C_11198

E-Rezept-Fachdienst: Anpassung ILF Clientsysteme – Thema Health-Checks

Änderungsbedarf:

Es hat sich herausgestellt, dass viele Clientsysteme den Begriff der E-Rezept-Fachdienst-Verfügbarkeit mit unterschiedlichen Mitteln und in verschiedener Frequenz behandeln. Ursächlich ist, dass die Clientsysteme für ihren Endnutzer die Softwarefunktionalität uneingeschränkt zur Verfügung stellen wollen, was dazu führt, dass ein Großteil dieser Softwaresysteme die technischen und fachlichen Endpunkte des E-Rezept-Fachdienstes missbraucht, um eine (auch fehlerhafte) Antwort zu erhalten, z.B. mit der Nutzung eines bereits eingelösten E-Rezeptes. Die Antwort dieses Fehlers nutzen dann die Clientsysteme, um festzustellen, dass der E-Rezept-Fachdienst erreichbar und funktional ist.

Dieses Verhalten erzeugt jedoch neben ihrer Last auch spezifizierte und nachverfolgte Fehlerzustände, sodass Auswertungen zu tatsächlichen Fehlern nicht möglich sind oder stark erschwert werden. Dabei übersteigt bei einigen Clientsystemen die Last der fehlerhaften "Verfügbarkeitsaufrufe" bei weitem die Last des originären Anwendungsfalls.

Es soll angeregt werden, dass die Hersteller von Clientsoftware bedachter mit zentralen Ressourcen umgehen und die frequenten "Checks" nur dann einsetzen, wenn diese unumgänglich sind.

Darum ist es notwendig, die eingesetzten Clientsysteme hinsichtlich ihres Fehleraufkommens zu beobachten und bei Bedarf geeignete Maßnahmen durchzuführen, um den Betrieb des E-Rezept-Fachdienstes nicht weiter zu stören und diesen dadurch ebenfalls zu entlasten.

Anpassung in gemILF_PS_eRp

Einfügen eines neues Kapitels 4.3:

4.3 Health-Checks

Ein Health-Check ist eine https-Abfrage mit der Aufgabe, die Erreichbarkeit und damit gleichzeitig die Nutzbarkeit des E-Rezept-Fachdienstes festzustellen. Ein Health-Check dient nicht dazu, die fachliche Korrektheit des E-Rezept-Fachdienstes zu überprüfen. Ein Health-Check kann genutzt werden, um die Erreichbarkeit des E-Rezept-Fachdienstes zu überprüfen.

Endanwender müssen sich darauf verlassen können, dass vom Betreiber des E-Rezept-Fachdienstes nur Endpunkte zur Verfügung gestellt werden, deren fachliche Korrektheit und Funktionalität kontinuierlich intern überwacht werden. Dadurch kann der Hersteller eines Primärsystems davon ausgehen, dass – sofern eine Erreichbarkeit eines Endpunktes gegeben ist – auch die fachliche Korrektheit und damit die Verfügbarkeit des Dienstes gegeben sind. Der Betreiber des E-Rezept-Fachdienstes prüft periodisch, ob alle verbunden Backendsysteme in den festgelegten Parametern ordnungsgemäß funktionieren. Sollte dies nicht der Fall sein, so wird der entsprechende Host automatisiert vom Netz getrennt, wodurch keine Anfragen an ihn mehr stattfinden können.

Durch die kontinuierliche Weiterentwicklung und Sicherstellung dieses Verfahrens kann damit bei Erreichbarkeit des E-Rezept-Fachdienstes von einer Verfügbarkeit der angebotenen Endpunkte ausgegangen werden.

Da jeglicher Aufruf am E-Rezept-Fachdienst Last erzeugt, ist es notwendig, dass zur Art und Weise der Durchführung dieser Health-Checks eine klarere Regelung getroffen wird.

Es wird folgend eine Klassifikation der Health-Checks vorgenommen, um den tatsächlichen Anwendungsfall konkret zu unterstützen und transparent zu machen.

4.3.1 Erweiterter Health-Check

Ein erweiterter Health-Check ist ein spezieller Aufruf auf den Endpunkt **/metadata** mit der http-Methode GET im inneren, verschlüsselten http-Request an die /VAU ⇒ ("POST /VAU [GET /metadata]"). Ziel dieses Health-Checks soll es sein, die Anmeldung am E-Rezept-Fachdienst und dem damit einhergehenden VAU-Protokoll zur Ver- und Entschlüsselung zu überprüfen. Dabei wird ebenfalls das Access-Token überprüft, welches vorher am IDP abgeholt wurde. Dieses Verfahren soll in der produktiven Betriebsumgebung nur dann angewandt werden, wenn z.B. ein neuer Client in Betrieb genommen wird. Als Abfrage zum Systemstart darf dieser Health-Check nicht eingesetzt werden!

Spezialfall: Für Hersteller von Primärsystemen der abgebenden LEI ist, ersetzend zum o.g. Verfahren, die Nutzung von **/Subscription** mit der http-Methode POST im inneren, verschlüsselten http-Request an die /VAU vorzuziehen, da dieses Verfahren bereits dazu dient, die Verbindungen zum E-Rezept-Fachdienst auf einen WebSocket zu reduzieren ⇒ ("POST /VAU [POST /Subscription]").

4.3.2 Einfacher Health-Check

Ein einfacher Health-Check ist ein leichtgewichtiger Aufruf auf den Fachdienst-Endpunkt **/** (root) mit der http-Methode GET ("äußerer http-Request"), ohne eine zusätzliche VAU-Verschlüsselung ⇒ ("GET / [---]"). Ziel dieses Health-Checks soll es sein, die Verfügbarkeit des E-Rezept-Fachdienstes vom Clientsystem aus sicherzustellen. Dabei werden weder Access-Token noch Verschlüsselung benötigt, was ihn für wiederkehrende Abfragen optimiert. Dieses Verfahren soll in der produktiven Betriebsumgebung nur dann angewandt werden, wenn z.B. binnen einer festgelegten Periode vom Clientsystem keine Anfragen an den E-Rezept-Fachdienst gestellt worden sind. Der Health-Check soll nicht in festgelegten Zeitintervallen, unabhängig von fachlichen Anwendungsfällen benutzt werden – sondern soll erst bei einem echten Idle-Zeitraum Anwendung finden.

4.3.3 Festlegungen zum Verfahren mit Health-Checks

A_23214 - PS: Health-Check - Datensparsamkeit
Das Primärsystem MUSS auf Grundlage der Datensparsamkeit sicherstellen, dass neben den fachlich notwendigen Anfragen an den E-Rezept-Fachdienst so sparsam wie möglich mit Health-Checks umgegangen wird.**[**funkt. Eignung: Herstellererklärung, <=**]**

A_23215 - PS: Health-Check - keine Health-Checks mit Fehlerrückgabe
Das Primärsystem DARF NICHT einen Health-Check durchführen, welcher die erwartete Rückgabe eines Fehlercodes vorsieht.**[**funkt. Eignung: Herstellererklärung, <=**]**

A_23223 - PS: erweiterter Health-Check
Das Primärsystem KANN einen erweiterten Health-Check auf der Endpunkt ⇒ "POST /VAU [GET /metadata]" durchführen.
[funkt. Eignung: Herstellererklärung, <=**]**

A_23217 - PS: erweiterter Health-Check - keine periodische Durchführung
Das Primärsystem DARF NICHT einen erweiterten Health-Check periodisch durchführen, welcher periodisch den Endpunkt
⇒ "POST /VAU [GET /metadata]" abfragt.**[**funkt. Eignung: Herstellererklärung, <=**]**

Der Spezialfall für den Aufruf von ⇒ ("POST /VAU [POST /Subscription]") ist von dieser Regelung nicht betroffen.

A_23216 - PS: erweiterter Health-Check - keine anderen Endpunkte zulässig
Das Primärsystems DARF NICHT einen erweiterten Health-Check durchführen, welcher andere als die jeweils vorgegebenen Endpunkte des E-Rezept-Fachdienstes nutzt.**[**funkt. Eignung: Herstellererklärung, <=**]**

A_23219 - PS: einfacher Health-Check
Das Primärsystem KANN einen einfachen Health-Check auf der Endpunkt / (root) mit Abfrage ⇒ ("GET / [---]") durchführen, welcher mit Ausnahmen periodisch die Erreichbarkeit des E-Rezept-Fachdienstes feststellt und folgende Kriterien erfüllt:

1. Die festgelegte Idle-Periode darf 10 Minuten nicht unterschreiten.
2. Der Zeitraum zwischen den Aufrufen (Idle-Periode) muss um eine zufällige Zeitspanne zwischen 0 und 10.000 Millisekunden verlängert werden, um eine Gleichverteilung der Anfragen am E-Rezept-Fachdienst über alle Clientsysteme zu erreichen.

[funkt. Eignung: Herstellererklärung, <=**]**

Ausnahme bei technischen Störungen: Das Primärsystem darf einen weiteren einfachen Health-Check innerhalb der Idle-Periode durchführen, sofern ein fachlicher Aufruf die Nichterreichbarkeit des E-Rezept Fachdienstes zurückmeldet. Die Wiederholung des Health-Checks muss dann den Exponential Backoff-Algorithmus zur Wiederherstellung der erfolgreichen Verbindung umsetzen.

Ausnahme bei parallel durchgeführten, fachlichen Aufrufen: Das Primärsystem DARF KEINEN Health-Check durchführen, wenn innerhalb der festgelegten Idle-Periode ein regulärer Aufruf an einem beliebigen Endpunkt des E-Rezept-Fachdienstes mit erhaltener Antwort durchgeführt wurde. Die Antwort des E-Rezept-Fachdienstes MUSS die festgelegte Idle-Periode von Beginn starten lassen.

A_23218 - PS: einfacher Health-Check - keine anderen Endpunkte zulässig
Das Primärsystem DARF NICHT einen einfachen Health-Check durchführen, welcher einen anderen Endpunkt als ⇒ ("GET / [---]") abfragt.**[**funkt. Eignung: Herstellererklärung, <=**]**

Das Primärsystem soll zur Vermittlung der Erreichbarkeit an den Endnutzer geeignete Informationen bereitstellen, um die Fehlerursache der Nichterreichbarkeit transparent darzustellen. Fehlerursachen für die Nichterreichbarkeit können beispielsweise sein: die Verbindung zum Konnektor, Verfügbarkeit der SMC-B, Verbindung zum VPN oder andere.