

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation

Implementierungsleitfaden

Primärsysteme – E-Rezept

Version:	1.34.0
Revision:	410407483901
Stand:	07.10.202109.08.2022
Status:	freigegeben
Klassifizierung:	öffentlich
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	19.02.21		Einarbeitung gemäß Änderungsliste P22.5	gematik
1.3.0 RC 2	19.05.21		Einarbeitung gemäß Änderungslisten E-Rezept_Maintenance_21.1 und _21.2	gematik
1.3.0 RC 3	20.05.21		Einarbeitung gemäß Änderungseintrag C_10474, C_10718 Übermittlung einer URL durch eine Apotheke an einen Versicherten	gematik
1.3.0 RC 4	28.06.21	Kap. 5.3.7 Kap. 5.1.3.1	Übermittlung url für alle Belieferungsoptionen Übergangsregelung für alternative Zertifikatsprüfung	gematik
1.3.0	07.10.21		freigegeben	gematik
1.4.0	09.08.22	Kap. 5.2.1	Einarbeitung gemäß Änderungslisten E-Rezept_Maintenance_21.3, _21.4, _22.1 und _22.2; Einarbeitung gemF_eRp_MVO, gemF_eRp_PKV, gemF_eRp_WF_LE redaktionelle Änderung: Ersetzung des Wortes „einstellen“ durch das Wort	gematik

**Implementierungsleitfaden Primärsysteme -
E-Rezept Klicken Sie hier, um Text
einzugeben.**

			„erstellen“ in den Überschriften folgender Anforderungen: A_19276, A_19275, A_19281-* und A_21243	
--	--	--	---	--

Inhaltsverzeichnis

1 Einordnung des Dokumentes	7
1.1 Zielsetzung	7
1.2 Zielgruppe	7
1.3 Geltungsbereich	7
1.4 Abgrenzungen	7
1.5 Methodik	8
1.5.1 Hinweis auf offene Punkte	8
2 Systemüberblick	9
3 Systemkontext	11
3.1 E-Rezept Status	11
3.2 FHIR-Ressourcen	13
4 Übergreifende Festlegungen	14
4.1 Logging und Meldungen	14
4.2 Namensauflösung	14
5 Funktionsmerkmale	16
5.1 Allgemein	16
5.1.1 Kommunikation zu den Diensten der TI	16
5.1.2 Verschlüsselte Kommunikation zur VAU des E-Rezept-Fachdienstes	18
5.1.3 Zertifikatsprüfung	19
5.1.3.1 Zertifikatsprüfung von Zertifikaten der TI	19
5.1.3.2 Zertifikatsprüfung von Internet-Zertifikaten	20
5.1.4 Authentifizierung der LEI	21
5.1.4.1 Übergreifende Festlegungen zur Nutzung des IDP-Dienstes	22
5.1.4.2 Abruf von Token beim IDP-Dienst	23
5.2 Anwendungsfälle verordnende LEI	27
5.2.1 E-Rezept erstellen	27
5.2.2 E-Rezept einstellen	31
5.2.3 E-Rezept löschen	33
5.3 Anwendungsfälle abgebende LEI	34
5.3.1 E-Rezept abrufen	34
5.3.2 Quittung abrufen	36
5.3.3 Quittung erneut abrufen	39
5.3.4 E-Rezept zurückgeben	40
5.3.5 E-Rezept löschen	41
5.3.6 Nachrichten von Versicherten empfangen	42
5.3.7 Nachricht an Versicherten versenden	46
5.3.8 Nachricht löschen	49

5.3.9 Abgabedatensatz signieren.....	50
5.3.10 2D-Code einscannen.....	51
5.4 Fehlerbehandlung.....	63
6 Informationsmodell.....	64
7 Anhang A – Verzeichnisse.....	67
7.1 Abkürzungen.....	67
7.2 Glossar.....	68
7.3 Abbildungsverzeichnis.....	68
7.4 Tabellenverzeichnis.....	69
7.5 Referenzierte Dokumente.....	70
7.5.1 Dokumente der gematik.....	70
7.5.2 Weitere Dokumente.....	71
1 Einordnung des Dokumentes.....	7
1.1 Zielsetzung.....	7
1.2 Zielgruppe.....	7
1.3 Geltungsbereich.....	7
1.4 Abgrenzungen.....	7
1.5 Methodik.....	8
1.5.1 Hinweis auf offene Punkte.....	8
1.6 Fachliche und technische Konzepte.....	8
2 Systemüberblick.....	9
3 Systemkontext.....	11
3.1 E-Rezept Status.....	11
3.2 FHIR-Ressourcen.....	13
4 Übergreifende Festlegungen.....	14
4.1 Logging und Meldungen.....	14
4.2 Namensauflösung.....	14
5 Funktionsmerkmale.....	16
5.1 Allgemein.....	16
5.1.1 Kommunikation zu den Diensten der TI.....	16
5.1.2 Verschlüsselte Kommunikation zur VAU des E-Rezept-Fachdienstes.....	18
5.1.3 Zertifikatsprüfung.....	19
5.1.3.1 Zertifikatsprüfung von Zertifikaten der TI.....	19
5.1.3.2 Zertifikatsprüfung von Internet-Zertifikaten.....	20
5.1.4 Authentifizierung der LEI.....	21
5.1.4.1 Übergreifende Festlegungen zur Nutzung des IDP-Dienstes.....	22

5.1.4.2 Abruf von Token beim IDP-Dienst.....	23
5.2 Anwendungsfälle verordnende LEI	27
5.2.1 E-Rezept erstellen	27
5.2.1.1 E-Rezept erstellen - Workflow 200/209	30
5.2.1.2 E-Rezept erstellen - Mehrfachverordnung	30
5.2.2 E-Rezept einstellen	31
5.2.2.1 E-Rezept einstellen - Workflow 169	32
5.2.3 E-Rezept löschen	33
5.3 Anwendungsfälle abgebende LEI.....	34
5.3.1 E-Rezept abrufen	34
5.3.2 Quittung abrufen.....	36
5.3.3 Quittung erneut abrufen	39
5.3.4 E-Rezept zurückgeben	40
5.3.5 E-Rezept löschen	41
5.3.6 Nachrichten von Versicherten empfangen.....	42
5.3.7 Nachricht an Versicherten versenden	46
5.3.8 Nachricht löschen	49
5.3.9 Abgabedatensatz signieren	50
5.3.10 2D-Code einscannen	51
5.3.11 Rezept-Informationen von verordnenden LEI empfangen	52
5.3.12 Abrechnungsinformationen	52
5.3.12.1 Abrechnungsinformation bereitstellen	52
5.3.12.2 PKV-Abgabedatensatz ändern	54
5.3.12.3 Abrechnungsinformation abrufen	55
5.3.13 Subscription für neue Communication	56
5.4 E-Rezept-spezifische KIM-Messages.....	59
5.4.1 E-Rezept-spezifische KIM-Messages - Workflow 169 /209	59
5.5 Fehlerbehandlung.....	63
6 Informationsmodell	64
7 Anhang A – Verzeichnisse	67
7.1 Abkürzungen	67
7.2 Glossar	68
7.3 Abbildungsverzeichnis.....	68
7.4 Tabellenverzeichnis	69
7.5 Referenzierte Dokumente	70
7.5.1 Dokumente der gematik.....	70
7.5.2 Weitere Dokumente.....	71

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.

1.6 Fachliche und technische Konzepte

Die den in diesem Dokument beschriebenen Anwendungsfälle liegen folgende fachliche und technische Konzepte für ärztliche und zahnärztliche Verordnungen für apothekenpflichtige Arzneimittel zugrunde:

Tabelle 1 : TAB_ILFERP_018 – Fachliche und technische Konzepte

Workflowtyp / Rezepttyp	Workflow	Konzeptionelle Beschreibung
E-Rezept für GKV-Versicherte	160	[gemSysL_eRp]
Workflowsteuerung durch Leistungserbringer	169	[gemF_eRp_WF_LE]
E-Rezept für PKV-Versicherte	200, 209	[gemF_eRp_PKV]
Mehrfachverordnung	160, 169, 200, 209	[gemF_eRp_MVO]

2 Systemüberblick

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

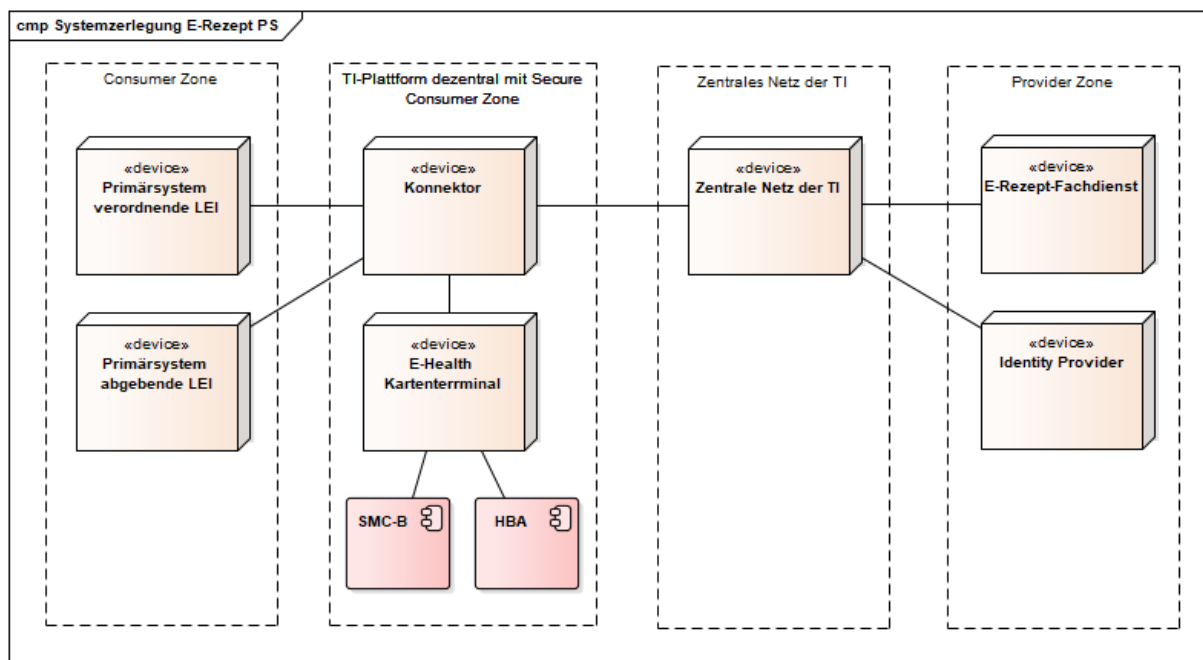


Abbildung 1 : ABB_ILFERP_001 – Systemzerlegung

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 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.

3 Systemkontext

3.1 E-Rezept Status

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

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

TAB_ILFERP_001 listet die möglichen Status.

Tabelle 2 : TAB_ILFERP_001 – E-Rezept-Status

E-Rezept Status	Task Status	Beschreibung
initialisiert	draft	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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".

		<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.

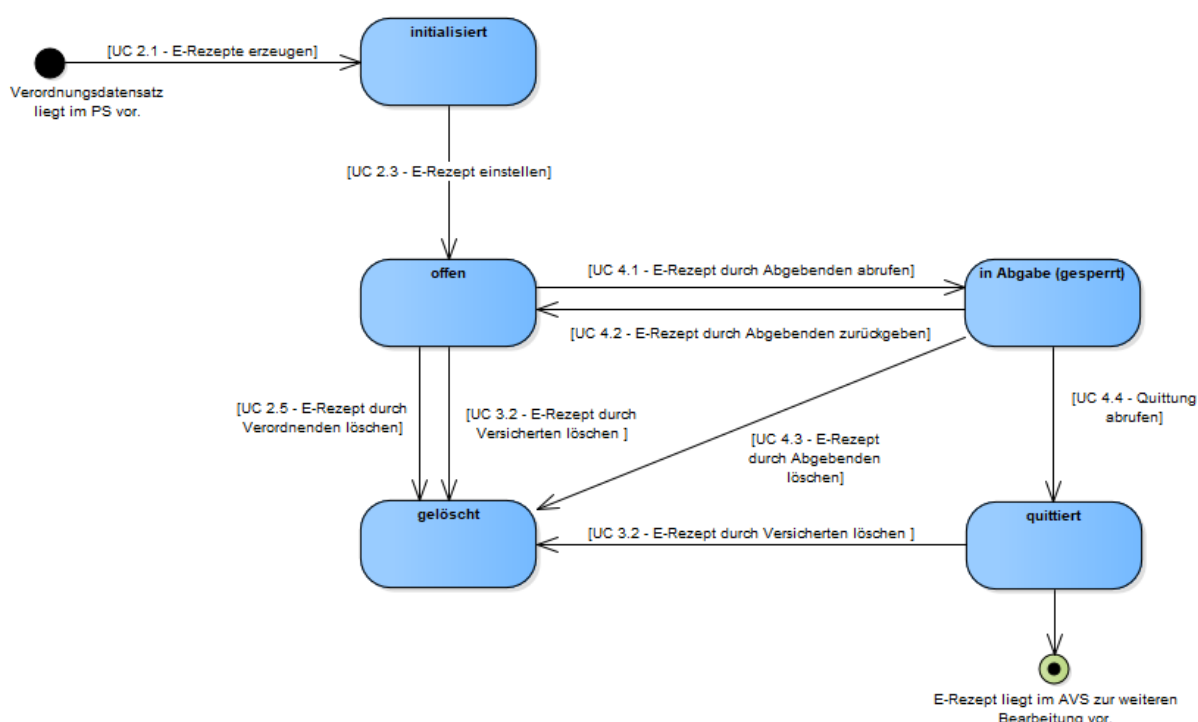


Abbildung 2 : ABB_ILFERP_002 – Statusübergänge

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 einen 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 Prinzip des Exponential Backoffs [ExpBack] durchführen. [≤]

4.2 Namensauflösung

Der E-Rezept-Fachdienst ist für Primärsysteme gemäß den 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 verschiedene IP-Adressen zum FQDN zurück. Diese 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 Betriebssystem 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 anderen/weiteren IP-Adressen 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.

Das Primärsystem erreicht den E-Rezept-Fachdienst und IDP über den Konnektor geroutet. Je nach Installationsumgebung des Primärsystems ist der Konnektor evtl. nicht das Default-Gateway. Um diese offenen Fachdienste zu erreichen, müssen ggfs. feste Routen und eine DNS-Konfiguration für das [Split-DNS] pro Arbeitsplatz-Computer im 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 Netzwerkinstallation, 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_19451-01 - PS: Lokalisierung E-Rezept-Fachdienst

Das Primärsystem MUSS für die zur Kommunikation mit dem E-Rezept-Fachdienst die FQDNs als Lokalisierungsinformationen in einer DNS-Abfrage gemäß [gemSpec_FD_eRP#5.1 Servicelokalisierung] nutzen.[<=]

Die Abfrage beim Namensdienst der TI erfolgt über einen DNS-Lookup. Hierfür muss der Konnektor als DNS-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_20015-01 - PS: HTTP-Header user-agent

Das Primärsystem MUSS in alle HTTP-Requests an Dienste der TI im äußeren HTTP-Request den HTTP-Header user-agent gemäß [RFC7231] mit

`<Produktname>/<Produktversion> <Herstellernamen>/<client_id>` mit

- `<Produktname>` gemäß eigener Definition, Länge 1-20 Zeichen, Zeichenvorrat[0-9a-zA-Z\-\.]
- `<Produktversion>` gemäß Produktidentifikation
- `<Herstellernamen>` gemäß eigener Definition, Länge 1-20 Zeichen, Zeichenvorrat[0-9a-zA-Z\-\.]

- <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 3 : TAB_ILFERP_014 - HTTP-Header "X-erp-resource"

Operation	X-erp-resource
DELETE /Communication/<id>	Communication
GET /Communication/	Communication
GET /Communication/<id>	Communication
GET /Device/	Device
GET /metadata/	metadata
POST /Communication/	Communication
POST /Subscription/	Subscription
POST /Task/\$create	Task
POST /Task/<id>/\$abort	Task
POST /Task/<id>/\$accept	Task
POST /Task/<id>/\$activate	Task
POST /Task/<id>/\$close	Task
POST /Task/<id>/\$reject	Task
GET /ChargeItem/<id>	ChargeItem

POST /ChargeItem/	ChargeItem
PUT /ChargeItem/<id>	ChargeItem

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 [\[gemSpec Krypt#7 Kommunikationsprotokoll zwischen E-Rezept-VAU und E-Rezept-Clients\]](#) .

Alternativ zur Umsetzung des TUC_PKI_018 gemäß [\[gemSpec Krypt#A 21216\]](#) 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 INVALID
- (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)}

Hinweis zum Fehlerhandling: Nur wenn der äußere Response der E-Rezept-Fachdienstes den Response-Code 200 liefert, enthält der payload eine mittels VAU-Protokoll verschlüsselte Response. Liefert der äußere Response eine Code >= 400, ist im VAU-Protokoll ein Fehler aufgetreten. Das PS muss nicht versuchen, den payload zu entschlüsseln.

5.1.3 Zertifikatsprüfung

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

Tabelle 4 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.

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. [`<=`]

Die Primärsysteme prüfen im Rahmen der Anwendungsfälle des E-Rezepts mittels der Konnektor-Operation `VerifyCertificate` (A_20764) u.a. die folgenden Zertifikate der TI:

- Zertifikat des VAU-Protokolls
- Signatur des Discovery-Dokumentes (gemILF_PS_eRp#A_20656-01),
- Signatur des ID_Token (gemILF_PS_eRp#A_20675)

Dies sind ECC-Zertifikate, deren Verwendung erst ab PTV4-Konnektor unterstützt werden.

Für (Z)PVS wird angenommen, dass sie in den Praxen PTV4-Konnektoren vorfinden, da zeitgleich die Anwendung ePA flächendeckend eingeführt wird, welche den PTV4-Konnektor bedingt.

Für Apotheken kann nicht vorausgesetzt werden, dass mindestens ein PTV4-Konnektor vorhanden ist. Hier können auch PTV3-Konnektoren genutzt werden.

Wird ein ECC-Zertifikat mittels `VerifyCertificate` eines PTV3-Konnektors geprüft, dann antwortet diese Operation mit einem Fehler (Konnektor Rise Fehlercode=1025, KoCo + Secunet Fehlercode=1027).

Im Fall, dass bei der Prüfung der obigen Zertifikate die genannten Fehler auftreten, muss ein AVS die alternative Zertifikatsprüfung analog zum E-Rezept-FdV gemäß [gemSpec_Krypt#A_21218] nutzen.

Dies bedeutet, dass die AVS-Hersteller beide Prüfverfahren implementieren müssen. Der E-Rezept-Fachdienst stellt den Primärsystemen für die alternative Zertifikatsprüfung die benötigten Ressourcen `/CertList` und `/OCSPList` an der Schnittstelle im zentralen Netz der TI übergangsweise zur Verfügung. "ee_certs" in `CertList` beinhaltet genau nur die oben gelisteten Zertifikate.

Dies stellt eine Übergangslösung dar, welche aufgrund der oben vorgeschlagenen Implementierung automatisch entfällt, wenn die Apotheke einen PTV4-Konnektor einsetzt. Das BSI hat der Übergangslösung bis zum 31.03.2022 zugestimmt. Bis zu diesem Zeitpunkt ist ein Update von PTV3-Konnektoren vorzunehmen.

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 t), 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

Das Primärsystem MUSS die JWS (JSON Web Signature) [RFC7515 # section-3 - Compact Serialization] Signatur des Discovery Document auf mathematische Korrektheit sowie über die Funktion "VerifyCertificate" des Konnektors gemäß [gemSpec_Kon#4.1.9.5.3] bzw. [gemILF_PS#4.4.4.3] auf Gültigkeit des ausstellenden Zertifikates innerhalb der TI prüfen.

[\leq]

Hinweis: Der genaue Aufbau entspricht [gemSpec_IDP_Dienst#Kapitel 7.7 Aufbau des Discovery Document].

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.

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] [\leq]

Der Authorization-Endpunkt legt nun eine "session_id" an, stellt alle nötigen Informationen zusammen und erzeugt 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. [<=]

A_20663-01 - Prüfung der Signatur des CHALLENGE_TOKEN

Das Primärsystem MUSS die Signatur des "CHALLENGE_TOKEN" gegen den aktuellen öffentlichen Schlüssel des Authorization-Endpunktes "PUK_IDP_SIG" prüfen. Liegt dem Primärsystem der öffentliche Schlüssel des Authorization-Endpunktes noch nicht vor, MUSS es diesen gemäß 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 das gehashte "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

Das Primärsystem MUSS für das Signieren des CHALLENGE_TOKEN des IdP-Dienstes mit der Identität ID.HCI.AUT 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 des CHALLENGE_TOKEN in Base64-Codierung übergeben.

[<=]

Hinweis: Der Aufbau der Anfrage und der einzureichenden Objekte entspricht [gemSpec_IDP_Dienst#Kapitel 7.3 Authentication Request].

Hinweis: Aktuell befinden sich vornehmlich SMC-B der Generation G2 im Feld. Bei diesen ist für die Signatur, entsprechend dem Default des Konnektors, das Verfahren RSASSA-PSS zu nutzen.

Wenn eine SMC-B G2.1-Karte vorhanden ist, ist ECDSA zu priorisieren. Beide Verfahren werden durch den IDP-Dienst unterstützt.

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

A_20666-01 - Auslesen des Authentisierungszertifikates

Das Primärsystem MUSS das Zertifikat ID.HCI.AUT 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 - 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_IDP_ENC" verschlüsselt, an diesen in Form eines HTTP-POST-Requests senden. [<=]

Hinweis: Der Aufbau der Anfrage und der einzureichenden Objekte entspricht [gemSpec_IDP_Dienst#Kapitel 7.3 Authentication Request].

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. <https://tools.ietf.org/html/draft-yusef-oauth-nested-jwt-03> zu realisieren. Im cty-Header ist "JWT" 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" vom IDP-Dienst und reicht 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. [<=]

A_21333 - Erzeugung des "Token-Key"

Das Primärsystem MUSS vor dem Abrufen von ID_Token und ACCESS_Token einen zufälligen 256bit-AES-Schlüssel ("Token-Key") erzeugen. [<=]

A_21334 - Erzeugung des "KEY_VERIFIER"

Das Primärsystem MUSS den "KEY_VERIFIER" bilden, indem "Token-Key" und "CODE_VERIFIER" in einem JSON-Objekt kodiert werden. [<=]

Hinweis: Der Aufbau des "KEY_VERIFIER" entspricht [gemSpec_IDP_Dienst#Kapitel 7.5Token Request].

A_20671-01 - Einreichen des AUTHORIZATION_CODE beim Token-Endpoint

Das Primärsystem MUSS den "Key_Verifier" mittels JWE und PUK_IDP_ENC verschlüsseln und zusammen mit dem "AUTHORIZATION_CODE" TLS-gesichert und als HTTP/1.1 POST Request an den Token-Endpoint senden.

[<=]

Hinweis: Der Aufbau der Anfrage entspricht [gemSpec_IDP_Dienst#Kapitel 7.5 Token Request].

Als Verschlüsselungsalgorithmus ist ECDH-ES (Elliptic Curve Diffie-Hellman Ephemeral Static key agreement) vorgesehen.

Der Token-Endpoint validiert den "CODE_VERIFIER" und gleicht diesen mit der "code_challenge" ab. Dann erzeugt er die erforderlichen Token und verschlüsselt beide mit dem "Token-Key".

Das Primärsystem erhält nun den signierten "ID_TOKEN" und den "ACCESS_TOKEN" vom Token-Endpoint und prüft die Signatur des "ID_TOKEN".

A_20672-01 - 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. [<=]

Hinweis: Der Aufbau der Antwort und des "ID_TOKEN" entspricht [gemSpec_IDP_Dienst#Kapitel 7.6 Token Response].

A_20673-01 - 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.

[<=]

Hinweis: Der Aufbau der Antwort und des "ACCESS_TOKEN" entspricht [gemSpec_IDP_Dienst#Kapitel 7.6 Token Response].

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.

Je nach Rezept-Typ oder Art der Zuweisung werden verschiedene Workflow-Typen des E-Rezept-Fachdienst. Die korrekte Auswahl des Workflow-Typs ist vor dem Erzeugen des E-Rezepts notwendig, da die Rezept-IDs workflow-spezifisch sind. Der Workflow-Typ für ein E-Rezept kann nachträglich nicht mehr geändert werden. Soll für ein E-Rezept, der Workflow geändert werden, dann ist der ursprüngliche Workflow zu löschen und ein neuer Workflow zu erstellen. Die mit dem neuen Workflow erstellte Rezept-ID ist in den Verordnungsdatensatz einzubetten und dieser erneut mit einer QES zu versehen.

A_21363 - PS verordnende LEI: Auswahl des Flowtypes

Das PS der verordnenden LEI MUSS beim Erstellen eines E-Rezeptes die Auswahl des gewünschten Workflows gemäß <https://gematik.de/fhir/CodeSystem/Flowtype> ermöglichen. [<=]

~~A_19274-01A~~ 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 5 : TAB_ILFERP_002 – E-Rezept durch Verordnenden erstellen

Name	E-Rezept durch Verordnenden erstellen
Auslöser	<ul style="list-style-type: none">Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter verordnende LEI
Vorbedingung	<ul style="list-style-type: none">Die LEI hat sich gegenüber der TI authentisiert.Der Workflow-Typ (<code>FlowType</code>) ist bekannt.
Nachbedingung	<ul style="list-style-type: none">Im PS steht ein QES-Datensatz über den Verordnungsdatensatz des E-Rezept bereit.

Standardablauf	<ol style="list-style-type: none">1. E-Rezept-ID von Fachdienst abrufen2. E-Rezept-Bundle erstellen1. Kanonisieren3. E-Rezept-Bundle QES signieren (nur durch LE ausführbar)
----------------	---

[<=]

**A_19276 - ~~PS-verordnende LEI: E-Rezept einstellen~~ — ~~E-Rezept-ID abrufen~~ PS
verordnende LEI: E-Rezept erstellen - 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~~ PS verordnende LEI: E-Rezept erstellen - 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.~~ [<=]

A_22926 - PS verordnende LEI: E-Rezept erstellen - Keine unspezifizierten Extensions

Das PS der verordnenden LEI DARF FHIR-Extensions NICHT im Verordnungsdatensatz verwenden, an denen diese nicht explizit gemäß KBV-Profilversion "kbv.ita.erp 1.0.2" genannt sind. [\leq]

Der E-Rezept-Fachdienst akzeptiert während einer Übergangsfrist Verordnungsdatensätze mit unspezifizierten Extensions mit einer Warnung (Http-Statuscode 202 Accepted). Nach dieser Frist lehnt er diese mit einem Http-Statuscode 400 und entsprechender Fehlermeldung ab. Mit einem Folgerelease zu "kbv.ita.erp 1.0.2" wird die Möglichkeit des OpenSlicing unterbunden.

A_22893 - PS verordnende LEI: E-Rezept erstellen - Gleichheit Ausstellungsdatum und QES Erstellung

Das PS der verordnenden LEI MUSS sicherstellen, dass das Datum authoredOn des Verordnungsdatensatzes dem Datum in QES.Erstellung im Signaturobjekt entspricht. [\leq]

Der E-Rezept-Fachdienst prüft die Gleichheit und weist bei Nicht-Übereinstimmen das E-Rezept beim Einstellen mit dem Fehler 400 und Operation-Outcome "Ausstellungsdatum und Signaturzeitpunkt weichen voneinander ab, müssen aber taggleich sein" ab.

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

A_19281-02 - PS verordnende LEI: E-Rezept erstellen - E-Rezept-Bundle QES signieren

~~A_19281-01 - 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 (CAAdES)
- Signaturtype für eine enveloping Signature
- dem base64-codierten E-Rezept-Bundle
- eingebetteter OCSP-Antwort (IncludeRevocationInfo = true)
- Angabe des Mimetypes "text/plain"

ausführen. [\leq]

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].

A_21243 - ~~PS verordnende LEI: E-Rezept einstellen - Unterstützung Signaturverfahren~~ PS verordnende LEI: E-Rezept-erstellen - Unterstützung Signaturverfahren

Das PS der verordnenden LEI MUSS die Erstellung der E-Rezepte mittels Einzelsignatur, Stapelsignatur und Komfortsignatur unterstützen. [\leq]

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

5.2.1.1 E-Rezept erstellen - Workflow 200/209

Der Verordnungsdatensatz für PKV-Versicherte basiert auf dem selben Datenmodell wie für GKV-Versicherte.

Folgende Anforderungen bestehen für einen Verordnungsdatensatz:

A_22541-01 - PS verordnende LEI: E-Rezept erstellen – Flowtype 200/209 – KVN als Identifier

Das PS der verordnenden LEI MUSS im Verordnungsdatensatz für ein E-Rezept des Flowtype 200 oder 209 als Identifier des Patienten in `Patient.identifier.value` die KVN des Versicherten verwenden.

[<=]

Im Verordnungsdatensatz für ein E-Rezept des Flowtype "200" bzw "209" muss für `Patient.identifier.type.coding.code` der Wert "PKV" gesetzt werden.

Im Verordnungsdatensatz für ein E-Rezept des Flowtype "200" bzw "209" wird das `Patient.identifier.system` nicht angegeben.

A_22542-01 - PS verordnende LEI: E-Rezept erstellen – Flowtype 200/209 – Versicherungstyp PKV

Das PS der verordnenden LEI MUSS im Verordnungsdatensatz für ein E-Rezept des Flowtype 200 oder 209 für `Coverage.type.coding.code` den Wert "PKV" verwenden.

[<=]

Hinweis: Diese Anforderungen beschreiben **nicht** abschließend die Unterschiede zwischen Verordnungsdatensätze für PKV-Versicherte und GKV-Versicherte.

In der Operation "E-Rezept erstellen" wird der Workflow-Typ "200" bzw. "209" als Rezept-Typ im Parameter FlowType übermittelt, um den Workflow für PKV-Versicherte zu initiieren.

5.2.1.2 E-Rezept erstellen - Mehrfachverordnung

Eine Mehrfachverordnung besteht aus bis zu 4 Teilverordnungen.

Folgende Anforderungen bestehen für den Verordnungsdatensatz jeder Teilverordnung:

A_22636 - PS verordnende LEI: E-Rezept erstellen - Mehrfachverordnung - Beginn Einlösefrist

Das PS der verordnenden LEI MUSS im Anwendungsfall "E-Rezept durch Verordnenden erstellen" beim Erstellen des E-Rezept-Bundles für die Teilverordnung einer Mehrfachverordnung den Beginn der Einlösefrist der Teilverordnung (`MedicationRequest.extension:Mehrfachverordnung.extension:Zeitraum.value[x]:valuePeriod.start`) angeben.[<=]

Die Angabe des Endes der Einlösefrist der Teilverordnung ist optional.

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 Einstellen des E-Rezepts muss innerhalb von 24h nach dem Erstellen des E-Rezept erfolgen. Anderenfalls wird das E-Rezept (Task mit Status "draft") auf dem E-Rezept-Fachdienst gelöscht. Nach dem Löschen kann das E-Rezept nicht mehr eingestellt werden.

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 6 : TAB_ILFERP_003 – E-Rezept durch Verordnenden einstellen

Name	E-Rezept durch Verordnenden einstellen
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI• kann durch "E-Rezept durch Verordnenden erstellen" getriggert werden
Akteur	Leistungserbringer, Mitarbeiter verordnende LEI
Vorbedingung	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ol style="list-style-type: none">1. Task auf dem E-Rezept-Fachdienst aktivieren2. optional, wenn das E-Rezept ausgedruckt werden soll:<ol style="list-style-type: none">a. E-Rezept-Token erzeugenb. E-Rezept-Ausdruck erstellen

[<=]

A_19273-01 - 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-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].

A_22503 - PS verordnende LEI: E-Rezept einstellen - kein Ausdruck bei Fehler beim Aktivieren

Das PS der verordnenden LEI DARF im Anwendungsfall "E-Rezept durch Verordnenden einstellen" NICHT einen Ausdruck für den Versicherten erstellen, wenn der E-Rezept-Fachdienst im Response der Operation `POST /Task/<id>/$activate` mit einem Fehler antwortet. [<=]

A_22423 - PS verordnende LEI: separater Ausdruck je Flowtype

Das PS der verordnenden LEI MUSS sicherstellen, dass für jeden Flowtype ein separater Ausdruck erfolgt, sofern der Nutzer verschiedene E-Rezepte aus unterschiedlichen Flowtypes gleichzeitig erzeugt und für diese Ausdrücke erzeugen möchte.[<=]

5.2.2.1 E-Rezept einstellen - Workflow 169

A_21400 - PS verordnende LEI: Übergabe E-Rezept-Token an Apotheke

Das PS der verordnenden LEI MUSS es dem Nutzer ermöglichen, die Einlöseinformationen (Task.id und AccessCode) als E-Rezept-Token über ein geeignetes Übermittlungsverfahren an eine Apotheke der Wahl zu schicken.[<=]

A_21349 - PS: Schutz des E-Rezept-Tokens bei Übertragung

Das Primärsystem MUSS für die Übertragung von E-Rezept-Token ein Verfahren nutzen, dass die sehr hohe Vertraulichkeit des E-Rezept-Tokens und seine Integrität schützt.[<=]

Geeignete Verfahren sind z.B. die Übermittlung des E-Rezept-Token mit dem sicheren Übermittlungsverfahren der TI, KIM.

**A_21453 - PS verordnende LEI: Herstellende Apotheke für
Übermittlungsverfahren**

Das PS der verordnenden LEI KANN die Auswahl und Verwaltung von herstellenden Apotheken für die Übermittlung der E-Rezept-Einlöseinformationen ermöglichen.
[<=]

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 abubrechen.[<=]

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 7 : TAB_ILFERP_004 – E-Rezept durch Verordnenden löschen

Name	E-Rezept durch Verordnenden löschen
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter verordnende LEI
Vorbedingung	<ul style="list-style-type: none">• Der Nutzer hat ein E-Rezept zum Löschen markiert und das Löschen bestätigt.• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	<ul style="list-style-type: none">• Das ausgewählte E-Rezept ist vom E-Rezept-Fachdienst unwiederbringlich gelöscht.
Standardablauf	<ol style="list-style-type: none">1. Task-ID und AccessCode des E-Rezepts bestimmen2. E-Rezept auf E-Rezept-Fachdienst löschen3. E-Rezept-Token in PS löschen

[<=]

A_19239-01 - 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-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 8 : TAB_ILFERP_005 – E-Rezept abrufen

Name	E-Rezept abrufen
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Das E-Rezept steht im PS bereit.

Standardablauf	<ol style="list-style-type: none">1. Task-ID und AccessCode des E-Rezepts bestimmen2. Task herunterladen3. QES prüfen4. Verordnung extrahieren5. E-Rezept-Daten speichern
----------------	---

[<=]

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.

Hinweis zu Mehrfachverordnung:

Wenn ein AVS eine Teilverordnung abrufen, deren Einlösezeitraum noch nicht erreicht ist, dann liefert der E-Rezept-Fachdienst einen Fehler 403. Im `OperationOutcome` der Fehlermeldung liefert der E-Rezept-Fachdienst das Datum des Beginns der Einlösefrist.

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. [≤]

Für den Flowtype "200" und "209" wird im Response Bundle eine Consent Ressource mit `Consent.category.coding.code = CHARGCONS` übermittelt, falls der Versicherte eine Einwilligung zum Speichern von Abrechnungsinformationen erteilt hat. Diese Information kann in der Abstimmung mit dem Versicherten genutzt werden, ob die Abrechnungsinformation digital oder als Papierbeleg bereitgestellt wird.

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 Online-Rezepteinlösung nutzen, kann die abgebende LEI die Belieferungs- 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 und zusätzlich sicherstellen, dass der Umfang der übertragenen Daten nur auf das unmittelbare für die Einlösung erforderliche Maß beschränkt (Datenminimierung) ist und keine Verwendung der Daten über die unmittelbare Rezepteinlösung hinaus erfolgt (Zweckbindung). [≤]

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 - 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 9 : TAB_ILFERP_006 – Quittung abrufen

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

[<=]

A_19288-01A_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 und dem Wert `whenHandedOver` sowie optional `whenPrepared` im 10-stelligen Datumsformat "yyyy-mm-dd" erstellen.[<=]

A_22071 - PS abgebende LEI: Quittung - Mehrere MedicationDispense erstellen

Das PS der abgebenden LEI MUSS im Anwendungsfall "Quittung abrufen" und Belieferung einer Verordnung durch mehrere Medikamente (z.B. Stückelung auf mehrere Packungen zu 50+50 Tabletten bei Nicht-Verfügbarkeit von 100 Tabletten) eine Standard-FHIR-Ressource Bundle mit je einer `MedicationDispense` mit den Informationen über das jeweils abgegebene Medikament erstellen.[<=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, sofern es sich bei dem abgegebenen Arzneimittel um ein Fertigarzneimittel handelt, das einen Data-Matrix-Code gemäß securPharm-System besitzt. [**<=**]

A_19289-01A_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 bzw. Bundle 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 quitierten 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].

Hinweis: Mit den Konnektor-Versionen PTV4, PTV4+ und PTV5 kann die Signatur der Quittung nicht geprüft werden, da die Signaturprüfung immer ein negatives Ergebnis liefert. Grund ist, dass für das Zertifikatsprofil des durch den E-Rezept-Fachdienstes verwendeten Signaturzertifikates die Signaturprüfung noch nicht spezifiziert und implementiert ist. Wenn eine Apotheke die Signatur der Quittung prüfen möchte, dann muss dies unabhängig vom Konnektor im AVS umgesetzt werden. Die Zertifikatsprüfung im Rahmen der Signaturprüfung kann mittels der Konnektorfunktion VerifyCertificate erfolgen.

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. [\leq]

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 10 : TAB_ILFERP_007 – Quittung erneut abrufen

Name	Quittung erneut abrufen
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• Die LEI hat bereits mindestens einmal die Quittung abgerufen (Anwendungsfall "Quittung abrufen").• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	<ul style="list-style-type: none">• Die Quittung zum E-Rezept steht im PS bereit.
Standardablauf	<ol style="list-style-type: none">1. Task-ID und Geheimnis des E-Rezepts bestimmen2. Quittung abrufen3. Quittung aus Response extrahieren

[\leq]

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 abzuberechnen.[<=]

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 11 : TAB_ILFERP_008 – E-Rezept durch Abgebenden zurückgeben

Name	E-Rezept durch Abgebenden zurückgeben
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Das ausgewählte E-Rezept hat auf dem E-Rezept-Fachdienst den Status "offen"
Standardablauf	<ol style="list-style-type: none">1. Task-ID und Geheimnis des E-Rezepts bestimmen2. E-Rezept Status auf Fachdienst ändern3. 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_22742 - PS abgebende LEI: E-Rezepte löschen - Flowtype 200/209 - Warnung Abgabeinformationen

Das PS der abgebenden LEI MUSS, falls der Nutzer ein E-Rezept mit Flowtype 200 oder 209 zum Löschen ausgewählt hat und für das E-Rezept noch keine Abrechnungsinformationen bereitgestellt wurden, eine Warnung anzeigen, dass ein Bereitstellen der Abrechnungsinformationen zum E-Rezept nach dem Löschen des E-Rezepts nicht mehr möglich ist. [`<=<=`]

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 abzuberechnen. [`<=`]

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 12 : TAB_ILFERP_009 – E-Rezept durch Abgebenden löschen

Name	E-Rezept durch Abgebenden löschen
------	-----------------------------------

Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Das ausgewählte E-Rezept ist vom E-Rezept-Fachdienst unwiederbringlich gelöscht.
Standardablauf	<ol style="list-style-type: none">1. Task-ID und Geheimnis des E-Rezepts bestimmen2. E-Rezept auf Fachdienst löschen3. 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_21556 - PS abgebende LEI: Häufigkeit des Abrufen von Nachrichten

Das PS der abgebenden LEI MUSS im Anwendungsfall "Nachrichten von Versicherten empfangen" zwischen den Aufrufen der Operation `GET /Communication` mindestens 5 Minuten warten. Der Zeitraum zwischen den Aufrufen muss um eine zufällige Zeitspanne

zwischen 0 und 10.000 Millisekunden verlängert werden, um eine Gleichverteilung der Anfragen am E-Rezept-Fachdienst über alle Apotheken zu erreichen. [<=]

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 13 : TAB_ILFERP_010 – Nachrichten von Versicherten empfangen

Name	Nachrichten von Versicherten empfangen
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI• periodische Abfrage durch das PS
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	<ul style="list-style-type: none">• Die auf dem E-Rezept-Fachdienst für die abgebende LEI hinterlegten Communication Ressourcen wurden übertragen. Die E-Rezept-Nachrichten stehen im PS bereit.
Standardablauf	<ol style="list-style-type: none">1. E-Rezept-Nachrichten am Fachdienst abrufen2. Mitteilung und E-Rezept-Token extrahieren

[<=]

A_19329-01 - PS abgebende LEI: Nachrichten empfangen - Abfragerequest

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 einlöserrelevanten Informationen beziehbar sind
 - optional: Mitteilung/Text
- **Übermittlung Abrechnungsinformation-Token (GEM_ERP_PR_Communication_ChargChangeReq)**
 - Referenz auf ein ChargeItem inkl. Zugriffsberechtigung
 - 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.

Wenn die Nachricht einen Abgabeinformation-Token enthält, dann hat der Versicherte die abgebende LEI autorisiert, den PKV-Abgabedatensatz zu ändern.

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 14 : TAB_ILFERP_015 – Nachricht von Versicherten empfangen - payload

Attribut	mandatory/optional	Bedeutung
version	mandatory	immer 1
supplyOptionsType	mandatory	Valide Inhalte: "onPremise", "delivery", "shipment"
name	mandatory	"onPremise": Name des Versicherten laut Rezept "delivery"/"shipment": Name des Lieferungsempfänger
address	mandatory	"onPremise": Adresse des Versicherten laut Rezept "delivery"/"shipment": Adresse des Lieferungsempfänger mindestens: Strasse+Hausnummer, PLZ+Ort werden gesetzt
hint	optional	nur bei "delivery": Hinweise zur Belieferung Freitext, max. 90 Zeichen
phone	optional	immer bei "delivery", internationales Format

Hinweis zur Bedeutung der Abhol-/Lieferoptionen:

- onPremise = Abholung in Apotheke
- delivery = Lieferung zum Versicherten durch Vor-Ort-Apotheke
- shipment = Versand zum Versicherten durch Online-Apotheke

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. [\leq]

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. [\leq]

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

Das PS der abgebenden LEI MUSS sicherstellen, dass die Einbettung einer externen URL ausschließlich für das Einlösen von E-Rezepten in einer externen Bestellplattform genutzt wird. [\leq]

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.

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 15 : TAB_ILFERP_011 – Nachricht an Versicherten versenden

Name	Nachricht an Versicherten versenden
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• Die LEI hat eine E-Rezept-Nachricht vom E-Rezept-Fachdienst heruntergeladen.• Der Nutzer hat eine Mitteilung als Antwort auf die Nachricht erfasst.

	<ul style="list-style-type: none">• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	<ul style="list-style-type: none">• Auf dem E-Rezept-Fachdienst steht eine E-Rezept-Nachricht für den Versicherten bereit.
Standardablauf	<ol style="list-style-type: none">1. Versicherten-ID aus der Nachricht des Versicherten bestimmen2. Communication Ressource erstellen3. E-Rezept-Nachricht auf Fachdienst einstellen

[<=]

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

A_19333-01 - 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`
- Task-ID des referenzierten E-Rezeptes in `basedOn`
- Nachrichten-ID der empfangenen Anfrage in `inResponseTo` (optional)
- Textnachricht in `payload contentString`
- optional: verfügbare Belieferungsoptionen ["Apotheke", "Bote", "Versand"] der Apotheke
- optional: Verfügbarkeitsstatus gemäß ValueSet 'AvailabilityStatusVS' [10, 20, ..., 90]
- optional: `Communication.topic` mit Code gemäß <https://www.hl7.org/fhir/codesystem-communication-topic.html> zur Kennzeichnung des Inhalts ("phone-consult", o.ä.)

erstellen.[<=]

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

Tabelle 16 : TAB_ILFERP_016 – Nachricht an Versicherten versenden - payload

Attribut	mandatory/optional	Bedeutung
version	mandatory	immer 1
supplyOptionsType	mandatory	Der supplyOptionsType, der bei der Zuweisung durch den Versicherten übergeben wurde, wird hier wiederholt. Valide Inhalte: "onPremise", "delivery", "shipment".
info_text	optional	Freitext, maximal 400 Zeichen
url	optional	Wenn gesetzt, wird dem Versicherten ein Button angezeigt, der einen Absprung auf die hinterlegte URL in den Browser des Betriebssystems auslöst.
pickUpCodeHR	optional	menschenlesbarer Abholcode Nur bei supplyOptionsType "onPremise". Wenn gesetzt, wird dem Nutzer der Inhalt des "pickUpCodeHR" optisch hervorgehoben angezeigt. Maximale Länge 8 Zeichen.
pickUpCodeDMC	optional	maschinenlesbarer Abholcode (Data-Matrix-Code) 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_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 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 abubrechen. [<=]

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 17 : TAB_ILFERP_013 – Nachricht durch Abgebenden löschen

Name	Nachricht durch Abgebenden löschen
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• Der Nutzer hat eine Nachricht zum Löschen markiert und das Löschen bestätigt.• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	<ul style="list-style-type: none">• Die ausgewählte Nachricht ist vom E-Rezept-Fachdienst unwiederbringlich gelöscht.

Standardablauf	<ol style="list-style-type: none">1. ID der Communication Ressource bestimmen2. Nachricht auf Fachdienst löschen3. Nachricht in PS löschen (optional)
----------------	---

[<=]

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 Löschfristen, auf dem E-Rezept-Fachdienst gelöscht wird, dann werden auch alle zugehörigen Nachrichten gelöscht.

5.3.9 Abgabedatensatz signieren

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

Die Inhalte und die Struktur des Abgabedatensatzes werden durch DAV und GKV-SV vorgegeben. Die Definition erfolgt in Form von FHIR-Profilen. Der Datensatz 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 Abgabedatensatzes wird der Konnektor verwendet.

A_21619 - PS abgebende 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

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

5.3.10 2D-Code einscannen

Eine Alternative zur Übermittlung eines E-Rezept-Token [oder eines Abrechnungsinformation-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_19630-01A_19630 - PS abgebende LEI: 2D-Code scannen~~

~~Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, einen 2D-Code für [E-Rezept](#) ~~das~~ [Zuweisen von E-Rezepten](#) oder zum [Ändern einer Abrechnungsinformation](#) einzuscannen. [<=]~~

A_22078 - PS abgebende LEI: 2D-Code scannen - Gescannte Inhalte prüfen

Das PS der abgebenden LEI MUSS die gescannten Inhalte vor einer weiteren Verarbeitung validieren, um sich vor Schadsoftware zu schützen. [<=]

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

Der

~~A_19631 - PS abgebende LEI: 2D-Code [scannen](#) - E-Rezept~~ für Abrechnungsinformation-Token ~~extrahieren~~ enthält genau einen Token.

A_19631-01 - PS abgebende LEI: 2D-Code scannen - Token extrahieren

Das PS der abgebenden LEI MUSS den oder die ~~E-Rezept~~-Token aus einem eingescannten ~~Datamatrix-2D-Code~~ extrahieren. [<=]

Für den Aufbau des 2D-Codes und Struktur des E-Rezept-Token [bzw. Abrechnungsinformation-Token](#) siehe [gemSpec_DM_eRp].

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

Mit der Information aus dem Abrechnungsinformation-Token kann die Abrechnungsinformation vom E-Rezept-Fachdienst heruntergeladen und der PKV-Abgabedatensatz einmalig auf dem E-Rezept-Fachdienst aktualisiert werden.

Hinweis zu Mehrfachverordnung:

Wenn Datamatrix-Codes einer Mehrfachverordnung von einem Ausdruck eingescannt werden, dann dürfen die E-Rezept-Token der Teilverordnungen, welche noch nicht ihren Gültigkeitszeitraum erreicht haben, nicht automatisch im AVS gespeichert werden, da der Versicherte das Recht hat, für diese ggf. eine andere Apotheke für das Einlösen auszuwählen.

Ein Speichern des E-Rezept-Token kann auf Wunsch des Versicherten erfolgen.

A_22637 - PS abgebende LEI: 2D-Code scannen - Mehrfachverordnung - Teilverordnungen nicht speichern

Das PS der abgebenden LEI DARF die E-Rezept-Token von Teilverordnungen einer Mehrfachverordnung, deren Einlösefrist noch nicht begonnen hat, NICHT automatisch speichern.[<=]

5.3.11 Rezept-Informationen von verordnenden LEI empfangen

Im Rahmen des Workflow 169 / 209 erfolgt die Zuweisung des E-Rezeptes an die abgebende LEI durch die verordnende LEI. Hierfür ist ein sicheres Übermittlungsverfahren, bspw. Kommunikation im Medizinwesen (KIM) zu verwenden.

A_21723 - PS abgebende LEI: Übergabe E-Rezept-Token an Apotheke

Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, die Einlöseinformationen (Task.id und AccessCode) als E-Rezept-Token über ein sicheres Übermittlungsverfahren zu empfangen.[<=]

5.3.12 Abrechnungsinformationen

5.3.12.1 Abrechnungsinformation bereitstellen

Mit diesem Anwendungsfall stellt die abgebende LEI die Abrechnungsinformation zu einem E-Rezept auf dem E-Rezept-Fachdienst ein.

A_22708 - PS abgebende LEI: Abrechnungsinformation bereitstellen – Einwilligung muss vorliegen

Das PS der abgebenden LEI DARF NICHT Abrechnungsinformation auf dem E-Rezept-Fachdienst bereitstellen, wenn ihm nicht zuvor die Information über die Einwilligung des Versicherten vom E-Rezept-Fachdienst übertragen wurde.[<=]

A_22186 - PS abgebende LEI: Abrechnungsinformation bereitstellen – E-Rezept auswählen

Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, ein E-Rezept auszuwählen, zu dem die Abrechnungsinformation auf dem E-Rezept-Fachdienst bereitgestellt werden soll.[<=]

Die Information, dass der Versicherte die Einwilligung zum Speichern der Abrechnungsinformationen auf dem E-Rezept-Fachdienst erteilt hat, wird im Anwendungsfall "E-Rezept abrufen" übermittelt.

A_22187 - PS abgebende LEI: Abrechnungsinformation bereitstellen

Das PS der abgebenden LEI MUSS den Anwendungsfall "Abrechnungsinformation durch Abgebenden bereitstellen" gemäß TAB_ILFERP_xxx umsetzen.

Tabelle 18 : TAB_ILFERP_xxx – Abrechnungsinformation bereitstellen

Name	Abrechnungsinformation bereitstellen
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• Die abgebende LEI hat den Workflow zum E-Rezept mit dem Anwendungsfall „Quittung abrufen“ abgeschlossen. Die Information Task-ID und dem Secret zum E-Rezept sind bekannt.• Im PS liegt die Information vor, dass der Versicherte die Einwilligung zum Speichern der Abrechnungsinformationen auf dem E-Rezept-Fachdienst erteilt hat.• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	<ul style="list-style-type: none">• Der PKV-Abgabedatensatz ist auf dem E-Rezept-Fachdienst gespeichert.
Standardablauf	<ol style="list-style-type: none">1. PKV-Abgabedatensatz erstellen2. PKV-Abgabedatensatz mit Konnektor signieren3. ChargeItem erstellen4. Task-ID und Geheimnis des E-Rezepts bestimmen5. PKV-Abgabedatensatz speichern

[<=]

A_22188 - PS abgebende LEI: Abrechnungsinformation bereitstellen – PKV-Abgabedatensatz erstellen

Das PS der abgebenden LEI MUSS im Anwendungsfall "Abrechnungsinformation bereitstellen" eine FHIR-Ressource des PKV-Abgabedatensatzes mit den Informationen zur Abrechnung des abgegebenen Medikaments erstellen.[<=]

Für die Spezifikation der Ressource PKV-Abgabedatensatz siehe [gemSpec_DM_eRp].

Das Signieren des PKV-Abgabedatensatzes erfolgt gemäß [gemILF_PS_eRp] Kap. "Abgabedatensatz signieren". Für die Wahl des Signaturverfahrens (QES oder nonQES) gelten die rechtlichen Vorgaben.

A_22189 - PS abgebende LEI: Abrechnungsinformation bereitstellen – ChargeItem erstellen

Das PS der abgebenden LEI MUSS im Anwendungsfall "Abrechnungsinformation bereitstellen" eine FHIR-Ressource `ChargeItem` erstellen und den PKV-Abgabedatensatzes als contained Ressource einfügen.[<=]

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

A_22190 - PS abgebende LEI: Abrechnungsinformation bereitstellen - Speicherrequest

Das PS der abgebenden LEI MUSS im Anwendungsfall "Abrechnungsinformation bereitstellen" die HTTP-Operation `POST /ChargeItem/` des E-Rezept-Fachdienstes mit

- `ACCESS_TOKEN` im Authorization-Header
- Task-ID als URL-Parameter `?task=`
- Geheimnis in URL-Parameter `?secret=`
- `ChargeItem` im http-Body des Aufrufs als `data`

ausführen. `<=[<=]`

Wenn das E-Rezept bereits vom E-Rezept-Fachdienst gelöscht wurde, dann enthält der Response den Fehlercode 405. Das Bereitstellen der Abrechnungsinformation zu einem E-Rezept ist nur möglich bevor das E-Rezept gelöscht wurde.

Wenn der Versicherte zwischenzeitlich die Einwilligung zum Speichern von Abrechnungsinformationen im E-Rezept-Fachdienst widerrufen hat, dann enthält der Response den Fehlercode 403.

5.3.12.2 PKV-Abgabedatensatz ändern

Mit diesem Anwendungsfall kann die abgebende LEI den PKV-Abgabedatensatz zu einem E-Rezept, welche die abgebende LEI zuvor auf dem E-Rezept-Fachdienst bereitgestellt hat, ändern. Als Voraussetzung muss der Versicherte der abgebenden LEI einen `AccessCode` übermitteln, um die abgebende LEI zu berechtigen.

A_22191 - PS abgebende LEI: PKV-Abgabedatensatz ändern - PKV- Abgabedatensatz zum Ändern auswählen

Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, die Abrechnungsinformation zu einem E-Rezept zum Ändern auf dem E-Rezept-Fachdienst auszuwählen. `<=[<=]`

A_22192 - PS abgebende LEI: PKV-Abgabedatensatz ändern

Das PS der abgebenden LEI MUSS den Anwendungsfall "PKV-Abgabedatensatz durch Abgebenden ändern" gemäß `TAB_ILFERP_xxx` umsetzen.

Tabelle 19 : TAB_ILFERP_xxx – Abrechnungsinformation ändern

Name	PKV-Abgabedatensatz ändern
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• Der Versicherte hat den <code>AccessCode</code> übermittelt.• Die abgebende LEI hat die Abrechnungsinformation für das E-Rezept auf dem E-Rezept-Fachdienst bereitgestellt. Die Information zur Prescription-ID ist bekannt.• Die LEI hat sich gegenüber der TI authentisiert.

Nachbedingung	<ul style="list-style-type: none">• Der geänderte PKV-Abgabedatensatz ist auf dem E-Rezept-Fachdienst gespeichert.
Standardablauf	<ol style="list-style-type: none">1. PKV-Abgabedatensatz erstellen2. PKV-Abgabedatensatz mit Konnektor signieren3. Prescription-ID und AccessCode der Abrechnungsinformation bestimmen4. Abrechnungsinformation speichern

[<=]

A_22193 - PS abgebende LEI: PKV-Abgabedatensatz ändern – PKV-Abgabedatensatz erstellen

Das PS der abgebenden LEI MUSS im Anwendungsfall "PKV-Abgabedatensatz ändern" eine FHIR-Ressource des PKV-Abgabedatensatzes mit den Informationen zur Abrechnung des abgegebenen Medikaments erstellen.[<=]

Für die Spezifikation der Ressource PKV-Abgabedatensatz siehe [gemSpec_DM_eRp].

Das Signieren des PKV-Abgabedatensatzes erfolgt gemäß [gemILF_PS_eRp] Kap. "Abgabedatensatz signieren".

A_22194 - PS abgebende LEI: PKV-Abgabedatensatz ändern – ChargeItem erstellen

Das PS der abgebenden LEI MUSS im Anwendungsfall "PKV-Abgabedatensatz ändern" eine FHIR-Ressource `ChargeItem` erstellen und den PKV-Abgabedatensatzes als contained Ressource einfügen.[<=]

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

A_22195 - PS abgebende LEI: PKV-Abgabedatensatz ändern - Speicherrequest

Das PS abgebende LEI MUSS im Anwendungsfall "PKV-Abgabedatensatz ändern" die HTTP-Operation `PUT /ChargeItem/<id>/` des E-Rezept-Fachdienstes mit

- `ACCESS_TOKEN` im Authorization-Header
- Prescription-ID in URL `<id>`
- AccessCode in URL-Parameter `?ac=`
- `ChargeItem` im http-Body des Aufrufs als `data`

ausführen.[<=]

Wenn der Versicherte zwischenzeitlich die Einwilligung zum Speichern von Abrechnungsinformationen im E-Rezept-Fachdienst widerrufen hat, dann enthält der Response den Fehlercode 403.

5.3.12.3 Abrechnungsinformation abrufen

Mit diesem Anwendungsfall kann eine abgebende LEI die Abrechnungsinformation vom E-Rezept-Fachdienst abrufen, welche durch sie zuvor bereitgestellt und noch nicht gelöscht wurde. Als Voraussetzung muss der Versicherte der abgebenden LEI einen AccessCode übermitteln, um die abgebende LEI zu berechtigen.

A_22202 - PS abgebende LEI: Abrechnungsinformation abrufen

Das PS der abgebenden LEI MUSS den Anwendungsfall "Abrechnungsinformation durch Abgebenden abrufen" gemäß TAB_ILFERP_xxx umsetzen.

Tabelle 20 : TAB_ILFERP_xxx – Abrechnungsinformation abrufen

Name	Abrechnungsinformation abrufen
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Leistungserbringer, Mitarbeiter der abgebenden LEI
Vorbedingung	<ul style="list-style-type: none">• Der Versicherte hat den AccessCode übermittelt.• Die Prescription-ID der Abrechnungsinformation ist im Primärsystem bekannt• Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	<ul style="list-style-type: none">• Die Informationen zum PKV-Abgabedatensatz liegen im PS vor
Standardablauf	<ol style="list-style-type: none">1. Prescription-ID und AccessCode der Abrechnungsinformation bestimmen2. Abrechnungsinformation abrufen

[<=]

A_22203 - PS abgebende LEI: Abrechnungsinformation abrufen - Leserequest

Das PS abgebende LEI MUSS im Anwendungsfall "Abrechnungsinformation abrufen" die HTTP-OperationGET /ChargeItem/<id> des E-Rezept-Fachdienstes mit

- ACCESS_TOKEN im Authorization-Header
- Prescription-ID in URL <id>
- AccessCode in URL-Parameter ?ac=

ausführen.[<=]

Im Response ist die ChargeItem Ressource mit dem Verordnungsdatensatz und dem zugehörigen PKV-Abgabedatensatz enthalten.

5.3.13 Subscription für neue Communication

Um die Last am E-Rezept-Fachdienst zu kontrollieren, wurde festgelegt, dass ein AVS nicht öfter als alle 5 min nach neuen Nachrichten anfragen darf (A_21556). Die dadurch bis zu 5 min entstehende Verzögerung verlängert die Zeit, bis eine Apotheke auf die Nachricht des Versicherten reagieren kann. Aus dem Grund wird eine Funktionalität eingeführt, mit der AVS eine Notification erhalten, dass eine neue Nachricht für eine Telematik-ID vorliegt. Nach Erhalt einer Notification darf das AVS die neue Nachricht sofort abrufen.

A_22426 - PS abgebende LEI: Subscription für neue Communication - eine Subscription pro Telematik-ID

Das PS der abgebenden LEI DARF NICHT mehr als eine Subscription pro Telematik-ID registrieren.[<=]

A_22372 - PS abgebende LEI: Subscription für neue Communication

Das PS der abgebenden LEI MUSS den Anwendungsfall "Subscription für neue Communication" gemäß TAB_ILFERP_017 umsetzen.

Tabelle 21: TAB_ILFERP_017 – Subscription für neue Communication

Name	Subscription für neue Communication
Auslöser	<ul style="list-style-type: none">Periodischer Aufruf, wenn keine Websocket-Verbindung für die Notification besteht
Akteur	AVS
Vorbedingung	<ul style="list-style-type: none">Die LEI hat sich gegenüber der TI authentisiert.
Nachbedingung	<ul style="list-style-type: none">Es besteht eine Websocket-Verbindung zum Empfang der Notification
Standardablauf	<ol style="list-style-type: none">Subscription Ressource erstellenSubscription registrierenWebsocket-Verbindung zu Subscription Service aufbauenListening

[<=]

A_22373 - PS abgebende LEI: Subscription für neue Communication - Subscription Ressource erstellen

Das PS der abgebenden LEI MUSS im Anwendungsfall "Subscription für neue Communication" eineSubscription Ressource mit

- Telematik-ID in Element criteria Attribut recipient

erstellen.[<=]

A_22374 - PS abgebende LEI: Subscription für neue Communication - Subscription registrieren

Das PS der abgebenden LEI MUSS im Anwendungsfall "Subscription für neue Communication" zum Registrieren im E-Rezept-Fachdienst die HTTP-OperationPOST /v1/Subscription mit

- ACCESS_TOKEN im Authorization-Header

ausführen.[<=]

Beispiel:

POST /v1/Subscription

```
<Subscription>
  <status value="requested"/>
  <criteria value="Communication?received=null&recipient=3-
```

```
05.2.1001000000.381"/>
  <channel>
    <type value="websocket"/>
  </channel>
</Subscription>
```

Im Response des POST /v1/Subscription Request ist die Subscription Ressource, ergänzt um die subscription-id und einen Authorization Header (Bearer-Token), enthalten.

A_22375 - PS abgebende LEI: Subscription für neue Communication - Subscription

Das PS der abgebenden LEI MUSS im Anwendungsfall "Subscription für neue Communication" nach der Registrierung eine Web Socket Verbindung zum Subscription Service mit

- Authorization Header

aufbauen und ein Upgrade durchführen.[<=]

Beispiel:

```
GET https://subscription.zentral.erp.splitdns.ti-dienste.de/subscription
Authorization: Bearer secret-token-abc-123
Connection: Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket
Sec-WebSocket-Version: 13
Sec-WebSocket-Key: q4xkc032u266gldTuKaSOw==
```

Der Subscription Service antwortet mit dem Upgrade

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: fA9dggdnMPU79lJgAE3W4TRnyDM=
```

Das Upgrade erfolgt mit einer "bind" Text-Nachricht über die Web Socket-Verbindung an den Server.

```
bind: <subscription id>
```

Der Subscription Service antwortet mit einer "bound" um die Einrichtung der Subscription zu bestätigen.

```
bound: <subscription id>
```

Wenn eine neue Nachricht für die Telematik-ID der Apotheke eingestellt wird, dann sendet der E-Rezept-Fachdienst eine Nachricht ping: <subscription-id>. Das AVS kann dann diese Nachricht mittels des Anwendungsfalls "Nachrichten von Versicherten empfangen" unter Nutzung des Requests GET /Communication?received=null&recipient=<Telematik-ID> abrufen.

Bei Nutzung des Subscription Services kann abweichend von der Anforderung "A_21556 - PS abgebende LEI: Häufigkeit des Abrufen von Nachrichten" die Operation GET /Communication häufiger als alle 5 Minuten, d.h. nach jeder Notification, mit den obigen Parametern angefragt werden.

Die Websocket-Verbindung kann bis zu 12 h bestehen. Danach muss das AVS die Subscription neu registrieren.

A_22379 - PS abgebende LEI: Subscription für neue Communication - Wartezeit

Der Primärsystem der abgebenden LEI KANN eine beliebige Wartezeit bis zum Abruf der Nachrichten mit Anwendungsfall „Nachrichten von Versicherten empfangen“ umsetzen, wenn in einem Zeitraum sehr viele ping-Benachrichtigungen empfangen werden. [\leq]

Hinweis: Jede eingestellte Nachricht führt zu einem Ping, ggfs. im Millisekundenbereich, wenn viele Nachrichten an einen Empfänger gerichtet werden. In Abhängigkeit von der Implementierung kann dieses Verhalten zu einer Überlastung des PS führen, wenn bspw. jedes einzelne Ping den Anwendungsfall „Nachrichten von Versicherten empfangen“ triggert.

5.4 E-Rezept-spezifische KIM-Messages

5.4.1 E-Rezept-spezifische KIM-Messages - Workflow 169 /209

Es werden zwei E-Rezept-spezifische KIM-Messages im Rahmen der Kommunikation zwischen verordnenden und abgebenden LEI für den Workflow 169 spezifiziert.

Eine Message dient der direkten Zuweisung eines E-Rezepts und enthält einen Mitteilungstext, den E-Rezept-Token und optional einen Therapieplan. Die strukturierte Message kann automatisiert verarbeitet werden.

Der zweite Message-Typ dient der freien Kommunikation zur Belieferung des E-Rezepts, bspw. Rückfragen durch die Apotheke.

A_21870 - E-Rezept - X-KIM-Dienstkennung - Zuweisung

Das PS der verordnenden LEI MUSS bei der Übermittlung eines E-Rezepts über KIM im KIM-Header "X-KIM-Dienstkennung" den Wert "eRezept;Zuweisung;V1.0" für die direkte Zuweisung und Übermittlung der Einlöseinformationen verwenden.[\leq]

A_21871 - E-Rezept - X-KIM-Dienstkennung - Kommunikation

Das PS der verordnenden oder abgebenden LEI MUSS in einer Nachricht zu einem E-Rezept über KIM im KIM-Header "X-KIM-Dienstkennung" den Wert "eRezept;Kommunikation;V1.0" für die sonstige Kommunikation untereinander im Rahmen der Belieferung durch eine Apotheke verwenden.[\leq]

A_21872 - E-Rezept - KIM-Header subject

Das PS der verordnenden und der abgebenden LEI MUSS die Angabe von personenbezogenen oder medizinischen Informationen im KIM-Header "subject" unterbinden.[\leq]

Das PS der vorordnenden LEI MUSS bei Versand einer Zuweisungs-Message eine Message mit "Content-Type: multipart/mixed;..." und der folgenden Struktur verwenden.

Teil	Inhalt	optional
Freitext	Freitextmessage für den Empfänger default: "direkte Zuweisung E-Rezept"	nein
Einlöseinformation	E-Rezept-Token als Link gemäß gemSpec_DM_eRp#A_19554 Nach 45 Zeichen MUSS ein Steuerzeichen "CRLF" eingefügt werden	nein
Therapieplan	Therapieplan als Anhang, base64 codiert	ja

Das Einfügen des "CRLF" erfolgt, um Warnungen im Validator zu vermeiden und muss beim Verarbeiten im abgebenden PS berücksichtigt werden.

Das PS der abgebenden LEI MUSS bei der Verarbeitung des Nachrichtenteils Einlöseinformation das Steuerzeichen "CRLF" aus dem E-Rezept-Token entfernen. [<=]

Validator <https://tools.ietf.org/tools/msglint/> für die Konformitätsprüfung genutzt werden. Im Produktivbetrieb ist die Nutzung aufgrund des Datenschutzes nicht zulässig.

Das PS der abgebenden und verordnenden LEI MUSS bei Versand einer Kommunikations-Message eine Message mit "Content-Type: text/plain;charset=UTF-8" verwenden. [=>]

Beispiel für eine E-Rezept-spezifische KIM-Message für die Zuweisung eines E-Rezeptes

Date: Sun, 20 Jun 2021 11:12:13 +0100
From: ArztABC@abc.kim.telematik
To: Apotheke123@xyz.kim.telematik
Subject: E-Rezept direkte Zuweisung Zytostatikum
X-KIM-Dienstkennung: eRezept;Zuweisung;V1.0
Disposition-Notification-To: ArztABC@abc.kim.telematik
Return-Path: <ArztABC@abc.kim.telematik>
Message-ID: <th1s1s43me55ageld@abc.kim.telematik>
MIME-Version: 1.0
Content-Type: multipart/mixed;boundary=boundarymultipartseparator42

This is a multi-part message in MIME format.

```
--boundarymultipartseparator42
Content-Type: text/plain;charset=UTF-8
```

Sehr geehrte Apotheke
TextTextTextTextTextTextTextTextTextText
TextTextTextTextTextTextTextTextTextTextText
TextTextTextTextTextTextTextTextTextTextText

```
Mit den besten Gruessen
Aerztin Mueller
--boundarymultipartseparator42
Content-Type: text/plain;charset=UTF-8

Task/4711/$accept?ac=777bea0e13cc9c42ceec14ae
c3dde2263325dc2c6c699db115f58fe423607ea
--boundarymultipartseparator42
Content-Type: application/pdf; name="therapieplan.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=therapieplan.pdf
```

```
JVBERi0xLjQKJcDIzNINCjEgMCBvYmoKPDwKL1RpdGx1I
ChuZXcgMikKL0Fl1dGhvcjAoaGVuZHZHJpay5qYWJs25za2
kpCi9DcmVhdG9yICchwZGZGYWN0b3J5IFBybyBwZGZmYWwN
0b3J5LmNvbSkKL1Byb2RlY2VyICchwZGZGYWN0b3J5IFBy
byA2LjM2IFwoV2luZG93cyAxMCB4NjQgR2VybyBWFuXCkpC
i9DcmVhdGlvbkrRhdGUgKEQ6MjAyMTA2MTcxMDA2MTUrMD
InMDANkQo+PgplbmRvYmoKNSAwIG9iago8PC9GaWw0ZXI
vRmxhdGEZGZWNvZGUgL0xlbmd0aCAxNTI+PnN0cmVhbQ0K
SIlVj00wJAMhPc8xY1lMXbaJM2KAIkRKS8QoRaEKCoRC
29P+AktOnnx5/PdDfJWOsIYauG8p1pDNxAmY5E69GoV1H
Ir8OQtQq8yQJnia1kTtwjrvOXsDgdUAmCBcFaboH4pzn9
T8rVohghx84kRP2N2TjSbidTG0R/N9Rgv1fdTmWqHOCdi
fupSHB8YL/FKpdMeTy9DntcKZW5kc3RyZWFTcmVuZG9ia
go0IDAga2JqCjw8Ci9UeXB1L1BhZ2UKL1BhcmVudCAzID
AgUgovTWVkaWFCb3hbMCAwIDU5NSA4NDJdCi9SZXNvdXJ
jZXM8PAovUHVhYVY1NldFsvUERGL1RleHRdCi9Gb250PDwv
RjEgNiAwIFI+PgogPgogQ29udGVudHMgNSAwIFIkPj4KZ
W5kb2JqCjYgMCBvYmoKPDwKL1R5cGUvRm9udAovU3VidH
lwZS9UcnVlVHlwZQovQmFzZUZvbnQgL0NvdXJpZXJ0ZXd
QU01UCi90YW11L0Yxci9GaXJzdENoYXJzIGZIKL0xhc3RD
aGFyIDI1NQovV21kdGhzIFs2MDAgNjAwIDYwMCA2MDAgN
jAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MD
AgNjAwIDYwMCA2MDAKNjAwIDYwMCA2MDAgNjAwIDYwMCA
2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYw
MCA2MDAgNjAwCjYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwI
DYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNj
AwIDYwMAo2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDA
gNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2
MDAKNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwM
CA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwCj
YwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjA
wIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMAo2MDAg
NjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2M
DAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAKNjAwIDYwMC
A2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDY
wMCA2MDAgNjAwIDYwMCA2MDAgNjAwCjYwMCA2MDAgNjAw
IDYwMCA2MDAgNjAwIDYwMAo2MDAgNjAwIDYwMCA2MD
AgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA
2MDAgNjAwIDYwMCA2MDAKNjAwIDYwMCA2MDAgNjAwIDYw
MCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwI
DYwMCA2MDAgNjAwCjYwMCA2MDAgNjAwIDYwMCA2MDAgNj
AwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDA
```

```
gNjAwIDYwMAo2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2
MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwM
CA2MDAKNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjAwID
YwMCA2MDAgNjAwIDYwMCA2MDAgNjAwIDYwMCA2MDAgNjA
wXQovRW5jb2RpbmV2luQW5zaUVuY29kaW5nCi9Gb250
RGVzY3JpcHRvcia3IDAgUgo+PgplbmRvYmoKNyAwIG9ia
go8PAovVHlwZS9Gb250RGVzY3JpcHRvcgovRm9udE5hbW
UgL0NvdXJpZXJOZXdQU01UCi9GbGFncyAzNQovRm9udEJ
Cb3hbLTEyMiAtNjgwIDYyMyAxMDIxXQovU3RlbVYgMzAw
Ci9JdGFsaWNBbmdsZSAwCi9DYXBIZWlnaHQgODMzCi9Bc
2NlbnQgODMzCi9EZXNjZW50IC0zMdAKPj4KZW5kb2JqCj
MgMCAvYmoKPDwKL1R5cGUvUGFnZXMKL0NvdW50IDEKL0t
pZHNbnCAwIFJdCj4+CmVuZG9iaGoyIDAgb2JqCjw8L1R5
cGUvQ2F0YWxvZyAvUGFnZXMKgMyAwIFlgl1BhZ2VMYXlvd
XQvU2luZ2xlUGFnZSAvVmlld2VyUHJlZmVyZW5jZXMKgOC
AwIFI+PgplbmRvYmoKOCAwIG9iaGo8PC9UeXB1L1ZpZXd
lc1ByZWZlcmVuY2VzPj4KZW5kb2JqCnhyZWYKMCA5CjAw
MDAwMDAwMDAgNjU1MzUgZg0KMDAwMDAwMDAxNiAwMDAwM
CBuDQowMDAwMDAxODc3IDAwMDAwIG4NCjAwMDAwMDE4Mj
IgMDAwMDAgbg0KMDAwMDAwMDQ0MCAwMDAwMCBuDQowMDA
wMDAwMjE5IDAwMDAwIG4NCjAwMDAwMDA1ODAgMDAwMDAg
bg0KMDAwMDAwMTY0NyAwMDAwMCBuDQowMDAwMDAxOTcxI
DAwMDAwIG4NCnRyYWlsZXIKPDwKL1NpemUgOQovSW5mbY
AxIDAgUgovUm9vdCAyIDAgUgovSURbPDREMzgyQkZENEf
GQzZDMEUxQzRGRUI0NjFCQ0NGOUYzPjw0RDM4MkJGRDRB
RkM2QzBFMUM0RkVCNDYxQkNDRj1GMz5dCj4+CnN0YXJ0e
HJlZgoyMDE0CiU1RU9GCg==
--boundarymultipartseparator42--
```

Beispiel für eine E-Rezept-spezifische KIM-MESSAGE für die Kommunikation zu einem E-Rezept

```
Date: Mon, 21 Jun 2021 11:12:13 +0100
From: Apotheke123@xyz.kim.telematik
To: ArztABC@abc.kim.telematik
Subject: E-Rezept Kommunikation
X-KIM-Dienstkennung: eRezept;Kommunikation;V1.0
Disposition-Notification-To: Apotheke123@xyz.kim.telematik
Return-Path: <Apotheke123@xyz.kim.telematik>
Message-ID: <thls1s43me55ag12a@xyz.kim.telematik>
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
```

Sehr geehrte Praxis
TextTextTextTextTextTextTextText
TextTextTextTextTextTextTextTextText
TextTextTextTextTextTextTextTextText

Mit den besten Gruessen
Apotheke 123

5.45.5 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	Lokalisierungsinformationen
Identity Provider: 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 /Task/\$create)	https://simplifier.net/erezept-workflow/gemerxtask
E-Rezept-ID	Task.identifizier 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	Verordnungsdatenschnittstell e 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.identifizier 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	https://simplifier.net/erezept-workflow/accesscode

	scannen oder E-Rezept-Nachricht (GET /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, die einen Data-Matrix-Code gemäß securPharm-System besitzen, 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
AVS	Apothekenverwaltungssystem
BMV	Bundesmantelvertrag
BSI	Bundesamt für Sicherheit in der Informationstechnik
DD	Discovery Document
DMC	Data-Matrix-Code
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
MVO	Mehrfachverordnung
PS	Primärsystem
PTV	Produkttypversion
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 Krankenversicherungsnummer (KVNR).

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

7.3 Abbildungsverzeichnis

Abbildung 1 : ABB_ILFERP_001 – Systemzerlegung	9
Abbildung 2 : ABB_ILFERP_002 – Statusübergänge	12
Abbildung 1 : ABB_ILFERP_001 – Systemzerlegung	9
Abbildung 2 : ABB_ILFERP_002 – Statusübergänge	12

7.4 Tabellenverzeichnis

Tabelle 1 : TAB_ILFERP_001 – E-Rezept-Status	11
Tabelle 2 : TAB_ILFERP_014 – HTTP-Header "X-erp-resource"	17
Tabelle 3 TAB_ILFERP_012 – Zertifikatsnutzung	19
Tabelle 4 : TAB_ILFERP_002 – E-Rezept durch Verordnenden erstellen	27
Tabelle 5 : TAB_ILFERP_003 – E-Rezept durch Verordnenden einstellen	31
Tabelle 6 : TAB_ILFERP_004 – E-Rezept durch Verordnenden löschen	33
Tabelle 7 : TAB_ILFERP_005 – E-Rezept abrufen	34
Tabelle 8 : TAB_ILFERP_006 – Quittung abrufen	37
Tabelle 9 : TAB_ILFERP_007 – Quittung erneut abrufen	39
Tabelle 10 : TAB_ILFERP_008 – E-Rezept durch Abgebenden zurückgeben	40
Tabelle 11 : TAB_ILFERP_009 – E-Rezept durch Abgebenden löschen	41
Tabelle 12 : TAB_ILFERP_010 – Nachrichten von Versicherten empfangen	43
Tabelle 13 : TAB_ILFERP_015 – Nachricht von Versicherten empfangen – payload	45
Tabelle 14 : TAB_ILFERP_011 – Nachricht an Versicherten versenden	46
Tabelle 15 : TAB_ILFERP_016 – Nachricht an Versicherten versenden – payload	48
Tabelle 16 : TAB_ILFERP_013 – Nachricht durch Abgebenden löschen	49
Tabelle 1 : TAB_ILFERP_018 – Fachliche und technische Konzepte	8
Tabelle 2 : TAB_ILFERP_001 – E-Rezept-Status	11
Tabelle 3 : TAB_ILFERP_014 – HTTP-Header "X-erp-resource"	17
Tabelle 4 TAB_ILFERP_012 – Zertifikatsnutzung	19
Tabelle 5 : TAB_ILFERP_002 – E-Rezept durch Verordnenden erstellen	27
Tabelle 6 : TAB_ILFERP_003 – E-Rezept durch Verordnenden einstellen	31
Tabelle 7 : TAB_ILFERP_004 – E-Rezept durch Verordnenden löschen	33
Tabelle 8 : TAB_ILFERP_005 – E-Rezept abrufen	34
Tabelle 9 : TAB_ILFERP_006 – Quittung abrufen	37
Tabelle 10 : TAB_ILFERP_007 – Quittung erneut abrufen	39
Tabelle 11 : TAB_ILFERP_008 – E-Rezept durch Abgebenden zurückgeben	40
Tabelle 12 : TAB_ILFERP_009 – E-Rezept durch Abgebenden löschen	41
Tabelle 13 : TAB_ILFERP_010 – Nachrichten von Versicherten empfangen	43
Tabelle 14 : TAB_ILFERP_015 – Nachricht von Versicherten empfangen – payload	45
Tabelle 15 : TAB_ILFERP_011 – Nachricht an Versicherten versenden	46
Tabelle 16 : TAB_ILFERP_016 – Nachricht an Versicherten versenden – payload	48
Tabelle 17 : TAB_ILFERP_013 – Nachricht durch Abgebenden löschen	49

Tabelle 18 : TAB_ILFERP_xxx – Abrechnungsinformation bereitstellen	53
Tabelle 19 : TAB_ILFERP_xxx – Abrechnungsinformation ändern	54
Tabelle 20 : TAB_ILFERP_xxx – Abrechnungsinformation abrufen	56
Tabelle 21: TAB_ILFERP_017 – Subscription für neue Communication	57

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
[gemF_eRp_MVO]	gematik: Feature: E-Rezept: Mehrfachverordnung
[gemF_eRp_PKV]	gematik: Feature: E-Rezepte für PKV-Versicherte: apothekenpflichtige Arzneimittel
[gemF_eRp_WF_LE]	gematik: Feature: E-Rezept: Workflow-Steuerung durch Leistungserbringer
[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
[Split-DNS]	Split-horizon DNS https://en.wikipedia.org/wiki/Split-horizon_DNS