

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 Implementierungsleitfaden Primärsysteme – E-Rezept

Version: 1.23.0 CC  
Revision: 326558363144  
Stand: 19.0206.05.2021  
Status: zur Abstimmung freigegeben  
Klassifizierung: öffentlich Entwurf  
Referenzierung: gemILF\_PS\_eRp

## Dokumentinformationen

### Änderungen zur Vorversion

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

### Dokumentenhistorie

| Version         | Stand           | Kap./<br>Seite | Grund der Änderung, besondere<br>Hinweise  | Bearbeitung    |
|-----------------|-----------------|----------------|--|----------------|
| 1.0.0           | 30.06.20        |                | freigegeben  | gematik        |
| 1.0.1           | 06.07.20        |                | Aktualisierung Hinweis zu<br>Dispensierinformation                               | gematik        |
| 1.1.0           | 12.11.20        |                | Einarbeitung gemäß Änderungsliste P22.2<br>/ Scope-Themen Systemdesign R4.0.1    | gematik        |
| 1.2.0           | 19.02.21        |                | Einarbeitung gemäß Änderungsliste<br>P22.5                                       | gematik        |
| <u>1.3.0 CC</u> | <u>06.05.21</u> |                | <u>Einarbeitung gemäß Änderungslisten<br/>E-Rezept Maintenance 21.1 und 21.2</u> | <u>gematik</u> |

## Inhaltsverzeichnis

|  |           |
|--|-----------|
| <b>1 Einordnung des Dokumentes .....</b>                                   | <b>5</b>  |
| <b>1.1 Zielsetzung .....</b>   | <b>5</b>  |
| <b>1.2 Zielgruppe .....</b>  | <b>5</b>  |
| <b>1.3 Geltungsbereich .....</b>   | <b>5</b>  |
| <b>1.4 Abgrenzungen .....</b>  | <b>5</b>  |
| <b>1.5 Methodik .....</b>  | <b>6</b>  |
| 1.5.1 Hinweis auf offene Punkte .....                                      | 6         |
| <b>2 Systemüberblick .....</b>   | <b>7</b>  |
| <b>3 Systemkontext.....</b>  | <b>9</b>  |
| <b>3.1 E-Rezept Status .....</b>   | <b>9</b>  |
| <b>3.2 FHIR-Ressourcen.....</b>  | <b>12</b> |
| <b>4 Übergreifende Festlegungen .....</b>                                  | <b>13</b> |
| <b>4.1 Logging und Meldungen.....</b>                                      | <b>13</b> |
| <b>4.2 Namensauflösung .....</b>   | <b>13</b> |
| <b>5 Funktionsmerkmale .....</b>   | <b>15</b> |
| <b>5.1 Allgemein .....</b>   | <b>15</b> |
| 5.1.1 Kommunikation zu den Diensten der TI.....                            | 15        |
| 5.1.2 Verschlüsselte Kommunikation zur VAU des E-Rezept-Fachdienstes ..... | 17        |
| 5.1.3 Zertifikatsprüfung .....   | 17        |
| 5.1.3.1 Zertifikatsprüfung von Zertifikaten der TI.....                    | 18        |
| 5.1.3.2 Zertifikatsprüfung von Internet-Zertifikaten.....                  | 19        |
| 5.1.4 Authentifizierung der LEI.....                                       | 19        |
| 5.1.4.1 Übergreifende Festlegungen zur Nutzung des IDP-Dienstes .....      | 20        |
| 5.1.4.2 Abruf von Token beim IDP-Dienst.....                               | 21        |
| <b>5.2 Anwendungsfälle verordnende LEI .....</b>                           | <b>28</b> |
| 5.2.1 E-Rezept erstellen .....   | 28        |
| 5.2.2 E-Rezept einstellen.....   | 30        |
| 5.2.3 E-Rezept löschen .....   | 31        |
| <b>5.3 Anwendungsfälle abgebende LEI.....</b>                              | <b>32</b> |
| 5.3.1 E-Rezept abrufen .....   | 33        |
| 5.3.2 Quittung abrufen.....  | 35        |
| 5.3.3 Quittung erneut abrufen .....  | 37        |
| 5.3.4 E-Rezept zurückgeben .....   | 38        |
| 5.3.5 E-Rezept löschen .....   | 39        |
| 5.3.6 Nachrichten von Versicherten empfangen.....                          | 40        |
| 5.3.7 Nachricht an Versicherten versenden .....                            | 43        |
| 5.3.8 Nachricht löschen.....   | 46        |
| 5.3.9 Abgabedatensatz signieren.....                                       | 47        |
| 5.3.10 2D-Code einscannen.....   | 48        |

|    |   |                  |
|----|---|------------------|
| 81 | <b><u>5.4 Fehlerbehandlung.....</u></b>         | <b><u>49</u></b> |
| 82 | <b><u>6 Informationsmodell .....</u></b>        | <b><u>50</u></b> |
| 83 | <b><u>7 Anhang A – Verzeichnisse .....</u></b>  | <b><u>53</u></b> |
| 84 | <b><u>7.1 Abkürzungen .....</u></b>             | <b><u>53</u></b> |
| 85 | <b><u>7.2 Glossar .....</u></b>                 | <b><u>54</u></b> |
| 86 | <b><u>7.3 Abbildungsverzeichnis.....</u></b>    | <b><u>54</u></b> |
| 87 | <b><u>7.4 Tabellenverzeichnis .....</u></b>     | <b><u>54</u></b> |
| 88 | <b><u>7.5 Referenzierte Dokumente .....</u></b> | <b><u>55</u></b> |
| 89 | <u>7.5.1 Dokumente der gematik.....</u>         | <u>55</u>        |
| 90 | <u>7.5.2 Weitere Dokumente.....</u>             | <u>56</u>        |
| 91 |   |                  |
| 92 |   |                  |

---

## 1 Einordnung des Dokumentes

---

### 1.1 Zielsetzung

Das Dokument beschreibt die für die Implementierung des E-Rezepts erforderlichen Vorgaben.

### 1.2 Zielgruppe

Das Dokument richtet sich maßgeblich an Hersteller von Primärsystemen (Praxisverwaltungssysteme, Krankenhausinformationssysteme und Apothekenverwaltungssysteme) von Leistungserbringerinstitutionen (LEI).

### 1.3 Geltungsbereich

Die in diesem Dokument formulierten Anforderungen sind informativ für Primärsysteme, die am Produktivbetrieb der Telematikinfrastruktur (TI) teilnehmen. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Die Anforderungen können für Implementierungsleitfäden bzw. Konformitätsprofile der Sektoren verwendet werden.

### 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

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zu den genutzten FHIR-Ressourcen und den E-Rezept-Token. Anforderungen hierzu befinden sich in [gemSpec\_DM\_eRp].

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zu Implementation des Authentisierungsmoduls. Anforderungen hierzu befinden sich in [gemSpec\_IDP\_Dienst] und [gemSpec\_IDP\_Frontend].

## 127 1.5 Methodik

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

132 Sie werden im Dokument wie folgt dargestellt:

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

134 Text / Beschreibung

135 [**<=>**]

136 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [**<=>**]  
137 angeführten Inhalte.

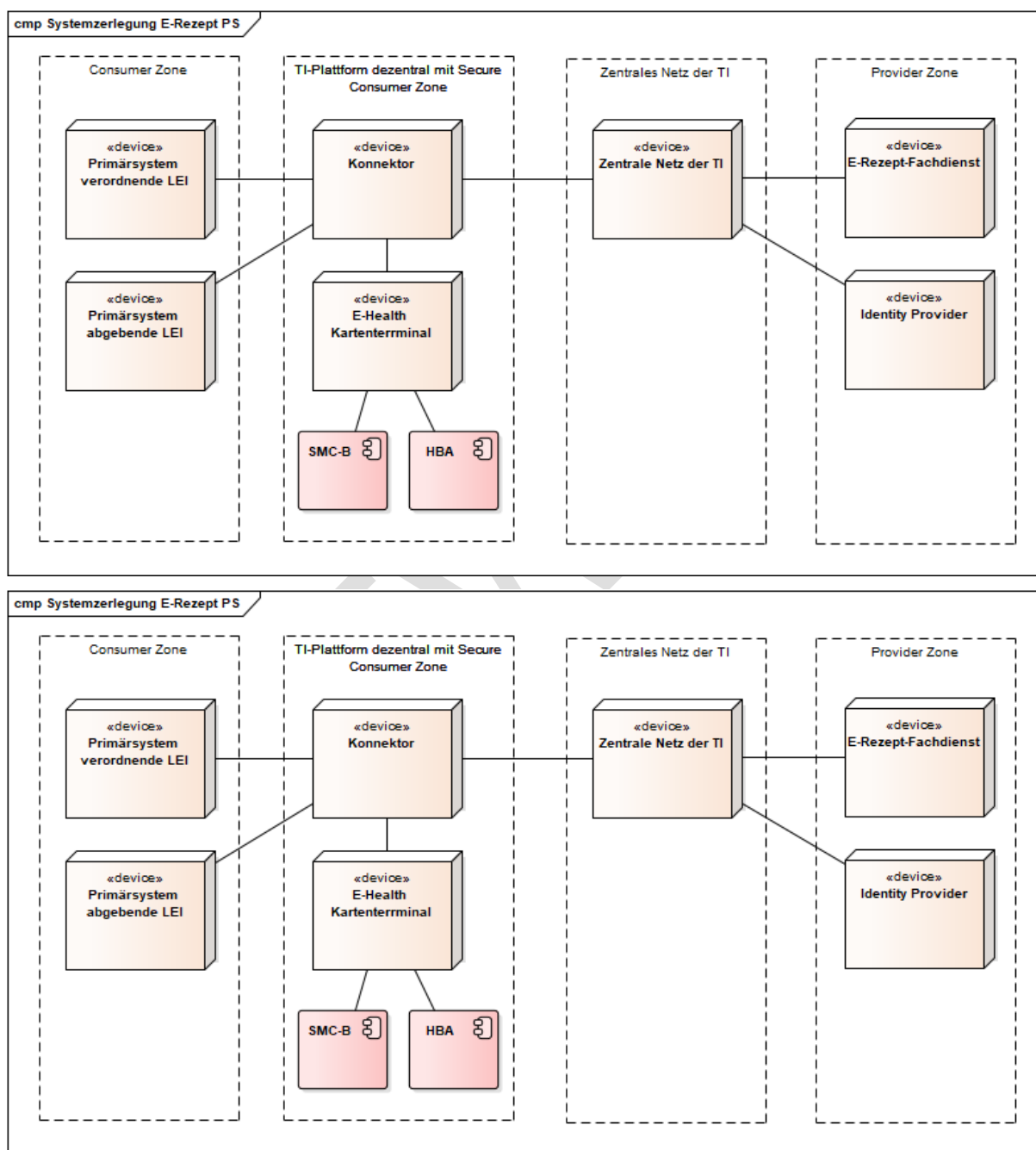
### 138 1.5.1 Hinweis auf offene Punkte

139 Themen, die noch intern geklärt werden müssen oder eine Entscheidung seitens der  
140 Gesellschafter erfordern, sind wie folgt im Dokument gekennzeichnet:

141 *Beispiel für einen offenen Punkt.*

## 2 Systemüberblick

Die folgende Abbildung zeigt einen Systemüberblick für die Primärsysteme verordnende LEI und abgebende LEI.



**Abbildung 1 : ABB\_ILFERP\_001 – Systemzerlegung**

Die von den Primärsystemen direkt erreichbaren Produkttypen der TI sind

- Identity Provider

- E-Rezept-Fachdienst

## **Identity Provider**

Der Identity Provider (IDP) ist ein Nutzerdienst der TI-Plattform, welcher die Authentifizierung von Nutzern und die Bereitstellung bestätigter Identitätsmerkmale der Nutzer als Plattformleistungen bereitstellt. Der IDP bietet außerdem die Möglichkeit, bereits erfolgte Authentifizierungen eines Nutzers im Sinne eines Single Sign-on nachzunutzen.

Der IDP besteht aus dem zentralen Nutzerdienst und einer dezentralen Komponente, dem Authentisierungsmodul des IDP.

## **Authentisierungsmodul des IDP**

Das Authentisierungsmodul ergänzt den IDP, um auf dem Gerät des Nutzers die fachliche Logik für die Authentisierung entsprechend dem OpenID Connect-Standard sowie das Challenge Response Verfahren mit der SMC-B umzusetzen. Der Zugriff auf die Smart Card des Nutzers erfolgt über die Außenschnittstellen des Konnektors.

Das Authentisierungsmodul wird durch das Primärsystem implementiert.

## **Konnektor**

Der Konnektor bildet das Gateway zum zentralen Netz der TI, d.h. es routet die Anfragen an den IDP und den E-Rezept-Fachdienst.

Für die Signatur des E-Rezepts bzw. des ~~Dispensierdatensatzes~~Abgabedatensatzes wird die CMS-Signatur (CAAdES) des Konnektors genutzt.

Der Konnektor kapselt die Zugriffe auf die SMC-B für die Authentisierung.

## **E-Rezept-Fachdienst**

Der E-Rezept-Fachdienst ist ein offener fachanwendungsspezifischer Dienst in der TI, welcher Workflow zu den E-Rezepten umsetzt.



175

## 3 Systemkontext

176

### 3.1 E-Rezept Status

177 Ein E-Rezept durchläuft vom Erstellen bis zum Einlösen verschiedene Status. Abhängig  
178 vom Status sind in den Primärsystemen verschiedene Anwendungsfälle möglich.

179 Der Status wird im E-Rezept-Fachdienst verwaltet. Ist ein Anwendungsfall aufgrund des  
180 Status nicht zulässig, antwortet der E-Rezept-Fachdienst mit einer Fehlermeldung.

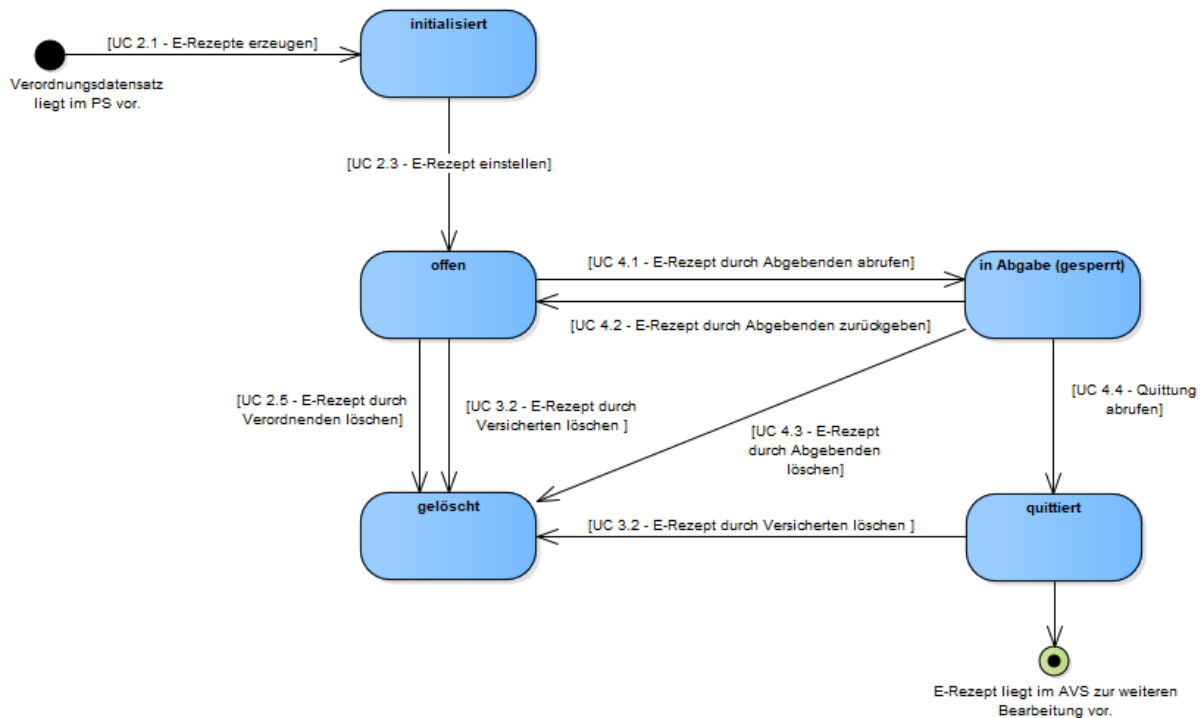
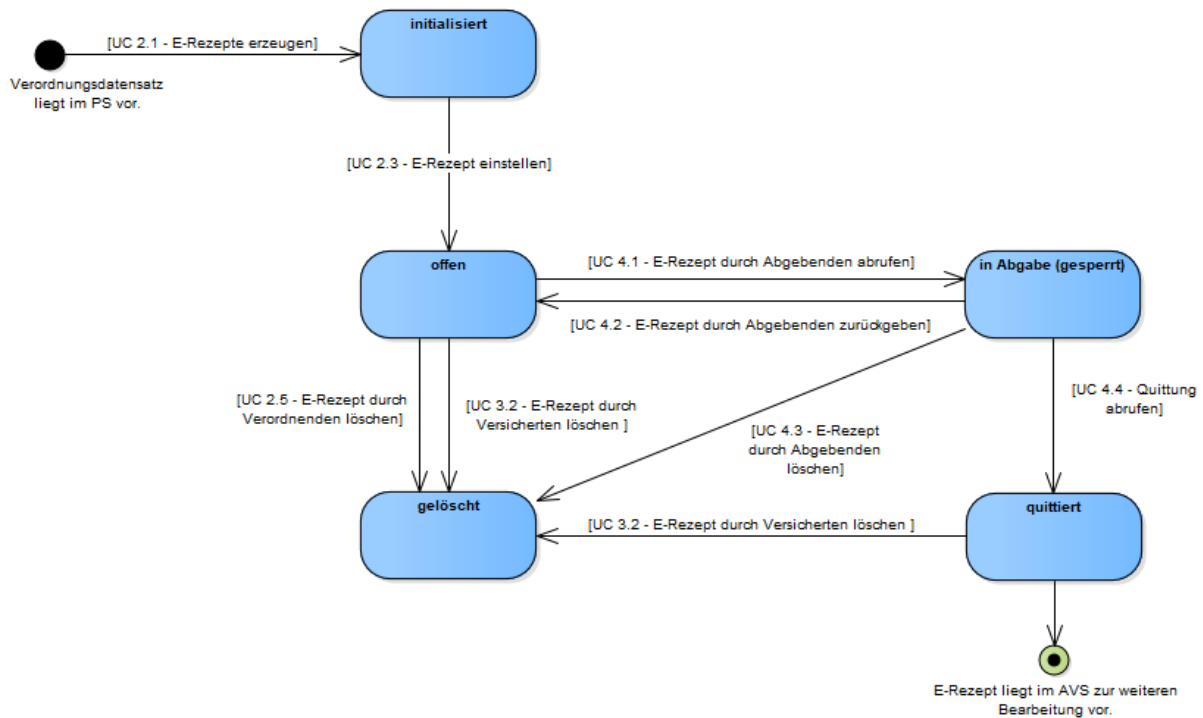
181 TAB\_ILFERP\_001 listet die möglichen Status.

182 **Tabelle 1 : TAB\_ILFERP\_001 – E-Rezept-Status**

| E-Rezept Status      | Task Status | Beschreibung  |
|----------------------|-------------|---|
| initialisiert        | draft       | <ul style="list-style-type: none"> <li>Beim Abruf der Rezept-ID durch eine verordnende LEI wird die FHIR-Ressource Task im E-Rezept-Fachdienst im Zustand "draft" erstellt.</li> <li>Die verordnende LEI kann das QES-signierte E-Rezept in der erstellten Ressource hinzufügen. Der Task wechselt dann in den Status "ready".</li> </ul>   |
| offen                | ready       | <ul style="list-style-type: none"> <li>Der QES-signierte Verordnungsdatensatz wurde von einer verordnenden LEI in den E-Rezept-Fachdienst eingestellt. Der Task wurde vom Fachdienst aktiviert.</li> <li>Der Task kann vom Versicherten bzw. seinem Vertreter abgerufen werden.</li> <li>Der Task kann von der verordnenden LEI oder dem Versicherten als gelöscht markiert werden. Der Task wechselt dann in den Status "cancelled".</li> <li>Der Abruf einer abgebenden LEI ändert den Status des Tasks auf "in-progress". Dieser sperrt den Zugriff durch andere abgebende LEI.</li> </ul> |
| in Abgabe (gesperrt) | in-progress | <ul style="list-style-type: none"> <li>Der Task wurde von einer abgebenden LEI abgerufen.</li> <li>Der Zugriff durch andere abgebende LEI oder die verordnende LEI ist gesperrt. Ebenso darf der Versicherte Tasks in diesem Zustand nicht löschen.</li> <li>Der Task kann durch die abgebende LEI zurückgewiesen werden und wechselt dann zurück in den Status "ready".</li> <li>Die abgebende LEI kann die Quittung abrufen. Dann wechselt der Task in den Status "completed".</li> </ul>   |

|           |           |  |
|-----------|-----------|--|
|           |           | <ul style="list-style-type: none"> <li>• Der Task kann durch die abgebende LEI als gelöscht markiert werden und wechselt dann in den Status "cancelled".</li> <li>• Der Task kann vom Versicherten bzw. seinem Vertreter weiterhin eingesehen werden (read only).</li> </ul>   |
| quittiert | completed | <ul style="list-style-type: none"> <li>• Die Quittung für das E-Rezept wurde durch die abgebende LEI abgerufen. Der Task ist beendet.</li> <li>• Der Task kann vom Versicherten bzw. seinem Vertreter abgerufen werden.</li> <li>• Der Task kann durch den Versicherten gelöscht werden und wechselt dann in den Status "cancelled".</li> <li>• Eine Reaktivierung des Tasks ist nicht möglich.</li> </ul> |
| gelöscht  | cancelled | <ul style="list-style-type: none"> <li>• Die personenbezogenen und medizinischen Daten wurden aus dem Task gelöscht.</li> <li>• Die Akteure können nicht auf den Task zugreifen.</li> </ul>  |

183 Die Abbildung ABB\_ILFERP\_002 zeigt die Anwendungsfälle, welche zu Statusübergängen  
184 führen.



**Abbildung 2 : ABB\_ILFERP\_002 – Statusübergänge**

Für weitere Details zu Statusübergängen siehe [gemKPT\_SysD\_TI] und [gemSysL\_eRp].

## **3.2 FHIR-Ressourcen**

Für die Spezifikation der Schnittstellen in dieser Anwendung wird der Standard FHIR (Fast Healthcare Interoperability Resources) verwendet. In FHIR werden Datenstrukturen und Elemente in "Ressourcen" beschrieben, welche über standardisierte Schnittstellen zwischen verschiedenen Komponenten übertragen werden können. Die Daten werden dabei in XML oder in JSON repräsentiert.

Durch die Primärsysteme werden folgende FHIR-Ressourcen in den Schnittstellen zum E-Rezept-Fachdienst verwendet:

- Bundle (durch die KBV profilierte Ressource für Verordnungen von Arzneimitteln)
- MedicationDispense
- Communication
- Task
- Bundle (für die Darstellung der zu signierenden signierten Quittung)
- Organization

Für eine Beschreibung der Ressourcen siehe [gemSpec\_DM\_eRp].

Der FHIR Standard erlaubt eine Darstellung von FHIR-Ressourcen im JSON als auch XML Format. Für die FHIR-Ressourcen wird ausschließlich die XML Darstellung genutzt.

208

## 4 Übergreifende Festlegungen

### 4.1 Logging und Meldungen

- 210 A\_20088 - PS: Schreiben eines Fehlerprotokolls  
211 Das Primärsystem SOLL alle in der Kommunikation mit den Diensten der TI auftretenden  
212 Fehler und Warnungen in ein dediziertes Fehlerprotokoll schreiben und diese  
213 Protokollinformationen für Supportmaßnahmen über einen Zeitraum von mindestens 14  
214 Tagen zur Verfügung halten. [ <= ]
- 215 A\_20089 - PS: Anzeige von Meldungen  
216 Das Primärsystem SOLL alle in der Kommunikation mit den Diensten der TI auftretenden  
217 Probleme für den Benutzer verständlich anzeigen und dabei erkennen lassen, ob durch  
218 den Anwender oder den verantwortlichen Leistungserbringer Maßnahmen zur Behebung  
219 eingeleitet werden müssen. [ <= ]
- 220 A\_20884 - PS: Exponential Backoff bei Verbindungsfehlern  
221 Das Primärsystem SOLL bei serverseitigen Fehlermeldungen, die auf eine Überlastung  
222 des Zielsystems schließen lassen (z.B. http-status 5xx, 429 - too many requests, etc.),  
223 erneute Verbindungsversuche nach dem Prinzip des Exponential Backoffs [ExpBack]  
224 durchführen. [ <= ]

### 4.2 Namensauflösung

226

- 227 Der E-Rezept-Fachdienst ist für Primärsysteme gemäß ~~der~~den Festlegungen in  
228 [gemSpec\_FD\_eRp] über die Adresse `erp.zentral.erp.splitdns.ti-dienste.de` lokalisierbar.  
229 Das Redundanzkonzept sieht mehrere Instanzen vor, die über verschiedene IP-Adressen  
230 angesprochen werden. Folglich liefert die DNS-Namensauflösung verschiedene IP-  
231 Adressen zum FQDN zurück. Diese Adressen werden vom DNS-Server in zufälliger  
232 Reihenfolge geschickt, sodass es legitim ist, immer den ersten Eintrag für den folgenden  
233 Operationsaufruf zu verwenden. Üblicherweise wird die DNS-Auflösung vom  
234 ~~Betriebssystem~~Betriebssystem gekapselt, eine Lastverteilung am E-Rezept-Fachdienst  
235 ergibt sich aus der zufälligen Reihenfolge der IP-Adressen der DNS-Abfrage.  
236
- 237 Unspezifiziert ist das Verhalten, wenn die erste Zieladresse nicht erreichbar ist.  
238 Empfehlenswert ist die Nutzung der anderen/weiteren IP-Adressen der DNS-Abfrage. Es  
239 muss aber angenommen werden, dass bestimmte Betriebssysteme bzw.  
240 Laufzeitumgebungen des Primärsystems diese mit der Nutzung der ersten Adresse  
241 bereits verworfen haben. Bei Nicht-Erreichbarkeit des Zielhosts der ersten IP-Adresse  
242 wird daher empfohlen, weitere Verbindungsversuche auf Basis einer neuen DNS-Abfrage  
243 zu tätigen, mit dem Ziel, eine andere IP-Adresse an erster Stelle der DNS-Antwort zu  
244 erhalten, als die des nicht erreichbaren Zielhosts.
- 245 Das Primärsystem erreicht den E-Rezept-Fachdienst und IDP über den Konnektor  
246 geroutet. Je nach Installationsumgebung des Primärsystems ist der Konnektor evtl. nicht  
247 das Default-Gateway. Um diese offenen Fachdienste zu erreichen, müssen ggfs. feste  
248 Routen und eine DNS-Konfiguration für das [Split-DNS] pro Arbeitsplatz-Computer im  
249 Rahmen der Installation festgelegt werden.

A 21468 - PS: Handbuch-Hinweis Konnektor Default-Gateway für offene Fachdienste  
Der Hersteller des Primärsystems MUSS in seinem Handbuch auf die verschiedenen  
Installationsszenarien und Konfigurationen des Konnektors in [gemSpec KON#Anhang K]  
hinweisen, damit der Konnektor im Rahmen der Installation und Konfiguration des PS für  
das E-Rezept als Default-Gateway bzw. notwendige Routinginformationen und DNS-  
Konfigurationen im Gerät festgelegt werden können. [≤]

Der Hersteller des Primärsystems kann die Konfiguration zum Installationszeitpunkt  
unterstützen, indem er bspw. eine Batch-Datei zum Hinterlegen der  
Netzwerkeinstellungen für die verschiedenen FQDN für E-Rezept-Fachdienst und IDP über  
den Konnektor als Gateway bereitstellt.

Mit dem E-Rezept wird ein Split-DNS eingeführt, um die Domainadresse "ti-dienste.de"  
auch im zentralen Netz für Fachdienste nutzen zu können. Für diesen Zweck wird  
"splitdns.ti-dienste.de" in die Bestandsnetzkonfiguration des Konnektors ergänzt. Der  
Konnektor übernimmt dann für die Domain splitdns.ti-dienste.de die Namensauflösung.  
Für lokale Netzwerkinstallationen, die den Konnektor nicht als Nameserver und Gateway  
in ihrem Netzwerk nutzen, müssen entsprechende Netzwerkkonfigurationen manuell  
vorgenommen werden.

Die gematik plant, ergänzende Informationen zu Netzwerkkonfigurationen zu  
veröffentlichen, bspw. auf der github-Seite <https://github.com/gematik> .

## 5 Funktionsmerkmale

### 5.1 Allgemein

#### 5.1.1 Kommunikation zu den Diensten der TI

Das PS einer verordnenden bzw. abgebenden LEI nutzt TLS-Verbindungen für die Kommunikation zu den Diensten der TI. Es verbindet sich mit dem E-Rezept-Fachdienst und einem Identity Provider.

**A\_19451-01A\_19451** - PS: Lokalisierung E-Rezept-Fachdienst  
Das Primärsystem MUSS für die zur Kommunikation mit dem E-Rezept-Fachdienst notwendig die FQDNs als Lokalisierungsinformationen perin einer DNS-Abfrage nach den ingemäß [gemSpec\_FD\_eRP# 5.1 Servicelokalisierung] nutzen. [<=Tab\_eRP\_Service Discovery] und [gemSpec\_FD\_eRP#Tab\_eRP\_FQDN] dargestellten Parametern ermitteln.[<=]

Die Abfrage beim Namensdienst der TI erfolgt über eineinen DNS-Abfrage beim Lookup. Hierfür muss der Konnektor. Der Konnektor bietet hierzu eine Operation GetIPAddress für das PS an. Siehe TIP1-A\_5035 – Operation GetIPAddress in [gemSpec\_KON]. Liefert die als DNS-Abfrage mehrere Ziel IP-Adressen, so ist es hilfreich, eine zufällig auszuwählen, um Lastspitzen in den einzelnen Zielsystemen zu reduzieren Resolver konfiguriert sein.

**A\_19744** - PS: Endpunkt Schnittstelle E-Rezept-Fachdienst  
Das Primärsystem MUSS die URL für die Kommunikation mit dem E-Rezept-Fachdienst gemäß `https://<FQDN aus DNS Lookup>:443/` bilden.[<=]

Die Informationen zu den Endpunkten des Identity Providers ermittelt das Primärsystem aus dem Discovery Document. Siehe auch [gemSpec\_IDP\_Dienst#Registrierung von Endgerät und Anwendungsfrontend]. Das Discovery Document ist vom IDP-Dienst unter der URL `/.well-known/openid-configuration` abrufbar.

**A\_19234** - PS: Kommunikation über TLS-Verbindung  
Das Primärsystem MUSS für die Anwendungsfälle der Anwendung E-Rezept mit den Diensten der TI ausschließlich über TLS kommunizieren.[<=]

Es gelten die Vorgaben aus [gemSpec\_Krypt] für TLS.

**A\_19235** - PS: Unzulässige TLS-Verbindungen ablehnen  
Das Primärsystem MUSS bei jedem Verbindungsaufbau den Dienst der TI anhand seines TLS-Zertifikats authentifizieren und MUSS die Verbindungen ablehnen, falls die Authentifizierung fehlschlägt.[<=]

**A\_20015-01A\_20015** - PS: HTTP-Header user-agent  
Das Primärsystem MUSS in alle HTTP-Requests an den E-Rezept-Fachdienst und den IDP-Dienst Dienste der TI den HTTP-Header user-agent gemäß [RFC7231] mit `<Herstellername><Produktname>/<Produktversion>/<client_id>` mit

- <Herstellername> gemäß eigener Definition, Maximallänge 20 Zeichen, darf "/" nicht enthalten

- <Produktname> gemäß eigener Definition, Maximallänge 20 Zeichen, darf "/" nicht enthalten
- <Produktversion> gemäß Produktidentifikation
- <client\_id> gemäß Registrierung bei der gematik

des Primärsystems befüllen. [ <= ]

A\_21242 - PS: Unterstützung Konnektorversion

Das Primärsystem MUSS Konnektoren ab PTV 3 für das E-Rezept unterstützen. [ <= ]

A\_21568 - PS: HTTP-Header X-erp-user

Das Primärsystem MUSS in alle Anfragen an den E-Rezept-Fachdienst im äußeren HTTP-Request den HTTP-Header "X-erp-user" mit dem Wert "l" (kleines L) einfügen. [ <= ]

A\_21569 - PS: HTTP-Header X-erp-resource

Das Primärsystem MUSS in alle Anfragen an den E-Rezept-Fachdienst im äußeren HTTP-Request den HTTP-Header "X-erp-resource" mit dem Wert gemäß der angefragten Ressource im FHIR-Request einfügen. [ <= ]

**Tabelle 2: TAB\_ILFERP\_014 - HTTP-Header "X-erp-resource"**

| <u>Operation</u>                        | <u>X-erp-resource</u> |
|---|-----------------------|
| <u>DELETE /Communication/&lt;id&gt;</u> | <u>Communication</u>  |
| <u>GET /Communication/</u>              | <u>Communication</u>  |
| <u>GET /Communication/&lt;id&gt;</u>    | <u>Communication</u>  |
| <u>GET /Device/</u>                     | <u>Device</u>         |
| <u>GET /metadata/</u>                   | <u>metadata</u>       |
| <u>POST /Communication</u>              | <u>Communication</u>  |
| <u>POST /Task/\$create</u>              | <u>Task</u>           |
| <u>POST /Task/&lt;id&gt;/\$abort</u>    | <u>Task</u>           |
| <u>POST /Task/&lt;id&gt;/\$accept</u>   | <u>Task</u>           |
| <u>POST /Task/&lt;id&gt;/\$activate</u> | <u>Task</u>           |
| <u>POST /Task/&lt;id&gt;/\$close</u>    | <u>Task</u>           |
| <u>POST /Task/&lt;id&gt;/\$reject</u>   | <u>Task</u>           |



## 5.1.2 Verschlüsselte Kommunikation zur VAU des E-Rezept-Fachdienstes

Die Kommunikation zum E-Rezept-Fachdienst wird zusätzlich zu TLS über einen sicheren Kanal (Verschlüsselung auf Http-Ebene) zwischen dem PS und der Vertrauenswürdigen Ausführungsumgebung (VAU) im E-Rezept-Fachdienst gesichert.

A\_19741 - PS: Umsetzung sicherer Kanal zur VAU des E-Rezept-Fachdienstes  
Das Primärsystem MUSS für alle Anfragen an den E-Rezept-Fachdienst für

- die Abfrage des capability statement
- den Zugriff auf Task oder Communication Ressourcen

das Kommunikationsprotokoll zwischen E-Rezept-VAU und E-Rezept-Clients in der Rolle E-Rezept-Client nutzen[<=]

Für Informationen zum Kommunikationsprotokoll zwischen E-Rezept-FdV und der VAU des E-Rezept-Fachdienstes siehe [\[gemSpec Krypt#3.16 E-Rezept-spezifische Vorgaben \(informativ\)\]](#) und [\[gemSpec Krypt#7 Kommunikationsprotokoll zwischen E-Rezept-VAU und E-Rezept-Clients\]](#) [\[gemSpec Krypt#3.16 E-Rezept-spezifische Vorgaben \(informativ\)\]](#) und [\[gemSpec Krypt#7 Kommunikationsprotokoll zwischen E-Rezept-VAU und E-Rezept-Clients\]](#).

Alternativ zur Umsetzung des TUC PKI 018 gemäß A 21216 soll das Primärsystem für die Prüfung des VAU-Zertifikates die VerifyCertificate Operation des Konnektors nutzen.

Folgendes kann umgesetzt werden:

- (1) Beziehen des VAU-Zertifikat von /VAUCertificate
- (2) Lokales Speichern der aktuellen Zeit mit dem VAU-Zertifikat als Tupel
- (3) Prüfen des VAU-Zertifikates mittels der Konnektor-Operation VerifyCertificate
- (4) Abbrechen falls REVOKED
- (5) if (get\_current\_time() < gespeicherte Zeit + 12h) { VAU-Zertifikat wird als gültig angesehen, Nutzen des VAU-Zertifikat }  
if (get\_current\_time() >= gespeicherte Zeit + 12h) { VAU-Zertifikat neu beziehen, siehe (1) }

## 5.1.3 Zertifikatsprüfung

Das Primärsystem der verordnenden und abgebenden LEI verwendet bei den in TAB\_ILFERP\_012 dargestellten Aktivitäten Zertifikate.

**Tabelle 3 TAB\_ILFERP\_012 – Zertifikatsnutzung**

| Aktivität | Zertifikat der TI | Zertifikatstyp | Rollen-OID | Nutzung |
|-----------|-------------------|----------------|------------|---------|
|           |                   |                |            |         |

|  |      |                         |             |       |
|--|------|-------------------------|-------------|-------|
| TLS-Verbindungsaufbau zum E-Rezept-Fachdienst                | nein | TLS Internet Zertifikat | n/a         | aktiv |
| TLS-Verbindungsaufbau zum Verzeichnisdienst der TI           | nein | TLS Internet Zertifikat | n/a         | aktiv |
| TLS-Verbindungsaufbau zum IDP                                | nein | TLS Internet Zertifikat | n/a         | aktiv |
| Aufbau sicherer Kanal zur VAU des E-Rezept-Fachdienstes      | ja   | C.FD.ENC                | oid_erp-vau | aktiv |
| Nur für PS der abgebenden LEI: Signaturzertifikat Fachdienst | ja   | C.FD.SIG                | oid_erezept | aktiv |

Es gelten folgende übergreifende Festlegungen für die Prüfung aktiv durch das E-Rezept-FdV genutzter Zertifikate.

A\_20769 - PS: verpflichtende Zertifikatsprüfung

Das Primärsystem MUSS alle Zertifikate, die es aktiv verwendet (bspw. TLS-Verbindungsaufbau), auf Integrität und Authentizität prüfen. Falls die Prüfung kein positives Ergebnis ("gültig") liefert, so MUSS es die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen.

Das Primärsystem MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können. [ $\leq$ ]

"Ein Zertifikat aktiv verwenden" bedeutet im Sinne von A\_20769, dass ein Primärsystem einen dort aufgeführten öffentlichen Schlüssel innerhalb einer kryptografischen Operation (Signaturprüfung, Verschlüsselung, Signaturprüfung von öffentlichen (EC)DH-Schlüsseln etc.) nutzt. Erhält ein Primärsystem bspw. einen Access-Token, in dem Signaturen und Zertifikate enthalten sind, und behandelt es diesen Token als opakes Datenobjekt, ohne die Zertifikate darin gesondert zu betrachten, dann verwendet das Primärsystem diese Zertifikate im Sinne von A\_20769 passiv.

§78

## 5.1.3.1 Zertifikatsprüfung von Zertifikaten der TI

A\_20764 - PS: Prüfung TI-Zertifikate

Das Primärsystem MUSS bei der Prüfung von X.509-Zertifikaten der TI den `CertificateService` des Konnektors mit der Operation `VerifyCertificate` gemäß [gemSpec\_Kon#4.1.9.5.3] verwenden und dabei

- das zu prüfende Zertifikat als Parameter `X509Certificate` verwenden
- die aktuelle Systemzeit als Parameter `VerificationTime` verwenden

Das Primärsystem MUSS bei Prüfung eines C.FD.ENC den Rückgabewert in `RoleList` gegen die erwartete Rollen-OID gemäß `TAB_ILFERP_012` prüfen und bei Abweichungen die Benutzung des Zertifikats für einen Verbindungsaufbau zur VAU ablehnen. [`<=`]

### **5.1.3.2 Zertifikatsprüfung von Internet-Zertifikaten**

Folgende Vorgaben gelten für die Prüfung von Internet-Zertifikaten.

A\_20091 - PS: Prüfung der Zertifikate für TLS-Verbindung zu E-Rezept-Fachdienst und Identity Provider

Das Primärsystem MUSS für die Prüfung eines Zertifikats für den TLS-Verbindungsaufbau zum E-Rezept-Fachdienst und IDP das Zertifikat auf ein CA-Zertifikat einer CA, die die "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" ( <https://cabforum.org/baseline-requirements-documents/>) erfüllt, kryptographisch (Signaturprüfung) zurückführen können. Ansonsten MUSS es das Zertifikat als "ungültig" bewerten.

Das PS MUSS die zeitliche Gültigkeit des Zertifikats prüfen. Falls diese Prüfung negativ ausfällt, muss es das Zertifikat als "ungültig" bewerten. [`<=`]

Hinweis: Der erste Teil von A\_20091 ist gleichbedeutend damit, dass das CA-Zertifikat im Zertifikats-Truststore eines aktuellen Webbrowsers ist.

### **5.1.4 Authentifizierung der LEI**

Die LEI authentisiert sich für Zugriffe auf Dienste der TI im Rahmen der Anwendung E-Rezept gegenüber dem IDP-Dienst.

Das Primärsystem übernimmt hierbei, wenn kein gültiger "ACCESS\_TOKEN" vorliegt, neben der Rolle der Anwendungsfrontend-Applikation auch die Aufgabe des Authenticator-Moduls (der in [RFC6749 # section-4.1] beschriebene User-Agent), um das zum Zugriff auf Fachdienste benötigte "ACCESS\_TOKEN" zu beantragen. Hierfür wird am Authorization-Endpunkt des IDP-Dienstes ein "AUTHORIZATION\_CODE" beantragt, der nach erfolgreicher Verifikation am Token-Endpunkt des IDP-Dienstes gegen ein "ID\_TOKEN" und ein "ACCESS\_TOKEN" getauscht wird.

Die für die Beantragung des "AUTHORIZATION\_CODE" im Challenge-Response-Verfahren notwendige elektronische Signatur mit der AUT-Identität einer SMC-B der LEI lässt das Primärsystem über die Schnittstellen des Konnektors generieren. Im Fall einer bereits freigeschalteten Smartcard passiert diese Aktion ohne Interaktion mit dem Nutzer im Hintergrund.

Der IDP-Dienst führt die Identifikation der LEI durch, und stattet diese anschließend mit "ID\_TOKEN" gemäß [openid-connect-core 1.0 # IDToken] und "ACCESS\_TOKEN" gemäß [RFC6749 # section-1.4 & RFC6749 # section-5] aus. Dabei wurde aus Sicherheitsaspekten der "Authorization Code Grant" gemäß [RFC6749 # section-4.1] gewählt, welcher in identischem Ablauf auch für mobile Endgeräte mit getrennten Komponenten für Authenticator-Modul und Anwendungsfrontend anwendbar ist. Um dem erforderlichen Sicherheitsniveau gerecht zu werden, wird zudem die Verwendung von PKCE (Proof Key for Code Exchange by OAuth Public Clients) gemäß [RFC7636]

vorgesehen.

Der IDP-Dienst selbst teilt sich in mehrere statisch adressierte Teildienste auf. Diese umfassen:

- Discovery-Endpunkt ("OAuth 2.0 Authorization Server Metadata" [RFC8414])
- Authorization-Endpunkt (Teil des "The OAuth 2.0 Authorization Framework" [RFC6749])
- Token-Endpunkt [RFC6749 # section-3.2]

Für weitere Informationen zum IDP-Dienst und zum Ablauf der Authentisierung siehe [gemSpec\_IDP\_Dienst] und [gemSpec\_IDP\_Frontend].

Die gematik wird Beispielsätze und weitere Hilfestellungen auf ihrer Webseite in jeweils aktueller Form bereitstellen.

#### 5.1.4.1 Übergreifende Festlegungen zur Nutzung des IDP-Dienstes

Zur Nutzung des IDP-Dienstes gelten einige grundlegende Voraussetzungen, welche das PS erfüllen muss.

A\_20654 - Registrierung des Primärsystems

Der Hersteller des Primärsystems MUSS sich über einen organisatorischen Prozess beim Anbieter des IDP-Dienstes für die Dienste, für welche Token abgerufen werden sollen, registrieren. Der IDP-Dienst vergibt dabei eine "client\_id". Diese "client\_id" MUSS vom Primärsystem bei Nutzung des IDP-Dienstes übertragen werden. [ $\leq$ ]

A\_20655 - Regelmäßiges Einlesen des Discovery Document

Das Primärsystem MUSS das Discovery Document (DD) [RFC8414] regelmäßig alle 24 Stunden einlesen und auswerten, und danach die darin aufgeführten URI zu den benötigten öffentlichen Schlüsseln (PUKs) und Diensten verwenden.

Der Downloadpunkt wird als Teil der organisatorischen Registrierung des Primärsystems beim IDP-Dienst übergeben.

Das Primärsystem MUSS den Downloadpunkt des Discovery Document als konfigurierbaren Parameter speichern. [ $\leq$ ]

A\_20656-01 - Prüfung der Signatur des Discovery Document

~~A\_20656 - Prüfung der CMS-Signatur des Discovery Document~~

Das Primärsystem MUSS die JWS (JSON Web Signature) [RFC7515 # section-3 ] - Compact Serialization Signatur des Discovery Document mittels "VerifyDocument" auf mathematische Korrektheit sowie über die Funktion "VerifyCertificate" des KonnektorKonnektors gemäß [gemSpec\_Kon#4.1.89.5.23] bzw. [gemILF\_PS#4.4.3] auf mathematische Korrektheit sowie 4.3 auf Gültigkeit des ausstellenden Zertifikates innerhalb der TI prüfen.

Der genaue Aufbau entspricht gemSpec\_IDP-Dienst#Kapitel 7.7 [ $\leq$  -  $\leftarrow$ ]

~~Als SignatureType ist urn:ietf:rfc:5652 für eine CMS-Signatur zu verwenden. Weitere optionale Parameter kommen nicht zur Anwendung.~~

Im Rahmen der Vorveröffentlichung finden sich Details zum Aufbau auf den Webseiten der gematik zur Entwicklungsunterstützung sowie in der Vorveröffentlichung des

Dokumentes gemF Tokenverschlüsselung. Das Dokument gemSpec IDP-Dienst  
beinhaltet noch keine aktuellen Angaben.

Bei Aufruf der Funktion "VerifyDocument" an der Außenschnittstelle des Konnektors ist es nicht möglich, direkt auch eine Prüfung des Zertifikatstyps und der Rollen-OID durchzuführen.

A\_20657 - Prüfung der Signatur des Discovery Document

Das Primärsystem MUSS die Signatur des Discovery Document auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID "oid\_idpd" zurückführen können. [ $\leq$ ]

Hinweis: Zur Durchführung der Prüfungen gemäß A\_20657 und ähnlicher Anforderungen ist zu verifizieren, ob im Feld certificatePolicies (2.5.29.32) des Zertifikates der richtige Zertifikatstyp FD.SIG (1.2.276.0.76.4.203) gemäß [gemSpec\_OID#Tabelle Tab\_PKI\_405] eingetragen ist und sich in der Admission (1.3.36.8.3.3) des Zertifikats die richtige "oid\_idpd" (1.2.276.0.76.4.260) findet.

A\_20658 - Sicheres Löschen der Token

Das Primärsystem MUSS, wenn es absichtlich gestoppt oder deaktiviert wird, vorhandene "ACCESS\_TOKEN", "ID\_TOKEN" und "AUTHORIZATION\_CODE"-Objekte sicher aus dem RAM löschen. [ $\leq$ ]

Darüber hinaus gelten für die Kommunikation mit dem IDP-Dienst die Vorgaben aus 5.1.1- Kommunikation zu den Diensten der TI. 5.1.1- Kommunikation zu den Diensten der TI.

A\_21337 - Löschung von TOKEN bei zeitlichem Ablauf

Das Primärsystem MUSS vorhandene "ACCESS\_TOKEN", "ID\_TOKEN" und "AUTHORIZATION\_CODE"-Objekte nach Ablauf ihrer Gültigkeit sicher löschen. [ $\leq$ ]

A\_21338 - Sichere Speicherung der Token

Das Primärsystem MUSS empfangene "ACCESS\_TOKEN", "ID\_TOKEN" und "AUTHORIZATION\_CODE"-Objekte gegen unberechtigten Zugriff schützen. [ $\leq$ ]

#### **5.1.4.2 Abruf von Token beim IDP-Dienst**

Im Folgenden wird der Ablauf der Token-Beantragung und Ausstellung detaillierter beschrieben und – wo für das Primärsystem notwendig – mit entsprechenden Anforderungen hinterlegt.

Im ersten Schritt erzeugt sich das Primärsystem einen zufälligen "CODE\_VERIFIER" und bildet darüber den Hash "CODE\_CHALLENGE". Mit dessen Hilfe kann es sich im späteren Verlauf als valider Empfänger des Tokens ausweisen.

A\_20659 - Erzeugen des CODE\_VERIFIER

Das Primärsystem MUSS zur Laufzeit einen "CODE\_VERIFIER" (Zufallswert) gemäß [RFC7636 # section-4.1] bilden. Der "CODE\_VERIFIER" MUSS eine Länge von mindestens 43 und maximal 128 Zeichen enthalten. Dabei sind die folgenden Zeichen zulässig: [A-Z] / [a-z] / [0-9] / "-" / "." / "\_" / "~". [ $\leq$ ]

A\_20660 - Erzeugen des Hash-Werts des CODE\_VERIFIER

Das Primärsystem MUSS über den "CODE\_VERIFIER" einen SHA256-HASH-Wert, die sogenannte "CODE\_CHALLENGE", gemäß [RFC7636 # section-4.2] bilden.  
code\_challenge = BASE64URL-ENCODE(SHA256(ASCII(code\_verifier)))[ $\leq$ ]

Anschließend werden der gehashte Zufallswert und die notwendigen Angaben als "CODE\_CHALLENGE" beim Authorization-Endpunkt des IDP-Dienstes eingereicht.

A\_20661 - Anfrage des "AUTHORIZATION\_CODE" für ein "ACCESS\_TOKEN"  
Das Primärsystem MUSS den Antrag zum "AUTHORIZATION\_CODE" für ein "ACCESS\_TOKEN" beim Authorization-Endpunkt (URI\_AUTH) in Form eines HTTP/1.1 GET Request stellen und dabei die folgenden Attribute anführen:

- "response\_type"
- "scope"
- "client\_id"
- "redirect\_uri"
- "code\_challenge" (Hashwert des "code\_verifier") [RFC7636 # section-4.2]
- "code\_challenge\_method" HASH-Algorithmus (S256) [RFC7636 # section-4.3][<=]

~~Hinweis: Der folgende Aufruf skizziert einen beispielhaften HTTP-GET-Request an den IDP-Dienst, welcher vom Authenticator-Modul initiiert wird:~~

~~GET  
/auth?response\_type=code&scope=openid%20erezept&state=af0ifjsldkj&client\_id=ZXJle  
mVwdC1hcHA&redirect\_uri=https%3A%2F%2Fapp.erezept.com%2Fauthnres&code\_chall  
enge\_method=S256&code\_challenge=S41HgHxhXL1CIpfGvivWYpbO9b\_QKzva-  
9ImuZbt0Is~~

~~HTTP/1.1  
Host: idp.com  
X-Authenticator-App: 1.0  
Accept: application/json  
User-Agent: Authenticator-App/1.0~~

Der Authorization-Endpunkt legt nun eine "session\_id" an, stellt alle nötigen Informationen zusammen und erzeugt ~~die verschlüsselte "challenge"~~das **CHALLENGE\_TOKEN**".  
Darüber hinaus stellt der Authorization-Endpunkt den im Claim des entsprechenden Fachdienstes vereinbarten "Consent" zusammen, welcher die für dessen Funktion notwendigen Attribute beinhaltet.

Der Authorization-Endpunkt liefert als Response zur Anfrage des "AUTHORIZATION\_CODE" einen "CHALLENGE\_TOKEN", um die Identität der LEI zu bestätigen, sowie den "consent" des im "scope" angefragten Fachdienstes.

A\_20662 - Annahme des "user\_consent" und des "CHALLENGE\_TOKEN"  
Das Primärsystem MUSS den "user\_consent" und den "CHALLENGE\_TOKEN" vom Authorization-Endpunkt des IDP-Dienstes annehmen. Der Authorization-Endpunkt liefert diese als Antwort auf den Authorization-Request des Primärsystems. [<=]

~~Hinweis: Nachfolgend wird beispielhaft ein "CHALLENGE\_TOKEN" in Form eines JSON Web Token (JWT) dargestellt:~~

~~Challenge-JWT:  
challenge\_headers = {  
 "typ": "JOSE+JSON",  
 "iat": 1591714252326,  
 "exp": 1591714552326,  
 "jti": "c3a8f9c8-aa62-11ea-ac15-6b7a3355d0f6",  
 "snc": "sLlxIkSkAyuzdDOwe8nZeeQVFBWgscNkRcpghmKidFc"  
}~~



```
challenge_payload={
  "response_type":"code",
  "scope":"openid-erezept",
  "client_id":"ZXJlemVwdC1hcHA",
  "state":"af0ifjsldkj",
  "redirect_uri":"https://app.erezept.com/authnres",
  "code_challenge_method":"S256",
  "code_challenge":"S41HgHxhXL1CipfGvivWYpbO9b_QKzva-9ImuZbt0Is"
}
```

Der Authorization-Endpunkt hat den "CHALLENGE\_TOKEN" mit seinem privaten Schlüssel "PRK\_AUTH" signiert. Der folgende Aufruf skizziert beispielhaft die Antwort des Authorization-Endpunktes, welche vom Primärsystem angenommen wird. Der "CHALLENGE\_TOKEN" wird dabei nur angedeutet:

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache
-
{
  "challenge":
    "eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp1PU0rSINPTiIsImhhdCI6MTU5MTcxNDI1MjMy.....",
  "user_consent": {
    "client_name": "eRezept App",
    "url": "https://erezept.com/",
    "requested_scope": {
      "openid": "Der Zugriff auf den ID-Token",
      "erezept": "Zugriff auf die eRezept-Funktionalität."
    },
    "show_once": true,
    "amr": ["JWT-Challenge-Response"]
    // ggf. mehr Informationen, welche dem Nutzer angezeigt werden sollen, wie die
    Auflistung der mit der Zustimmung weitergegebenen Daten
  }
}
```

### A\_20663-01A\_20663 - Prüfung der Signatur des CHALLENGE\_TOKEN

Das Primärsystem MUSS die Signatur des "CHALLENGE\_TOKEN" gegen den aktuellen öffentlichen Schlüssel des Authorization-Endpunktes "PUK\_AUTHIDP\_SIG" prüfen. Liegt dem Primärsystem der öffentliche Schlüssel des Authorization-Endpunktes noch nicht vor, MUSS es diesen gemäß den Angaben der Adresse PUK\_URI\_AUTH im dem „kid“-Parameter "puk\_idp\_sig" aus dem Discovery Document abrufen.[<=]

Das Primärsystem verwendet nun die AUT-Identität der SM-B der LEI und deren Konnektor, um die 256-Bit "challenged" des gehashten "CHALLENGE\_TOKEN" des IDP-Dienstes zu signieren. Wenn es sich um eine erstmalige Anmeldung des Benutzers bei diesem Fachdienst handelt, werden diesem darüber hinaus die für den Zugriff übermittelten Daten der LEI angezeigt.

### A\_20664 - Bestätigung des Consent

Das Primärsystem MUSS dem Nutzer einmalig vor der Signatur der "challenge" anzeigen, dass ein tokenbasierter Zugriff auf den im "scope" genannten Dienst initiiert wird. [ <= ]

Hinweis: Die erfolgte Zustimmung des Nutzers darf gespeichert werden und weitere Abfragen können entfallen.

### A\_20665-01 - Signatur der Challenge des IdP-Dienstes

#### **~~A\_20665~~ — Signatur der Challenge des IDP-Dienstes**

Das Primärsystem MUSS für das Signieren ~~der "challenge"~~ des IDPCHALLENGE\_TOKEN des IdP-Dienstes mit der Identität ID.HCI.OSIGAUT der SM-B die Operation ExternalAuthenticate des Konnektors gemäß [gemSpec\_Kon#4.1.13.4] bzw. [gemILF\_PS#4.4.6.1] verwenden und als zu signierende ~~Daten~~BinaryString den SHA-256-Hashwert ~~der challenge~~des CHALLENGE\_TOKEN in Base64-Codierung übergeben.

Der Aufbau der der Anfrage und des der einzureichenden Objekte entspricht gemSpec IDP-Dienst#Kapitel 7.3.- [ <= ]

Im Rahmen der Vorveröffentlichung finden sich Details zum Aufbau auf den Webseiten der gematik zur Entwicklungsunterstützung sowie in der Vorveröffentlichung des Dokumentes gemF Tokenverschlüsselung. Das Dokument gemSpec IDP-Dienst beinhaltet noch keine aktuellen Angaben.

Für weitere Informationen siehe Kapitel "Als Nutzer gegenüber der Telematikinfrastruktur authentisieren" in der API-Schnittstelle [E-Rezept API Dokumentation].

### A\_20666-01**~~A\_20666~~** - Auslesen des Authentisierungszertifikates

Das Primärsystem MUSS das Zertifikat ID.HCI.OSIGAUT der SM-B über die Operation ReadCardCertificate des Konnektors gemäß [gemSpec\_Kon#4.1.9.5.2] bzw. [gemILF\_PS#4.4.4.2] auslesen. [ <= ]

Hinweis: Im Rahmen der Signatur wird auf privates Schlüsselmaterial zugegriffen. Die verwendeten Karten müssen sich daher in einem erhöhten Sicherheitszustand befinden, der ggf. erst durch eine PIN-Eingabe hergestellt werden muss. Das Primärsystem muss den Kartenzustand abfragen und die Karte ggf. durch den Nutzer freischalten lassen. Mit dem (optionalen) Einblenden eines Hinweises der Form "Bitte beachten Sie die Anzeige an Ihrem Kartenterminal" muss das Primärsystem dafür sorgen, dass die Abfrage einer PIN-Eingabe am Kartenterminal vom Benutzer nicht übersehen wird.

Anschließend werden die signierte "challenge" und das verwendete Authentisierungszertifikat der Smartcard an den IDP-Dienst übermittelt.

### A\_20667-01**~~A\_20667~~** - Response auf die Challenge des Authorization-Endpunktes

Das Primärsystem MUSS das eingereichte "CHALLENGE\_TOKEN" zusammen mit der von der Smartcard signierten Challenge-Signatur "signed\_challenge" (siehe A\_20665) und dem Authentifizierungszertifikat der Smartcard (siehe A\_20666), mit dem öffentlichen Schlüssel des Authorization-Endpunktes "PUK\_AUTHIDP\_ENC" verschlüsselt, an diesen in Form eines HTTP-~~signed\_challenge~~POSTPOST-Requests senden.

Der Aufbau der der Anfrage und des der einzureichenden Objekte entspricht gemSpec IDP-Dienst#Kapitel 7.3 [ <= ]

~~Hinweis: Der folgende beispielhafte Aufruf skizziert den HTTP-POST-Request, welcher vom Authenticator-Modul an den Authorization-Endpunkt des IDP-Dienstes übertragen wird. Dabei wird das signierte und verschlüsselte "CHALLENGE\_TOKEN" nur angedeutet:~~



POST /sign\_response HTTP/1.1

Host: idp.com

Content-Type: application/x-www-form-urlencoded

signed\_challenge=eyJhbGciOiJFUzI1NiIsInR5cCI6IkpPU0UrSINPTiIsIng.....

Der

*Im Rahmen der Vorveröffentlichung finden sich Details zum Aufbau auf den Webseiten der gematik zur Entwicklungsunterstützung sowie in der Vorveröffentlichung des Dokumentes gemF Tokenverschlüsselung. Das Dokument gemSpec IDP-Dienst beinhaltet noch keine aktuellen Angaben.*

Hinweis: Das Signieren und Verschlüsseln des "CHALLENGE\_TOKEN" ist durch die Verwendung eines Nested JWT [angelehnt an den folgenden Draft: <https://tools.ietf.org/html/draft-yusef-oauth-nested-jwt-03>] zu realisieren. Im ctty-Header ist "NJWT" zu setzen, um anzuzeigen, dass es sich um einen Nested JWT handelt. Das Signieren wird dabei durch die Verwendung einer JSON Web Signature (JWS) [RFC7515 # section-3 - Compact Serialization] gewährleistet. Die Verschlüsselung des signierten Token wird durch die Nutzung der JSON Web Encryption (JWE) [RFC7516 # section-3] sichergestellt. Als Verschlüsselungsalgorithmus ist ECDH-ES (Elliptic Curve Diffie-Hellman Ephemeral Static key agreement) vorgesehen.

Der Authorization-Endpunkt validiert nun die "session" sowie die "signed\_challenge"-und prüft das Zertifikat der LEI. Anschließend verknüpft er die "session" mit der Identität aus dem Authentisierungszertifikat und erstellt einen "AUTHORIZATION\_CODE", welchen er als Antwort zurücksendet.

Das Primärsystem empfängt nun diesen "AUTHORIZATION\_CODE" von IDP-Dienst und prüftrecht ihn zusammen mit dem KEY VERIFIER beim Token-Endpunkt ein.

A\_20668 - Annahme des "AUTHORIZATION\_CODE"

Das Primärsystem MUSS den vom Authorization-Endpunkt als Antwort auf die signierte Challenge gesendeten "AUTHORIZATION\_CODE" verarbeiten. Das Primärsystem MUSS das "AUTHORIZATION\_CODE" ablehnen, wenn dieser außerhalb der mit dem Authorization-Endpunkt etablierten TLS-Verbindung übertragen wird.[<=]

~~Hinweis: Der Authorization-Endpunkt liefert den "AUTHORIZATION\_CODE" innerhalb einer HTTP-Redirection (HTTP-Status-Code 302) an das Primärsystem zurück. Der Wert des Attributs "location" der HTTP-302-Response ist nicht relevant. Nachfolgend wird ein beispielhafter Response des Authorization-Endpunkt skizziert, dabei wird der "AUTHORIZATION\_CODE", nur angedeutet:~~

HTTP/1.1 302 Found

Location: <https://app.erezept.com/authnres?code=eyJhbGciOiJkaXIiL...&state=af0ifjsldkj>

A\_21333 - Erzeugung des "Token-Key"

~~A\_20669 - Formale Prüfung der Signatur des AUTHORIZATION\_CODE~~



Der Token-Endpoint validiert den "CODE\_VERIFIER" und gleicht diesen mit der "code\_challenge" ab. Dann erzeugt er die erforderlichen Token und verschlüsselt ~~das "ACCESS\_TOKEN" für den empfangenden Fachdienst. beide mit dem "Token-Key".~~

Das Primärsystem erhält nun den signierten "ID\_TOKEN" und den ~~für es nicht lesbaren~~ "ACCESS\_TOKEN" vom Token-Endpoint und prüft die Signatur des "ID\_TOKEN".

~~A 20672-01A\_20672~~ - Annahme des ID\_TOKEN

Das Primärsystem MUSS das vom Token-Endpoint ausgegebene "ID\_TOKEN" als HTTP/1.1 Statusmeldung 200 verarbeiten- und mittels "Token-Key" entschlüsseln. Das Primärsystem MUSS das "ID\_TOKEN" ablehnen, wenn dieses außerhalb der mit dem Token-Endpoint etablierten TLS-Verbindung übertragen wird oder nicht mit dem vorher übermittelten "Token-Key" verschlüsselt war.

Die Aufbau der Antwort und des "ID\_TOKEN" entspricht gemSpec IDP-Dienst#Kapitel 7.6[<=.-{<=.]

Im Rahmen der Vorveröffentlichung finden sich Details zum Aufbau auf den Webseiten der gematik zur Entwicklungsunterstützung sowie in der Vorveröffentlichung des Dokumentes gemF Tokenverschlüsselung. Das Dokument gemSpec IDP-Dienst beinhaltet noch keine aktuellen Angaben.

~~A 20673-01A\_20673~~ - Annahme des "ACCESS\_TOKEN"

Das Primärsystem MUSS das vom Token-Endpoint ausgegebene "ACCESS\_TOKEN" in der HTTP/1.1 Statusmeldung 200 verarbeiten- und mittels "Token-Key" entschlüsseln. Das Primärsystem MUSS das "ACCESS\_TOKEN" ablehnen, wenn dieses außerhalb der mit dem Token-Endpoint etablierten TLS-Verbindung übertragen wird oder nicht mit dem vorher übermittelten "Token-Key" verschlüsselt war.

Die Aufbau der Antwort und des ACCESS\_TOKEN entspricht gemSpec IDP-Dienst#Kapitel 7.6[<=.-{<=.]

~~Hinweis: Das Primärsystem nimmt sowohl den "ID\_TOKEN" als auch den "ACCESS\_TOKEN" aus der Antwort des Token-Endpunktes des IDP-Dienstes. Der Token-Endpoint antwortet mit den Token auf die erfolgreiche Übergabe und Validierung des "AUTHORIZATION\_CODES" durch das Anwendungsfrontend. Nachfolgend wird beispielhaft die Antwort des Token-Endpunktes skizziert. Der "ID\_TOKEN" und der "ACCESS\_TOKEN" werden dabei nur angedeutet:~~

~~HTTP/1.1 200 OK~~

~~Content-Type: application/json~~

~~Cache-Control: no-store~~

~~Pragma: no-cache~~

~~-~~

~~{"token\_type": "Bearer",~~

~~"expires\_in": 300,~~

~~"id\_token": "...",~~

~~"access\_token": "...",~~

~~}Im Rahmen der Vorveröffentlichung finden sich Details zum Aufbau auf den Webseiten der gematik zur Entwicklungsunterstützung sowie in der Vorveröffentlichung des Dokumentes gemF Tokenverschlüsselung. Das Dokument gemSpec IDP-Dienst beinhaltet noch keine aktuellen Angaben.~~

810 A\_20674 - Formale Prüfung der Signatur des ID\_TOKEN  
811 Das Primärsystem MUSS die Signatur des ID\_TOKEN mathematisch prüfen und auf ein  
812 zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID "oid\_idpd" zurückführen  
813 können. [≤]

814 Zur Prüfung von Zertifikatstyp- und Rollen-OID siehe Hinweis zu A\_20657.

815 A\_20675 - Gültigkeitsprüfung der Signatur des ID\_TOKEN innerhalb der TI  
816 Das Primärsystem MUSS das zur Signatur des ID\_TOKEN verwendete Zertifikat über die  
817 Funktion „VerifyCertificate“ des Konnektors gemäß [gemSpec\_Kon#4.1.9.5.3] bzw.  
818 [gemILF\_PS#4.4.4.3] auf Gültigkeit innerhalb der TI prüfen. [≤]

819  
820 Im weiteren Verlauf kann der "ACCESS\_TOKEN" innerhalb seiner Gültigkeitsdauer bei  
821 verschiedenen Aufrufen des Fachdienstes eingereicht werden. Der Fachdienst  
822 entschlüsselt das "ACCESS\_TOKEN" mit seinem privaten Schlüssel, validiert es, zieht die  
823 notwendigen Informationen entsprechend seinem Claim heraus und verwendet diese für  
824 seine fachlichen Operationen.

## 825 **5.2 Anwendungsfälle verordnende LEI**

826 Folgende Anwendungsfälle werden im Primärsystem einer verordnenden LEI umgesetzt.

### 827 **5.2.1 E-Rezept erstellen**

828 Mit diesem Anwendungsfall werden die Aufbewahrungspflichten der verordnenden LEI  
829 unterstützt. Das PS der verordnenden LEI fragt für das Erstellen eines E-Rezepts beim E-  
830 Rezept-Fachdienst eine über 11 Jahre eindeutige Rezept-ID ab, die für das E-Rezept  
831 verwendet wird.

832 A\_19274 - PS verordnende LEI: E-Rezept durch Verordnenden erstellen  
833 Das PS der verordnenden LEI MUSS den Anwendungsfall "UC 2.1 - E-Rezepte  
834 erzeugen" aus [gemSysL\_eRp] gemäß TAB\_ILFERP\_002 umsetzen.

#### 835 **Tabelle 4 : TAB\_ILFERP\_002 – E-Rezept durch Verordnenden erstellen**

|                |  |
|----------------|--|
| Name           | E-Rezept durch Verordnenden erstellen  |
| Auslöser       | <ul style="list-style-type: none"><li>• Aufruf des Anwendungsfalls in der GUI</li></ul>  |
| Akteur         | Leistungserbringer, Mitarbeiter verordnende LEI  |
| Vorbedingung   | <ul style="list-style-type: none"><li>• Die LEI hat sich gegenüber der TI authentisiert.</li></ul>   |
| Nachbedingung  | <ul style="list-style-type: none"><li>• Im PS steht ein QES-Datensatz über den Verordnungsdatensatz des E-Rezept bereit.</li></ul>                 |
| Standardablauf | <ol style="list-style-type: none"><li>1. E-Rezept-ID von Fachdienst abrufen</li><li>2. E-Rezept-Bundle erstellen</li><li>3. Kanonisieren</li></ol> |

|  |  |
|--|--|
|  | 4. E-Rezept-Bundle QES signieren (nur durch LE ausführbar) |
|--|--|

[<=]

A\_19276 - PS verordnende LEI: E-Rezept einstellen - E-Rezept-ID abrufen

Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch

Verordnenden erstellen" für das E-Rezept die HTTP-Operation `POST /Task/$create` mit

- `ACCESS_TOKEN` im Authorization-Header
- Rezept-Typ im `FlowType` als Parameter der FHIR-Operation `$create` für Task

ausführen.[<=]

Für weitere Informationen siehe Operation "E-Rezept erstellen" aus der API-Schnittstelle [E-Rezept API Dokumentation].

Der Value-Katalog für `FlowType` ist in [gemSpec\_DM\_eRp] beschrieben.

Der Response des Fachdienstes liefert

- die Rezept-ID (`Task.Identifizier` mit "<https://gematik.de/fhir/NamingSystem/PrescriptionID>"), mit der das E-Rezept-Bundle vervollständigt wird,
- die Task-ID (`Task.id`), mit dem der Task bei Aufrufen des E-Rezept-Fachdienstes referenziert wird,
- und den `AccessCode` (`Task.Identifizier` mit "<https://gematik.de/fhir/NamingSystem/accessCode>"), welcher für den Zugriff auf das E-Rezept im Fachdienst berechtigt

A\_19275 - PS verordnende LEI: E-Rezept einstellen - E-Rezept-Bundle erstellen

Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch

Verordnenden erstellen" eine Bundle-FHIR-Ressource gemäß

Profilierung [https://fhir.kbv.de/StructureDefinition/KBV\\_PR\\_ERP\\_Bundle](https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle)

- Rezept-ID aus der Task-Ressource als Identifizier

erstellen.[<=]

Dieses Bundle wird in diesem Dokument als E-Rezept-Bundle bezeichnet. Ein E-Rezept-Bundle enthält genau eine Verordnungszeile.

A\_19559 - PS verordnende LEI: E-Rezept einstellen - E-Rezept-Bundle kanonisieren

Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch

Verordnenden erstellen" das E-Rezept-Bundle vor dem Signieren kanonisieren und dazu die Kanonisierungsregeln <https://www.w3.org/TR/2008/REC-xml-c14n11-20080502/> für

Canonical XML Version 1.1 für XML-Dokumente anwenden.[<=]

Für die qualifizierte elektronische Signatur des E-Rezept Bundels wird der Konnektor verwendet. Es wird eine CMS-Signatur (CADES) erstellt. Die Operation für die QES muss durch den Leistungserbringer durchgeführt werden.

~~A\_19281-01~~ **A\_19281** - PS verordnende LEI: E-Rezept einstellen - E-Rezept-Bundle QES signieren

874 Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch  
875 Verordnenden erstellen" für das E-Rezept die Signaturoperation des Konnektors mit

- 876 • der Referenz RFC-5652 für CMS-Signatur (CAvES)
- 877 • Signaturtype für eine enveloping Signature
- 878 • dem base64-codierten E-Rezept-Bundle
- 879 • eingebetteter OCSP-Antwort (IncludeRevocationInfo = true)

880 ausführen. [ <= ]

881 Für weitere Informationen siehe Operation "E-Rezept qualifiziert signieren" aus der API-  
882 Schnittstelle [E-Rezept API Dokumentation].

883 Für die Nutzung der Komfortsignatur siehe [gemILF\_PS].

884 A\_21243 - PS verordnende LEI: E-Rezept-einstellen - Unterstützung Signaturverfahren  
885 Das PS der verordnenden LEI MUSS muss die Erstellung der E-Rezepte mittels  
886 Einzelsignatur, Stapelsignatur und Komfortsignatur unterstützen. [ <= ]

887 Falls keine Komfortsignatur zur Verfügung steht oder die Komfortsignatur deaktiviert ist,  
888 soll das PS der verordnenden LEI die Stapelsignatur verwenden ist, falls mehrere E-  
889 Rezepte signiert werden sollen.

## 890 5.2.2 E-Rezept einstellen

891 Mit diesem Anwendungsfall wird das von der verordnenden LEI erstellte E-Rezept auf  
892 dem Fachdienst eingestellt, damit es für den Versicherten verfügbar ist.

893 Das erstellte E-Rezept-Bundle wird innerhalb einer PKCS#7-Datei (enveloping) für die  
894 QES an den Task in der \$activate-Operation übergeben.

895 A\_19272 - PS verordnende LEI: E-Rezept durch Verordnenden einstellen  
896 Das PS der verordnenden LEI MUSS den Anwendungsfall "UC 2.3 - E-Rezept  
897 einstellen" aus [gemSysL\_eRp] gemäß TAB\_ILFERP\_003 umsetzen.

898 **Tabelle 5 : TAB\_ILFERP\_003 – E-Rezept durch Verordnenden einstellen**

| Name          | E-Rezept durch Verordnenden einstellen  |
|---------------|---|
| Auslöser      | <ul style="list-style-type: none"> <li>• Aufruf des Anwendungsfalls in der GUI</li> <li>• kann durch "E-Rezept durch Verordnenden erstellen" getriggert werden</li> </ul>   |
| Akteur        | Leistungserbringer, Mitarbeiter verordnende LEI   |
| Vorbedingung  | <ul style="list-style-type: none"> <li>• Das E-Rezept wurde erstellt. (Anwendungsfall "E-Rezept erstellen"). Es stehen ein QES-signiertes E-Rezept-Bundle als PKCS#7-Datei bereit.</li> <li>• Die LEI hat sich gegenüber der TI authentisiert.</li> </ul> |
| Nachbedingung | <ul style="list-style-type: none"> <li>• Das E-Rezept ist auf dem E-Rezept-Fachdienst gespeichert. Es kann durch den Versicherten oder einen Apotheker in Kenntnis</li> </ul>   |



|                |   |
|----------------|---|
|                | der Einlöseinformationen (Task-ID + AccessCode) abgerufen werden.   |
| Standardablauf | <ol style="list-style-type: none"><li>1. Task auf dem E-Rezept-Fachdienst aktivieren</li><li>2. optional, wenn das E-Rezept ausgedruckt werden soll:<ol style="list-style-type: none"><li>a. E-Rezept-Token erzeugen</li><li>b. E-Rezept-Ausdruck erstellen</li></ol></li></ol> |

899 **[<=]**

900 A\_19273-01 - PS verordnende LEI: E-Rezept einstellen - Task auf Fachdienst aktivieren  
901 Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch  
902 Verordnenden einstellen" für das E-Rezept die HTTP-Operation `POST`  
903 `/Task/<id>/$activate` mit

- 904
  - `ACCESS_TOKEN` im Authorization-Header
  - 905 • `Task-ID` in URL `<id>`
  - 906 • `AccessCode` im `X-AccessCode-Header` oder als URL-Parameter `?ac=`
  - 907 • QES signiertes E-Rezept-Bundle im `http-Body` des Aufrufs als `data`

908 ausführen. **[<=]**

909 Für weitere Informationen siehe Operation "E-Rezept vervollständigen und Task  
910 aktivieren" aus der API-Schnittstelle [E-Rezept API Dokumentation].

911 Es gelten vorrangig die Regelungen zum Ausdruck eines E-Rezepts aus den  
912 Bundesmantelverträgen [BMV] und [BMV-Z].

913 A\_19279 - PS verordnende LEI: E-Rezept einstellen - E-Rezept-Token erstellen  
914 Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch  
915 Verordnenden einstellen" einen E-Rezept-Token erstellen, wenn ein Ausdruck der  
916 Einlöseinformationen des E-Rezepts erstellt werden soll. **[<=]**

917 Für die Spezifikation des E-Rezept-Token siehe [gemSpec\_DM\_eRp#2.3].

918 A\_19280 - PS verordnende LEI: E-Rezept einstellen - E-Rezept ausdrucken  
919 Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch  
920 Verordnenden einstellen", wenn ein Ausdruck des E-Rezepts erstellt werden soll, den  
921 Datamatrix-Code für den E-Rezept-Token erstellen und diesen zusammen mit  
922 Zusatzinformationen ausdrucken. **[<=]**

923 Für die Spezifikation des Datamatrix-Code für E-Rezept-Token siehe  
924 [gemSpec\_DM\_eRp#2.3].

925 Für Regelungen zum Inhalt des Ausdrucks siehe auch Bundesmantelverträge [BMV] und  
926 [BMV-Z]

## 927 **5.2.3 E-Rezept löschen**

928 Mit diesem Anwendungsfall kann die verordnende LEI ein E-Rezept löschen, welches sie  
929 zuvor auf den E-Rezept-Fachdienst eingestellt hat.

930 A\_19236 - PS verordnende LEI: E-Rezepte löschen - E-Rezept zum Löschen auswählen  
931 Das PS der verordnenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept zum  
932 Löschen auf dem Fachdienst auszuwählen. **[<=]**

933 A\_19237 - PS verordnende LEI: E-Rezept löschen - Bestätigung  
934 Das PS der verordnenden LEI MUSS vom Nutzer eine Bestätigung einholen, dass das  
935 ausgewählte E-Rezept gelöscht werden soll und die Möglichkeit geben, das  
936 Löschen abubrechen.[<=]

937 A\_19238 - PS verordnende LEI: E-Rezept durch Verordnenden löschen  
938 Das PS der verordnenden LEI MUSS den Anwendungsfall "UC 2.5 - E-Rezept durch  
939 Verordnenden löschen" aus [gemSysL\_eRp] gemäß TAB\_ILFERP\_004 umsetzen.

940 **Tabelle 6 : TAB\_ILFERP\_004 – E-Rezept durch Verordnenden löschen**

|                |   |
|----------------|---|
| Name           | E-Rezept durch Verordnenden löschen   |
| Auslöser       | <ul style="list-style-type: none"><li>• Aufruf des Anwendungsfalls in der GUI</li></ul>   |
| Akteur         | Leistungserbringer, Mitarbeiter verordnende LEI   |
| Vorbedingung   | <ul style="list-style-type: none"><li>• Der Nutzer hat ein E-Rezept zum Löschen markiert und das Löschen bestätigt.</li><li>• Die LEI hat sich gegenüber der TI authentisiert.</li></ul>      |
| Nachbedingung  | <ul style="list-style-type: none"><li>• Das ausgewählte E-Rezept ist vom E-Rezept-Fachdienst unwiederbringlich gelöscht.</li></ul>  |
| Standardablauf | <ol style="list-style-type: none"><li>1. Task-ID und AccessCode des E-Rezepts bestimmen</li><li>2. E-Rezept auf E-Rezept-Fachdienst löschen</li><li>3. E-Rezept-Token in PS löschen</li></ol> |

941 [<=]

942 A\_19239-01 - PS verordnende LEI: E-Rezept löschen - Löschrequest  
943 Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch  
944 Verordnenden löschen" für das zu löschende E-Rezept die HTTP-OperationPOST  
945 /TASK/<id>/\$abort mit

- 946
  - ACCESS\_TOKEN im Authorization-Header
  - Task-ID in URL <id>
  - AccessCode im X-AccessCode-Header oder als URL-Parameter ?ac=

949 ausführen.[<=]

950 Für weitere Informationen siehe Operation "Ein E-Rezept löschen" aus der API-  
951 Schnittstelle [E-Rezept API Dokumentation].

952 A\_19240 - PS verordnende LEI: E-Rezept löschen - E-Rezept-Token löschen  
953 Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch Verordnenden  
954 löschen" für das zu löschende E-Rezept nach erfolgreichem Aufruf der Operation "Ein E-  
955 Rezept löschen" die Task-ID und den AccessCode im PS löschen.[<=]

## 956 **5.3 Anwendungsfälle abgebende LEI**

957 Folgende Anwendungsfälle werden im Primärsystem einer abgebenden LEI umgesetzt.



### 5.3.1 E-Rezept abrufen

Mit diesem Anwendungsfall kann die abgebende LEI Daten zum E-Rezept inklusive QES zu einem vom Versicherten empfangenen E-Rezept-Token vom E-Rezept-Fachdienst abrufen, um das E-Rezept einzulösen.  
Darüber hinaus wird durch die Gültigkeit der QES sichergestellt, dass es sich um ein gegenüber der Krankenkasse abrechenbares gültiges E-Rezept handelt.

A\_19293 - PS abgebende LEI: E-Rezept abrufen - E-Rezept-Token auswählen  
Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept-Token auszuwählen, zu dem das E-Rezept vom Fachdienst abgerufen werden soll. [**<=**]

A\_19294 - PS abgebende LEI: E-Rezept abrufen  
Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.1 - E-Rezept abrufen" aus [gemSysL\_eRp] gemäß TAB\_ILFERP\_005 umsetzen.

**Tabelle 7 : TAB\_ILFERP\_005 – E-Rezept abrufen**

|                |   |
|----------------|---|
| Name           | E-Rezept abrufen  |
| Auslöser       | <ul style="list-style-type: none"><li>Aufruf des Anwendungsfalls in der GUI</li></ul>   |
| Akteur         | Leistungserbringer, Mitarbeiter der abgebenden LEI  |
| Vorbedingung   | <ul style="list-style-type: none"><li>Die LEI hat den E-Rezept-Token zum E-Rezept übermittelt bekommen. Der E-Rezept-Token steht im PS bereit.</li><li>Der Nutzer hat das E-Rezept zum Abruf markiert.</li><li>Die LEI hat sich gegenüber der TI authentisiert.</li></ul> |
| Nachbedingung  | <ul style="list-style-type: none"><li>Das E-Rezept steht im PS bereit.</li></ul>  |
| Standardablauf | <ol style="list-style-type: none"><li>Task-ID und AccessCode des E-Rezepts bestimmen</li><li>Task herunterladen</li><li>QES prüfen</li><li>Verordnung extrahieren</li><li>E-Rezept-Daten speichern</li></ol>  |

[**<=**]

A\_19558-01 - PS abgebende LEI: E-Rezept abrufen - Task herunterladen  
Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept abrufen" zum Herunterladen des E-Rezepts die HTTP-Operation `POST /Task/<id>/$accept` mit

- ACCESS\_TOKEN im Authorization-Header
- Task-ID in URL `<id>`
- AccessCode im `X-AccessCode-Header` oder als URL-Parameter `?ac=`

ausführen. [**<=**]

Für weitere Informationen siehe Operation "E-Rezepte abrufen" aus der API-Schnittstelle [E-Rezept API Dokumentation].

Der Response liefert eine `Task` Ressource. Für die Spezifikation der `Task` Ressource siehe [gemSpec\_DM\_eRp]. Jeder Task enthält die folgenden fachlichen Informationen:

- `Secret` - Dieser Code wurde vom E-Rezept-Fachdienst spezifisch für diesen Abruf des E-Rezepts erstellt. Er berechtigt, die weiteren Statusänderungen auf dem E-Rezept-Fachdienst vorzunehmen.
- `signature` - base64 kodierter PKCS#7-Datei mit dem E-Rezept-Bundle und der Signatur, wie sie vom Konnektor der verordnenden LEI generiert wurde.

Für die QES-Prüfung wird die PKCS#7-Datei verwendet. Die Verordnungsdaten des E-Rezepts sind innerhalb der PKCS#7-Datei enthalten und müssen für die Weiterverarbeitung extrahiert werden.

A\_19745 - PS abgebende LEI: E-Rezept abrufen - QES prüfen

Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept abrufen" zum Prüfen der QES des E-Rezepts die Operation `POST //Konnektorservice` mit

- Header "`SOAPAction: \"http://ws.gematik.de/conn/SignatureService/v7.4#VerifyDocument\"`"
- PKCS#7-Datei in `SignatureObject`

ausführen. [`<=`]

Für weitere Informationen siehe Operation "Qualifizierte Signatur des E-Rezepts prüfen" aus der API-Schnittstelle [E-Rezept API Dokumentation]. Implementierungshinweise zur Signaturprüfung für Primärsysteme sind in [gemILF\_PS#4.4.2] beschrieben. Die Außenschnittstelle des Konnektors ist in [gemSpec\_Kon#TIP1-A\_5034-x Operation `VerifyDocument` (nonQES und QES)] beschrieben.

Als Response liefert der Konnektor einen standardisierten Prüfbericht in einer `VerificationReport`-Struktur gemäß [OASIS-VR].

Für die weitere Verarbeitung wird das E-Rezept-Bundle aus der PKCS#7-Datei verwendet.

A\_19900 - PS abgebende LEI: E-Rezept abrufen - E-Rezept-Bundle extrahieren

Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept abrufen" die Daten zum E-Rezept-Bundle zur Weiterverarbeitung extrahieren. [`<=`]

A\_19901 - PS abgebende LEI: E-Rezept abrufen - Daten speichern

Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept abrufen" das E-Rezept-Bundle und das `Secret` im PS speichern. [`<=`]

Möchte der Versicherte die Möglichkeit einer Rezepteinlösung mit Versandbestellung nutzen, kann die abgebende LEI die Versand- und ggfs. Zuzahlungsmodalitäten über ihr Warenwirtschaftssystem ("Onlineshop") abwickeln. Hierzu ist ggfs. die Übernahme von Rezeptinformationen zur Befüllung eines Warenkorbs erforderlich.

A\_21372 - PS abgebende LEI: Übernahme Rezeptinformationen in Warenwirtschaftssystem

Das PS der abgebenden LEI MUSS bei der Übernahme von E-Rezept-Informationen in ein Warenwirtschaftssystem die Integrität und Vertraulichkeit der personenbezogenen und medizinischen Daten sicherstellen. [`<=<=>`]

### 1023 5.3.2 Quittung abrufen

1024 Mit diesem Anwendungsfall kennzeichnet das PS der abgebenden LEI das E-Rezept nach  
1025 der Belieferung im E-Rezept-Fachdienst als abgegeben und lädt die Quittung herunter,  
1026 die für die weiteren Abrechnungsprozesse genutzt wird.  
1027 Darüber hinaus werden dem E-Rezept-Fachdienst Informationen über das abgegebene  
1028 Medikament bereitgestellt, die dann vom Versicherten auf seinem FdV heruntergeladen  
1029 werden können.

1030 A\_19286 - PS abgebende LEI: Quittung abrufen - E-Rezept auswählen  
1031 Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept als  
1032 abgegeben auszuwählen. [ $\leq$ ]

1033 A\_19287-01 - PS abgebende LEI: Quittung abrufen  
1034 Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.4 - Quittung abrufen" aus  
1035 [gemSysL\_eRp] gemäß TAB\_ILFERP\_006 umsetzen.

#### 1036 **Tabelle 8 : TAB\_ILFERP\_006 – Quittung abrufen**

|                |   |
|----------------|---|
| Name           | Quittung abrufen  |
| Auslöser       | <ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>   |
| Akteur         | Leistungserbringer, Mitarbeiter der abgebenden LEI  |
| Vorbedingung   | <ul style="list-style-type: none"> <li>Die LEI hat das E-Rezept vom E-Rezept-Fachdienst heruntergeladen.</li> <li>Der Nutzer hat ein E-Rezept als abgegeben markiert.</li> <li>Die LEI hat sich gegenüber der TI authentisiert.</li> </ul>  |
| Nachbedingung  | <ul style="list-style-type: none"> <li>Die Quittung des E-Rezepts steht im PS bereit.</li> </ul>  |
| Standardablauf | <ol style="list-style-type: none"> <li>Informationen über das abgegebene Medikament erstellen</li> <li>nur für Fertigarzneimittel, die einen Data-Matrix-Code gemäß securPharm-System besitzen: Chargeninfo und Verfallsdatum ergänzen</li> <li>Task-ID und Geheimnis des E-Rezepts bestimmen</li> <li>E-Rezept-Status auf E-Rezept-Fachdienst ändern</li> <li>Quittung aus Response extrahieren</li> <li>optional: Signatur der Quittung prüfen</li> </ol> |

1037 [ $\leq$ ]

1038 A\_19288 - PS abgebende LEI: Quittung - MedicationDispense erstellen  
1039 Das PS der abgebenden LEI MUSS im Anwendungsfall "Quittung abrufen" eine FHIR-  
1040 Ressource `MedicationDispense` mit den Informationen über das abgegebene Medikament  
1041 erstellen. [ $\leq$ ]

1042 Für die Spezifikation der Ressource `MedicationDispense` siehe [gemSpec\_DM\_eRp]. Die  
1043 Befüllung des Medication-Objekts der MedicationDispense kann in Abhängigkeit eines  
1044 Austauschs aus der Übernahme der wesentlichen Attribute (PZN, Wirkstoff,

1045 Darreichungsform, Dosierinformationen) aus dem Verordnungsdatensatz und den Daten  
1046 aus dem Securpharm-Scan in die MedicationDispense und Medication kopiert werden.  
1047 Weitere Informationen, die sich aus dem Scan des Securpharm-Codes für  
1048 Fertigarzneimittel ergeben (z.B. Charge, Haltbarkeitsdatum) und im Primärsystem  
1049 vorliegen, können ebenfalls übernommen werden.

1050 A\_21105 - PS abgebende LEI: Chargeninfo in Medication ergänzen  
1051 Das PS der abgebenden LEI MUSS im Anwendungsfall "Quittung abrufen" die FHIR-  
1052 Ressource "Medication" der erstellten MedicationDispense um Chargeninformation und  
1053 Verfallsdatum aus dem SecurPharm-Scan [SecurPharm] ergänzen, sofern es sich bei dem  
1054 abgegebenen Arzneimittel um ein Fertigarzneimittel handelt, das einen Data-Matrix-Code  
1055 gemäß securPharm-System besitzt. [**<=**]

1056 A\_19289 - PS abgebende LEI: Quittung abrufen - Statusrequest  
1057 Das PS der abgebenden LEI MUSS im Anwendungsfall "Quittung abrufen" für das  
1058 abgegebene E-Rezept die HTTP-Operation `POST /Task/<id>/$close` mit

- 1059 • `ACCESS_TOKEN` im Authorization-Header
- 1060 • Task-ID in URL `<id>`
- 1061 • Geheimnis in URL-Parameter `?secret=`
- 1062 • `MedicationDispense` Ressource

1063 ausführen. [**<=**]

1064 Für weitere Informationen siehe Operation "E-Rezept-Abgabe vollziehen" aus der API-  
1065 Schnittstelle [E-Rezept API Dokumentation].

1066 Der Response enthält ein signiertes Quittungs-Bundle, welches im Abrechnungsprozess  
1067 genutzt wird.

1068

1069 Der E-Rezept-Fachdienst prüft regelmäßig den Status seines Signaturzertifikats, die  
1070 mandatorische Signaturprüfung der Quittung obliegt dem Quittungsempfänger, kann  
1071 aber vom AVS vor der Weitergabe in die Abrechnungsprozesse ebenfalls geprüft werden.

1072 Die Quittung wird als PKCS#7-Datei erstellt. Die quitierten Daten sind innerhalb der  
1073 PKCS#7-Datei enthalten.

1074 A\_20766 - PS abgebende LEI: Quittung - Quittungssignatur prüfen  
1075 Das PS der abgebenden LEI KANN im Anwendungsfall "Quittung abrufen" zum Prüfen der  
1076 Quittung des E-Rezepts die Operation `POST //Konnektorservice` mit

- 1077 • Header `"SOAPAction:`  
1078 `\"http://ws.gematik.de/conn/SignatureService/v7.4#VerifyDocument\""`
- 1079 • `PKCS#7-Datei` in `SignatureObject`

1080 ausführen. [**<=**]

1081 Implementierungshinweise zur Signaturprüfung für Primärsysteme sind in  
1082 [gemILF\_PS#4.4.2] beschrieben. Die Außenschnittstelle des Konnektors ist in  
1083 [gemSpec\_Kon#TIP1-A\_5034-x Operation VerifyDocument (nonQES und QES)]  
1084 beschrieben.

1085 Als Response liefert der Konnektor einen standardisierten Prüfbericht in einer  
1086 `VerificationReport`-Struktur gemäß [OASIS-VR].

### **5.3.3 Quittung erneut abrufen**

Mit diesem Anwendungsfall kann die abgebende LEI die Quittung erneut abrufen, falls bei der Übermittlung vom E-Rezept-Fachdienst ein Fehler aufgetreten ist.

Der Anwendungsfall kann bei Bedarf wiederholt werden.

A\_19290 - PS abgebende LEI: Quittung erneut abrufen - E-Rezept auswählen

Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept auszuwählen, zu dem die Quittung erneut abgerufen werden soll. [**<=**]

A\_19291 - PS abgebende LEI: Quittung erneut abrufen

Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.8 - Quittung erneut abrufen" aus [gemSysL\_eRp] gemäß TAB\_ILFERP\_007 umsetzen.

**Tabelle 9 : TAB\_ILFERP\_007 – Quittung erneut abrufen**

|                |  |
|----------------|--|
| Name           | Quittung erneut abrufen  |
| Auslöser       | <ul style="list-style-type: none"><li>Aufruf des Anwendungsfalls in der GUI</li></ul>  |
| Akteur         | Leistungserbringer, Mitarbeiter der abgebenden LEI   |
| Vorbedingung   | <ul style="list-style-type: none"><li>Die LEI hat bereits mindestens einmal die Quittung abgerufen (Anwendungsfall "Quittung abrufen").</li><li>Die LEI hat sich gegenüber der TI authentisiert.</li></ul> |
| Nachbedingung  | <ul style="list-style-type: none"><li>Die Quittung zum E-Rezept steht im PS bereit.</li></ul>  |
| Standardablauf | <ol style="list-style-type: none"><li>Task-ID und Geheimnis des E-Rezepts bestimmen</li><li>Quittung abrufen</li><li>Quittung aus Response extrahieren</li></ol>   |

[**<=**]

A\_19292 - PS abgebende LEI: Quittung erneut abrufen - Statusrequest

Das PS der abgebenden LEI MUSS im Anwendungsfall "Quittung erneut abrufen" für das E-Rezept die HTTP-Operation `GET /Task/<id>` mit

- ACCESS\_TOKEN im Authorization-Header
- Task-ID in URL `<id>`
- Geheimnis in URL Parameter `?secret=`

ausführen. [**<=**]

Für weitere Informationen siehe Operation "Quittung erneut abrufen" aus der API-Schnittstelle [E-Rezept API Dokumentation].

Der Response enthält ein signiertes Quittungs-Bundle, welches im Abrechnungsprozess genutzt wird.

### 1110 **5.3.4 E-Rezept zurückgeben**

1111 Mit diesem Anwendungsfall kann die abgebende LEI ein E-Rezept, welches vom E-  
1112 Rezept-Fachdienst abgerufen wurde, wieder zurückgeben, z.B. weil das E-Rezept nicht  
1113 beliefert werden kann oder weil der Versicherte darum gebeten hat. Nachfolgend kann es  
1114 durch den Versicherten einer anderen abgebenden LEI zugewiesen werden.

1115 A\_19246 - PS abgebende LEI: E-Rezepte zurückgeben - E-Rezept auswählen  
1116 Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept zum  
1117 Zurückgeben auszuwählen. [**<=**]

1118 A\_19247 - PS abgebende LEI: E-Rezept zurückgeben - Bestätigung  
1119 Das PS der abgebenden LEI MUSS vom Nutzer eine Bestätigung einholen, dass das  
1120 ausgewählte E-Rezept zurückgegeben werden soll und die Möglichkeit geben, das  
1121 Zurückgeben abubrechen. [**<=**]

1122 A\_19249 - PS abgebende LEI: E-Rezept durch Abgebenden zurückgeben  
1123 Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.2 - E-Rezept durch  
1124 Abgebenden zurückgeben" aus [gemSysL\_eRp] gemäß TAB\_ILFERP\_008 umsetzen.

1125 **Tabelle 10 : TAB\_ILFERP\_008 – E-Rezept durch Abgebenden zurückgeben**

|                |  |
|----------------|--|
| Name           | E-Rezept durch Abgebenden zurückgeben  |
| Auslöser       | <ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>  |
| Akteur         | Leistungserbringer, Mitarbeiter der abgebenden LEI   |
| Vorbedingung   | <ul style="list-style-type: none"> <li>Die LEI hat das E-Rezept vom E-Rezept-Fachdienst heruntergeladen und es befindet sich im Status "in Abgabe (gesperrt)".</li> <li>Der Nutzer hat ein E-Rezept zum Zurückgeben markiert und das Zurückgeben bestätigt.</li> <li>Die LEI hat sich gegenüber der TI authentisiert.</li> </ul> |
| Nachbedingung  | <ul style="list-style-type: none"> <li>Das ausgewählte E-Rezept hat auf dem E-Rezept-Fachdienst den Status "offen"</li> </ul>  |
| Standardablauf | <ol style="list-style-type: none"> <li>Task-ID und Geheimnis des E-Rezepts bestimmen</li> <li>E-Rezept Status auf Fachdienst ändern</li> <li>E-Rezept und E-Rezept-Token in PS löschen</li> </ol>  |

1126 [**<=**]

1127 A\_19250 - PS abgebende LEI: E-Rezept zurückgeben - Statusrequest  
1128 Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept durch Abgebenden  
1129 zurückgeben" für das zurückzugebende E-Rezept die HTTP-Operation **POST**  
1130 `/Task/<id>/$reject` mit

1131 

- ACCESS\_TOKEN im Authorization-Header

1132 

- Task-ID in URL `<id>`

1133 

- Geheimnis in URL-Parameter `?secret=`

1134 ausführen.[<=]

1135 Für weitere Informationen siehe Operation "Ein E-Rezept zurückweisen" aus der API-  
1136 Schnittstelle [E-Rezept API Dokumentation].

1137 A\_19251 - PS abgebende LEI: E-Rezept zurückgeben - E-Rezept löschen  
1138 Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept durch Abgebenden  
1139 zurückgeben" für das zurückzugebende E-Rezept nach erfolgreichem Aufruf der  
1140 Operation "Ein E-Rezept zurückweisen" die Daten zum E-Rezept, E-Rezept-Token und das  
1141 Geheimnis im PS löschen.[<=]

### 1142 **5.3.5 E-Rezept löschen**

1143 Mit diesem Anwendungsfall kann die abgebende LEI ein E-Rezept, welches auf dem E-  
1144 Rezept-Fachdienst gespeichert ist, löschen, z.B. wenn ein Fehler an der Verordnung  
1145 gefunden wurde, der sich nur durch das Ausstellen eines neuen E-Rezepts durch die  
1146 verordnende LEI beheben lässt.

1147 A\_19241 - PS abgebende LEI: E-Rezepte löschen - E-Rezept auswählen  
1148 Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept zum  
1149 Löschen auf dem Fachdienst auszuwählen.[<=]

1150 A\_19242 - PS abgebende LEI: E-Rezept löschen - Bestätigung  
1151 Das PS der abgebenden LEI MUSS vom Nutzer eine Bestätigung einholen, dass das  
1152 ausgewählte E-Rezept gelöscht werden soll, und die Möglichkeit geben, das  
1153 Löschen abzuberechnen.[<=]

1154 A\_19243 - PS abgebende LEI: E-Rezept durch Abgebenden löschen  
1155 Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.3 - E-Rezept durch  
1156 Abgebenden löschen" aus [gemSysL\_eRp] gemäß TAB\_ILFERP\_009 umsetzen.

#### 1157 **Tabelle 11 : TAB\_ILFERP\_009 – E-Rezept durch Abgebenden löschen**

|                |  |
|----------------|--|
| Name           | E-Rezept durch Abgebenden löschen  |
| Auslöser       | <ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>  |
| Akteur         | Leistungserbringer, Mitarbeiter der abgebenden LEI   |
| Vorbedingung   | <ul style="list-style-type: none"> <li>Die LEI hat das E-Rezept vom E-Rezept-Fachdienst heruntergeladen.</li> <li>Der Nutzer hat ein E-Rezept zum Löschen markiert und das Löschen bestätigt.</li> <li>Die LEI hat sich gegenüber der TI authentisiert.</li> </ul> |
| Nachbedingung  | <ul style="list-style-type: none"> <li>Das ausgewählte E-Rezept ist vom E-Rezept-Fachdienst unwiederbringlich gelöscht.</li> </ul>   |
| Standardablauf | <ol style="list-style-type: none"> <li>Task-ID und Geheimnis des E-Rezepts bestimmen</li> <li>E-Rezept auf Fachdienst löschen</li> <li>E-Rezept-Token in PS löschen</li> </ol>   |

1158 [<=]



1159 A\_19244 - PS abgebende LEI: E-Rezept löschen - Löschrequest  
1160 Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept durch Abgebenden  
1161 löschen" für das zu löschende E-Rezept die HTTP-Operation `POST /Task/<id>/$abort` mit

- 1162 • `ACCESS_TOKEN` im Authorization-Header
- 1163 • Task-ID in URL `<id>`
- 1164 • Geheimnis in URL Parameter `?secret=`

1165 ausführen. [`<=>`]

1166 Für weitere Informationen siehe Operation "Ein E-Rezept löschen" aus der API-  
1167 Schnittstelle [E-Rezept API Dokumentation].

1168 A\_19245 - PS abgebende LEI: E-Rezept löschen - E-Rezept-Token löschen  
1169 Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept durch Abgebenden  
1170 löschen" für das zu löschende E-Rezept nach erfolgreichem Aufruf der Operation "Ein E-  
1171 Rezept löschen" die Daten zum E-Rezept-Token und das Geheimnis im PS löschen. [`<=>`]

### 1172 **5.3.6 Nachrichten von Versicherten empfangen**

1173 Mit diesem Anwendungsfall kann die abgebende LEI den Token eines E-Rezepts  
1174 empfangen, um es zu beliefern. Darüber hinaus kann es Nachrichten des Versicherten,  
1175 wie z.B. Anfragen zur Belieferung durch eine Apotheke, empfangen.

1176

1177 A\_21556 - PS abgebende LEI: Häufigkeit des Abrufen von Nachrichten  
1178 Das PS der abgebenden LEI MUSS im Anwendungsfall "Nachrichten von Versicherten  
1179 empfangen" zwischen den Aufrufen der Operation `GET /Communication` mindestens 5  
1180 Minuten warten. Der Zeitraum zwischen den Aufrufen muss um eine zufällige Zeitspanne  
1181 zwischen 0 und 10000 Millisekunden verlängert werden, um eine Gleichverteilung der  
1182 Anfragen am E-Rezept-Fachdienst über alle Apotheken zu erreichen. [`<=>`]

1183 A\_19328 - PS abgebende LEI: Nachrichten von Versicherten empfangen  
1184 Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.6 - Nachrichten durch  
1185 Abgebenden empfangen" aus [gemSysL\_eRp] gemäß TAB\_ILFERP\_010 umsetzen.

1186 **Tabelle 12 : TAB\_ILFERP\_010 – Nachrichten von Versicherten empfangen**

|               |  |
|---------------|--|
| Name          | Nachrichten von Versicherten empfangen   |
| Auslöser      | <ul style="list-style-type: none"><li>• Aufruf des Anwendungsfalls in der GUI</li><li>• periodische Abfrage durch das PS</li></ul>   |
| Akteur        | Leistungserbringer, Mitarbeiter der abgebenden LEI   |
| Vorbedingung  | <ul style="list-style-type: none"><li>• Die LEI hat sich gegenüber der TI authentisiert.</li></ul>   |
| Nachbedingung | <ul style="list-style-type: none"><li>• Die auf dem E-Rezept-Fachdienst für die abgebende LEI hinterlegten Communication Ressourcen wurden übertragen. Die E-Rezept-Nachrichten stehen im PS bereit.</li></ul> |



|                |  |
|----------------|--|
| Standardablauf | <ol style="list-style-type: none"><li>1. E-Rezept-Nachrichten am Fachdienst abrufen</li><li>2. Mitteilung und E-Rezept-Token extrahieren</li></ol> |
|----------------|--|

1187 [`<=`]

1188

1189 [A\\_19329-01 - PS abgebende LEI: Nachrichten empfangen - Abfragerequest](#)

1190 ~~[A\\_19329 - PS abgebende LEI: Nachrichten empfangen - Löschanfrage](#)~~

1191 Das PS der abgebenden LEI MUSS im Anwendungsfall "Nachrichten von Versicherten  
1192 empfangen" die HTTP-Operation `GET /Communication` mit

- 1193
- `ACCESS_TOKEN` im Authorization-Header
  - 1194 • optional: `?received=null` für nur ungelesene Nachrichten
  - 1195 • optional: `?received=gtYYYY-MM-DD` für Nachrichten nach Datum DD.MM.YYY

1196 ausführen. [`<=`]

1197 Für weitere Informationen siehe Operationen "Anwendungsfall auf neue Nachrichten  
1198 prüfen" und "Anwendungsfall Alle Nachrichten vom E-Rezept-Fachdienst abrufen" aus  
1199 der API-Schnittstelle [E-Rezept API Dokumentation].

1200 Falls eine oder mehrere E-Rezept-Nachrichten für die abgebende LEI auf dem Fachdienst  
1201 bereitstehen, übermittelt der Fachdienst ein Bundle von `Communication` Ressourcen.

1202 Eine `Communication` Ressource kann unterschiedlichen Typs sein und beinhaltet  
1203 typabhängige, fachliche Informationen:

- 1204
- Absender-ID (Versicherten-ID) für die Korrespondenz möglicher  
1205 Antwortnachrichten
  - 1206 • Nachrichten-ID, um auf eine konkrete Nachricht zu antworten
  - 1207 • unverbindliche Anfrage zur Belieferung durch eine Apotheke
  - 1208 • Informationen zum verordneten bzw. angefragten Medikament als Medication-  
1209 Ressource
  - 1210 • Anzahl der Packungen des verordneten bzw. angefragten Medikamentes
  - 1211 • IK-Nummer des begünstigten Versicherten (unabhängig von der Versicherten-  
1212 ID, da auch Vertreter Anfragen zur Belieferung durch eine Apotheke stellen  
1213 können)
  - 1214 • Aut-Idem-Feld entsprechend der Festlegung im E-Rezept-Datensatz
  - 1215 • Rezepttyp als Wert des Flowtypes im Task des E-Rezept-Workflows
  - 1216 • optional: bevorzugte Belieferungsoptionen ["Apotheke", "Bote", "Versand"]  
1217 des Versicherten
  - 1218 • optional: Mitteilung/Text
  - 1219 • verbindlicher Einlöseauftrag
  - 1220 • Referenz auf den aktiven E-Rezept-Task inkl. Zugriffsberechtigung (E-Rezept-  
1221 Token), über den sämtliche einlöserrelevanten Informationen beziehbar sind
  - 1222 • optional: Mitteilung/Text

Wenn die Nachricht einen E-Rezept-Token enthält, dann hat der Versicherte das E-Rezept der Apotheke zugewiesen. Mit den Informationen aus dem E-Rezept-Token kann das E-Rezept vom Fachdienst abgerufen (Anwendungsfall "E-Rezept abrufen") und beliefert werden.

Wenn die Nachricht Informationen zum verordneten Mittel und keinen E-Rezept-Token enthält, dann kann die Information entsprechend der Mitteilung des Versicherten (bspw. Anfrage zur Belieferung durch eine Apotheke) verarbeitet werden.

Die unverbindliche Anfrage zur Belieferung wird mit dem Start des E-Rezepts am 01.07.2021 noch nicht unterstützt.

Der verbindliche Einlöseauftrag wird mit dem Start des E-Rezepts am 01.07.2021 die optionale Mitteilung/Text als Freitext für den Versicherten nicht unterstützt. Anstelle des im Freitext zu definierenden Belieferungswunsches werden Informationen zum Belieferungswunsch in der folgenden JSON Struktur in Communication.payload übermittelt.

Für payload wird folgende strukturierte Übermittlung vorgesehen

```
{
  "version": "1",
  "supplyOptionsType": "delivery",
  "name": "Dr. Maximilian von Muster",
  "address": [ "wohnhaft bei Emilia Fischer", "Bundesallee 312", "123.
OG", "12345 Berlin" ],
  "hint": "Bitte im Morsecode klingeln: -.-.",
  "phone": "004916094858168"
}
```

**Tabelle 13 : TAB\_ILFERP\_015 – Nachricht von Versicherten empfangen - payload**

| Attribut                 | mandatory/optional | Bedeutung   |
|--------------------------|--------------------|---|
| <u>version</u>           | <u>mandatory</u>   | <u>immer 1</u>  |
| <u>supplyOptionsType</u> | <u>mandatory</u>   | <u>Valide Inhalte: "onPremise", "delivery", "shipment"</u>  |
| <u>name</u>              | <u>mandatory</u>   | <u>"onPremise": Name des Versicherten laut Rezept</u><br><u>"delivery"/"shipment": Name des Lieferungsempfänger</u>       |
| <u>address</u>           | <u>mandatory</u>   | <u>"onPremise": Adresse des Versicherten laut Rezept</u><br><u>"delivery"/"shipment": Adresse des Lieferungsempfänger</u> |

|              |                 |   |
|--------------|-----------------|---|
|              |                 | <u>mindestens: Strasse+Hausnummer, PLZ+Ort werden gesetzt</u>                         |
| <u>hint</u>  | <u>optional</u> | <u>nur bei "delivery":<br/>Hinweise zur Belieferung<br/>Freitext, max. 90 Zeichen</u> |
| <u>phone</u> | <u>optional</u> | <u>immer bei "delivery",<br/>internationales Format</u>                               |

### 5.3.7 Nachricht an Versicherten versenden

Mit diesem Anwendungsfall kann die abgebende LEI auf Nachrichten eines Versicherten antworten, z.B. um mitzuteilen, ob das E-Rezept durch die Apotheke beliefert werden kann oder wann die Arzneimittel zur Abholung bereitstehen.

A\_19330 - PS abgebende LEI: Nachricht versenden - E-Rezept auswählen  
Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, eine E-Rezept-Nachricht auszuwählen, um eine Antwort zu senden.【<=】

A\_19331 - PS abgebende LEI: Nachricht versenden - Mitteilung erfassen  
Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, für eine E-Rezept-Nachricht an einen Versicherten eine Textnachricht zu erfassen.【<=】

~~Innerhalb der Textnachricht sind keine Internet-Links zulässig.~~

Wickelt die abgebende LEI ein E-Rezept über einen Onlineshop ab, kann dem Versicherten das Weiterbearbeiten seines Warenkorbs in einer externen Bestellplattform (z.B. Versandadresse, Zuzahlung) ermöglicht werden. Hierzu erlaubt der E-Rezept-Fachdienst den Versand einer Warenkorb-URL in der Nachricht an den Versicherten.

A\_21373 - PS abgebende LEI: Nachricht versenden - Externe URL ausschließlich für Einlösung

~~**A\_20012 - E-Rezept-FdV: E-Rezept zuweisen - Textnachricht ohne Link**~~  
Das PS der abgebenden LEI MUSS ~~prüfen~~prüfen, dass die Einbettung einer externen URL ausschließlich für das Einlösen von E-Rezepten in einer externen Bestellplattform genutzt wird.【<=durch den Nutzer erfasste Textnachricht keinen Internet-Link enthält, und die Textnachricht nur bei erfolgreicher Prüfung weiterverarbeiten.【<=】

Für die Nutzerführung im E-Rezept-FdV ist es wichtig zu erkennen, ob es sich um eine automatisierte Antwort oder bspw. die Bitte um Rückruf handelt. Hierfür kann optional das Feld Communication.topic verwendet werden. Es kommen die Werte des Standard-Codesystems <https://www.hl7.org/fhir/codesystem-communication-topic.html> zur Anwendung.

Der Nachricht an den Versicherten kann

A\_19332 - PS abgebende LEI: Nachricht an Versicherten versenden

1284 Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.7 - Nachricht durch  
1285 Abgebenden übermitteln" aus [gemSysL\_eRp] gemäß TAB\_ILFERP\_011 umsetzen.

1286 **Tabelle 14 : TAB\_ILFERP\_011 – Nachricht an Versicherten versenden**

|                |   |
|----------------|---|
| Name           | Nachricht an Versicherten versenden   |
| Auslöser       | <ul style="list-style-type: none"> <li>Aufruf des Anwendungsfalls in der GUI</li> </ul>   |
| Akteur         | Leistungserbringer, Mitarbeiter der abgebenden LEI  |
| Vorbedingung   | <ul style="list-style-type: none"> <li>Die LEI hat eine E-Rezept-Nachricht vom E-Rezept-Fachdienst heruntergeladen.</li> <li>Der Nutzer hat eine Mitteilung als Antwort auf die Nachricht erfasst.</li> <li>Die LEI hat sich gegenüber der TI authentisiert.</li> </ul> |
| Nachbedingung  | <ul style="list-style-type: none"> <li>Auf dem E-Rezept-Fachdienst steht eine E-Rezept-Nachricht für den Versicherten bereit.</li> </ul>  |
| Standardablauf | <ol style="list-style-type: none"> <li>Versicherten-ID aus der Nachricht des Versicherten bestimmen</li> <li>Communication Ressource erstellen</li> <li>E-Rezept-Nachricht auf Fachdienst einstellen</li> </ol>   |

1287 [`<=`]

1288 Als ID des Empfängers wird die Versicherten-ID des Absenders aus der empfangenen E-  
1289 Rezept-Nachricht verwendet.

1290 A\_19333-01A\_19333 - PS abgebende LEI: Nachricht versenden - Communication  
1291 Ressource erstellen

1292 Das PS der abgebenden LEI MUSS im Anwendungsfall "Nachricht an Versicherten  
1293 versenden" eine `Communication` Ressource mit

1294 

- Versicherten-ID des Absenders der empfangenen Nachricht in `recipient`

1295 

- Task-ID des referenzierten E-Rezeptes in `basedOn`

1296 

- Nachrichten-ID der empfangenen Anfrage in `inResponseTo` (optional)

1297 

- Textnachricht in `payload contentString`

1298 Die Textnachricht kann optional eine externe URL enthalten.

1299 

- optional: verfügbare Belieferungsoptionen ["Apotheke", "Bote", "Versand"] der  
1300 Apotheke

1301 

- optional: Verfügbarkeitsstatus gemäß ValueSet 'AvailabilityStatusVS' [10, 20, ..., 90]

1303 

- optional: Communication.topic mit Code gemäß  
1304 <https://www.hl7.org/fhir/codesystem-communication-topic.html> zur  
1305 Kennzeichnung des Inhalts ("phone-consult", o.ä.)

1306 erstellen. [`<=`]

1307 Für die Spezifikation der `Communication` Ressource siehe [gemSpec\_DM\_eRp].

Die unverbindliche Anfrage zur Belieferung wird mit dem Start des E-Rezepts am 01.07.2021 noch nicht unterstützt. Aus dem Grund wird die Attribute verfügbare Belieferungsoptionen, Verfügbarkeitsstatus und Communication.topic nicht durch das E-Rezept-FdV ausgewertet.

Für payload wird folgende strukturierte Übermittlung vorgesehen

```
{
  "version": "1",
  "supplyOptionsType": "onPremise",
  "info_text": "Wir möchten Sie informieren, dass Ihre bestellten Medikamente zur Abholung bereitstehen. Den Abholcode finden Sie anbei.",
  "pickUpCodeHR": "12341234",
  "pickUpCodeDMC": "",
  "url": ""
}
```

Es können folgende Fälle abgewickelt werden:

- Zustellung + Anzeige eines Freitextes
- Zustellung + Anzeige eines menschenlesbaren Abholcodes \*
- Zustellung + Anzeige eines maschinenlesbaren Abholcodes \*
- Zustellung + Anzeige einer URL für den Absprung in einen Warenkorb

\* nicht garantiert zum 01.07.2021.

**Tabelle 15 : TAB\_ILFERP\_016 – Nachricht an Versicherten versenden - payload**

| <u>Attribut</u>          | <u>mandatory/optional</u> | <u>Bedeutung</u>  |
|--------------------------|---------------------------|---|
| <u>version</u>           | <u>mandatory</u>          | <u>immer 1</u>  |
| <u>supplyOptionsType</u> | <u>mandatory</u>          | <u>Der supplyOptionsType, der bei der Zuweisung durch den Versicherten übergeben wurde, wird hier wiederholt. Valide Inhalte: "onPremise", "delivery", "shipment".</u>                        |
| <u>info_text</u>         | <u>optional</u>           | <u>Freitext, maximal 400 Zeichen</u>  |
| <u>url</u>               | <u>optional</u>           | <u>Nur bei supplyOptionsType "shipment". Wenn gesetzt, wird dem Versicherten ein Button angezeigt, der einen Absprung auf die hinterlegte URL in den Browser des Betriebssystems auslöst.</u> |

|                                      |                                 |   |
|--------------------------------------|---------------------------------|---|
| <u><a href="#">pickUpCodeHR</a></u>  | <u><a href="#">optional</a></u> | <u><a href="#">Nur bei supplyOptionsType "onPremise". Wenn gesetzt, wird dem Nutzer der Inhalt des "pickUpCodeHR" optisch hervorgehoben angezeigt. Maximale Länge 8 Zeichen.</a></u>  |
| <u><a href="#">pickUpCodeDMC</a></u> | <u><a href="#">optional</a></u> | <u><a href="#">Nur bei supplyOptionsType "onPremise". Wenn gesetzt, kann sich der Nutzer den Inhalt als Data-Matrix-Code anzeigen lassen. Der Inhalt wird gemäß ISO/IEC 16022:2006 in einen DMC gewandelt. Fehlt die Interpretation, so wird der Code als Freitext angezeigt.</a></u> |

A\_19334 - PS abgebende LEI: Nachricht versenden - Nachricht auf Fachdienst einstellen  
Das PS der abgebenden LEI MUSS im Anwendungsfall "Nachricht an Versicherten versenden" die HTTP-Operation POST /Communication mit

- ACCESS\_TOKEN im Authorization-Header
- Communication Ressource im HTTP-Request-Body

ausführen. [ <= ]

Für weitere Informationen siehe Operationen "Anwendungsfall Nachricht als Apotheke an einen Versicherten schicken" aus der API-Schnittstelle [E-Rezept API Dokumentation].

### **5.3.8 Dispensierdatensatz Nachricht löschen**

[Mit diesem Anwendungsfall kann die abgebende LEI von ihr versendete Nachrichten an einen Versicherten auf dem E-Rezept-Fachdienst löschen.](#)

[A\\_21486 - PS abgebende LEI: Nachricht löschen - Nachricht auswählen](#)  
[Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, eine Nachricht zum Löschen auf dem Fachdienst auszuwählen. \[ <= \]](#)

[A\\_21487 - PS abgebende LEI: Nachricht löschen - Bestätigung](#)  
[Das PS der abgebenden LEI MUSS vom Nutzer eine Bestätigung einholen, dass die ausgewählte Nachricht gelöscht werden soll, und die Möglichkeit geben, das Löschen abzubrechen. \[ <= \]](#)

[A\\_21488 - PS abgebende LEI: Nachricht durch Abgebenden löschen](#)  
[Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.9 - Nachricht durch Abgebenden löschen" aus \[gemSysL\\_eRp\] gemäß TAB ILFERP 013 umsetzen.](#)

#### **Tabelle 16 : TAB ILFERP 013 – Nachricht durch Abgebenden löschen**

|                                 |  |
|---------------------------------|--|
| <u><a href="#">Name</a></u>     | <u><a href="#">Nachricht durch Abgebenden löschen</a></u>  |
| <u><a href="#">Auslöser</a></u> | <ul style="list-style-type: none"> <li>• <u><a href="#">Aufruf des Anwendungsfalls in der GUI</a></u></li> </ul> |

|                       |  |
|-----------------------|--|
| <u>Akteur</u>         | <u>Leistungserbringer, Mitarbeiter der abgebenden LEI</u>  |
| <u>Vorbedingung</u>   | <ul style="list-style-type: none"> <li>• <u>Der Nutzer hat eine Nachricht zum Löschen markiert und das Löschen bestätigt.</u></li> <li>• <u>Die LEI hat sich gegenüber der TI authentisiert.</u></li> </ul>    |
| <u>Nachbedingung</u>  | <ul style="list-style-type: none"> <li>• <u>Die ausgewählte Nachricht ist vom E-Rezept-Fachdienst unwiederbringlich gelöscht.</u></li> </ul>   |
| <u>Standardablauf</u> | <ol style="list-style-type: none"> <li>1. <u>ID der Communication Ressource bestimmen</u></li> <li>2. <u>Nachricht auf Fachdienst löschen</u></li> <li>3. <u>Nachricht in PS löschen (optional)</u></li> </ol> |

**[<=]**

A 21489 - PS abgebende LEI: Nachricht löschen - Löschrequest  
Das PS der abgebenden LEI MUSS im Anwendungsfall "Nachricht durch Abgebenden löschen" für die zu löschende Nachricht die HTTP-Operation **DELETE**  
/Communication/<id> mit

- ACCESS TOKEN im Authorization-Header
- Communication-ID in URL <id>

ausführen. [<=]

Der E-Rezept-Fachdienst prüft anhand der Telematik-ID im ACCESS TOKEN, ob die LEI der Absender der zu löschenden Nachricht ist.

Wenn die Nachricht bereits vom Versicherten abgerufen wurde, dann wird im Response des E-Rezept-Fachdienstes im HTTP-Header eine Warnung mit dem Zeitpunkt des Abrufes übermittelt.

Für weitere Informationen siehe API-Schnittstelle [E-Rezept API Dokumentation].

A 21490 - PS abgebende LEI: Nachricht löschen - Nachricht im PS löschen  
Das PS der abgebenden LEI KANN im Anwendungsfall "Nachricht durch Abgebenden löschen" dem Nutzer ermöglichen, die Nachricht auch lokal im PS zu löschen. [<=]

Hinweis: Nachrichten an Versicherte sind immer an E-Rezept-Workflows gebunden. Wenn ein E-Rezept-Workflow, bspw. durch den Versicherten oder aufgrund von durch den E-Rezept-Fachdienst durchgesetzte Löschrufen, auf dem E-Rezept-Fachdienst gelöscht wird, dann werden auch alle zugehörigen Nachrichten gelöscht.

### **5.3.85.3.9 Abgabedatensatz signieren**

Nach der Belieferung eines E-Rezepts erstellt das PS der abgebenden LEI einen DispensierdatensatzAbgabedatensatz, welcher zusammen mit dem E-Rezept-Bundle und der Quittung für die Abrechnung des E-Rezepts verwendet wird.

Die Inhalte und die Struktur des DispensierdatensatzesAbgabedatensatzes werden durch DAV und GKV-SV vorgegeben.

Die Definition erfolgt in Form von FHIR-Profilen. Der DispensierdatensatzDatensatz selbst sollte zur Vereinfachung der Verarbeitung in Folgeprozessen in Analogie der KBV-Festlegungen im XML-Format (anstelle von bspw. JSON) dargestellt sein.



Der Abgabedatensatz dient der Abrechnung. Demgegenüber stehen die Dispensierinformationen der MedicationDispense-Ressource für den Versicherten (vgl. Abschnitt 5.3.2).

Für die Signatur des Dispensierdatensatzes/Abgabedatensatzes wird der Konnektor verwendet.

A 21619 - PS abgebenden LEI: Abgabedatensatz signieren  
Das PS der abgebenden LEI MUSS beim Signieren des Abgabedatensatzes die Signaturoperation des Konnektors mit

- eingebetteter OCSP-Antwort (IncludeRevocationInfo = true)

ausführen. [ <= ]

A 21244-01 - PS abgebende LEI: Abgabedatensatz signieren - Signaturverfahren

~~A\_21244 - PS abgebende LEI: Dispensierdatensatz signieren - Signaturverfahren~~

Das PS der abgebenden LEI MUSS die Signatur des Dispensierdatensatzes/Abgabedatensatzes mittels Einzelsignatur, Stapelsignatur und Komfortsignatur unterstützen. - [ <= ]

### **5.3.95.3.10 2D-Code einscannen**

Eine Alternative zur Übermittlung eines E-Rezept-Token vom Versicherten mittels E-Rezept-Nachricht ist die persönliche Übergabe in der Apotheke vor Ort. Hierzu übergibt der Kunde (Versicherter oder Vertreter) dem Mitarbeiter der abgebenden LEI einen Papiausdruck mit 2D-Code oder präsentiert einen 2D-Code auf dem Display seines mobilen Gerätes. Ebenso besteht die Möglichkeit, dass ein Versicherter den Papiausdruck eines E-Rezept-Tokens an eine Versandapotheke sendet. Der 2D-Code wird eingescannt.

A\_19629 - PS abgebende LEI: 2D-Code Scanner

Das PS der abgebenden LEI MUSS einen 2D-Code Scanner für Datamatrix Code unterstützen. [ <= ]

A\_19630 - PS abgebende LEI: 2D-Code scannen

Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, einen 2D-Code für E-Rezepte einzuscannen. [ <= ]

Der 2D-Code auf einem durch eine verordnende LEI erstellten Ausdruck enthält genau den E-Rezept-Token für ein E-Rezept. Der Versicherte kann in seinem E-Rezept-FdV bis zu 3 E-Rezept-Token in einem 2D-Code zusammenfassen. Dies dient einer besseren Usability.

A\_19631 - PS abgebende LEI: 2D-Code scannen - E-Rezept-Token extrahieren

Das PS der abgebenden LEI MUSS den oder die E-Rezept-Token aus einem eingescannten Datamatrix Code extrahieren. [ <= ]

Für den Aufbau des 2D-Codes und Struktur des E-Rezept-Token siehe [gemSpec\_DM\_eRp].

Mit den Informationen aus einem E-Rezept-Token kann das E-Rezept vom E-Rezept-Fachdienst heruntergeladen werden.

1428 **5.4 Fehlerbehandlung**

- 1429 Tritt ein Fehler bei der Verarbeitung von Operationsaufrufen an einem Dienst der TI  
1430 (bspw. E-Rezept-Fachdienst) auf, dann antwortet der Dienst mit einer Fehlermeldung.  
1431 Das Format und die verwendeten Fehlercodes sind in den Spezifikationen der Interfaces  
1432 (bspw. [gemSpec\_FD\_eRp]) beschrieben. Weiterhin können Fehler in der lokalen  
1433 Verarbeitung auftreten.
- 1434 A\_20152 - PS: Verständliche Fehlermeldung  
1435 Das PS MUSS im Falle von Fehlern Fehlermeldungen bereitstellen, die es den Mitarbeitern  
1436 der Leistungserbringerinstitution ermöglichen, die Ursache des Fehlers zu identifizieren  
1437 und mögliche Gegenmaßnahmen zu ergreifen. [≤]

## 6 Informationsmodell

Dienste der TI:

| Datenfeld                              | Herkunft                 | Beschreibung                |
|--|--------------------------|-----------------------------|
| E-Rezept-Fachdienst:<br>FQDN, Port     | DNS-Abfrage am Konnektor | Lokalisierungsinformationen |
| Identity Provider:<br>FQDN, Port, Path | DNS-Abfrage am Konnektor | Lokalisierungsinformationen |

Authentisierung

| Datenfeld | Herkunft   | Beschreibung |
|-----------|--|--------------|
| client_id | Organisatorischer Prozess zur Registrierung beim IDP |              |
|           |  |              |

Session-Daten

| Datenfeld          | Herkunft | Beschreibung   |
|--------------------|----------|--|
| ACCESS_TOKEN       | IDP      | Authentisierungs-Token für den Zugriff auf Dienste der TI  |
| ID_TOKEN           | IDP      | zur Befüllung der Claims für neu ausgestellte ACCESS_TOKEN während einer aktiven Session durch den IDP, ohne dass der IDP das Zertifikat neu authentifizieren muss |
| AUTHORIZATION_CODE | IDP      | Code für den Bezug eines ID_TOKENS und ACCESS_TOKENS nach einer erfolgreichen Authentifizierung zwischen Authenticator-Funktion im Client und dem IDP              |

**für PS verordnende LEI**

E-Rezept:

| Datenfeld | Herkunft | Beschreibung |
|-----------|----------|--------------|
|-----------|----------|--------------|

|                 |   |   |
|-----------------|---|---|
| Task            | E-Rezept-Fachdienst (POST<br>/Task/\$create)  | <a href="https://simplifier.net/erezept-workflow/gemerxtask">https://simplifier.net/erezept-workflow/gemerxtask</a>                     |
| E-Rezept-ID     | Task.identifizier<br>mit NamingSystem<br>"PrescriptionID"<br>E-Rezept-ID (POST<br>/Task/\$create) | <a href="https://simplifier.net/erezept-workflow/gemerxprescriptionid">https://simplifier.net/erezept-workflow/gemerxprescriptionid</a> |
| Task-ID         | E-Rezept-Fachdienst (POST<br>/Task/\$create)  | <a href="https://hl7.org/fhir/http.html">https://hl7.org/fhir/http.html</a>   |
| AccessCode      | E-Rezept-ID (POST<br>/Task/\$create)  | <a href="https://simplifier.net/erezept-workflow/accesscode">https://simplifier.net/erezept-workflow/accesscode</a>                     |
| E-Rezept-Bundle | Verordnungsdatenschnittstell<br>e oder durch PS erstellt  | <a href="https://simplifier.net/erezept/kbvprerpbundle">https://simplifier.net/erezept/kbvprerpbundle</a>                               |

1448

1449 **für PS abgebende LEI:**

1450 E-Rezept:

| Datenfeld   | Herkunft   | Beschreibung  |
|-------------|--|---|
| Task        | E-Rezept-Fachdienst (POST<br>/Task/<id>/\$accept)  | <a href="https://simplifier.net/erezept-workflow/gemerxtask">https://simplifier.net/erezept-workflow/gemerxtask</a>                     |
| E-Rezept-ID | E-Rezept-Fachdienst (POST<br>/Task/<id>/\$accept)<br>Task.identifizier<br>mit NamingSystem<br>"PrescriptionID" | <a href="https://simplifier.net/erezept-workflow/gemerxprescriptionid">https://simplifier.net/erezept-workflow/gemerxprescriptionid</a> |
| Task-ID     | E-Rezept-Token<br>2D-Code<br>scannen oder E-Rezept-Nachricht<br>(GET<br>/Communication)                        | <a href="https://hl7.org/fhir/http.html">https://hl7.org/fhir/http.html</a>   |
| AccessCode  | E-Rezept-Token<br>2D-Code<br>scannen oder E-   | <a href="https://simplifier.net/erezept-workflow/accesscode">https://simplifier.net/erezept-workflow/accesscode</a>                     |

|                      |   |  |
|----------------------|---|--|
|                      | Rezept-Nachricht (GET /Communication)   |  |
| Secret               | E-Rezept-Fachdienst (POST /Task/<id>/\$accept)  | <a href="https://simplifier.net/erezept-workflow/secret">https://simplifier.net/erezept-workflow/secret</a>  |
| E-Rezept-Bundle      | Enveloping in QES-Datensatz enthalten<br>E-Rezept-Fachdienst (POST /Task/<id>/\$accept) | <a href="https://simplifier.net/erezept/kbvprerpbundle">https://simplifier.net/erezept/kbvprerpbundle</a>  |
| E-Rezept-Nachrichten | E-Rezept-Fachdienst (GET /Communication)  | Anfrage Belieferung durch eine Apotheke:<br><a href="https://gematik.de/fhir/StructureDefinition/erxCommunicationInfoReq">https://gematik.de/fhir/StructureDefinition/erxCommunicationInfoReq</a><br>Einlöseauftrag:<br><a href="https://gematik.de/fhir/StructureDefinition/erxCommunicationDispReq">https://gematik.de/fhir/StructureDefinition/erxCommunicationDispReq</a><br>Antwort der Apotheke:<br><a href="https://gematik.de/fhir/StructureDefinition/erxCommunicationReply">https://gematik.de/fhir/StructureDefinition/erxCommunicationReply</a><br><br><a href="https://simplifier.net/erezept-workflow/gemerxcommunication">https://simplifier.net/erezept-workflow/gemerxcommunication</a> |
| Chargeninformation   | Securpharm-Scan   | Befüllung des Feldes <b>Medication.batch</b> im Profil <a href="https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Medication_PZN">https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Medication_PZN</a><br>wenn Fertigarzneimittel, die einen Data-Matrix-Code gemäß securPharm-System besitzen, dispensiert werden   |
| MedicationDispense   | durch PS erstellt   | <a href="https://simplifier.net/erezept-workflow/gemerxmedicationdispense">https://simplifier.net/erezept-workflow/gemerxmedicationdispense</a>  |

1451

## 7 Anhang A – Verzeichnisse

1452

### 7.1 Abkürzungen

| Kürzel     | Erläuterung                                    |
|------------|--|
| API        | application programming interface              |
| BMV        | Bundesmantelvertrag                            |
| DD         | Discovery Document                             |
| <u>DMC</u> | <u>Data-Matrix-Code</u>                        |
| FdV        | Frontend des Versicherten                      |
| FHIR       | Fast Healthcare Interoperable Resources        |
| HTTP       | Hypertext Transfer Protocol                    |
| IDP        | Identity Provider                              |
| JWT        | JSON Web Token                                 |
| KBV        | Kassenärztliche Bundesvereinigung              |
| KVNR       | Krankenversichertennummer                      |
| LE         | Leistungserbringer                             |
| LEI        | Leistungserbringerinstitution                  |
| PS         | Primärsystem                                   |
| PUK        | Öffentlicher Schlüssel                         |
| QES        | Qualifizierte Elektronische Signatur           |
| TLS        | Transport Layer Security                       |
| SMC-B      | Security Module Card Typ B, Institutionenkarte |
| UC         | Use Case                                       |

|     |                                       |
|-----|---------------------------------------|
| VAU | Vertrauenswürdige Ausführungsumgebung |
|-----|---------------------------------------|

## 1453 7.2 Glossar

| Begriff            | Erläuterung  |
|--------------------|--|
| E-Rezept-Bundle    | Ein E-Rezept-Bundle ist eine Bundle-FHIR-Ressource gemäß der Profilierung <a href="https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle">https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle</a> . Sie wird durch das PS der verordnenden LEI erstellt.   |
| Funktionsmerkmal   | Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.  |
| MedicationDispense | Ein MedicationDispense ist eine FHIR-Ressource gemäß der Profilierung <a href="https://gematik.de/fhir/StructureDefinition/erxMedicationDispense">https://gematik.de/fhir/StructureDefinition/erxMedicationDispense</a> . Sie wird durch das PS der abgebenden LEI erstellt und beinhaltet Informationen zum abgegebenen Mittel. Ein Versicherter, welcher ein E-Rezept-FdV nutzt, kann auf die MedicationDispense-Information zu seinen E-Rezepten zugreifen. |
| Task               | Ein Task ist eine Task FHIR-Ressource gemäß der Profilierung <a href="https://gematik.de/fhir/StructureDefinition/erxTask">https://gematik.de/fhir/StructureDefinition/erxTask</a> . Sie beinhaltet die Metadaten zum Workflow eines E-Rezepts sowie die Informationen zum E-Rezept (u.a. E-Rezept-Bundle).  |
| Versicherten-ID    | Die Versicherten-ID ist der 10-stellige unveränderliche Teil der Krankenversichertennummer (KVNR).   |

1454 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung  
1455 gestellt.

## 1456 7.3 Abbildungsverzeichnis

|      |   |           |
|------|---|-----------|
| 1457 | <u>Abbildung 1 : ABB_ILFERP_001 – Systemzerlegung .....</u> | <u>7</u>  |
| 1458 | <u>Abbildung 2 : ABB_ILFERP_002 – Statusübergänge .....</u> | <u>11</u> |
| 1459 |   |           |

## 1460 7.4 Tabellenverzeichnis

|      |   |           |
|------|---|-----------|
| 1461 | <u>Tabelle 1 : TAB_ILFERP_001 – E-Rezept-Status .....</u>                       | <u>9</u>  |
| 1462 | <u>Tabelle 2 : TAB_ILFERP_014 - HTTP-Header "X-erp-resource" .....</u>          | <u>16</u> |
| 1463 | <u>Tabelle 3 TAB_ILFERP_012 – Zertifikatsnutzung .....</u>                      | <u>17</u> |
| 1464 | <u>Tabelle 4 : TAB_ILFERP_002 – E-Rezept durch Verordnenden erstellen .....</u> | <u>28</u> |



|      |  |    |
|------|--|----|
| 1465 | <a href="#">Tabelle 5 : TAB ILFERP 003 – E-Rezept durch Verordnenden einstellen.....</a>           | 30 |
| 1466 | <a href="#">Tabelle 6 : TAB ILFERP 004 – E-Rezept durch Verordnenden löschen.....</a>              | 32 |
| 1467 | <a href="#">Tabelle 7 : TAB ILFERP 005 – E-Rezept abrufen .....</a>                                | 33 |
| 1468 | <a href="#">Tabelle 8 : TAB ILFERP 006 – Quittung abrufen .....</a>                                | 35 |
| 1469 | <a href="#">Tabelle 9 : TAB ILFERP 007 – Quittung erneut abrufen .....</a>                         | 37 |
| 1470 | <a href="#">Tabelle 10 : TAB ILFERP 008 – E-Rezept durch Abgebenden zurückgeben .....</a>          | 38 |
| 1471 | <a href="#">Tabelle 11 : TAB ILFERP 009 – E-Rezept durch Abgebenden löschen .....</a>              | 39 |
| 1472 | <a href="#">Tabelle 12 : TAB ILFERP 010 – Nachrichten von Versicherten empfangen.....</a>          | 40 |
| 1473 | <a href="#">Tabelle 13 : TAB ILFERP 015 – Nachricht von Versicherten empfangen - payload .....</a> | 42 |
| 1474 | <a href="#">Tabelle 14 : TAB ILFERP 011 – Nachricht an Versicherten versenden.....</a>             | 44 |
| 1475 | <a href="#">Tabelle 15 : TAB ILFERP 016 – Nachricht an Versicherten versenden - payload.....</a>   | 45 |
| 1476 | <a href="#">Tabelle 16 : TAB ILFERP 013 – Nachricht durch Abgebenden löschen.....</a>              | 46 |
| 1477 |  |    |

## 1478 7.5 Referenzierte Dokumente

### 1479 7.5.1 Dokumente der gematik

1480 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument  
 1481 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der  
 1482 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und  
 1483 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und  
 1484 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht  
 1485 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der  
 1486 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die  
 1487 vorliegende Version aufgeführt wird.

1488

| [Quelle]                     | Herausgeber: Titel   |
|------------------------------|--|
| [E-Rezept API Dokumentation] | gematik: <a href="https://github.com/gematik/api-erp/tree/4.0.0-Pre2">https://github.com/gematik/api-erp/tree/4.0.0-Pre2</a><br>gematik: <a href="https://github.com/gematik/api-erp">https://github.com/gematik/api-erp</a> |
| [gemGlossar]                 | gematik: Einführung der Gesundheitskarte – Glossar   |
| [gemILF_PS]                  | gematik: Implementierungsleitfaden Primärsysteme - Telematikinfrastruktur (TI)   |
| [gemKPT_eRp]                 | gematik: Konzept E-Rezept  |
| [gemKPT_SysL_TI]             | gematik: Systemdesign der Telematikinfrastruktur - Release 4.0   |

|                        |   |
|------------------------|---|
| [gemSpec_DM_eRp]       | gematik: Spezifikation Datenmodell E-Rezept   |
| [gemSpec_FD_eRp]       | gematik: Spezifikation E-Rezept-Fachdienst  |
| [gemSpec_IDP_Dienst]   | gematik: Spezifikation Identity Provider – Dienst   |
| [gemSpec_IDP_Frontend] | gematik: Spezifikation Identity Provider – Frontend   |
| [gemSpec_Kon]          | gematik: Spezifikation Konnektor  |
| [gemSpec_Krypt]        | gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur |
| [gemSpec_OID]          | gematik: Spezifikation Festlegung von OIDs  |
| [gemSysL_eRp]          | gematik: Systemspezifisches Konzept E-Rezept  |

## 1489 7.5.2 Weitere Dokumente

| [Quelle]     | Herausgeber (Erscheinungsdatum): Titel  |
|--------------|---|
| [BMV]        | Bundesmantelvertrag Ärzte<br><a href="https://www.kbv.de/html/bundesmantelvertrag.php">https://www.kbv.de/html/bundesmantelvertrag.php</a>  |
| [BMV-Z]      | Bundesmantelvertrag - Zahnärzte<br><a href="https://www.kzbv.de/bundesmantelvertrag.1223.de.html">https://www.kzbv.de/bundesmantelvertrag.1223.de.html</a>  |
| [ExpBack]    | Exponential Backoff<br><a href="https://en.wikipedia.org/wiki/Exponential_backoff">https://en.wikipedia.org/wiki/Exponential_backoff</a>  |
| [OASIS-VR]   | OASIS: Profile for comprehensive multi-signature verification reports for OASIS Digital Signature Services Version 1.0, Committee Specification 01, 12 November 2010, <a href="http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf">http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf</a> |
| [RFC7231]    | Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content<br><a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a>  |
| [SecurPharm] | Inhalte und Struktur SecurPharm-Codes<br><a href="http://www.securpharm.de/wp-content/uploads/2018/08/securPharm_Codierung_Regeln_DE_V2_03.pdf">http://www.securpharm.de/wp-content/uploads/2018/08/securPharm_Codierung_Regeln_DE_V2_03.pdf</a><br>Kapitel 5.2.3 und 5.2.4 für Chargeninformation + Verfallsdatum  |
| [Split-DNS]  | Split-horizon DNS<br><a href="https://en.wikipedia.org/wiki/Split-horizon_DNS">https://en.wikipedia.org/wiki/Split-horizon_DNS</a>  |

1490