gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Addendum zur Spezifikation Autorisierung ePA

Version:	1.2.0
Revision:	167254
Stand:	02.10.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_Autorisierung_UEePA

Dokumentinformationen

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	15.05.2019		freigegeben	gematik
1.1.0	28.06.19		Anpassung aufgrund Kommentierung zur Vertreterregelung	gematik
			Einarbeitung P20.1	gematik
1.1.0	28.06.19		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Mit der „Übergangsregelung ePA“ wird einem Zulassungsnehmer die Möglichkeit eröffnet in einem Übergangszeitraum mit einem reduzierten Funktionsumfang eine Zulassung mit Nebenbestimmungen zu erhalten. Der Umfang der Reduktion umfasst genau folgende Funktionen:

- Anbieterwechsel
- Vertreterregelungen und
- Bereitstellung und Verarbeitung Kostenträgerdokumente

Das vorliegende Dokument definiert für die Übergangsregelung ePA entsprechend die notwendigen Änderungen gegenüber dem Dokument [gemSpec_Autorisierung].

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von im letzten Kapitel benannten Produkt- bzw. Anbietertypen, sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

Basis für dieses Dokument ist die Spezifikation [gemSpec_Autorisierung]. Das vorliegende Dokument spezifiziert die für die Übergangsregelung ePA notwendigen Änderungen gegenüber [gemSpec_Autorisierung].

Die zusätzlichen, geänderten oder gelöschten Anforderungen und Hinweise werden unter den jeweiligen Kapitelüberschriften aus [gemSpec_Autorisierung] aufgeführt. In dem vorliegendem Dokument erfolgt ansonsten keine Wiederholung der Inhalte aus [gemSpec_Autorisierung].

Die vollständige Anforderungslage für einen Produkt- bzw. Anbietertypen ergibt sich aus dem Produkt- bzw. Anbietertypsteckbrief des jeweiligen Produkt- bzw. Anbietertyps aus Release 3.1.0 im Verbund mit den im letzten Kapitel verzeichneten Änderungen in allen Addenda.

1.5 Methodik

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

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

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

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

Neueinfügungen gegenüber dem OPB 3.1.0-Stand sind magenta hinterlegt markiert.

Streichungen gegenüber dem OPB 3.1.0-Stand sind ~~magenta hinterlegt und gestrichen markiert.~~

2 Funktionsmerkmale

Es werden zusätzliche Festlegungen getroffen, die die folgenden Kapitel von [gemSpec_Autorisierung] ergänzen:

2.1 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 3.1 Akteure und Rollen

Die Nutzer sind dabei gesetzlich Versicherte und Leistungserbringerinstitutionen ~~und Kostenträger~~, welche durch ihre jeweilige Karte der TI repräsentiert werden. Über eine kartenbasierte Authentifizierungsbestätigung authentisieren sie sich gegenüber der Komponente Autorisierung. ~~Ein Spezialfall des gesetzlichen Versicherten ist der berechtigte Vertreter.~~

Für die oben genannten Nutzer verwaltet die Komponente Autorisierung empfängerbezogen verschlüsseltes Schlüsselmaterial

- für Versicherte~~, plus den Spezialfall des Vertreters~~ - verschlüsselt für die individuelle KVNR
- für Leistungserbringerinstitutionen ~~und Kostenträger~~ - verschlüsselt für die individuelle Telematik-ID

Eine Leistungserbringerinstitution kann auf das für sie hinterlegte Schlüsselmaterial lesend zugreifen. ~~Analog kann ein Kostenträger nur auf das für ihn hinterlegte Schlüsselmaterial lesend zugreifen~~.

In der Umgebung des Versicherten hat ein Versicherter vollen Zugriff auf das hinterlegte Schlüsselmaterial mit folgender Ausnahme - ein Versicherter darf das eigene Schlüsselmaterial für die eGK des Versicherten nicht löschen. ~~Ein Vertreter führt Anwendungsfälle der Vertretung ausschließlich in der Umgebung eines Versicherten aus. Ebenso darf der Vertreter nicht das Schlüsselmaterial des Versicherten löschen und auch nicht Schlüsselmaterial für andere eGK-Inhaber hinzufügen (kein Einrichten weiterer Vertretungen durch einen Vertreter).~~

Tabelle 1: Anwendungsfälle der Schlüsselverwaltung nach Umgebung

Assoziation	Actor	Regel zur Identifikation des Nutzers*
A	Versicherter	subject-id == OwnerKVNR == ActorID
B		
C		
D	Leistungserbringer-institution	subject-id == ActorID != OwnerKVNR (für HBA – erst in Folgestufe) organization-id == ActorID != OwnerKVNR (für SMC-B)

E	Versicherter	subject-id == OwnerKVNR
~~F~~	~~Vertreter~~	~~subject-id == ActorID != OwnerKVNR (beim Verwalten des Vertretungsschlüssels)~~ ~~subject-id != ActorID != OwnerKVNR (beim Verwalten aller übrigen Schlüssel)~~
~~G~~	~~Kostenträger~~	~~organization-id == ActorID != OwnerKVNR (für SMC-B KTR)~~

Eine Leistungserbringerinstitution wird bei Einsatz einer SMC-B (Anwendungsfälle C und D) anhand ihrer Telematik-ID aus der organization-id eines AuthenticationTokens erkannt. Für diese Telematik-ID muss ein AuthorizationKey mit gleichlautender ActorID vorhanden sein, andernfalls ist diese Leistungserbringerinstitution nicht autorisiert. ~~Das gleiche gilt für die Kostenträger (Anwendungsfälle G und H).~~

~~Der Vertreter wird zunächst als Versicherter mit eigener eGK anhand der KVNR als subject-id eines AuthenticationTokens erkannt. In der Wahrnehmung einer Vertretung (Anwendungsfälle F) ist seine KVNR ungleich der OwnerKVNR des Eigentümers der Akte. Für seine KVNR muss ein AuthorizationKey mit gleichlautender ActorID vorhanden sein, andernfalls ist der Vertreter für den Zugriff nicht autorisiert.~~

2.2 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 3.2 Nachbarsysteme

Die Komponente Autorisierung stellt die Schnittstellen `I_Authorization` und `I_Authorization_Management` zur Nutzung aus der Umgebung der Leistungserbringer~~und Kostenträger~~ bereit. Von dort werden sie aus der Secure Consumer Zone aufgerufen.

2.3 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 5.1 Datenschutz und Datensicherheit

A_17839 - Komponente Autorisierung - Prüfung der Empfänger-Rolle

Die Komponente Autorisierung MUSS beim Aufruf einer der Operation

- I_Authorization::getAuthorizationKey

den übergebenen Parameter `AuthenticationAssertion` dahingehend prüfen, ob mindestens eine `ProfessionOID` der ZertifikatsExtension`Admission` gemäß [gemSpec_PKI#Tab_PKI_226] im Signaturzertifikat C.HCI.OSIG `/saml2:Assertion/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate` in der Liste der zulässigen Autorisierungsempfänger-Rollen gemäß [gemSpec_OID#Tab_PKI_402] und [gemSpec_OID#Tab_PKI_403]

- oid_praxis_arzt
- oid_zahnarztpraxis
- oid_praxis_psychotherapeut
- oid_krankenhaus

- oid_oeffentliche_apotheke
- oid_krankenhausapotheke
- oid_bundeswehrapotheke
- oid_mobile_einrichtung_rettungsdienst
- ~~oid_kostentraeger~~

enthalten ist und sofern nicht, die Operation mit dem Fehler AUTHORIZATION_ERROR abbrechen.**[<=]**

A_17840 - Komponente Autorisierung Vers. - Prüfung Identitätswechsel des Versicherten
Die Komponente Autorisierung MUSS eine übergebene `AuthenticationAssertion` für einen Versicherten (Das SAML:Assertion/SAML:AttributeStatement/SAML:Attribute `urn:gematik:subject:subject-id` enthält eine KVNR) dahingehend prüfen, ob die in der Behauptung `urn:gematik:subject:authreference` mit der `serialNumber` des zur Authentifizierung verwendeten AUT- bzw. AUT_ALT-Zertifikats in der Liste der bekannten AUT-Referenzen an der KeyChain des im RecordIdentifier benannten Aktenkontos ist und falls nicht, MUSS die Komponente Autorisierung den Versicherten ~~sowie im Vertretungsfall zusätzlich den Vertreter~~ über die Nutzung eines neuen Authentisierungsmittels in einer E-Mail-Nachricht an die hinterlegte E-Mailadresse `NotificationInfo` des Versicherten ~~bzw. des Vertreters~~ informieren. Anschließend MUSS die benannte `serialNumber` in die WhiteList der AUT-Referenzen an der KeyChain des im RecordIdentifier benannten Aktenkontos übernommen werden.**[<=]**

~~Nutzt der Versicherte ein im Aktensystem bisher unbekanntes Authentisierungsmittel (z.B. eine Folge-eGK) erhält er eine E-Mailbenachrichtigung, der Anwendungsfall wird nicht unterbrochen. Es obliegt dem Versicherten die Legitimität des Zugriffs bzw. des Authentisierungsmittels zu prüfen und sich gegebenenfalls mit dem ePA-Aktenanbieter und seiner Kasse in Verbindung zu setzen.~~

~~Nutzt der Vertreter des Versicherten ein bisher unbekanntes Authentisierungsmittel, erhalten sowohl der Versicherte als auch der Vertreter eine Benachrichtigung.~~

Eine Prüfung von Identitätsbestätigungen gemäß den Festlegungen für TBAuth bezieht sich auf Identitätsbestätigungen für Leistungserbringerinstitutionen~~und Kostenträger~~.

Bei Zugriffen aus der Umgebung des Versicherten wird ein Identitätsmerkmal des verwendeten Geräts abgefragt (DeviceID). Bei Zugriffen aus der Umgebung der Leistungserbringer erfolgt dies nicht, da hier als zugreifende Geräte ausschließlich zugelassene Konnektoren mit geprüfter Fachlogik zum Einsatz kommen. ~~Ebenso wird keine Geräteidentität für den Zugang der Kostenträger über ihr jeweiliges Rechenzentrum geprüft, da auch hier ausschließlich zugelassene Produkttypen in einer kontrollierten Betriebsumgebung zum Einsatz kommen.~~

2.4 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 5.3 Protokollierung

Der Aufruf der Operation `I_Authorization::getAuthorizationKey` aus der Umgebung der Leistungserbringer ~~und der Kostenträger~~ wird nicht protokolliert.

2.5 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.1 Übergreifende Festlegungen

Im Folgenden werden übergreifende Festlegungen formuliert, die in allen Operationen umgesetzt werden.

A_14500 - Komponente Autorisierung - Identifizierung eines Vertreters anhand einer AuthenticationAssertion
~~Die Komponente Autorisierung MUSS einen berechtigten Vertreter anhand seiner KVNR als `urn:gematik:subject:subject-id` in `SAML:Assertion/SAML:AttributeStatement/SAML:Attribute/@Name` einer übergebenen, gültigen AuthenticationAssertion eindeutig identifizieren, wenn die `subject-id` ungleich der OwnerKVNR zu einem im Operationsaufruf angegebenen RecordIdentifier ist und für die KVNR der AuthenticationAssertion ein AuthorizationKey zu der im Operationsaufruf angegebenen RecordIdentifier existiert.~~**[<=]**

A_18014 - Komponente Autorisierung - Ausschluss sonstiger Akteure
Die Komponente Autorisierung MUSS jeden Operationsaufruf mit dem Fehler TECHNICAL_ERROR abbrechen, in dessen Aufrufparameter AuthenticationAssertion eine KVNR als `urn:gematik:subject:subject-id` in `SAML:Assertion/SAML:AttributeStatement/SAML:Attribute/@Name` übergebenen wird, die ungleich der OwnerKVNR zu einem im Operationsaufruf angegebenen RecordIdentifier ist.**[<=]**

A_15620 - Komponente Autorisierung - Read-only bei suspendiertem Konto
~~Die Komponente Autorisierung MUSS die folgenden Operationen mit dem Standardfehler ACCESS_DENIED abbrechen,
wenn der RecordState der KeyChain des im Aufrufparameter der Operation benannten `RecordIdentifier` den Zustand `SUSPENDED` ausweist:~~

- ~~I_Authorization_Management::putAuthorizationKey~~
- ~~I_Authorization_Management_Insurant::putAuthorizationKey~~
- ~~I_Authorization_Management_Insurant::deleteAuthorizationKey~~
- ~~I_Authorization_Management_Insurant::replaceAuthorizationKey~~
- ~~I_Authorization_Management_Insurant::putNotificationInfo~~

[<=]

~~Damit soll verhindert werden, dass ein zur Umschlüsselung berechtigter Vertreter fälschlich einen ungültigen oder einschränkenden AuthorizationKey für den Versicherten hinterlegt. Dies berührt nicht die Ausstellung einer AuthorizationAssertion mit~~

~~ACCOUNT_AUTHORIZATION für den Fall eines nicht vorhandenen AuthorizationKey bei Kontoaktivierung/ -umzug.~~

2.6 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.2 Schnittstellen der Komponente Autorisierung

Das Funktionsmerkmal 'Autorisierung' der Komponente Autorisierung wird durch die in der folgenden Tabelle beschriebenen Schnittstellen mit den jeweiligen Operationen umgesetzt.

Tabelle 2: Schnittstellen der Komponente Autorisierung

Schnittstellen der Komponente Autorisierung	
I_Authorization	
`getAuthorizationKey`	Mit der Operation `getAuthorizationKey` wird das für einen Berechtigten verschlüsselte Schlüsselmaterial für ein konkretes Aktenkonto eines Versicherten in der Leistungserbringer-Umgebung und durch den Kostenträger heruntergeladen.
I_Authorization_Management	
`putAuthorizationKey`	Mit der Operation `putAuthorizationKey` wird das für einen Berechtigten verschlüsselte Schlüsselmaterial für ein konkretes Aktenkonto eines Versicherten im Aktensystem ePA gespeichert.
`checkRecordExists`	Mit der Operation `checkRecordExists` kann ein anderer Anbieter bei einem Anbieter einer Aktenlösung den Status und die Existenz eines Aktenkontos über die KVNR eines Versicherten abfragen.
`getAuthorizationList`	Die Operation `getAuthorizationList` liefert die Liste aller OwnerKVNRs des Aktensystems, in denen für die anfragende Institution ein AuthorizationKey hinterlegt ist. (horizontale Abfrage)
I_Authorization_Insurant	
`getAuthorizationKey`	Mit der Operation `getAuthorizationKey` wird das für einen Berechtigten verschlüsselte Schlüsselmaterial (kryptografische Berechtigung) für ein konkretes Aktenkonto eines Versicherten in der Personal-Zone heruntergeladen.
I_Authorization_Management_Insurant	
`putAuthorizationKey`	Mit der Operation `putAuthorizationKey` wird das für einen Berechtigten verschlüsselte Schlüsselmaterial AuthorizationKey für ein konkretes Aktenkonto eines Versicherten im ePA-Aktensystem gespeichert.
`deleteAuthorizationKey`	Mit der Operation `deleteAuthorizationKey` kann ein authentifizierter Versicherter ~~bzw. ein berechtigter Vertreter~~ die kryptografische Berechtigung für einen Nutzer innerhalb seines Aktenkontos löschen.

`replaceAuthorizationKey`	Mit der Operation `replaceAuthorizationKey` kann ein authentifizierter Versicherter ~~bzw. ein berechtigter Vertreter~~ das für eine alte eGK verschlüsselte Schlüsselmaterial durch neues für eine Folgekarte verschlüsseltes Schlüsselmaterial ersetzen.
`getAuditEvents`	Mit der Operation `getAuditEvents` kann ein authentifizierter Versicherter ~~bzw. ein berechtigter Vertreter~~ das Verwaltungsprotokoll der Komponente Autorisierung auslesen.
`putNotificationInfo`	Mit der Operation `putNotificationInfo` kann ein authentifizierter Versicherter ~~bzw. ein berechtigter Vertreter~~ die eigene, im Benachrichtigungskanal hinterlegten Daten aktualisieren.
`getAuthorizationList`	Die Operation `getAuthorizationList` liefert die Liste aller AuthorizationKeys zu einer angefragten Akte eines Versicherten. (vertikale Abfrage)

2.6.1.1 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.2.1.2 Umsetzung I_Authorization::getAuthorizationKey

A_17790 - Komponente Autorisierung LE - Vertretung wahrnehmen Freischaltprüfung

~~Die Komponente Autorisierung MUSS bei Wahrnehmung einer Vertretung für einen Versicherten mittels `I_Authorization::getAuthorizationKey` (`subject-id` der AuthenticationAssertion != `OwnerKVNR`) vor der Herausgabe prüfen, ob ein wartender Vertreter-Freischaltprozess für [OwnerKVNR des benannten RecordIdentifiers, subject-id als ActorID] aktiv ist und falls ja, die Operation mit dem Fehler REPRESENTATIVE_PENDING abbrechen.~~[<=]

A_15618 - Komponente Autorisierung LE - Autorisierung bei suspendiertem Konto

~~Die Komponente Autorisierung MUSS bei Aufruf der Operation `I_Authorization::getAuthorizationKey` bei Vorhandensein eines *AuthorizationKey* in der *KeyChain* des benannten `RecordIdentifier` für den mittels `AuthenticationAssertion` authentifizierten Nutzer (`subject-id` = *ActorID* des *AuthorizationKey*) eine Autorisierungsbestätigung mit AuthorizationType = ACCOUNT_AUTHORIZATION gemäß [A_14491] ausstellen, wenn der RecordState der KeyChain des benannten `RecordIdentifier` den Zustand `SUSPENDED` ausweist.~~[<=]

2.6.1.2 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.2.2.2 Umsetzung I_Authorization_Insurant::getAuthorizationKey

A_17789 - Komponente Autorisierung Vers. - Vertretung wahrnehmen Freischaltprüfung

~~Die Komponente Autorisierung MUSS bei Wahrnehmung einer Vertretung für einen Versicherten mittels `I_Authorization_Insurant::getAuthorizationKey` (`subject-id` der AuthenticationAssertion != `OwnerKVNR`) vor der Herausgabe prüfen, ob ein wartender Vertreter-Freischaltprozess für [OwnerKVNR des benannten RecordIdentifiers, subject-id als ActorID] aktiv ist und falls ja, die Operation mit dem Fehler REPRESENTATIVE_PENDING abbrechen.~~[<=]

A_15619 - Komponente Autorisierung Vers. - Autorisierung bei suspendiertem Konto

Die Komponente Autorisierung MUSS bei Aufruf der Operation `I_Authorization_Insurant::getAuthorizationKey` bei Vorhandensein eines *AuthorizationKey* in der *KeyChain* des benannten `RecordIdentifier` für den mittels `AuthenticationAssertion` authentifizierten Nutzer (`subject-id` = *ActorID* des *AuthorizationKey*) eine Autorisierungsbestätigung mit AuthorizationType = ACCOUNT_AUTHORIZATION gemäß [A_14491] ausstellen, wenn der RecordState der KeyChain des benannten `RecordIdentifier` den Zustand `SUSPENDED` ausweist.**[<=]**

2.6.1.3 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.2.3.2 Umsetzung I_Authorization_Management::putAuthorizationKey

Mit dieser Prüfung wird sichergestellt, dass nur Versicherte bzw. Vertreter einen Schlüssel für einen Berechtigten hinterlegen können. Eine Berechtigung wird nicht von einer Leistungserbringerinstitution oder von einem Kostenträger hinterlegt.

2.6.1.4 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.2.4.2 Umsetzung I_Authorization_Management_Insurant::putAuthorizationKey

A_14447 - Komponente Autorisierung Vers. - Berechtigungsprüfung Schlüsselhinterlegung

Die Komponente Autorisierung MUSS beim Aufruf der Operation `I_Authorization_Management_Insurant::putAuthorizationKey` an hand der subject-id (KVNR) der `AuthenticationAssertion` und des `RecordIdentifier` prüfen, ob für den aufrufenden Nutzer ein AuthorizationKey mit ActorID = KVNR hinterlegt ist und falls nicht, die Operation mit dem Fehler ACCESS_DENIED abbrechen.**[<=]**

Mit dieser Prüfung wird sichergestellt, dass nur Versicherte sowie berechtigte Vertreter Schlüsselmaterial für Versicherte, und Leistungserbringerinstitutionen und Kostenträger hinterlegen können, die selbst bereits über einen AuthorizationKey verfügen.

A_18184 - Komponente Autorisierung Vers. - Prüfung auf Vertretungsberechtigung für Prüfidentität

Die Komponente Autorisierung MUSS bei Hinterlegung einer Vertretungsberechtigung durch Aufruf der Operation `I_Authorization_Management_Insurant::putAuthorizationKey` mit (subject-id der AuthenticationAssertion != ActorID des Übergabeparameters AuthorizationKey und ActorID des Übergabeparameters AuthorizationKey != OwnerKVNR) prüfen, ob die Hinterlegung für eine Prüfidentität gemäß [gemSpec_PK_eGK#Card-G2-A_3820] erfolgen soll und falls ja, den Anwendungsfall mit dem Fehler TECHNICAL_ERROR abbrechen.**[<=]**

A_18751 - Komponente Autorisierung Vers. - Begrenzung zu registrierender Vertreter

Die Komponente Autorisierung MUSS bei Hinterlegung einer Vertretungsberechtigung durch Aufruf der Operation `I_Authorization_Management_Insurant::putAuthorizationKey` (vgl. A_17670) prüfen, ob die maximale Anzahl von fünf Vertretern erreicht wurde. Trifft dies zu, MUSS der Anwendungsfall mit dem Fehler TECHNICAL_ERROR abgebrochen werden. Eine Prüfung MUSS berücksichtigen, ob zum Zeitpunkt der Vertretungsregistrierung Freischaltprozesse gestartet wurden bzw. im Gange sind. Diese Prozesse sind in der maximalen Anzahl an Vertretern

zu berücksichtigen.
[<=]

A_17670 - Komponente Autorisierung Vers. - Freischaltprozess Vertreterberechtigung
Die Komponente Autorisierung MUSS bei Hinterlegung einer Vertretungsberechtigung durch Aufruf der Operation `I_Authorization_Management_Insurant::putAuthorizationKey` mit (subject-id der AuthenticationAssertion != ActorID des Übergabeparameters AuthorizationKey und ActorID des Übergabeparameters AuthorizationKey != OwnerKVNR) die Operation abschließen, sofern kein technischer oder fachlicher Fehler dies verhindert und anschließend den Freischaltprozess für Vertretereinrichtung starten (2.7- betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.6 Freischaltprozess Vertretereinrichtung), sofern für die im Übergabeparameter AuthorizationKey benannte ActorID noch kein AuthorizationKey in der Komponente Autorisierung für die im `RecordIdentifier` benannte OwnerKVNR vorhanden ist. **[<=]**

A_18039 - Komponente Autorisierung Vers. - Ausschluss Vertreterinformationen
Die Komponente Autorisierung MUSS die Operation `I_Authorization_Management_Insurant::putAuthorizationKey` mit dem Fehler TECHNICAL_ERROR abbrechen, wenn der Übergabeparameter `NotificationInfoRepresentative` einen Wert ungleich NULL bzw. ungleich "" (leere Zeichenkette) enthält.**[<=]**

2.6.1.5 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.2.4.4 Umsetzung I_Authorization_Management_Insurant::deleteAuthorizationKey

A_14451 - Komponente Autorisierung Vers. - Prüfen Löschberechtigung
Die Komponente Autorisierung MUSS bei Aufruf der Operation `I_Authorization_Management_Insurant::deleteAuthorizationKey` prüfen, ob der in der `AuthenticationAssertion` benannte Nutzer über einen *AuthorizationKey* mit AuthorizationType = DOCUMENT_AUTHORIZATION für den benannten `RecordIdentifier` verfügt, und andernfalls die Operation mit der Fehlermeldung ACCESS_DENIED abbrechen.**[<=]**

2.6.1.6 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.2.4.6 Umsetzung I_Authorization_Management_Insurant::replaceAuthorizationKey

A_14454 - Komponente Autorisierung Vers. - Prüfung Datensatz für bestehenden AuthorizationKey
Die Komponente Autorisierung MUSS für die Operation `I_Authorization_Management_Insurant::replaceAuthorizationKey` prüfen, ob ein *AuthorizationKey* für den benannten `RecordIdentifier` und den in der `AuthenticationAssertion` benannten Nutzer (subject-id == ActorID des vorhandenen AuthorizationKey) hinterlegt ist, und andernfalls die Operation mit der Fehlermeldung ACCESS_DENIED abbrechen.**[<=]**

A_15120 - Komponente Autorisierung Vers. - Fixierung des AuthorizationType für Vertreter
Die Komponente Autorisierung MUSS bei Aufruf der Operation `I_Authorization_Management_Insurant::replaceAuthorizationKey` prüfen, ob ein Vertreter seinen eigenen Schlüssel ersetzt (`OwnerKVNR != subject-id`

~~== ActorID des vorhandenen AuthorizationKey == ActorID in NewAuthorizationKey) und in diesem Fall den AuthorizationType des vorhandenen AuthorizationKey in den zu speichernden NewAuthorizationKey übernehmen.~~
~~Die Komponente Autorisierung MUSS die Operation mit dem Fehler ACCESS_DENIED abbrechen, wenn ein lediglich zur Umschlüsselung berechtigter Vertreter (RECOVERY_AUTHORIZATION im hinterlegten AuthorizationKey des Vertreters) versucht einen anderen AuthorizationKey zu ersetzen als den eigenen oder den des Versicherten.~~**[<=]**

2.6.1.7 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.2.4.10 Umsetzung I_Authorization_Management_Insurant::putNotificationInfo

Mit dieser Funktion kann ein Versicherter ~~oder ein berechtigter Vertreter~~ seine persönliche Benachrichtigungsadresse zur Gerätefreischaltung ändern.~~Sowohl für Versicherte als auch deren berechtigte Vertreter sind vor deren jeweiligem Zugriff Benachrichtigungsadressen vorhanden, da diese Operation ohne Gerätefreischaltung über ihre Adresse nicht aufrufbar ist.~~

Für Versicherte wird die Benachrichtigungsadresse initial im Rahmen der Kontoeröffnung hinterlegt. ~~Für Vertreter erfolgt die initiale Hinterlegung der Benachrichtigungsadresse durch den Versicherten mittels I_Authorization_Management_Insurant::putAuthorizationKey während der Vergabe der Zugriffsberechtigung.~~

2.6.2 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.5.1 Freischaltprozess neuer Geräte

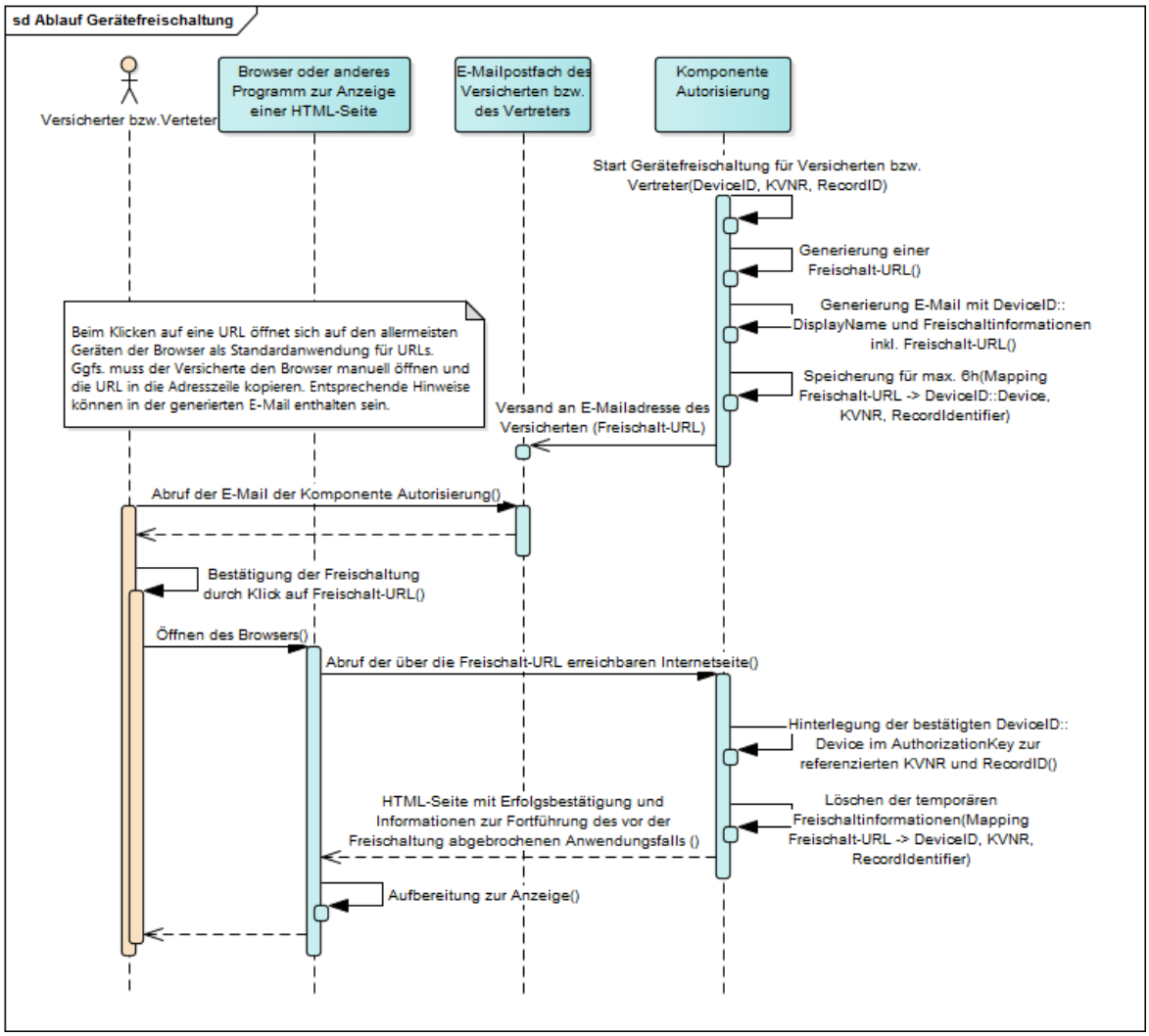


Abbildung 1: Informativer Ablauf des Geräte-Freischaltprozesses

Die Komponente Autorisierung startet den Freischaltprozess für jedes über `DeviceID::Device` identifizierte Gerät, das für den AuthorizationKey eines per KVNR identifizierten Versicherten bzw. Vertreter zu einer genannten RecordID als unbekannt gilt. ~~D.h. ein vom Vertreter im eigenen Aktenkonto verwendetes Gerät kann dort bereits registriert sein, im Rahmen der Vertretung eines anderen Versicherten kann das gleiche Gerät am Vertretungsschlüssel unbekannt sein. In diesem Fall ist der Freischaltprozess für die Wahrnehmung der Vertretung erforderlich.~~

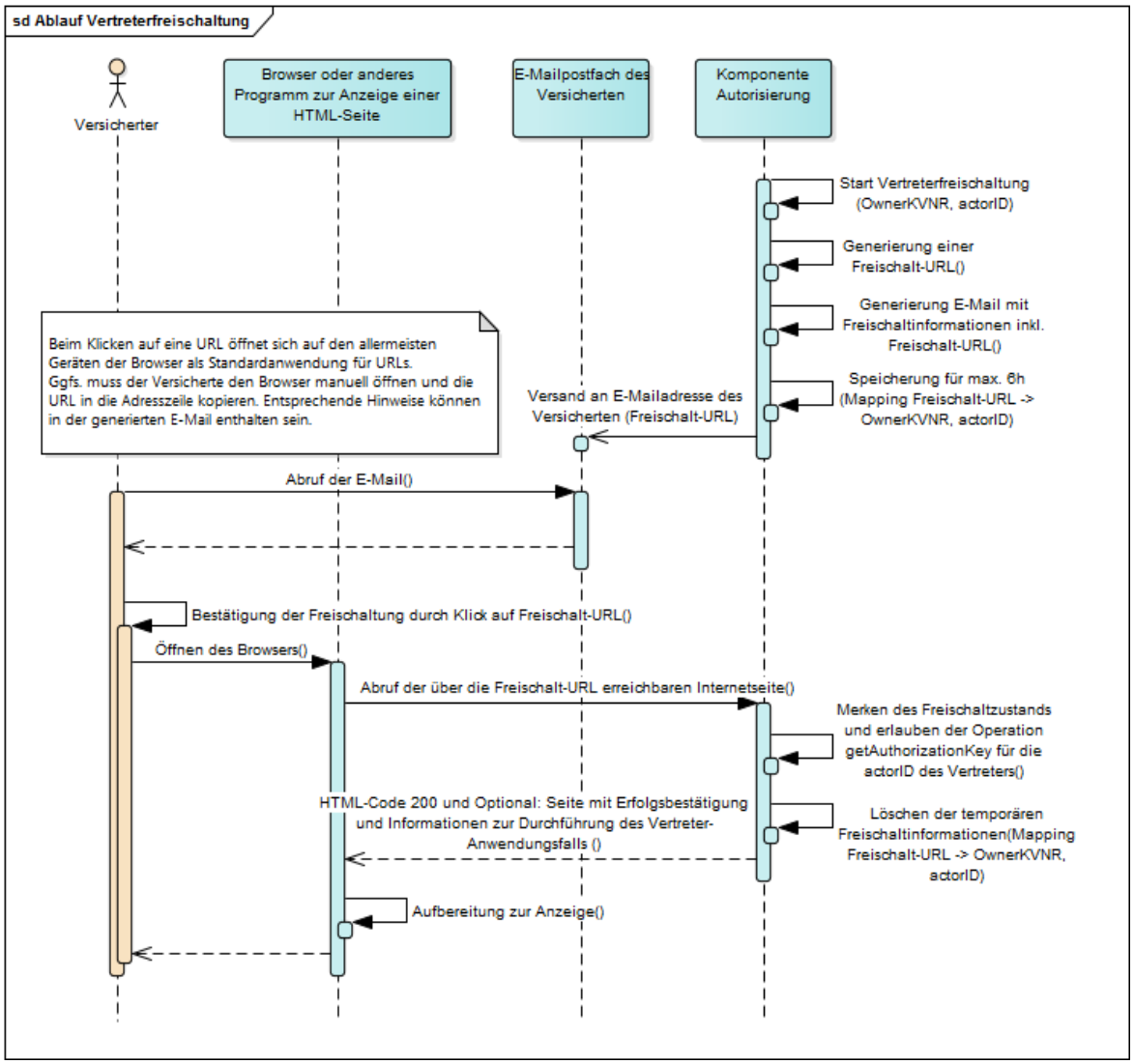
~~Mit der Generierung der Device-Kennung auf Basis einer Zufallszahl je Konto ergibt sich, dass die Verwendung eines Geräts in verschiedenen Konten (z.B. eigenes Konto + Vertretungsberechtigung in einem anderen Konto) zur Erzeugung zweier verschiedener Device-IDs führt, die im jeweiligen Aufrufkontext zu verwenden sind.~~

2.6.3 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.5.2 Geräteadministration

A_15551 - Komponente Autorisierung - Deregistrierung in fremden Konten
~~Die Komponente Autorisierung MUSS sicherstellen, dass der Versicherte nur diejenigen registrierten Geräte verwalten kann, die der Versicherte oder ein Vertreter in seinem Konto verwendet. Eine Deregistrierung eines Gerätes in einem Konto DARF NICHT automatisch zu einer Deregistrierung in einem anderen Konto führen (z.B. im Konto eines anderen Versicherten, für das der Versicherte Vertretungsrechte besitzt).~~**[<=]**

2.7 betroffenes Kapitel aus gemSpec_Autorisierung / Kapitel 6.6 Freischaltprozess Vertretereinrichtung

~~Die Komponente Autorisierung führt eine zusätzliche Autorisierung durch den Versicherten bei Einrichtung einer Vertretung für einen Vertreter durch. Der Versicherte wird aufgefordert, auf einen Link in einer E-Mail zu klicken, um die Speicherung eines AuthorizationKey für einen Vertreter zu autorisieren, den er über `I_Authorization_Management_Insurant::putAuthorizationKey` für diesen Vertreter hinterlegt. Die E-Mail mit dem Link zur Freischaltung wird an die E-Mail-Adresse des Versicherten geschickt, die auch für die Gerätefreischaltung des Versicherten verwendet wurde. Der folgende Ablauf zeigt informativ einen möglichen Ablauf des Freischaltprozesses.~~



~~Abbildung 2: Informativer Ablauf des Freischaltprozesses für Vertretung~~

~~Die Komponente Autorisierung startet den Freischaltprozess wenn der Versicherte mittels `I_Authorization_Management_Insurant::putAuthorizationKey` für einen konkreten mittels KVNR identifizierten Vertreter (als `ActorID` am AuthorizationKey) erstmalig eine Berechtigung hinterlegen möchte. Die Operation wird zunächst erfolgreich abgeschlossen, sofern kein fachlicher oder technischer Fehler dies verhindert. Dem Vertreter wird der Zugriff auf diesen Schlüssel jedoch solange verwehrt, wie der Versicherte noch nicht auf einen Freischaltlink in einer generierten Freischalt-E-Mail klickt. Die Komponente Autorisierung generiert zum Freischaltprozess der Vertretung einen eindeutigen Link auf Basis von Zufallszahlen und verschickt ihn an die vom Versicherten hinterlegte Benachrichtigungs-E-Mail-Adresse.~~

~~Durch Klicken auf diesen Link signalisiert der Versicherte der Komponente Autorisierung, dass die Hinterlegung eines AuthorizationKey für die KVNR d.h. `ActorID` des Vertreters rechtmäßig ist. Die Komponente Autorisierung speichert diesen Freischaltzustand für die `ActorID` des Vertreters und teilt dem Versicherten über die mittels Freischaltlink abgerufene Webseite mit, dass der UseCase des Schlüsselabrufs mittels `I_Authorization_Insurant::getAuthorizationKey` durch den Vertreter nun~~

autorisiert ist. Der Vertreter kann nun den hinterlegten Schlüssel abrufen und eine Vertretung wahrnehmen.

A_17672 - Komponente Autorisierung - Freischaltprozess Vertretung Freischalt-URL
Die Komponente Autorisierung MUSS im Freischaltprozess Vertretereinrichtung eine Freischalt-URL erzeugen, die einzig aus dem FQDN der Komponente Autorisierung und einer Zufallszahl (base64-kodiert) mit mindestens 120 Bit Entropie und Erzeugung gemäß [gemSpec_Krypt#GS-A_4367] besteht und diese Freischalt-URL an die E-Mail-Adresse des via `OwnerKVNR` referenzierten Versicherten verschicken.[<=]

A_17673 - Komponente Autorisierung - Freischaltprozess Vertretung Freischalt-URL Transportsicherheit
Die Komponente Autorisierung MUSS in der generierten Freischalt-URL das https-Protokoll verwenden.[<=]

A_17674 - Komponente Autorisierung - Freischaltprozess Vertretung getAuthorizationKey erlauben
Die Komponente Autorisierung MUSS bei Abruf des Bestätigungslinks eines aktiven Freischaltprozesses zur `OwnerKVNR` und `ActorId` des zukünftigen Vertreters die Operation `I_Authorization_Insurant::getAuthorizationKey` für das Abrufen eines AuthorizationKey durch den Vertreter (`ActorId` = KVNR des zukünftigen Vertreters) erlauben und den Freischaltprozess für den Vorgang zu `OwnerKVNR` und `ActorID` beenden.[<=]

Damit wird die Operation `I_Authorization_Insurant::getAuthorizationKey` bei zukünftigen Aufrufen durch den Vertreter für die freigeschaltete `ActorID` nicht mehr mit Fehler REPRESENTATIVE_PENDING abgebrochen.

A_17677 - Komponente Autorisierung - Freischaltprozess Vertretung Information
Die Komponente Autorisierung KANN in der HTTP-Response zum URL-Aufruf der Vertreterfreischaltung eine Meldung über die erfolgreiche Freischaltung an den aufrufenden Versicherten zurückgeben.[<=]

A_17675 - Komponente Autorisierung - Freischaltprozess Vertretung beenden
Die Komponente Autorisierung MUSS den Vorgang eines Freischaltprozesses Vertretung zur `OwnerKVNR` und `ActorID` nach 6 Stunden Wartezeit beenden.[<=]

A_17676 - Komponente Autorisierung - Freischaltprozess Vertretung Löschen nach Beendigung
Die Komponente Autorisierung MUSS beim Beenden des Vorgangs eines Freischaltprozesses die generierte Freischalt-URL und alle dazugehörigen temporären Daten löschen.[<=]

3 Ergänzungen für Produkttypsteckbriefe/Anbietersteckbriefe

Folgende Anforderungen werden im jeweiligen Produkttypsteckbrief/Anbietersteckbrief in Kapitel „3 Blattanforderungen“ ergänzt bzw. geändert:

3.1 gemProdT_Aktensystem_ePA_ePF

Afo-ID	Afo-Bezeichnung	Prüfverfahren (für neue Anforderungen)
A_18039	Komponente Autorisierung Vers. - Ausschluss Vertreterinformationen	Sich.techn. Eignung: Produktgutachten
A_18014	Komponente Autorisierung - Ausschluss sonstiger Akteure	Sich.techn. Eignung: Produktgutachten
A_17840	Komponente Autorisierung Vers. - Prüfung Identitätswechsel des Versicherten	
A_17839	Komponente Autorisierung - Prüfung der Empfänger-Rolle	
~~A_18184~~	~~Komponente Autorisierung Vers. - Prüfung auf Vertretungsberechtigung für Prüfidentität~~	
~~A_17790~~	~~Komponente Autorisierung LE - Vertretung wahrnehmen Freischaltprüfung~~	
~~A_17789~~	~~Komponente Autorisierung Vers. - Vertretung wahrnehmen Freischaltprüfung~~	
~~A_17677~~	~~Komponente Autorisierung - Freischaltprozess Vertretung Information~~	
~~A_17676~~	~~Komponente Autorisierung - Freischaltprozess Vertretung Löschen nach Beendigung~~	
~~A_17675~~	~~Komponente Autorisierung - Freischaltprozess Vertretung~~	

	~~beenden~~	
~~A_17674~~	~~Komponente Autorisierung - Freischaltprozess Vertretung getAuthorizationKey erlauben~~	
~~A_17673~~	~~Komponente Autorisierung - Freischaltprozess Vertretung Freischalt-URL Transportsicherheit~~	
~~A_17672~~	~~Komponente Autorisierung - Freischaltprozess Vertretung Freischalt-URL~~	
~~A_17670~~	~~Komponente Autorisierung Vers. - Freischaltprozess Vertreterberechtigung~~	
~~A_15620~~	~~Komponente Autorisierung - Read-only bei suspendiertem Konto~~	
~~A_15619~~	~~Komponente Autorisierung Vers. - Autorisierung bei suspendiertem Konto~~	
~~A_15618~~	~~Komponente Autorisierung LE - Autorisierung bei suspendiertem Konto~~	
~~A_15551~~	~~Komponente Autorisierung - Deregistrierung in fremden Konten~~	
~~A_15120~~	~~Komponente Autorisierung Vers. - Fixierung des AuthorizationType für Vertreter~~	
~~A_14500~~	~~Komponente Autorisierung - Identifizierung eines Vertreters anhand einer AuthenticationAssertion~~	
~~A_14454~~	~~Komponente Autorisierung Vers. - Prüfung Datensatz für bestehenden AuthorizationKey~~	
~~A_14451~~	~~Komponente Autorisierung Vers. - Prüfen Löschberechtigung~~	

~~A_14447~~	~~Komponente Autorisierung Vers. - Berechtigungsprüfung Schlüsselhinterlegung~~	