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.~~1~~2.0 CC
Revision:	~~294971~~304510
Stand:	09.12.~~11.~~2020
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./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.06.20		freigegeben	gematik
1.0.1	06.07.20		Aktualisierung Hinweis zu Dispensierinformation	gematik
1.1.0	12.11.20		Einarbeitung gemäß Änderungsliste P22.2 / Scope-Themen Systemdesign R4.0.1	gematik
1.2.0 CC	09.12.20		Einarbeitung gemäß Änderungsliste P22.5	gematik

Inhaltsverzeichnis

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].

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

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

1.5.1 Hinweis auf offene Punkte

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

Beispiel für einen offenen Punkt.

2 Systemüberblick

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

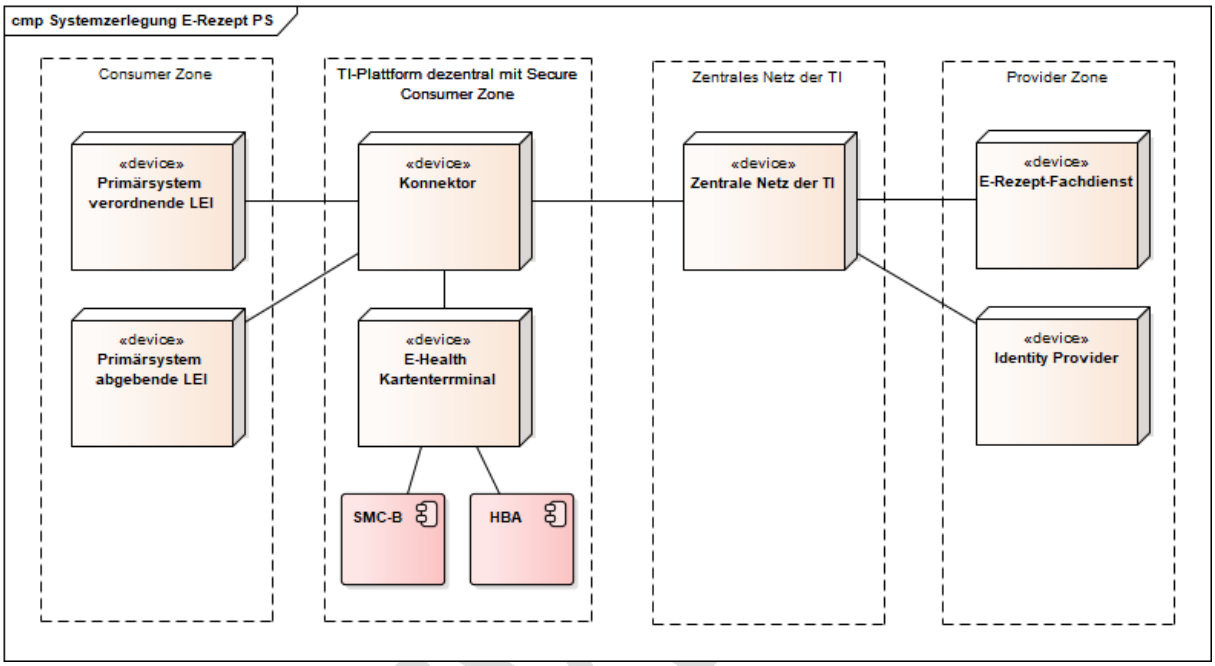

Abbildung 1 : ABB_ILFERP_001 – Systemzerlegung

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

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

214 Für die Signatur des E-Rezepts bzw. des Dispensierdatensatzes wird die CMS-Signatur
215 (CAdES) des Konnektors genutzt.

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

217 **E-Rezept-Fachdienst**

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

220 # 3 Systemkontext

221 ## 3.1 E-Rezept Status

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

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

226 TAB_ILFERP_001 listet die möglichen Status.

227 **Tabelle 1 : TAB_ILFERP_001 – E-Rezept-Status**

E-Rezept Status	Task Status	Beschreibung
initialisiert	draft	• Beim Abruf der Rezept-ID durch eine verordnende LEI wird die FHIR-Ressource Task im E-Rezept-Fachdienst im Zustand "draft" erstellt. • Die verordnende LEI kann das QES-signierte E-Rezept in der erstellten Ressource hinzufügen. Der Task wechselt dann in den Status "ready".
offen	ready	• Der QES-signierte Verordnungsdatensatz wurde von einer verordnenden LEI in den E-Rezept-Fachdienst eingestellt. Der Task wurde vom Fachdienst aktiviert. • Der Task kann vom Versicherten bzw. seinem Vertreter abgerufen werden. • Der Task kann von der verordnenden LEI oder dem Versicherten als gelöscht markiert werden. Der Task wechselt dann in den Status "cancelled". • Der Abruf einer abgebenden LEI ändert den Status des Tasks auf "in-progress". Dieser sperrt den Zugriff durch andere abgebende LEI.
in Abgabe (gesperrt)	in-progress	• Der Task wurde von einer abgebenden LEI abgerufen. • Der Zugriff durch andere abgebende LEI oder die verordnende LEI ist gesperrt. Ebenso darf der Versicherte Tasks in diesem Zustand nicht löschen. • Der Task kann durch die abgebende LEI zurückgewiesen werden und wechselt dann zurück in den Status "ready". • Die abgebende LEI kann die Quittung abrufen. Dann wechselt der Task in den Status "completed".

		• Der Task kann durch die abgebende LEI als gelöscht markiert werden und wechselt dann in den Status "cancelled". • Der Task kann vom Versicherten bzw. seinem Vertreter weiterhin eingesehen werden (read only).
quittiert	completed	• Die Quittung für das E-Rezept wurde durch die abgebende LEI abgerufen. Der Task ist beendet. • Der Task kann vom Versicherten bzw. seinem Vertreter abgerufen werden. • Der Task kann durch den Versicherten gelöscht werden und wechselt dann in den Status "cancelled". • Eine Reaktivierung des Tasks ist nicht möglich.
gelöscht	cancelled	• Die personenbezogenen und medizinischen Daten wurden aus dem Task gelöscht. • Die Akteure können nicht auf den Task zugreifen.

Die Abbildung ABB_ILFERP_002 zeigt die Anwendungsfälle, welche zu Statusübergängen führen.

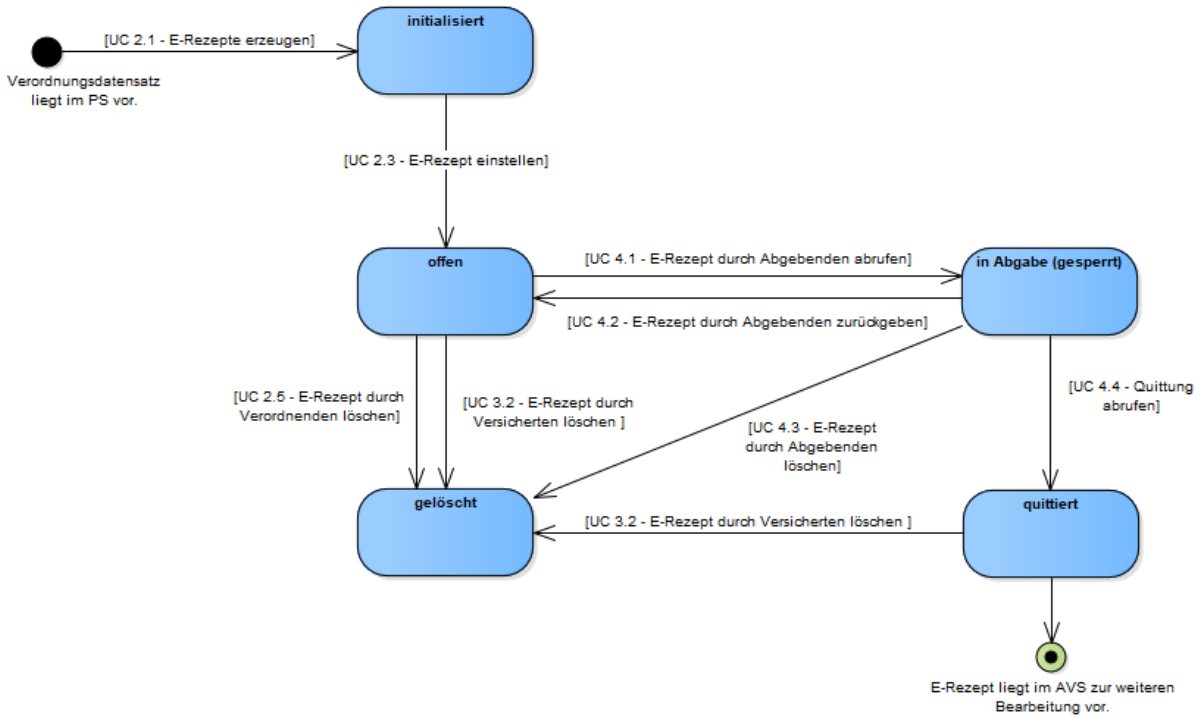

Abbildung 2 : ABB_ILFERP_002 – Statusübergänge

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.

4 Übergreifende Festlegungen

4.1 Logging und Meldungen

A_20088 - PS: Schreiben eines Fehlerprotokolls
Das Primärsystem SOLL alle in der Kommunikation mit den Diensten der TI auftretenden Fehler und Warnungen in ein dediziertes Fehlerprotokoll schreiben und diese Protokollinformationen für Supportmaßnahmen über eine Zeitraum von mindestens 14 Tagen zur Verfügung halten.**[<=]**

A_20089 - PS: Anzeige von Meldungen
Das Primärsystem SOLL alle in der Kommunikation mit den Diensten der TI auftretenden Probleme für den Benutzer verständlich anzeigen und dabei erkennen lassen, ob durch den Anwender oder den verantwortlichen Leistungserbringer Maßnahmen zur Behebung eingeleitet werden müssen.**[<=]**

A_20884 - PS: Exponential Backoff bei Verbindungsfehlern
Das Primärsystem SOLL bei serverseitigen Fehlermeldungen, die auf eine Überlastung des Zielsystems schließen lassen (z.B. http-status 5xx, 429 - too many requests, etc.), erneute Verbindungsversuche nach dem Prinzips des Exponential Backoffs [ExpBack] durchführen.**[<=]**

4.2 Namensauflösung

Der E-Rezept-Fachdienst ist für Primärsysteme gemäß der Festlegungen in [gemSpec_FD_eRp] über die Adresse erp.zentral.erp.splitdns.ti-dienste.de lokalisierbar. Das Redundanzkonzept sieht mehrere Instanzen vor, die über verschiedene IP-Adressen angesprochen werden. Folglich liefert die DNS-Namensauflösung 4 verschiedene IP-Adressen zum FQDN zurück. Diese 4 Adressen werden vom DNS-Server in zufälliger Reihenfolge geschickt, sodass es legitim ist, immer den ersten Eintrag für den folgenden Operationsaufruf zu verwenden. Üblicherweise wird die DNS-Auflösung vom Betriebsystem gekapselt, eine Lastverteilung am E-Rezept-Fachdienst ergibt sich aus der zufälligen Reihenfolge der IP-Adressen der DNS-Abfrage.

Unspezifiziert ist das Verhalten, wenn die erste Zieladresse nicht erreichbar ist. Empfehlenswert ist die Nutzung der 2., 3. bzw. 4. IP-Adresse der DNS-Abfrage. Es muss aber angenommen werden, dass bestimmte Betriebssysteme bzw. Laufzeitumgebungen des Primärsystems diese mit der Nutzung der ersten Adresse bereits verworfen haben. Bei Nicht-Erreichbarkeit des Zielhosts der ersten IP-Adresse wird daher empfohlen, weitere Verbindungsversuche auf Basis einer neuen DNS-Abfrage zu tätigen, mit dem Ziel, eine andere IP-Adresse an erster Stelle der DNS-Antwort zu erhalten, als die des nicht erreichbaren Zielhosts.

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 - PS: Lokalisierung E-Rezept-Fachdienst
Das Primärsystem MUSS die zur Kommunikation mit dem E-Rezept-Fachdienst notwendigen Lokalisierungsinformationen per DNS-Abfrage nach den in [gemSpec_FD_eRP#Tab_eRP_Service Discovery] und [gemSpec_FD_eRP#Tab_eRP_FQDN] dargestellten Parametern ermitteln.**[<=]**

Die Abfrage beim Namensdienst der TI erfolgt über eine DNS-Abfrage beim Konnektor. Der Konnektor bietet hierzu eine Operation GetIPAddress für das PS an. Siehe TIP1-A_5035 - Operation GetIPAddress in [gemSpec_KON]. Liefert die DNS-Abfrage mehrere Ziel-IP-Adressen, so ist es hilfreich, eine zufällig auszuwählen, um Lastspitzen in den einzelnen Zielsystemen zu reduzieren.

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 - PS: HTTP-Header user-agent
Das Primärsystem MUSS in alle HTTP-Requests an den E-Rezept-Fachdienst und den IDP-Dienst den HTTP-Header user-agent gemäß [RFC7231] befüllen.**[<=]**

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] .

5.1.3 Zertifikatsprüfung

Das Primärsystem der verordnenden und abgebenden LEI verwendet bei den in TAB_ILFERP_012 dargestellten Aktivitäten Zertifikate.

Tabelle 2 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:	ja	C.FD.SIG	oid_erezept	aktiv

Signaturzertifikat Fachdienst				

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.**[<=]**

"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.

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].

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. **[<=]**

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. **[<=]**

A_20656 - Prüfung der CMS Signatur des Discovery Document
Das Primärsystem MUSS die Signatur des Discovery Document mittels "VerifyDocument" Funktion des Konnektor gemäß [gemSpec_Kon#4.1.8.5.2] bzw. [gemILF_PS#4.4.3] auf mathematische Korrektheit sowie auf Gültigkeit des ausstellenden Zertifikates innerhalb der TI prüfen. **[<=]**

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

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.**[<=]**

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.**[<=]**

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

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_VERFIER" 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] / "-" / "." / "_" / "~".**[**<=**]**

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)))**[**<=**]**

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".
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":"sLlxlkskAyuzdDOwe8nZeeQVFBWgscNkRcpgHmKidFc"
}
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":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpPU0UrSlNPTiIsImlhdCI6MTU5MTcxNDI1MjMy.....",
  "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 - Prüfung der Signatur des CHALLENGE_TOKEN
Das Primärsystem MUSS die Signatur des "CHALLENGE_TOKEN" gegen den aktuellen öffentlichen Schlüssel des Authorization-Endpunktes "PUK_AUTH" 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 Discovery Document abrufen.**[<=]**

Das Primärsystem verwendet nun die AUT-Identität der SM-B der LEI und deren Konnektor, um die 256-Bit "challenge" 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 - Signatur der Challenge des IDP-Dienstes
Das Primärsystem MUSS für das Signieren der "challenge" des IDP-Dienstes mit der Identität ID.HCI.OSIG 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 in Base64-Codierung übergeben. **[<=]**

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

A_20666 - Auslesen des Authentisierungszertifikates
Das Primärsystem MUSS das Zertifikat ID.HCI.OSIG 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 - 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_AUTH" verschlüsselt, an diesen in Form eines HTTP-signed_challengecPOST-Requests senden.**[<=]**

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=eyJhbGciOiJFUzI1NiIsInR5cCI6IkpPU0UrSlNPTiIsIng.....
```

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 prüft ihn.

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_20669 - Formale Prüfung der Signatur des AUTHORIZATION_CODE
Das Primärsystem MUSS die Signatur des AUTHORIZATION_CODE mathematisch prüfen und auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID oid_idpd zurückführen können.**[<=]**

Zur Prüfung von Zertifikatstyp-OID und Rollen-OID siehe Hinweis zu A_20657.

A_20670 - Gültigkeitsprüfung der Signatur des AUTHORIZATION_CODE innerhalb der TI
Das Primärsystem MUSS das zur Signatur des AUTHORIZATION_CODE verwendete Zertifikat über die Funktion "VerifyCertificate" des Konnektors gemäß [gemSpec_Kon#4.1.9.5.3] bzw. [gemILF_PS#4.4.4.3] auf Gültigkeit innerhalb der TI prüfen.**[<=]**

Anschließend werden der zu Beginn des Prozesses erzeugte "CODE_VERFIER" und der "AUTHORIZATION_CODE" zum Token-Endpunkt des IDP-Dienstes gesendet, um dort gegen "ID_TOKEN" und "ACCESS_TOKEN" eingetauscht zu werden

A_20671 - Einreichen des AUTHORIZATION_CODE beim Token-Endpunkt
Das Primärsystem MUSS den "AUTHORIZATION_CODE" zusammen mit dem "code_verifier" TLS-gesichert an den Token-Endpunkt URI_TOKEN als HTTP/1.1 GET Request übertragen.**[<=]**

Hinweis: Der folgende Aufruf skizziert beispielhaft den HTTP-POST-Request an den Token-Endpunkt. Der mitgegebene "AUTHORIZATION_CODE" wird dabei nur angedeutet:

```
POST /token HTTP/1.1
Host: idp.com
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code
&code=eyJhbGciOiJkaXIiLCJlbmMiOiJBMjU2R0NNIiwiZXhwIjoxNTkx.....
```

&redirect_uri=https%3A%2F%2Fapp.erezept.com%2Fauthnres
&code_verifier=MApN61C4itdm4-58dCjMkoucuu00jipPlNibsAxjyJk

Der Token-Endpunkt validiert den "CODE_VERFIER" und gleicht diesen mit der "code_challenge" ab. Dann erzeugt er die erforderlichen Token und verschlüsselt das "ACCESS_TOKEN" für den empfangenden Fachdienst.

Das Primärsystem erhält nun den signierten "ID_TOKEN"und den für es nicht lesbaren "ACCESS_TOKEN" vom Token-Endpunkt und prüft die Signatur des "ID_TOKEN".

A_20672 - Annahme des ID_TOKEN
Das Primärsystem MUSS das vom Token-Endpunkt ausgegebene "ID_TOKEN" als HTTP/1.1 Statusmeldung 200 verarbeiten. Das Primärsystem MUSS das "ID_TOKEN" ablehnen, wenn dieses außerhalb der mit dem Token-Endpunkt etablierten TLS-Verbindung übertragen wird.**[**<=**]**

A_20673 - Annahme des "ACCESS_TOKEN"
Das Primärsystem MUSS das vom Token-Endpunkt ausgegebene "ACCESS_TOKEN" in der HTTP/1.1 Statusmeldung 200 verarbeiten. Das Primärsystem MUSS das "ACCESS_TOKEN" ablehnen, wenn dieses außerhalb der mit dem Token-Endpunkt etablierten TLS-Verbindung übertragen wird.**[**<=**]**

Hinweis: Das Primärsystem nimmt sowohl den "ID_TOKEN" als auch den "ACCESS_TOKEN" aus der Antwort des Token-Endpunktes des IDP-Dienstes. Der Token-Endpunkt 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": "...",
}
```

A_20674 - Formale Prüfung der Signatur des ID_TOKEN
Das Primärsystem MUSS die Signatur des ID_TOKEN mathematisch prüfen und auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID "oid_idpd" zurückführen können.**[**<=**]**

Zur Prüfung von Zertifikatstyp- und Rollen-OID siehe Hinweis zu A_20657.

A_20675 - Gültigkeitsprüfung der Signatur des ID_TOKEN innerhalb der TI
Das Primärsystem MUSS das zur Signatur des ID_TOKEN verwendete Zertifikat über die Funktion „VerifyCertificate" des Konnektors gemäß [gemSpec_Kon#4.1.9.5.3] bzw. [gemILF_PS#4.4.4.3] auf Gültigkeit innerhalb der TI prüfen.**[**<=**]**

Im weiteren Verlauf kann der "ACCESS_TOKEN" innerhalb seiner Gültigkeitsdauer bei verschiedenen Aufrufen des Fachdienstes eingereicht werden. Der Fachdienst

entschlüsselt das "ACCESS_TOKEN" mit seinem privaten Schlüssel, validiert es, zieht die notwendigen Informationen entsprechend seinem Claim heraus und verwendet diese für seine fachlichen Operationen.

5.2 Anwendungsfälle verordnende LEI

Folgende Anwendungsfälle werden im Primärsystem einer verordnenden LEI umgesetzt.

5.2.1 E-Rezept erstellen

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

A_19274 - PS verordnende LEI: E-Rezept durch Verordnenden erstellen
Das PS der verordnenden LEI MUSS den Anwendungsfall "UC 2.1 - E-Rezepte erzeugen" aus [gemSysL_eRp] gemäß TAB_ILFERP_002 umsetzen.

Tabelle 3 : TAB_ILFERP_002 – E-Rezept durch Verordnenden erstellen

Name	E-Rezept durch Verordnenden erstellen
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter verordnende LEI
Vorbedingung	• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Im PS steht ein QES-Datensatz über den Verordnungsdatensatz des E-Rezept bereit.
Standardablauf	1. E-Rezept-ID von Fachdienst abrufen 2. E-Rezept-Bundle erstellen 3. Kanonisieren 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.Identifier` 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.Identifier` 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

- Rezept-ID aus der Task-Ressource als Identifier

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 - PS verordnende LEI: E-Rezept einstellen - E-Rezept-Bundle QES signieren
Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch Verordnenden erstellen" für das E-Rezept die Signaturoperation des Konnektors mit

- der Referenz RFC-5652 für CMS-Signatur (CAdES)
- Signaturtype für eine enveloping Signature
- dem base64-codierten E-Rezept-Bundle

ausführen.**[<=]**

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

Für die Nutzung der Komfortsignatur siehe [gemILF_PS].

5.2.2 E-Rezept einstellen

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

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

A_19272 - PS verordnende LEI: E-Rezept durch Verordnenden einstellen
Das PS der verordnenden LEI MUSS den Anwendungsfall "UC 2.3 - E-Rezept einstellen" aus [gemSysL_eRp] gemäß TAB_ILFERP_003 umsetzen.

Tabelle 4 : TAB_ILFERP_003 – E-Rezept durch Verordnenden einstellen

Name	E-Rezept durch Verordnenden einstellen
Auslöser	• Aufruf des Anwendungsfalls in der GUI • kann durch "E-Rezept durch Verordnenden erstellen" getriggert werden
Akteur	Leistungserbringer, Mitarbeiter verordnende LEI
Vorbedingung	• Das E-Rezept wurde erstellt. (Anwendungsfall "E-Rezept erstellen"). Es stehen ein QES-signiertes E-Rezept-Bundle als PKCS#7-Datei bereit. • Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Das E-Rezept ist auf dem E-Rezept-Fachdienst gespeichert. Es kann durch den Versicherten oder einen Apotheker in Kenntnis der Einlöseinformationen (Task-ID + AccessCode) abgerufen werden.
Standardablauf	1. Task auf dem E-Rezept-Fachdienst aktivieren 2. optional, wenn das E-Rezept ausgedruckt werden soll: a. E-Rezept-Token erzeugen b. E-Rezept-Ausdruck erstellen

[<=]

A_19273-01~~A_19273~~ - PS verordnende LEI: E-Rezept einstellen - Task auf Fachdienst aktivieren
Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch Verordnenden einstellen" für das E-Rezept die HTTP-Operation `POST /Task/<id>/$activate` mit

- ACCESS_TOKEN im Authorization-Header
- `Task-ID` in URL `<id>`
- AccessCode im `X-`~~Access-Code~~`AccessCode`-Header oder als URL-Parameter `?ac=`
- QES signiertes E-Rezept-Bundle im http-Body des Aufrufs als `data`

ausführen. **[<=]**

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

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

A_19279 - PS verordnende LEI: E-Rezept einstellen - E-Rezept-Token erstellen
Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch Verordnenden einstellen" einen E-Rezept-Token erstellen,wenn ein Ausdruck der Einlöseinformationen des E-Rezepts erstellt werden soll. **[<=]**

Für die Spezifikation des E-Rezept-Token siehe[gemSpec_DM_eRp#2.3].

A_19280 - PS verordnende LEI: E-Rezept einstellen - E-Rezept ausdrucken
Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch Verordnenden einstellen", wenn ein Ausdruck des E-Rezepts erstellt werden soll, den Datamatrix-Code für den E-Rezept-Token erstellen und diesen zusammen mit Zusatzinformationen ausdrucken.**[<=]**

Für die Spezifikation des Datamatrix-Code für E-Rezept-Token siehe[gemSpec_DM_eRp#2.3].

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

5.2.3 E-Rezept löschen

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

A_19236 - PS verordnende LEI: E-Rezepte löschen - E-Rezept zum Löschen auswählen
Das PS der verordnenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept zum Löschen auf dem Fachdienst auszuwählen.**[<=]**

A_19237 - PS verordnende LEI: E-Rezept löschen - Bestätigung
Das PS der verordnenden LEI MUSS vom Nutzer eine Bestätigung einholen, dass das ausgewählte E-Rezept gelöscht werden soll und die Möglichkeit geben, das Löschen abzubrechen.**[<=]**

A_19238 - PS verordnende LEI: E-Rezept durch Verordnenden löschen
Das PS der verordnenden LEI MUSS den Anwendungsfall "UC 2.5 - E-Rezept durch Verordnenden löschen" aus [gemSysL_eRp] gemäß TAB_ILFERP_004 umsetzen.

Tabelle 5 : TAB_ILFERP_004 – E-Rezept durch Verordnenden löschen

Name	E-Rezept durch Verordnenden löschen
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter verordnende LEI
Vorbedingung	• Der Nutzer hat ein E-Rezept zum Löschen markiert und das Löschen bestätigt. • Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Das ausgewählte E-Rezept ist vom E-Rezept-Fachdienst unwiederbringlich gelöscht.

Standardablauf	1. Task-ID und AccessCode des E-Rezepts bestimmen 2. E-Rezept auf E-Rezept-Fachdienst löschen 3. E-Rezept-Token in PS löschen

[<=]

A_19239-01~~A_19239~~ - PS verordnende LEI: E-Rezept löschen - Löschrequest
Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch Verordnenden löschen" für das zu löschende E-Rezept die HTTP-Operation `POST /TASK/<id>/$abort` mit

- ACCESS_TOKEN im Authorization-Header
- `Task-ID` in URL `<id>`
- AccessCode im `X-`~~Access-Code~~`AccessCode`-Header oder als URL-Parameter `?ac=`

ausführen. **[<=]**

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

A_19240 - PS verordnende LEI: E-Rezept löschen - E-Rezept-Token löschen
Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch Verordnenden löschen" für das zu löschende E-Rezept nach erfolgreichem Aufruf der Operation "Ein E-Rezept löschen" die Task-ID und den AccessCode im PS löschen.**[<=]**

5.3 Anwendungsfälle abgebende LEI

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 6 : TAB_ILFERP_005 – E-Rezept abrufen

Name	E-Rezept abrufen
Auslöser	• Aufruf des Anwendungsfalls in der GUI

Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	• Die LEI hat den E-Rezept-Token zum E-Rezept übermittelt bekommen. Der E-Rezept-Token steht im PS bereit. • Der Nutzer hat das E-Rezept zum Abruf markiert. • Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Das E-Rezept steht im PS bereit.
Standardablauf	1. Task-ID und AccessCode des E-Rezepts bestimmen 2. Task herunterladen 3. QES prüfen 4. Verordnung extrahieren 5. E-Rezept-Daten speichern

[<=]

A_19558-01~~A_19558~~ - 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 ~~in~~ `?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.**[**<=**]**

5.3.2 Quittung abrufen

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

A_19286 - PS abgebende LEI: Quittung abrufen - E-Rezept auswählen
Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept als abgegeben auszuwählen.**[**<=**]**

A_19287-01~~A_19287~~ - PS abgebende LEI: Quittung abrufen
Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.4 - Quittung abrufen" aus [gemSysL_eRp] gemäß TAB_ILFERP_006 umsetzen.

Tabelle 7 : TAB_ILFERP_006 – Quittung abrufen

Name	Quittung abrufen
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	• Die LEI hat das E-Rezept vom E-Rezept-Fachdienst heruntergeladen. • Der Nutzer hat ein E-Rezept als abgegeben markiert. • Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Die Quittung des E-Rezepts steht im PS bereit.

Standardablauf	1. Informationen über das abgegebene Medikament erstellen 2. nur für Fertigarzneimittel: Chargeninfo und Verfallsdatum ergänzen ~~2.~~3. Task-ID und Geheimnis des E-Rezepts bestimmen ~~3.~~4. E-Rezept-Status auf E-Rezept-Fachdienst ändern ~~4.~~5. Quittung aus Response extrahieren ~~5.~~6. optional: Signatur der Quittung prüfen

[<=]

A_19288 - PS abgebende LEI: Quittung - MedicationDispense erstellen
Das PS der abgebenden LEI MUSS im Anwendungsfall "Quittung abrufen" eine FHIR-Ressource `MedicationDispense` mit den Informationen über das abgegebene Medikament erstellen.**[<=]**

Für die Spezifikation der Ressource `MedicationDispense` siehe [gemSpec_DM_eRp]. Die Befüllung des Medication-Objekts der MedicationDispense kann in Abhängigkeit eines Austauschs aus der Übernahme der wesentlichen Attribute (PZN, Wirkstoff, Darreichungsform, Dosierinformationen) aus dem Verordnungsdatensatz und den Daten aus dem Securpharm-Scan in die MedicationDispense und Medication kopiert werden. Weitere Informationen, die sich aus dem Scan des Securpharm-Codes für Fertigarzneimittel ergeben (z.B. Charge, Haltbarkeitsdatum) und im Primärsystem vorliegen, können ebenfalls übernommen werden.

A_21105 - PS abgebende LEI: Chargeninfo in Medication ergänzen
Das PS der abgebenden LEI MUSS im Anwendungsfall "Quittung abrufen" die FHIR-Ressource "Medication" der erstellten MedicationDispense um Chargeninformation und Verfallsdatum aus dem SecurPharm-Scan [SecurPharm] ergänzen. **[<=]**

A_19289 - PS abgebende LEI: Quittung abrufen - Statusrequest
Das PS der abgebenden LEI MUSS im Anwendungsfall "Quittung abrufen" für das abgegebene E-Rezept die HTTP-Operation `POST /Task/<id>/$close` mit

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

ausführen.**[<=]**

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

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

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

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

A_20766 - PS abgebende LEI: Quittung - Quittungssignatur prüfen
Das PS der abgebenden LEI KANN im Anwendungsfall "Quittung abrufen" zum Prüfen der Quittung 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.**[<=]**

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].

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 8 : TAB_ILFERP_007 – Quittung erneut abrufen

Name	Quittung erneut abrufen
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	• Die LEI hat bereits mindestens einmal die Quittung abgerufen (Anwendungsfall "Quittung abrufen"). • Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Die Quittung zum E-Rezept steht im PS bereit.
Standardablauf	1. Task-ID und Geheimnis des E-Rezepts bestimmen 2. Quittung abrufen 3. Quittung aus Response extrahieren

[<=]

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.

5.3.4 E-Rezept zurückgeben

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

A_19246 - PS abgebende LEI: E-Rezepte zurückgeben - E-Rezept auswählen
Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept zum Zurückgeben auszuwählen.**[<=]**

A_19247 - PS abgebende LEI: E-Rezept zurückgeben - Bestätigung
Das PS der abgebenden LEI MUSS vom Nutzer eine Bestätigung einholen, dass das ausgewählte E-Rezept zurückgegeben werden soll und die Möglichkeit geben, das Zurückgeben abzubrechen.**[<=]**

A_19249 - PS abgebende LEI: E-Rezept durch Abgebenden zurückgeben
Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.2 - E-Rezept durch Abgebenden zurückgeben" aus [gemSysL_eRp] gemäß TAB_ILFERP_008 umsetzen.

Tabelle 9 : TAB_ILFERP_008 – E-Rezept durch Abgebenden zurückgeben

Name	E-Rezept durch Abgebenden zurückgeben
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	• Die LEI hat das E-Rezept vom E-Rezept-Fachdienst heruntergeladen und es befindet sich im Status "in Abgabe (gesperrt). • Der Nutzer hat ein E-Rezept zum Zurückgeben markiert und das Zurückgeben bestätigt. • Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Das ausgewählte E-Rezept hat auf dem E-Rezept-Fachdienst den Status "offen"

Standardablauf	1. Task-ID und Geheimnis des E-Rezepts bestimmen 2. E-Rezept Status auf Fachdienst ändern 3. E-Rezept und E-Rezept-Token in PS löschen

[<=]

A_19250 - PS abgebende LEI: E-Rezept zurückgeben - Statusrequest
Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept durch Abgebenden zurückgeben" für das zurückzugebende E-Rezept die HTTP-Operation `POST /Task/<id>/$reject` mit

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

ausführen.**[<=]**

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

A_19251 - PS abgebende LEI: E-Rezept zurückgeben - E-Rezept löschen
Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept durch Abgebenden zurückgeben" für das zurückzugebende E-Rezept nach erfolgreichem Aufruf der Operation "Ein E-Rezept zurückweisen" die Daten zum E-Rezept, E-Rezept-Token und das Geheimnis im PS löschen.**[<=]**

5.3.5 E-Rezept löschen

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

A_19241 - PS abgebende LEI: E-Rezepte löschen - E-Rezept auswählen
Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept zum Löschen auf dem Fachdienst auszuwählen.**[<=]**

A_19242 - PS abgebende LEI: E-Rezept löschen - Bestätigung
Das PS der abgebenden LEI MUSS vom Nutzer eine Bestätigung einholen, dass das ausgewählte E-Rezept gelöscht werden soll, und die Möglichkeit geben, das Löschen abzubrechen.**[<=]**

A_19243 - PS abgebende LEI: E-Rezept durch Abgebenden löschen
Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.3 - E-Rezept durch Abgebenden löschen" aus [gemSysL_eRp] gemäß TAB_ILFERP_009 umsetzen.

Tabelle 10 : TAB_ILFERP_009 – E-Rezept durch Abgebenden löschen

Name	E-Rezept durch Abgebenden löschen
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI

Vorbedingung	• Die LEI hat das E-Rezept vom E-Rezept-Fachdienst heruntergeladen. • Der Nutzer hat ein E-Rezept zum Löschen markiert und das Löschen bestätigt. • Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Das ausgewählte E-Rezept ist vom E-Rezept-Fachdienst unwiederbringlich gelöscht.
Standardablauf	1. Task-ID und Geheimnis des E-Rezepts bestimmen 2. E-Rezept auf Fachdienst löschen 3. E-Rezept-Token in PS löschen

[<=]

A_19244 - PS abgebende LEI: E-Rezept löschen - Löschrequest
Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept durch Abgebenden löschen" für das zu löschende E-Rezept die HTTP-Operation `POST /Task/<id>/$abort` mit

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

ausführen.**[<=]**

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

A_19245 - PS abgebende LEI: E-Rezept löschen - E-Rezept-Token löschen
Das PS der abgebenden LEI MUSS im Anwendungsfall "E-Rezept durch Abgebenden löschen" für das zu löschende E-Rezept nach erfolgreichem Aufruf der Operation "Ein E-Rezept löschen" die Daten zum E-Rezept-Token und das Geheimnis im PS löschen.**[<=]**

5.3.6 Nachrichten von Versicherten empfangen

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

A_19328 - PS abgebende LEI: Nachrichten von Versicherten empfangen
Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.6 - Nachrichten durch Abgebenden empfangen" aus [gemSysL_eRp] gemäß TAB_ILFERP_010 umsetzen.

Tabelle 11 : TAB_ILFERP_010 – Nachrichten von Versicherten empfangen

Name	Nachrichten von Versicherten empfangen
Auslöser	• Aufruf des Anwendungsfalls in der GUI • periodische Abfrage durch das PS
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI

Vorbedingung	• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	• Die auf dem E-Rezept-Fachdienst für die abgebende LEI hinterlegten Communication Ressourcen wurden übertragen. Die E-Rezept-Nachrichten stehen im PS bereit.
Standardablauf	1. E-Rezept-Nachrichten am Fachdienst abrufen 2. Mitteilung und E-Rezept-Token extrahieren

[<=]

A_19329 - PS abgebende LEI: Nachrichten empfangen - Löschrequest
Das PS der abgebenden LEI MUSS im Anwendungsfall "Nachrichten von Versicherten empfangen" die HTTP-Operation`GET /Communication` mit

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

ausführen.**[<=]**

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

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

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

- Absender-ID (Versicherten-ID) für die Korrespondenz möglicher Antwortnachrichten
- Nachrichten-ID, um auf eine konkrete Nachricht zu antworten
- unverbindliche Anfrage zur Belieferung durch eine Apotheke
  - Informationen zum verordneten bzw. angefragten Medikament als Medication-Ressource
  - Anzahl der Packungen des verordneten bzw. angefragten Medikamentes
  - IK-Nummer des begünstigten Versicherten (unabhängig von der Versicherten-ID, da auch Vertreter Anfragen zur Belieferung durch eine Apotheke stellen können)
  - Aut-Idem-Feld entsprechend der Festlegung im E-Rezept-Datensatz
  - Rezepttyp als Wert des Flowtypes im Task des E-Rezept-Workflows
  - optional: bevorzugte Belieferungsoptionen ["Apotheke", "Bote", "Versand"] des Versicherten
  - optional: Mitteilung/Text

- verbindlicher Einlöseauftrag
  - Referenz auf den aktiven E-Rezept-Task inkl. Zugriffsberechtigung (E-Rezept-Token), über den sämtliche einlöserelevanten Informationen beziehbar sind
  - 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.

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.

A_20012 - E-Rezept-FdV: E-Rezept zuweisen - Textnachricht ohne Link
Das PS der abgebenden LEI MUSS prüfen, dass die durch den Nutzer erfasste Textnachricht keinen Internet-Link enthält, und die Textnachricht nur bei erfolgreicher Prüfung weiterverarbeiten.**[**<=**]**

A_19332 - PS abgebende LEI: Nachricht an Versicherten versenden
Das PS der abgebenden LEI MUSS den Anwendungsfall "UC 4.7 - Nachricht durch Abgebenden übermitteln" aus [gemSysL_eRp] gemäß TAB_ILFERP_011 umsetzen.

Tabelle 12 : TAB_ILFERP_011 – Nachricht an Versicherten versenden

Name	Nachricht an Versicherten versenden
Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	• Die LEI hat eine E-Rezept-Nachricht vom E-Rezept-Fachdienst heruntergeladen. • Der Nutzer hat eine Mitteilung als Antwort auf die Nachricht erfasst. • Die LEI hat sich gegenüber der TI authentisiert.

Nachbedingung	• Auf dem E-Rezept-Fachdienst steht eine E-Rezept-Nachricht für den Versicherten bereit.
Standardablauf	1. Versicherten-ID aus der Nachricht des Versicherten bestimmen 2. Communication Ressource erstellen 3. E-Rezept-Nachricht auf Fachdienst einstellen

[<=]

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

A_19333 - PS abgebende LEI: Nachricht versenden - Communication Ressource erstellen
Das PS der abgebenden LEI MUSS im Anwendungsfall "Nachricht an Versicherten versenden" eine`Communication` Ressource mit

- Versicherten-ID des Absenders der empfangenen Nachricht in `recipient`
- Nachrichten-ID der empfangenen Anfrage in `inResponseTo` (optional)
- Textnachricht in `payload contentString`
- optional: verfügbare Belieferungsoptionen ["Apotheke", "Bote", "Versand"] der Apotheke

erstellen.**[<=]**

Für die Spezifikation der `Communication` Ressource siehe [gemSpec_DM_eRp].

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 signieren

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

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

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

Für die Signatur des Dispensierdatensatzes wird der Konnektor verwendet.

5.3.9 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 Papierausdruck mit 2D-Code oder präsentiert einen 2D-Code auf dem Display seines mobilen Gerätes. Ebenso besteht die Möglichkeit, dass ein Versicherter den Papierausdruck 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.

5.4 Fehlerbehandlung

Tritt ein Fehler bei der Verarbeitung von Operationsaufrufen an einem Dienst der TI (bspw. E-Rezept-Fachdienst) auf, dann antwortet der Dienst mit einer Fehlermeldung. Das Format und die verwendeten Fehlercodes sind in den Spezifikationen der Interfaces (bspw. [gemSpec_FD_eRp]) beschrieben. Weiterhin können Fehler in der lokalen Verarbeitung auftreten.

A_20152 - PS: Verständliche Fehlermeldung
Das PS MUSS im Falle von Fehlern Fehlermeldungen bereitstellen, die es den Mitarbeitern der Leistungserbringerinstitution ermöglichen, die Ursache des Fehlers zu identifizieren und mögliche Gegenmaßnahmen zu ergreifen.**[<=]**

6 Informationsmodell

Dienste der TI:

Datenfeld	Herkunft	Beschreibung
E-Rezept-Fachdienst: FQDN, Port	DNS-Abfrage am Konnektor	Lokalisierunginformationen
Identity Provider: FQDN, Port, Path	DNS-Abfrage am Konnektor	Lokalisierunginformationen

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 /Task/$create`)	https://simplifier.net/erezept-workflow/gemerxtask

E-Rezept-ID	`Task.identifier` mit NamingSystem "PrescriptionID" E-Rezept-ID (`POST /Task/$create`)	https://simplifier.net/erezept-workflow/gemerxprescriptionid
Task-ID	E-Rezept-Fachdienst (`POST /Task/$create`)	https://hl7.org/fhir/http.html
AccessCode	E-Rezept-ID (`POST /Task/$create`)	https://simplifier.net/erezept-workflow/accesscode
E-Rezept-Bundle	Verordnungsdatenschnittstelle oder durch PS erstellt	https://simplifier.net/erezept/kbvprerpbundle

für PS abgebende LEI:

E-Rezept:

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

	/Communication)	
Secret	E-Rezept-Fachdienst (POST /Task/<id>/$accept)	https://simplifier.net/erezept-workflow/secret
E-Rezept-Bundle	Enveloping in QES-Datensatz enthalten E-Rezept-Fachdienst (POST /Task/<id>/$accept)	https://simplifier.net/erezept/kbvprerpbundle
E-Rezept-Nachrichten	E-Rezept-Fachdienst (GET /Communication)	Anfrage Belieferung durch eine Apotheke: https://gematik.de/fhir/StructureDefinition/erxCommunicationInfoReq Einlöseauftrag: https://gematik.de/fhir/StructureDefinition/erxCommunicationDispReq Antwort der Apotheke: https://gematik.de/fhir/StructureDefinition/erxCommunicationReply https://simplifier.net/erezept-workflow/gemerxcommunication
Chargeninformation	Securpharm-Scan	Befüllung des Feldes **Medication.batch** im Profil https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Medication_PZN wenn Fertigarzneimittel dispensiert werden
MedicationDispense	durch PS erstellt	https://simplifier.net/erezept-workflow/gemerxmedicationdispense

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

Kürzel	Erläuterung
API	application programming interface
BMV	Bundesmantelvertrag
DD	Discovery Document
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

7.2 Glossar

Begriff	Erläuterung
E-Rezept-Bundle	Ein E-Rezept-Bundle ist eine Bundle-FHIR-Ressource gemäß der Profilierung https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle. 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 https://gematik.de/fhir/StructureDefinition/erxMedicationDispense . 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 https://gematik.de/fhir/StructureDefinition/erxTask . 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).

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

7.3 Abbildungsverzeichnis

7.4 Tabellenverzeichnis

7.5 Referenzierte Dokumente

7.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[E-Rezept API Dokumentation]	gematik: https://github.com/gematik/api-erp/tree/4.0.0-Pre2

[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

7.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BMV]	Bundesmantelvertrag Ärzte https://www.kbv.de/html/bundesmantelvertrag.php
[BMV-Z]	Bundesmantelvertrag - Zahnärzte https://www.kzbv.de/bundesmantelvertrag.1223.de.html
[ExpBack]	Exponential Backoff https://en.wikipedia.org/wiki/Exponential_backoff
[OASIS-VR]	OASIS: Profile for comprehensive multi-signature verification reports for OASIS Digital Signature Services Version 1.0, Committee Specification 01, 12 November 2010, http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0- profiles-vr-cs01.pdf
[RFC7231]	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content https://tools.ietf.org/html/rfc7231

[SecurPharm]	Inhalte und Struktur SecurPharm-Codes http://www.securpharm.de/wp-content/uploads/2018/08/securPharm_Codierung_Regeln_DE_V2_03.pdf Kapitel 5.2.3 und 5.2.4 für Chargeninformation + Verfallsdatum

1247