Anlagedokument C_10511 - Lastreduktion für Anfragen zu Nachrichten durch Apothekenverwaltungssysteme

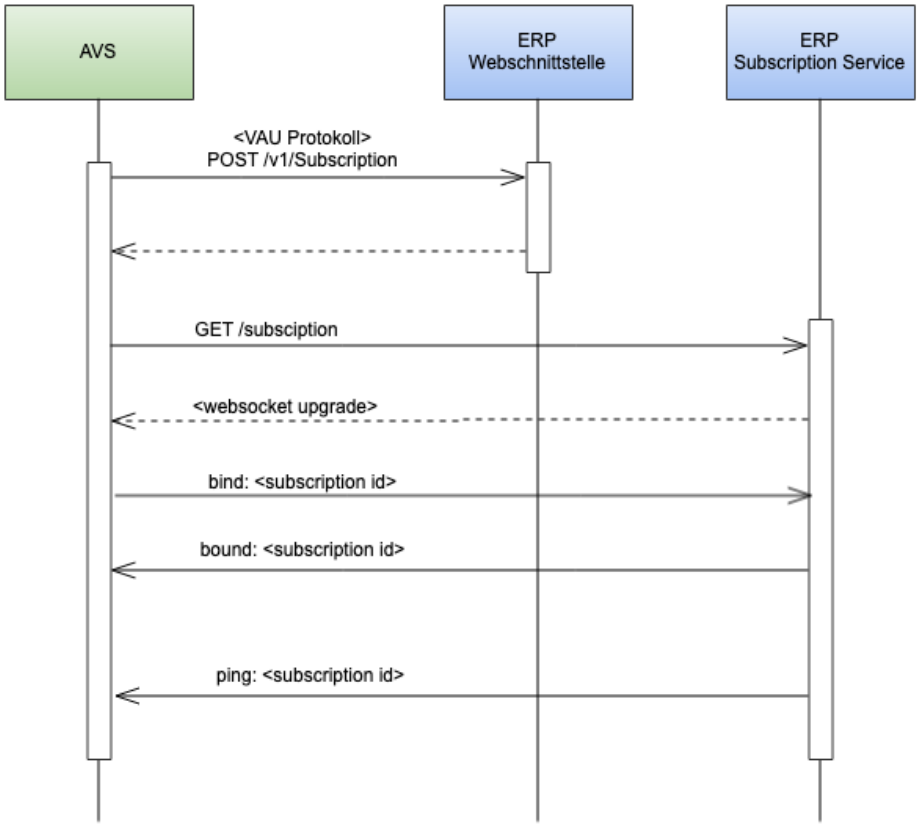
1 Änderungsbedarf

Der Versicherte kann über das E-Rezept-FdV E-Rezepte einer Apotheke zuweisen. Dafür erzeugt das E-Rezept-FdV eine Nachricht und stellt diese auf dem E-Rezept-Fachdienst ein. Ein Apothekenverwaltungssystem fragt periodisch am E-Rezept-Fachdienst nach neu vorliegenden Nachrichten an, um diese zu empfangen.

Um die Last am E-Rezept-Fachdienst zu kontrollieren, wurde festgelegt, dass die AVS nicht öfter als alle 5 min nach neuen Nachrichten anfragen dürfen (A_21556). Die dadurch bis zu 5 min entstehende Verzögerung, verlängert die Zeit, bis eine Apotheke auf die Nachricht des Versicherten reagieren kann. Aus dem Grund wird eine Funktionalität eingeführt, mit der AVS eine Notification erhalten, dass eine neue Nachricht für eine Telematik-ID vorliegt.

2 Konzept

Der Ablauf orientiert sich am FIHR-Standard
(siehe https://www.hl7.org/fhir/subscription.html#2.46.7.2):



3 Änderung in gemSpec_FD_eRp

Erweiterung A_19412-* Anbieter E-Rezept-Fachdienst - Schnittstellenadressierung
Der Anbieter des E-Rezept-Fachdienstes MUSS die den Primärsystemen und die im Internet angebotenen Schnittstellen des E-Rezept-Fachdienstes unter den folgenden URLs zur Verfügung stellen:

- https://subscription.zentral.erp.splitdns.ti-dienste.de - Schnittstelle Subscription Service

... <=

6.6 Ressource Subscription

6.6.1 HTTP-Operation POST

A_22362 - E-Rezept-Fachdienst – Subscription registrieren – Rollenprüfung Apotheke
Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf die /Subscription Ressource sicherstellen, dass ausschließlich Nutzer in der Rolle

- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am E-Rezept-Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit eine Subscription nicht durch Unberechtigte registriert werden kann.**[**<=**]**

Prüfverfahren: eRp_FD, Sich.techn. Eignung: Produktgutachten

A_22363 - E-Rezept-Fachdienst – Subscription registrieren – Prüfung Telematik-ID
Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf die /Subscription Ressource durch eine abgebende Leistungserbringerinstitution (Apotheke), diese anhand der Telematik-ID aus dem ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, diese gegen die in der Ressource im Element`criteria` Attribut `receipient` hinterlegte Telematik-ID prüfen und bei Ungleichheit den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich die Apotheke für sich selbst eine Subscription registrieren kann.**[**<=**]**

Prüfverfahren: funktionaler Test

A_22364 - E-Rezept-Fachdienst – Subscription registrieren – Response
Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf die /Subscription Ressource mit einem Response antworten, welcher eine Subscription Ressource mit

- Pseudonym der Telematik-ID in `id`
- aktueller Timestamp + 12h in `end`
- Bearer Token in `Authorization`

enthält.**[**<=**]**

Prüfverfahren: funktionaler Test

Beispiel:

```
<Subscription>
  <id
value="838dabe4e05416c776d60256c511558f6831f679c613f203d30b58b05555618a"/>
  <status value="active"/>
  <end value="2021-01-01T00:00:00Z"/>
  <criteria value="Communication?received=null&amp;recipient=3-
05.2.1001000000.381"/>
  <channel>
    <type value="websocket"/>
    <header value="Authorization: Bearer secret-token-abc-123"/>
  </channel>
</Subscription>
```

Hinweis: Der Header wird beim Web Socket Upgrade durch den Client an den Subscription Service übermittelt.

A_22365 - E-Rezept-Fachdienst – Subscription registrieren – Pseudonym der Telematik-ID
Der E-Rezept-Fachdienst MUSS das Pseudonym innerhalb der VAU mittels eines 128-Bit-AES-CMAC-Schlüssels erstellen und hexadezimal kodieren (32 Byte lang) (vgl gemSpec_Krypt#A_20163).**[**<=**]**

Prüfverfahren: Sicherheitstechn. Eignung Produktgutachten

A_22383 - E-Rezept-Fachdienst – Generierungsschlüssel – Pseudonym der Telematik-ID
Der Anbieter des E-Rezept-Fachdienstes MUSS den AES-CMAC-Schlüssel zur Pseudonymgenerierung regelmäßig mindestens alle 3 Monate ändern.**[**<=**]**

Prüfverfahren: Sicherheitstechn. Eignung Anbietergutachten

A_22366 - E-Rezept-Fachdienst – Subscription registrieren – Barrier-Token
Der E-Rezept-Fachdienst MUSS für die Registrierung der Subscription einen Bearer-Token mit den Claims

- subscriptionid: Pseudonym der Telematik-ID
- iAt: Timestamp wann Subscription erstellt wurde
- exp: Timestamp Ablauf der Subscription

erstellen und mit einer Identität des E-Rezept-Fachdienstes signieren (Signature Algortihm: ES256).**[**<=**]**

Prüfverfahren: Sicherheitstechn. Eignung Produktgutachten

Hinweise:

Das Signaturzertifikat muss nicht aus der Komponenten-PKI der TI abgeleitet werden.

Es wird kein fester Turnus festgelegt, in dem der Schlüssel gewechselt wird. Ein Wechsel kann über betriebliche Prozesse initiiert werden.

Der Schlüssel für die Signatur muss sicher gespeichert, jedoch nicht zwingend im HSM abgelegt werden.

6.3 Ressource Communication

6.3.2.1 POST /Communication/

A_22367 - E-Rezept-Fachdienst - Nachricht einstellen - Notification Apotheke
Der E-Rezept-Fachdienst MUSS beim Einstellen einer Nachricht des Profils "https://gematik.de/fhir/StructureDefinition/erxCommunicationDispReq" oder "https://gematik.de/fhir/StructureDefinition/erxCommunicationInfoReq" zur Versicherter-zu-Apotheken-Kommunikation über die http-Operation POST auf den Endpunkt`/Communication` prüfen, ob für die Telematik-ID des Empfängers Subscriptions registriert sind und für Registrierungen über den Subscription Service eine Notification (`ping : subscription-id`) senden.**[<=]**

Prüfverfahren: Funktionaler Test

6.7 Subscription Service

Der Subscription Service wird außerhalb der VAU betrieben.

A_22368 - E-Rezept-Fachdienst - Subscription Service - Webschnittstelle
Der E-Rezept-Fachdienst MUSS eine Webschnittstelle anbieten, welche Websocket Verbindungen mit einer Dauer von bis zu 12h unterstützt.**[<=]**

Prüfverfahren: Funktional Herstellererklärung

A_22369 - E-Rezept-Fachdienst - Subscription Service - Prüfung Bearer-Token
Der E-Rezept-Fachdienst MUSS an der Webschnittstelle des Subscription Service beim Verbindungsaufbau prüfen, dass der Client einen zeitlich und kryptographisch gültigen Bearer-Token der Schnittstelle `GET /Subscription` übermittelt und bei nicht-erfolgreicher Prüfung die Verbindung mit dem Fehler 403 ablehnen.**[<=]**

Prüfverfahren: Sicherheitstechn. Eignung Produktgtachten

A_22370 - E-Rezept-Fachdienst - Subscription Service - Upgrade
Der E-Rezept-Fachdienst MUSS an der Webschnittstelle des Subscription Service beim Verbindungsaufbau ein Upgrade durchführen. **[<=]**

Prüfverfahren: Funktionaler Test

A_22371 - E-Rezept-Fachdienst - Subscription Service - abgelaufene Verbindungen schließen
Der E-Rezept-Fachdienst MUSS an der Webschnittstelle des Subscription Service sicherstellen, dass Verbindungen nach Überschreiten des Timestamp Ablauf der Subscription geschlossen werden. **[<=]**

Prüfverfahren: Funktionaler Test

A_22378 - E-Rezept-Fachdienst - Subscription Service - Verbot Profilbildung
Der E-Rezept-Fachdienst DARF in der Verbindung zum Subscription Service anfallende Metadaten (Client-IP-Adresse, etc.) NICHT für eine unbefugte Profilbildung der verbundenen Clients verwenden. **[<=]**

Prüfverfahren: sicherheitstechn. Herstellererklärung

Hinweis: Eine Verwendung zur Sicherung der Schnittstelle (DDoS-Schutz, Fehleranalyse in sehr eingeschränktem Maß) ist zulässig (im Sinne einer befugten Profilbildung).

4 Änderung in gemILF_PS_eRp

5.1.1 Kommunikation zu Diensten der TI

Die Tabelle TAB_ILFERP_014 wird wie folgt ergänzt:

Tabelle 1 : TAB_FdVERP_014 - HTTP-Header "X-erp-resource"

Operation	X-erp-resource
POST /Subscription	Subscription

5.3.11 Subscription für neue Communication

Um die Last am E-Rezept-Fachdienst zu kontrollieren, wurde festgelegt, dass ein AVS nicht öfter als alle 5 min nach neuen Nachrichten anfragen dürfen (A_21556). Die dadurch bis zu 5 min entstehende Verzögerung, verlängert die Zeit, bis eine Apotheke auf die Nachricht des Versicherten reagieren kann. Aus dem Grund wird eine Funktionalität eingeführt, mit der AVS eine Notification erhalten, dass eine neue Nachricht für eine Telematik-ID vorliegt. Nach Erhalt einer Notification darf das AVS die neue Nachricht sofort abrufen.

A_22426 - PS abgebende LEI: Subscription für neue Communication - eine Subscription pro Telematik-ID
Das PS der abgebenden LEI DARF NICHT mehr als eine Subscription pro Telematik-ID registrieren.**[<=]**

A_22372 - PS abgebende LEI: Subscription für neue Communication
Das PS der abgebenden LEI MUSS den Anwendungsfall "Subscription für neue Communication" gemäß TAB_ILFERP_xxx umsetzen.

Tabelle 2 : TAB_ILFERP_xxx – Subscription für neue Communication

Name	Subscription für neue Communication
Auslöser	• Periodischer Aufruf, wenn keine Websocket Verbindung für die Notification besteht
Akteur	AVS
Vorbedingung	• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Es besteht eine Websocket Verbindung zum Empfang der Notification
Standardablauf	1. Subscription Ressource erstellen 2. Subscription registrieren 3. Websocket Verbindung zu Subscription Service aufbauen 4. Listening

[<=]

Prüfverfahren: Funktionale Herstellererklärung

A_22373 - PS abgebende LEI: Subscription für neue Communication - Subscription Ressource erstellen

Das PS der abgebenden LEI MUSS im Anwendungsfall "Subscription für neue Communication" eine`Subscription` Ressource mit

- Telematik-ID in Element criteria Attribut receipient

erstellen.**[<=]**

Prüfverfahren: Funktionale Herstellererklärung

A_22374 - PS abgebende LEI: Subscription für neue Communication - Subscription registrieren
Das PS der abgebenden LEI MUSS im Anwendungsfall "Subscription für neue Communication" zum Registrieren im E-Rezept-Fachdienst die HTTP-Operation`POST /v1/Subscription` mit

- ACCESS_TOKEN im Authorization-Header

ausführen.**[<=]**

Prüfverfahren: Funktionale Herstellererklärung

Beispiel:

```
POST /v1/Subscription

<Subscription>
  <status value="requested"/>
  <criteria value="Communication?received=null&amp;recipient=3-
05.2.1001000000.381"/>
  <channel>
    <type value="websocket"/>
  </channel>
</Subscription>
```

Im Response des `POST /v1/Subscription` Request ist die Subscription Ressource, ergänzt um die subscription-id und einen Authorization Header (Bearer-Token), enthalten.

A_22375 - PS abgebende LEI: Subscription für neue Communication - Subscription
Das PS der abgebenden LEI MUSS im Anwendungsfall "Subscription für neue Communication" nach der Registrierung eine Web Socket Verbindung zum Subscription Service mit

- Authorization Header

aufbauen und ein Upgrade durchführen.**[<=]**

Prüfverfahren: Funktionale Herstellererklärung

Beispiel:

```
GET https://subscription.zentral.erp.splitdns.ti-dienste.de/subscription
Authorization: Bearer secret-token-abc-123
Connection: Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket
Sec-WebSocket-Version: 13
Sec-WebSocket-Key: q4xkcO32u266gldTuKaSOw==
```

Der Subscription Service antwortet mit dem Upgrade

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: fA9dggdnMPU79lJgAE3W4TRnyDM=
```

Das Upgrade erfolgt mit einer "bind" Text Nachricht über die Web Socket Verbindung an den Server.

```
bind: <subscription id>
```

Der Subscription Service antwortet mit einer "bound" um die Einrichtung der Subscription zu bestätigen.

```
bound: <subscription id>
```

Wenn eine neue Nachricht für die Telematik-ID der Apotheke eingestellt wird, dann sendet der E-Rezept-Fachdienst eine Nachricht `ping: <subscription-id>`. Das AVS kann dann diese Nachricht mittels des Anwendungsfalls "Nachrichten von Versicherten empfangen" unter Nutzung des Requests`GET /Communication?received=null&recipient=<Telematik-ID>` abrufen.

Bei Nutzung des Subscription Services kann abweichend von der Anforderung "A_21556 - PS abgebende LEI: Häufigkeit des Abrufen von Nachrichten" die Operation GET /Communication häufiger als alle 5 Minuten, d.h. nach jeder Notification, mit den obigen Parametern angefragt werden.

Die Websocket Verbindung kann bis zu 12h bestehen. Danach muss das AVS die Subscription neu registrieren.

A_22379 - PS abgebende LEI: Subscription für neue Communication - Wartezeit
Der Primärsystem der abgebenden LEI KANN eine beliebige Wartezeit bis zum Abruf der Nachrichten mit Anwendungsfall „Nachrichten von Versicherten empfangen“ umsetzen, wenn in einem Zeitraum sehr viele ping-Benachrichtigungen empfangen werden. **[<=]**

Prüfverfahren: Herstellererklärung

Hinweis: Jede eingestellte Nachricht führt zu einem Ping, ggfs. im Millisekundenbereich, wenn viele Nachrichten an einen Empfänger gerichtet werden. In Abhängigkeit von der Implementierung kann dieses Verhalten zu einer Überlastung des PS führen, wenn bspw. jedes einzelne Ping den Anwendungsfall „Nachrichten von Versicherten empfangen“ triggert.