Inhaltsverzeichnis

1 Änderungsbeschreibung

2 Änderung in gemSpec_Aktensystem_ePAfuerAlle

Neues Kapitel

3.9.6 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)

Die Erstellung von Befugnissen durch Primärsysteme der Leistungserbringerinstitutionen wird durch das Aktensystem mengenmäßig über einen Zeitraum begrenzt. Diese Maßnahme verhindert den massenhaften Zugriff auf Aktenkonten durch Fehlbedienung seitens eines Primärsystems oder durch unzulässige Nutzung der Aktensysteme.

Die maximal zulässige Befugnismenge ist dabei so bemessen, dass die intendierte Nutzung der ePA durch Leistungserbringerinstitutionen im Versorgungsalltag nicht eingeschränkt wird. Diese maximale Befugnismenge ist pro Nutzerrolle separat festgelegt.

Jedes Aktensystem führt dazu aktensystemweit Zähler für erteilte Befugnisse aus der Umgebung der Leistungserbringer pro Telematik-ID. Die Erfassung erfolgt somit pro Leistungserbringerinstitutionen separat. Die Zuordnung erfolgt zur Telematik-ID der befugniserstellenden Nutzer (nicht des zu befugenden Nutzers). Die Befugnisvergabe aus der Umgebung des Versicherten mittels ePA-FdV wird nicht erfasst und geht nicht in die Zählerstände ein.

Das Entitlement Mangement wertet diese Menge der erfassten Befugnisvergaben im Falle einer weiteren Befugnisvergabe durch ein Primärsystem aus der Umgebung der LEI aus und verhindert die Befugniserstellung bei Erreichen der maximal zulässigen Befugnismenge.

Die zulässige Befugnisrate limitiert dabei einerseits die Menge der innerhalb einer Stunde erstellbaren Befugnisse, als auch die Menge der insgesamt monatlich erstellbaren. Die Zählung erfolgt aktensystemweit pro Aktensystem eines Herstellers und unabhängig vom adressierten Aktenkonto und berücksichtigt nur erfolgreiche Befugnisvergaben. Der Zeitraum pro Stunde, bzw. pro Monat, bezieht sich dabei auf den Zeitraum der aktuellen Stunde, bzw. des aktuellen Monats.

A_27311 - Entitlement Management – RateLimit-oid-List
Das Entitlement Management MUSS eine *RateLimit-oid-List* führen, in der pro oid

- der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden Befugnisse innerhalb einer Stunde,
- der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden Befugnisse innerhalb eines Monats und
- der Zeitpunkt der letzten Änderung der Werte

gespeichert werden.**[**<=, Aktensystem_ePA, funkt. Eignung: Test Produkt/FA**]**

Initial ist die RateLimit-oid-List mit folgenden Werten zu belegen:

A_27290 - Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Stunde
Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass eine LEI mit der Rolle

- oid_praxis_arzt maximal 200 Befugnisse

- oid_krankenhaus maximal 1.000 Befugnisse
- oid_institution-vorsorge-reha maximal 1.000 Befugnisse
- oid_zahnarztpraxis maximal 200 Befugnisse
- oid_öffentliche_apotheke maximal 200 Befugnisse
- oid_praxis_psychotherapeut maximal 100 Befugnisse
- oid_institution-pflege maximal 100 Befugnisse
- oid_institution-geburtshilfe maximal 100 Befugnisse
- oid_praxis-physiotherapeut maximal 100 Befugnisse
- oid_institution-oegd maximal 100 Befugnisse
- oid_institution-arbeitsmedizin maximal 100 Befugnisse

innerhalb einer Stunde durch das Primärsystem im Aktensystem registrieren kann.
[<=, Aktensystem_ePA, funkt. Eignung: Test Produkt/FA**]**

A_27291 - Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Monat
Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass

- oid_praxis_arzt maximal 10.000 Befugnisse
- oid_krankenhaus maximal 200.000 Befugnisse
- oid_institution-vorsorge-reha maximal 200.000 Befugnisse
- oid_zahnarztpraxis maximal 10.000 Befugnisse
- oid_öffentliche_apotheke maximal 25.000 Befugnisse
- oid_praxis_psychotherapeut maximal 10000 Befugnisse
- oid_institution-pflege maximal 10000 Befugnisse
- oid_institution-geburtshilfe maximal 10000 Befugnisse
- oid_praxis-physiotherapeut maximal 10000 Befugnisse
- oid_institution-oegd maximal 10000 Befugnisse
- oid_institution-arbeitsmedizin maximal 10000 Befugnisse

innerhalb eines Monats durch das Primärsystem im Aktensystem registrieren kann.
[<=, Aktensystem_ePA, funkt. Eignung: Test Produkt/FA**]**

Hinweis zu A_27290-* und A_27291-*: Die Stunde bzw. der Tag müssen sich nicht auf die aktuelle Stunde bzw. Kalendertag beziehen, sondern können auch je Leistungserbringerinstitution auf Requestzeitpunkte bezogen werden. Dann gilt für einen Monat 30 Tage.

A_27318 - ePA-Aktensystem - RatelLimit-oid-List: Maßnahmen zum Schutz der Konfiguration
Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen umsetzen, die eine unautorisierte Änderung der *RateLimit-oid-List* verhindern.
[<=, Anb_Aktensystem_ePA, Sich.techn. Eignung: Gutachten (Anbieter)**]**

A_27312 - ePA-Aktensystem - RatelLimit-oid-List: Konfiguration durch Betreiber
Der Betreiber des ePA-Aktensystem MUSS sicherstellen, dass die Werte für die Anzahl der maximalen Befugnisse in der RateLimit-oid-List durch den Betreiber des ePA-Aktensystems außschließlich im Vier-Augen-Prinzip konfigurierbar sind.
[<=, Anb_Aktensystem_ePA, Sich.techn. Eignung: Gutachten (Anbieter)**]**

Stellen LEI Befugnisse mittels der Operation `setEntitlementsPs` über das Primärsystem in das ePA-Aktensystem ein, wird für diese LEI geprüft, ob diese bereits das zulässige Limit erreicht hat. Nur falls dies nicht der Fall ist, kann die Befugnis eingestellt werden. Hierzu erfasst das ePA-Aktensystem außerhalb der VAU wann ein Nutzer mit welcher Rolle eine Befugnis registriert hat. Für den Nutzer wird außerhalb der VAU ein Nutzerpseudonym geführt.

A_27313 - Entitlement Management - Prüfen der RateLimit-oid-List beim Einstellen von Befugnissen
Das Entitlement Management MUSS bei Aufruf der Operation `setEntitlementsPs` prüfen, ob für das zur LEI gehörende Nutzerpseudonym und die oid der LEI bereits das in der *RateLimit-oid-List* vorgegebene maximale Limit pro Stunde oder Monat erreicht wurde. Falls ein Limit erreicht wurde, wird die Operation `setEntitlementsPs` mit einem Fehler abgebrochen. Falls kein Limit erreicht wurde, ist die Registrierung für das zur LEI gehörende Nutzerpseudonym zu vermerken.**[**<=, Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten**]**

A_27310 - ePA-Aktensystem - Erfassung der Nutzer zur Prüfung RateLimit-oid-List
Das ePA-Aktensystem MUSS sicherstellen dass bei der Erfassung der Nutzerdaten außerhalb der VAU zur Prüfung der *RateLimit-oid-List* eine Profilierung über die Nutzer nicht möglich ist und zu diesem Zweck aus der TelematikId eines Nutzers ein Nutzerpseudonym abgeleitet wird, gemäß gemSpec_Krypt#7.5 Routing auf VAU-Instanzen.
[<=, Aktensystem_ePA, Sich.techn. Eignung: Produktgutachten**]**

3 Änderung in I_Entitlement_Management.yaml

Erweiterung in Operation setEntitlementPs für A_27289, A_27290, A_27291

```
       **Provider**:</br>
       ...
       The entitlement management enforces the requirements for rate
limiting.
       ...


       | Conditions | Status code | Error code | Remarks |
       |------------|-------------|------------|---------|
       ...
       | Rate limiting exeeced | 423 | locked||
```