

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation E-Rezept-Fachdienst

Version: 1.12.0 CC  
Revision: 294994305794  
Stand: 09.12.11.2020  
Status: zur Abstimmung freigegeben  
Klassifizierung: öffentlich Entwurf  
Referenzierung: gemSpec\_FD\_eRp

## Dokumentinformationen

### Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.06.2020		freigegeben	gematik
1.0.1	06.07.2020		Aktualisierung Hinweis zu Dispensierinformation	gematik
1.1.0	12.11.2020		Einarbeitung gemäß Änderungsliste P22.2 / Scope-Themen zu R4.0.1	gematik
<a href="#">1.1.1</a>	<a href="#">13.11.2020</a>		<a href="#">Einarbeitung gemäß Änderungsliste P22.4</a>	<a href="#">gematik</a>
<a href="#">1.2.0 CC</a>	<a href="#">09.12.2020</a>		<a href="#">Einarbeitung gemäß Änderungsliste P22.5</a>	<a href="#">gematik</a>

36

## Inhaltsverzeichnis

37	<b>1 Einordnung des Dokumentes .....</b>	<b>5</b>
38	<b>1.1 Zielsetzung .....</b>	<b>5</b>
39	<b>1.2 Zielgruppe .....</b>	<b>5</b>
40	<b>1.3 Geltungsbereich .....</b>	<b>5</b>
41	<b>1.4 Abgrenzungen .....</b>	<b>5</b>
42	<b>1.5 Methodik .....</b>	<b>6</b>
43	1.5.1 Hinweis auf offene Punkte .....	6
44	<b>2 Systemüberblick .....</b>	<b>7</b>
45	<b>3 Systemkontext.....</b>	<b>9</b>
46	<b>3.1 Nachbarsysteme .....</b>	<b>9</b>
47	<b>3.2 Akteure und Rollen .....</b>	<b>9</b>
48	<b>4 Zerlegung des Produkttyps .....</b>	<b>11</b>
49	<b>5 Übergreifende Festlegungen .....</b>	<b>12</b>
50	<b>5.1 Servicelokalisierung .....</b>	<b>12</b>
51	<b>5.2 Authentifizierung von Nutzern.....</b>	<b>14</b>
52	5.2.1 Registrierung beim Identity Provider.....	14
53	5.2.2 Claims der Identitätsbestätigung.....	16
54	5.2.3 Verwaltung der Nutzersession.....	17
55	<b>5.3 Fehlercodes .....</b>	<b>19</b>
56	<b>5.4 Protokollierung.....</b>	<b>22</b>
57	<b>5.5 Löschfristen.....</b>	<b>25</b>
58	<b>5.6 Sicherheit .....</b>	<b>26</b>
59	5.6.1 Allgemeine Sicherheitsanforderungen .....	26
60	5.6.2 Identifikation des Clientsystems.....	27
61	5.6.3 Vertrauensraum der TI .....	28
62	5.6.4 Sicherheit der Netzübergänge.....	29
63	5.6.5 Vertrauenswürdige Ausführungsumgebung .....	31
64	5.6.5.1 Verarbeitungskontext.....	31
65	5.6.5.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld .....	33
66	5.6.5.3 Konsistenz des Systemzustands, Logging und Monitoring .....	35
67	5.6.5.4 Client-Verbindungen zum Verarbeitungskontext .....	35
68	<b>6 Funktionsmerkmale .....</b>	<b>37</b>
69	<b>6.1 Ressource Task.....</b>	<b>38</b>
70	6.1.1 HTTP-Operation GET.....	38
71	6.1.2 HTTP-Operation POST.....	39
72	6.1.2.1 POST /Task/\$create.....	40
73	6.1.2.2 POST /Task/<id>/\$activate .....	41

74	<i>6.1.2.3 POST /Task/&lt;id&gt;/\$accept.....</i>	<i>44</i>
75	<i>6.1.2.4 POST /Task/&lt;id&gt;/\$reject.....</i>	<i>45</i>
76	<i>6.1.2.5 POST /Task/&lt;id&gt;/\$close.....</i>	<i>45</i>
77	<i>6.1.2.6 POST /Task/&lt;id&gt;/\$abort.....</i>	<i>47</i>
78	<b>6.2 Ressource MedicationDispense.....</b>	<b>49</b>
79	6.2.1 HTTP-Operation GET /MedicationDispense .....	49
80	<b>6.3 Ressource Communication.....</b>	<b>50</b>
81	6.3.1 HTTP-Operation GET.....	50
82	6.3.1.1 GET /Communication/.....	51
83	6.3.2 HTTP-Operation POST.....	51
84	6.3.2.1 POST /Communication/.....	51
85	6.3.3 HTTP-Operation DELETE.....	53
86	6.3.3.1 DELETE /Communication/.....	53
87	<b>6.4 Ressource AuditEvent.....</b>	<b>54</b>
88	6.4.1 HTTP-Operation GET /AuditEvent .....	54
89	<b>6.5 Ressource Device .....</b>	<b>55</b>
90	<b>7 Informationsmodell .....</b>	<b>56</b>
91	<b>8 Anhang A – Verzeichnisse .....</b>	<b>58</b>
92	8.1 Abkürzungen .....	58
93	8.2 Glossar .....	58
94	8.3 Abbildungsverzeichnis.....	59
95	8.4 Tabellenverzeichnis .....	59
96	8.5 Referenzierte Dokumente.....	59
97	8.5.1 Dokumente der gematik.....	59
98	8.5.2 Weitere Dokumente.....	60
99		
100		

---

## 1 Einordnung des Dokumentes

---

### 1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps E-Rezept-Fachdienst.

### 1.2 Zielgruppe

Das Dokument richtet sich an den Hersteller des E-Rezept-Fachdienstes, sowie an Hersteller und Anbieter von weiteren Produkttypen der Fachanwendung E-Rezept.

### 1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) fest-gelegt und bekannt gegeben.

#### Schutzrechts-/Patentrechtshinweis

*Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.*

### 1.4 Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps <Produkttyp> verzeichnet.

134 Nicht Bestandteil des vorliegenden Dokumentes sind die informativen Ergänzungen zur  
 135 Nutzung der Schnittstellen des E-Rezept-Fachdienstes in der separaten API-  
 136 Dokumentation, sowie zur Profilierung der verwendeten FHIR-Ressourcen.

## 137 1.5 Methodik

138 Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in  
 139 eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in  
 140 Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL,  
 141 SOLL NICHT, KANN gekennzeichnet.

142

143 Sie werden im Dokument wie folgt dargestellt:

144 **<AFO-ID> - <Titel der Afo>**

145 Text / Beschreibung

146 [ $\leq$ ]

### 147 1.5.1 Hinweis auf offene Punkte

148 Themen, die noch intern geklärt werden müssen oder eine Entscheidung, sind wie folgt  
 149 im Dokument gekennzeichnet:

*Beispiel für einen offenen Punkt.*

150

151

---

## 2 Systemüberblick

---

152 Der E-Rezept-Fachdienst verwaltet E-Rezepte in der Telematikinfrastuktur als ein  
153 zentraler Ressourcenserver auf Basis des FHIR-Standards mit einer RESTful API. Die  
154 Rezepte werden dabei über eine eindeutige Ressourcen-ID (Rezept-ID) adressiert.  
155 Zusätzlich protokolliert der E-Rezept-Fachdienst alle Zugriffe auf ein E-Rezept für den  
156 Versicherten und verwaltet die Statusübergänge eines E-Rezepts. Für einen  
157 Nachrichtenaustausch zwischen Apotheken und Versicherten über die Verfügbarkeit von  
158 Medikamenten, die Belieferung von E-Rezepten und der Vertretung beim Einlösen eines  
159 E-Rezepts ist zusätzlich eine Kommunikation über den E-Rezept-Fachdienst möglich.

160 Der E-Rezept-Fachdienst realisiert die Vertraulichkeit und Integrität der verarbeiteten  
161 Daten über das Konzept der vertrauenswürdigen Ausführungsumgebung (VAU), die eine  
162 durchgängige Verschlüsselung der E-Rezepte und der dazu gehörigen Daten aus einer  
163 Kombination kryptografischer Verfahren während des Transports, der  
164 vertrauenswürdigen Verarbeitung und in der verschlüsselten Persistierung der Daten  
165 sicherstellt.

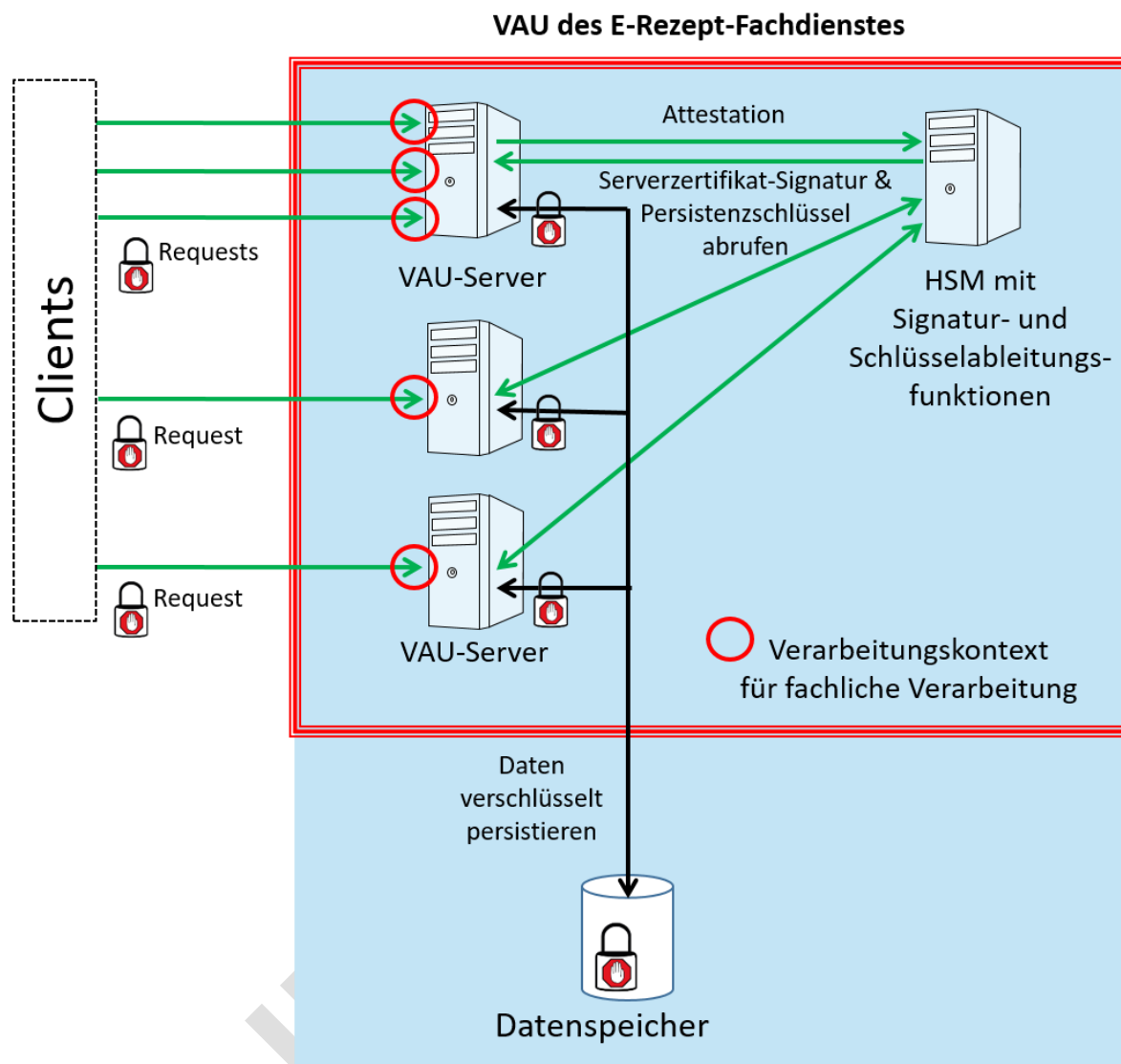


Abbildung 1: Systemüberblick



### 3 Systemkontext

Der E-Rezept-Fachdienst stellt Schnittstellen für die Verwaltung von E-Rezepten und für den Nachrichtenaustausch bereit. Diese werden von Leistungserbringerorganisationen und Versicherten genutzt, die über ihre jeweiligen Clientsysteme auf den E-Rezept-Fachdienst zugreifen.

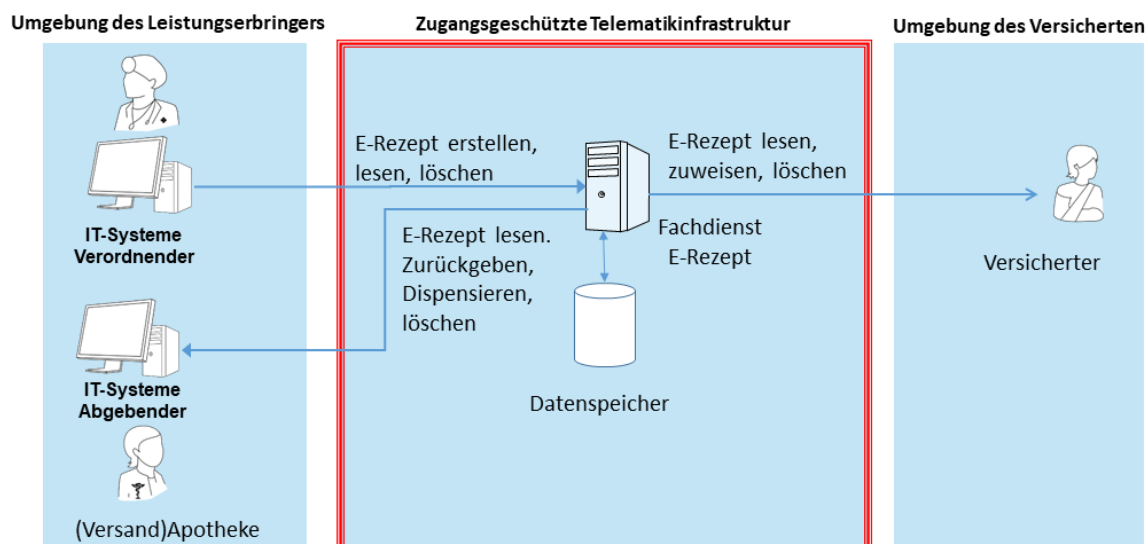


Abbildung 2: Systemkontext E-Rezept-Fachdienst

### 3.1 Nachbarsysteme

Die Schnittstellen des E-Rezept-Fachdienstes werden durch die Praxisverwaltungs- und Krankenhausinformationssysteme der verordnenden Leistungserbringer im Verordnungsprozess genutzt. Die Apothekenverwaltungssysteme nutzen die Schnittstellen des E-Rezept-Fachdienstes im Rahmen der Dispensierung. Außerdem werden sie vom E-Rezept-Frontend des Versicherten (E-Rezept-FdV) aufgerufen. Als Fachdienst der Telematikinfrastruktur bedient sich der E-Rezept-Fachdienst der weiteren Infrastrukturdienste wie TSP für die Gültigkeitsabfrage für Signaturzertifikate, des HBA (für QES-Prüfung) und des IdentityManagements, bei dem ein IDP Identitätsbestätigungen (ID\_TOKEN, ACCESS\_TOKEN) für Nutzer im Rahmen eines Sessionmanagements für das Single Sign-On ausstellt.

### 3.2 Akteure und Rollen

Leistungserbringerinstitutionen und Versicherte weisen sich gegenüber dem E-Rezept-Fachdienst mit einer Identitätsbestätigung (ACCESS\_TOKEN) aus, die sie von einem Identitätsprovider, z.B. SmartCard-IDP, beziehen. In diesen ACCESS\_TOKEN ist ihre Rollen-OID sowie ihr Identitätskennzeichen Versicherten-ID (10-stelliger unveränderlicher Anteil der KVNVR) bzw. Telematik-ID enthalten. Anhand der jeweiligen Rolle wird die Zulässigkeit einer aufgerufenen Operation geprüft. Das

- 193 Identitätskennzeichen wird für die Protokollierung von Zugriffen sowie die Zuordnung von  
194 Datensätzen, insbesondere bei E-Rezepten zu Versicherten, genutzt.

195

## 4 Zerlegung des Produkttyps

196 Der E-Rezept-Fachdienst verwaltet E-Rezepte über einen medizinischen Workflow. Dabei  
197 muss er die Vertraulichkeit und Integrität der verarbeiteten Daten sicherstellen. Daraus  
198 ergeben sich Sicherheitsanforderungen an die Betriebsumgebung, an die Fachlogik der  
199 Prozessverarbeitung sowie an die Ausführungsumgebung des Programmcodes.

### 200 **A\_19586 - Anbieter E-Rezept-Fachdienst Speicherung Schlüsselmaterial in HSM**

201 Der Anbieter des E-Rezept-Fachdienstes MUSS das private Schlüsselmaterial für  
202 kryptografische Verfahren (Entschlüsselung, Signaturen) in einem HSM speichern, dessen  
203 Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als  
204 Evaluierungsschemata kommen dabei Common Criteria, ITSEC oder Federal Information  
205 Processing Standard (FIPS) in Frage.  
206 Die Prüftiefe MUSS mindestens

- 207 1. FIPS 140-2 Level 3,
- 208 2. Common Criteria EAL 4+ mit hohem Angriffspotenzial oder
- 209 3. ITSEC E3 der Stärke „hoch“ entsprechen.

### 210 **[<=]**

211 Eine über die Schlüsselspeicherung in einem Hardware Security Module (HSM)  
212 hinausgehende Anforderung an die Zerlegung des E-Rezept-Fachdienstes gibt es aus  
213 funktionaler Sicht nicht.

## 5 Übergreifende Festlegungen

Der folgende Abschnitt beschreibt übergreifende Anforderungen an den E-Rezept-Fachdienst zur Unterstützung der Fachlogik.

### 5.1 Servicelokalisierung

Die Schnittstellen des E-Rezept-Fachdienstes werden über verschiedene Netzsegmente von Leistungserbringern und Versicherten aufgerufen. Dafür müssen diese Schnittstellen über DNS-Abfragen lokalisierbar sein.

#### ~~A\_19410 – Anbieter E-Rezept-Fachdienst – PTR für Anbieterliste (RFC Service-Discovery)~~

~~Der Anbieter des E-Rezept-Fachdienstes MUSS DNS-PTR, SRV und TXT Resource Records im Namensraum der TI gemäß folgender Tabelle verwalten.~~

~~Tabelle 1: TAB\_eRPFD\_001 Service-Discovery~~

<del>Resource-Record Bezeichner</del>	<del>Resource Record Type</del>	<del>Beschreibung</del>
<del>_erp._tcp.erp.ti- dienste.de</del>	<del>PTR</del>	<del>Ermittlung der E-Rezeptschnittstelle &lt;erp_service_name&gt;</del>
<del>—&lt;erp_service_name&gt;</del>	<del>SRV und TXT</del>	<del>SRV Resource Record zur Ermittlung des FQDN des E-Rezept-Dienstes TXT Resource Record zur Ermittlung des Pfades der URL zum E-Rezept-Dienst "path=&lt;Bezeichner der Schnittstelle als Pfadbestandteil (ohne /)&gt;"</del>

~~[<=>]~~

~~Der Eintrag <erp\_service\_name> ist als Variable zu verstehen und kann zum Beispiel für die Namensauflösung durch die Primärsysteme folgende Ausprägung besitzen:~~

~~\_erp.\_tcp.erp.ti-dienste.de 86400 IN PTR \_erp-fd.\_tcp.erp.ti-dienste.de~~  
~~\_erp-fd.\_tcp.erp.ti-dienste.de 86400 IN SRV 5 10 443 \_erp-~~  
~~srv.zentral.erp.ti-dienste.de~~  
~~\_erp-fd.\_tcp.erp.ti-dienste.de 86400 IN TXT „txtvers=1“ „path=/“~~

#### ~~A\_19411 – Anbieter E-Rezept-Fachdienst – Resource Records FQDN-eRP~~

~~Der Anbieter des E-Rezept-Fachdienstes MUSS im Namensraum der TI und in den Nameservern Internet die Resource Records gemäß nachstehender Tabelle verwalten.~~

Tabelle 2: TAB\_eRPFD\_002 FQDN

Resource Record Bezeichner	Resource Record Type	Beschreibung
<del>erp-srv.zentral.erp.ti-dienste.de</del>	A Record	<del>A Resource Records zur Namensauflösung von FQDN des E-Rezept-Fachdienstes in IP-Adressen im Namensraum der TI</del>
<del>erp-srv.zentral.erp.ti-dienste.de</del>	A Record	<del>A Resource Records zur Namensauflösung von FQDN des E-Rezept-Fachdienstes in IP-Adressen im Namensraum Internet</del>
<del>erp-srv.zentral.erp.ti-dienste.de</del>	AAAA Record	<del>AAAA Resource Records zur Namensauflösung von FQDN des E-Rezept-Fachdienstes in IP-Adressen im Namensraum Internet</del>
<del>_erp._tcp.erp.ti-dienste.de</del>	TXT	<p><del>TXT Resource Records zur Ermittlung der Aufruf-Schnittstelle des E-Rezept-Fachdienstes. Der für die Adressierung benötigte Resource Record MUSS bereitgestellt werden. Das in den Klammern angegebene Kürzel MUSS verwendet werden.</del></p> <ul style="list-style-type: none"> <li><del>• E-Rezept-Schnittstelle (erp)</del></li> <li><del>• OCSP-Status-Proxy (ocspf)</del></li> </ul> <p><del>Das key/value-Paar des TXT-Records hat folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes):</del></p> <p><del>"erp=&lt;Schnittstelle E-Rezept&gt;"</del></p>

**[<=]**

Exemplarisch können die DNS-Einträge im Namensraum Internet für den E-Rezept-Fachdienst wie folgt aussehen:

~~\_erp.\_tcp.erp.ti-dienste.de 86400 IN TXT „txtvers=1“ „path=“~~

~~erp-srv.zentral.erp.ti-dienste.de IN A 10.28.2.42~~

~~erp-srv.zentral.erp.ti-dienste.de IN AAAA~~

## **A 19412-01A\_19412 - Anbieter E-Rezept-Fachdienst - Schnittstellenadressierung**

Der Anbieter des E-Rezept-Fachdienstes MUSS die den Primärsystemen und die im Internet angebotene Schnittstelle angebotenen Schnittstellen des E-Rezept-Fachdienstes unter derden folgenden URLs zur Verfügung stellen:

- ~~https://<FQDN aus DNS Lookup>:443/<Aufrufschnittstelle aus TXT Record "path">~~

~~z.B.: //erp.zentral.erp.splitdns.ti-dienste.de/VAU - Schnittstelle E-Rezept~~

- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAUCertificate> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAUCertificateOCSPResponse> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.zentral.erp.splitdns.ti-dienste.de/ocspf> - Schnittstelle OCSP-Forwarder
- <https://erp.zentral.erp.splitdns.ti-dienste.de/TSL.xml> - Schnittstelle Download TSL-Datei
- <https://erp.zentral.erp.splitdns.ti-dienste.de/TSL.sha2> - Schnittstelle Download Hashwert TSL-Datei
- <https://erp.zentral.erp.splitdns.ti-dienste.de/.well-known> - Schnittstelle well-known locations
- <https://erp.zentral.erp.splitdns.ti-dienste.de/CertList>
- <https://erp.zentral.erp.splitdns.ti-dienste.de/OCSPList>

#### [<=]

Um Benutzern den Umgang mit E-Rezepten zu erleichtern, wird die Nutzung der Endnutzeranwendung E-Rezept-FdV als App auf ihrem privaten Smartphone empfohlen. Der E-Rezept-Fachdienst unterstützt dabei die App-Nutzung durch Digital Asset Links (für Android) [DAL\_ANDROID] und Universal Links (für iOS/macOS) [UL\_APPLE].

#### **A\_19695 - E-Rezept-Fachdienst - Android Digital Asset Link**

Der E-Rezept-Fachdienst MUSS ein Asset Link Statement gemäß [DAL\_ANDROID] mit der Liste der Hashwerte der aktuell zugelassenen Android-Versionen des E-Rezept-FdV für den Wert "sha256\_cert\_fingerprints" unter der Internetadresse <https://<FQDN für DNS Lookup>/.well-known/assetlinks.json> veröffentlichen und pflegen, damit Versicherte mit einem Android-Smartphone E-Rezepte standardmäßig mit dem E-Rezept-FdV verwalten können. [<=]

## **5.2 Authentifizierung von Nutzern**

Die Identifikation von Nutzern erfolgt nach dem Standard OpenID-Connect, hierfür stellt ein Identity Provider der Telematikinfrastruktur ACCESS\_TOKEN für Nutzer aus, die er anhand ihrer identifizierenden Merkmale (z.B. eGK, SMC-B) authentifiziert.

### **5.2.1 Registrierung beim Identity Provider**

Der E-Rezept-Fachdienst delegiert die Authentifizierung von Nutzern an einen Identity Provider. Für diesen Zweck muss er sich bei diesem als Relying Party registrieren und die für die Fachlogik notwendigen Attribute in den Identitätsbestätigungen (ACCESS\_TOKEN) festlegen. Die Umsetzung des IdentityManagements über Identity Provider startet mit einem einzelnen IDP (Smartcard-IDP), später werden weitere Identity Provider bei den verschiedenen identitätsbestätigenden Stellen realisiert. Verwaltet ein solcher IDP Identitäten von Nutzern der Telematikinfrastruktur und gilt als vertrauenswürdig für die Umsetzung von UseCases unter Nutzung der Schnittstellen des E-Rezept-Fachdienstes, obliegt es dem E-Rezept-Fachdienst, sich bei diesem IDP als **RelyingParty** zu registrieren.

**A\_19985-01A\_19985 - Anbieter E-Rezept-Fachdienst - Registrierung beim IDP als Relying Party**

Der Anbieter des E-Rezept-Fachdienstes MUSS sich über einen organisatorischen Prozess bei einem vertrauenswürdigen Identity Provider (IDP) der Telematikinfrastruktur als Relying Party registrieren und die Bereitstellung der folgenden Claims in für Nutzer ausgestellte ACCESS\_TOKEN mit dem IDP vereinbaren:

- professionOID
- given\_name
- family\_name
- organizationName
- idNummer
- acr
- aud

damit der E-Rezept-Fachdienst die Fachlogik der Autorisierung und Protokollierung auf diesen Attributen umsetzen kann. [ $\leq$ ]

**A\_20706 - Anbieter E-Rezept-Fachdienst - Claims für ID\_TOKEN für FdV**

Der Anbieter des E-Rezept-Fachdienstes MUSS bei der Registrierung als Relying Party im IDP die Bereitstellung der folgenden Claims in für Nutzer ausgestellte ID\_TOKEN mit dem IDP vereinbaren:

- professionOID
- given\_name
- family\_name
- organizationName
- idNummer
- acr

damit ein E-Rezept-Client diese Informationen bei Bedarf auswerten kann. [ $\leq$ ]

**A\_20754 - Anbieter E-Rezept-Fachdienst - Registrierung Scope**

Der Anbieter des E-Rezept-Fachdienstes MUSS bei der Registrierung als Relying Party im IDP das Attribut "Scope" mit dem Wert "openid profile prescriptionservice.lei" zur Nutzung durch Primärsysteme und dem Wert "openid profile prescriptionservice.vers" zur Nutzung durch Clients der Internetschnittstelle beantragen. [ $\leq$ ]

**A\_19986 - Anbieter E-Rezept-Fachdienst - E-Rezept-Sessiondauer im IDP**

Der Anbieter des E-Rezept-Fachdienstes MUSS bei der Registrierung als Relying Party im IDP die Ausstellung von ACCESS\_TOKEN für authentifizierte Nutzer für die maximale Dauer von 12 Stunden erlauben, sodass der IDP spätestens 12 Stunden nach auth\_time eine Re-Authentifizierung des Nutzers erzwingt. [ $\leq$ ]

**A\_20710 - Anbieter E-Rezept-Fachdienst - E-Rezept-Lebensdauer ACCESS\_TOKEN**

Der Anbieter des E-Rezept-Fachdienstes MUSS bei der Registrierung als Relying Party im IDP eine Lebensdauer von ausgestellten ACCESS\_TOKEN durch den IDP für die Berechnung des Werts "tokenTimeout" von 300 Sekunden festlegen. [ $\leq$ ]

### **A\_19987 - Anbieter E-Rezept-Fachdienst - URI für öffentl. Schlüssel Tokenverschlüsselung**

Der Anbieter des E-Rezept-Fachdienstes MUSS bei der Registrierung als Relying Party im IDP die beiden URI bzw. FQDN der Schnittstellen im Namensraum der TI und im Internet sowie die Abrufadresse des öffentlichen Schlüssels PUK\_FD mit Angabe des zu verwendenden Algorithmus für die Verschlüsselung des ACCESS\_TOKEN dem Identity Provider bekannt machen. [ $\leq$ ]

### **A\_19993 - E-Rezept-Fachdienst - Prüfung eingehender ACCESS\_TOKEN**

Der E-Rezept-Fachdienst MUSS jedes mit einem eingehenden HTTP-Request übergebene ACCESS\_TOKEN gemäß der Festlegungen in [gemSpec\_IDP\_FD#Kapitel 6 ACCESS\_TOKEN] prüfen und Fehler bzw. ungültige Token gemäß dieser Festlegungen und dem HTTP-Status-Code 401 abweisen. [ $\leq$ ]

## **5.2.2 Claims der Identitätsbestätigung**

### **A\_19130 - E-Rezept-Fachdienst - Authentifizierung erforderlich LEI-Endpunkt**

Der E-Rezept-Fachdienst MUSS alle eingehenden HTTP-Requests über den Endpunkt für Leistungserbringerinstitutionen mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "WWW-Authenticate: Bearer realm='prescriptionserver.telematik'

scope=openid profile prescriptionservice.lei"abweisen, die kein ACCESS\_TOKEN als JSON-Web-Token-Format gemäß [JWT] im HTTP-Request-Header "Authorization" bereitstellen, damit ausschließlich authentifizierte Nutzer Zugriff auf die HTTP-Schnittstelle des E-Rezept-Fachdienstes erhalten. [ $\leq$ ]

### **A\_19389 - E-Rezept-Fachdienst - Authentifizierung erforderlich Vers-Endpunkt**

Der E-Rezept-Fachdienst MUSS alle eingehenden HTTP-Requests über den Endpunkt für den Zugriff für Versicherte mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "WWW-Authenticate: Bearer realm='prescriptionserver.telematik'

scope=openid profile prescriptionservice.vers"abweisen, die kein ACCESS\_TOKEN als JSON-Web-Token-Format gemäß [JWT] im HTTP-Request-Header "Authorization" bereitstellen, damit ausschließlich authentifizierte Nutzer Zugriff auf die HTTP-Schnittstelle des E-Rezept-Fachdienstes erhalten. [ $\leq$ ]

### **A\_19131 - E-Rezept-Fachdienst - Authentifizierung ungültig**

Der E-Rezept-Fachdienst MUSS alle eingehenden HTTP-Requests mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "WWW-Authenticate: Bearer realm='prescriptionserver.telematik', error='invalidACCESS\_TOKEN'" abweisen, die ein unsigniertes oder ungültiges ACCESS\_TOKEN im HTTP-Request-Header "Authorization" bereitstellen, damit ausschließlich authentifizierte Nutzer Zugriff auf die HTTP-Schnittstelle des E-Rezept-Fachdienstes erhalten. [ $\leq$ ]

### **A\_19902 - E-Rezept-Fachdienst - Authentifizierung abgelaufen**

Der E-Rezept-Fachdienst MUSS alle eingehenden HTTP-Requests mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "WWW-Authenticate: Bearer realm='prescriptionserver.telematik', error='invalidACCESS\_TOKEN'" abweisen, die ein ACCESS\_TOKEN im HTTP-Request-Header "Authorization" bereitstellen, dessen Gültigkeitsendezeitpunkt "exp" älter als die aktuelle Systemzeit oder dessen Ausstellzeitpunkt "iat" älter als die aktuelle Systemzeit - 5 Minuten ist, damit ausschließlich authentifizierte Nutzer Zugriff auf die HTTP-Schnittstelle des E-Rezept-Fachdienstes erhalten. [ $\leq$ ]

### **A\_19132 - E-Rezept-Fachdienst - Authentifizierung Signaturprüfung**

Der E-Rezept-Fachdienst MUSS die Signatur jedes im HTTP-Header "Authorization" eines eingehenden HTTP-Requests übergebenen JSON-Web-Tokens gemäß [JWS] prüfen und



385 bei Ungültigkeit oder bei Signatur durch einen Identity Provider, bei dem der E-Rezept-  
386 Fachdienst nicht als Relying Party registriert ist, den HTTP-Request mit dem HTTP-  
387 Fehlercode 401 abweisen. [≤]

#### 388 **A\_19390 - E-Rezept-Fachdienst - Authentifizierung Nutzerrolle**

389 Der E-Rezept-Fachdienst MUSS die fachliche Rolle eines Nutzers in jedem  
390 Operationsaufruf anhand des Attributs "professionOID" im übergebenen IDP-Token im  
391 HTTP-Header "Authorization" feststellen und für die nachfolgende Rollenprüfung je  
392 Operationsaufruf verwenden. [≤]

#### 393 **A\_19391 - E-Rezept-Fachdienst - Authentifizierung Nutzername**

394 Der E-Rezept-Fachdienst MUSS den Namen eines Nutzers in jedem Operationsaufruf  
395 anhand der Attribute "given\_name", "family\_name" und "organizationName" im  
396 übergebenen IDP-Token im HTTP-Header "Authorization" feststellen und für die  
397 Protokollierung des Zugriffs auf personenbezogene medizinische Daten je  
398 Operationsaufruf verwenden. [≤]

#### 399 **A\_19392 - E-Rezept-Fachdienst - Authentifizierung Nutzerkennung**

400 Der E-Rezept-Fachdienst MUSS die Nutzerkennung (10-stelliger Teil der KVNR,  
401 Telematik-ID für Leistungserbringerinstitutionen) eines Nutzers in jedem  
402 Operationsaufruf anhand des Attributs "idNummer" im übergebenen IDP-Token im HTTP-  
403 Header "Authorization" feststellen und für die Protokollierung des Zugriffs auf  
404 personenbezogene medizinische Daten je Operationsaufruf verwenden. [≤]

#### 405 **A\_19439 - E-Rezept-Fachdienst - Authentifizierung Authentifizierungsstärke**

406 Der E-Rezept-Fachdienst MUSS die Authentifizierungsstärke des übergebenen IDP-Token  
407 anhand des Attributs "acr" im übergebenen IDP-Token im HTTP-Header "Authorization"  
408 auf dem Authentifizierungsniveau "hoch" feststellen und einen anderen Wert als bzw. ein  
409 Authentifizierungsniveau unterhalb von "<http://eidas.europa.eu/LoA/high>" mit dem  
410 HTTP-Status-Code 401 ablehnen. [≤]

### 411 **5.2.3 Verwaltung der Nutzersession**

412 Der Identity Provider übernimmt für den E-Rezept-Fachdienst als Relying Party die  
413 Verwaltung von Nutzersessions und stellt dem Client während der Gültigkeit der  
414 Nutzersession ACCESS\_TOKEN für den Zugriff auf den E-Rezept-Fachdienst aus. Der E-  
415 Rezept-Fachdienst prüft diese ACCESS\_TOKEN auf Gültigkeit gemäß der Festlegungen in  
416 [gemSpec\_IDP\_FD].

#### 417 **A\_19992 - E-Rezept-Fachdienst - Blocklisting zu häufig verwendeter** 418 **ACCESS\_TOKEN**

419 Der E-Rezept-Fachdienst MUSS ein während einer konfigurierbaren Dauer vielfach  
420 vorgelegtes ACCESS\_TOKEN (z.B. mehr als 10 mal innerhalb einer Sekunde) für den Rest  
421 der angegebenen Gültigkeitsdauer auf einer Blocklist führen und eingehende HTTP-  
422 Requests mit diesem ACCESS\_TOKEN mit dem HTTP-Status-Code 429 ablehnen, damit  
423 ein Überlastungsangriff (DOS-Attacke) auf den E-Rezept-Fachdienst unterbunden werden  
424 kann. [≤]

#### 425 **~~A\_20158-01A-20158~~ - E-Rezept-Fachdienst - Prüfung Signaturzertifikat IDP**

426 Der E-Rezept-Fachdienst MUSS mindestens einmal täglich das Signatur-Zertifikat des  
427 IDP-Dienstes für die Signatur von ACCESS\_TOKEN gemäß [gemSpec\_PKI#TUC\_PKI\_018]  
428 mit folgenden Parametern auf Gültigkeit prüfen:

429 **Tabelle 1: TAB\_eRPFD\_005 Parameter Prüfung Signaturzertifikat IDP**

Parameter	
Zertifikat	Signaturzertifikat des IDP ( <del>eingebettet in ACCESS_TOKEN</del> ) C.FD.SIG ( <u>wird im Discovery Document referenziert, siehe [gemSpec IDP Dienst#Kapitel 4]</u> )
PolicyList	oid_fd_sig
intendedKeyUsage	nonRepudiation
intendedExtendedKeyUsage	(leer)
OCSP-Graceperiod	60 Minuten
Offline-Modus	nein
Prüfmodus	OCSP

430 Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND  
 431 zeitlich gültig UND online gültig ] befunden werden und der HTTP-Request andernfalls mit  
 432 dem HTTP-Status-Code 401 abgelehnt werden, damit sichergestellt wird dass,  
 433 ausschließlich ACCESS\_TOKEN von einem vertrauenswürdigen IDP akzeptiert  
 434 werden.[<=]

#### 436 **A\_20765 - E-Rezept-Fachdienst - Prüfung Signaturzertifikat E-Rezept-** 437 **Fachdienst**

438 Der E-Rezept-Fachdienst MUSS sein Signatur-Zertifikat für die Signatur der E-Rezept-  
 439 Quittung gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit folgenden Parametern auf Gültigkeit  
 440 prüfen:

441 **Tabelle 2: TAB\_eRPFD\_010 Parameter Prüfung Signaturzertifikat**

Parameter	
Zertifikat	Signaturzertifikat des E-Rezept-Fachdienstes C.FD.SIG
PolicyList	oid_fd_sig
intendedKeyUsage	nonRepudiation
intendedExtendedKeyUsage	(leer)
OCSP-Graceperiod	60 Minuten
Offline-Modus	nein
Prüfmodus	OCSP

Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig ] befunden werden und eingehende HTTP-Request zur Erstellung einer Quittung andernfalls mit dem HTTP-Status-Code 500 abgelehnt werden, damit sichergestellt wird, dass ausschließlich Quittungen mit einem gültigen Signaturzertifikat erstellt werden. [ <= ]

#### **A\_20974 - E-Rezept-Fachdienst - Prüfungsintervall Signaturzertifikat E-Rezept-Fachdienst**

Der E-Rezept-Fachdienst MUSS mindestens einmal täglich sein Signatur-Zertifikat für die Signatur der E-Rezept-Quittung auf Gültigkeit prüfen. [ <= ]

### **5.3 Fehlercodes**

Der E-Rezept-Fachdienst stellt eine http-Schnittstelle für den Aufruf durch Clientsysteme bereit. Das Ergebnis der Operation wird in der Verwendung von [http-StatusCodes](#) [HTTP-STATUS-CODES] mitgeteilt. Die folgende Tabelle listet die vom E-Rezept-Fachdienst genutzten [http-StatusCodes](#) auf.

#### **A\_19514 - E-Rezept-Fachdienst - Http-Status-Codes**

Der E-Rezept-Fachdienst MUSS die in der folgenden Tabelle aufgelisteten HTTP-Status-Codes im http-Response-Header der aufgerufenen Operation gemäß der angegebenen Bedingung zurückgeben.

**Tabelle 3: TAB\_eRPFD\_003 Übersicht HTTP-Statuscodes**

HTTP-Status-Code	Bedeutung	in welchen Operationen als Statuscode möglich	Bedingung
200	Operation erfolgreich beendet, in der Rückgabe ist ggfs. das Ergebnis der Operation enthalten	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/<id>/\$activate POST /Task/<id>/\$accept POST /Task/<id>/\$close GET /notifications/opt-in GET /notifications/opt-out GET, etc für alle übrigen Operationen	Die Operation wurde erfolgreich bearbeitet. In der Rückgabe sind die erzeugten bzw. gelesenen Daten enthalten.
201	Neues Objekt wurde erfolgreich angelegt, in der Rückgabe ist das Objekt enthalten	POST /Task/<id>/\$create POST /Communication	Der E-Rezept-Fachdienst hat die Ressource in der angeforderten Operation erzeugt.
204	Die Operation liefert keinen Rückgabewert	POST /Task/<id>/\$abort POST /Task/<id>/\$reject	Das Löschen eines E-Rezepts löscht alle personenbezogenen und medizinischen Daten,

			daher gibt es keine Daten in der Rückgabe der Operation. Das Zurückweisen eines Rezepts bedeutet die Nicht-Bearbeitung durch eine Apotheke, daher sind hier keine Rückgabedaten erforderlich.
400	Bad Request, der Operationsaufruf enthält ungültige Daten.	POST /Task/\$create POST /Task/<id>/\$activate POST /Task/<id>/\$accept POST /Task/<id>/\$reject POST /Task/<id>/\$close POST /Task/<id>/\$abort POST /Communication GET /notifications/opt-in GET, POST, etc für alle übrigen Operationen	In der aufgerufenen Operation werden vom Client Daten für die Verarbeitung erwartet. Entsprechen sie nicht dem erwarteten FHIR-Profil oder sind sie ungültig (bspw. Signatur), werden sie vom E-Rezept-Fachdienst zurückgewiesen.
401	Der Nutzer konnte nicht authentifiziert werden	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/\$create POST /Task/<id>/\$activate POST /Task/<id>/\$accept POST /Task/<id>/\$reject POST /Task/<id>/\$close POST /Task/<id>/\$abort POST /Communication	Der Aufruf enthält keine oder abgelaufene oder ungültige Authentifizierungsinformationen im HTTP-Request-Header "Authorization"
403	Der Nutzer ist nicht berechtigt, die aufgerufene Operation anzufordern	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/\$create POST /Task/<id>/\$activate POST /Task/<id>/\$accept POST /Task/<id>/\$reject POST /Task/<id>/\$close POST /Task/<id>/\$abort POST /Communication	Gemäß Rollenprüfung in jedem Operationsaufruf sind nur bestimmte Operationen je aufrufendem Nutzer zulässig.
404	Die adressierte Ressource wurde nicht gefunden.	GET /Task/<id> POST /Task/<id>/\$activate POST /Task/<id>/\$accept	Die über die <id> adressierte Ressource existiert nicht, d.h. wurde auch nicht

		POST /Task/<id>/\$reject POST /Task/<id>/\$close POST /Task/<id>/\$abort GET /AuditEvent/<id> GET /Communication/<id> GET /MedicationDispense/<id> > GET /notifications/opt-out	zwischenzeitlich gelöscht (siehe Code 410).
405	Die Anfrage ist gültig, jedoch in Kombination mit anderen Aufrufparametern nicht gültig	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/\$create POST /Task/<id>/\$activate POST /Task/<id>/\$accept POST /Task/<id>/\$reject POST /Task/<id>/\$close POST /Task/<id>/\$abort POST /Communication	In der Operation wird eine unzulässige Kombination aus http-Operation auf eine bestimmte Ressource ggfs. in Verbindung mit einer FHIR-Operation aufgerufen, z.B. POST /AuditEvent POST /Task/\$activate POST /Task/<id>/\$create PUT /<Ressource>/ HEAD /<Ressource> DELETE /<Ressource>/ PATCH /<Ressource>
408	Request Timeout. Die Anfrage konnte innerhalb der erwarteten Zeit nicht beantwortet werden	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/\$create POST /Task/<id>/\$activate POST /Task/<id>/\$accept POST /Task/<id>/\$reject POST /Task/<id>/\$close POST /Task/<id>/\$abort POST /Communication	Der E-Rezept-Fachdienst ist überlastet und kann die Anfrage innerhalb der Wartezeit des Clients (PVS, AVS, FdV) nicht beantworten
409	Konflikt im Aufruf verschiedener Nutzer um das gleiche Objekt	POST /Task/<id>/\$accept POST /Task/<id>/\$abort	Das E-Rezept befindet sich bereits in Belieferung durch einen Apotheker. Daher kann es vom Verordnenden und Versicherten nicht gelöscht werden (\$abort) und von keinem anderen Apotheker heruntergeladen werden (\$accept)
410	Das aufgerufene Objekt wurde	GET /Task/<id> POST /Task/<id>/\$accept POST /Task/<id>/\$abort	Der Client (PVS, AVS, FdV) versucht ein E-Rezept zu lesen,

	zwischenzeitlich gelöscht		das zwischenzeitlich gelöscht wurde
429	Der Client hat zu viele Aufrufe innerhalb einer festgelegten Zeitspanne getätigt	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/\$create POST /Task/<id>/\$activate POST /Task/<id>/\$accept POST /Task/<id>/\$reject POST /Task/<id>/\$close POST /Task/<id>/\$abort POST /Communication	Der Client (PVS, AVS, FdV) hat innerhalb des konfigurierten Zeitabschnitts zu viele Requests geschickt
500	Interner Serverfehler	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/\$create POST /Task/<id>/\$activate POST /Task/<id>/\$accept POST /Task/<id>/\$reject POST /Task/<id>/\$close POST /Task/<id>/\$abort POST /Communication GET, POST, etc für alle übrigen Operationen	In allen Operationen, die aufgrund eines internen Fehlers nicht bearbeitet werden können. Die Rückgabe liefert keine weiteren Informationen.

462 [**<=**]463 **5.4 Protokollierung**

464 Der E-Rezept-Fachdienst soll Protokolldateien schreiben, die eine Analyse technischer  
 465 Vorgänge erlauben. Diese Protokolldateien sind dafür vorgesehen, aufgetretene Fehler zu  
 466 identifizieren und die Performance zu analysieren. Für diese Zwecke führt der E-Rezept-  
 467 Fachdienst ein Systemprotokoll, mit dem der Anbieter des Dienstes jederzeit den  
 468 Betriebszustand des Systems kontrollieren kann.

469 **A\_19282 - E-Rezept-Fachdienst - Systemprotokoll für Betriebszustand**

470 Der E-Rezept-Fachdienst MUSS ein Systemprotokoll über durchgeführte Operationen und  
 471 deren Erfolg/Misserfolg führen, um dem Anbieter des Dienstes jederzeit eine Übersicht  
 472 über den aktuellen Betriebszustand zu ermöglichen. [**<=**]

473 **A\_19283 - E-Rezept-Fachdienst - Systemprotokoll ohne personenbezogene und  
474 ohne medizinische Daten**

475 Der E-Rezept-Fachdienst MUSS in jedem zu tätigenden Systemprotokolleintrag alle  
 476 personenbezogenen, personenbeziehbaren und medizinischen Informationen vor der

477 Speicherung entfernen, damit vom administrativen Personal keine personenbezogenen  
478 Daten der Versicherten oder Leistungserbringer eingesehen werden können.[<=]

479 **A\_19678 - E-Rezept-Fachdienst -Systemprotokoll Verfügbarkeit interner**  
480 **Logdaten**

481 Der Betreiber des E-Rezept-Fachdienstes MUSS im Rahmen von Testmaßnahmen dem  
482 Testbetriebsverantwortlichen auf Anforderung die Log-Dateien des Systemprotokolls  
483 übermitteln.[<=]

484 **A\_20001 - E-Rezept-Fachdienst -Systemprotokoll zu Ergebnis einer**  
485 **aufgerufenen Operation**

486 Der E-Rezept-Fachdienst MUSS ein Systemprotokoll über durchgeführte Operationen und  
487 deren Erfolg/Misserfolg führen.[<=]

488 Der E-Rezept-Fachdienst führt außerdem Zugriffsprotokolle für Versicherte, in denen alle  
489 Zugriffe auf die personenbezogenen und medizinischen Daten eines Versicherten für den  
490 Versicherten einsehbar sind. Diese Zugriffsprotokolle sind unabhängig vom  
491 Systemprotokoll und stehen ausschließlich dem Versicherten zur Wahrnehmung seiner  
492 Betroffenenrechte zur Einsicht zur Verfügung.

493 **A\_19284 - E-Rezept-Fachdienst - Versichertenprotokoll zu Operationen**

494 Der E-Rezept-Fachdienst MUSS jeden Aufruf der folgenden Operationen protokollieren:  
495

496 **Tabelle 4: TAB\_eRPFD\_004 Versichertenprotokoll**

Operation	Rolle des zugreifenden Nutzers	Beschreibung (ggfs. als Vorschlag für einen lesbaren Protokolleintrag in einfacher Sprache)
<b>http GET /Task bzw. http GET /Task/&lt;id&gt;</b>		
-	Versicherter, Vertreter	Patient/Versicherter/Vertreter hat das E-Rezept heruntergeladen
	Apotheker	Apotheke hat die E-Rezept-Quittung heruntergeladen
<b>http POST /Task</b>		
\$activate	Arzt- /Zahnarztpraxis/Krankenhaus	Arzt-/Zahnarztpraxis/Krankenhaus hat das E-Rezept bereitgestellt
\$accept	Apotheke	Apotheke hat das E-Rezept heruntergeladen
\$reject	Apotheke	Apotheke hat das E-Rezept zurückgegeben
\$close	Apotheke	Apotheke hat das E-Rezept beliefert



\$abort	Versicherter, Vertreter	Patient/Versicherter/Vertreter hat das E-Rezept gelöscht
	Arzt- /Zahnarztpraxis/Krankenhaus	Arzt- /Zahnarztpraxis/Krankenhaus hat das E-Rezept gelöscht
	Apotheke	Apotheke hat das E-Rezept gelöscht
<b>http GET /MedicationDispense</b>		
	Versicherter, Vertreter	Patient/Versicherter hat Medikament-Informationen heruntergeladen
<b>Automatisches Löschen durch den Fachdienst</b>		
Ressource Task	E-Rezept-Fachdienst	Veraltete E-Rezepte vom Fachdienst automatisch gelöscht
Ressource MedicationDispense		Veraltete Medikament-Informationen vom Fachdienst automatisch gelöscht
Ressource AuditEvent		Veraltete Protokolleinträge vom Fachdienst automatisch gelöscht
Ressource Communication		Veraltete Nachrichten vom Fachdienst automatisch gelöscht

und die gelesene bzw. geschriebene Ressource im Protokolleintrag  
 AuditEvent.entity.what als Referenz hinzufügen, sowie die KVNR des betroffenen  
 Versicherten in AuditEvent.entity.name speichern.

Mit diesen Informationen kann der Versicherte die Zugriffe auf seine Daten  
 nachvollziehen und bei einem unberechtigten Zugriff ggfs. intervenieren. [ <= ]

#### **A\_19302 - E-Rezept-Fachdienst -Protokolleintrag Versichertenprotokoll leicht verständlich**

Der E-Rezept-Fachdienst MUSS in jedem zu tätigenden Eintrag des Protokolls für  
 Versicherte einen lesbaren Text in einfacher Sprache (deutsch und englisch) erzeugen,  
 der mindestens den Namen des Zugreifenden, die auslösende Operation und das  
 Ergebnis der Operation umfasst, damit Versicherte ohne technisches Vorwissen den  
 Inhalt des Zugriffsprotokolls verstehen können. [ <= ]



## 5.5 Löschrufen

Der E-Rezept-Fachdienst soll eine Datensparsamkeit realisieren. Dafür werden nicht mehr benötigte Ressourcen, abgelaufene E-Rezepte und veraltete Kommunikationsnachrichten automatisch nach einer festen Frist gelöscht.

### A\_19252 - E-Rezept-Fachdienst - Löschrufen abgelaufener Rezepte

Der E-Rezept-Fachdienst MUSS einen Task nach Ablauf der Löschrufen gemäß der folgenden Festlegung in TAB\_eRPFD\_007 automatisch löschen und das Löschrufen in einem AuditEvent für den Versicherten nachvollziehbar protokollieren, damit nicht mehr benötigte Informationen gelöscht sind.

**Tabelle 5: TAB\_eRPFD\_007 Löschrufen**

Task.status nach Statuswechsel	Löschrufen
draft	1 Tage nach Statuswechsel
ready	10 Tage nach Datum in <code>Task.expiryDate</code>
in-progress	100 Tage nach Statuswechsel
completed	100 Tage nach Statuswechsel
cancelled	10 Tage nach Statuswechsel

[<=]

### A\_19254 - E-Rezept-Fachdienst - Löschrufen referenzierter Bundles

Der E-Rezept-Fachdienst MUSS bei jedem Löschrufen eines Tasks alle referenzierten Bundles (QES-Datensatz, Quittungs-Bundle) ebenfalls löschen, damit die Informationen rund um ein gelöschtes E-Rezept ebenfalls entfernt werden. [<=]

### A\_19255 - E-Rezept-Fachdienst Löschrufen veralteter MedicationDispense

Der E-Rezept-Fachdienst MUSS eine gespeicherte Ressource MedicationDispense nach 100 Tagen ab ihrem Erzeugungsdatum `MedicationDispense.whenHandedOver` automatisch löschen, damit Informationen zu veralteten und gelöschten Rezepten ebenfalls entfernt werden. [<=]

### A\_19253 - E-Rezept-Fachdienst - Löschrufen veraltete Nachrichten

Der E-Rezept-Fachdienst MUSS eine gespeicherte Ressource Communication ohne eine Referenz auf einen Task in `Communication.basedOn` nach 100 Tagen ab ihrem Sendedatum `Communication.sent` und solche mit einer Referenz auf einen Task gemäß der Löschrufen in TAB\_eRPFD\_007 beim Löschrufen des Tasks automatisch löschen, damit nicht mehr relevante Nachrichten zu gelöschten Rezepten ebenfalls gelöscht werden. [<=]

### A\_19256 - E-Rezept-Fachdienst - Löschrufen veraltete Protokolleinträge

Der E-Rezept-Fachdienst MUSS eine gespeicherte Ressource AuditEvent nach 3 Jahren ab dem Erzeugungsdatum `AuditEvent.recorded` löschen, damit veraltete Einträge nach Ende der regulären Aufbewahrungsfrist entfernt werden. [<=]

## 5.6 Sicherheit

### 5.6.1 Allgemeine Sicherheitsanforderungen

#### **A\_19260 - E-Rezept-Fachdienst – Ausschluss unbekannter FdV-Versionsnummern von der Kommunikation**

Der E-Rezept-Fachdienst MUSS an der Schnittstelle zum Internet die Produktidentifikation (Produktbezeichnung, Produktversion) des Clients erkennen und nicht zugelassene Produkte oder bestimmte Produktversionen von der Kommunikation mit dem E-Rezept-Fachdienst ausschließen zu können. Der E-Rezept-Fachdienst MUSS in diesen Fällen eine entsprechende Fehlermeldung mit dem http-StatusCode 403 an den aufrufenden Client geben. [ $\leq$ ]

Hinweis: Der Ausschluss soll über ein Whitelisting gültiger Produktidentifikationen erfolgen.

#### **A\_19261 - E-Rezept-Fachdienst – Ausschluss von FdV-Versionen**

Der Anbieter des E-Rezept-Fachdienstes MUSS ausschließlich auf Anweisung der gematik Clients mit einer bestimmten Produktidentifikation für die Kommunikation mit dem E-Rezept-Fachdienst zulassen. [ $\leq$ ]

#### **A\_19266 - E-Rezept-Fachdienst - Berücksichtigung OWASP-Top-10-Risiken**

Der E-Rezept-Fachdienst MUSS Maßnahmen zum Schutz vor den OWASP-Top-10-Risiken in der aktuellen Version umsetzen. [ $\leq$ ]

#### **A\_19111 - E-Rezept-Fachdienst - Versionierung von Ressourcen**

Der E-Rezept-Fachdienst MUSS eine Versionierung der FHIR-Ressource Task gemäß des Versionierungskonzepts [FHIR-ResVers] des FHIR-Standards umsetzen und in seinem CapabilityStatement ausweisen, damit für den Versicherten Zustandsänderungen nachvollziehbar und in der Versionshistorie des Tasks einsehbar sind. [ $\leq$ ]

Der E-Rezept-Fachdienst soll sich vor Anfragen, die nicht auf ein übliches Verhalten von Leistungserbringerinstitutionen und Versicherten während des Verordnungsprozesses schließen lassen, schützen. Diesen Anomalien wird mit einer Drosselung der Bearbeitungsgeschwindigkeit begegnet, um bspw. Brute-Force-Attacken auf das Erraten von AccessCodes für den Zugriff auf E-Rezept-Daten unattraktiv zu machen.

#### **A\_20703 - E-Rezept-Fachdienst - Drosselung Brute-Force-Anfragen**

Der E-Rezept-Fachdienst MUSS jede Antwort auf einen Funktionsaufruf, der einen AccessCode oder Secret enthält um den konfigurierbaren http-Response-Header "Warning" (default "999 Throttling active") ergänzt und um ein konfigurierbares Zeitintervall (default: 500 Millisekunden) verzögert zurückschicken, sofern der erwartete AccessCode bzw Secret nicht mit dem übergebenen AccessCode bzw. Secret übereinstimmt, um BruteForce-Angriffe durch einen hohen Zeitaufwand unattraktiv zu machen. [ $\leq$ ]

#### **A\_20704 - E-Rezept-Fachdienst - Drosselung Rezeptfälschungen**

Der E-Rezept-Fachdienst MUSS jede Antwort auf den Funktionsaufruf zum Aktivieren eines Tasks mittels Übergabe des QES-signierten Datensatzes um den konfigurierbaren http-Response-Header "Warning" (default "999 Throttling active") ergänzt und um ein konfigurierbares Zeitintervall (default: 500 Millisekunden) verzögert zurückschicken, sofern die QES in der Prüfung während der Operation POST /Task/<id>/\$activate als ungültig erkannt wird, um Angriffe durch Rezeptfälschungen durch einen hohen Zeitaufwand unattraktiv zu machen. [ $\leq$ ]

## **A\_20705 - Anbieter E-Rezept-Fachdienst - Konfiguration und Deaktivierung Drosselung**

Der Anbieter des E-Rezept-Fachdienstes MUSS die Funktion der Drosselung sowie die Konfiguration auf Weisung der gematik aktivieren oder deaktivieren bzw. die Konfigurationsparameter anpassen, um die Wirksamkeit des Mechanismus im Feld bei Bedarf zu verbessern. [ $\leq$ ]

Die gematik stellt mit der Prüfkarte eGK eine elektronische Identität zur Überprüfung verschiedener Anwendungsfälle in der TI und wird vorrangig von Dienstleistern vor Ort (DVOs) genutzt. Die Prüfkarte eGK ist nicht für die Nutzung im regulären Versorgungsalltag von Leistungserbringern oder Versicherten vorgesehen. Die folgenden Anforderungen verhindern eine Vermischung von Prüfkarten mittels der Prüfkarte eGK und den Anwendungsfällen von Versicherten einer Krankenkasse.

## **A\_20751 - E-Rezept-Fachdienst - Erkennen der Prüfidentität**

Der E-Rezept-Fachdienst MUSS eine eGK-Prüfkartenidentität anhand der Bildungsregel in Card-G2-A\_3820 (X0000nnnnP, mit nnnn aus der Menge {0001 .. 5000} und P = Prüfziffer) für die KVNR der Prüfkarte eGK erkennen. [ $\leq$ ]

## **A\_20752 - E-Rezept-Fachdienst - Ausschluss Vertreterkommunikation von bzw. an Prüf-Identität**

Der E-Rezept-Fachdienst MUSS das Einstellen einer Communication-Ressource mit dem http-Status-Code 400 ablehnen wenn diese in den Absender-und Empfänger-Informationen eine Kombination von KVNR der Prüfkarte eGK und KVNR von Versicherten enthält. [ $\leq$ ]

## **A\_20753 - E-Rezept-Fachdienst - Ausschluss Vertreterzugriff auf bzw. mittels Prüf-Identität**

Der E-Rezept-Fachdienst MUSS jeden Zugriff auf E-Rezepte mittels AccessCode (Vertreterzugriff) mit dem http-Status-Code 400 ablehnen, wenn sich aus dem Zugriff eine Kombination aus KVNR der Prüfkarte eGK und KVNR von Versicherten ergibt, d.h. Versicherte dürfen nicht auf Prüfrezepte und mit Prüfkarte eGK darf nicht auf Rezepte von Versicherten zugegriffen werden. [ $\leq$ ]

## **5.6.2 Identifikation des Clientsystems**

Der E-Rezept-Fachdienst verwaltet und steuert den Einlöseprozess für elektronische Verordnungen. Damit kommt ihm eine Relevanz in der Medikamentenversorgung zu, die sich zum einen in einer hohen Verfügbarkeit und zum anderen in einem hohen Angriffspotential widerspiegelt. Zur Unterstützung der betrieblichen Überwachung des E-Rezept-Fachdienstes wird die Nutzung der im Feld befindlichen Clientsysteme protokolliert. Dabei ist der Zugriff auf die Schnittstellen des E-Rezept-Fachdienstes nur durch Primärsysteme der Leistungserbringer und zugelassene E-Rezept-FdVs zulässig. Der E-Rezept-Fachdienst erkennt die Clientsysteme anhand des User-Agent-Header eingehender HTTP-Requests und protokolliert diesen Wert.

## **A\_20013 - E-Rezept-Fachdienst - Erkennung Clientsystem User-Agent**

Der E-Rezept-Fachdienst MUSS das vom aufrufenden Nutzer verwendete Clientsystem anhand des im HTTP-Request enthaltenen Header-Feld "User-Agent" gemäß [RFC7231] erkennen und in den Einträgen zur Performance-Rohdatenerfassung gemäß [gemSpec\_Perf] protokollieren. Der E-Rezept-Fachdienst MUSS bei fehlendem User-Agent-Header den Request mit dem HTTP-Status-Code 400 beantworten, damit in der Betriebsüberwachung des E-Rezept-Fachdienstes die Nutzung unzulässiger Frontends erkannt werden kann. [ $\leq$ ]

### 5.6.3 TSL und OCSP-StatusVertrauensraum der TI

Der E-Rezept-Fachdienst muss das E-Rezept-Frontend des Versicherten (E-Rezept-FdV) bei den Aufgaben unterstützen, regelmäßig die TSL-Aktualisierung vorzunehmen [gemSpec\_eRp\_FdV#A\_20028] und Sperrinformationen für Zertifikate zu ermitteln [gemSpec\_eRp\_FdV#A\_20032]. Die OCSP-Responder und der TSL-Dienst haben deutlich höhere SLAs in Bezug auf die Verfügbarkeit innerhalb der TI. Manche OCSP-Responder besitzen keine direkte Anbindung an das Internet (Komponenten-PKI, Kontext: Prüfung Identität vertrauenswürdige Ausführungsumgebung). Es wird damit auch möglich, bessere Aussagen über die Verfügbarkeit von E-Rezept-Anwendungsfällen zu treffen, weil weniger nicht-SLA-belegte Datenverbindungen für die Anwendungsfälle notwendig sind. (Wenn eine funktionierende Datenverbindung zwischen E-Rezept-FdV und E-Rezept-Fachdienst besteht, dann kann eine in [gemSpec\_Perf] definierte Verfügbarkeit garantiert werden.) Aufgrund der Verwendung der Schnittstellen-Funktionalität über die schon etablierte TLS-Verbindung sind OCSP-Requests des E-Rezept-FdV nicht im Klartext im Internet sichtbar.

#### **A\_20023 - E-Rezept-Fachdienst - Bereitstellung TSL**

Der E-Rezept-Fachdienst MUSS folgende Vorgaben umsetzen:

1. Er MUSS mindestens einmal täglich aus der TI (TI-interne Verbindung) die "TSL(ECC-RSA)" und deren zugehörigen Hashwert aus der TI herunterladen.
2. Er MUSS unter dem Pfadnamen "/TSL.xml" über das vom E-Rezept-FdV genutzte HTTPS-Interface die "TSL(ECC-RSA)" der TI zur Verfügung stellen (HTTP-GET, HTTP Content-Type: text/xml).
3. Er MUSS unter dem Pfadnamen "/TSL.sha2" über das vom E-Rezept-FdV genutzte HTTPS-Interface den vom TSL-Dienst heruntergeladenen SHA-256 Hashwert der Datei TSL.xml aus Spiegelstrich 2 zur Verfügung stellen (HTTP Content-Type: text/plain, Hashwert als hexdump kodiert (64 Byte + Newline))

[<=]

Hinweise:

1. "TI-interne Verbindung" hat den Hintergrund, dass dort über SLAs eine ausreichende Verfügbarkeit gewährleistet ist.
2. Hashwert der TSL.xml bedeutet der Hashwert der Datei TSL.xml, so wie sie vom TSL-Dienst der TI bereitgestellt wird und als wenn man die Datei als Binärdatei interpretiert (vgl. [gemSpec\_TSL]).

#### **A\_20024-01A\_20024 - E-Rezept-Fachdienst - Bereitstellung OCSP-Forwarder**

Der E-Rezept-Fachdienst MUSS folgende Vorgaben umsetzen:

1. Er MUSS unter ~~dem in A\_19411 in Tabelle: TAB\_eRPFD\_002 FQDN angegeben~~ ~~Pfadnamen für den key "ocspf" der Adresse <FQDN>/ocspf~~ eine Möglichkeit zur Statusabfrage über das vom E-Rezept-FdV genutzte HTTPS-Interface zur Verfügung stellen (HTTP-POST, vgl. auch [RFC-6960, Appendix [gemSpec\_PKI]]).
2. Er MUSS über die Schnittstelle aus Spiegelstrich 1 OCSP-Requests [RFC-6960] entgegen nehmen.
3. Aus einem solchen OCSP-Request MUSS er aus dem issuerKeyHash [RFC-6960] die URL des entsprechenden OCSP-Responders in der TI ermitteln (Datengrundlage ist die TSL der TI) und den OCSP-Request an diese ermittelte URL weiterleiten.

4. Er MUSS die erhaltenen OCSP-Response an das die OCSP-Anfrage stellende E-Rezept-FdV unverändert weiterreichen.

[<=]

Auf Anfrage stellt die gematik eine Beispielimplementierung für A\_20024 Spiegelstrich 3 bereit.

#### **A\_20025 - E-Rezept-Fachdienst - Caching OCSP-Antworten**

Der E-Rezept-Fachdienst KANN OCSP-Antworten aus A\_20024 bis zu 4 Stunden cachen und bei einer entsprechend passenden OCSP-Anfrage, anstatt neu den OCSP-Responder anzufragen, die im Cache befindliche OCSP-Antwort ausliefern.[<=]

#### **A\_20026 - E-Rezept-Fachdienst - OCSP-Stapling**

Der E-Rezept-Fachdienst MUSS an der HTTPS-Schnittstelle zum Internet OCSP-Stapling [RFC-6066] unterstützen.[<=]

Als Alternative zur TSL-Verarbeitung stellt der E-Rezept-Fachdienst eine kurze Zertifikatskette in einer JSON-Struktur bereit, die sich in Plattformen mobiler Betriebssysteme leichter verarbeiten lässt. Diese Zertifikatskette muss regelmäßig aktualisiert und über einen Downloadpunkt für Primärsysteme und das E-Rezept-FdV zur Verfügung gestellt werden. Die normativen Festlegungen finden sich in der Spezifikation [gemSpec Krypt] in Abschnitt 7.2.2 "Client-seitige Prüfung der E-Rezept-VAU-Identität".

### **~~5.6.35.6.4~~ Sicherheit der Netzübergänge**

Der E-Rezept-Fachdienst wird für Versicherte über das Internet erreichbar gemacht und für Leistungserbringer über das Netz der TI. Die folgenden Anforderungen beschreiben die für diese Netzübergänge erforderlichen Sicherheitsmechanismen. Für den Netzübergang aus dem Internet als Transportnetz zum E-Rezept-Fachdienst ist ein Paketfilter erforderlich.

#### **A\_19813 - E-Rezept-Fachdienst – Sicherung zum Transportnetz Internet durch Paketfilter**

Der E-Rezept-Fachdienst MUSS zum Transportnetz Internet durch einen Paketfilter (ACL) gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der Paketfilter des E-Rezept-Fachdienstes MUSS frei konfigurierbar sein auf der Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.[<=]

#### **A\_19814 - E-Rezept-Fachdienst – Platzierung des Paketfilters Internet**

Der Paketfilter des E-Rezept-Fachdienstes, zum Schutz in Richtung Transportnetz Internet, DARF NICHT physisch auf Systemen der VAU des E-Rezept-Fachdienstes oder dem vorgeschalteten TLS-terminierenden Load Balancer implementiert werden.[<=]

#### **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 .[<=]

Hinweis zu A\_19815:



Der Anbieter des E-Rezept-Fachdienstes muss für seine HTTPS-Schnittstelle ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-Zertifikat also über einen aktuellen Webbrowser prüfbar ist, vgl. A\_19823). Für dieses TLS-Zertifikat fragt der E-Rezept-Fachdienst regelmäßig für das OCSP-Stapling nach A\_20026 den OCSP-Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält der E-Rezept-Fachdienst eine OCSP-Response. Diese wird nach A\_20022 geprüft und anschließend von der HTTPS-Schnittstelle verwendet (vgl. <https://tools.ietf.org/html/rfc6066#section-8> und bspw. [http://nginx.org/en/docs/http/ngx\\_http\\_ssl\\_module.html#ssl\\_stapling](http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling) ).

Um dies zu ermöglichen muss der Paketfilter entsprechende stateful-Firewall-Regeln gemäß A\_19815 und A\_20022 definieren.

### **A\_20022 - E-Rezept-Fachdienst - OCSP-Status für das OCSP-Stapling**

Der Paketfilter des E-Rezept-Fachdienstes MUSS bezüglich des OCSP-Stapling gemäß A\_20026 folgende Vorgaben umsetzen:

1. Für das vom Anbieter des E-Rezept-Fachdienstes erworbene TLS-Zertifikat (vgl. Hinweis zu A\_19815) MUSS der E-Rezept-Fachdienst initial die IP-Adresse (ggf. die IP-Adressen) des entsprechenden OCSP-Responders ermitteln.
2. Diese IP-Adresse(n) MÜSSEN gemäß A\_19815 per stateful-Firewalling Verbindungen von der HTTPS-Schnittstelle an den OCSP-Responder erlaubt werden (Whitelisting).
3. Gemäß OCSP-Stapling ( <https://tools.ietf.org/html/rfc6066#section-8> ) MUSS der E-Rezept-Fachdienst regelmäßig eine OCSP-Response vom entsprechenden OCSP-Responder beziehen (Die Regelmäßigkeit wird vom zertifikatsausgebenden TSP und der Gültigkeitsdauer dessen OCSP-Responses bestimmt).
4. Die OCSP-Responses MÜSSEN vom E-Rezept-Fachdienst geprüft werden (Signaturprüfung, CertID in der OCSP-Response passt zum angefragten Zertifikat). Falls eine der Prüfungen ein nicht-positives Ergebnis liefert so MUSS die erhaltene OCSP-Response verworfen werden.
5. Sollte die letzte im E-Rezept-Fachdienst vorhandene OCSP-Response zeitlich nicht mehr gültig sein (bspw. der OCSP-Responder im Internet war länger nicht erreichbar), so MUSS diese OCSP-Response verworfen werden und ein von einem Klienten (E-Rezept-FdV) initiiertes TLS-Verbindungsaufbau der HTTPS-Schnittstelle ohne OCSP-Stapling durchgeführt werden.

[<=]

### **A\_19824 - E-Rezept-Fachdienst – Verhalten bei Vollauslastung**

Der Paketfilter des E-Rezept-Fachdienstes MUSS so konfiguriert sein, dass bei Vollauslastung der Systemressourcen im E-Rezept-Fachdienst keine weiteren Verbindungen angenommen werden. [<=]

Durch die Zurückweisung von Verbindungen wird sichergestellt, dass Clients einen Verbindungsaufbau mit einer anderen Instanz des Fachdienstes versuchen, bei dem die erforderlichen Ressourcen zur Verfügung stehen.

Da der E-Rezept-Fachdienst die Verarbeitung der fachlichen Operationen in einer VAU ausführt, ist der Zugang zum Schutz dieser VAU zweistufig. Der E-Rezept-Fachdienst verfügt über einen Eingangspunkt (einen Load Balancer), an dem die TLS-Verbindung terminiert wird. Der Eingangspunkt wertet dann den HTTP-Header aus, um aus der Ziel-URL des Requests den für die Verarbeitung zu adressierenden Verarbeitungskontext zu ermitteln. An diesen Verarbeitungskontext wird der Request durch den Eingangspunkt weitergeleitet. In umgekehrter Richtung sendet der Eingangspunkt die Response des Verarbeitungskontextes über die TLS-Verbindung an den Client.

## **A\_19720 - E-Rezept-Fachdienst – Verbindungen von Clients zu Verarbeitungskontexten der VAU über den Eingangspunkt**

Der Eingangspunkt des E-Rezept-Fachdienstes MUSS Verbindungen von Clients (Internet oder TI) ausschließlich über TLS akzeptieren. Er MUSS die TLS-Verbindung terminieren und HTTP Requests und Responses zwischen dem Client und dem für die jeweilige Sitzung zugeordneten Verarbeitungskontext der VAU vermitteln. [ <= ]

## **A\_19823 - E-Rezept-Fachdienst – Richtlinien zum TLS-Verbindungsaufbau**

Der Eingangspunkt des E-Rezept-Fachdienstes MUSS sich beim TLS-Verbindungsaufbau über das Transportnetz gegenüber dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren. Das Zertifikat MUSS an die jeweilige Schnittstelle des Eingangspunkts für Primärsysteme und Frontends der Versicherten des E-Rezept-Fachdienstes gebunden werden, damit Clientsysteme beim TLS-Verbindungsaufbau eine vereinfachte Zertifikatsprüfung mit TLS-Standardbibliotheken durchführen können. [ <= ]

## **5.6.45.6.5 Vertrauenswürdige Ausführungsumgebung**

In diesem Abschnitt werden die Anforderungen an den E-Rezept-Fachdienst zur Umsetzung einer Vertrauenswürdigen Ausführungsumgebung (VAU) dargestellt. Die VAU dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten Klartextdaten innerhalb des E-Rezept-Fachdienstes sowie dem technischen Ausschluss der Profilbildung durch den Anbieter bzw. Betreiber. Die VAU stellt dazu Verarbeitungskontexte (d. h. Instanzen der VAU) bereit, in denen die Verarbeitung sensibler Daten im Klartext erfolgen kann. Diese Verarbeitungskontexte sind entsprechend zu schützen.

## **A\_19683 - E-Rezept-Fachdienst – Umsetzung der fachlichen Operationen in einer Vertrauenswürdigen Ausführungsumgebung (VAU)**

Der E-Rezept-Fachdienst MUSS die Verarbeitung aller fachlichen Operationen des Fachdienstes in einer Vertrauenswürdigen Ausführungsumgebung umsetzen. [ <= ]

### **5.6.4-15.6.5.1 Verarbeitungskontext**

Die Gesamtheit aus der für eine Klartextverarbeitung erforderlichen Software, dem für eine Klartextverarbeitung genutzten physikalischen System sowie den für die Integrität einer Klartextverarbeitung erforderlichen organisatorischen und physischen Rahmenbedingungen bildet den Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung.

Zur Vertrauenswürdigen Ausführungsumgebung gehören neben den Verarbeitungskontexten alle für ihre Erreichbarkeit und betriebliche Steuerung erforderlichen Komponenten.

Der Verarbeitungskontext grenzt sich von allen weiteren, im betrieblichen Kontext beim Anbieter des E-Rezept-Fachdienstes vorhandenen Systemen und Prozessen dadurch ab, dass die sensiblen Klartextdaten von Komponenten innerhalb des Verarbeitungskontextes aus erreichbar sind oder sein können, während sie dies von außerhalb des Verarbeitungskontextes nicht sind. Sensible Daten verlassen den Verarbeitungskontext ausschließlich gemäß wohldefinierten (Zugriffs-)Regeln und in verschlüsselter Form.

## **A\_19684 - E-Rezept-Fachdienst – Verarbeitungskontext der VAU**

Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sämtliche physikalischen Systemkomponenten sowie sämtliche Softwarekomponenten umfassen, deren Sicherheitseigenschaften sich auf den Schutz der personenbezogenen medizinischen

820 Daten vor Zugriff durch Unbefugte bei ihrer Verarbeitung im Klartext auswirken  
821 können.[<=]

822 **A\_19688 - E-Rezept-Fachdienst – Verschlüsselung von außerhalb des**  
823 **Verarbeitungskontextes der VAU gespeicherten Daten**

824 Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass sämtliche  
825 schützenswerten Daten vor einer Speicherung außerhalb der VAU verschlüsselt werden.  
826 Der Verarbeitungskontext MUSS dazu Schlüssel für nur jeweils ein individuelles E-Rezept  
827 (inkl. aller mit diesem E-Rezept verbundenen Daten) verwenden oder mindestens einmal  
828 pro Sekunde den verwendeten Schlüssel wechseln, so dass nur die innerhalb einer  
829 Sekunde neu angelegten E-Rezepte mit einem Schlüssel verschlüsselt werden.[<=]

830 **A\_19699 - E-Rezept-Fachdienst – Ableitung der Persistenzschlüssel durch ein**  
831 **HSM**

832 Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS die zur Verschlüsselung der  
833 persistierten E-Rezept-Daten verwendeten Schlüssel von einem HSM innerhalb der VAU  
834 abrufen.[<=]

835 **A\_19700 - E-Rezept-Fachdienst - Ableitung der Persistenzschlüssel aus**  
836 **Merkmal der E-Rezepte**

837 Das HSM der VAU des E-Rezept-Fachdienstes MUSS eine Schnittstelle zur Ableitung von  
838 symmetrischen Schlüsseln für die Persistierung von E-Rezept-Daten bereitstellen. Das  
839 HSM der VAU des E-Rezept-Fachdienstes MUSS zur Ableitung des jeweiligen Schlüssels  
840 ein nach der ersten Erstellung unveränderliches Merkmal des E-Rezept-Datensatzes als  
841 Ableitungsparameter verwenden (z. B. den Zeitstempel der Registrierung von Rezept-ID  
842 und Access Code oder den Access Code selbst).[<=]

843 **A\_19694 - E-Rezept-Fachdienst – Geschützte Weitergabe von Daten an**  
844 **autorisierte Nutzer durch die VAU**

845 Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass sämtliche  
846 schützenswerten Daten ausschließlich über sichere Verbindungen an autorisierte Nutzer  
847 weitergegeben werden.[<=]

848 **A\_19262 - E-Rezept-Fachdienst - Transportverschlüsselte Übertragung von**  
849 **Daten mit PVS**

850 Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass er nur  
851 transportverschlüsselt mit dem PVS kommuniziert.[<=]

852 **A\_19263 - E-Rezept-Fachdienst - Transportverschlüsselte Übertragung von**  
853 **Daten mit AVS**

854 Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass er nur  
855 transportverschlüsselt mit dem AVS kommuniziert.[<=]

856 **A\_19264 - E-Rezept-Fachdienst - Transportverschlüsselte Übertragung von**  
857 **Daten mit FdV**

858 Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass er nur  
859 transportverschlüsselt mit dem FdV kommuniziert.[<=]

860 **A\_19265 - E-Rezept-Fachdienst – vertrauliche Kommunikation**

861 Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass er nur  
862 transportverschlüsselt mit Komponenten außerhalb des Verarbeitungskontextes  
863 kommuniziert.[<=]

864 Hinweis: für die Qualität der Transportverschlüsselung gelten die Anforderungen aus  
865 [gemSpec\_Krypt].



**A\_19267 - E-Rezept-Fachdienst - Authentisierung gegenüber Clients**

Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sich gegenüber Clients, die mit ihm kommunizieren, mittels der Fachdienstidentität oid\_erp-vau mit Zertifikatsprofil C.FD.ENC (oid\_fd\_enc) ausweisen. [ <= ]

**A\_19702 - E-Rezept-Fachdienst – Isolation zwischen****Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS die in ihr ablaufenden Verarbeitungen für die Daten eines Verarbeitungskontextes von den Verarbeitungen für die Daten anderer Verarbeitungskontexte in solcher Weise trennen, dass mit technischen Mitteln ausgeschlossen wird, dass die Verarbeitungen eines Verarbeitungskontextes schadhaft auf die Verarbeitungen eines anderen Verarbeitungskontextes einwirken können. [ <= ]

*Hinweis: Da der Verarbeitungskontext der VAU des E-Rezept-Fachdienstes für jede fachliche Operation neu aufgebaut werden muss, ist ein Low-Level-Mechanismus zur Kontextseparation aus Gründen der Performance bzw. Skalierung nicht zwingend vorgeschrieben. Der hier geforderte Separationsmechanismus kann daher auch als Server-Thread, Worker, o. Ä. ausgeführt sein, solange für den dadurch gebildeten Verarbeitungskontext die geforderte Separation nachgewiesen werden kann. Dies setzt voraus, dass die Umsetzung der Verarbeitungskontexte und der in ihnen ablaufenden Verarbeitungsvorgänge technisch möglichst einfach und nachvollziehbar gestaltet ist.*

**A\_19726 - E-Rezept-Fachdienst – Unabhängige Skalierung der Dienst-Ressourcen für verschiedene Anwendergruppen**

Die VAU des E-Rezept-Fachdienstes MUSS für die Anwendergruppen Leistungserbringer (E-Rezepte ausstellen, E-Rezepte einlösen) und Versicherte (E-Rezepte einsehen, zuweisen und löschen) auf jeweils getrennten physischen Servern betrieben werden, so dass eine Überlastung aufgrund außergewöhnlich hoher Aktivität einer Anwendergruppe (primär der Versicherten) keine Beeinträchtigung der Arbeitsfähigkeit der anderen Anwendergruppen (primär der Ärzte und Apotheker) zur Folge hat. [ <= ]

**5.6.4.25.6.5.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld**

Der Schutzbedarf der in der VAU verarbeiteten Klartextdaten erfordert den technischen Ausschluss von Zugriffen des Anbieters. Dies umfasst insbesondere Zugriffe durch Personen aus dem betrieblichen Umfeld des Anbieters.

**A\_19704 - E-Rezept-Fachdienst – Isolation der VAU von Datenverarbeitungsprozessen des Anbieters**

Die VAU des E-Rezept-Fachdienstes MUSS die in ihren Verarbeitungskontexten ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters trennen und damit gewährleisten, dass der Anbieter des E-Rezept-Fachdienstes vom Zugriff auf die in der VAU verarbeiteten schützenswerten Daten ausgeschlossen ist. [ <= ]

*Hinweis: Für die Separation zwischen Verarbeitungskontexten und Verarbeitungsprozessen des Anbieters, die der betrieblichen Steuerung des Systems dienen, ist eine Low-Level Separation anzustreben, da - im Unterschied zur Separation zwischen Verarbeitungskontexten - hier technisch sehr verschiedene Aspekte getrennt werden müssen.*

**A\_19706 - vE-Rezept-Fachdienst – Ausschluss von Manipulationen an der Software der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS eine Manipulation der eingesetzten Software erkennen und eine Ausführung der manipulierten Software verhindern. [ <= ]

**A\_19707 - E-Rezept-Fachdienst – Ausschluss von Manipulationen an der Hardware der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter des E-Rezept-Fachdienstes ausschließen.[<=]

**A\_19708 - E-Rezept-Fachdienst – Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter des E-Rezept-Fachdienstes mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann.[<=]

**A\_19709 - E-Rezept-Fachdienst – Kein physischer Zugang des Anbieters zu Systemen der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter des E-Rezept-Fachdienstes, während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.[<=]

**A\_19710 - E-Rezept-Fachdienst – Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln sicherstellen, dass physischer Zugang zu Hardware-Komponenten der Verarbeitungskontexte nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten extrahiert werden können.[<=]

**A\_19711 - E-Rezept-Fachdienst – Private Schlüssel von Dienstzertifikaten im HSM**

Der E-Rezept-Fachdienst MUSS die folgenden privaten Schlüssel in einem Hardware Security Module (HSM) erzeugen und anwenden:

- TI-Fachdienst-Identität zur Authentisierung des Dienstes gegenüber dem Primärsystem des Leistungserbringers (TLS)
- TI-Fachdienst-Identität zur Authentisierung des Verarbeitungskontextes gegenüber dem Primärsystem des Leistungserbringers (sicherer Kanal auf Anwendungsebene),
- Privater Schlüssel des Schlüsselpaars zur Authentisierung des Verarbeitungskontextes gegenüber dem E-Rezept-Frontend des Versicherten (sicherer Kanal auf Anwendungsebene).

Die Prüftiefe des HSM MUSS dabei den in [A\_19712] angegebenen Standards entsprechen.[<=]

*Hinweis: Die TLS-TI-Fachdienst-Identität kann z. B. auf einem außerhalb der VAU betriebenen Load Balancer mit TLS-Terminierung verwendet werden. Hierfür muss dann ein HSM außerhalb der VAU verwendet werden.*

**A\_19712 - E-Rezept-Fachdienst – Einsatz zertifizierter HSM**

Der Anbieter des E-Rezept-Fachdienstes MUSS beim Einsatz eines HSM sicherstellen, dass dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria, ITSEC oder Federal Information Processing Standard (FIPS) in Frage.

Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3,
2. Common Criteria EAL 4+ mit hohem Angriffspotenzial oder

3. ITSEC E3 der Stärke „hoch“ entsprechen.

[<=]

#### **A\_19713 - E-Rezept-Fachdienst – HSM-Kryptographieschnittstelle verfügbar nur für Instanzen der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln, die auch Manipulationen durch den Anbieter des E-Rezept-Fachdienstes ausschließen, gewährleisten, dass nur Instanzen der VAU Zugriff auf die Kryptographieschnittstelle des HSM zur Nutzung des privaten Schlüsselmaterials für ihre Dienstzertifikate erhalten können.[<=]

*Hinweis: Falls die Verarbeitungskontexte als Threads, Workers, o. Ä. umgesetzt sind und daher gemeinsam in einem übergreifenden Anwendungsprozess ausgeführt werden, kann dieser Anwendungsprozess eine authentifizierte Verbindung zur Kryptographieschnittstelle des HSM herstellen und aufrecht erhalten, um darüber die Kryptographieschnittstelle des HSM den Verarbeitungskontexten (und nur diesen) lokal zur Verfügung zu stellen.*

#### **A\_19714 - E-Rezept-Fachdienst – Sicherer Kanal vom Client zum Verarbeitungskontext der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS den Aufbau eines vertraulichen und integritätsgeschützten Kommunikationskanals gemäß [gemSpec\_Krypt#3.16] und [gemSpec\_Krypt#7] zwischen einem Client und einem Verarbeitungskontext erzwingen, bevor der Verarbeitungskontext seine fachlichen Schnittstellen für den Client nutzbar macht.[<=]

### **5.6.4.35.6.5.3 Konsistenz des Systemzustands, Logging und Monitoring**

#### **A\_19715 - E-Rezept-Fachdienst – Konsistenter Systemzustand des Verarbeitungskontextes der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS sicherstellen, dass ein konsistenter Zustand des Verarbeitungskontextes auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw. wiederhergestellt werden kann.[<=]

#### **A\_19716 - E-Rezept-Fachdienst – Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU**

Die VAU des E-Rezept-Fachdienstes MUSS die für den Betrieb eines Fachdienstes erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dem Anbieter des E-Rezept-Fachdienstes oder Dritten vertrauliche oder zur Profilbildung geeignete Daten zur Kenntnis gelangen.[<=]

### **5.6.4.45.6.5.4 Client-Verbindungen zum Verarbeitungskontext**

Um Verbindungen vom E-Rezept-Frontend des Versicherten nach [gemSpec\_eRp\_FdV] zum Verarbeitungskontext zu ermöglichen, ist ein der VAU vorgelagertes Routing ausgehend von einem netztechnischen Eingangspunkt (z. B. in Form eines TLS-terminierenden Load Balancers) erforderlich. Der Eingangspunkt ist im Netzwerk der TI für das Primärsystem unter mindestens einer IP-Adresse/Port-Kombination erreichbar, die im Namensdienst der TI registriert sein muss. Der Eingangspunkt vermittelt die Verbindungen zwischen dem Client und dem jeweils benötigten Verarbeitungskontext.

#### **A\_19719 - E-Rezept-Fachdienst – Verarbeitungskontexte der VAU über gemeinsame Host-Adressen erreichbar**

Die VAU des E-Rezept-Fachdienstes MUSS ihre Verarbeitungskontexte über gemeinsame IP-Adressen und Ports des Eingangspunkts des Fachdienstes erreichbar machen.[<=]

1008 **A\_19724 - E-Rezept-Fachdienst – Identität des Verarbeitungskontextes für**  
1009 **Clients**

1010 Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sich gegenüber Clients  
1011 mittels der Fachdienstidentität `oid_erp-vau` mit Zertifikatsprofil  
1012 `C.FD.ENC` ausweisen.[<=]

1013 **A\_19721 - E-Rezept-Fachdienst – Sicherer Kanal zum Verarbeitungskontext der**  
1014 **VAU auf Inhaltsebene**

1015 Der Eingangspunkt des E-Rezept-Fachdienstes MUSS Clients den Aufbau eines sicheren  
1016 Kanals auf Inhaltsebene, d. h. einen Verbindungsaufbau gemäß [gemSpec\_Krypt#3.16]  
1017 und [gemSpec\_Krypt#7], zum Verarbeitungskontext ermöglichen.[<=]

1018 **A\_19722 - E-Rezept-Fachdienst – Automatisierter Abbau des sicheren Kanals**

1019 Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS den sicheren Kanal zu einem  
1020 Client nach Abschluss einer fachlichen Operation (die aus mehreren Requests bestehen  
1021 kann) abbauen, sodass anschließend keine Zugriffe dieses Clients auf den  
1022 Verarbeitungskontext mehr möglich sind, ohne dass eine neue Verbindung aufgebaut  
1023 wird.[<=]

1024

## 6 Funktionsmerkmale

1025 In diesem Abschnitt werden die vom E-Rezept-Fachdienst verwalteten Ressourcen mit  
1026 ihren zulässigen Operationen und der Workflow des E-Rezepts spezifiziert. Dabei werden  
1027 sowohl die relevanten HTTP-Operationen als auch die möglichen FHIR-Operationen auf  
1028 Ressourcen-Endpunkte bzw. konkrete über eine <id> referenzierte Instanz vorgestellt.  
1029 Die HTTP-Operationen dienen dabei der Zugriffssteuerung gemäß HTTP-Protokoll, um mit  
1030 GET Daten von einem Server abzurufen und mittels POST Daten an einen Server zu  
1031 schicken. Die FHIR-Operationen setzen in Kombination mit den HTTP-Operationen die  
1032 Workflow-Steuerung um, wobei die entsprechenden FHIR-Operationen jeweils  
1033 Zustandsänderungen triggern und bei den HTTP-Operationen POST vom Client  
1034 Übergabeparameter erwarten und bei HTTP-GET ohne Übergabeparameter funktionieren.

### 1035 **A\_19536 - E-Rezept-Fachdienst - RESTful API**

1036 Der E-Rezept-Fachdienst MUSS seine Schnittstellen für alle Zugriffe auf alle Datenobjekte  
1037 und alle Ressourcen in einer RESTful API gemäß der FHIR-Spezifikation  
1038 in <http://hl7.org/fhir/http.html> der Version v4.0.1 R4 umsetzen. [≤]

### 1039 **A\_19537 - E-Rezept-Fachdienst - RESTful API MimeType fhir+xml**

1040 Der E-Rezept-Fachdienst MUSS in seinen Schnittstellen für die Zugriffe durch  
1041 Leistungserbringer und Leistungserbringerinstitutionen standardmäßig den MimeType  
1042 `application/fhir+xml` akzeptieren und in Responses verwenden. [≤]

### 1043 **A\_19538 - E-Rezept-Fachdienst - RESTful API MimeType fhir+json**

1044 Der E-Rezept-Fachdienst MUSS in seinen Schnittstellen für die Zugriffe durch Versicherte  
1045 standardmäßig den MimeType `application/fhir+json` akzeptieren und in Responses  
1046 verwenden. [≤]

### 1047 **A\_19539 - E-Rezept-Fachdienst - RESTful API MimeType Aufrufparameter**

1048 Der E-Rezept-Fachdienst MUSS in seinen Schnittstellen einen von der  
1049 Standardfestlegung abweichenden MimeType umsetzen, wenn der jeweilige Client eine  
1050 entsprechende Anforderung in der Aufrufschnittstelle über den URL-Parameter  
1051 `_format=fhir+xml` bzw. `_format=fhir+json` gemäß  
1052 <http://hl7.org/fhir/http.html#general> oder mittels des `Accept`-Attributs im HTTP-  
1053 Request-Header als `application/fhir+xml` bzw. `application/fhir+json` anfordert,  
1054 damit Clientsysteme ein für sie leichter verarbeitbares Format in der Antwort erhalten  
1055 können. [≤]

### 1056 **A\_20171 - E-Rezept-Fachdienst - RESTful API CapabilityStatement**

1057 Der E-Rezept-Fachdienst MUSS an seinen Schnittstellen eine http-GET-Operation auf den  
1058 Endpunkt `/metadata` erlauben, in welcher er ein `CapabilityStatement`  
1059 gemäß <https://www.hl7.org/fhir/capabilitystatement.html> veröffentlicht, welches die  
1060 vom E-Rezept-Fachdienst verarbeiteten Ressourcen mit den zugehörigen http-  
1061 Operationen der angebotenen REST-Schnittstelle auflistet:

- 1062 • Task – GET-, POST-Operation, FHIR-Operations für die Workflow-Steuerung und  
1063 Einsicht durch den Versicherten
- 1064 • MedicationDispense – GET-Operation für das Einsehen der  
1065 Medikamentinformationen durch den Versicherten
- 1066 • Communication – GET-, POST, DELETE-Operation für das Senden, Empfangen und  
1067 Löschen von Nachrichten
- 1068 • AuditEvent – GET-Operation für die Einsicht in Protokolleinträge durch den  
1069 Versicherten



1070 • Device – GET-Operation mit statischen Informationen zur serverseitigen Signatur  
1071 damit der Client eine Information über die FHIR-Kompatibilität zum Fachdienst  
1072 erhält.[<=]  
1073

## 1074 6.1 Ressource Task

1075 Die FHIR-Resource Task [FHIR-TASK] bildet den Workflow für ein E-Rezept ab. Diese  
1076 wird vom verordnenden Leistungserbringer mittels FHIR-Operationen \$create und  
1077 \$activate im E-Rezept-Fachdienst erstellt. Der Versicherte kann die Ressource einsehen  
1078 bzw. herunterladen und auf Wunsch mittels einer FHIR-Operation \$abort löschen, die  
1079 den Workflow abbricht. Die abgebende Apotheke greift ebenso wie der Verordnende  
1080 ausschließlich über FHIR-Operationen \$accept und \$close zur Workflow-Steuerung auf  
1081 einen Task zu.

### 1082 A\_19030 - E-Rezept-Fachdienst - unzulässige Operationen Task

1083 Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource Task mittels der HTTP-  
1084 Operationen PUT, PATCH, HEAD und DELETE sowie POST ohne die Angabe einer gültigen  
1085 FHIR-Operation unterbinden, damit keine unzulässigen Operationen auf den Rezeptdaten  
1086 ausgeführt werden können.[<=]

### 1087 6.1.1 HTTP-Operation GET

1088 Der Zugriff mittels der HTTP-Operation GET steht ausschließlich für die Einsichtnahme in  
1089 E-Rezepte durch den Versicherten bzw. einen Vertreter mit Wissen um den AccessCode  
1090 bzw. einen Apotheker mit Wissen um das Secret zur Verfügung. Die GET-Operation ohne  
1091 Referenz einer FHIR-Operation führt zu keiner Statusänderung.

### 1092 A\_19113 - E-Rezept-Fachdienst - Rollenprüfung Versicherter oder Apotheker liest Rezept

1093 Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt  
1094 /Task und auf einen konkreten über <id> adressierten/Task/<id> (ohne die Referenz  
1095 einer FHIR-Operation) sicherstellen, dass ausschließlich Versicherte oder Apotheken in  
1096 einer der Rollen  
1097

- 1098 • oid\_versicherter
- 1099 • oid\_oeffentliche\_apotheke
- 1100 • oid\_krankenhausapotheke

1101 die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des  
1102 Aufrufers im ACCESS\_TOKEN im HTTP-RequestHeader "Authorization" feststellen,  
1103 damit E-Rezepte nicht durch Unberechtigte ausgelesen werden können.[<=]

### 1104 A\_19115 - E-Rezept-Fachdienst - Filter Tasks auf KVNR des Versicherten

1105 Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt  
1106 /Task die dem Versicherten zugeordneten Task-Ressourcen anhand der KVNR des  
1107 Versicherten aus dem ACCESS\_TOKEN im "Authorization"-Header des HTTP-Requests  
1108 identifizieren, die inTask.for mit dem Value-  
1109 Set <http://fhir.de/NamingSystem/gkv/kvid-10> die entsprechende KVNR des  
1110 begünstigten Patienten referenziert haben, damit ausschließlich Versicherte ihre eigenen  
1111 E-Rezepte einsehen können.[<=]

**A\_19116 - E-Rezept-Fachdienst - Prüfung AccessCode bei KVNR-Mismatch**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf einen einzelnen /Task/<id> und Ungleichheit der KVNR des Aufrufenden (KVNR des ACCESS\_TOKEN im "Authorization"-Header des HTTP-Requests UNGLEICH KVNR inTask.for mit Value-Set <http://fhir.de/NamingSystem/gkv/kvid-10>) prüfen, ob der im HTTP-Request-Header "X-AccessCode" oder URL-Parameter "?ac=..." übergebene AccessCode gleich dem AccessCode inTask.identifizier ist, damit auch Vertreter in Kenntnis des AccessCodes ein einzelnes E-Rezept einsehen können. [≤]

**A\_19129 - E-Rezept-Fachdienst - Rückgabe Task inkl. Bundle im Bundle Versicherter**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task oder auf einen einzelnen /Task/<id> die gültige Ergebnisliste der Task-Ressourcen um das jeweils referenzierte, serverseitig signierte E-Rezept-Bundle aus Task.input mit Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 2 und sofern vorhanden aus Task.output als search.include im Ergebnis-Bundle ergänzen und die Ergebnismenge Task[s] + E-Rezept-Bundle[s] an den Aufrufer zurückgeben, damit der Versicherte eine vollständige Einsicht in den Task und den signierten Verordnungsdatensatz und bei Vorhandensein die Quittung für eigene Dokumentationszwecke erhält. [≤]

**A\_20702 - E-Rezept-Fachdienst - Keine Einlöseinformationen in unbekannten Clients**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task oder auf einen einzelnen /Task/<id> ausschließlich Primärsystemen und solchen Clients die AccessCode Information (Task.identifizier mit system=" <https://gematik.de/fhir/NamingSystem/AccessCode> ") in den Task-Ressourcen zurückgeben, welche anhand der mitgeteilten, gültigen Produktidentifikation als zulässige Clients erkannt werden. [≤]

**A\_19226 - E-Rezept-Fachdienst - Rückgabe Task inkl. Bundle im Bundle Apotheker**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf einen einzelnen Task mittels "/Task/<id>?secret=..." durch einen Apotheker den Task, sofern er den Status "completed" hat, um das referenzierte, serverseitig signierte Quittungs-Bundle ausTask.output mit Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 3 als search.include im Ergebnis-Bundle ergänzen und die Ergebnismenge Task + Quittungs-Bundle an den Apotheker zurückgeben, damit ein Apotheker, der ein konkretes E-Rezept beliefert hat, bei Bedarf genau dieses belieferte E-Rezept inkl. der Quittung erneut abrufen kann. [≤]

**A\_19569 - E-Rezept-Fachdienst - Suchparameter Task**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task eine Suche nach einem Task mit einer konkreten Task.id und \_revinclude der Ressource AuditEvent:entity:what gemäß <https://www.hl7.org/fhir/search.html#revinclude> und <https://www.hl7.org/fhir/task.html#search> zulassen, sodass der Versicherte zu einem Task alle zugehörigen Protokolleinträge abrufen kann. [≤]

**6.1.2 HTTP-Operation POST**

Der Zugriff auf einen Task mittels der HTTP-Operation POST erfolgt immer in Verbindung mit dem Aufruf einer FHIR-Operation, die den Workflow des Tasks steuert. Je nach

1160 Anwendungsfall erfolgt der POST-Aufruf auf den Ressourcen-Endpunkt /Task oder eine  
1161 konkrete über die ID referenzierte Task-Ressource /Task/<id>.

#### 1162 **6.1.2.1 POST /Task/\$create**

1163 Die FHIR-Operation \$create erzeugt einen neuen FHIR-Task für ein E-Rezept. Diese  
1164 Operation steht ausschließlich verordnenden Leistungserbringern zur Verfügung.

#### 1165 **A\_19018 - E-Rezept-Fachdienst - Rollenprüfung Verordnender stellt Rezept ein**

1166 Der E-Rezept-Fachdienst MUSS beim Erzeugen eines Tasks mittels HTTP-POST/\$create-  
1167 Operation die Rolle "professionOID" des Aufrufenden im ACCESS\_TOKEN im HTTP-  
1168 RequestHeader "Authorization" feststellen und sicherstellen, dass ausschließlich  
1169 verordnende Leistungserbringer in der Rolle

- 1170 • oid\_arzt
- 1171 • oid\_zahnarzt
- 1172 • oid\_praxis\_arzt
- 1173 • oid\_zahnarztpraxis
- 1174 • oid\_praxis\_psychotherapeut
- 1175 • oid\_krankenhaus

1176 die Operation im Fachdienst aufrufen dürfen, damit E-Rezepte nicht durch zur  
1177 Verordnung Unberechtigte eingestellt werden können.[<=]

#### 1178 **A\_19257 - E-Rezept-Fachdienst - Schemavalidierung Rezept anlegen**

1179 Der E-Rezept-Fachdienst MUSS die im Body der HTTP-POST-Operation auf die Ressource  
1180 Task übertragenen Parameter gegen das Schema  
1181 <http://gematik.de/fhir/OperationDefinition/CreateOperationDefinition> prüfen und bei  
1182 Nicht-Konformität das Anlegen der Ressource im Fachdienst mit dem http-Status-Code  
1183 400 beantworten, damit kein Schadcode und keine "fachfremden" Daten in den E-Rezept-  
1184 Fachdienst hochgeladen werden.[<=]

#### 1185 **A\_19112 - E-Rezept-Fachdienst - Parametrierung Task für Workflow-Typ**

1186 Der E-Rezept-Fachdienst MUSS beim Erzeugen eines Tasks mittels HTTP-POST/\$create-  
1187 Operation den Parameter workflowType (Rezepttyp) aus dem HTTP-Body des POST-  
1188 Requests entnehmen, als Attribut Task.extension:flowType des zu erstellenden Tasks  
1189 verwenden und bei Fehlen bzw. Nicht-Konformität des Parameters den Request als  
1190 unzulässig abweisen, damit auf Basis dieser Parameter ausschließlich gültige Workflows  
1191 gestartet werden können und dem Versicherten bei Einsicht des Tasks der Weg in  
1192 entweder eine Apotheke oder ein Sanitätshaus oder eine andere zuständige Einrichtung  
1193 gewiesen werden kann.[<=]

#### 1194 **A\_19214 - E-Rezept-Fachdienst - Ergänzung Performer-Typ für** 1195 **Einlöseinstitutstyp**

1196 Der E-Rezept-Fachdienst MUSS beim Erzeugen eines Tasks das Feld  
1197 Task.performerType aus dem übergebenen, gültigen  
1198 Parameter Task.extension:flowType gemäß der Prozessparameter  
1199 [gemSpec\_DM\_eRp#19445] übernehmen.[<=]

#### 1200 **A\_19019 - E-Rezept-Fachdienst - Generierung Rezept-ID**

1201 Der E-Rezept-Fachdienst MUSS beim Anlegen eines neuen Tasks eine Rezept-ID gemäß  
1202 der Bildungsregel [gemSpec\_DM\_eRp#19217] generieren und als Identifier mit  
1203 Namenssystem <https://gematik.de/fhir/NamingSystem/PrescriptionID> dem Task  
1204 hinzufügen und sicherstellen, dass diese Rezept-ID innerhalb von 11 Jahren nach ihrer



1205 Erzeugung nicht erneut vergeben wird, damit es innerhalb der Aufbewahrungsfrist der  
1206 Abrechnungsdaten bei den Krankenkassen zu keinen Dubletten kommt. [`<=`]

1207

#### 1208 **A\_19021 - E-Rezept-Fachdienst - Generierung AccessCode**

1209 Der E-Rezept-Fachdienst MUSS beim Erzeugen eines Tasks mittels HTTP-POST/\$create-  
1210 Operation eine 256 Bit Zufallszahl mit einer Mindestentropie von 120 Bit  
1211 erzeugen, hexadezimal kodieren ([0-9a-f]{64}) und diese im zu speichernden Task als  
1212 externe ID in Task.identifizier:AccessCode  
1213 als <https://gematik.de/fhir/Namingsystem/AccessCode> hinzufügen, damit nachfolgende  
1214 Zugriffe auf diesen Datensatz nur durch Berechtigte in Kenntnis des AccessCodes  
1215 erfolgen. [`<=`]

#### 1216 **A\_19114 - E-Rezept-Fachdienst - Status draft**

1217 Der E-Rezept-Fachdienst MUSS die zulässige Anlage eines Tasks mittels HTTP-  
1218 POST/\$create-Operation im Status `Task.status = draft` vollziehen und beim  
1219 erfolgreichen Abschluss der Operation die angelegte Ressource Task im HTTP-Body der  
1220 HTTP-Response zurückgeben, damit der verordnende Leistungserbringer die generierte  
1221 Rezept-ID für die QES verwenden kann. [`<=`]

#### 1222 **6.1.2.2 POST /Task/<id>/\$activate**

1223 Die FHIR-Operation \$activate startet einen E-Rezept-Workflow eines zuvor unter einer  
1224 <id> angelegten neuen Tasks. Diese Operation steht ausschließlich verordnenden  
1225 Leistungserbringern zur Verfügung.

#### 1226 **A\_19022 - E-Rezept-Fachdienst - Rollenprüfung Verordnender aktiviert Rezept**

1227 Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks für ein E-Rezept mittels  
1228 HTTP-POST/\$activate-Operation auf den in der URL referenzierten /Task/<id>  
1229 sicherstellen, dass ausschließlich verordnende Leistungserbringer in der Rolle

- 1230 • oid\_arzt
- 1231 • oid\_zahnarzt
- 1232 • oid\_praxis\_arzt
- 1233 • oid\_zahnarztpraxis
- 1234 • oid\_praxis\_psychotherapeut
- 1235 • oid\_krankenhaus

1236 die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des  
1237 Aufrufers im ACCESS\_TOKEN im HTTP-RequestHeader "Authorization" feststellen,  
1238 damit E-Rezepte nicht durch Unberechtigte eingestellt werden können. [`<=`]

#### 1239 **~~A\_19024-01A\_19024~~ - E-Rezept-Fachdienst - Prüfung AccessCode Rezept** 1240 **aktualisieren**

1241 Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation  
1242 über /Task/<id>/\$activate den im HTTP-RequestHeader "X-AccessCode"  
1243 ~~übertragenen~~ oder URL-Parameter "`?ac=...`" ~~übertragenen~~ AccessCode gegen den im  
1244 referenzierten Task gespeicherten AccessCode Task.identifizier:AccessCode als  
1245 <https://gematik.de/fhir/Namingsystem/AccessCode> und den Status des Tasks auf  
1246 `Task.status = draft` prüfen und bei Ungleichheit oder Fehlen des HTTP-Headers die  
1247 Operation mit dem HTTP-Fehlercode 403 abbrechen, damit Zugriffe auf diesen Datensatz  
1248 nur durch Berechtigte in Kenntnis des AccessCodes erfolgen. [`<=`]

**A\_19020 - E-Rezept-Fachdienst - Schemavalidierung Rezept aktivieren**

Der E-Rezept-Fachdienst MUSS den im Aufrufparameter der HTTP-POST-Operation /Task/<id>/\$activate übergebenen FHIR-Operationsparameter des QES-Datensatzes als PKCS#7-Datei einer Enveloping CAdES-Signatur entgegennehmen und verarbeiten und bei Fehlen oder ungültiger ASN.1 Datenstruktur die Weiterverarbeitung im Fachdienst mit dem http-Status-Code 400 beantworten, damit kein Schadcode und keine "fachfremden" Daten in den E-Rezept-Fachdienst hochgeladen werden. [ <= ]

**A\_19025 - E-Rezept-Fachdienst - QES prüfen Rezept aktualisieren**

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/\$activate die qualifizierte Signatur des QES-Datensatzes gemäß [ETSI\_QES] prüfen und bei nicht gültiger qualifizierter Signatur die Operation mit Status 400 abbrechen bzw. bei gültiger Signatur den Datensatz als PKCS#7-Datei sicher speichern und inTask.input mit Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 1 über eine interne, eindeutige UUID referenzieren, damit der nachfolgende Workflow ausschließlich auf Basis medizinisch korrekter und vom Leistungserbringer mittels Signatur freigegebener Daten erfolgt. [ <= ]

**A\_20159 - E-Rezept-Fachdienst - QES Prüfung Signaturzertifikat des HBA**

Der E-Rezept-Fachdienst MUSS das QES-Signaturzertifikat C.HP.QES in der Signatur des übergebenen QES-Datensatzes gemäß [gemSpec\_PKI#TUC\_PKI\_030] mit folgenden Parametern auf Gültigkeit prüfen:

**Tabelle 6 : TAB\_eRPF\_D\_006 Parameter Prüfung Signaturzertifikat QES des HBA**

Parameter	
Zertifikat	Signaturzertifikat des HBA (eingebettet in Signatur-Objekt des QES-Datensatzes) C.HP.QES
Referenzzeitpunkt	<Zeitpunkt der QES-Erstellung gemäß signingTime im QES-Datensatz>
Offline-Modus	nein
OCSP-Response	(leer)

und darf die OCSP-Response für die Abfrage des Zertifikatsstatus für 12 Stunden zwischenspeichern.

Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig ] befunden werden und der HTTP-Request andernfalls mit dem HTTP-Status-Code 400 abgelehnt werden, damit sichergestellt wird, dass ausschließlich E-Rezepte verwaltet werden die von einer gültigen, nicht gesperrten Heilberufsidentität eines HBA signiert wurden. [ <= ]

**A\_19225 - E-Rezept-Fachdienst - QES durch berechtigte Berufsgruppe**

Der E-Rezept-Fachdienst MUSS die Aktivierung eines E-Rezept-Tasks mit dem HTTP-Status-Code 400 abbrechen, wenn die QES gemäß der professionOID des Signaturzertifikats des Signierers nicht von einer Berufsgruppe ausgestellt wurde, die der folgenden professionOID entspricht:

- oid\_arzt
- oid\_zahnarzt

damit nur solche Leistungserbringer ein signiertes E-Rezept einstellen, die zur Verordnung von Medikamenten ermächtigt sind. [≤]

#### **A\_19999 - E-Rezept-Fachdienst - Ergänzung PerformerTyp für Einlöseinstitutstyp**

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks aus dem Feld `Task.performerType` die Prozessparameter des Tasks gemäß `[gemSpec_DM_eRp#19445]` ableiten und befüllen. [≤]

#### **A\_19127 - E-Rezept-Fachdienst - Übernahme der KVN des Patienten**

Der E-Rezept-Fachdienst MUSS im Zugriff auf einen Task mittels HTTP-POST-Operation über `/Task/<id>/$activate` und bei gültiger qualifizierter elektronischer Signatur die KVN des Patienten dem Identifier <http://fhir.de/NamingSystem/gkv/kvid-10> der Patient-Ressource im signierten E-Rezept-Bundle gemäß [https://fhir.kbv.de/StructureDefinition/KBV\\_PR\\_ERP\\_Bundle](https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle) des QES-Datensatzes entnehmen und diese als Identifier mit dem Value-Set <http://fhir.de/NamingSystem/gkv/kvid-10> dem Task in `Task.for` hinzufügen, damit ausschließlich eine gültige, vom Arzt signierte Patientenreferenz im Workflow verwendet wird. [≤]

#### **A\_19128 - E-Rezept-Fachdienst - Status aktivieren**

Der E-Rezept-Fachdienst MUSS die zulässige Aktivierung eines Tasks mittels `/Task/<id>/$activate`-Operation im `StatusTask.status = ready` vollziehen und bei erfolgreichem Abschluss der Operation die Ressource Task im HTTP-Body der HTTP-Response zurückgeben, damit der verordnende Leistungserbringer über den erfolgreichen Abschluss der Operation in Kenntnis gesetzt wird. [≤]

#### **A\_19029-01A\_19029 - E-Rezept-Fachdienst - Serversignatur Rezept aktivieren**

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels `/Task/<id>/$activate` das im QES-Datensatz enthaltene FHIR-E-Rezept-Bundle vom Profil [https://fhir.kbv.de/StructureDefinition/KBV\\_PR\\_ERP\\_Bundle](https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle) in ein Bundle gleichen Typs in JSON-Repräsentation transformieren, einen neuen Identifier für `Bundle.id` als UUID generieren, das Bundle entsprechend der Kanonisierungsregeln <http://hl7.org/fhir/canonicalization/json#static> normalisieren und mit der Signaturidentität des Fachdienstes `IDC.FD.SIG` gemäß [FHIR-Sig] signieren und das signierte Bundle mit Referenz in `Task.input` mit Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 2 speichern, damit der Versicherte einen Nachweis über die Integrität der gespeicherten Daten einsehen kann. [≤]

Die Festlegungen in [FHIR-Sig] sind in Teilen unspezifisch, konkrete Beispiele finden sich in der gematik-API-Beschreibung für das E-Rezept auf <https://github.com/gematik/api-erp>

Die Signatur soll als JSON Web Signature [JWS] detached erstellt werden, dementsprechend bleibt das `data`-Feld der JWS-Struktur leer. Im JWS-Header muss das Zertifikat `C.FD.SIG` eingebettet werden, mit dessen zugehörigen privaten Signaturschlüssel signiert wurde. Als Wert für `targetFormat` ist der `MimeType application/fhir+json` und für `sigFormat` ist der `MimeType application/jose` zu verwenden.

### 6.1.2.3 POST /Task/<id>/\$accept

Die FHIR-Operation \$accept weist ein E-Rezept einem abgebenden Leistungserbringer (bzw. der Apotheke als Leistungserbringerinstitution) als "in Abgabe" befindlich über die <id> referenzierten Tasks zu. Diese Operation steht ausschließlich abgebenden Leistungserbringern in Kenntnis des AccessCodes zur Verfügung.

#### **A\_19166 - E-Rezept-Fachdienst - Rollenprüfung Abgebender ruft Rezept ab**

Der E-Rezept-Fachdienst MUSS beim Abrufen eines Tasks für ein E-Rezept mittels HTTP-POST/\$accept-Operation auf den in der URL referenzierten /Task/<id> sicherstellen, dass ausschließlich abgebende Leistungserbringer in der Rolle

- oid\_oeffentliche\_apotheke
- oid\_krankenhausapotheke

die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS\_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit E-Rezepte nicht durch Unberechtigte abgerufen werden können. [ <= ]

#### **~~A\_19167-01A\_19167~~ - E-Rezept-Fachdienst - Prüfung AccessCode Rezept abrufen**

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/\$accept den im HTTP-Header "X-AccessCode" oder URL-Parameter "?ac=..." ~~übertragenenenübertragenen~~ AccessCode gegen den im referenzierten Task gespeicherten AccessCode `Task.identifizier:AccessCode` als <https://gematik.de/fhir/Namingsystem/AccessCode> prüfen und bei Ungleichheit oder Fehlen des URL-Parameters die Operation mit dem HTTP-Fehlercode 403 abbrechen, damit Zugriffe auf diesen Datensatz nur durch Berechtigte in Kenntnis des AccessCodes erfolgen. [ <= ]

#### **A\_19168 - E-Rezept-Fachdienst - Rezept bereits in Abgabe oder Bearbeitung**

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/\$accept die Operation mit dem HTTP-Fehlercode 409 abbrechen, wenn der `StatusTask.status = completed`, `Task.status = in-progress` oder `Task.status = draft` ist, damit ein bereits in Abgabe befindliches oder beliefertes E-Rezept nicht durch eine zweite Apotheke bearbeitet werden kann. [ <= ]

#### **A\_19169 - E-Rezept-Fachdienst - Generierung Secret, Statuswechsel in Abgabe und Rückgabewert**

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/\$accept den Status des Tasks auf `Task.status = in-progress` setzen, eine 256 Bit Zufallszahl mit einer Mindestentropie von 120 Bit erzeugen, hexadezimal kodieren ([0-9a-f]{64}) und diese im zu speichernden Task als externe ID in `Task.identifizier:Secret` als <https://gematik.de/fhir/Namingsystem/Secret> hinzufügen und den Task im Bundle mit dem in `Task.input` mit Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 1 referenzierten QES-Datensatz als Binary-Ressource <https://www.hl7.org/fhir/binary.html> an den Aufrufer zurückgeben, damit das E-Rezept für die nachfolgende Bearbeitung durch den abrufenden Apotheker reserviert ist. [ <= ]

#### **A\_19149 - E-Rezept-Fachdienst - Prüfung Datensatz zwischenzeitlich gelöscht**

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/\$accept die Operation mit dem HTTP-Fehlercode 410 abbrechen, wenn der referenzierte /Task/<id> existiert, jedoch kein AccessCode im `Task.identifizier:AccessCode` als <https://gematik.de/fhir/Namingsystem/AccessCode> vorhanden ist oder der Status

1382 `Task.status = cancelled` ist, damit ein Apotheker den Versicherten über die  
1383 zwischenzeitliche Löschung des Datensatzes in Kenntnis setzen kann. [ <= ]

1384

#### 1385 **6.1.2.4 POST /Task/<id>/\$reject**

1386 Die FHIR-Operation `$reject` nutzt die abgebende LEI, um ein E-Rezept zurück zu geben.  
1387 Anschließend kann das E-Rezept von einer anderen Apotheke in Kenntnis des  
1388 AccessCodes und der ID des Tasks wieder abgerufen werden oder der Versicherte das E-  
1389 Rezept bei Bedarf löschen.

#### 1390 **A\_19170 - E-Rezept-Fachdienst - Rollenprüfung Abgebender ruft Rezept ab**

1391 Der E-Rezept-Fachdienst MUSS beim Zurückweisen eines Tasks für ein E-Rezept mittels  
1392 HTTP-POST/`$reject`-Operation auf den in der URL referenzierten `/Task/<id>`  
1393 sicherstellen, dass ausschließlich abgebende Leistungserbringer in der Rolle

- 1394 • `oid_oeffentliche_apotheke`
- 1395 • `oid_krankenhausapotheke`

1396 die Operation am Fachdienst aufrufen dürfen und die Rolle "`professionOID`" des  
1397 Aufrufers im `ACCESS_TOKEN` im HTTP-RequestHeader "`Authorization`" feststellen,  
1398 damit das E-Rezept nicht durch einen Unberechtigten zurückgewiesen werden kann. [ <= ]

#### 1399 **A\_19171 - E-Rezept-Fachdienst - Prüfung Secret Rezept zurückweisen**

1400 Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation  
1401 über `/Task/<id>/$reject` das im URL-Parameter "`?secret=...`" übertragene Secret  
1402 gegen das im referenzierten Task gespeicherte `SecretTask.identifizier:Secret` als  
1403 <https://gematik.de/fhir/Namingsystem/Secret> und auf `Task.status = in-progress`  
1404 prüfen und bei Ungleichheit oder Fehlen des URL-Parameters die Operation mit dem  
1405 HTTP-Fehlercode 403 abbrechen, damit der Zugriff auf diesen Datensatz nur durch den  
1406 Berechtigten in Kenntnis des Secrets erfolgt. [ <= ]

#### 1407 **A\_19172 - E-Rezept-Fachdienst - Löschung Secret und Status**

1408 Der E-Rezept-Fachdienst MUSS beim Zurückweisen eines Tasks mittels HTTP-POST-  
1409 Operation über `/Task/<id>/$reject` die externe ID in `Task.identifizier:Secret` als  
1410 <https://gematik.de/fhir/Namingsystem/Secret> löschen und den Status des referenzierten  
1411 Tasks auf `Task.status = ready` setzen, damit nachfolgende Zugriffe auf diesen  
1412 Datensatz durch Berechtigte in Kenntnis des AccessCodes erfolgen können. [ <= ]

#### 1413 **6.1.2.5 POST /Task/<id>/\$close**

1414 Die FHIR-Operation `$close` beendet den E-Rezept-Workflow des unter der `<id>` geführten  
1415 Tasks, erzeugt eine Quittung als Signatur über das vom abgebenden Leistungserbringer  
1416 eingestellte MedicationDispense und speichert die vom Apotheker übermittelten  
1417 Dispensierinformationen für den Versicherten. Diese Operation steht ausschließlich  
1418 abgebenden Leistungserbringern in Kenntnis eines generierten Secrets zur Verfügung.

#### 1419 **A\_19230 - E-Rezept-Fachdienst - Rollenprüfung Abgebender vollzieht Abgabe des Rezepts**

1421 Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks für ein E-Rezept mittels HTTP-  
1422 POST/`$close`-Operation auf den in der URL referenzierten `/Task/<id>` sicherstellen, dass  
1423 ausschließlich abgebende Leistungserbringer in der Rolle

- 1424 • `oid_oeffentliche_apotheke`
- 1425 • `oid_krankenhausapotheke`



die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS\_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit der E-Rezept-Workflow nicht durch einen Unberechtigten abgeschlossen werden kann. [ <= ]

#### A\_19231 - E-Rezept-Fachdienst - Prüfung Secret Rezept beenden

Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels HTTP-POST-Operation über /Task/<id>/<close> das im URL-Parameter "?secret=..." übertragene Secret gegen das im referenzierten Task gespeicherte SecretTask.identifizier:Secret als <https://gematik.de/fhir/Namingsystem/Secret> und auf Task.status = in-progress prüfen und bei Ungleichheit oder Fehlen des URL-Parameters die Operation mit dem HTTP-Fehlercode 403 abbrechen, damit der Zugriff auf diesen Datensatz nur durch den Berechtigten in Kenntnis des Secrets erfolgt. [ <= ]

#### A\_19248-01A\_19248 - E-Rezept-Fachdienst - Schemaprüfung und Speicherung MedicationDispense

Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels /Task/<id>/<close> das im http-Body des Requests enthaltene MedicationDispense-Objekt gegen das Profil <https://gematik.de/fhir/StructureDefinition/erxMedicationDispense> prüfen ~~und bei Gültigkeit, insbesondere~~

- die Korrektheit der Rezept-ID <https://gematik.de/fhir/NamingSystem/PrescriptionID> als zusätzlichen MedicationDispense.identifizier ,
- die KVRN <http://fhir.de/NamingSystem/gkv/kvid-10> des Versicherten ~~aus dem~~ referenzierten Task ~~in gegen~~ MedicationDispense.subject:identifizier und
- ob die ~~TelematikID~~ Telematik-ID der Apotheke gemäß ACCESS\_TOKEN mit dem Wert in MedicationDispense.performer.actor:identifizier sowie übereinstimmt.

Der E-Rezept-Fachdienst MUSS die Referenz auf den aufgerufenen Task /Task/<id> als MedicationDispense.supportingInformation übernehmen und die MedicationDispense für den Abruf durch den Versicherten speichern. [ <= ]

#### A\_19232 - E-Rezept-Fachdienst - Status beenden

Der E-Rezept-Fachdienst MUSS die zulässige Beendigung eines Tasks mittels /Task/<id>/<close>-Operation im StatusTask.status = completed vollziehen, damit der Workflow für den Versicherten als beendet und das E-Rezept somit als eingelöst dargestellt wird. [ <= ]

#### A\_20513 - E-Rezept-Fachdienst - nicht mehr benötigte Einlösekommunikation

Der E-Rezept-Fachdienst MUSS bei erfolgreicher Beendigung eines Tasks mittels /Task/<id>/<close>-Operation alle Communication-Ressourcen löschen, die eine Referenz auf diesen Task inCommunication.basedOn enthalten, damit nicht mehr benötigte Informationen über die Kommunikation zur Einlösung des E-Rezepts vom E-Rezept-Fachdienst entfernt werden. [ <= ]

#### A\_19233 - E-Rezept-Fachdienst - Serversignatur Rezept beenden (Quittung erstellen)

Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels /Task/<id>/<close> ein Quittungsbundle gemäß des FHIR-Profiles <https://gematik.de/fhir/StructureDefinition/erxReceipt> erstellen, die Telematik-ID der diese Operation aufrufenden Apotheke als Beneficiary in die erxComposition übernehmen, dieses Quittungs-Bundle in XML-Darstellung gemäß <http://hl7.org/fhir/canonicalization/xml#static> kanonisieren und mit der Signaturidentität des Fachdienstes ID.FD.SIG gemäß [RFC5652] mit Profil CAdES-BES

1475 ([CADES]) im Enveloping signieren, das Signatur-Ergebnis in der Codierung als  
1476 dss:Base64Signature-Objekt in `Bundle.signature` einbetten und dieses Quittungs-  
1477 Bundle mit Referenz in `Task.output` mit  
1478 Codingsystem <https://gematik.de/fhir/CodeSystem/Documenttype> = 3 speichern sowie als  
1479 Response des http-Requests an den Aufrufer zurückgeben, damit der Apotheker einen  
1480 Nachweis über den ordnungsgemäßen Abschluss des E-Rezept-Workflows als Quittung  
1481 erhält. [`<=`]

#### 1482 **6.1.2.6 POST /Task/<id>/\$abort**

1483 Die FHIR-Operation `$abort` bricht einen unter der `<id>` angelegten Task als aktiven E-  
1484 Rezept-Workflow ab und führt zum Löschen aller personenbezogenen und medizinischen  
1485 Daten. Diese Operation steht dem Versicherten, für den das E-Rezept erstellt wurde,  
1486 sowie allen Nutzern in Kenntnis des AccessCodes (verordnende und abgebende  
1487 Leistungserbringer, Vertreter) zur Verfügung.

#### 1488 **A\_19026 - E-Rezept-Fachdienst - Rollenprüfung Nutzer löscht Rezept**

1489 Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der `<id>`  
1490 adressierten `/Task/<id>/$abort` sicherstellen, dass ausschließlich Nutzer in der Rolle

- 1491 • `oid_versicherter`
- 1492 • `oid_arzt`
- 1493 • `oid_zahnarzt`
- 1494 • `oid_praxis_arzt`
- 1495 • `oid_zahnarztpraxis`
- 1496 • `oid_praxis_psychotherapeut`
- 1497 • `oid_krankenhaus`
- 1498 • `oid_oeffentliche_apotheke`
- 1499 • `oid_krankenhausapotheke`

1500 die Operation am Fachdienst aufrufen dürfen und die Rolle "`professionOID`" des  
1501 Aufrufers im ACCESS\_TOKEN im HTTP-RequestHeader "`Authorization`" feststellen,  
1502 damit E-Rezepte nicht durch Unberechtigte gelöscht werden können. [`<=`]

#### 1503 **A\_19145 - E-Rezept-Fachdienst - Statusprüfung Apotheker löscht Rezept**

1504 Der E-Rezept-Fachdienst MUSS das Löschen eines E-Rezepts über den mittels der `<id>`  
1505 adressierten `/Task/<id>/$abort` verhindern und die Operation mit dem HTTP-Fehlercode  
1506 403 abweisen, wenn der Status des adressierten Tasks gleich "`in-progress`" ist und die  
1507 Rolle des aufrufenden Nutzers einer der folgenden Rollen entspricht:

- 1508 • `oid_versicherter`
- 1509 • `oid_arzt`
- 1510 • `oid_zahnarzt`
- 1511 • `oid_praxis_arzt`
- 1512 • `oid_zahnarztpraxis`
- 1513 • `oid_praxis_psychotherapeut`
- 1514 • `oid_krankenhaus`

1515 damit Nutzer außerhalb der Apotheke keine Rezepte löschen, die sich aktuell in  
1516 Belieferung befinden. [`<=`]



## **A\_19146 - E-Rezept-Fachdienst - Statusprüfung Nutzer (außerhalb Apotheke) löscht Rezept**

Der E-Rezept-Fachdienst MUSS das Löschen eines E-Rezepts über den mittels der <id> adressierten/Task/<id>/\$abort verhindern und die Operation mit dem HTTP-Fehlercode 403 abweisen, wenn der Status des adressierten Tasks ungleich "in-progress" ist und die Rolle des aufrufenden Nutzers einer der folgenden Rollen entspricht:

- oid\_oeffentliche\_apotheke
- oid\_krankenhausapotheke

damit kein Apotheker ein Rezept löscht, das ihm nicht ausdrücklich zugewiesen wurde. [ <= ]

## **~~A\_20546-01A\_20546~~ - E-Rezept-Fachdienst - Prüfung KVNR, Versicherter löscht Rezept**

Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts durch einen Versicherten, wenn der HTTP-Request keinen HTTP-Header "X-AccessCode" oder URL-Parameter "?ac=..." enthält, den Versicherten anhand der KVNR aus dem ACCESS\_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, diese gegen die inTask.for mit dem Value-Set <http://fhir.de/NamingSystem/gkv/kvid-10> hinterlegte KVNR des begünstigten Patienten prüfen und bei Mismatch den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich der begünstigte Patient als Berechtigter ohne Kenntnis des AccessCodes ein E-Rezept löscht. [ <= ]

## **~~A\_20547 - E-Rezept-Fachdienst - Prüfung KVNR, Vertreter löscht Rezept~~**

~~Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts durch einen Versicherten, wenn der HTTP-Request einen HTTP-Header "X-AccessCode" enthält, diesen gegen den im referenzierten Task enthaltenen AccessCode prüfen und bei Mismatch den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich Vertreter in Kenntnis des AccessCodes als Berechtigte ein E-Rezept löschen. [ <= ]~~

## **~~A\_19120-01A\_19120~~ - E-Rezept-Fachdienst - Prüfung AccessCode, Verordnender löscht Rezept**

Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der <id> adressierten/Task/<id>/\$abort durch verordnende Leistungserbringer den im HTTP-Header "X-AccessCode" bzw. URL-Parameter "?ac=..." gegen den im referenzierten Task enthaltenen AccessCode prüfen und bei Mismatch oder Fehlen im HTTP-Header den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich die verordnende Leistungserbringerinstitution in Kenntnis des AccessCodes als Berechtigte ein E-Rezept löschen. [ <= ]

## **A\_19224 - E-Rezept-Fachdienst - Prüfung Secret, Apotheker löscht Rezept**

Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der <id> adressierten/Task/<id>/\$abort durch abgebende Leistungserbringer (Apotheken) das im URL-Parameter "?secret=..." übertragene Geheimnis gegen das im referenzierten Task enthaltene Secret inTask.identifizier prüfen und bei Mismatch oder Fehlen des URL-Parameters den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich Apotheker in Kenntnis des Secret als Berechtigte ein E-Rezept löschen. [ <= ]

## **~~A\_19027-01A\_19027~~ - E-Rezept-Fachdienst - Rezept löschen**

Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der <id> adressierten/Task/<id>/\$abort alle personenbezogenen medizinischen Daten aus dem referenzierten Task und allen Versionen der Historie des Task entfernen. Dies gilt insbesondere für:

- Task.for (KVNR des Patienten)--> löschen
- Task.input --> löschen (inkl. aller referenzierten Elemente)

- 1566 • Task.output --> löschen (inkl. aller referenzierten Elemente)
- 1567 • Task.identifizier (AccessCode) --> löschen
- 1568 • Task.identifizier (Secret, falls vorhanden) --> löschen
- 1569 • MedicationDispense --> die in MedicationDispense.supportingInformation auf
- 1570 Task.id verweist
- 1571 • Communication --> die in Communication.basedOn auf Task.id verweist

1572 damit dem Betroffenenrecht auf Löschen durch den Versicherten entsprochen wird und  
1573 beim Löschen durch den Verordnenden dem Versicherten eine aussagekräftige  
1574 Fehlermeldung durch einen Apotheker vermittelt werden kann. [`<=`]

#### 1575 **A\_19121 - E-Rezept-Fachdienst - Finaler Status cancelled**

1576 Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der `<id>`  
1577 adressierten/Task/`<id>`/abort den Status des Tasks `Task.status` auf den Wert  
1578 "cancelled" setzen, damit das E-Rezept nicht weiter bearbeitet werden kann. [`<=`]

## 1579 **6.2 Ressource MedicationDispense**

1580 Dem Versicherten werden über die Ressource MedicationDispense Informationen über ein  
1581 eingelöstes E-Rezept bereitgestellt. Im MedicationDispense ist dabei die Referenz auf das  
1582 abgegebene Medikament enthalten. Diese Informationen unterstützen den Versicherten  
1583 im Versorgungsprozess, indem ihm bspw. mittels dieser Informationen ein digitaler  
1584 Beipackzettel oder weitere Informationen wie Applikationsanleitungen zur Verfügung  
1585 gestellt werden können. Der Zugriff auf die Ressource MedicationDispense erfolgt  
1586 ausschließlich lesend über die http-GET-Operation. Das Löschen erfolgt indirekt über das  
1587 Löschen des der MedicationDispense zugrunde liegenden Tasks.

#### 1588 **A\_19400 - E-Rezept-Fachdienst - unzulässige Operationen MedicationDispense**

1589 Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource MedicationDispense  
1590 mittels der HTTP-Operationen PUT, PATCH, HEAD und DELETE sowie POST unterbinden,  
1591 damit keine unzulässigen Operationen auf den Rezeptdaten ausgeführt werden  
1592 können. [`<=`]

### 1593 **6.2.1 HTTP-Operation GET /MedicationDispense**

#### 1594 **A\_19405 - E-Rezept-Fachdienst - Rollenprüfung Versicherter liest** 1595 **MedicationDispense**

1596 Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt  
1597 /MedicationDispense und auf einen konkreten über `<id>`  
1598 adressierten/MedicationDispenses/`<id>` sicherstellen, dass ausschließlich Versicherte in  
1599 der Rolle

- 1600 • oid\_versicherter

1601 die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des  
1602 Aufrufers im ACCESS\_TOKEN im HTTP-RequestHeader "Authorization" feststellen,  
1603 damit Dispensierinformationen nicht durch Unberechtigte ausgelesen werden  
1604 können. [`<=`]

**A\_19406 - E-Rezept-Fachdienst - Filter MedicationDispense auf KVNR des Versicherten**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /MedicationDispense die dem Versicherten zugeordneten MedicationDispense-Ressourcen anhand der KVNR des Versicherten im ACCESS\_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, die in MedicationDispense.identifizier mit Codesystem <http://fhir.de/NamingSystem/gkv/kvid-10> die entsprechende KVNR des begünstigten Patienten referenziert haben, damit ausschließlich Versicherte ihre eigenen Dispensierinformationen einsehen können. [ <= ]

**A\_19518 - E-Rezept-Fachdienst - Suchparameter für MedicationDispense**

Der E-Rezept-Fachdienst MUSS das Eingrenzen einer Suchanfrage auf /MedicationDispense über die URL-Parameter gemäß <https://www.hl7.org/fhir/medicationdispense.html#search> für die Attribute MedicationDispense.whenHandedOver und MedicationDispense.performer.actor erlauben, damit Versicherte eine Suche und Sortierung nach Ausgabedatum sowie der aufgesuchten Apotheke durchführen können. [ <= ]

**6.3 Ressource Communication**

Der E-Rezept-Fachdienst ermöglicht eine direkte Kommunikation zwischen Versicherten und Apotheken über die Belieferung von E-Rezepten über den Endpunkt <Fachdienst-URL>/Communication gemäß der FHIR-Definition in <https://www.hl7.org/fhir/communication.html>.

**A\_19401 - E-Rezept-Fachdienst - unzulässige Operationen Communication**

Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource Communication mittels der HTTP-Operationen PUT, PATCH und HEAD unterbinden, damit keine unzulässigen Operationen auf den Kommunikationsnachrichten ausgeführt werden können. [ <= ]

**A\_19446 - E-Rezept-Fachdienst - Rollenprüfung Versicherter oder Apotheker liest Rezept**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET und POST-Operation auf den Endpunkt /Communication sicherstellen, dass ausschließlich Versicherte und Apotheken in der Rolle

- oid\_versicherter
- oid\_oeffentliche\_apotheke
- oid\_krankenhausapotheke

die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS\_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit der Nachrichtenaustausch nicht zwischen Unbefugten erfolgt. [ <= ]

**6.3.1 HTTP-Operation GET**

Die HTTP-Operation GET wird für den Nachrichtenabruf verwendet. Dabei werden alle Anfragen auf Basis der KVNR bzw. Telematik-ID im übergebenen ACCESS\_TOKEN gefiltert, um die Nachrichten des jeweiligen Empfängers zu finden. Zusätzliche Filteranfragen für den Abruf ungelesener Nachrichten oder eine Sortierung nach Sendedatum sind zusätzlich möglich.

### 6.3.1.1 GET /Communication/

#### A\_19520 - E-Rezept-Fachdienst - Nachrichten für Empfänger filtern

Der E-Rezept-Fachdienst MUSS beim Abrufen von Nachrichten über die http-Operation GET auf den Endpunkt `/Communication` bzw. beim Abruf einer einzelnen Nachricht über `/Communication/<id>` ausschließlich die Nachrichten an den Aufrufer zurückgeben, die im Attribut `Communication.recipient` oder `Communication.sender` mit dem entsprechenden NamingSystem <https://gematik.de/fhir/NamingSystem/TelematikID> für Apotheken bzw. <http://fhir.de/NamingSystem/gkv/kvid-10> für Versicherte den gleichen Typ und den identischen Wert haben wie im Attribut "idNummer" des übergebenen ACCESS\_TOKEN im HTTP-Header "Authorization" für KVN- bzw. Telematik-ID, damit keine Nachrichten an Dritte unrechtmäßig ausgelesen werden. [ $\leq$ ]

#### A\_19521 - E-Rezept-Fachdienst - Nachrichten als abgerufen markieren

Der E-Rezept-Fachdienst MUSS beim Abrufen von Nachrichten über die http-Operation GET auf den Endpunkt `/Communication` bzw. beim Abruf einer einzelnen Nachricht über `/Communication/<id>` den Wert des Attributs `Communication.received` = <aktuelle Systemzeit> setzen, wenn dieser Wert zum Zeitpunkt des Abrufs der Nachrichten NULL ist, damit Nutzer eine Filtermöglichkeit auf "neue Nachrichten" haben. [ $\leq$ ]

#### A\_19522 - E-Rezept-Fachdienst - Nachrichtenabruf Suchparameter

Der E-Rezept-Fachdienst MUSS das Eingrenzen einer Suchanfrage auf `/Communication` über die URL-Parameter gemäß <https://www.hl7.org/fhir/communication.html#search> für die Attribute `Communication.sent`, `Communication.received`, `Communication.recipient` und `Communication.sender` erlauben, damit Versicherte eine Suche nach neuen Nachrichten, Sende- bzw. Empfangsrichtung und eine Sortierung nach Sende- und Empfangsdatum durchführen können. [ $\leq$ ]

#### A\_19534 - E-Rezept-Fachdienst - Rückgabe Communication im Bundle Paging

Der E-Rezept-Fachdienst KANN beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Communication` die Ergebnisliste der Communication-Ressourcen bei mehr als 50 Einträgen das Suchergebnis in einem Paging-Mechanismus auf mehrere Ergebnis-Bundle aufteilen, damit der Nutzer eine komfortable Navigationsmöglichkeit in seinen Nachrichten erhält. [ $\leq$ ]

## 6.3.2 HTTP-Operation POST

Mit der HTTP-Operation POST erfolgt der Versand einer Kommunikationsnachricht an eine Identität der Telematikinfrastruktur, welche über ihre systemweit eindeutige Identifikationsnummer Telematik-ID bzw. Versicherten-ID (10-stelliger Anteil der KVN- bzw. Telematik-ID) adressiert wird.

### 6.3.2.1 POST /Communication/

#### A\_19447 - E-Rezept-Fachdienst - Nachricht einstellen Schemaprüfung

Der E-Rezept-Fachdienst MUSS beim Einstellen einer Nachricht über die http-Operation POST auf den Endpunkt `/Communication` die im http-Request-Body übergebene Communications-Ressource gegen das aus der Kommunikationsbeziehung ableitbare, zulässige Schema gemäß TAB\_eRPFD\_008

**Tabelle 7: TAB\_eRPFD\_008 Nachrichtentyp zu Kommunikationsbeziehung**

sender	recipient	zusätzliche Bedingung	Schema
--------	-----------	-----------------------	--------

KVNR	Telema tikID	Communication. basedOn referenziert Task	<a href="https://gematik.de/fhir/StructureDefinition/erxCommunicationDispReq">https://gematik.de/fhir/StructureDefinition/erxCommunicationDispReq</a>
KVNR	Telema tikID	Communication. about referenziert Medication	<a href="https://gematik.de/fhir/StructureDefinition/erxCommunicationInfoReq">https://gematik.de/fhir/StructureDefinition/erxCommunicationInfoReq</a>
Telema tikID	KVNR	-	<a href="https://gematik.de/fhir/StructureDefinition/erxCommunicationReply">https://gematik.de/fhir/StructureDefinition/erxCommunicationReply</a>
KVNR	KVNR	-	<a href="https://gematik.de/fhir/StructureDefinition/erxCommunicationRepresentative">https://gematik.de/fhir/StructureDefinition/erxCommunicationRepresentative</a>

1690

1691 prüfen und den Aufruf bei Nicht-Konformität mit dem http-Status-Code 400 ablehnen,

1692 damit ausschließlich konforme E-Rezept-Nachrichten ausgetauscht werden. [ &lt;= ]

1693 **A\_19448 - E-Rezept-Fachdienst - Nachricht einstellen Absender und**1694 **Sendedatum**

1695 Der E-Rezept-Fachdienst MUSS beim Einstellen einer Nachricht über die http-Operation  
 1696 POST auf den Endpunkt /Communication die Absenderidentifikation aus dem Attribut  
 1697 "idNummer" des übergebenen IDP-Token im HTTP-Header "Authorization" mit dem  
 1698 entsprechenden NamingSystem <https://gematik.de/fhir/NamingSystem/TelematikID> für  
 1699 Apotheken bzw. <http://fhir.de/NamingSystem/gkv/kvid-10> für Versicherte übernehmen  
 1700 sowie das Absendedatum Communication.sent auf die aktuelle Systemzeit des E-Rezept-  
 1701 Fachdienstes setzen, damit Absender und Sendezeitpunkt für den Empfänger eindeutig  
 1702 sind. [ <= ]

1703 **A\_20229 - E-Rezept-Fachdienst - Nachrichtenzähler bei Versicherter-zu-**1704 **Versichertem-Kommunikation**

1705 Der E-Rezept-Fachdienst MUSS die zulässige Anzahl der Communication-Ressourcen des  
 1706 Schemas <https://gematik.de/fhir/StructureDefinition/erxCommunicationRepresentative>  
 1707 zur Versicherter-zu-Versichertem-Kommunikation auf einen konfigurierbaren  
 1708 Maximalwert (Default: 10) je referenziertem Task beschränken und bei Überschreiten des  
 1709 Maximalwerts das Einstellen einer Nachricht mit dem http-Status-Code 429 abbrechen,  
 1710 damit Versicherte den E-Rezept-Fachdienst nicht für beliebige Kommunikation außerhalb  
 1711 der Vertretung in der Einlösung von E-Rezepten benutzen. [ <= ]

1712 **A\_20511 - E-Rezept-Fachdienst - Nachrichtenzähler zweckgebunden**

1713 Der E-Rezept-Fachdienst DARF die Anzahl der Communication-Ressourcen je  
 1714 referenziertem Task für die Versicherter-zu-Versichertem-Kommunikation NICHT zu  
 1715 anderen Zwecken verwenden, als für die Beschränkung der Anzahl auf den maximalen  
 1716 Wert. [ <= ]

1717 **A\_20230 - E-Rezept-Fachdienst - Einlösbare E-Rezepte für Versicherter-zu-**1718 **Versichertem-Kommunikation**

1719 Der E-Rezept-Fachdienst MUSS beim Einstellen einer Nachricht des  
 1720 Schemas <https://gematik.de/fhir/StructureDefinition/erxCommunicationRepresentative>  
 1721 zur Versicherter-zu-Versichertem-Kommunikation über die http-Operation POST auf den  
 1722 Endpunkt /Communication mit dem http-Status-Code 400 abbrechen, wenn der  
 1723 referenzierte Task nicht im Zustand "ready" oder "in-progress" ist, damit die Weitergabe



1724 des Zugriffs auf E-Rezepte ausschließlich auf einlösbare bzw. in Arbeit befindliche  
1725 Verordnungen beschränkt wird. [ <= ]

1726 **A\_20231 - E-Rezept-Fachdienst - Ausschluss Nachrichten an Empfänger gleich**  
1727 **Absender**

1728 Der E-Rezept-Fachdienst MUSS das Einstellen einer Nachricht über die http-Operation  
1729 POST auf den Endpunkt /Communication mit dem http-Status-Code 400 abbrechen,  
1730 wenn der Empfänger Communication.recipient gleich der Absenderidentifikation im  
1731 Attribut "idNummer" des übergebenen IDP-Token im HTTP-Header "Authorization" ist,  
1732 damit irreführende Kommunikationsbeziehungen nicht zu einer vermeidbaren  
1733 Mehrbelastung des E-Rezept-Fachdienstes führen. [ <= ]

1734 **A\_19450 - E-Rezept-Fachdienst - Nachricht einstellen Schadcodeprüfung**

1735 Der E-Rezept-Fachdienst MUSS das Einstellen einer Nachricht über die http-Operation  
1736 POST auf den Endpunkt /Communication mit dem http-Status-Code 400 abbrechen,  
1737 wenn der Nachrichteninhalt Communication.payload größer als 10 kByte ist oder externe  
1738 URLs enthält oder ein Attachment mit MimeType "application/\*" enthält, damit über  
1739 den E-Rezept-Fachdienst kein Schadcode verteilt wird. [ <= ]

1740 **A\_20885 - E-Rezept-Fachdienst - Nachricht einstellen Prüfung**  
1741 **Versichertenbezug und Berechtigung**

1742 Der E-Rezept-Fachdienst MUSS das Einstellen einer Nachricht über die http-Operation  
1743 POST auf den Endpunkt /Communication mit dem http-Status-Code 400 abbrechen,  
1744 wenn der Wert Communication.basedOn einen Task referenziert und dabei die KVNR des  
1745 referenzierten Tasks Task.for ungleich der KVNR des Einstellenden in "idNummer" des  
1746 übergebenen ACCESS\_TOKEN und auch der AccessCode der Task-Referenz ungleich dem  
1747 AccessCode in Task.identifizier ist, um irreführende Testnachrichten zu unterbinden, die  
1748 eine vermeidbare Mehrbelastung für den E-Rezept-Fachdienst darstellen. [ <= ]

1749 **6.3.3 HTTP-Operation DELETE**

1750 Mit der HTTP-Operation DELETE kann ein Nutzer eine verschickte  
1751 Kommunikationsnachricht als Absender löschen, um bspw. einen Irrläufer zurückzurufen.  
1752 Der E-Rezept-Fachdienst prüft, ob die Nachricht bereits abgerufen wurde. Das Löschen  
1753 einer ungelesenen Nachricht erfolgt sofort, das Löschen einer bereits abgerufenen  
1754 Nachricht wird vom E-Rezept-Fachdienst abgelehnt, um darauf hinzuweisen, dass die  
1755 Nachricht als Kopie im Clientsystem des Empfängers vorliegt und das Löschen nicht vor  
1756 unberechtigter Einsichtnahme schützt.

1757 Um den Schutz vor unberechtigter Einsichtnahme in persönliche Daten durchzusetzen, ist  
1758 es ratsam bei bereits gelesenen Nachrichten den referenzierten E-Rezept-Task zu  
1759 löschen. Für eine geeignete Nutzerführung auf Clientseite ergänzt der E-Rezept-  
1760 Fachdienst die http-Response um das Header-Attribut "Warning" mit einem  
1761 entsprechenden Hinweis. Das Löschen des Task führt direkt auch zum Löschen aller  
1762 Kommunikationsnachrichten, die auf diesen Task verweisen. Damit kann ein fälschlich  
1763 adressierter Vertreter eines Versicherten keine Einsicht in die Daten des E-Rezepts mehr  
1764 nehmen bzw. das E-Rezept in keiner Apotheke mehr einlösen.

1765 **6.3.3.1 DELETE /Communication/**

1766 **A\_20258 - E-Rezept-Fachdienst - Communication löschen auf Basis Absender-ID**

1767 Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-DELETE-Operation  
1768 auf /Communication/<id> die über <id> identifizierte Communication-Ressource anhand  
1769 der KVNR bzw. Telematik-ID des aufrufenden Nutzers im ACCESS\_TOKEN im  
1770 "Authorization"-Header des HTTP-Requests über das Absender-

1771 Attribut `Communication.sender` lokalisieren und löschen, damit Nutzer irrtümlich  
1772 versendete oder nicht mehr gewünschte Nachrichten vom E-Rezept-Fachdienst entfernen  
1773 können.[<=]

1774 **A\_20259 - E-Rezept-Fachdienst - Communication löschen mit Warnung wenn**  
1775 **vom Empfänger bereits abgerufen**

1776 Der E-Rezept-Fachdienst MUSS beim Löschen einer Communication-Ressource der http-  
1777 Response das http-Header-Feld "Warning" mit dem Zeitpunkt des Nachrichtenabrufs  
1778 durch den Empfänger ergänzen (z.B. "Warning: 'Deleted message delivered at  
1779 2020-07-01 10:30:00'"), wenn die Nachricht bereits durch den Empfänger abgerufen  
1780 wurde (`Communication.received` ungleich NULL, bzw. enthält Datum des Abrufs), um  
1781 dem Absender einen Hinweis anzeigen zu können.[<=]

1782 **6.4 Ressource AuditEvent**

1783 Der E-Rezept-Fachdienst protokolliert alle Zugriffe auf personenbezogene und  
1784 medizinische Daten der E-Rezepte von Versicherten. Über den Endpunkt `<Fachdienst-  
1785 URL>/AuditEvent` stehen diese für den Abruf durch den jeweils betroffenen Versicherten  
1786 zur Verfügung. Die Protokolleinträge werden gemäß der Löschfrist im E-Rezept-  
1787 Fachdienst gespeichert und nach Ablauf dieser Frist automatisch gelöscht.

1788 **A\_19402 - E-Rezept-Fachdienst - unzulässige Operationen AuditEvent**

1789 Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource AuditEvent mittels der  
1790 HTTP-Operationen PUT, PATCH, HEAD, DELETE und POST unterbinden, damit keine  
1791 unzulässigen Operationen auf den Protokolldaten ausgeführt werden können.[<=]

1792 **6.4.1 HTTP-Operation GET /AuditEvent**

1793 **A\_19395 - E-Rezept-Fachdienst - Rollenprüfung Versicherter liest AuditEvent**

1794 Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt  
1795 `/AuditEvent` und auf einen konkreten über `<id>`  
1796 adressierten `/AuditEvent/<id>` sicherstellen, dass ausschließlich Versicherte in der Rolle  
1797 

- `oid_versicherter`

1798 die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des  
1799 Aufrufers im ACCESS\_TOKEN im HTTP-RequestHeader "Authorization" feststellen,  
1800 damit E-Rezept-Protokolleinträge nicht durch Unberechtigte ausgelesen werden  
1801 können.[<=]

1802 **A\_19396 - E-Rezept-Fachdienst - Filter AuditEvent auf KVNR des Versicherten**

1803 Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt  
1804 `/AuditEvent` die dem Versicherten zugeordneten AuditEvent-Ressourcen anhand der  
1805 KVNR des Versicherten im ACCESS\_TOKEN im "Authorization"-Header des HTTP-  
1806 Requests identifizieren, die in `AuditEvent.entity.name` die entsprechende KVNR des  
1807 begünstigten Patienten referenziert haben, damit ausschließlich Versicherte ihre eigenen  
1808 E-Rezept-Protokolleinträge einsehen können.[<=]

1809 **A\_19399 - E-Rezept-Fachdienst - Suchparameter AuditEvent**

1810 Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt  
1811 `/AuditEvent` eine Sortierung über die Attribute der Protokolleinträge "date", "agent"  
1812 und "subType" gemäß der Festlegungen für die Ressource  
1813 AuditEvent <https://www.hl7.org/fhir/auditevent.html#search> in den URL-Parametern  
1814 zulassen, damit sich Versicherte in ihrem Zugriffsprotokoll besser zurecht finden.[<=]



**A\_19397 - E-Rezept-Fachdienst - Rückgabe AuditEvents im Bundle**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /AuditEvent die Ergebnisliste der AuditEvent-Ressourcen bei mehr als einem Eintrag als Ergebnis-Bundle an den Aufrufer zurückgeben, damit der Versicherte eine vollständige Einsicht in das Zugriffsprotokoll erhält. [ <= ]

**A\_19398 - E-Rezept-Fachdienst - Rückgabe AuditEvents im Bundle Paging**

Der E-Rezept-Fachdienst KANN beim Aufruf der HTTP-GET-Operation auf den Endpunkt /AuditEvent die Ergebnisliste der AuditEvent-Ressourcen bei mehr als 50 Einträgen das Suchergebnis in einem Paging-Mechanismus auf mehrere Ergebnis-Bundle aufteilen, damit der Versicherte eine komfortable Navigationsmöglichkeit in seinem Zugriffprotokoll erhält. [ <= ]

**6.5 Ressource Device**

Gemäß CapabilityStatement und FHIR-Profilierung stellt der E-Rezept-Fachdienst statische Informationen über seine Produkttypversion zur Verfügung. Mit diesen erhalten Clients eine entsprechende Auskunft und bei Bedarf das Signaturzertifikat C.FD.SIG für die Signaturprüfung, für welches der E-Rezept-Fachdienst serverseitige Signaturen für die E-Rezept-Quittung und den E-Rezept-Datensatz für Versicherte erstellt.

**A\_20744 - E-Rezept-Fachdienst - Selbstauskunft Device-Informationen**

Der E-Rezept-Fachdienst MUSS über die http-Operation GET /Device dem aufrufenden Clientsystem eine statische Auskunft gemäß der Profilierung der Device-Ressource bereitstellen. [ <= ]

1837

## 7 Informationsmodell

1838 Der E-Rezept-Fachdienst verwaltet E-Rezepte mittels der HL7-FHIR-Workflow-Ressource  
1839 Task. Die Statusübergänge im Task werden durch verschiedene FHIR-Operationen der  
1840 Ressource Task getriggert. Als Payload eines Tasks werden verschiedene E-Rezept-  
1841 Bundles als Nutzdaten transportiert bzw. fachdienstseitig erzeugt.

- 1842 • E-Rezept-Bundle, enveloping in QES-Datensatz enthalten (Task.input),  
1843 Enthält die eigentlichen Verordnungsdaten, inkl. qualifizierter elektronischer  
1844 Signatur des Arztes bzw. Zahnarztes
- 1845 • Kopie des E-Rezept-Bundles (Task.input),  
1846 Kopie der Verordnungsdaten für die Einsicht durch den Versicherten, inkl.  
1847 serverseitiger Signatur
- 1848 • Quittungs-Bundle (Task.output),  
1849 Zusammenstellung aus QES-signierten Verordnungsdaten und Workflowdaten,  
1850 inkl. serverseitiger Signatur

1851 Für die Nachvollziehbarkeit der Medikamentenabgabe an den Versicherten erwartet der  
1852 E-Rezept-Fachdienst zum Abschluss des Workflows die Übergabe einer  
1853 MedicationDispense-Ressource von der abgebenden Leistungserbringereinstitution  
1854 (Apotheke), die das abgegebene Medikament in einer Medication-Ressource  
1855 dokumentiert. Die Verbindung zwischen MedicationDispense und Task erfolgt über  
1856 MedicationDispense.supportingInformation.

1857 Über den Zugriff auf personenbezogene medizinische Daten des Tasks und der  
1858 MedicationDispenses führt der E-Rezept-Fachdienst ein Zugriffsprotokoll mittels der  
1859 Ressource AuditEvent zum Abruf durch den Versicherten. Das Attribut AuditEvent.entity  
1860 speichert dabei die Referenz des betroffenen Datenobjekts und die KVNR des  
1861 Versicherten.

1862 Über die Ressource Communication steht Versicherten und Apotheken ein  
1863 Nachrichtenaustausch zur Verfügung. Communication-Einträge können dabei vom  
1864 Versicherten eingestellt an Apotheken adressiert werden, Apotheken können  
1865 Communication-Einträge für Versicherte bereitstellen. Mit der Communication-Ressource  
1866 stellt der E-Rezept-Fachdienst keine vollwertige Messenger-Plattform zur Verfügung.  
1867 Nachrichten von Versicherten an Versicherte sind im begrenzten Rahmen (Referenz eines  
1868 Tasks und maximale Anzahl Nachrichten zu einem Task) zulässig, die Größe  
1869 transportierbarer Communications-Einträge ist bewusst auf wenige Kilobytes begrenzt,  
1870 um den Transport von Schadcode zu erschweren und den Nachrichtenaustausch auf die  
1871 Belieferung von E-Rezepten zu beschränken. Um verschiedene  
1872 Kommunikationsbeziehungen [Versicherter - Apotheke, Apotheke - Versicherter,  
1873 Versicherter - Versicherter] abzubilden, werden dezidierte Profile für die Communication-  
1874 Ressource definiert. Mit diesen Profilen werden Nachrichtentypen realisiert, um die  
1875 jeweiligen Restriktionen für Verfügbarkeitsanfrage, Einlöseauftrag und  
1876 Vertreterkommunikation abzubilden.

1877 Der E-Rezept-Fachdienst speichert und verwaltet keine Patient-, Practitioner und  
1878 Organization-Ressourcen. Sämtliche Bezüge zu verordnenden und abgebenden  
1879 Leistungserbringern, Praxen und Apotheken sowie Versicherten erfolgen über logische  
1880 Referenzen. Somit wird der Aufbau einer zentralen Patienten-Kartei und Liste  
1881 verordnender Ärzte im E-Rezept-Fachdienst unnötig. Zudem löscht der E-Rezept-  
1882 Fachdienst regelmäßig veraltete Daten, um die Verfügbarkeit der für den Workflow  
1883 notwendigen Daten auf ein Minimum zu beschränken.

- 1884 Der E-Rezept-Fachdienst startet einen E-Rezept-Workflow ausschließlich bei einer  
 1885 gültigen Verordnung, das heißt, das E-Rezept-Bundle muss über eine gültige QES eines  
 1886 zur Verordnung berechtigten Leistungserbringers verfügen. Zudem wird die  
 1887 Patientenreferenz (KVN) aus genau diesem Datensatz verwendet, um dem Patienten,  
 1888 dem diese Verordnung gemäß ärztlicher Signatur gilt, die Hoheit über das E-Rezept  
 1889 einzuräumen.
- 1890 Die nachfolgende Abbildung gibt eine Übersicht der verwalteten FHIR-Ressourcen.

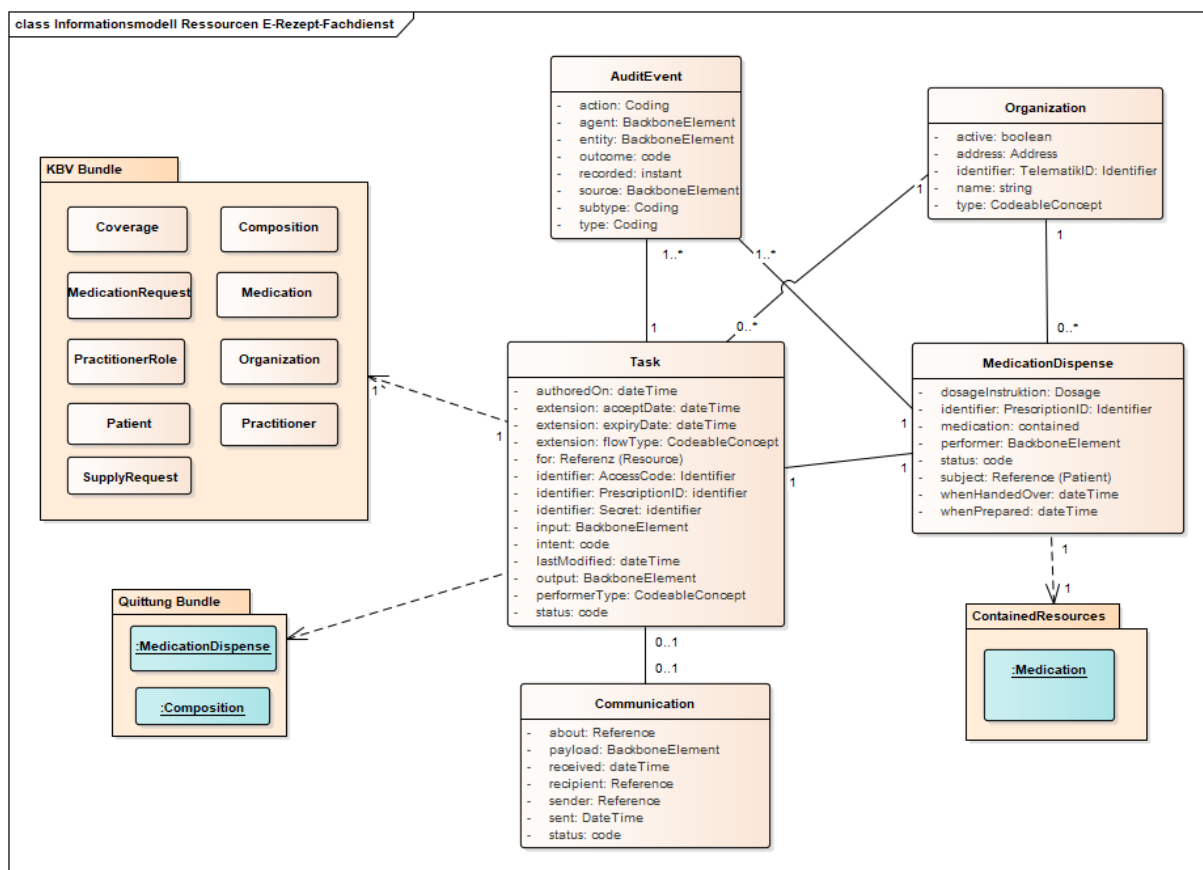


Abbildung 3: Informationsmodell FHIR-Ressourcen E-Rezept-Fachdienst

1893

## 8 Anhang A – Verzeichnisse

1894

### 8.1 Abkürzungen

Kürzel	Erläuterung
AVS	Apothekenverwaltungssystem
FdV	Frontend des Versicherten
FHIR	Fast Healthcare Interoperable Resources
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
KVNR	Krankenversichertennummer
LEI	Leistungserbringerinstitution
OCSP	Online Certificate Status Protocol
OWASP	Open Web Application Security Project
PVS	Praxisverwaltungssystem
QES	Qualifizierte Elektronische Signatur
SLA	Service Level Agreement
SMC-B	Security Module Card Typ B, Institutionenkarte
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust Service Status List
VAU	Vertrauenswürdige Ausführungsumgebung

1895

### 8.2 Glossar

Begriff	Erläuterung
---------	-------------

Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
------------------	---

1896 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung  
1897 gestellt.

## 1898 8.3 Abbildungsverzeichnis

1899	<a href="#">Abbildung 1: Systemüberblick .....</a>	8
1900	<a href="#">Abbildung 2: Systemkontext E-Rezept-Fachdienst .....</a>	9
1901	<a href="#">Abbildung 3: Informationsmodell FHIR-Ressourcen E-Rezept-Fachdienst .....</a>	57
1902		

## 1903 8.4 Tabellenverzeichnis

1904	<a href="#">Tabelle 1: TAB_eRPFD_005 Parameter Prüfung Signaturzertifikat IDP .....</a>	18
1905	<a href="#">Tabelle 2: TAB_eRPFD_010 Parameter Prüfung Signaturzertifikat .....</a>	18
1906	<a href="#">Tabelle 3: TAB_eRPFD_003 Übersicht HTTP-Statuscodes .....</a>	19
1907	<a href="#">Tabelle 4: TAB_eRPFD_004 Versichertenprotokoll .....</a>	23
1908	<a href="#">Tabelle 5: TAB_eRPFD_007 Löschfristen .....</a>	25
1909	<a href="#">Tabelle 6 : TAB_eRPFD_006 Parameter Prüfung Signaturzertifikat QES des HBA.....</a>	42
1910	<a href="#">Tabelle 7: TAB_eRPFD_008 Nachrichtentyp zu Kommunikationsbeziehung.....</a>	51
1911		

## 1912 8.5 Referenzierte Dokumente

### 1913 8.5.1 Dokumente der gematik

1914 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument  
1915 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der  
1916 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und  
1917 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und  
1918 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht  
1919 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der  
1920 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die  
1921 vorliegende Version aufgeführt wird.

1922

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur

[gemSpec_IDP_FD]	Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste
------------------	---

## 1923 8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[rfc6902]	Definition JSON Patch-Operation <a href="https://tools.ietf.org/html/rfc6902">https://tools.ietf.org/html/rfc6902</a>
[ETSI_QES]	DEN/ESI-0019122 Electronic Signatures and Infrastructures (ESI); CADES digital signatures ETSI EN 319 102-1 Procedures for Creation and Validation of AdES Digital Signatures
[RFC5652]	Cryptographic Message Syntax (CMS), RFC 5652 (September 2009) <a href="http://tools.ietf.org/html/rfc5652">http://tools.ietf.org/html/rfc5652</a>
[CADES]	ETSI: Electronic Signature Formats, Electronic Signatures and Infrastructures (ESI) – Technical Specification, ETSI TS 101 733 V2.2.1, via <a href="http://www.etsi.org">http://www.etsi.org</a>
[FHIR-Sig]	FHIR - Signature (JSON Signature rules for FHIR Resources) <a href="https://www.hl7.org/fhir/datatypes.html#Signature">https://www.hl7.org/fhir/datatypes.html#Signature</a>
[FHIR-TASK]	FHIR Ressource Task <a href="https://www.hl7.org/fhir/task.html">https://www.hl7.org/fhir/task.html</a>
[FHIR-ResVers]	FHIR Policy für <del>Ressourcen</del> VersionierungRessourcen Versionierung <a href="https://www.hl7.org/fhir/valueset-versioning-policy.html">https://www.hl7.org/fhir/valueset-versioning-policy.html</a>
[HTTP-STATUS-CODES]	HTTP- <del>Status Code</del> Status-Code gemäß RFC-2616 <a href="https://tools.ietf.org/html/rfc2616">https://tools.ietf.org/html/rfc2616</a>
[JWT]	JSON Web Token (JWT) <a href="https://tools.ietf.org/html/rfc7519">https://tools.ietf.org/html/rfc7519</a>
[JWS]	JSON Web Signature (JWS) <a href="https://tools.ietf.org/html/rfc7515">https://tools.ietf.org/html/rfc7515</a>
[DAL_ANDROID]	Asset Owners Guide - Use statements to enable App Linking, declare default app handlers, ... <a href="https://developers.google.com/digital-asset-links/v1/getting-started">https://developers.google.com/digital-asset-links/v1/getting-started</a>
[RFC7231]	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content <a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a>

[UL_APPLE]	Allowing Apps and Websites to Link to Your Content <a href="https://developer.apple.com/documentation/uikit/inter-process-communication/allowing_apps_and_websites_to_link_to_your_content">https://developer.apple.com/documentation/uikit/inter-process-communication/allowing_apps_and_websites_to_link_to_your_content</a>
------------	---

1924  
1925