
C_12136_Anlage - E-Rezept-Fachdienst: Abfrage von Daten vom FHIR-VZD

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Konzept asynchroner Zugriff.....	3
3 Datenschutz und Informationssicherheit.....	4
3.1 Kommunikation mit dem FHIR-VZD.....	4
3.2 Maßnahmen des E-Rezept-Fachdienstes.....	5
4 Änderungen in gemSpec_FD_eRp.....	6
4.1 Referenzierte Dokumente.....	6
4.1.1 Dokumente der gematik.....	6

1 Änderungsbeschreibung

Für das Feature "Einlösen von E-Rezepten im europäischen Ausland" (ePeD) und zukünftig weitere UseCases wird die Anbindung des E-Rezept-Fachdienst an den FHIR-VZD benötigt. Der FHIR-VZD ist nur über das Internet erreichbar. Um diese Anbindung zu realisieren, sind spezifikatorische Anpassungen vorzunehmen.

Diese Seite beschreibt das Konzept und konkrete Vorgehensweisen, um die Abfrage der Ländercodes, die das Feature ePeD unterstützen, zu realisieren.

Zur weiteren Beschreibung des Features und welche konkreten Anwendungsfälle dieses Konzept benötigt, siehe [gemF_eRp_EU].

2 Konzept asynchroner Zugriff

Um die Trusted Computing Base (TCB) der VAU zu minimieren, erfolgt die Abfrage von Informationen aus dem Internet nach Möglichkeit über einen Webservice (Agent) des E-Rezept-Fachdienstes. Die ermittelten Daten werden dann lokal in der Datenbank gespeichert und für die Nutzung in der VAU bereitgestellt.

Im diesem Konzept ist vorgesehen, dass eine Komponente des E-Rezept-Fachdienst asynchron Daten des FHIR-VZD abrufen und in eine Datenbank schreibt. Diese Daten können dann von der VAU genutzt werden. Dies erhöht die Performance und reduziert Sicherheitsrisiken für die VAU, da aus der VAU heraus keine Verbindung ins Internet notwendig ist.

Der Agent sorgt dafür, dass aus dem FHIR-VZD benötigten Daten in nach Anwendungsfall definierten Intervallen abgefragt und im E-Rezept-Fachdienst lokal vorgehalten werden.

Im Moment der Verarbeitung in der VAU wird auf die in der lokalen Datenbank abgelegten Daten zugegriffen und für die Verarbeitung genutzt.

Abbildung 1 beschreibt schematisch das Konzept zum asynchronen Zugriff des E-Rezept-Fachdienst auf den FHIR-VZD.

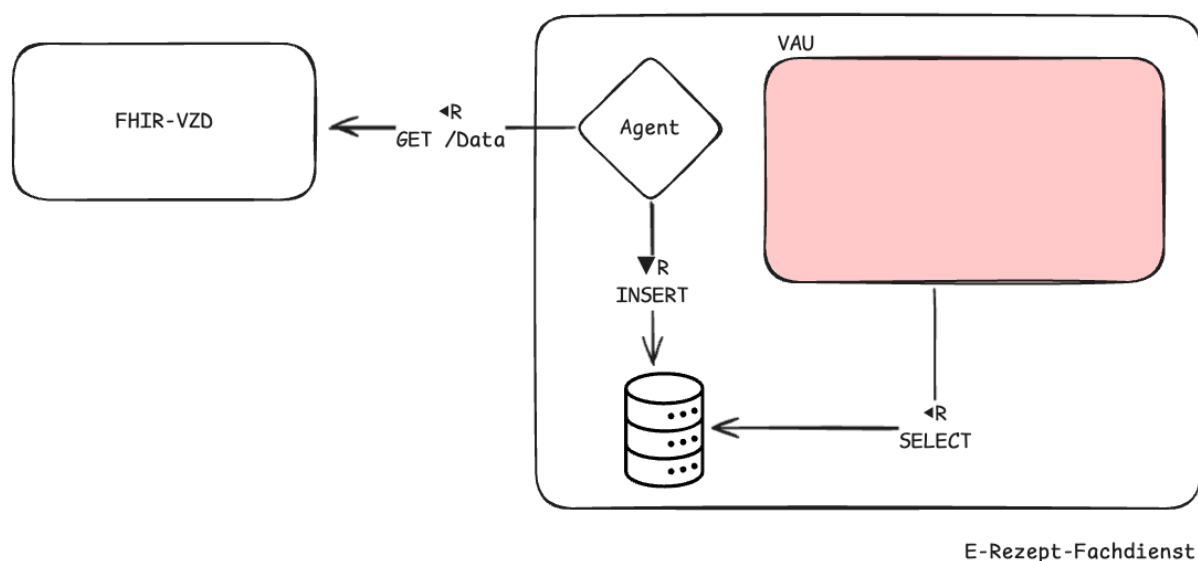


Abbildung 1: Konzept Abfrage des FHIR-VZD

3 Datenschutz und Informationssicherheit

Die Anbindung des E-Rezept-Fachdienstes an den FHIR-VZD ist eine neu zu etablierende Kommunikation, die erforderlich ist, um den Anwendungsfall des Ladens der Liste von Ländern, die das Feature ePeD zu unterstützen. Das dabei zu betrachtende Informationsobjekt ist die Liste mit den Ländercodes.

Der Schutzbedarf hierfür wird wie folgt festgelegt:

Informationsobjekt	Vertraulichkeit	Integrität
Liste der Ländercodes	niedrig Die Information über die teilnehmenden Länder ist öffentlich zugänglich.	hoch Ein Schaden für einen Versicherten kann entstehen, falls er sich in einem Land B befindet und sein E-Rezept nicht wie vorgesehen einlösen kann, weil der E-Rezept-Fachdienst dieses Land fälschlicher Weise nicht in der bei ihm gespeicherten Liste der Länder findet und damit die Anfrage ablehnt.

Die Verfügbarkeit des Prozesses zum Abruf der Liste beim FHIR-VZD wird mit "mittel" festgelegt, da die Änderungshäufigkeit dieser Liste gering ist und der E-Rezept-Fachdienst bei einer Nichtverfügbarkeit des Prozesses (z.B. bei Nichterreichbarkeit des FHIR-VZD) längere Zeit mit der lokalen Kopie arbeiten kann, ohne dass dadurch Sicherheitsrisiken entstehen.

3.1 Kommunikation mit dem FHIR-VZD

Die Kommunikation mit dem FHIR-VZD erfolgt mittels TLS. Dabei wird der FHIR-VZD mittels seines TLS-Dienstzertifikats vom E-Rezept-Fachdienst (Komponente Agent) authentifiziert. Die Verwendung von TLS gewährleistet ebenfalls die Integrität der Liste der Ländercodes bei der Übertragung.

Um missbräuchlichen Zugriff am FHIR-VZD zu vermeiden, ist es vorgesehen, dass ein Fachdienst über einen organisatorischen Prozess Client Credentials vom Betreiber des FHIR-VZD bezieht. Diese werden in einem Authentisierungsflow genutzt, um ein search-access-token vom FHIR-VZD Auth Service zu beziehen. Dieser Token wird dann für die Suche am FHIR-VZD genutzt.

Ref: [C_11785_Anlage#5.11 Fachdienst sucht Einträge im FHIR-Directory].

3.2 Maßnahmen des E-Rezept-Fachdienstes

Die Kommunikation des "Agent" mit der Datenbank, in der die Ländercodes abgelegt werden und die Kommunikation des Verarbeitungskontextes der VAU mit der Datenbank erfolgt unter den etablierten und geprüften Regeln und Maßnahmen des sicheren Betriebs des Anbieters des E-Rezept-Fachdienstes. Dies gilt für den Betrieb aller Komponenten im E-Rezept-Fachdienst.

4 Änderungen in gemSpec_FD_eRp

Der E-Rezept-Fachdienst darf keine unkontrollierten Verbindungen ins Internet herstellen, um zu verhindern, dass im Falle einer Kompromittierung der Fachlogik in der VAU unerwünschter Code nachgeladen wird.

Eine Ausnahme besteht bereits für OCSP-Abfragen, und es wird eine weitere Ausnahme für Anfragen an den FHIR-VZD hinzugefügt.

alt

A_19815 -E-Rezept-Fachdienst - Richtlinien für den Paketfilter zum Internet

Der Paketfilter des E-Rezept-Fachdienstes MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

1. HTTPS, und
2. OCSP-Zugriffe für das OCSP-Stapling nach A_20026 (vgl. Hinweis nach A_19815), ggf. notwendige DNS Anfragen (und Antworten)

Ein Verbindungsaufbau aus dem E-Rezept-Fachdienst in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 .

[<=,eRp_FD,Sich.techn. Eignung: Produktgutachten]

neu

A_19815-01 -E-Rezept-Fachdienst - Richtlinien für den Paketfilter zum Internet

Der Paketfilter des E-Rezept-Fachdienstes MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

1. HTTPS, und
2. OCSP-Zugriffe für das OCSP-Stapling nach A_20026 (vgl. Hinweis nach A_19815), ggf. notwendige DNS Anfragen (und Antworten)
3. Zugriff auf den FHIR-VZD

Ein Verbindungsaufbau aus dem E-Rezept-Fachdienst in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkten 2 und 3.

[<=,eRp_FD,Sich.techn. Eignung: Produktgutachten]

4.1 Referenzierte Dokumente

4.1.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber: Titel

[gemF_eRp_EU]	gematik: Feature: EU Zugriff E-Rezept
[C_11785_Anlage]	gematik:C_11785_Anlage