

---

## C\_12145\_Anlage

---

# Inhaltsverzeichnis

<b>1 Änderungsbeschreibung.....</b>	<b>2</b>
<b>2 Änderung in gemSpec_Aktensystem_ePAfuerAlle.....</b>	<b>3</b>

---

## 1 Änderungsbeschreibung

---

*Es wird eine EntitlementAllowList für LEI-Identitäten eingeführt. Identitäten, die nicht auf dieser EntitlementAllowList stehen, können keine Befugnis erzeugen, d.h. der Aufruf der Operation setEntitlementPs wird vom Aktensystem abgebrochen und mit einem Fehler beendet.*

---

## 2 Änderung in gemSpec\_Aktensystem\_ePAfuerAlle

---

### Neues Kapitel in 3.9 Entitlement Management

#### 3.9.5 EntitlementAllowList

Ein Primärsystem einer Leistungserbringerorganisation (LEI) kann eine Befugnis für ein Aktenkonto eines Versicherten in einer Behandlungssituation ("Stecken" der eGK, VSDM-Prüfungsnachweis) eigenständig erstellen, wenn der Versicherte der Nutzung der ePA nicht widersprochen hat, für die konkrete Leistungserbringerorganisation im Aktenkonto kein Befugnisausschluss (ref-> Kapitel 3.9.4 Blocked User Policy) vorliegt und die Leistungserbringerorganisation einer grundsätzlich befugbaren Nutzergruppe angehört (ref-> 3.9 Entitlement Management).

Darüber hinaus wird die Erstellung von Befugnissen in einer Behandlungssituation auf eine Teilmenge von definiert benannten LEI innerhalb der befugbaren Nutzergruppen eingeschränkt. Diese LEI werden in einer Liste, der EntitlementAllowList, aktensystemweit verwaltet und anhand ihrer Telematik-ID identifiziert. Ausschließlich LEI mit einem Eintrag auf dieser Liste können durch ein Primärsystem befugt werden.

Die Befugnisvergabe durch den Versicherten oder einen Vertreter mittel ePA-FdV ist durch die EntitlementAllowList nicht eingeschränkt. Über ein ePA-FdV können auch LEI befugt werden, die keinen Eintrag in der EntitlementAllowList haben.

Die EntitlementAllowList wird durch das Aktensystem bei jedem Aufruf einer Operation zur Befugnisvergabe durch ein Primärsystem ausgewertet. Diese Operation wird mit einem Fehler beendet, wenn die zu befugende LEI nicht Bestandteil der Liste ist. Eventuell vorhandene Befugnisse dieser LEI, etwa aus einer Befugnisvergabe mittels ePA-FdV, verbleiben im Fehlerfall der Operation unverändert.

Die EntitlementAllowList wird für alle Aktenkonten eines Aktensystems einheitlich verwaltet. Die Verwaltung erfolgt außerhalb der VAU, die Liste muss aber für Operationen der Befugnisvergabe innerhalb der VAU zugänglich sein. Die maßgebliche Liste außerhalb der VAU wird dazu mindestens einmalig innerhalb von 24 Stunden in die VAU synchronisiert, auch, wenn keine Änderung der Liste erfolgt ist. Neu zur EntitlementAllowList hinzugefügte LEI sind dadurch innerhalb von maximal 24 Stunden durch ihr Primärsystem befugbar. Werden LEI von der EntitlementAllowList entfernt, so sind diese unverzüglich von einer Befugnisvergabe durch das Primärsystem auszuschließen, bzw. muss die Synchronisation in die VAU unverzüglich erfolgen.

#### **A\_27304 - ePA-Aktensystem - EntitlementAllowList außerhalb der VAU**

Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen umsetzen, die eine unautorisierte Änderung der EntitlementAllowList verhindern.  
[<=, Anb\_Aktensystem\_ePA, Sich.techn. Eignung: Gutachten (Anbieter)]

#### **A\_27305 - ePA-Aktensystem - EntitlementAllowList in VAU aktualisieren**

Das ePA-Aktensystem MUSS sicherstellen, dass in der VAU nach spätestens 24 Stunden die EntitlementAllowList aktualisiert wird. [<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten]

#### **A\_27306 - ePA-Aktensystem - EntitlementAllowList in VAU aktualisieren - Ausschluss einer LEI**

Falls mindestens eine LEI von der EntitlementAllowList entfernt wird, MUSS der Betreiber des ePA-Aktensystems sicherstellen, dass die EntitlementAllowList in der VAU

unverzüglich aktualisiert wird.【<=, Anb\_Aktensystem\_ePA, Sich.techn. Eignung: Gutachten (Anbieter)】

Hinweise zu A\_27306-\*: Die Anforderung dient dem Fall, dass eine Telematik-ID einer LEI aus Sicherheitsgründen von der EntitlementAllowList genommen werden muss.

- Die gematik übermittelt die komplette aktuelle EntitlementAllowList, in welcher die Telematik-ID der betroffenen LEI entfernt wurde, an den Anbieter des ePA-Aktensystems.
- Die gematik übermittelt die aufgrund von Sicherheitsgründen aktualisierte EntitlementAllowList über die etablierten Incident-Prozesse.

#### **A\_27302 - Entitlement Management - setEntitlementPs in Abhängigkeit von EntitlementAllowList**

Falls der Nutzer nicht auf der EntitlementAllowList enthalten ist, MUSS das Entitlement Management die Operation setEntitlementPs ohne Erzeugung einer Befugnis mit dem HTTP-Statuscode 409 requestMismatch abbrechen.【<=, Aktensystem\_ePA, Sich.techn. Eignung: Produktgutachten】

#### **A\_27327 - ePA-Aktensystem - EntitlementAllowList nicht in RU und TU wirksam**

Das ePA-Aktensystem DARF die EntitlementAllowList NICHT in der RU bzw. TU anwenden. 【<=, Aktensystem\_ePA, funkt. Eignung: Herstellererklärung】