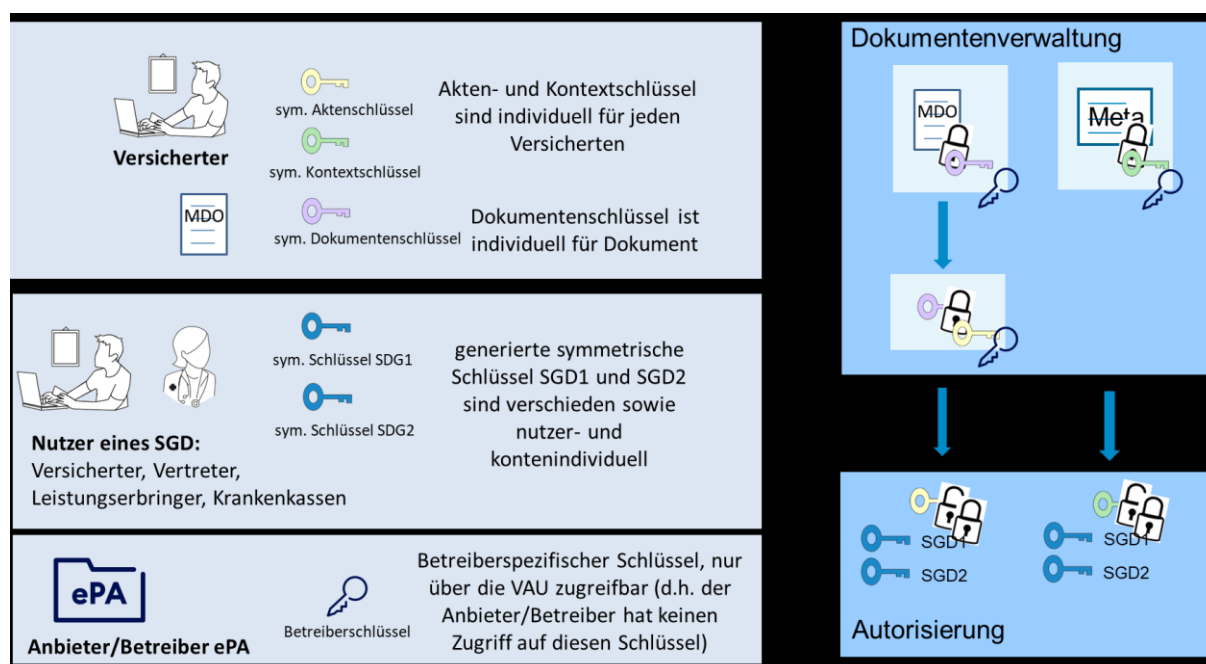
### 6.1.7 Umschlüsselung der Dokumente

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.

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 berechnigte 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.

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.

[<=]

## **6.1.8 ePA-FdV für Desktop-Plattformen**

Wird das FdV nicht auf einem mobilen Gerät betrieben, muss die Verwendung des FdV durch mehrere Versicherte für den Zugriff auf die individuellen ePA möglich sein.

## **A\_21358 - ePA-FdV für Desktop-Plattformen: Mehrbenutzerfähigkeit des Desktop-Clients**

Das ePA-FdV MUSS die Ausführung der Aktensteuerung über verschiedene, lokale Benutzerkonten des Betriebssystems oder alternativ eine FdV-interne Benutzer-Kontensteuerung ermöglichen. [<=]

## **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\_15567-05 - ePA-Frontend des Versicherten: Zulässigkeit der Anwendungsfälle

Das ePA-Frontend des Versicherten MUSS die Zulässigkeit des Anwendungsfalles 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)]

**Tabelle 9: 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	Dismissed Start_Migration Suspended	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	OK VERIFYABLE
Eingerichtete Vertretungen auflisten	Aktenkontoinhaber Vertreter	n/a	immer
Berechtigung für LEI ändern	Aktenkontoinhaber Vertreter	Activated Dismissed <a href="#">Start_Migration</a> <a href="#">Suspended</a>	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
Dokumente einstellen	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
Dokumente suchen	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
Dokumente löschen	Aktenkontoinhaber Vertreter	Activated Dismissed	OK VERIFYABLE
Dokumente herunterladen	Aktenkontoinhaber Vertreter	Activated Dismissed	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 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 - 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 10: 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 11: TAB\_FdV\_108 – Behandlung von Fehlern des ePA-Aktensystems

Fehlercode	Fehlertext	Spezifische Aktion durch ePA-Frontend des Versicherten
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	<p>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.</p> <p>In Kürze erhalten Sie den Bestätigungslink für Ihre Autorisierung an die hinterlegte E-Mail Adresse.</p> <p>Falls Sie diese E-Mail nicht erhalten haben, prüfen Sie bitte Ihren Spam-Ordner.</p> <p>Falls Sie keinen Zugriff mehr auf Ihre hinterlegte E-Mail Adresse</p>	Der Anwendungsfall wird abgebrochen.

	haben, können Sie uns gerne kontaktieren.	
wst:InvalidSecurityToken	Ihre Gesundheitskarte ist ungültig, bitte wenden Sie sich an Ihre Krankenkasse.	

[&lt;=]

### 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.[<=]

### 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 12: TAB\_FdV\_109 – Authentisieren des Nutzers**

I_Authentication_Insurant:: LoginCreateChallenge Request erstellen	RequestSecurityToken (RST) erstellen
I_Authentication_Insurant:: LoginCreateChallenge Response verarbeiten	RequestSecurityTokenResponse (RSTR) verarbeiten Rückgabedaten: <ul style="list-style-type: none"> <li>st:Challenge = Challenge</li> </ul>

<p><code>I_Authentication_Insurant::LoginCreateToken</code> Request erstellen</p>	<p>RequestSecurityTokenResponse (RSTR) erstellen Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• <code>wst:Challenge</code> = Challenge aus RSTR</li> </ul> <p>Der Request wird signiert und die Signatur im SOAP Header eingefügt.</p> <ul style="list-style-type: none"> <li>• <code>wsse:BinarySecurityToken</code> = C.CH.AUT des Nutzers</li> <li>• <code>ds:SignatureValue</code> = signierter Hashwert</li> </ul>
<p>wenn Authentisierung mittels eGK: Plattformbaustein <code>PL_TUC_SIGN_HASH_nonQES</code> zum Signieren nutzen</p>	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• <code>Identifikator</code> = für eGK G2: <code>PrK.CH.AUT.R2048</code> für eGK höhere Generation: <code>PrK.CH.AUT.E256</code></li> <li>• <code>Signaturverfahren</code> = für eGK G2: <code>signPSS</code> für eGK höhere Generation: <code>signECDSA</code></li> <li>• Hashwert = <code>soap:Body</code></li> </ul> <p>Der Body der SOAP-Nachricht wird gemäß <code>[gemSpec_Authentisierung_Vers]</code> 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 (<code>MRPIN.home</code>) für seine eGK aufgefordert, falls der notwendige Sicherheitszustand der eGK noch nicht erreicht ist.</p> <p>Rückgabedaten:</p> <ol style="list-style-type: none"> <li>1. OK + Hashsignatur oder</li> <li>2. Fehler</li> </ol>
<p>wenn Authentisierung mittels alternativer kryptographischer Versichertenidentität:</p>	<p>Aufruf der signaturdienstspezifischen Schnittstelle <code>I_Remote_Sign_Operations::sign_Data</code> Eine Beschreibung der konkreten Ausgestaltung der Schnittstelle befindet sich in <code>[vesta]</code>. Der Response liefert u.a. das C.CH.AUT_ALT Zertifikat. Dieses wird in die Session-Daten übernommen.</p>



I_Authentication_Insurant:: LoginCreateToken Response verarbeiten	RequestSecurityTokenResponse Collection (RSTRC) verarbeiten Rückgabedaten: <ul style="list-style-type: none"> <li>saml2:Assertion = AuthenticationAssertion</li> </ul> AuthenticationAssertion (Authentisierungstoken) in Session-Daten übernehmen
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.

[&lt;=]

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 13: TAB\_FdV\_173 – Logout - Authentisierungstoken abmelden**

Vorbedingung	AuthenticationAssertion in Session-Daten
I_Authentication_Insurant:: RenewToken Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> <li>RenewTarget: AuthenticationAssertion aus Session-Daten</li> </ul>

I_Authentication_Insurant::RenewToken Response verarbeiten	RequestSecurityTokenResponse (RSTR) verarbeiten Rückgabedaten: <ul style="list-style-type: none"> <li>RequestedSecurityToken = AuthenticationAssertion</li> </ul> AuthenticationAssertion (Authentisierungstoken) in Session-Daten ersetzen.
---	--

[&lt;=]

Der vorher genutzte Authentisierungstoken wird gelöscht.

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

### 6.2.3.3 Dokumentenset in Dokumentenverwaltung hochladen

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

#### A\_15314-01 - 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 14: TAB\_FdV\_111 – Dokumentenset in Dokumentenverwaltung hochladen**

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

[&lt;=]

#### 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. [ $\leq$ ]

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. [ $\leq$ ]

## **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. [ $\leq$ ]

## **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. [ $\leq$ ]

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 15: TAB\_FdV\_112 – Dokumentenset aus Dokumentenverwaltung herunterladen**

<p>I_Document_Management_Insurant:: RetrieveDocumentSet Request erstellen</p>	<p>Eingangsparameter:</p> <ul style="list-style-type: none"> <li>RetrieveDocumentSet_Message gemäß IHE XDS-Transaktion [ITI-43]</li> <li>AuthenticationAssertion aus Session-Daten</li> </ul>
<p>I_Document_Management_Insurant:: RetrieveDocumentSet Response verarbeiten</p>	<p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>RetrieveDocumentSetResponse_Message gemäß IHE XDS-Transaktion [ITI-43]</li> </ul> <p>RetrieveDocumentSetResponse_Message beinhaltet ein oder mehrere Dokumente. Jedes medizinische Dokument ist mit einem individuellen Dokumentenschlüssel verschlüsselt. Der Dokumentenschlüssel ist mit dem Aktenschlüssel verschlüsselt.</p>
<p>für jedes medizinische Dokument aus RetrieveDocumentSetResponse_Message: Plattformbaustein PL_TUC_SYMM_DECIPHER nutzen</p> <p>Hinweis: Der Begriff "medizinische Dokumente" umfasst alle Dokumente, welche durch LEI, KTR oder Versicherte in das ePA-Aktensystem eingestellt wurden. Davon abgegrenzt werden die technischen Dokumente (Policy Documents). Sie werden unverschlüsselt übertragen.</p>	<p>Für Vorgaben zum Entschlüsseln eines Dokumentes aus dem ePA-Aktensystem siehe <a href="#">[gemSpec_DM_ePA#2.4.2 Entschlüsselung]</a>.</p> <p>Dokumentenschlüssel mit PL_TUC_SYMM_DECIPHER entschlüsseln Eingangsdaten:</p> <ul style="list-style-type: none"> <li>verschlüsselter Dokumentenschlüssel aus EncryptedData\EncryptedKey\CipherData</li> <li>Aktenschlüssel (RecordKey) aus Session-Daten</li> <li>Der optionale Parameter AD wird nicht verwendet.</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>entschlüsselter Dokumentenschlüssel</li> </ul> <p>Dokument mit PL_TUC_SYMM_DECIPHER entschlüsseln Eingangsdaten:</p> <ul style="list-style-type: none"> <li>verschlüsseltes Dokument aus EncryptedData\CipherData</li> <li>entschlüsselter Dokumentenschlüssel</li> </ul>

	<ul style="list-style-type: none"> <li>• Der optionale Parameter AD wird nicht verwendet.</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• entschlüsseltes Dokument</li> </ul>
--	---

[&lt;=]

**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.[<=]

**6.2.3.5 Dokumentenset in Dokumentenverwaltung löschen**

Mit dieser Operation werden ein oder mehrere Dokumente anhand ihrer 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 16: TAB\_FdV\_113 – Dokumentenset in Dokumentenverwaltung löschen**

I_Document_Management_Insurant::RemoveMetadata Request erstellen	<b>Eingangsdaten:</b> <ul style="list-style-type: none"> <li>AuthenticationAssertion aus Session-Daten</li> <li>xds:DeleteDocumentSet_Message gemäß IHE RMD-Transaktion [ITI-62]</li> </ul>
I_Document_Management_Insurant::RemoveMetadata Response verarbeiten	<b>Rückgabedaten:</b> <ul style="list-style-type: none"> <li>xds:DeleteDocumentSetResponse_Message gemäß IHE RMD-Transaktion [ITI-62]</li> </ul>

[<=]

### 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 17: TAB\_FdV\_114 – Suche nach Dokumenten in Dokumentenverwaltung**

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

[<=]

**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 `$XSDSDocumentEntryTitle` sowie dem optionalen Parameter `$XSDSDocumentEntryAuthorInstitution` nutzen können. [≤]

Der zusätzliche Parameter "`$XSDSDocumentEntryTitle`" filtert die Suchergebnismenge über das Attribut `XSDSDocumentEntry.title`. Dabei ist die Angabe von Platzhaltern (wie für Suchanfragen über den Parameter `$XSDSDocumentEntryAuthorPerson`) 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 "`$XSDSDocumentEntryAuthorInstitution`" filtert die Suchergebnismenge über das Attribut `XSDSDocumentEntry.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 18: TAB\_FdV\_115 – Vergebene Berechtigungen bestimmen**

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

[≤]

**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. [ $\leq$ ]

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. [ $\leq$ ]

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 bzw. den XDS-Metadaten ermittelt werden.

**Berechtigung für LEI:** Telematik-ID, Name der LEI, Berechtigung "erteilt am", Berechtigung "gültig bis", Zugriffsrecht der LEI berechnete 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.

#### **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 (31.12.9999) 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 Chiffre mit dem verschlüsselten Akten- und Kontextschlüssel sowie `AssociatedData`.

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

#### 6.2.3.8.2 Schlüsselableitung für Ver- und Entschlüsselung

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

#### **A\_17842-01 - 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	<a href="#">[gemSpec_SGD_ePA#2.4 Initiale Schlüsselableitung für den Kontoinhaber]</a>
Berechtigung für LEI vergeben Vertretung einrichten Berechtigung für Kostenträger vergeben Berechtigung für LEI ändern	Versicherter	Verschlüsseln	<a href="#">[gemSpec_SGD_ePA#2.6 Schlüsselableitung für einen Berechtigungsempfänger]</a>

Berechtigung für LEI vergeben Berechtigung für Kostenträger vergeben Berechtigung für LEI ändern	Vertreter	Verschlüssel n	<a href="#">[gemSpec SGD ePA#2.8 Schlüsselableitung für einen Berechtigungsempfänger durch einen Vertreter]</a>
Login	Versicherte r Vertreter	Entschlüssel n	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:AssociatedData 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 [\[gemSpec SGD ePA#A 17990\]](#).

##### *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.

**Tabelle 19: TAB\_FdV\_179 – Akten- und Kontextschlüssel verschlüsseln**

Plattformbaustein PL_TUC_SYMM_EN CIPHER nutzen	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• Doc: Klartextpräsentation von Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel)</li> <li>• Cert: aus SGD1 abgeleiteter symmetrischer Schlüssel</li> <li>• AD: Berechnung siehe gemSpec_SGD_ePA A_17930</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• Doc<sub>enc</sub></li> </ul> <p>Mit Doc<sub>enc</sub> und AD<sub>SGD1</sub> wird eine Struktur gemäß [gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht] gebildet -&gt; Doc<sub>enc1</sub></p>
Plattformbaustein PL_TUC_SYMM_EN CIPHER nutzen	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• Doc: Doc<sub>enc1</sub></li> <li>• Cert: aus SGD2 abgeleiteter symmetrischer Schlüssel</li> <li>• AD: Berechnung siehe gemSpec_SGD_ePA A_17930</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• Doc<sub>enc</sub></li> </ul> <p>Mit Doc<sub>enc</sub>, AD<sub>SGD1</sub> und AD<sub>SGD2</sub> wird der EncryptedKeyContainer des AuthorizationKey gebildet.</p>

[&lt;=]

#### 6.2.3.8.4 AuthorizationKey entschlüsseln

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

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

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

Es gelten für das Entschlüsseln die Vorgaben aus [\[gemSpec\\_SGD\\_ePA#8 Interoperables Austauschformat\]](#) sowie [\[gemSpec\\_Krypt#A\\_17872 - Ver- und Entschlüsselung der Akten und Kontextschlüssel \(Schlüsselableitungsfunktionalität ePA\)\]](#).

### **A\_17843 - ePA-Frontend des Versicherten: Akten- und Kontextschlüssel entschlüsseln**

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

**Tabelle 20: TAB\_FdV\_180 – Akten- und Kontextschlüssel entschlüsseln**

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

[<=]

### **6.2.3.9 Schlüsselmateriale aus ePA-Aktensystem laden**

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

### A\_15330-02 - 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 21: TAB\_FdV\_116 – Schlüsselmaterial aus ePA-Aktensystem laden**

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

	Key (erfolgreich/nicht erfolgreich)
--	-------------------------------------

[&lt;=]

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 22: TAB\_FdV\_163 – Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden**

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

[&lt;=]

### 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\_15331-02 - 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 23: TAB\_FdV\_117 – Schlüsselmaterial im ePA-Aktensystem speichern**

<pre>I_Authorization_Management_Insurant: : putAuthorizationKey Request erstellen</pre>	<p>Eingangsparameter:</p> <ul style="list-style-type: none"> <li>• AuthenticationAssertion aus Session-Daten</li> <li>• RecordIdentifier aus Session-Daten</li> <li>• AuthorizationKey</li> <li>• DeviceID aus Geräte-Daten</li> <li>• optional: NotificationInfoRepresentative</li> </ul>
<pre>I_Authorization_Management_Insurant: : putAuthorizationKey Response verarbeiten</pre>	<p>HTTP OK ohne SOAP-Response oder gematik Fehlermeldung</p> <p>Für Fehler KEY_ERROR siehe A_15332-01 ePA-Frontend des Versicherten: Schlüsselmaterial im ePA-Aktensystem speichern KEY_ERROR"</p>

[<=]

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.[<=]



### 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 24: TAB\_FdV\_118 – Schlüsselmaterial im ePA-Aktensystem ersetzen**

I_Authorization_Management_Insurant:: replaceAuthorizationKey Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> <li>• AuthenticationAssertion aus Session-Daten</li> <li>• RecordIdentifier aus Session-Daten</li> <li>• NewAuthorizationKey</li> <li>• DeviceID aus Gerät-Daten</li> </ul>
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 25: TAB\_FdV\_119 – Schlüsselmaterial im ePA-Aktensystem löschen**

I_Authorization_Management_Insurant:: deleteAuthorizationKey Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> <li>• AuthenticationAssertion aus Session-Daten</li> <li>• RecordIdentifier aus Session-Daten</li> <li>• ActorID</li> <li>• DeviceID aus Gerät-Daten</li> </ul>
---	---

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

[&lt;=]

#### 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.

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

#### A\_15335-01 - 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 26: TAB\_FdV\_120 – Suchkriterien LDAP Search**

Suchkriterium	Beschreibung für die Suche nach Heilberuflern	Beschreibung der Suche nach Leistungserbringerinstitutionen	LDAP-Directory Basisdatensatz Attribut
Anzeigename	Nachname, Vorname des Heilberuflers	Name der Organisation/Einrichtung des Gesundheitswesens	displayName
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
Institution/Berufsguppe	Berufsguppe	Institution	professionOID
Fachgebiet	medizinisches Fachgebiet	Fachabteilung	specialization
TelematikID	Eindeutige ID des Heilberufers in der TI	Eindeutige ID der Institution in der TI	telematikID

[&lt;=]

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

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

#### **A\_17435-01 - 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 Markup 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 27: TAB\_FdV\_121 – Abfrage Verzeichnisdienst**

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

**[<=]**

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 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 Verschlüsselungszertifikate, 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 28: TAB\_FdV\_122 – PIN-Eingabe durch Nutzer**

Plattformbaustein PL_TUC_CARD_VERIFY_PIN	Durch den Plattformbaustein PL_TUC_CARD_INFORMATION wird eine Nutzerverifikation durchgeführt.
Eingangsdaten	<ul style="list-style-type: none"> <li>• Identifikator = MRPIN.home</li> <li>• Nutzerhinweis für PIN-Eingabe default: "EingabePIN:"</li> </ul>
Beschreibung	Der Nutzerhinweis wird bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT im Nutzerinterface (GUI) bzw. bei Nutzung eines Kartenterminal Sicherheitsklasse 3 im Display des Kartenterminals angezeigt.
Rückgabedaten	<ul style="list-style-type: none"> <li>• OK - PIN erfolgreich verifiziert Es wird mit der folgenden Aktivität fortgefahren</li> </ul>
Varianten/Alternati-ven	<ul style="list-style-type: none"> <li>• 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.</li> <li>• PasswordBlocked - PIN ist durch Fehleingaben blockiert Dem Nutzer wird der Anwendungsfall "PIN der eGK entsperren" angeboten.</li> </ul>

[&lt;=]

### **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.

Bei der Anmeldung eines Nutzers als Vertreter oder bei der Anmeldung des Versicherten bei seinem alten Aktensystem während des Anbieterwechsels erfolgt das Login immer explizit. Dabei unterstützt das ePA-Frontend des Versicherten den Benutzer bei der Auswahl des Aktensystems des zu Vertretenen.

#### **A\_13695-03 - ePA-Frontend des Versicherten: Login Aktensession**

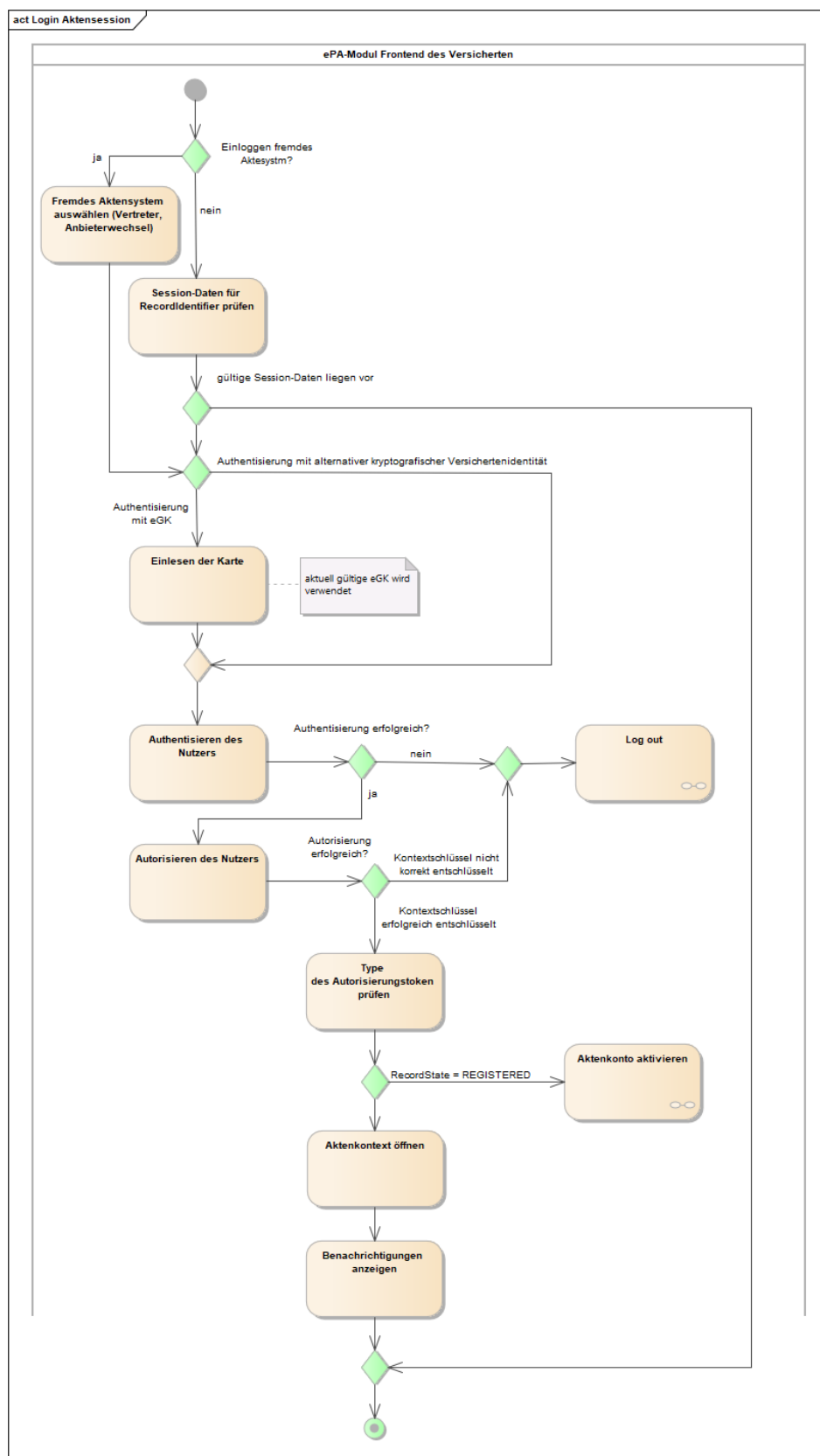
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 1.1 - Login durch einen Versicherten" aus [gemSysL\_ePA] gemäß TAB\_FdV\_123 umsetzen.

**Tabelle 29: TAB\_FdV\_123 – Login Aktensession**

Name	Login Aktensession
Auslöser	<ul style="list-style-type: none"> <li>• Der Akteur möchte einen fachlichen Anwendungsfall mit Datenzugriff auf das ePA-Aktensystem ausführen.</li> <li>• optional: explizites Login im Verlauf des Starts des FdV</li> </ul>
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	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> <li>optional: wenn Einloggen im "fremden" Aktensystem (als Vertreter, beim Anbieterwechsel) <ol style="list-style-type: none"> <li>FQDN fremdes Aktensystem auswählen (Nutzung von <code>I_Authorization_Management_Insurant::getRecordProviderList</code>)</li> </ol> </li> <li>Session-Daten für RecordIdentifier prüfen</li> <li>optional: wenn Authentisieren mittels eGK <ol style="list-style-type: none"> <li>Einlesen der Karte</li> </ol> </li> <li>Authentisieren des Nutzers</li> <li>Autorisieren des Nutzers</li> <li>Status des Aktenkontos prüfen</li> <li>Aktenkontext öffnen</li> <li>optional: Benachrichtigungen anzeigen</li> </ol>
Varianten/Alternativen	<p>Wenn nach der Aktivität "Autorisieren des Nutzers" ein Autorisierungstoken mit <code>RecordState = REGISTERED</code> vorliegt, dann wird der Anwendungsfall "Login Aktensession" ohne Fehler abgebrochen und der Anwendungsfall "Aktenkonto aktivieren" gestartet.</p> <p>In allen – nicht behebbaren – Fehlerfällen wird der Anwendungsfall abgebrochen und der Anwendungsfall "Logout Aktensession" gestartet.</p>

[&lt;=]





aot Login Aktensession

ePA-Modul Frontend des Versicherten

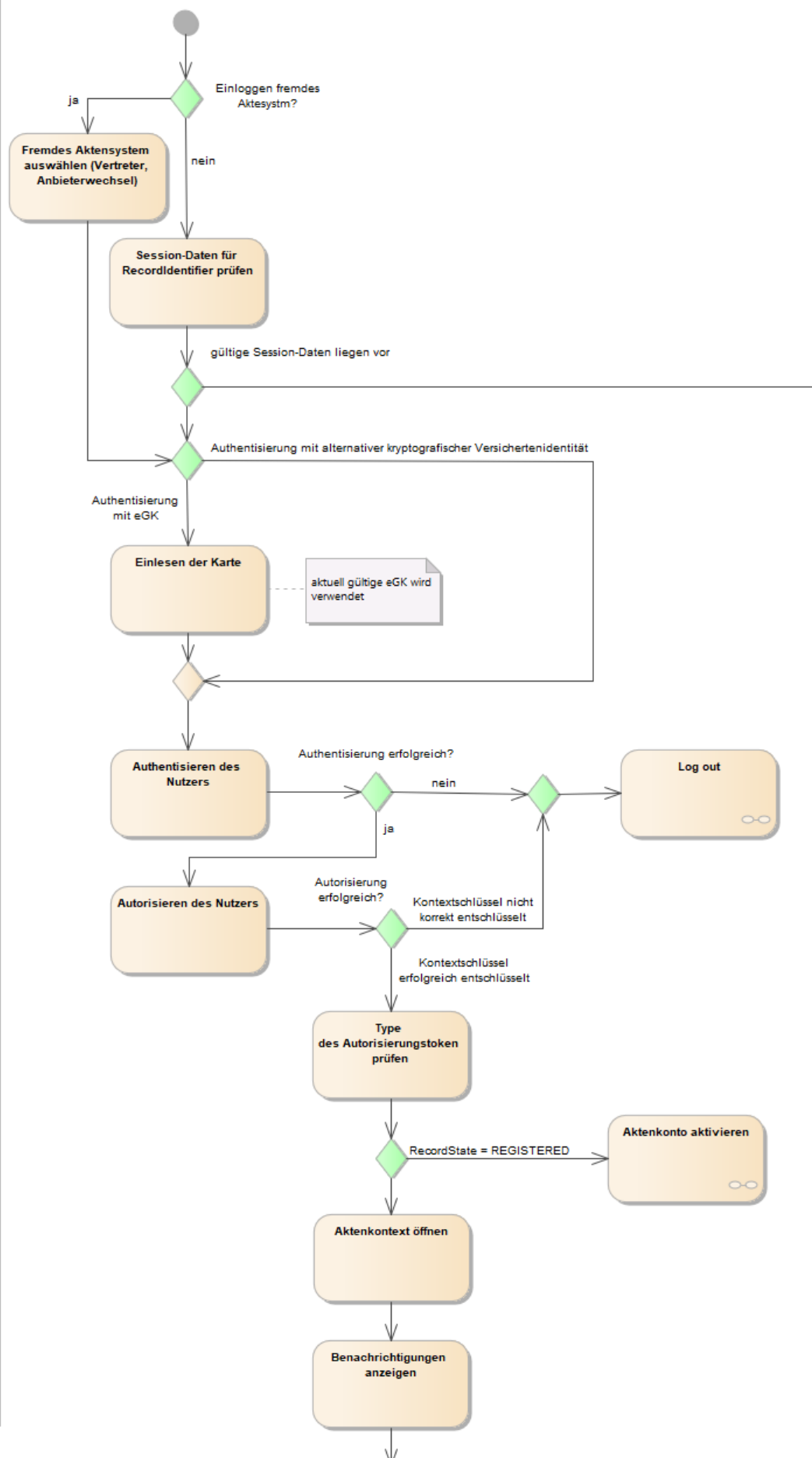


Abbildung 4: Aktivitätsdiagramm "Login Aktensession"

**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 30: TAB\_FdV\_124 – Login - Einlesen der Karte

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

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

**A\_15342 - ePA-Frontend des Versicherten: Login - Abbruch bei Karte lesen**

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

## Authentisieren und Autorisieren

### **A\_15343-01 - 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 - 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.[<=]

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 [\[gemSpec\\_Dokumentenverwaltung#Schnittstelle I\\_Document\\_Management\\_Connect\]](#) ).

**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. [ $\leq$ ]

**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. [ $\leq$ ]

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 31: TAB\_FdV\_126 – Login - Aktenkontext öffnen - Operation OpenContext**

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

[ $\leq$ ]

**Benachrichtigungen**

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

**A\_15350 - ePA-Frontend des Versicherten: Login - Benachrichtigungen anzeigen optional**

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

**A\_15351 - ePA-Frontend des Versicherten: Login - Benachrichtigungen anzeigen unterdrücken**

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

**A\_15352-01 - 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\_15352-01-15485 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 umsetzen, in der die Protokolleinträge für folgende Zugriffe übersichtlich dargestellt werden:

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

[ <= ]

Es 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.

**Tabelle 32: TAB\_FdV\_127 – Logout Aktensession**

Name	Logout Aktensession
Auslöser	<ul style="list-style-type: none"> <li>• Aufruf des Anwendungsfalls in der GUI</li> <li>• Der Akteur war innerhalb seiner Aktensession über einen maximalen Zeitraum hinaus inaktiv.</li> <li>• Fehler im Anwendungsfall "Login Aktensession"</li> </ul>
Akteur	Versicherter, berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Die Session-Daten sind gelöscht.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> <li>1. Aktenkontext schließen</li> <li>2. Authentisierungstoken abmelden</li> <li>3. optional, wenn eine alternative kryptographische Versichertenidentität für die Authentisierung genutzt wurde: Freischaltung des Signaturdienstes beenden</li> <li>4. Session-Daten löschen</li> </ol>

[&lt;=]

**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 33: 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

[&lt;=]

### 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 34: TAB\_FdV\_172 – Logout - Authentisierungstoken abmelden**

Vorbedingung	AuthenticationAssertion in Session-Daten
I_Authentication_Insurant::LogoutToken Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> <li>CancelTarget: AuthenticationAssertion aus Session-Daten</li> </ul>
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. [<=]

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 35: TAB\_FdV\_130 – Aktenkonto aktivieren**

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

[<=]

**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.



**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. [ $\leq$ ]

**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. [ $\leq$ ]

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\_21545 - ePA-Frontend des Versicherten: Anbieter wechseln - Steuerung des Wechsels über das FdV des neuen Anbieters**

Die Steuerung des Anbieterwechsels MUSS über das FdV des neuen Anbieters erfolgen. [ $\leq$ ]

**A\_15369-01 - 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. Der Versicherte MUSS auf die Möglichkeit des signierten Exports der Protokolle hingewiesen werden.

[ $\leq$ ]

### **A\_15371-01 - ePA-Frontend des Versicherten: Anbieter wechseln - Informationen zum anderen am Wechsel beteiligten Anbieter**

Das ePA-Frontend des Versicherten MUSS dem Versicherten ermöglichen, die folgenden Registrierungsinformationen des anderen am Wechsel beteiligten Anbieters zu erfassen bzw. auszuwählen:

- Akten-ID
- FQDN des Anbieter

Das FdV kann die Operation

`I_Authorization_Management_Insurant::getRecordProviderList` nutzen, um dem Versicherten die Auswahl des abgebenden Aktensystems zu ermöglichen. Alternativ kann das FdV auch eine optionale Schnittstelle des ePA-Aktensystems zur Ermittlung des FQDN des abgebenden Aktensystems entsprechend `gemSpec_Aktensystem#A_21740` nutzen.  
[<=]

### **A\_15372-02 - PA-Frontend des Versicherten: Anbieter wechseln - Zugriffsberechtigungen anzeigen und Umzug bestätigen**

Das ePA-Frontend des Versicherten MUSS dem Versicherten die zugriffsberechtigten Leistungserbringerinstitutionen und Vertreter aus dem ePA-Aktensystem des alten Anbieters anzeigen und dem Versicherten die Möglichkeit geben, zu entscheiden, welche der bestehenden Berechtigungen in das ePA-Aktensystem des neuen Anbieters übernommen werden sollen. [<=]

Die Anzeige der zugriffsberechtigten LEIs und, Vertreter 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\_15370-02 - ePA-Frontend des Versicherten: Anbieter wechseln**

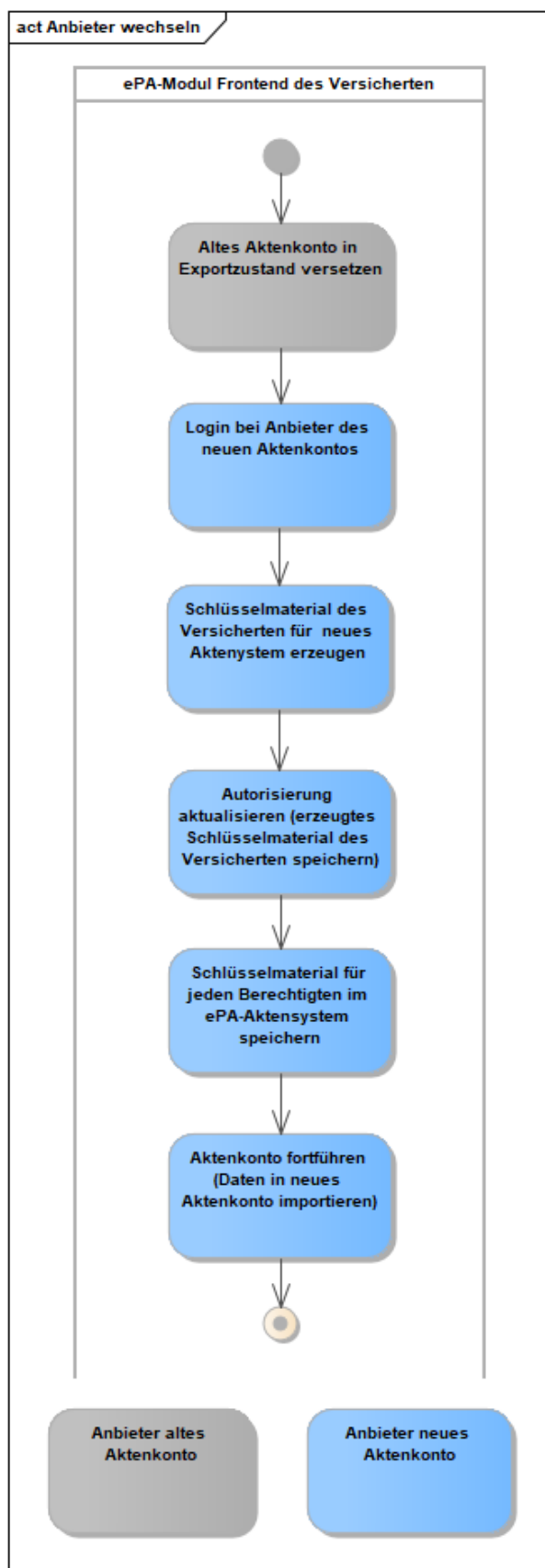
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 2.5 - Anbieter wechseln" aus [gemSysL\_ePA] gemäß TAB\_FdV\_131 umsetzen.

**Tabelle 36: TAB\_FdV\_131 – Anbieter wechseln**

Name	Anbieter wechseln
Auslöser	<ul style="list-style-type: none"> <li>• Aufruf des Anwendungsfalls in der GUI</li> </ul>
Akteur	Versicherter
Vorbedingung	<p>Der Versicherte hat ein neues Aktenkonto bei einem anderen Anbieter eröffnet. Das neue Aktenkonto ist bereit für den Datenimport.</p> <p>Der Versicherte ist im Aktenkonto des alten Anbieters angemeldet. Aktenschlüssel und Kontextschlüssel liegen unverschlüsselt in den Session-Daten vor.</p> <p>Der Versicherte hat die Registrierungsinformationen des alten Anbieters erfasst/ausgewählt.</p> <p>Der Versicherte hat eine Auswahl getroffen, welche Zugriffsberechtigungen zum neuen Anbieter übernommen werden sollen.</p>

Nachbedingung	<p>Das Aktenkonto beim alten Anbieter befindet sich im Status START_MIGRATION. Es ist kein Zugriff mehr möglich.</p> <p>Der neue Anbieter ist informiert, dass zeitnah ein Transferpaket für den Import in das Aktenkonto vom alten Anbieter bereitgestellt wird.</p> <p>Die Berechtigungen sind vom Aktenkonto des alten in das des neuen Anbieters übernommen worden.</p>
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> <li>1. Altes Aktenkonto in Exportzustand versetzen</li> <li>2. Login beim Anbieter des neuen Aktenkontos</li> <li>3. Schlüsselmaterial des Versicherten für neues Aktensystem erzeugen</li> <li>4. Autorisierung aktualisieren (erzeugtes Schlüsselmaterial des Versicherten speichern)</li> <li>5. für jeden Berechtigten: Schlüsselmaterial im ePA-Aktensystem speichern</li> <li>6. Aktenkonto fortführen (Daten in neues Aktenkonto importieren)</li> </ol>

[&lt;=]



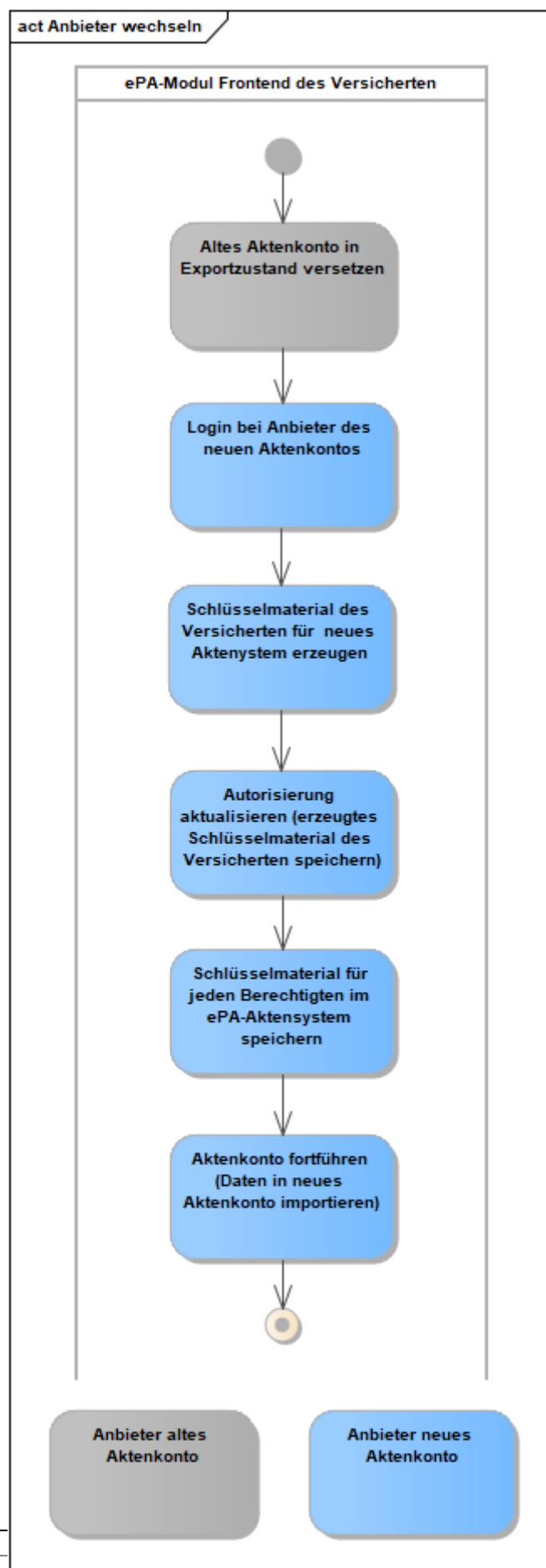


Abbildung 5: Aktivitätsdiagramm "Anbieter wechseln"

**A\_15377-02 - 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 37: TAB\_FdV\_132 – Anbieter wechseln - Aktenkonto in Exportzustand versetzen**

I_Account_Management_Insurant::SuspendAccount Request erstellen	<b>Eingangsparameter:</b> <ul style="list-style-type: none"> <li>• AuthenticationAssertion aus Session-Daten</li> <li>• ENC-VAU-Zertifikat des Betreibers des neuen Anbieters</li> </ul>
I_Account_Management_Insurant::SuspendAccount Response verarbeiten	<b>Rückgabedaten:</b> <ul style="list-style-type: none"> <li>• PackageURL</li> </ul> <p>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.</p>

[<=]

Nachdem das Aktenkonto den Zustand SUSPENDED ("bereit für Anbieterwechsel") erhalten hat, kann der Versicherte oder ein berechtigter Nutzer nicht mehr auf das 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".

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\_15347-\*,

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.

#### **A\_21839 - ePA-Frontend des Versicherten: ENC-VAU-Zertifikat des Betreibers für Anbieterwechsel**

Das ePA-Frontend des Versicherten MUSS das ENC-VAU-Zertifikat des Betreibers im UseCase Anbieterwechsel verfügbar machen. [`<=`]

Hinweis: Das ENC-VAU-Zertifikat des Betreibers darf im ePA-FdV persistent gespeichert werden.

#### **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. [`<=`]

Die bestehenden Berechtigungen werden in das ePA-Aktensystem des neuen Anbieters übernommen.

#### **A\_15598-02 - ePA-Frontend des Versicherten: Anbieter wechseln - Berechtigung LEI 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 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\_15635-01 - ePA-Frontend des Versicherten: Anbieter wechseln - Benachrichtigungsadresse Vertreter erfassen**

Das ePA-Frontend des Versicherten MUSS es dem Nutzer im Anwendungsfall "Anbieter wechseln" ermöglichen, bei der Übernahme der Berechtigungen in das Aktenkonto des neuen Anbieters für jeden Vertreter die Benachrichtigungsadresse für den Geräteautorisierung zu erfassen. Dabei MUSS die bestehende Benachrichtigungsadresse jedes Verteters mittels `GetNotificationInfo` ermittelt werden, um sie dem Versicherten zur Übernahme anzubieten. [`<=`]

### 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 Eingangsparameter `AuthorizationKey` = erstellter `AuthorizationKey`. Der optionale Parameter `NotificationInfoRepresentative` wird für LEI und KTR nicht belegt.

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

### 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 38: TAB\_FdV\_133 – Anbieter wechseln - Aktenkonto fortführen**

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

[≤]

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.

### 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 ePA-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. [ <= ]

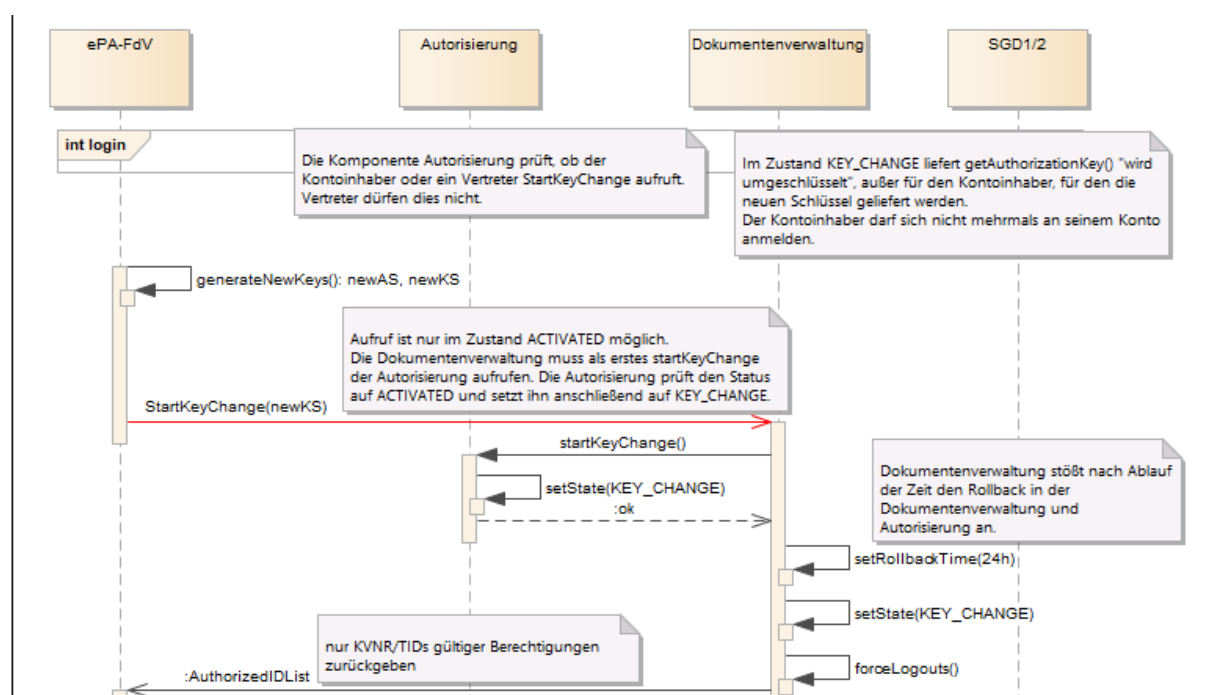
### A\_21129 - Revisionssicherer Export der Protokolle

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

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.



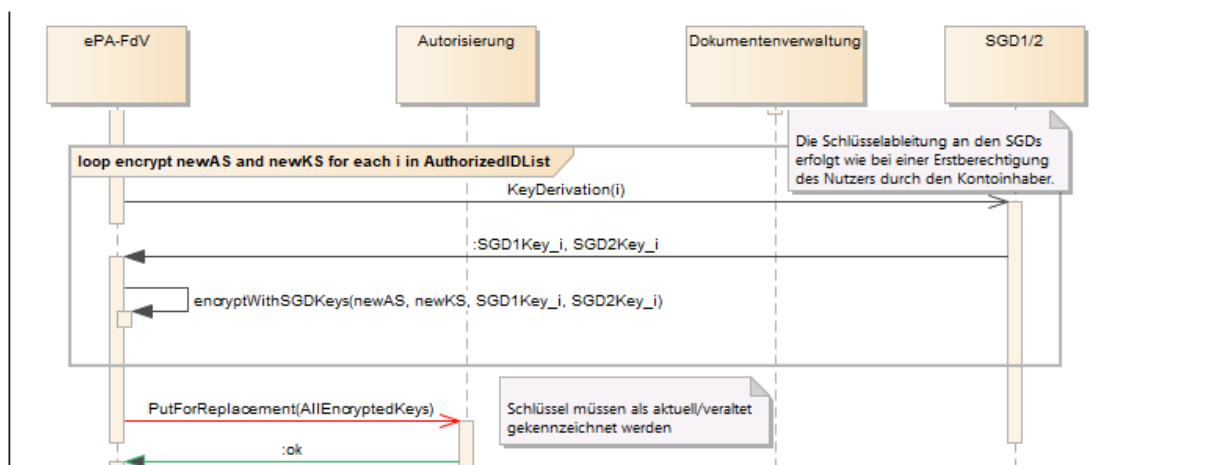


Abbildung 7: Umschlüsselung II

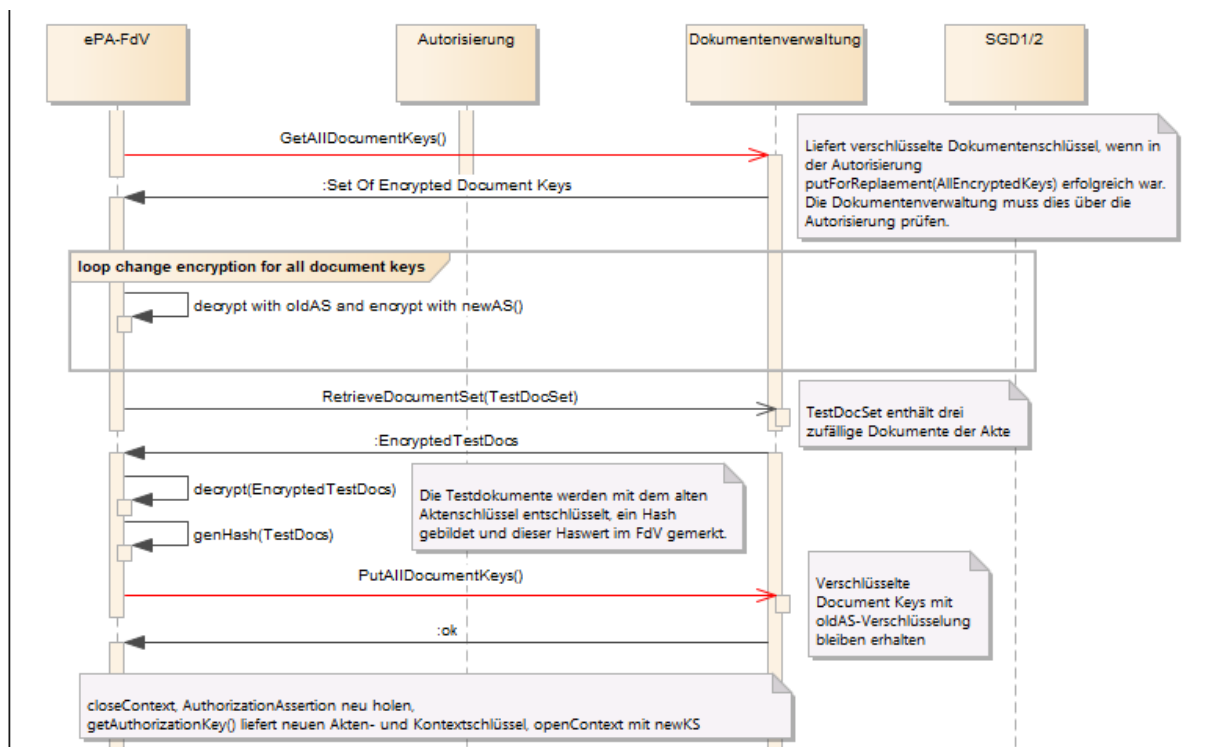


Abbildung 8: Umschlüsselung III

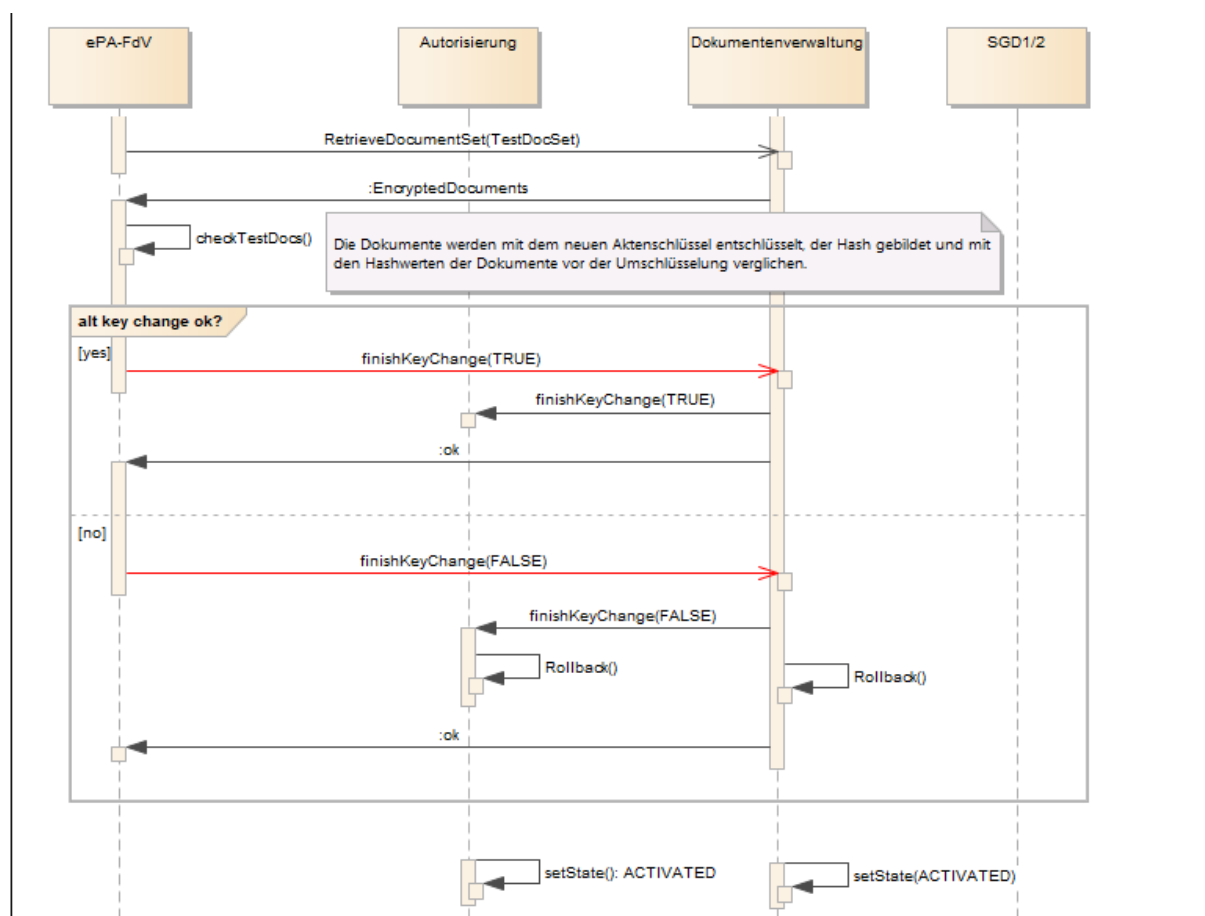


Abbildung 9: Umschlüsselung IV

#### A\_20507-01 - ePA-Frontend des Versicherten: Funktions-Timeout für Aufrufe an die Dokumentenverwaltung, die Autorisierungskomponente und die Schlüsselgenerierungsdienste SGD1 und SGD2

Das ePA-Frontend des Versicherten MUSS während der Umschlüsselung bei allen Funktionsaufrufen an die Dokumentenverwaltung, die Autorisierungskomponente und die Schlüsselgenerierungsdienste nach Ablauf der Timeout-Zeit von mindestens 60 Minuten die Umschlüsselung abbrechen und die Methode `finishKeyChange(FALSE)` bei der Komponente Dokumentenverwaltung aufrufen. [ $\leq$ ]

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.

#### A\_20725-01 - ePA-Frontend des Versicherten: Abbruch der Umschlüsselung durch den Versicherten

Das ePA-Frontend des Versicherten MUSS während der Umschlüsselung dem Nutzer anbieten, die Umschlüsselung abubrechen. Wenn der Nutzer die Umschlüsselung abbricht, dann sendet das FdV die Nachricht `finishKeyChange(FALSE)` an die Dokumentenverwaltung. Die Dokumentenverwaltung ihrerseits sendet dann die Nachricht `finishKeyChange(FALSE)` an die Komponente Autorisierung. [ $\leq$ ]

Die Komponenten Autorisierung und Dokumentenverwaltung führen nach Erhalt der 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\_20479-04 - 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	<ol style="list-style-type: none"> <li>1. Neuer Aktenschlüssel ist erzeugt</li> <li>2. Neuer Kontextschlüssel ist erzeugt.</li> <li>3. Für jeden Berechtigten sind neue SGD1 und SGD2 Schlüssel erzeugt</li> <li>4. Für alle Berechtigten sind der neue Akten- und der neue Kontextschlüssel mit den neuen SGD Schlüssel in der Autorisierungskomponente hinterlegt.</li> <li>5. Alle Dokumentenschlüssel in der Dokumentenverwaltungskomponente sind mit dem neuen Aktenschlüssel umgeschlüsselt.</li> <li>6. Die Akte befindet sich im Zustand "ACTIVATED".</li> </ol>
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> <li>1. Das FdV generiert einen neuen Akten- und einen neuen Kontextschlüssel wie in gemSpecFdv#6.2.5.1. beschrieben.</li> <li>2. Der Versicherte startet die Umschlüsselung mit dem Aufruf der Funktion <code>StartKeyChange()</code> (gemSpec_Dokumentenverwaltung#5.3.2.1) an der Komponente Dokumentenverwaltung. Die Dokumentenverwaltung ihrerseits ruft <code>startKeyChange()</code> in der Autorisierung auf. Wenn innerhalb der <code>rollbackTime</code> (z.B. 24</li> </ol>

	<p>h) die Umschlüsselung nicht abgeschlossen ist, werden sowohl die Autorisierung als auch das Aktensystem den Zustand einnehmen, den sie vor der Umschlüsselung hatten. Die Autorisierungskomponente setzt den Status der Akte auf den Zustand KEY_CHANGE. 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 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.</p> <p>3. Das FdV ruft für den Versicherten, jede berechnigte LEI, für jede berechnigte Kasse und für jeden Vertreter die Funktion <code>KeyGeneration()</code> 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.</p> <p>4. Das FdV verschlüsselt für den Versicherten, für jede berechnigte LEI, jede berechnigte Kasse und jeden berechtigten Vertreter den neuen Aktenschlüssel mit den von den SGD1 und SGD2 generierten nutzerindividuellen Schlüsseln.</p> <p>5. Das FdV verschlüsselt für den Versicherten, für jede berechnigte LEI, jede berechnigte Kasse und jeden berechtigten Vertreter den neuen Kontextschlüssel mit den von den SGD1 und SGD2 generierten nutzerindividuellen Schlüsseln.</p> <p>6. Das FdV übermittelt mit dem Aufruf der Methode <code>PutForReplacement(SetOfEncryptedKeys)</code> die in (4 und 5) 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.</p> <p>7. Das FdV ruft mit der Methode <code>GetAllDocumentKeys()</code> der Komponente Dokumentenverwaltung alle verschlüsselten Dokumentenschlüssel (Rückgabewert <code>DocumentKeyList</code>) vom</p>
--	---

	<p>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.</p> <ol style="list-style-type: none"> <li>8. Das FdV entschlüsselt die verschlüsselten Dokumentenschlüssel mit dem alten Aktenschlüssel.</li> <li>9. Das FdV verschlüsselt die entschlüsselten Dokumentenschlüssel mit dem neuen Aktenschlüssel.</li> <li>10. 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.</li> <li>11. Das FdV übermittelt mit dem Aufruf der Methode <code>PutAllDocumentKeys()</code> 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.</li> <li>12. Das FdV schließt die VAU in der Dokumentenverwaltung über <code>closeContext()</code>.</li> <li>13. 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 10 gespeicherten Dokumenten-IDs die verschlüsselten Dokumente aus der Dokumentenverwaltung.</li> <li>14. Das FdV entschlüsselt die in Schritt 13 heruntergeladenen Dokumente und bildet mit der in Schritt 10 verwendeten Hashfunktion erneut den Hashwert über jedes der entschlüsselten Dokumente.</li> <li>15. Anschließend vergleicht das FdV die in Schritt 10 und Schritt 14 für jedes Dokument erzeugten Hashwerte, wenn sie identisch sind, dann ist die Umschlüsselung erfolgreich durchgeführt worden.</li> <li>16. Wenn in Schritt 15 die erfolgreiche Umschlüsselung festgestellt worden ist, dann ruft das FdV an der Komponente Dokumentenverwaltung die Methode <code>finishKeyChange(true)</code> auf. Diese ersetzt die mit dem alten Aktenschlüssel verschlüsselten Dokumentenschlüssel durch die mit dem neuen Aktenschlüssel verschlüsselten sowie den mit dem alten Kontextschlüssel verschlüsselten Kontext durch den mit dem neuen Kontextschlüssel verschlüsselten. Anschließend ruft die Dokumentenverwaltung <code>finishKeyChange(true)</code> in der</li> </ol>
--	---

	<p>Autorisierungskomponente auf. Die Autorisierung setzt den Status der Akte wieder auf ACTIVATED. Damit ist die Umschlüsselung abgeschlossen.</p> <p>17. Wenn in Schritt 15 die Umschlüsselung als fehlgeschlagen erkannt wurde (weil die verglichenen Hashwerte nicht gleich waren), dann ruft das FdV an der Komponente Dokumentenverwaltung die Methode <code>finishKeyChange(FALSE)</code> auf. Diese ruft die <code>Rollback()</code>-Methode auf, welche die alten verschlüsselten Dokumentschlüssel und den alten Kontext wieder aktiviert sowie die neuen verschlüsselten Dokumentschlüssel und den neuen Kontext löscht. Anschließend ruft die Dokumentenverwaltung an der Autorisierungskomponente die Methode <code>finishKeyChange(FALSE)</code> auf. Diese ruft die <code>Rollback()</code>-Methode auf, welche die alten gespeicherten Schlüssel wieder aktiviert und die neuen löscht. Anschließend setzt die Autorisierungskomponente den Status der Akte wieder auf ACTIVATED. Damit ist die Umschlüsselung abgeschlossen.</p>
--	--

[&lt;=]

### 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.[<=]

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

#### 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\_20196-01 - 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\_4443-01 ermittelte Berufsgruppe der Leistungserbringerinstitution bei der Berechtigungsvergabe anzeigen.[<=]

**A\_20254-01 - ePA-Frontend des Versicherten: Anzeige der Dokumente, auf die in Abhängigkeit eines Policy Document eine Berechtigung wirkt**

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, sich die Dokumente (anhand der zurückgegeben UniqueIDs) anzeigen zu lassen, auf die eine konkrete Leistungserbringerinstitution des vorliegenden Policy Document berechtigt werden kann. Dazu MUSS ein Policy Document für eine aktensystemseitige Simulation hochgeladen werden können (vgl. A\_21705).[<=]

**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 39: TAB\_FdV\_134 – Berechtigung an LEI für Aktenkonto vergeben**

Name	Berechtigung an LEI für Aktenkonto vergeben
Auslöser	<ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	<p>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.</p>
Nachbedingung	<p>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.</p>
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> <li>1. AuthorizationKey für LEI erstellen</li> <li>2. Schlüsselmaterial im ePA-Aktensystem speichern</li> <li>3. Policy Document für LEI erstellen</li> <li>4. Policy Document in Dokumentenverwaltung laden</li> </ol>

[<=]



**A\_20198-01 - 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 40: TAB\_FdV\_178 Anzeige der auf ein Dokument berechtigten LEI**

Name	Anzeige der auf ein Dokument berechtigten LEI
Auslöser	<ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>
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 <ol style="list-style-type: none"> <li>Alle Policy Documents für LEI herunterladen</li> <li>Für jede gefundene LEI-Policy werden folgende Unteraktivitäten durchgeführt: <ol style="list-style-type: none"> <li>eine Dokumenten-Suchanfrage mit simulierter Berechtigung gemäß A_21705 als die ausgewählte LEI an das Aktensystem absenden</li> <li>Antwort des Aktensystems nach der DocumentEntry.uniqueId des ausgewählten Dokumentes durchsuchen.</li> <li>Wenn die DocumentEntry.uniqueId enthalten ist, dann hat die LEI Zugriff auf das Dokument und die LEI wird der Liste der zugriffsberechtigten LEI hinzugefügt.</li> </ol> </li> <li>Liste mit den zugriffsberechtigten LEI dem Nutzer anzeigen.</li> </ol>

[<=]

**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 41: TAB\_FdV\_179: Ändern der Vertraulichkeitsstufe eines Dokumentes**

Name	Ändern der Vertraulichkeitsstufe eines Dokumentes
Auslöser	<ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>

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	<ol style="list-style-type: none"> <li>1. Der Nutzer wählt die neue Vertraulichkeitsstufe für das Dokument in einem Menü aus</li> <li>2. Das FdV sendet die bestehenden Metadaten des Dokuments mit geänderter Vertraulichkeitsstufe an das Aktensystem.</li> <li>3. Das FdV zeigt dem Versicherten die neue Vertraulichkeitsstufe des Dokumentes an.</li> </ol>

[&lt;=]

#### **A\_20201-01 - 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
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Im Aktensystem ist die geänderte Zugriffsberechtigung einer LEI auf Dokumentenkategorien gespeichert
Standardablauf	<ol style="list-style-type: none"> <li>1. Der Nutzer wählt eine LEI aus, deren Policy Document schon heruntergeladen wurde.</li> <li>2. Es werden die gespeicherten Berechtigungen angezeigt.</li> <li>3. Der Nutzer kann die Zugriffsberechtigungen auf die Dokumentenkategorien ändern, indem er in einem Menü den Zugriff auf entsprechende Kategorien auswählt oder abwählt.</li> <li>4. Das FdV sendet das geänderte Policy Document an das Aktensystem.</li> </ol>

[&lt;=]

**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\_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. [<=]

**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\_20109-04 - 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 für die erteilte Zugriffsberechtigung zu konfigurieren. Folgende Optionen MUSS das ePA-Frontend anbieten:

- flexibles Enddatum
- 1 Tag (heutiges Datum)

- 7 Tage [default] (heutiges Datum + 6 Kalendertage)
- 18 Monate (heutiges Datum + 18 Monate)
- Unbefristet (31.12.9999)

[<=]

### 6.2.7.1 Spezifische Zugriffsregeln

Das Aktensystem setzt folgende Regeln um: Die kategorienbasierte Berechtigung in Form eines Policy Document berechtigt eine LEI abhängig von den Zugriffsunterbindungsregeln auch zum Einstellen eines Dokuments. Diese Autorisierung kann über Vertraulichkeitsstufen weiter eingeschränkt werden. Der lesende Zugriff auf Dokumente kann weiterhin feingranular gewährt oder entzogen werden ("Whitelisting" und "Blacklisting").

#### 6.2.7.1.1 kategorienbasierte Berechtigung

Bei der kategorienbasierten 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 ePA-Dokumentenverwaltung 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\_19685-01 - ePA-Frontend des Versicherten: Anzeige der zugehörigen Dokumentenkategorie**

Das ePA-Frontend des Versicherten MUSS dem Nutzer die dem Dokument zugeordnete Dokumentenkategorie, die in der gemSpec\_DM\_ePA in den Anforderungen A\_14761 und A\_19388 aufgeführt sind, anzeigen können. [<=]

#### **A\_19686-02 - ePA-Frontend des Versicherten: Auswahl der Leistungserbringerinstitutionen in der kategorienbasierten Berechtigung**

Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, eine oder mehrere LEI, die über die Anforderung A\_15380 gefunden wurden, den Zugriff auf eine oder mehrere Dokumentenkategorien zu ermöglichen. [<=]

#### **A\_19989-01 - ePA-Frontend des Versicherten: Ermittlung der ProfessionOID in der kategorienbasierten Berechtigung**

Das ePA-Frontend des Versicherten MUSS bei der kategorienbasierten Berechtigung die ProfessionOID der Leistungserbringerinstitution aus dem Zertifikat C.HCI.ENC (Extension Admission) der Leistungserbringerinstitution ermitteln.

[<=]

#### **A\_19687-01 - ePA-Frontend des Versicherten: Berücksichtigung der Zugriffsunterbindungsregeln bei der Anzeige der Dokumentenkategorien**

Das ePA-Frontend des Versicherten MUSS bei der kategorienbasierten Berechtigung 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 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. [ <= ]

#### **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 Leistungserbringerinstitution zugriffsberechtigt ist, über die dokumentenspezifische Berechtigung könnte der Leistungserbringerinstitution hingegen der Zugriff auf dieses Dokument entzogen worden sein. Im Resultat wird von der ePA-Dokumentenverwaltung durchgesetzt, dass diese Leistungserbringerinstitution 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\_19698-01 - ePA-Frontend des Versicherten: Erstellen eines Policy Document für die kategorienbasierte Berechtigung**

Das ePA-Frontend des Versicherten MUSS bei der Erteilung einer Berechtigung für den Zugriff auf eine Dokumentenkategorie ein Policy Document für diese Leistungserbringerinstitution erzeugen und in der ePA-Dokumentenverwaltung speichern. Dieses muss in ihren Regeln die Freigabe der einzelnen Dokumentenkategorien enthalten. Wenn es für die LEI noch kein Policy Document gibt, dann muss das ePA-Frontend des Versicherten diese erstellen. [ <= ]

##### **6.2.7.1.1.1 Weitere Einschränkung über Vertraulichkeitsstufen**

Bei der kategorienbasierten Berechtigung kann der Zugriff auf die vorhandenen Dokumente einer Dokumentenkategorie weiterhin in drei Vertraulichkeitsstufen näher festgelegt werden. 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. Es ist auch möglich, einen generellen Zugriff auf diese beiden oder einer der beiden Vertraulichkeitsstufen zu

vergeben. Dazu müssen in einer Autorisierung zusammen mit einer Vertraulichkeitsstufe alle Dokumentenkategorien für einen Zugriff ausgewählt werden.

Der Zugriff auf Dokumente der Vertraulichkeitsstufe **streng vertraulich** ist der Leistungserbringerinstitution nur dann möglich, wenn eine gesonderte Freigabe über eine Whitelist vorgenommen wird.

Eine einmal getroffene Entscheidung bezüglich der Zuordnung eines Dokumentes zu einer Vertraulichkeitsstufe und bezüglich des Zugriffs einer Leistungserbringerinstitution kann vom Versicherten durch das ePA-Frontend des Versicherten jederzeit revidiert werden.

#### **A\_19566-02 - ePA-Frontend des Versicherten: Vertraulichkeitsstufen in der kategorienbasierten Berechtigung**

Das ePA-Frontend des Versicherten MUSS dem Nutzer die Möglichkeit geben, bei der kategorienbasierten Berechtigungsvergabe pro Kategorie ein normales oder ein erweitertes Zugriffsrecht auszuwählen. [ <= ]

#### **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. [ <= ]

Beim Aufruf von `I_Document_Management_Insurant::RestrictedUpdateDocumentSet` muss immer für "previousVersion" in der Nachricht der Wert "1" angegeben werden, da der Aufruf seitens der ePA-Dokumentenverwaltung nicht für eine echte Versionierung des alten Dokuments genutzt wird. Serverseitig wird `DocumentEntry.version` entsprechend nicht verwaltet und besitzt standardmäßig deshalb immer den impliziten Wert 1.

#### **A\_21232 - ePA-Frontend des Versicherten: Konfiguration der Vertraulichkeitsstufe**

Das ePA-Frontend des Versicherten MUSS dem Nutzer die Konfiguration des Defaultwertes der Vertraulichkeitsstufe beim Einstellen von Dokumenten jederzeit ermöglichen. [ <= ]

Das Abspeichern des Defaultwertes erfolgt lokal im ePA-FdV, d.h. bei Nutzung eines weiteren Gerätes ist dieser Defaultwert nicht bekannt.

#### **A\_20178-01 - ePA-Frontend des Versicherten: Vorauswahl der Vertraulichkeitsstufe**

Das ePA-Frontend des Versicherten MUSS beim Einstellen von Dokumenten den vom Nutzer konfigurierten Defaultwert der Vertrauensstufe vorschlagen. [ <= ]

#### **A\_19567-02 - ePA-Frontend des Versicherten: Vertraulichkeits-Kennzeichnung hochgeladener Dokumente**

Das ePA-Frontend des Versicherten MUSS bei allen Dokumenten die vom Nutzer ausgewählte Vertraulichkeitsstufe in den Metadaten jedes Dokuments setzen. [ <= ]

#### **A\_19578-02 - ePA-Frontend des Versicherten: Abbildung der Vertraulichkeitsstufen auf confidentialityCodes**

Das ePA-Frontend des Versicherten MUSS, wenn der Nutzer seine Dokumente mittels der kategorienbasierten Berechtigung freigeben möchte, bei diesen Dokumenten die vom Nutzer ausgewählte Vertraulichkeitsstufe über folgende confidentialityCodes abbilden:

- **normal** -> confidentialityCode**normal**
- **vertraulich** -> confidentialityCode**restricted**

Im Detail ist dies auch schon in Kapitel 6.2.6 in den Anforderungen A\_15386 und A\_15387 übergreifend beschrieben. [ <= ]

#### **A\_19568-01 - ePA-Frontend des Versicherten: Auswahl der Leistungserbringerinstitution für die kategorienbasierte Berechtigung**

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, einer oder mehreren Leistungserbringerinstitutionen, die über die Anforderungen A\_15380 gefunden wurden, eines der folgenden Zugriffsrechte zu erteilen:

- einfaches Zugriffsrecht (Vertraulichkeitsstufe "normal")
- erweitertes Zugriffsrecht (Vertraulichkeitsstufen "normal" und "vertraulich")

[ <= ]

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

#### **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. [ $\leq$ ]

**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. [ $\leq$ ]

**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. [ $\leq$ ]

**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. [ $\leq$ ]

#### 6.2.7.1.2 Dokumentenspezifische Berechtigung

Bei der dokumentenspezifischen oder feingranularen Berechtigung wird der Zugriff einer Leistungserbringerinstitution auf die vorhandenen Dokumente der elektronischen Patientenakte auf der Ebene einzelner Dokumente organisiert. Dazu erzeugt das ePA Frontend des Versicherten für jedes freizugegebende Dokument (d.h. intern pro documentEntry.entryUUID) einen Eintrag auf einer sogenannten Whitelist, um einen Zugriff zu gewähren. Ein explizites Verbot kann der Versicherte über eine sogenannte Blacklist aussprechen. Auf einer Blacklist kann - im Gegensatz zur Whitelist - auch ein Ordner (d.h. intern pro Folder.entryUUID) der Dokumentenkategorien Kinderuntersuchungsheft als auch Mutterpass stehen, um bei potentiell mehreren Pässen spezifisch Zugriffe zu untersagen (welche u.U. durch eine Freigabe über die Dokumentenkategorien möglich wären). Beim Aktualisieren der Whitelist- oder Blacklist-Einträge muss das ePA-Frontend des Versicherten sicherstellen, dass diese Policies keine widersprüchlichen Einträge enthalten.

**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. [ $\leq$ ]

**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. [ $\leq$ ]

**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. [ $\leq$ ]



**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\_19778-01 - ePA\_Frontend des Versicherten: Abbilden eines erteilten Zugriffs in dem Policy Document**

Das ePA-Frontend des Versicherten MUSS für jede zu einem Dokument für eine LEI erteilte Berechtigung einen Whitelist-Eintrag mit der DocumentEntry.entryUUID des Dokumentes in der Whitelist-Policy des Policy Document 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\_19781-01 - ePA\_Frontend des Versicherten: Abbilden eines entzogenen Zugriffs in dem Policy Document**

Das ePA-Frontend des Versicherten MUSS einen Blacklist-Eintrag mit der DocumentEntry.entryUUID oder Folder.entryUUID (eines Folders mit zugehörigem Code "childsrecord" oder "mothersrecord" in Folder.codeList) in der Whitelist-Policy des Policy Document der LEI erstellen, wenn der Nutzer dieser LEI den Zugriff auf ein konkretes Dokument bzw. ein Kinderuntersuchungsheft oder Mutterpass entziehen möchte. [ <= ]

**6.2.7.2 Vertretung einrichten**

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

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

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

**A\_15389 - ePA-Frontend des Versicherten: Daten des Vertreters**

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

Die Berechtigungsdauer für Vertreter kann nicht zeitlich 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 42: TAB\_FdV\_135 – Vertretung einrichten**

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

[ <= ]

**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\_15400-01A\_15400 - ePA-Frontend des Versicherten: PDF mit Information für Vertretung**

Das ePA-Frontend des Versicherten MUSS dem Versicherten die Möglichkeit geben, ein druckbares Format (z.B. 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.

**A\_21534 - Einwilligung des Vertreters bestätigen**

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung einrichten" vom Versicherten bestätigen lassen, dass der Vertreter der Vertretung und der Verarbeitung der dafür erforderlichen personenbezogenen Daten im ePA-Aktensystem zugestimmt hat und den Anwendungsfall abbrechen, falls die Bestätigung durch den Versicherten nicht erfolgt. [`<=`]

### **A\_21535 - Information zu verarbeiteten personenbezogenen Daten des Vertreters im ePA-Aktensystem**

Der Hersteller des ePA-Frontends des Versicherten MUSS sicherstellen, dass dem Versicherten die notwendigen Informationen zur Verfügung gestellt werden, die für die Einholung der Zustimmung des Vertreters benötigt werden, insbesondere welche personenbezogenen Daten vom Vertreter im Rahmen der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine Vertreterberechtigung widerrufen kann, gegenüber wem er seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann und wo die Datenschutzerklärungen der entsprechenden Krankenkassen zu finden sind. [ <= ]

### **6.2.7.3 Berechtigung für Kostenträger vergeben**

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

### **A\_21547 - ePA-Frontend des Versicherten: Telematik-ID des Kostenträgers ermitteln**

Das ePA-Frontend des Versicherten MUSS die Telematik-ID des zu berechtigten Kostenträgers mittels der

Operation `I_Authorization_Management_Insurant::getKtrTelematikID` ermitteln. [ <= ]

### **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 43: TAB\_FdV\_171 – Berechtigung an Kostenträger für Aktenkonto vergeben**

Name	Berechtigung an Kostenträger für Aktenkonto vergeben
Auslöser	<ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	<p>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.</p>
Nachbedingung	<p>Der Kostenträger ist zum Zugriff auf das Aktenkonto berechtigt. Das notwendige Schlüsselmaterial ist in der Autorisierung hinterlegt.</p>

	Ein Policy Document für den Kostenträger ist in der Dokumentenverwaltung hinterlegt.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> <li>1. AuthorizationKey für Kostenträger erstellen</li> <li>2. Schlüsselmaterial im ePA-Aktensystem speichern</li> <li>3. Policy Document für Kostenträger erstellen</li> <li>4. Policy Document in Dokumentenverwaltung laden</li> </ol>

[&lt;=]

#### **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.

[&lt;=]

### **6.2.7.4 Vergebene Berechtigungen anzeigen**

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

zugriffsberechtigten Leistungserbringer, die berechtigten Vertreter und 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 44: TAB\_FdV\_137 – Vergebene Berechtigungen anzeigen**

Name	Vergebene Berechtigungen anzeigen
Auslöser	<ul style="list-style-type: none"> <li>• Aufruf des Anwendungsfalls in der GUI</li> <li>• Anwendungsfall "Anbieter wechseln"</li> </ul>
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\_15403-07 - 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 (Nur für den Fall, dass der Aufrufende der Versicherte ist. Bei Aufruf durch einen Vertreter erfolgt die Ausgabe der Namen der Vertreter nicht.) im Klartext,
- für LEI: Berechtigte Kategorien samt Vertraulichkeitsstufe
- für LEI: Explizit erlaubte oder geblockte Dokumente gemäß dokumentenspezifischer Berechtigung
- für LEI: verbleibende Berechtigungsdauer

- für Vertreter: Anzeige der E-Mail-Adresse der berechtigten Vertreter (Nur für den Fall, dass der Aufrufende der Versicherte ist. Bei Aufruf durch einen Vertreter erfolgt die Ausgabe der E-Mail-Adresse der Vertreter nicht.)

anzeigen.

[<=]

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.

### **6.2.7.5 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.[<=]

### **6.2.7.6 Bestehende Berechtigungen verwalten**

#### *6.2.7.6.1 Berechtigung für LEI ändern*

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

#### **A\_15407-04 - ePA-Frontend des Versicherten: Bestehende Berechtigungen einer Leistungserbringerinstitution ändern**

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, für bereits berechtigte Leistungserbringerinstitutionen kategorienbasierte als auch dokumentenspezifische Berechtigungsvorgaben sowie die Berechtigungsdauer anzupassen.[<=]

Die zum Zugriff auf das Aktenkonto berechtigten LEIs werden mit der übergreifenden 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 45: TAB\_FdV\_138 – Berechtigung für LEI ändern**

Name	Berechtigung für LEI ändern
Auslöser	<ul style="list-style-type: none"> <li>Aufruf der Aktion zum Ändern der Berechtigung in der GUI</li> </ul>
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 <ol style="list-style-type: none"> <li>Policy Document für LEI anpassen</li> <li>Wenn die Berechtigungsdauer geändert wurde               <ol style="list-style-type: none"> <li>AuthorizationKey für LEI erstellen</li> <li>Schlüsselmaterial im ePA-Aktensystem ersetzen</li> </ol> </li> <li>Neues Policy Document in Dokumentenverwaltung laden</li> </ol>

**[<=]**

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 - Schlüsselmateriale 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 Schlüsselmateriale in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmateriale im ePA-Aktensystem ersetzen" mit den Eingangsparametern `NewAuthorizationKey` = geänderter `AuthorizationKey` ausführen. [ <= ]

**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.

#### 6.2.7.6.2 Berechtigung für LEI löschen

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

**A\_15415 - ePA-Frontend des Versicherten: LEI zum Entzug der Berechtigung markieren**

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

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

**A\_15416-01 - 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 46: TAB\_FdV\_139 – Berechtigung löschen**

Name	Berechtigung für LEI löschen
Auslöser	<ul style="list-style-type: none"> <li>Aufruf der Aktion zum Löschen der Berechtigung in der GUI</li> </ul>
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	<p>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 <code>AuthorizationKey</code> der LEI stehen zur Verfügung.</p>

Nachbedingung	Die LEI ist nicht mehr für den Zugriff auf das Aktenkonto autorisiert.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> <li>1. Policy Document in Dokumentenverwaltung löschen</li> <li>2. Schlüsselmaterial in ePA-Aktensystem löschen</li> </ol>

[&lt;=]

#### **A\_15417-02 - 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 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.[<=]

#### *6.2.7.6.3 Berechtigung für Vertreter löschen*

Mit diesem Anwendungsfall kann ein Versicherter einem berechtigten Vertreter die Berechtigung entziehen. Ferner soll es einem Vertreter auch möglich sein, sich seine eigene Berechtigung zu entziehen.

#### **A\_16044-01 - 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. Sofern der Nutzer ein Vertreter ist, darf er nur seine eigene Berechtigung auswählen.[<=]

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

#### **A\_16045-02 - 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 47: TAB\_FdV\_168 – Berechtigung für Vertreter löschen**

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

Akteur	Versicherter, Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat einen Vertreter zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt. Wenn der Nutzer ein Vertreter ist, darf er nur seine eigene Berechtigung ausgewählt haben. 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.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> <li>1. Policy Document in Dokumentenverwaltung löschen</li> <li>2. Schlüsselmaterial in ePA-Aktensystem löschen</li> </ol>

[&lt;=]

#### **A\_16046-02 - 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 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. [<=]

##### *6.2.7.6.4 Berechtigung für Kostenträger löschen*

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

#### **A\_17194 - ePA-Frontend des Versicherten: Kostenträger zum Entzug der Berechtigung markieren**

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

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

### A\_17195-01 - 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 48: TAB\_FdV\_166 – Berechtigung für Kostenträger löschen**

Name	Berechtigung für Kostenträger löschen
Auslöser	<ul style="list-style-type: none"> <li>Aufruf der Aktion zum Löschen der Berechtigung in der GUI</li> </ul>
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat einen Kostenträger zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt. Das Policy Document und Informationen zum AuthorizationKey des Kostenträgers stehen zur Verfügung.
Nachbedingung	Der Kostenträger ist nicht mehr für den Zugriff auf das Aktenkonto autorisiert.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> <li>Policy Document in Dokumentenverwaltung löschen</li> <li>Schlüsselmateriale in ePA-Aktensystem löschen</li> </ol>

[<=]

### A\_17196-02 - 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 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 - Schlüsselmateriale in ePA-Aktensystem löschen

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

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- 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\_20223-03 - ePA-Frontend des Versicherten: Zusätzliche Auswahl der Kategorie "Dokumente der eGA"**

Falls dem ePA-Frontend des Versicherten im kassenspezifischen Teil des FdV eGA-Daten bereitgestellt werden, MUSS das ePA-Frontend des Versicherten dem Nutzer ermöglichen, diese eGA-Dokumente anhand der Vorgaben aus A\_19388 in die ePA hochzuladen.[<=]

#### **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 49: TAB\_FdV\_146 – Dokumente einstellen**

Name	Dokumente einstellen
Auslöser	<ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>
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.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> <li>1. Prüfung auf zulässige Dateigröße</li> <li>2. Prüfung der Metadaten zu Dokumenten</li> <li>3. für jedes Dokument: <ol style="list-style-type: none"> <li>a. Dokument verschlüsseln</li> <li>b. Dokumentenschlüssel löschen</li> </ol> </li> <li>4. Dokumentenset in Dokumentenverwaltung hochladen</li> </ol>

**[<=]**

Das ePA-Aktensystem unterstützt nur Dokumente mit bestimmten MIME Types. Die initial zulässigen Typen sind in [gemSpec\_DM\_ePA#A\_] 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\_21483 - ePA-Frontend des Versicherten: Dokumente einstellen - Kein Einstellen von Ordern**

Das ePA-Frontend des Versicherten DARF im Anwendungsfall "Dokumente einstellen" KEINE neuen Ordner in die Dokumentenverwaltung einstellen.

[<=]

#### **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.

**Tabelle 50: TAB\_FdV\_147 – Dokumente einstellen - Dokument verschlüsseln**

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

[<=]

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. [ <= ]

**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 (\$XDSSubmissionSetAuthorPerson, \$XDSDocumentEntryAuthorPerson, \$XDSDocumentEntryAuthorInstitution siehe [\[gemSpec\\_Dokumentenverwaltung#A\\_18070\]](#) und A\_17854)
- Suche nach in einem Zeitraum erstellten bzw. eingestellten Dokumenten (\$XDSDocumentEntryCreationTimeFrom/To / \$XDSSubmissionSetSubmissionTimeFrom/To)
- Suche nach Dokumententitel (siehe [\[gemSpec\\_Dokumentenverwaltung#A\\_17185\]](#) und A\_17854)
- Suche nach durch LEIs bereitgestellte Dokumente
- Suche nach Dokumenten mit Kennzeichnung "Versicherteninformation"(siehe [\[gemSpec\\_DM\\_ePA#A\\_14986\]](#))
- Suche nach durch Krankenkassen bereitgestellte Informationen
- Suche nach Dokumenten im DocumentEntry.availabilityStatus "Deprecated" oder "Approved"



**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 51: TAB\_FdV\_148 – Dokumente suchen**

Name	Dokumente suchen
Auslöser	<ul style="list-style-type: none"> <li>Auswahl der Aktion zur Suche von Dokumenten in der GUI</li> </ul>
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

[&lt;=]

**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.

[&lt;=]

**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.

**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 52: TAB\_FdV\_149 – Dokumente aus Aktenkonto herunterladen**

Name	Dokumente herunterladen
Auslöser	<ul style="list-style-type: none"> <li>Auswahl der Aktion zum Herunterladen, Anzeigen oder lokalen Speichern für markierte Dokumente in einer Suchanfrage in der GUI</li> </ul>
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	<p>Es besteht eine Aktensession mit gültigen Session-Daten.</p> <p>Es wurde eine Suchanfrage nach Dokumenten in der Dokumentenverwaltung durchgeführt.</p> <p>Die Dokumente sind im Ergebnis einer Suchanfrage selektiert.</p> <p>Die Identifier der Dokumente (uniqueId) sind aus den Metadaten der Suchanfrage bekannt.</p>
Nachbedingung	Die Dokumente liegen unverschlüsselt temporär in einem Speicher im Gerät des Versicherten vor.
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> <li>markierte Dokumente herunterladen und entschlüsseln</li> </ol>

[ &lt;= ]

**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. [ <= ]

**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 abubrechen. [ <= ]

**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 53: TAB\_FdV\_150 – Dokumente löschen**

Name	Dokumente löschen
Auslöser	<ul style="list-style-type: none"> <li>Auswahl der Aktion Löschen für zum Löschen markierte Dokument in einer Suchanfrage in der GUI</li> </ul>
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	<p>Es besteht eine Aktensession mit gültigen Session-Daten.          Es wurde eine Suchanfrage nach Dokumenten in der Dokumentenverwaltung durchgeführt.          Die zu löschenden Dokumente sind im Ergebnis einer Suchanfrage selektiert.          Die Identifier für die Dokumente sind aus den Metadaten der Suchanfrage bekannt.          Der Nutzer hat das Löschen bestätigt.</p>
Nachbedingung	Die Dokumente sind im Aktenkonto unwiederbringlich gelöscht.
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> <li>1. Dokumentenset in Dokumentenverwaltung löschen</li> </ol>

[ &lt;= ]

**A\_15483-03 - 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 RemoveMetadata\_Message für alle über die XDS-Metadaten ermittelten Dokument Identifier (entryUUIDs) der ausgewählten Dokumente ausführen. [≤]

**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 54: TAB\_FdV\_151 – Protokolldaten einsehen**

Name	Protokolldaten einsehen
Auslöser	<ul style="list-style-type: none"> <li>Auswahl der Aktion zum Anzeigen der Protokolldaten in der GUI</li> </ul>
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Die Protokolldaten können dem Nutzer angezeigt werden.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> <li>1. Protokolldaten Dokumentenverwaltung abfragen</li> <li>2. Protokolldaten Autorisierung abfragen</li> <li>3. Protokolldaten Authentisierung abfragen</li> </ol>

[&lt;=]

**A\_15486-01 - ePA-Frontend des Versicherten: Protokoll einsehen - Dokumentenverwaltung abfragen**

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Protokolldaten einsehen" die Aktivität "Protokolldaten Dokumentenverwaltung abfragen" gemäß TAB\_FdV\_152 umsetzen.

**Tabelle 55: TAB\_FdV\_152 – Protokolldaten einsehen - Dokumentenverwaltung abfragen**

I_Account_Management_Insurant::GetAuditEvents Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> <li>AuthenticationAssertion aus Session-Daten</li> </ul>
I_Account_Management_Insurant::GetAuditEvents Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> <li>Audit Event List</li> </ul>

[&lt;=]

**A\_22331 - ePA-Frontend des Versicherten: Protokoll einsehen - mehrere ParticipantObjectIdentification-Tags innerhalb einer AuditMessage**

Das ePA-Frontend des Versicherten MUSS zusammengefasste Protokolleinträge mit mehreren ParticipantObjectIdentification-Elementen innerhalb einer AuditMessage verarbeiten und zur Anzeige bringen können.[<=]

**A\_15487-01 - ePA-Frontend des Versicherten: Protokoll einsehen -  
Autorisierung abfragen**

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Protokolldaten einsehen" die Aktivität "Protokolldaten Autorisierung abfragen" gemäß TAB\_FdV\_153 umsetzen.

**Tabelle 56: TAB\_FdV\_153 – Protokolldaten einsehen - Autorisierung abfragen**

I_Authorization_Management_Insurant::getAuditEvents Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> <li>• AuthenticationAssertion aus Session-Daten</li> <li>• RecordIdentifier aus Session-Daten</li> <li>• DeviceID aus Gerät-Daten</li> </ul>
I_Authorization_Management_Insurant::getAuditEvents Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> <li>• AuditMessage[0..*]</li> </ul>

[<=]

**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 57: TAB\_FdV\_154 – Protokolldaten einsehen - Zugangsgateway des Versicherten abfragen**

I_Authentication_Insurant::getAuditEvents Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> <li>• AuthenticationAssertion aus Session-Daten</li> </ul>
I_Authentication_Insurant::getAuditEvents Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> <li>• AuditMessage[0..*]</li> </ul>
Varianten/Alternativen	Wenn in der Abarbeitung der Operation ein Fehler auftritt und kein Resultset vorliegt, kann der Anwendungsfall fortgesetzt werden, denn dieses Resultset ist nicht Teil der Standard-Anzeige. Der Nutzer ist darauf hinzuweisen, dass keine Protokolleinträge zur Authentisierung abgerufen werden konnten.

[<=]

Die Ergebnisse der Abfragen an die Komponenten des ePA-Aktensystems werden vereint.

Die Information eines Protokolleintrages sind in [\[gemSpec DM ePA#A\\_14471 - Objektstruktur Eintrag für Protokoll\]](#) beschrieben.

**Tabelle 58: TAB\_FdV\_155 – Felder im Protokolleintrag**

Protokolldatum	Bezeichnung in GUI	Hinweis zur Anzeige	optional in Standard-Anzeige
Aufgerufene Operation	Art des Zugriffs auf das Aktenkonto	DisplayName anzeigen	
Datum und Uhrzeit des Zugriffs	Zeitpunkt des Zugriffs		
Ergebnis der aufgerufenen Operation	Ergebnis Zugriff	0 - erfolgreich 1 - nicht erfolgreich	
UserID	Identifiziert des Nutzers		x
UserName	Name des Nutzers		
ObjectID	Identifiziert des Objektes, auf das zugegriffen wurde		x
ObjectName	Bezeichner des Objektes, auf das zugegriffen wurde		
ObjectDetail	Details zum zugegriffenen Objekt		
DeviceID	Geräteerkennung		x
Home-CommunityID des ePA-Aktensystems	ID des Aktenanbieters		x
Name des Aktenanbieters	Name des Aktenanbieters		x

#### **A\_21312 - ePA-Frontend des Versicherten: Suchparameter beim Protokollabruf**

Das ePA-Frontend des Versicherten SOLL beim Abruf von Protokolldaten von den Komponenten ePA-Dokumentenverwaltung, Authentisierung und Autorisierung Parameter für den seitenweisen Abruf gemäß [\[gemSpecAktensystem#A\\_21303\]](#) verwenden.  
[<=]

## **A\_15489-05 - 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:

- 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 Ordern aus der ärztlichen Umgebung)
- PHR-610 (Hinzufügen eines Dokuments aus der privaten Umgebung)
- PHR-620 (Suchanfrage aus der privaten Umgebung)
- PHR-630 (Löschen eines Dokuments aus der privaten Umgebung)
- PHR-640 (Abruf eines Dokuments aus der privaten Umgebung)
- PHR-680 (Löschen von Dokumenten, Ordern 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-870 (Erfolgreicher Abschluss des Umschlüsselungsvorgangs durch den Versicherten)
- PHR-860 (Abbruch des Umschlüsselungsvorgangs)

[<=]

## **A\_15490 - ePA-Frontend des Versicherten: Erweiterte-Anzeige für Protokolldaten**

Das ePA-Frontend des Versicherten MUSS eine Erweiterte-Anzeige für die Protokolldaten umsetzen, in der alle Protokolleinträge der vom ePA-Aktensystem erstellten Protokolle (§ 291a-konformes Zugriffsprotokoll und Verwaltungsprotokolle der Komponenten) übersichtlich dargestellt werden. [<=]

Das FdV kann in der Standard-Anzeige die gemäß TAB\_FdV\_155 optionalen Felder verbergen. Der Nutzer muss dann die Möglichkeit haben, sich die verborgenen Felder anzeigen zu lassen.

## **A\_15491-01 - ePA-Frontend des Versicherten: Felder Protokolldaten**

Das ePA-Frontend des Versicherten MUSS es dem Nutzer in der Standard-Anzeige und in der Erweiterte-Anzeige für die Protokolldaten ermöglichen, alle Felder aus TAB\_FdV\_155 darzustellen. [<=]

Das 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 59: TAB\_FdV\_156 – PIN der eGK ändern**

Name	PIN der eGK ändern
Auslöser	<ul style="list-style-type: none"> <li>Auswahl des Anwendungsfalls in der GUI</li> </ul>
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Die eGK des Nutzers ist im Kartenleser gesteckt.
Nachbedingung	PIN wurde geändert
Standardablauf	<p>Die Umsetzung ist in TAB_FdV_157 beschrieben</p> <ol style="list-style-type: none"> <li>PL_TUC_CARD_CHANGE_PIN nutzen</li> <li>PL_TUC_CARD_CHANGE_PIN Ergebnis verarbeiten</li> <li>Ergebnis anzeigen</li> </ol>

**Tabelle 60: TAB\_FdV\_157 – Ablaufaktivitäten – PIN der eGK ändern**

<b>1. PL_TUC_CARD_CHANGE_PIN nutzen</b>	
Plattformoperation	PL_TUC_CARD_CHANGE_PIN

<i>Eingangsdaten</i>	
Identifikator	MRPIN.home
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	Alte PIN: "Eingabe alte PIN: " bzw. Neue PIN: "Eingabe neue PIN: "
<i>Beschreibung</i>	Der Plattformbaustein wird zur Änderung den PIN genutzt.
<b>2. Rückgabewert von PL_TUC_CARD_CHANGE_PIN verarbeiten</b>	
<i>Rückgabedaten</i>	
OK	PIN erfolgreich geändert
Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_CHANGE_PIN
<i>Beschreibung</i>	<p>Das Ändern einer PIN auf der eGK basiert auf der parametrisierten Plattformbaustein PL_TUC_CARD_CHANGE_PIN. Diese liefert ein <i>Ergebnis</i> zurück. Zur Änderung muss zwingend die Eingabe der alten PIN erfolgen.</p> <p>Wird durch den Versicherten ein falsches altes PIN-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PINs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung entsprechenden Details zurückgegeben.</p>
<b>3. Ergebnis anzeigen</b>	

<p><i>Hinweis an den Versicherten</i></p>	<p>Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.</p> <p>Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt. Bei einer Fehleingabe der PIN des Versicherten wird dem Versicherten die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet.</p>
---	---

[<=]

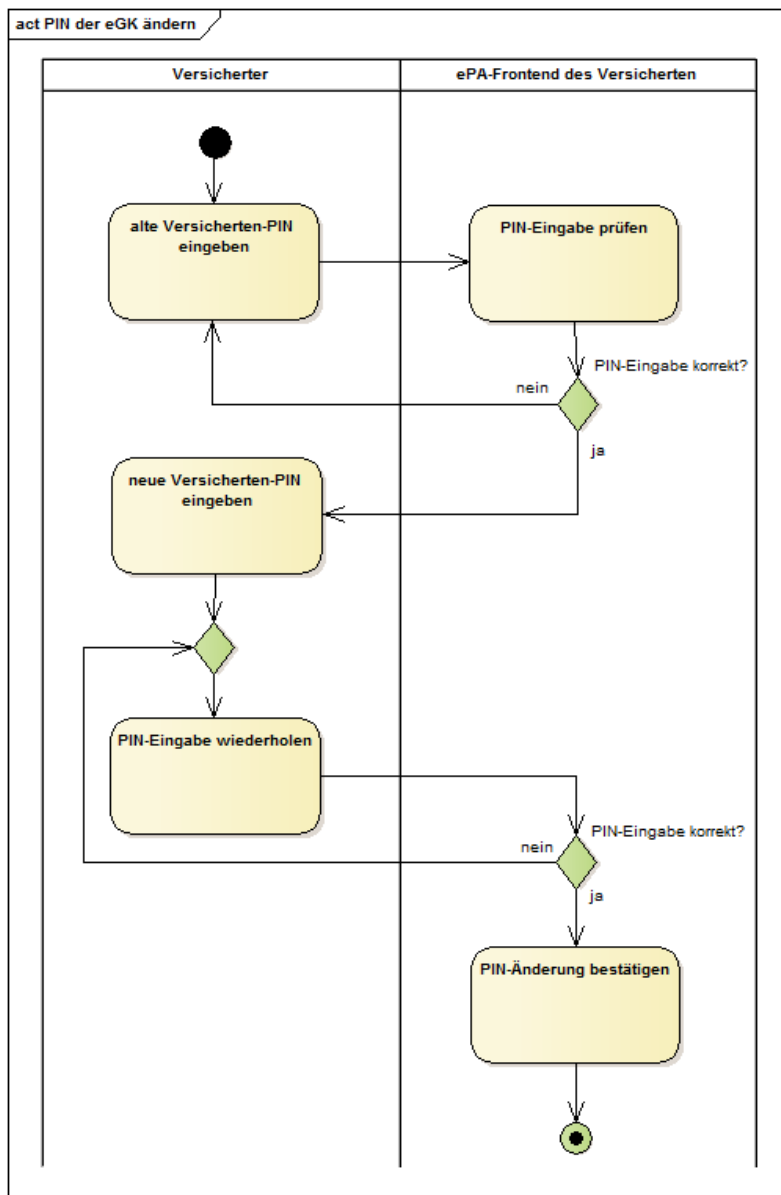


Abbildung 10: Aktivitätsdiagramm "PIN der eGK ändern"

### 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.

**Tabelle 61: TAB\_FdV\_158 – PIN der eGK entsperren**

Name	PIN der eGK entsperren
Auslöser	<ul style="list-style-type: none"> <li>Auswahl des Anwendungsfalls in der GUI</li> </ul>
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Die eGK des Nutzers ist im Kartenleser gesteckt. Die PIN der eGK (MRPIN.home) ist gesperrt.
Nachbedingung	PIN des Versicherten wurde entsperrt.
Standardablauf	Die Umsetzung ist in TAB_FdV_159 beschrieben <ol style="list-style-type: none"> <li>1. PL_TUC_CARD_UNBLOCK_PIN nutzen</li> <li>2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten</li> <li>3. Ergebnis anzeigen</li> </ol>

**Tabelle 62: TAB\_FdV\_159 – Ablaufaktivitäten – PIN der eGK entsperren**

<b>1. PL_TUC_CARD_UNBLOCK_PIN aufrufen</b>	
Plattformbaustein	PL_TUC_CARD_UNBLOCK_PIN
<i>Eingangsdaten</i>	
Identifikator	MRPIN.home
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	PUK: "Eingabe PUK: " bzw. Neue PIN: "Eingabe neue PIN: "
Beschreibung	Für das Entsperren der PIN wird ein Plattformbaustein genutzt.
<b>2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten</b>	
<i>Rückgabedaten</i>	

OK	PIN wurde entsperrt.
PasswordBlocked	Die PUK wurde wegen zu häufiger Nutzung gesperrt. Der Versicherte muss darüber in verständlicher Form informiert und auf die Notwendigkeit einer neuen eGK hingewiesen werden.
Weitere Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_UNBLOCK_PIN
<i>Beschreibung</i>	Das Entsperren einer PIN auf der eGK basiert auf dem parametrisierten Plattformbaustein PL_TUC_CARD_UNBLOCK_PIN. Zum Entsperren muss zwingend die Eingabe einer PUK erfolgen.  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.
<b>3. Ergebnis anzeigen</b>	
<i>Hinweis an den Versicherten</i>	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.

[&lt;=]

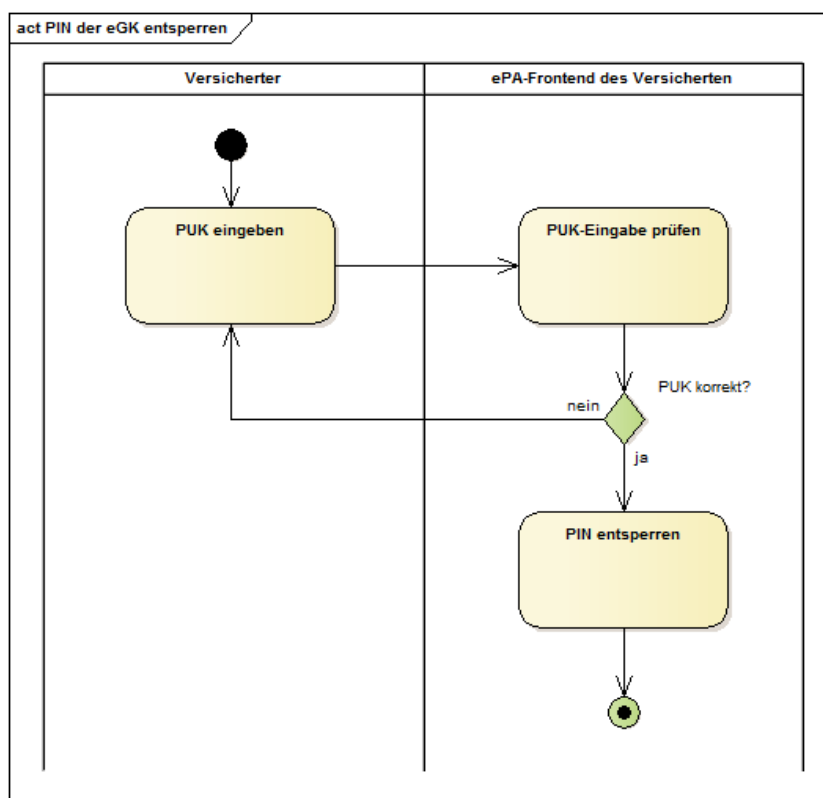


Abbildung 11: Aktivitätsdiagramm "PIN der eGK entsperren"

## 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.

**Tabelle 63: TAB\_FdV\_160 – Benachrichtigungsadresse aktualisieren**

I_Authorization_Management_Insurant:: putNotificationInfo Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> <li>• AuthenticationAssertion aus Session-Daten</li> <li>• RecordIdentifizier aus Session-Daten</li> <li>• DeviceID aus Gerät-Daten</li> <li>• NewNotificationInfo = vom Nutzer eingegebene Benachrichtigungsadresse</li> </ul>
I_Authorization_Management_Insurant:: putNotificationInfo Response verarbeiten	Http OK ohne SOAP-Response oder gematik Fehlermeldung

[&lt;=]

### 6.2.11.2 Benachrichtigungsadressen abfragen

Bei der Einrichtung eines Vertreters wird dessen Benachrichtigungsadresse im AS hinterlegt. Die Schnittstelle `GetNotificationInfo` wird durch den Versicherten dafür genutzt, diese Benachrichtigungsadresse vom AS abfragen zu können, insbesondere im Rahmen des Aktenwechsels oder zur Prüfung, ob eine Korrektur der Benachrichtigungsadresse des Vertreters erforderlich ist.

#### A\_21254-02 - ePA-Frontend des Versicherten: Benachrichtigungsadresse abfragen

Das ePA-Frontend des Versicherten MUSS das Abfragen einer Benachrichtigungsadresse im ePA-Aktensystem gemäß TAB\_FdV\_161 Benachrichtigungsadresse abfragen umsetzen

I_Authorization_Management_Insurant:: getNotificationInfo Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> <li>• AuthenticationAssertion aus Session-Daten</li> <li>• RecordIdentifizier aus Session-Daten</li> <li>• DeviceID aus Gerät-Daten</li> <li>• ActorID des Nutzers, dessen Benachrichtigungskanal zu ermitteln ist. Bei fehlender ActorID wird eine Liste aller Benachrichtigungskanäle zurück gegeben.</li> </ul>
I_Authorization_Management_Insurant:: getNotificationInfo Response verarbeiten	NotificationInfoList = Liste der abgefragten Benachrichtigungskanäle (ActorID, Benachrichtigungsadresse) oder gematik Fehlermeldung



[&lt;=]

## 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 64: TAB\_FdV\_177 – Verwendete Plattformleistungen**

Kürzel	Bezeichnung
PL_TUC_CARD_CHANGE_PIN	PIN ändern
PL_TUC_CARD_INFORMATION	Gesammelte Statusinformationen zu einer Karte
PL_TUC_CARD_UNBLOCK_PIN	PIN mit PUK entsperren
PL_TUC_CARD_VERIFY_PIN	Benutzer verifizieren
PL_TUC_GET_CHALLENGE	Auslesen einer Zufallszahl
PL_TUC_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 können Kartenterminalvarianten der Sicherheitsklassen 1 (reine Kontaktiereinheit) zum Einsatz kommen. Es sollen bevorzugt Kartenterminalvarianten der Sicherheitsklassen 2 (Kartenterminal mit eigenem PIN-Pad) oder 3 (PIN-Pad plus Display) verwendet 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\_21828 - ePA-FdV für Desktop-Plattformen: Unterstützung von Kartenlesern ab Sicherheitsklasse 2**

Das ePA-Frontend des Versicherten für Desktop-Plattformen MUSS es dem Nutzer ermöglichen, das ePA-Frontend des Versicherten mit einem Kartenleser einer höheren Sicherheitsklasse als Sicherheitsklasse 1 (Sicherheitsklasse 2 oder höher) zu nutzen [ <= ]

#### **A\_15503 - ePA-Frontend des Versicherten: PIN-Eingabe nicht speichern**

Das ePA-Frontend des Versicherten DARF ein eingegebenes PIN-Geheimnis NICHT temporär und NICHT persistent speichern. [ <= ]

#### **A\_15504-01 - 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\_21829 - ePA-FdV für Desktop-Plattformen: Hinweis bei Kartenlesern der Sicherheitsklasse 1**

Falls das ePA-Frontend des Versicherten für Desktop-Plattformen mit einem Kartenleser der Sicherheitsklasse 1 genutzt wird, MUSS das ePA-Frontend des Versicherten für Desktop-Plattformen den Nutzer in einer für den Nutzer verständlichen Form darauf hinzuweisen,

- dass Kartenleser der Sicherheitsklasse 1 geringere Sicherheitsleistungen als Kartenleser der Sicherheitsklassen 2 oder 3 erbringen und welche handelsüblichen Kartenleser der Sicherheitsklassen 2 und 3 vom Nutzer am ePA-Frontend des Versicherten für Desktop-Plattformen genutzt werden könnten,
- welche Risiken bei einer Nutzung von Kartenlesern der Sicherheitsklasse 1 für den Nutzer bestehen und welche Maßnahmen der Versicherte auf seinem Gerät treffen sollte, um diese Risiken zu verringern.

Das ePA-Frontend des Versicherten für Desktop-Plattformen MUSS es dem Nutzer ermöglichen, auf die Anzeige des Hinweises bei einer zukünftigen Nutzung des Kartenlesers der Sicherheitsklasse 1 zu verzichten, sofern der Nutzer dies explizit bestätigt und die Bestätigung so gestaltet ist, das eine versehentliche Bestätigung vermieden wird.

[<=]

#### **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.

#### **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. [ <= ]

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

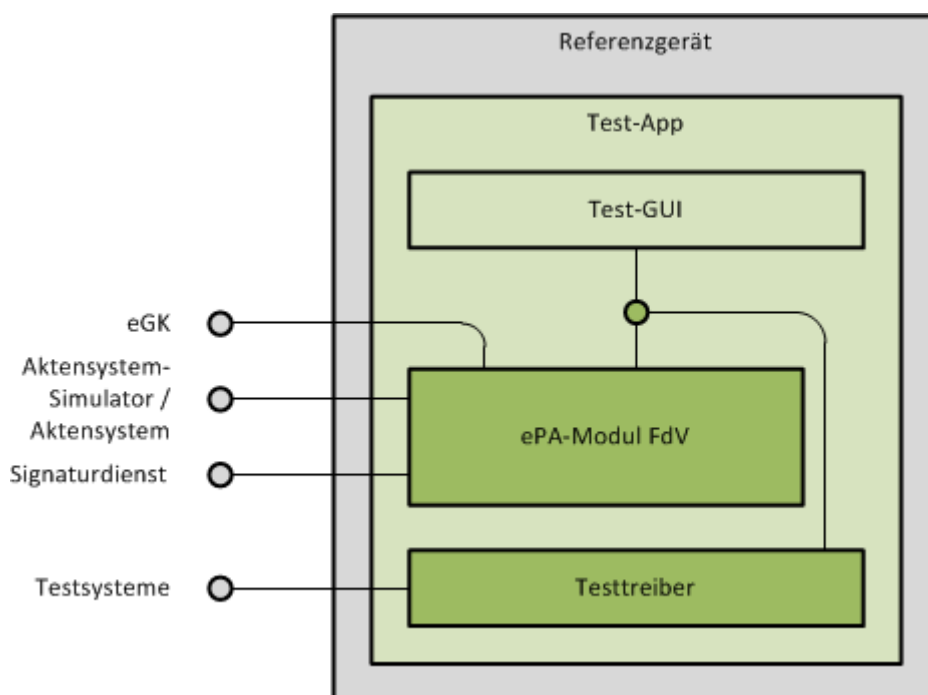
und die Antwortnachricht der Karte als `responseApdu` an den Aufrufer zur Auswertung zurückgegeben wird. [ <= ]

**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 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 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.

Die konkrete Ausgestaltung der Schnittstellen [gemTestTreiberFdV] ist im Fachportal der gematik und in GitHub verfügbar.,



## 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

		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

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	

Versicherten-ID des Nutzers	Authentisierungszertifikat des Nutzers	
Benachrichtigungskanal für Geräteverwaltung (E-Mail)		durch den Nutzer während des Eröffnens des Aktenkontos angegeben.

## Berechtigungen:

Datenfeld	Herkunft	Beschreibung
Name des Berechtigten	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 gültig bis	Policy Document	LEI, KTR, Vertreter
Berechtigung für LEI	PolicyDocument mit "urn:gematik:policy:2.0:<record-id>:lei:<telematik-id>"	LEI
Berechtigung für KTR	Policy Document mit "urn:gematik:policy:2.0:<record-id>:ktr:<telematik-id>"	KTR
Berechtigung für Vertreter	Policy Document mit "urn:gematik:policy:2.0:<record-id>:rep:<kvnr>"	Vertreter

---

## 8 Verteilungssicht

---

Eine Darstellung der hardwareseitigen Verteilung des Produkttyps bzw. seiner Teilsysteme und der Einbettung in die physikalische Umgebung wird nicht benötigt.

---

## 9 Anhang A – Verzeichnisse

---

### 9.1 Abkürzungen

Kürzel	Erläuterung
DSMLv2	Directory Services Markup Language v2.0
eGK	Elektronische Gesundheitskarte
ePA	Elektronische Patientenakte
FdV	ePA-Frontend des Versicherten
FQDN	Fully-Qualified Domain Name
GdV	Gerät des Versicherten
IHE	Integrating the Healthcare Enterprise
KTR	Kostenträger, d.h. die gesetzlichen Krankenkassen
KVNR	Krankenversichertennummer
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
MTOM	Message Transmission Optimization Mechanism
NFC	Near Field Communication
OWASP	Open Web Application Security Project
PDF	Portable Document Format
PIN	Personal Identification Number
PUK	Personal Unblocking Key
SGD	Schlüsselgenerierungsdienst
SOAP	Simple Object Access Protocol

TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust-service Status List
VZD	Verzeichnisdienst der TI

## 9.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
Patienteninformation	Ist ein durch eine Leistungserbringerinstitution im Aktenkonto bereitgestelltes Dokument, welches vorrangig der Information von Versicherten dient. Das Dokument wird durch den Leistungserbringer als Versicherteninformation gekennzeichnet.
Policy Document	Das Policy Document ist ein technisches Dokument. Es enthält die Zugriffsregeln eines Berechtigten im Aktenkonto des Versicherten in der Komponente "Dokumentenverwaltung". Berechtigte der Aktenkontoinhaber, Vertreter oder LEIs.
Versicherten-ID	Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen 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

Abbildung 1: Systemüberblick FdV.....	13
Abbildung 2: Komponenten ePA-Frontend des Versicherten .....	16
Abbildung 3: Kryptographische Schlüssel der ePA .....	57
Abbildung 4: Aktivitätsdiagramm "Login-Aktensession" .....	90
Abbildung 5: Aktivitätsdiagramm "Anbieter wechseln" .....	102

Abbildung 6: Umschlüsselung I .....	105
Abbildung 7: Umschlüsselung II .....	106
Abbildung 8: Umschlüsselung III .....	106
Abbildung 9: Umschlüsselung IV .....	107
Abbildung 10: Aktivitätsdiagramm "PIN der eGK ändern" .....	148
Abbildung 11: Aktivitätsdiagramm "PIN der eGK entsperren" .....	151
Abbildung 12: Test-App mit ePA-Frontend des Versicherten und Testtreiber .....	159
Abbildung 1: Systemüberblick FdV .....	13
Abbildung 2: Komponenten ePA-Frontend des Versicherten .....	16
Abbildung 3: Kryptographische Schlüssel der ePA .....	57
Abbildung 4: Aktivitätsdiagramm "Login Aktensession" .....	90
Abbildung 5: Aktivitätsdiagramm "Anbieter wechseln" .....	102
Abbildung 6: Umschlüsselung I .....	105
Abbildung 7: Umschlüsselung II .....	106
Abbildung 8: Umschlüsselung III .....	106
Abbildung 9: Umschlüsselung IV .....	107
Abbildung 10: Aktivitätsdiagramm "PIN der eGK ändern" .....	148
Abbildung 11: Aktivitätsdiagramm "PIN der eGK entsperren" .....	151
Abbildung 12: Test-App mit ePA-Frontend des Versicherten und Testtreiber .....	159

## 9.4 Tabellenverzeichnis

Tabelle 1: TAB_FdV_101 — Akteure und Rollen .....	12
Tabelle 2: TAB_FdV_102 — Schnittstellen des ePA-Aktensystems .....	13
Tabelle 3: TAB_FdV_167 — Komponenten des FdV .....	16
Tabelle 4: TAB_FdV_103 — IHE Akteure und Transaktionen .....	33
Tabelle 5: TAB_FdV_104 — Parameter FdV .....	42
Tabelle 6: TAB_FdV_105 — Session-Daten .....	48
Tabelle 7: TAB_FdV_106 — DNS-RR ePA-Aktensystem-Komponenten .....	49
Tabelle 8: TAB_FdV_110 — Zertifikatsnutzung .....	52
Tabelle 9: TAB_FdV_161 — Zulässigkeit von Anwendungsfällen .....	59
Tabelle 10: TAB_FdV_107 — Behandlung von Fehlercodes von Plattformbausteinen .....	61
Tabelle 11: TAB_FdV_108 — Behandlung von Fehlern des ePA-Aktensystems .....	62
Tabelle 12: TAB_FdV_109 — Authentisieren des Nutzers .....	63
Tabelle 13: TAB_FdV_173 — Logout — Authentisierungstoken abmelden .....	65

Tabelle 14: TAB_FdV_111	Dokumentenset in Dokumentenverwaltung hochladen	66
Tabelle 15: TAB_FdV_112	Dokumentenset aus Dokumentenverwaltung herunterladen	68
Tabelle 16: TAB_FdV_113	Dokumentenset in Dokumentenverwaltung löschen	70
Tabelle 17: TAB_FdV_114	Suche nach Dokumenten in Dokumentenverwaltung	70
Tabelle 18: TAB_FdV_115	Vergebene Berechtigungen bestimmen	71
Tabelle 19: TAB_FdV_179	Akten und Kontextschlüssel verschlüsseln	76
Tabelle 20: TAB_FdV_180	Akten und Kontextschlüssel entschlüsseln	77
Tabelle 21: TAB_FdV_116	Schlüsselmaterial aus ePA Aktensystem laden	78
Tabelle 22: TAB_FdV_163	Schlüsselmaterial aller Berechtigten aus ePA Aktensystem laden	79
Tabelle 23: TAB_FdV_117	Schlüsselmaterial im ePA Aktensystem speichern	80
Tabelle 24: TAB_FdV_118	Schlüsselmaterial im ePA Aktensystem ersetzen	81
Tabelle 25: TAB_FdV_119	Schlüsselmaterial im ePA Aktensystem löschen	81
Tabelle 26: TAB_FdV_120	Suchkriterien LDAP Search	82
Tabelle 27: TAB_FdV_121	Abfrage Verzeichnisdienst	84
Tabelle 28: TAB_FdV_122	PIN-Eingabe durch Nutzer	85
Tabelle 29: TAB_FdV_123	Login Aktensession	86
Tabelle 30: TAB_FdV_124	Login Einlesen der Karte	90
Tabelle 31: TAB_FdV_126	Login Aktenkontext öffnen Operation OpenContext	92
Tabelle 32: TAB_FdV_127	Logout Aktensession	94
Tabelle 33: TAB_FdV_128	Logout Aktenkontext schließen	94
Tabelle 34: TAB_FdV_172	Logout Authentisierungstoken abmelden	95
Tabelle 35: TAB_FdV_130	Aktenkonto aktivieren	96
Tabelle 36: TAB_FdV_131	Anbieter wechseln	98
Tabelle 37: TAB_FdV_132	Anbieter wechseln Aktenkonto in Exportzustand versetzen	102
Tabelle 38: TAB_FdV_133	Anbieter wechseln Aktenkonto fortführen	104
Tabelle 39: TAB_FdV_134	Berechtigung an LEI für Aktenkonto vergeben	112
Tabelle 40: TAB_FdV_178	Anzeige der auf ein Dokument berechtigten LEI	113
Tabelle 41: TAB_FdV_179	Ändern der Vertraulichkeitsstufe eines Dokumentes	113
Tabelle 42: TAB_FdV_135	Vertretung einrichten	122
Tabelle 43: TAB_FdV_171	Berechtigung an Kostenträger für Aktenkonto vergeben	124
Tabelle 44: TAB_FdV_137	Vergebene Berechtigungen anzeigen	126
Tabelle 45: TAB_FdV_138	Berechtigung für LEI ändern	128
Tabelle 46: TAB_FdV_139	Berechtigung löschen	129
Tabelle 47: TAB_FdV_168	Berechtigung für Vertreter löschen	130



Tabelle 48: TAB_FdV_166 – Berechtigung für Kostenträger löschen .....	132
Tabelle 49: TAB_FdV_146 – Dokumente einstellen .....	134
Tabelle 50: TAB_FdV_147 – Dokumente einstellen – Dokument verschlüsseln .....	135
Tabelle 51: TAB_FdV_148 – Dokumente suchen .....	137
Tabelle 52: TAB_FdV_149 – Dokumente aus Aktenkonto herunterladen .....	138
Tabelle 53: TAB_FdV_150 – Dokumente löschen .....	139
Tabelle 54: TAB_FdV_151 – Protokolldaten einsehen .....	141
Tabelle 55: TAB_FdV_152 – Protokolldaten einsehen – Dokumentenverwaltung abfragen .....	141
Tabelle 56: TAB_FdV_153 – Protokolldaten einsehen – Autorisierung abfragen .....	142
Tabelle 57: TAB_FdV_154 – Protokolldaten einsehen – Zugangsgateway des Versicherten abfragen .....	142
Tabelle 58: TAB_FdV_155 – Felder im Protokolleintrag .....	143
Tabelle 59: TAB_FdV_156 – PIN der eGK ändern .....	145
Tabelle 60: TAB_FdV_157 – Ablaufaktivitäten – PIN der eGK ändern .....	145
Tabelle 61: TAB_FdV_158 – PIN der eGK entsperren .....	149
Tabelle 62: TAB_FdV_159 – Ablaufaktivitäten – PIN der eGK entsperren .....	149
Tabelle 63: TAB_FdV_160 – Benachrichtigungsadresse aktualisieren .....	152
Tabelle 64: TAB_FdV_177 – Verwendete Plattformleistungen .....	153
Tabelle 1: TAB_FdV_101 – Akteure und Rollen .....	12
Tabelle 2: TAB_FdV_102 – Schnittstellen des ePA-Aktensystems .....	13
Tabelle 3: TAB_FdV_167 – Komponenten des FdV .....	16
Tabelle 4: TAB_FdV_103 – IHE Akteure und Transaktionen .....	33
Tabelle 5: TAB_FdV_104 – Parameter FdV .....	42
Tabelle 6: TAB_FdV_105 – Session-Daten .....	48
Tabelle 7: TAB_FdV_106 – DNS RR ePA-Aktensystem Komponenten .....	49
Tabelle 8: TAB_FdV_110 – Zertifikatsnutzung .....	52
Tabelle 9: TAB_FdV_161 – Zulässigkeit von Anwendungsfällen .....	59
Tabelle 10: TAB_FdV_107 – Behandlung von Fehlercodes von Plattformbausteinen .....	61
Tabelle 11: TAB_FdV_108 – Behandlung von Fehlern des ePA-Aktensystems .....	62
Tabelle 12: TAB_FdV_109 – Authentisieren des Nutzers .....	63
Tabelle 13: TAB_FdV_173 – Logout - Authentisierungstoken abmelden .....	65
Tabelle 14: TAB_FdV_111 – Dokumentenset in Dokumentenverwaltung hochladen .....	66
Tabelle 15: TAB_FdV_112 – Dokumentenset aus Dokumentenverwaltung herunterladen .....	68
Tabelle 16: TAB_FdV_113 – Dokumentenset in Dokumentenverwaltung löschen .....	70
Tabelle 17: TAB_FdV_114 – Suche nach Dokumenten in Dokumentenverwaltung .....	70

Tabelle 18: TAB_FdV_115 – Vergebene Berechtigungen bestimmen.....	71
Tabelle 19: TAB_FdV_179 – Akten- und Kontextschlüssel verschlüsseln .....	76
Tabelle 20: TAB_FdV_180 – Akten- und Kontextschlüssel entschlüsseln .....	77
Tabelle 21: TAB_FdV_116 – Schlüsselmaterial aus ePA-Aktensystem laden .....	78
Tabelle 22: TAB_FdV_163 – Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden .....	79
Tabelle 23: TAB_FdV_117 – Schlüsselmaterial im ePA-Aktensystem speichern .....	80
Tabelle 24: TAB_FdV_118 – Schlüsselmaterial im ePA-Aktensystem ersetzen.....	81
Tabelle 25: TAB_FdV_119 – Schlüsselmaterial im ePA-Aktensystem löschen .....	81
Tabelle 26: TAB_FdV_120 – Suchkriterien LDAP Search .....	82
Tabelle 27: TAB_FdV_121 – Abfrage Verzeichnisdienst.....	84
Tabelle 28: TAB_FdV_122 – PIN-Eingabe durch Nutzer.....	85
Tabelle 29: TAB_FdV_123 – Login Aktensession .....	86
Tabelle 30: TAB_FdV_124 – Login - Einlesen der Karte.....	90
Tabelle 31: TAB_FdV_126 – Login - Aktenkontext öffnen - Operation OpenContext.....	92
Tabelle 32: TAB_FdV_127 – Logout Aktensession .....	94
Tabelle 33: TAB_FdV_128 – Logout - Aktenkontext schließen.....	94
Tabelle 34: TAB_FdV_172 – Logout - Authentisierungstoken abmelden .....	95
Tabelle 35: TAB_FdV_130 – Aktenkonto aktivieren .....	96
Tabelle 36: TAB_FdV_131 – Anbieter wechseln .....	98
Tabelle 37: TAB_FdV_132 – Anbieter wechseln - Aktenkonto in Exportzustand versetzen .....	102
Tabelle 38: TAB_FdV_133 – Anbieter wechseln - Aktenkonto fortführen .....	104
Tabelle 39: TAB_FdV_134 – Berechtigung an LEI für Aktenkonto vergeben.....	112
Tabelle 40: TAB_FdV_178 Anzeige der auf ein Dokument berechtigten LEI .....	113
Tabelle 41: TAB_FdV_179: Ändern der Vertraulichkeitsstufe eines Dokumentes .....	113
Tabelle 42: TAB_FdV_135 – Vertretung einrichten .....	122
Tabelle 43: TAB_FdV_171 – Berechtigung an Kostenträger für Aktenkonto vergeben ..	124
Tabelle 44: TAB_FdV_137 – Vergebene Berechtigungen anzeigen.....	126
Tabelle 45: TAB_FdV_138 – Berechtigung für LEI ändern .....	128
Tabelle 46: TAB_FdV_139 – Berechtigung löschen .....	129
Tabelle 47: TAB_FdV_168 – Berechtigung für Vertreter löschen .....	130
Tabelle 48: TAB_FdV_166 – Berechtigung für Kostenträger löschen .....	132
Tabelle 49: TAB_FdV_146 – Dokumente einstellen .....	134
Tabelle 50: TAB_FdV_147 – Dokumente einstellen - Dokument verschlüsseln .....	135
Tabelle 51: TAB_FdV_148 – Dokumente suchen .....	137
Tabelle 52: TAB_FdV_149 – Dokumente aus Aktenkonto herunterladen .....	138

Tabelle 53: TAB_FdV_150 – Dokumente löschen .....	139
Tabelle 54: TAB_FdV_151 – Protokolldaten einsehen .....	141
Tabelle 55: TAB_FdV_152 – Protokolldaten einsehen - Dokumentenverwaltung abfragen .....	141
Tabelle 56: TAB_FdV_153 – Protokolldaten einsehen - Autorisierung abfragen .....	142
Tabelle 57: TAB_FdV_154 – Protokolldaten einsehen - Zugangsgateway des Versicherten abfragen .....	142
Tabelle 58: TAB_FdV_155 – Felder im Protokolleintrag .....	143
Tabelle 59: TAB_FdV_156 – PIN der eGK ändern .....	145
Tabelle 60: TAB_FdV_157 – Ablaufaktivitäten – PIN der eGK ändern.....	145
Tabelle 61: TAB_FdV_158 – PIN der eGK entsperren.....	149
Tabelle 62: TAB_FdV_159 – Ablaufaktivitäten – PIN der eGK entsperren .....	149
Tabelle 63: TAB_FdV_160 – Benachrichtigungsadresse aktualisieren.....	152
Tabelle 64: TAB_FdV_177 – Verwendete Plattformleistungen .....	153

## 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
[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
[gemTestTreiberFdV]	<p><del>gematik: Datei "testtreiber_fdv.yaml" mit den Schnittstellen I_FDV und I_FDV_Management. Veröffentlicht über</del></p> <p><del><a href="https://fachportal.gematik.de/downloadcenter">https://fachportal.gematik.de/downloadcenter</a> und <a href="https://github.com/gematik/api-ePA/tree/master/src/openapi">https://github.com/gematik/api-ePA/tree/master/src/openapi</a></del></p> <p>gematik: Testtreiber-Schnittstellen I_FDV und I_FDV_Management (src/openapi/testtreiber_fdv.yaml), <a href="https://github.com/gematik/api-ePA">https://github.com/gematik/api-ePA</a></p>

## 9.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[DSML2.0]	OASIS: Directory Services Markup Language v2.0 December 18, 2001 <a href="https://www.oasis-open.org/standards">https://www.oasis-open.org/standards</a> <a href="http://www.oasis-open.org/committees/dsml/docs/DSMLv2.doc">http://www.oasis-open.org/committees/dsml/docs/DSMLv2.doc</a> <a href="http://oasis-open.org/committees/dsml/errata">http://oasis-open.org/committees/dsml/errata</a> <a href="https://www.oasis-open.org/committees/dsml/docs/DSMLv2.xsd">https://www.oasis-open.org/committees/dsml/docs/DSMLv2.xsd</a>

[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, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf</a>
[IHE-ITI-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, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf</a>
[IHE-ITI-TF2b]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf</a>
[IHE-ITI-TF2x]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2x) – Volume 2 Appendices, Revision 15.1, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf</a>
[IHE-ITI-RMD]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.2 – Trial Implementation <a href="https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf">https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf</a>
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, <a href="https://www.w3.org/TR/soap12-mtom/">https://www.w3.org/TR/soap12-mtom/</a>
[OWASP Proactive Control]	OWASP Top Ten Proactive Controls Project OWASP Proactive Controls For Developers v3.0 <a href="https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf">https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf</a>

[OWASP SAMP Project]	OWASP SAMP Project <a href="https://www.owasp.org/index.php/OWASP_SAMP_Project#tab=Browse_Online">https://www.owasp.org/index.php/OWASP_SAMP_Project#tab=Browse_Online</a>
[OWASPMobileTop10]	OWASP Mobile Security Project: Top 10 Mobile Risks <a href="https://owasp.org/www-project-mobile-top-10/">https://owasp.org/www-project-mobile-top-10/</a>
[OWASP MASVS]	OWASP Mobile Application Security Verification Service <a href="https://owasp.org/www-chapter-geneva/assets/slides/OWASP_Geneva-Chapter_Meeting-20161212_Jeremy_Matos-MASVS.pdf">https://owasp.org/www-chapter-geneva/assets/slides/OWASP_Geneva-Chapter_Meeting-20161212_Jeremy_Matos-MASVS.pdf</a>
[OWASP TTMC]	OWASP Mobile Security Project <a href="https://owasp.org/www-project-mobile-security/">https://owasp.org/www-project-mobile-security/</a>
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP <a href="https://tools.ietf.org/html/rfc6960">https://tools.ietf.org/html/rfc6960</a>
[vesta]	Zentrales Interoperabilitätsverzeichnis des deutschen Gesundheitswesens <a href="https://www.vesta-gematik.de/">https://www.vesta-gematik.de/</a>
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), <a href="http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html">http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html</a>
[XMLEnc-1.1]	XML Encryption Syntax and Processing, W3C Recommendation 11 April 2013, <a href="http://www.w3.org/TR/xmlenc-core1/">http://www.w3.org/TR/xmlenc-core1/</a>