

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

Elektronische Gesundheitskarte und Telematikinfrastuktur

Systemspezifisches Konzept E-Rezept

Version: 1.0.0 CC6
Revision: 231181
Stand: 30.04.2020
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSysL_eRp

26

Dokumentinformationen

Änderungen zur Vorversion

Überarbeitung des Dokuments: siehe Dokumentenhistorie.

29

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0 CC	20.09.2019		zur Abstimmung freigegeben	gematik
1.0.0 CC2	31.01.2020		umfangreiche Überarbeitung: – Verarbeitung der E-Rezeptdaten in strukturierter Form in einer vertrauenswürdigen Ausführungsumgebung (VAU) – Verzicht auf Pseudonymisierung der Identität des Versicherten und der LEI – Verlagerung der Protokollierung und des Nachrichtendienstes in den E-Rezept- Fachdienst – Verzicht auf zentrale Autorisierung (IdP bleibt bestehen, Autorisierung erfolgt in den Diensten)	gematik
1.0.0 CC5	17.03.2020		– UC 3.3 und 4.6: statt "E-Rezept-Token" > "Nachrichten"	gematik
1.0.0 CC6	30.04.2020		– Anpassung Inhalte E-Rezept-Token, Prüfung Leistungserbringer-Typ, Anpassung Löschfristen E-Rezept – zusätzlicher Anwendungsfall für die abgebende LEI „UC 4.8 - Quittung erneut abrufen“	gematik

Inhaltsverzeichnis

31		
32	1 Einordnung des Dokuments	6
33	1.1 Zielsetzung	6
34	1.2 Zielgruppe	6
35	1.3 Geltungsbereich	6
36	1.4 Abgrenzung des Dokuments	6
37	1.5 Methodik	7
38	1.5.1 Anforderungen	7
39	1.5.2 Hinweis auf offene Punkte	7
40	2 Systemüberblick	8
41	2.1 Einführung	8
42	2.2 Übergeordnete Ziele	9
43	2.2.1 Sicherheit und Datenschutz	9
44	2.2.2 Datenhoheit und Flexibilität	9
45	2.2.3 Erweiterbarkeit	10
46	2.2.4 Betrieb	10
47	2.3 Akteure und Rollen	10
48	2.3.1 Fachliche Rollen	10
49	2.3.2 Technische Rollen	14
50	2.4 Funktionale Zerlegung	14
51	2.4.1 Konzept Identifikation und Zugang zum E-Rezept	16
52	2.4.2 Konzept Zugriffsberechtigung auf E-Rezepte	17
53	2.4.3 Konzept der E-Rezept-Ressourcenverwaltung	18
54	2.4.4 Konzept der Verschlüsselung des E-Rezepts	19
55	2.4.5 Konzept der Übermittlung eines E-Rezept-Tokens	19
56	2.4.6 Konzept Status E-Rezept	20
57	2.4.7 Unterstützung betrieblicher Prozesse	22
58	3 Anwendungsfälle	26
59	3.1 Übersicht der Anwendungsfälle	26
60	3.2 Übergreifende Vorbedingungen	26
61	3.3 Übergreifende Nachbedingungen	27
62	3.4 E-Rezept ausstellen	27
63	3.4.1 E-Rezepte durch Verordnenden erzeugen	27
64	3.4.2 E-Rezept einstellen	28
65	3.4.3 E-Rezept-Token durch Verordnenden an Versicherten oder Apotheker	
66	übermitteln	30
67	3.4.4 E-Rezept durch Verordnenden löschen	31
68	3.5 E-Rezept durch Versicherten verwalten	32
69	3.5.1 E-Rezepte durch Versicherten abrufen	32
70	3.5.2 E-Rezept durch Vertreter abrufen	33
71	3.5.3 E-Rezept durch Versicherten löschen	34
72	3.5.4 Nachricht durch Versicherten an Abgebenden übermitteln	35

73	3.5.5 E-Rezept-Token durch Versicherten an Vertreter übermitteln.....	37
74	3.5.6 Nachrichten durch Versicherten empfangen.....	37
75	3.5.7 Protokolldaten durch Versicherten einsehen.....	38
76	3.6 E-Rezept in Apotheke einlösen	39
77	3.6.1 Nachrichten durch Abgebenden empfangen	39
78	3.6.2 Nachricht durch Abgebenden an Versicherten übermitteln	40
79	3.6.3 E-Rezept durch Abgebenden abrufen	41
80	3.6.4 E-Rezept durch Abgebenden zurückgeben	43
81	3.6.5 E-Rezept durch Abgebenden löschen	44
82	3.6.6 Quittung abrufen.....	46
83	3.6.7 Quittung erneut abrufen	47
84	3.6.8 Dispensierdatensatz durch Abgebenden signieren	49
85	3.7 Anfordern von Identitätsbestätigungen.....	50
86	3.7.1 Identitätsbestätigung durch den Versicherten anfordern	50
87	3.7.2 Identitätsbestätigung durch LEI anfordern.....	52
88	4 Systemzerlegung (Deployment)	55
89	4.1 Produkttypen der Fachanwendung E-Rezept	56
90	4.1.1 Produkttyp E-Rezept-Fachdienst	56
91	4.1.1.1 Vertrauenswürdige Ausführungsumgebung	60
92	4.1.1.2 Betriebliche Aspekte	61
93	4.1.2 Produkttyp E-Rezept-Frontend des Versicherten.....	62
94	4.1.3 Primärsysteme.....	64
95	4.1.3.1 Primärsystem verordnender Leistungserbringer.....	65
96	4.1.3.2 Primärsystem abgebender Leistungserbringer	66
97	4.2 Fachanwendungsübergreifende Produkttypen.....	68
98	4.2.1 Produkttyp Identity Provider.....	68
99	4.2.1.1 Funktionale Anforderungen	68
100	4.2.1.2 Betriebliche Aspekte	70
101	4.2.2 Authentisierungsmodul	71
102	4.2.3 Produkttyp Verzeichnisdienst der TI.....	72
103	4.3 Schnittstelle der Fachanwendung E-Rezept.....	72
104	4.3.1 Schnittstelle für die Ressource E-Rezept	72
105	4.3.2 Schnittstelle für die Ressource E-Rezept-Nachricht	81
106	4.3.3 Schnittstelle für die Ressource Zugriffsprotokolleintrag	82
107	4.3.4 Schnittstelle für die Ressource signierte Challenge	82
108	4.3.5 Schnittstelle für die Ressource Einwilligung	83
109	5 Datenschutz- und Sicherheitsaspekte	84
110	5.1 Anforderungen an den E-Rezept-Fachdienst.....	85
111	5.1.1 Anforderungen an die Vertrauenswürdige Ausführungsumgebung	87
112	5.1.2 Verarbeitungskontext	87
113	5.1.3 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	88
114	5.1.4 Trennung von Session- und Request-Kontexten	90
115	5.2 Anforderungen an das E-Rezept-Frontend des Versicherten.....	91
116	5.3 Anforderungen an den Identity Provider	91
117	5.4 Grenzen der Sicherheitsleistung der Fachanwendung E-Rezept	92
118	6 Informationsmodell	94

119	6.1 Technisches Informationsmodell	94
120	6.2 Fachliches Informationsmodell.....	95
121	7 Anhang – Verzeichnisse	96
122	7.1 Abkürzungen	96
123	7.2 Glossar	97
124	7.3 Abbildungsverzeichnis.....	98
125	7.4 Tabellenverzeichnis	98
126	7.5 Referenzierte Dokumente.....	100
127	7.5.1 Dokumente der gematik.....	100
128	7.5.2 Weitere Dokumente.....	101
129		
130		

1 Einordnung des Dokuments

1.1 Zielsetzung

Das vorliegende Dokument beschreibt die systemspezifische Lösung der Fachanwendung E-Rezept.

In diesem systemspezifischen Konzept werden insbesondere die Komponenten der Lösung von E-Rezept sowie ihre Schnittstellen untereinander und mit der Telematikinfrastruktur-Plattform beschrieben. Dieses Dokument bildet somit die Grundlage für die Spezifikationen, Produkttyp- und Anbietersteckbriefe der Komponenten der Fachanwendung E-Rezept.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter der Produkttypen der Fachanwendung E-Rezept.

1.3 Geltungsbereich

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

Wichtiger Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass das Konzept 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 Abgrenzung des Dokuments

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zu den Themenbereichen:

- fachliche Inhalte des Informationsmodells für die Fachanwendung E-Rezept (siehe auch 6.2- Fachliches Informationsmodell)
- Prozesse für die Abrechnung von E-Rezepten der abgebenden Leistungserbringerinstitutionen gegenüber den Kostenträgern

165 1.5 Methodik

166 1.5.1 Anforderungen

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

171 Sie werden im Dokument wie folgt dargestellt:

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

173 **Text / Beschreibung**

174 **[<=]**

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

177 1.5.2 Hinweis auf offene Punkte

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

180 *Beispiel für einen offenen Punkt.*

2 Systemüberblick

2.1 Einführung

Die Fachanwendung E-Rezept ermöglicht eine Übermittlung von ärztlichen und zahnärztlichen Verordnungen für apothekenpflichtige Arzneimittel in elektronischer Form. Sie setzt sich aus den in ABB_SYSLERP_001 dargestellten Bestandteilen zusammen.

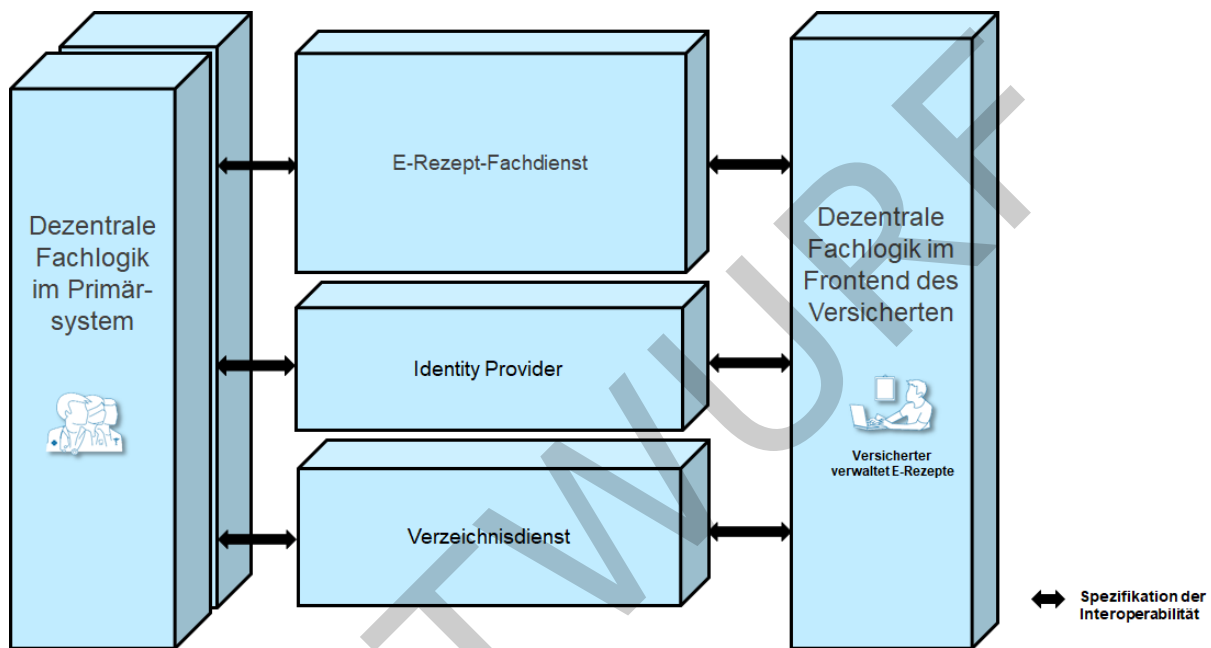


Abbildung 1: ABB_SYSLERP_001 Übersicht der Fachanwendung E-Rezept

Der verordnende Leistungserbringer erstellt für einen Versicherten ein E-Rezept, welches auf dem zentralen E-Rezept-Fachdienst abgelegt wird. Der Standardfall sieht vor, dass der Versicherte seine E-Rezepte mit dem E-Rezept-Frontend auf seinem technischen Gerät verwaltet. Mit dem E-Rezept-Frontend kann der Versicherte einen E-Rezept-Token generieren, der eine Apotheke für den Zugriff auf ein konkretes E-Rezept im E-Rezept-Fachdienst berechtigt. Der Versicherte übermittelt den E-Rezept-Token elektronisch an eine Apotheke oder legt ihn in Form eines 2D-Codes in einer Apotheke vor. Die elektronische Übertragung des E-Rezept-Tokens an eine Apotheke erfolgt über den E-Rezept-Fachdienst.

Für Versicherte, welche kein E-Rezept-Frontend nutzen, erstellt der verordnende Leistungserbringer den E-Rezept-Token und übergibt ihn in Form eines 2D-Code auf einem Ausdruck dem Versicherten. Der Ausdruck kann in einer Apotheke vorgelegt werden.

Durch die Übergabe eines E-Rezept-Token an eine andere Person kann diese als Vertreter das E-Rezept in einer Apotheke einlösen.

Der Versicherte hat die Hoheit über das E-Rezept, da jeglicher Zugriff auf ein konkretes Rezept im E-Rezept-Fachdienst entweder nur dem Versicherten, dem das E-Rezept verordnet wurde, oder einer Apotheke oder einem Vertreter nach Vorlage eines im E-Rezept-Token enthaltenen AccessCodes gestattet ist. Der E-Rezept-Token realisiert ein

207 Besitzmodell, d.h. wer im Besitz des E-Rezept-Tokens und damit des AccessCodes ist,
208 kann damit die Dispensierung in einer Apotheke veranlassen.

209 Mit der Übergabe bzw. dem Einlesen des E-Rezept-Tokens an einen/durch einen
210 Apotheker erfolgt die Aufforderung zur Dispensierung. Der Apotheker lädt das E-Rezept
211 vom zentralen E-Rezept-Fachdienst und verarbeitet es. Zugriffe auf den E-Rezept-
212 Fachdienst werden im E-Rezept-Fachdienst protokolliert und sind durch den jeweils
213 betroffenen Versicherten einsehbar.

214 Die dezentrale E-Rezept-Fachlogik wird im Primärsystem der verordnenden und
215 abgebenden Leistungserbringer und im E-Rezept-Frontend des Versicherten (FdV)
216 umgesetzt. Alle Client-Systeme nutzen Dienste der zentralen TI-Plattform, wobei die
217 Primärsysteme der Leistungserbringer zusätzlich auf Funktionalitäten des Konnektors
218 zurückgreifen.

219 In der TI gibt es genau einen Anbieter für den E-Rezept-Fachdienst und einen Anbieter
220 für das E-Rezept-Frontend des Versicherten.

221 Das E-Rezept-Frontend des Versicherten muss diskriminierungsfrei, werbefrei und
222 unabhängig sein.

223 Für den Zugang zum E-Rezept-Fachdienst nutzt der Versicherte seine eGK mit NFC-
224 Schnittstelle, sodass eine Nutzung des E-Rezepts auch ohne weitere Hardware an den
225 Geräten des Versicherten möglich ist.

226 2.2 Übergeordnete Ziele

227 2.2.1 Sicherheit und Datenschutz

228 Die Fachanwendung E-Rezept muss sicherstellen, dass nur berechtigte Akteure auf
229 medizinische personenbezogene Daten vom E-Rezept zugreifen dürfen. Sie muss
230 sicherstellen, dass die Daten der Fachanwendung E-Rezept beim Anbieter und Betreiber
231 beteiligter Komponenten nicht für Zwecke der Profilbildung verarbeitet werden können.
232 Die Fachanwendung E-Rezept muss ferner sicherstellen, dass die Sicherheit der TI durch
233 die Nutzung der Fachanwendung E-Rezept nicht beeinträchtigt wird.

234 Eine Identifikation von Akteuren soll nur da erfolgen, wo sie notwendig ist. Beispielsweise
235 ist es heute mit dem Papier-Rezept nicht notwendig, dass sich die einlösende Person in
236 der Apotheke ausweist.

237 2.2.2 Datenhoheit und Flexibilität

238 Die Fachanwendung E-Rezept soll die Flexibilität des Papier-Rezepts bewahren. Der
239 Versicherte muss die Apotheke, in der das E-Rezept eingelöst wird, frei wählen können.
240 Das Einlösen durch Dritte ist explizit erlaubt. Das Delegieren an Vertreter soll leicht und
241 flexibel erfolgen können.

242 In der Fachanwendung E-Rezept erfolgt eine Trennung zwischen medizinischen Daten (E-
243 Rezept) und der Berechtigung auf den Zugriff auf die medizinischen Daten (E-Rezept-
244 Token). Der Besitz des E-Rezept-Tokens soll einzige Voraussetzung für die Autorisierung
245 zum Einlösen des E-Rezepts sein.

246 Versicherte müssen das E-Rezept auch ohne eigene technische Geräte und
247 Softwarekomponenten einlösen können. Ein zusätzliches durch den Versicherten
248 genutztes Frontend des Versicherten kann jedoch den Komfort der Anwendung heben.

2.2.3 Erweiterbarkeit

Die Fachanwendung E-Rezept soll um weitere Rezepttypen (bspw. Heilmittel, Hilfsmittel, T-Rezepte oder BtM-Rezepte) erweiterbar sein.

2.2.4 Betrieb

Die Fachanwendung E-Rezept muss für Nutzer eine ihrem Bedarf entsprechende angemessene Funktionalität, Verfügbarkeit, Stabilität und Zuverlässigkeit, Performanz, Kontinuität und Vorhersehbarkeit der Anwendungsfälle des E-Rezepts sicherstellen. Die Produkttypen E-Rezept-Fachdienst und Identity Provider (IdP) und die damit zusammenfallenden technischen Systeme und Komponenten müssen entsprechende Schnittstellen zur Prüfung dieser Aspekte vorsehen. Die Betreiber bzw. Anbieter der operativen Betriebsleistungen dieser Produkttypen sind für die Überwachung, Prüfung, Analyse und Aufrechterhaltung der genannten Aspekte verantwortlich.

2.3 Akteure und Rollen

Im folgenden Abschnitt werden die am E-Rezept beteiligten Akteure/Rollen betrachtet. Ein Akteur ist eine Person oder ein technisches System, die/das mit der Fachanwendung E-Rezept interagiert. Diese Interaktion wird durch einen Anwendungsfall ausgelöst.

Akteure innerhalb der Fachanwendung E-Rezept sind jedoch keine konkreten beteiligten Personen oder Systeme, sondern Rollen, die jene im Rahmen des Anwendungsfalles einnehmen. Insofern kann eine Person oder ein technisches System in mehreren Rollen mit dem E-Rezept-System interagieren.

2.3.1 Fachliche Rollen

Die folgende Abbildung stellt die im Kontext der Fachanwendung E-Rezept beteiligten Rollen dar.

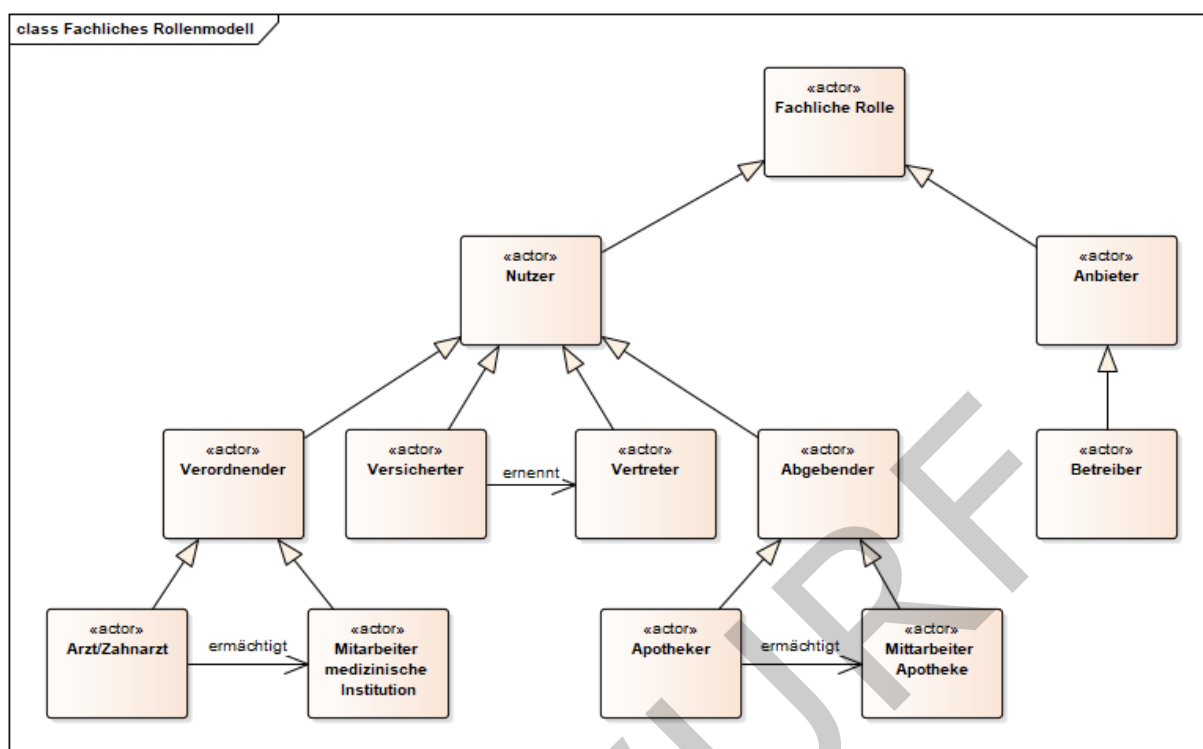


Abbildung 2: ABB_SYSLERP_002 Fachliches Rollenmodell

Tabelle 1 : TAB_SYSLERP_048 Fachliche Rollen

Rolle	Beschreibung
Versicherter	<ul style="list-style-type: none"> Ein Versicherter ist eine Person, die in einem Versicherungsverhältnis mit einer gesetzlichen Krankenkasse steht und eine eGK besitzt.
Vertreter	<ul style="list-style-type: none"> Ein Vertreter ist die Person, die für den Versicherten bestimmte Anwendungsfälle in Bezug auf die Anwendung E-Rezept durchführen kann. Die Voraussetzung ist hierfür der Besitz des E-Rezept-Tokens für das jeweilige E-Rezept. Der Vertreter muss nicht in einem Versicherungsverhältnis mit einer gesetzlichen Krankenkasse stehen. Im Kontext der Fachanwendung E-Rezept ist die technische Autorisierung des Vertreters gegenüber der TI nicht notwendig.

Verordnende Akteure - Arzt, Zahnarzt	<ul style="list-style-type: none"> Ein (Zahn-)Arzt ist ein approbierter Heilberufler und aufgrund seiner Mitgliedschaft in einer (Zahn-)Ärztekammer im Besitz eines HBA. Er ist befugt, vertragsärztliche Verordnungen am PVS zu erzeugen, mit einer QES zu versehen und diese als E-Rezept in der TI bereitzustellen. Die hier zu berücksichtigenden (Zahn-)Ärzte sind immer einer Institution zuzuordnen (z. B. eigene Praxis, med. Berufsausübungsgemeinschaft, MVZ, Krankenhaus).
Verordnende Akteure - Mitarbeiter medizinische Institution	<ul style="list-style-type: none"> Ein „Mitarbeiter medizinische Institution“ arbeitet in einer Institution zur medizinischen Versorgung (z. B. einer Praxis, med. Berufsausübungsgemeinschaft, MVZ, Krankenhaus) auf Weisung des verantwortlichen Vorgesetzten als berufsmäßiger Gehilfe des Arztes/Zahnarztes oder zur Vorbereitung auf den Beruf.
Abgebende Akteure - Apotheker und pharmazeutisches Personal	<ul style="list-style-type: none"> Ein Apotheker ist ein approbierter Heilberufler, der im Besitz eines HBA ist. Pharmazeutisches Personal (Pharmazieingenieure und Apothekerassistenten), das zur Vertretung des Apothekenleiters gem. § 2 (7) ApBetrO beauftragt und im Besitz eines HBA ist. Sie sind befugt, Arzneimittel auf Grundlage eines E-Rezeptes abzugeben und die Abgabe mit einem fortgeschrittenen signierten Dispensierdatensatz im AVS zu dokumentieren. Im Falle einer Änderung am E-Rezept sind sie befugt, diese zusammen mit dem Dispensierdatensatz durch eine QES zu dokumentieren. Die hier benannten Akteure sind immer einer Institution zuzuordnen (z.B. öffentliche Apotheke (Haupt-/Filialapotheke), Versandapotheke als Bestandteil einer öffentlichen Apotheke, Krankenhausapotheke).

<p>Abgebende Akteure - Mitarbeiter Apotheke</p>	<ul style="list-style-type: none"> • Ein „Mitarbeiter Apotheke (abzeichnungsberechtigt)“ arbeitet in einer Apotheke (z.B. öffentliche Apotheke (Haupt-/Filialapotheken), Versandapotheke als Bestandteil einer öffentlichen Apotheke, Krankenhausapotheke) auf Weisung des verantwortlichen Vorgesetzten und ist zur Abgabe von Arzneimitteln auf Grundlage einer Verordnung befugt sowie abzeichnungsberechtigt. Die Dokumentation der Abgabe erfolgt durch eine fortgeschrittene Signatur des Dispensierdatensatzes. • Ein „Mitarbeiter Apotheke (nicht abzeichnungsberechtigt)“ arbeitet in einer Apotheke (z.B. öffentliche Apotheke (Haupt-/Filialapotheken), Versandapotheke als Bestandteil einer öffentlichen Apotheke, Krankenhausapotheke) auf Weisung bzw. unter Aufsicht des verantwortlichen Vorgesetzten und ist nicht berechtigt, Verordnungen abzuzeichnen, jedoch zu deren Entgegennahme, zur Vorbereitung der Arzneimittel zur Abgabe und nach Maßgabe des § 3 ApBetrO ggf. zur Abgabe der Arzneimittel befugt.
<p>Anbieter E-Rezept- Fachdienst, Anbieter anwendungsübergreifender Dienste</p>	<ul style="list-style-type: none"> • Die Anbieter der Produkttypen <ul style="list-style-type: none"> • E-Rezept-Fachdienst, • Identity Provider (IdP) sind Dienstleister, welche die operativen Betriebsleistungen für den jeweiligen Produkttyp in der TI erbringen. Die Anbieter verantworten die Betriebsführung des jeweiligen Produkttyps. • Der Anbieter E-Rezept-Fachdienst ist nicht zugriffsberechtigt auf die medizinischen Daten des E-Rezepts.
<p>Betreiber E-Rezept- Fachdienst, Betreiber anwendungsübergreifender Dienste</p>	<ul style="list-style-type: none"> • Der Betreiber eines der Produkttypen erbringt im Auftrag des Anbieters dessen organisatorische und technische Betriebsleistung. Der Betreiber nimmt für den Anbieter am TI-ITSM teil. • Der Betreiber E-Rezept-Fachdienst ist nicht zugriffsberechtigt auf die medizinischen Daten des E-Rezepts.

276 Die folgende Tabelle listet die für die Fachanwendung E-Rezept verwendeten
277 kryptografischen Identitäten auf und ordnet sie den verschiedenen Akteuren mit ihrer
278 jeweiligen Rolle zu.

Tabelle 2: TAB_SYSERP_001 Kryptografische Identitäten der Akteure und ihre jeweilige Rolle

Komponente	Identität (gem. [gemKPT_Arch_TIP #Anhang B])	Rolle	Verwendungszweck	Prüfende Komponente
SMC-B	ID.HCI.AUT	Mitarbeiter LEI	Authentisierung der LEI	Identityprovider LE
	ID.HCI.OSIG		Fortgeschrittene Signatur der LEI für E-Rezept/Dispensierdatensatz	Konnektor, Komponenten außerhalb der TI
HBA	ID.HP.QES	Verordnender, Abgebender	Qualifizierte elektronische Signatur des LE für E-Rezept	Konnektor, Komponenten außerhalb der TI
eGK	ID.CH.AUT	Versicherter, Vertreter	Authentisierung des Versicherten	Identity Provider Versicherter
E-Rezept-Fachdienst	ID.FD.TLS-S	Anbieter	TLS Server-Authentisierung	Clientsystem
	ID.C.FD.SIG		Signatur der Quittung	
Identity Provider	ID.FD.TLS-S	Anbieter	TLS Server-Authentisierung	Client System, E-Rezept-Fachdienst
	ID.C.FD.SIG		Signatur des AuthN-Token	

2.3.2 Technische Rollen

Neben den fachlichen Rollen existieren technische Rollen. Diese technischen Rollen kommen zum Tragen, wenn nicht eine Person mit dem System interagiert, sondern eine technische Komponente, ein Produkttyp der Fachanwendung E-Rezept oder das Primärsystem der Leistungserbringerumgebung. Die entsprechenden Produkttypen und Komponenten der Fachanwendung werden im Kapitel 4- Systemzerlegung.(Deployment) dargestellt.

2.4 Funktionale Zerlegung

Die folgende Abbildung zeigt die funktionale Zerlegung.

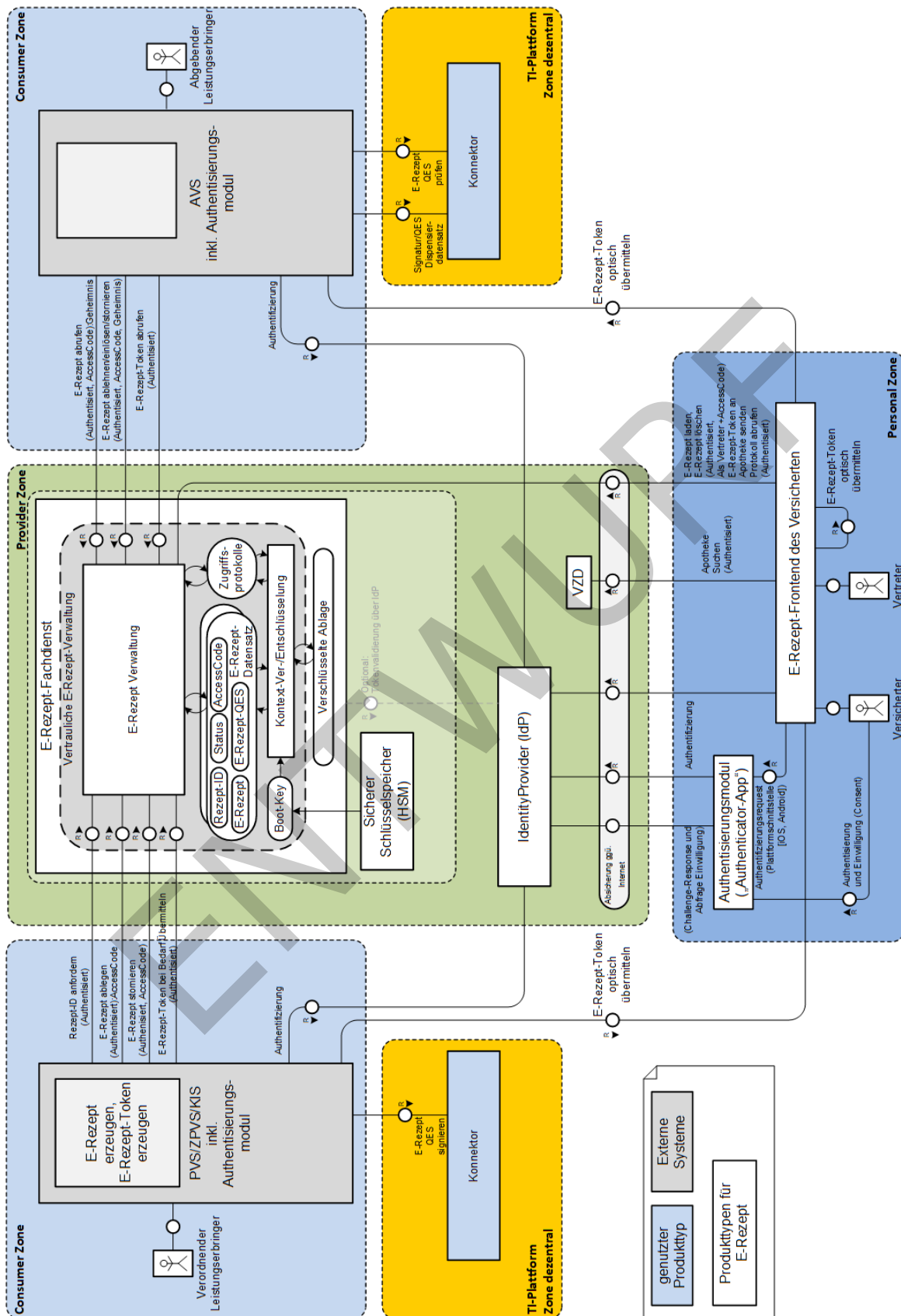


Abbildung 3: ABB_SYSLERP_003 Funktionale Zerlegung E-Rezept

2.4.1 Konzept Identifikation und Zugang zum E-Rezept

Der Zugang zur Fachanwendung E-Rezept erfolgt für die LEI mittels Konnektor in seiner Funktion als VPN-Router. Dieser enthält keine E-Rezept-spezifische Funktionalität, d.h. die Verbindung zu zentralen Diensten in der Provider-Zone und der TI-Plattform wird direkt durch die Client-Systeme aufgebaut. Der Versicherte greift auf die Schnittstellen der Dienste für das E-Rezept mittels des Frontends über das Internet zu.

Die Schnittstellen sind für den Nutzer ausschließlich nach einer erfolgreichen Authentifizierung durch einen Identity Provider (IdP) nutzbar, der die Identität des Versicherten bzw. der LEI über ein AuthN-Token als Identitätsbestätigung zusichert. Arzt-, Zahnarztpraxen, Krankenhäuser und Apotheken werden dabei über ihre Institutsidentität der jeweiligen SMC-B authentifiziert. Der Versicherte weist sich mit seiner eGK-Identität aus. Zukünftig werden neben der Authentisierung mit einer Smartcard auch alternative Verfahren zur Authentisierung ermöglicht.

Der IdP als TIP-Nutzerdienst übernimmt im zentralen Bereich die Authentifizierung des Nutzers. Ergänzt wird dieser durch ein Authentisierungsmodul, welches bei der LEI das Primärsystem bzw. beim Versicherten das E-Rezept-Frontend des Versicherten ergänzt. Das Authentisierungsmodul greift in der Consumer Zone bzw. Personal Zone auf die SMC-B bzw. eGK als Authentisierungsmittel (AUT-Identität) zu. Das Authentisierungsmodul steuert die Interaktion mit dem Nutzer, falls dies für die Authentisierung erforderlich ist oder eine Zustimmung (Consent) zur Freigabe von Identitätsmerkmalen an die Anwendung benötigt wird.

Nach erfolgreicher Authentifizierung durch den IdP erhält das Primärsystem bzw. das FdV ein AuthN-Token, welches als Bearer-Token verwendet wird, um auf die Dienste des E-Rezeptes zuzugreifen. Das AuthN-Token enthält die bestätigten Identitätsmerkmale, die der aufgerufene Dienst benötigt, um daraus die Berechtigung des Nutzers abzuleiten. Des Weiteren können dem Token erforderlichenfalls Identitätsattribute entnommen werden, die für die Fachlogik benötigt werden, z.B. zur Protokollierung.

Die folgende Abbildung zeigt eine Übersicht der an der Authentifizierung des Nutzers beteiligten Komponenten.

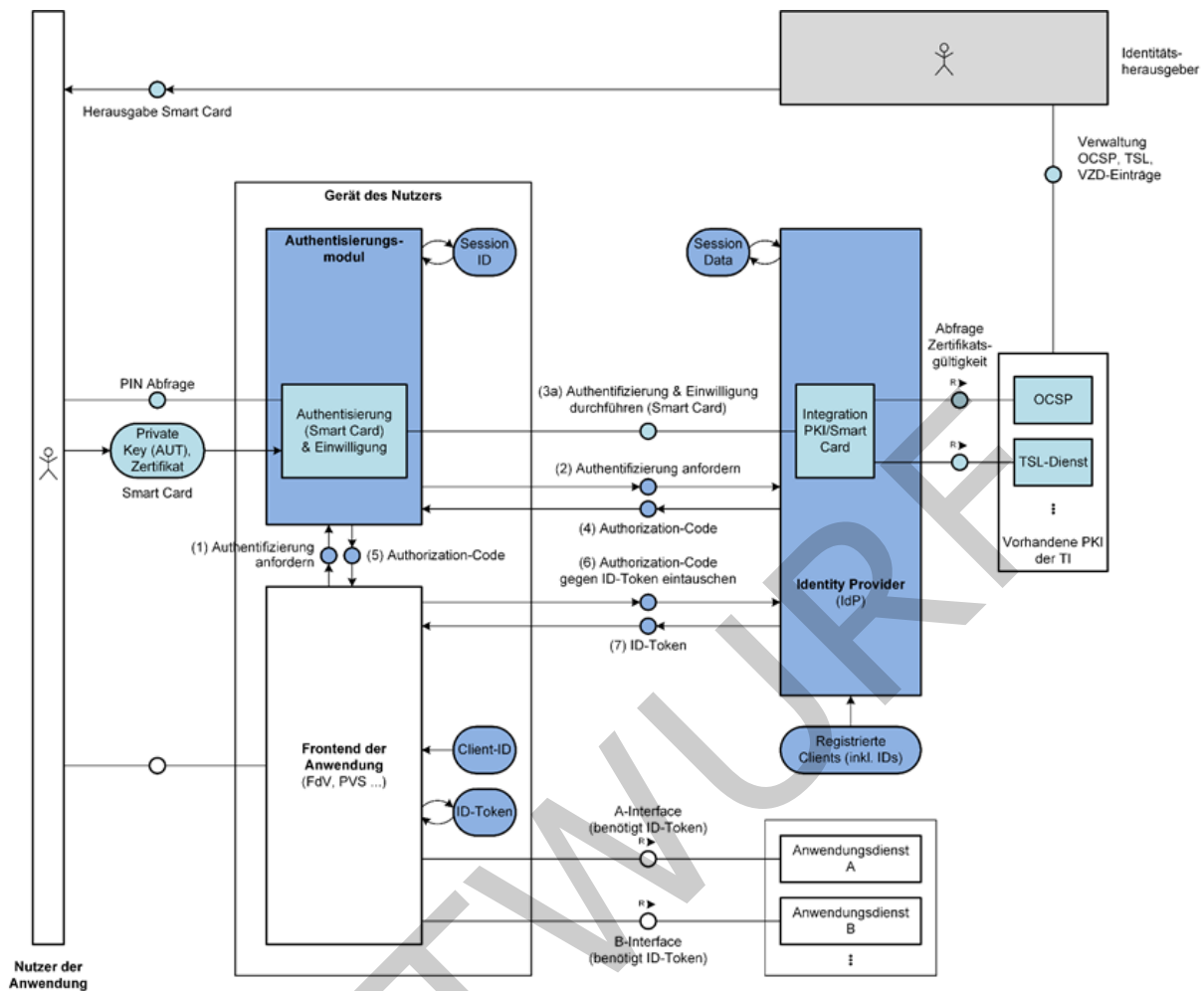


Abbildung 4 ABB_SYSLERP_009 Übersicht Identity Provider im Kontext E-Rezept

Der Authentifizierungsdienst (IdP) stellt der Fachlogik eines E-Rezept-Frontends eine Schnittstelle für den Bezug von Authentifizierungsbestätigungen bereit. Die Fachlogik nutzt dafür einen AuthN-Code, den sie über ein Authentisierungsmodul bezieht. Das Authentisierungsmodul steuert die konkrete Benutzerauthentifizierung gegenüber dem IdP unter Nutzung festgelegter bzw. durch den IdP prüfbare Identitätsmerkmale z.B. SmartCard + PIN.

2.4.2 Konzept Zugriffsberechtigung auf E-Rezepte

Alle Zugriffe auf Komponenten/Dienste und Schnittstellen für das E-Rezept setzen eine Identifikation der zugreifenden Nutzer voraus.

Um einen unberechtigten Zugriffe von E-Rezepten zu unterbinden und das Einlösen in einer ausgewählten Apotheke zu steuern, übermittelt der Versicherte eine Zugriffsberechtigung in Form eines AccessCodes an die Apotheke seiner Wahl. Nur durch Übergabe dieses AccessCodes beim Abruf eines E-Rezeptes erlangt diese Apotheke Zugriff auf genau dieses E-Rezept im E-Rezept-Fachdienst. Diesen AccessCode kann der Versicherte aus dem E-Rezept-Datensatz herunterladen und in einen E-Rezept-Token einbringen. Mit der Weitergabe dieses E-Rezept-Tokens an einen Vertreter kann der Versicherte das Einlösen eines E-Rezeptes an einen Dritten delegieren.

Das Einlösen in einer Apotheke setzt voraus, dass die Apotheke diesen AccessCode an den E-Rezept-Fachdienst beim Zugriff auf ein E-Rezept übermittelt. Der Versicherte oder Vertreter übergibt den AccessCode an die Apotheke durch Vorzeigen des E-Rezept-Tokens in der Apotheke oder mittels elektronischer Übermittlung in der TI an eine Versandapotheke (siehe 2.4.5- Konzept der Übermittlung eines E-Rezept-Tokens).

2.4.3 Konzept der E-Rezept-Ressourcenverwaltung

Die Verwaltung der E-Rezepte in der Telematikinfrastruktur setzt auf einen zentralen Ressourcenserver als E-Rezept-Fachdienst. Dieser soll alle E-Rezepte auf Basis des FHIR-Standards als MedicationRequests [FHIR] in strukturierter Form verwalten. Die Rezepte werden dabei über eine eindeutige Ressourcen-ID (Rezept-ID) adressiert. Zusätzlich protokolliert der E-Rezept-Fachdienst alle Zugriffe auf ein E-Rezept für den Versicherten und verwaltet die Statusübergänge eines E-Rezepts.

Mit der Verwaltung der E-Rezepte in strukturierter Form setzt der E-Rezept-Fachdienst die Einhaltung medizinischer Workflows durch. In der ersten Stufe der Umsetzung des "Muster 16" ist der Workflow relativ einfach. Mit der Umsetzung weiterer Verordnungstypen (Betäubungsmittel, Heil- und Hilfsmittel) kommen zusätzliche Beteiligte ins Spiel, die insbesondere bei Verordnungen mit Freigabezyklen (bspw. bei Hilfsmitteln durch Kostenträger und Gegenzeichnung einer absolvierten Maßnahme durch den Versicherten bei Heilmittelverordnungen) in den Verordnungsprozess eingebunden werden müssen. Hier lässt sich mit der Digitalisierung der fachlichen Workflows eine Zeitersparnis realisieren.

Mit der Erweiterung der E-Rezept-Ressourcen um MedicationStatements in einer zukünftigen Ausbaustufe wäre es Patienten zusätzlich möglich, auf eigenen Wunsch die Einnahme von Medikamenten über sein Frontend des Versicherten zu dokumentieren.

Zur Sicherstellung der Integrität des verwalteten, QES-signierten E-Rezepts als strukturierter Datensatz erfolgt beim Einstellen eines E-Rezepts eine Signatur der E-Rezept-Ressource durch den E-Rezept-Fachdienst, sofern die Daten der E-Rezept-Ressource schematisch und anhand der QES des E-Rezept-Datensatzes valide sind. Mit der serverseitigen QES-Prüfung wird sichergestellt, dass ausschließlich fachlich korrekte Daten, durch QES des Verordnenden bestätigt, in der Steuerung der fachlichen Workflows verwendet werden. Zusätzlich stellt die serverseitige QES-Prüfung sicher, dass ausschließlich signierte Rezepte der Apotheke zugewiesen werden, wodurch sich die Qualität der eingereichten Rezepte gegenüber einer ungeprüften Überbringung in die Apotheke steigert. Hier sind in der Folge weniger Korrekturschleifen zwischen Verordnendem Arzt/Zahnarzt und Apotheker zu erwarten.

Der E-Rezept-Fachdienst prüft die Autorisierung des Zugriffs auf E-Rezepte und Protokolleinträge anhand der Identitätsbestätigungen der zugreifenden Nutzer. Dabei wird die Rechtmäßigkeit eines Aufrufs durch Leistungserbringer auf Rollenbasis geprüft. Beim Aufruf durch den Versicherten zum Abruf "seiner" E-Rezepte und Protokollinformationen erfolgt die Autorisierung anhand der Versicherten-ID (10-stelliger unveränderlicher Teil der 30-stelligen Krankenversicherungsnummer (KVRN)) des Versicherten.

Das Einstellen von E-Rezepten ist verordnenden Leistungserbringern (Ärzte, Zahnärzte, etc.) und ihren Mitarbeitern gestattet. Hier genügt eine einfache Rollenprüfung anhand der Identität der Leistungserbringereinstitution. E-Rezepte abrufen und die Abgabe vollziehen dürfen ausschließlich Apotheken, deren Rolle ebenfalls anhand der Identität der Apotheke als Leistungserbringereinstitution geprüft wird. Zusätzlich erfordert das Abrufen eines E-Rezepts durch eine Apotheke die Vorlage des vom Versicherten an den

390 Apotheker übergebenen AccessCode, der beim Abruf des E-Rezepts mit dem am E-
391 Rezept-Datensatz gespeicherten AccessCode übereinstimmen muss.

392 Ist eine Apotheke für den Abruf eines E-Rezepts autorisiert, generiert der E-Rezept-
393 Fachdienst beim Abruf ein Geheimnis, das der Apotheke zusammen mit dem E-Rezept-
394 Datensatz übergeben wird. Der Zugriff auf genau dieses E-Rezept durch andere
395 Apotheken ist gesperrt, da die Apotheke das Geheimnis beim Zurückgeben des E-Rezepts
396 oder Abfragen der Quittung an den E-Rezept-Fachdienst übermitteln muss.

397 **2.4.4 Konzept der Verschlüsselung des E-Rezepts**

398 Der E-Rezept-Fachdienst verarbeitet die gespeicherten E-Rezepte im Klartext. Zum
399 Schutz der in den E-Rezepten enthaltenen personenbezogenen medizinischen Daten
400 muss eine unberechtigte Einsichtnahme durch Dritte verhindert werden. Hierfür wird das
401 für die elektronische Patientenakte (ePA) entwickelte Konzept der "Vertrauenswürdigen
402 Ausführungsumgebung" (VAU) aufgegriffen. Die VAU stellt technisch sicher, dass
403 während des Betriebs keine Daten für den Betreiber des E-Rezept-Fachdienstes
404 einsehbar sind. Zusätzlich erfolgt die Speicherung der Daten außerhalb der VAU derart
405 verschlüsselt, dass der Betreiber die Daten nicht entschlüsseln kann, da der notwendige
406 kryptographische Schlüssel nicht im Zugriff des Betreibers liegt. Gegenüber dem Nutzer
407 authentisiert sich die VAU beim Verbindungsaufbau mit einer kryptografischen Identität,
408 die dem Nutzer die Integrität der ausgeführten Fachlogik im E-Rezept-Fachdienst
409 zusichert.

410 Der Transport der personenbezogenen medizinischen Informationen zwischen der
411 Clientlogik des Nutzers und der Vertrauenswürdigen Ausführungsumgebung erfolgt
412 transportverschlüsselt mittels TLS.

413 Anmerkung:

414 Die Schutzziele der Vertrauenswürdigen Ausführungsumgebung im E-Rezept-Fachdienst
415 entsprechen denen der Vertrauenswürdigen Ausführungsumgebung der elektronischen
416 Patientenakte, mit einer Ausnahme. Das Schutzziel der Kontextseparierung in der ePA ist
417 im E-Rezept-Fachdienst nicht notwendig, da Versicherte keinen schreibenden Zugriff über
418 ihre Clientsysteme auf die E-Rezepte im E-Rezept-Fachdienst haben. Somit entfällt
419 gegenüber der VAU der ePA die Notwendigkeit eines versichertenindividuellen
420 Kontextschlüssels und ebenso ist ein Sandboxing der verarbeiteten Daten verschiedener
421 Versicherter während des Betriebs nicht erforderlich.

422 **2.4.5 Konzept der Übermittlung eines E-Rezept-Tokens**

423 Um ein E-Rezept einzusehen und beliefern zu können benötigt eine Apotheke einen
424 AccessCode, den sie vom Versicherten bzw. Vertreter übermittelt bekommt (Nachricht
425 innerhalb des E-Rezept-Fachdienstes an die Apotheke) bzw. von einem vorgelegten
426 Medium einscannt. Dieser AccessCode plus weitere Metainformationen (Rezept-ID etc.)
427 formen den E-Rezept-Token.

428 Im Standardfall lädt der Versicherte die für das E-Rezept-Token benötigten
429 Informationen aus dem E-Rezept-Fachdienst und generiert den E-Rezept-Token in
430 seinem Frontend, welcher dann als 2D-Code dargestellt werden kann. Nutzt der
431 Versicherte kein Frontend auf einem eigenen Gerät, erhält er den E-Rezept-Token von
432 der verordnenden Leistungserbringerinstitution als ausgedruckten 2D-Code.

433 Der 2D-Code kann in der einlösenden Apotheke vom Frontend abgescannt werden. Die
434 Darstellung des Tokens als 2D-Code ist ein optisches Übertragungsverfahren. Für die
435 Einlösung durch einen Vertreter kann der Versicherte den Token über die "Teilen"-

Funktion auf seinem Gerät an einen Vertreter über ein zwischen Versichertem und Vertreter etabliertes Kommunikationsmittel weitergegeben werden.

Für den digitalen Versand des E-Rezept-Tokens an eine Apotheke und für die weitere Kommunikation rund um den Einlösevorgang mit der Apotheke (Verfügbarkeit, Terminabsprache zum Abholen, ...) benötigt der Versicherte ein Übermittlungsverfahren. In einer ersten Umsetzungsstufe erfolgt das über den E-Rezept-Fachdienst. Hierbei erzeugt das Frontend des Versicherten bzw. Vertreters eine strukturierte Nachricht (E-Rezept-Token und Freitext). Die Apotheke ruft die an sie adressierte Nachricht vom E-Rezept-Fachdienst ab. Die Rückantwort erfolgt analog.

Die Versorgungsprozesse beim E-Rezept erfordern weitere Kommunikationsbeziehungen:

- Versicherter/Vertreter ==> Verordnender, bspw. für die Bestellung von Folgeverordnungen
- Verordnender ==> Versicherter/Vertreter, bspw. für Textnachrichten bezüglich der Bestellung von Folgeverordnungen
- Verordnender ==> Abgebender, bspw. für Tokenversand für Zytostatika-Verordnungen (§11 ApoG)

Diese Kommunikationsbeziehungen werden mit dem E-Rezept-Fachdienst nicht adressiert. Hier setzt die Anwendung E-Rezept auf die Weiterentwicklung der Anwendung KOM-LE, über welche dann auch die Kommunikationsbeziehung Versicherter/Vertreter ==> Abgebender in einem einheitlichen Kommunikationsverfahren umgesetzt werden kann.

2.4.6 Konzept Status E-Rezept

Ein E-Rezept durchläuft während seines Lebenszyklus verschiedene Status.

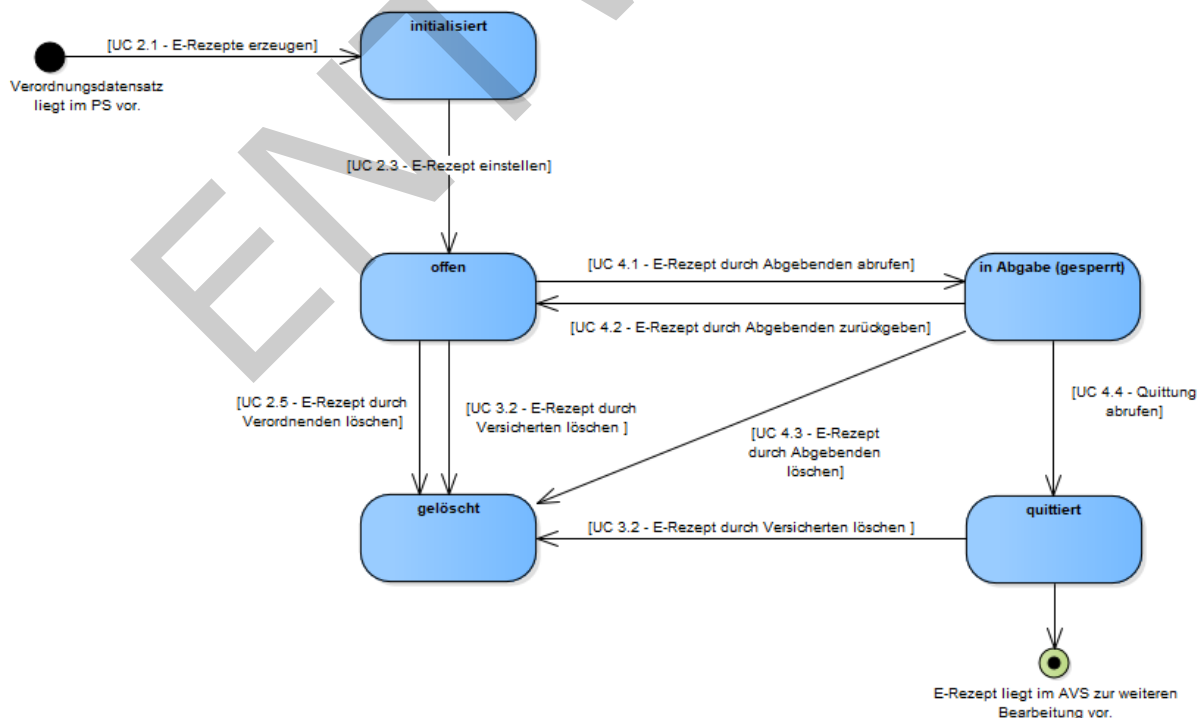


Abbildung 5: ABB_SYSLERP_004 Statusübergänge E-Rezept

461

462 Da ein E-Rezept-Token vervielfältigt werden kann, besteht die Möglichkeit, dass ein E-
 463 Rezept-Token an mehrere Apotheken übermittelt wird. Um sicherzustellen, dass die
 464 Statusübergänge "in Abgabe (gesperrt)" zu "quittiert", "gelöscht" oder "offen" nur durch
 465 die Apotheke ausgelöst wird, welche das E-Rezept zuvor abgerufen hat, wird der
 466 Apotheke beim Abruf eines E-Rezepts vom E-Rezept-Fachdienst ein Geheimnis
 467 übermittelt. Dieses Geheimnis zur Statusänderung "in Abgabe (gesperrt)" wird beim
 468 Aufruf zum Statuswechsel zurück an den E-Rezept-Fachdienst übermittelt. Der E-Rezept-
 469 Fachdienst kann anhand des Geheimnisses sicherstellen, ob der Statusübergang zulässig
 470 ist.

471 Da ein vom E-Rezept-Fachdienst heruntergeladenes E-Rezept elektronisch vervielfältigt
 472 werden kann, besteht die Möglichkeit, dass ein E-Rezept außerhalb der TI zu einer
 473 Apotheke übermittelt wird und der Status zur Abgabe des E-Rezepts im E-Rezept-
 474 Fachdienst nicht korrekt nachgehalten wird. Der E-Rezept-Fachdienst übermittelt der
 475 Apotheke beim Statuswechsel eines E-Rezepts von "in Abgabe (gesperrt)" zu "quittiert"
 476 eine Quittung. Der Besitz der Quittung belegt, dass die Apotheke die Abgabe des E-
 477 Rezepts entsprechend dem in der Fachanwendung vorgesehenen Ablauf durchgeführt
 478 hat. Die Quittung kann beispielsweise in der Abrechnung genutzt werden, um eine
 479 ungewollte mehrfache Abrechnung der Abgabe eines E-Rezepts zu vermeiden.

480 Die Verwaltung des Status im E-Rezept-Fachdienst erfolgt im Feld "status" der FHIR-
 481 Ressource Task (<https://www.hl7.org/fhir/task.html>). Die Zuordnung der Status des E-
 482 Rezepts zum FHIR-Code-System findet sich in Tabelle TAB_SYSLERP_006 . Die
 483 Umsetzung des Statusmodells für ein einzelnes E-Rezept wird über die Zustände der
 484 FHIR-Ressource Task gemäß des Workflow-Modells [FHIR_MED_WORKFLOW]
 485 realisiert. Der E-Rezept-Fachdienst prüft vor jedem Statuswechsel, ob ein von einem
 486 Akteur initiiertes Statuswechsel zulässig ist.

487 **Tabelle 3 : TAB_SYSLERP_006 Beschreibung Status Task**

Status E-Rezept	Status Task	Beschreibung und mögliche Folgezustände
initialisiert	(in FHIR 4.0.1: "draft")	<ul style="list-style-type: none"> Beim Abruf der Rezept-ID durch eine verordnende LEI wird die 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 "offen" (ready).
offen	(in FHIR 4.0.1: "ready")	<ul style="list-style-type: none"> Der Task wurde von einer verordnenden LEI in den E-Rezept-Fachdienst eingestellt. Es kann vom Versicherten bzw. seinem Vertreter abgerufen werden. Es kann von der verordnenden LEI oder dem Versicherten als gelöscht markiert werden und wechselt dann in den Status "gelöscht" (cancelled) Der Abruf einer abgebenden LEI ändert den Status des Tasks auf "in Abgabe (gesperrt)" (in-progress). Dieser sperrt den Zugriff durch andere abgebende LEI.

in Abgabe (gesperrt)	(in FHIR 4.0.1: "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 "offen" (<i>ready</i>). • Die abgebende LEI kann die Quittung abrufen. Dann wechselt das E-Rezept in den Status "quittiert" (<i>completed</i>) und es wird eine MedicationDispense zur Dokumentation für den Versicherten erzeugt. • Der Task kann durch die abgebende LEI als gelöscht markiert werden und wechselt dann in den Status "gelöscht" (<i>cancelled</i>). • Der Task kann vom Versicherten bzw. seinem Vertreter weiterhin eingesehen werden (<i>read only</i>).
quittiert	(in FHIR 4.0.1: "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 "gelöscht" (<i>cancelled</i>). • Eine Reaktivierung des Tasks ist nicht möglich.
gelöscht	(in FHIR 4.0.1: "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. • Hinweis: Das eigentliche physische Löschen des Datensatzes erfolgt automatisch durch den E-Rezept-Fachdienst nach einer Löschfrist.

488

489 2.4.7 Unterstützung betrieblicher Prozesse

490

491 Die DVOs verordnender und abgebender LEIs benötigen eine einfache und schnell
 492 anwendbare Möglichkeit, nach Inbetriebnahme von Client-Systemen in der
 493 Produktivumgebung deren Funktionsfähigkeit zu überprüfen. Dies ist etwa nach
 494 Neuinstallation und Update oder auch regelmäßig im laufenden Betrieb hilfreich. Die
 495 Prüfung sollte einerseits keine explizite Anwendungslogik erfordern und andererseits ist
 496 die Abgabe von Arzneimitteln sowie eine gegenüber Kostenträgern abrechenbare
 497 Leistung auszuschließen.

Unter diesen Voraussetzungen sieht das Konzept eine durch die DVOs selbstbestimmte Prüfung der Konnektivität zwischen Client-Systemen und E-Rezept-Fachdienst wie folgt vor:

- **Verordnende LEI:** Mit "E-Rezept erzeugen" (UC 2.1) wird eine gültige E-Rezept-ID vom E-Rezept-Fachdienst abgerufen. Diese kann (muss aber nicht) nachher für das Einstellen eines vom LEI signierten E-Rezepts verwendet werden. Ist der Abruf einer E-Rezept-ID erfolgreich, gilt die Konnektivität zur Fachanwendung als gegeben.
- **Abgebende LEI:** Hierbei handelt es sich um einen Negativtestfall, der eine Fehlermeldung durch den E-Rezept-Fachdienst provoziert: Der DVO ruft ein E-Rezept (UC 4.1) mit zufälligen (und dadurch nicht validen) Werten für AccessCode und E-Rezept-ID ab. Der E-Rezept-Fachdienst antwortet mit einer entsprechenden Fehlermeldung.

In beiden Testfällen wird die Erstellung eines AuthN-Token gemäß UC 5.2 und die Verbindung zum E-Rezept-Fachdienst sowie die korrekte Verarbeitung der Anfragen inkl. Fehlermeldungen geprüft. Eine DVO-Prüfkarte wird hierzu nicht benötigt. Die Prüfungen können auch regelmäßig automatisiert durchgeführt werden (z.B. durch das TI-Service Monitoring).

Generell sollte für die Konnektivitätsprüfung auf die Erstellung eines signierten Prüf-E-Rezeptes (Rezept wird auf die KVNR einer DVO-Prüfkarte ausgestellt) verzichtet werden. Zwar kann mit einem solchen Rezept keine Verordnung eingelöst oder in Abrechnung gebracht werden, allerdings ist ggf. der Signierungsvorgang durch den verordnenden LE u.U. nicht immer trennscharf von dem eines Echt-Rezeptes zu unterscheiden. Auf ein Verbot der Erstellung eines Prüf-E-Rezeptes wird allerdings verzichtet.

Weitere betriebliche Aufgaben sind bspw.

- die Bereitstellung von Probes zur Messung der Verfügbarkeit auf Anwendungsebene,
- die Verifikation von Änderungen in der PU auf Anwendungsebene.

Betriebliche Anforderungen

A_18966 - Überwachung von Verfügbarkeit und Zuverlässigkeit der Fachanwendung

Die an der Fachanwendung E-Rezept beteiligten Produkttypen E-Rezept-Fachdienst und Identity Provider (IdP) MÜSSEN sämtliche technischen, funktionalen, interoperablen und organisatorischen Voraussetzungen zur Überwachung von Verfügbarkeit und Zuverlässigkeit des jeweiligen Produkttyps umsetzen und auf Schnittstellen-Aufrufe durch Probes des TI-Service Monitorings innerhalb der TI mit aussagekräftigen Meldungen antworten. [\leq]

A_18967 - Erhebung und Speicherung von Performance-Messdaten

Die an der Fachanwendung E-Rezept beteiligten Produkttypen E-Rezept-Fachdienst und Identity Provider (IdP) MÜSSEN fortlaufend Last- und Performance-Messdaten erheben, sammeln, ggfs. zusammenführen sowie speichern, und diese - zur eindeutigen Lokalisierung der betroffenen technischen Produktinstanz und/oder Komponente - mit Metadaten anreichern (z.B. Produktversion), um sie einer weiterführenden betrieblichen Analyse und Auswertung durch die gematik zuführen zu können. Dies gilt auch für zusammengehörig definierte Operationen (im Sinne eines Bearbeitungsprozesses oder des Ablaufs eines Anwendungsfalls), sofern eine entsprechende Relevanz im Rahmen der Überwachung von Verfügbarkeit und Performance durch die gematik festgestellt wird. [\leq]

A_18992 - Lieferung von Performance-Messdaten

547 Die Anbieter der Produkttypen E-Rezept-Fachdienst und Identity Provider (IdP) MÜSSEN
548 Performance-Messdaten an die vom Gesamtverantwortlichen TI definierte Schnittstelle
549 liefern. [<=]

550 **A_18991 - E-Rezept-Fachdienst - Erhebung von Performance-Messdaten**

551 Der E-Rezept-Fachdienst MUSS mindestens für die Operationen "E-Rezept-ID abrufen",
552 "E-Rezept einstellen", "E-Rezept durch Abgebenden abrufen", "Quittung abrufen", "E-
553 Rezept-Nachricht einstellen" und "E-Rezept-Nachricht abrufen" Performance-Messdaten
554 erheben. [<=]

555 **A_18993 - Identity Provider - Erhebung von Performance-Messdaten**

556 Der Produkttyp Identity Provider MUSS mindestens für die Operation(en) zur
557 Anforderung bis zur Übergabe von Identitätsbestätigungen (AuthN-Token) Performance-
558 Messdaten erheben, inkl. der Durchführung des Challenge-Response-Verfahrens. Beim
559 Challenge-Response-Verfahren ist dabei auch die Dauer der Antwortzeit des
560 Authentisierungsmoduls (Einwilligung in die Nutzung von Identitätsattributen) zu messen
561 und separat auszuweisen. Die Ausstellung von Versicherten-Identitätsbestätigungen bzw.
562 die über die Internet-Schnittstelle angeforderten und übergebenden
563 Identitätsbestätigungen sind separat auszuweisen. [<=]

564 **A_18969 - Unterstützung des TI-ITSM-Anbieter- und des Endanwender-
565 Supports durch aussagekräftige Fehlermeldungen**

566 Die an den Anwendungsfällen der Fachanwendung E-Rezept beteiligten Produkttypen E-
567 Rezept-Fachdienst, Identity Provider und deren Komponenten sowie die jeweiligen
568 Frontend-Komponenten der Nutzer MÜSSEN zur Unterstützung des Endanwender-
569 Supports bei einer entstehenden Störung oder einem Abbruch, gleich aus welchem
570 Grunde, eine eindeutige, aussagekräftige und interoperable Fehlermeldung bereitstellen,
571 die es den Supporteinheiten ermöglichen, die Störungsursache und den oder die
572 Lösungsverantwortlichen der Störung zu identifizieren und mögliche eigene
573 Gegenmaßnahmen zu ergreifen. [<=]

574 **A_18999 - Anzeige des E-Rezept-Betriebszustandes**

575 Das TI-Service Monitoring MUSS den Anbietern der Produkttypen E-Rezept-Fachdienst,
576 Identity Provider, Verzeichnisdienst, VPN-Zugangsdienst und dem Anbieter des E-Rezept-
577 Frontends des Versicherten den E-Rezept-Betriebszustand anzeigen. Störungen oder
578 Service-Einschränkungen der Fachanwendung E-Rezept werden allen vorgenannten
579 Anbietern gemeldet. Die Anzeige und die Meldungen enthalten Angaben zum
580 verursachenden Dienst und unabhängig davon, durch welchen Produkttyp oder durch
581 welchen Anbieter die Störung verursacht wird. [<=]

582 Der E-Rezept Betriebszustand wird durch die Betriebszustände der Produkttypen E-
583 Rezept-Fachdienst, Identity Provider und Verzeichnisdienst repräsentiert.

584 **A_18997 - Anbieter E-Rezept-Fachdienst - Supportverantwortung im TI-ITSM-
585 Teilnehmersupport**

586 Der Anbieter des E-Rezept-Fachdienstes MUSS zur Unterstützung der Hochverfügbarkeit
587 der Fachanwendung E-Rezept für die im TI-ITSM-Teilnehmersupport gemeldeten
588 Störungen mit E-Rezept-Kontext die Supportverantwortung übernehmen und diese
589 koordinieren. [<=]

590 **A_18998 - Anbieter E-Rezept-Fachdienst - 24/7 TI-ITSM-Teilnehmersupport**

591 Der Anbieter E-Rezept-Fachdienst MUSS seinen TI-ITSM-Teilnehmersupport 24/7
592 anbieten. [<=]

593 **A_18970 - Versichertensupport durch Anbieter Frontend des Versicherten**

594 Anbieter operativer Betriebsleistungen des E-Rezept-Frontend des Versicherten MÜSSEN
595 einen Versichertensupport anbieten. [<=]

596 **A_18996 - TI-ITSM-Teilnahme von Anbietern Frontend des Versicherten**

597 Anbieter operativer Betriebsleistungen des E-Rezept-Frontend des Versicherten KÖNNEN
598 am TI-ITSM teilnehmen.[<=]

ENTWURF

599

3 Anwendungsfälle

3.1 Übersicht der Anwendungsfälle

Die folgende Abbildung zeigt eine Übersicht über die Anwendungsfälle der Fachanwendung E-Rezept.

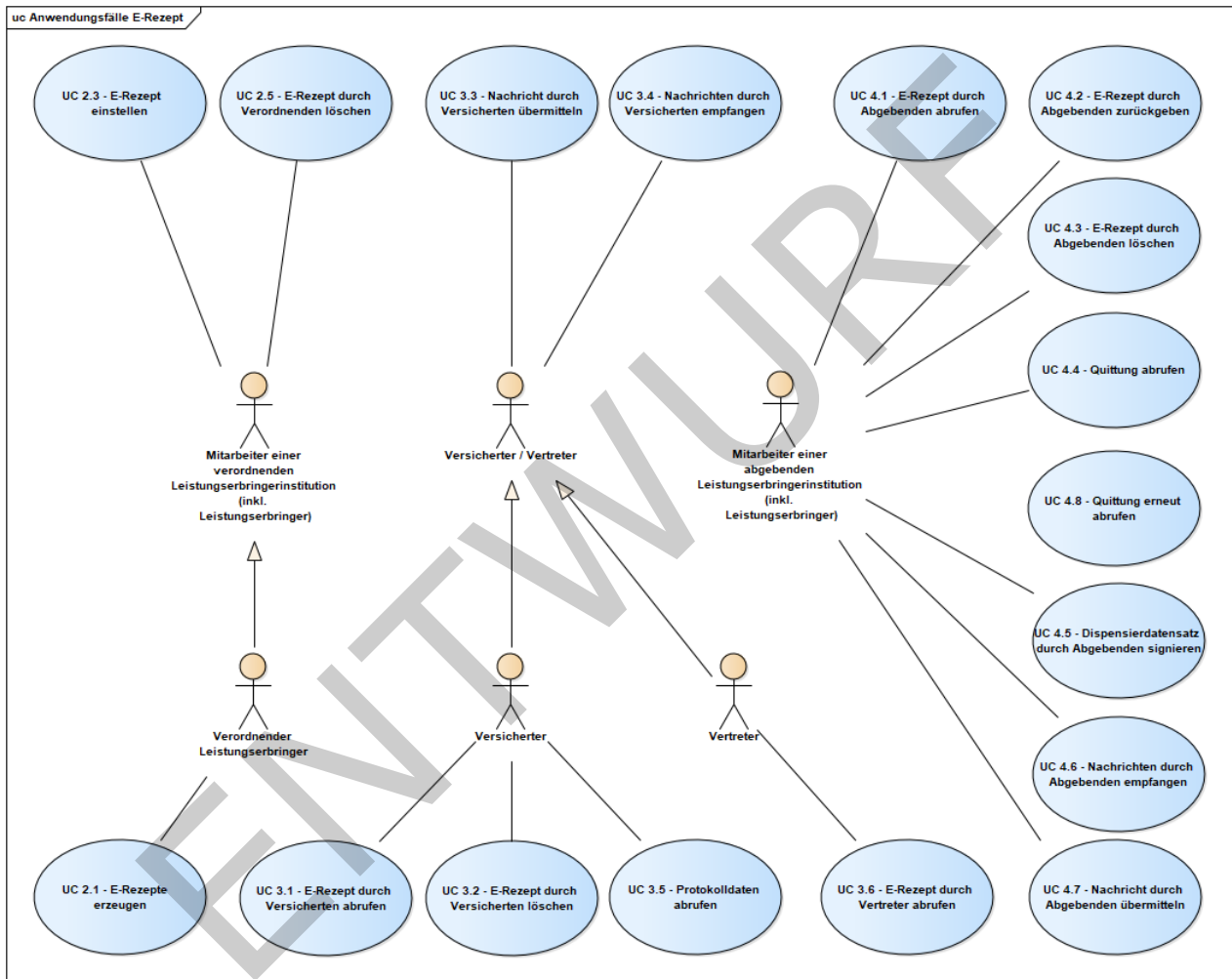


Abbildung 6: ABB_SYSLERP_005 Anwendungsfälle E-Rezept

3.2 Übergreifende Vorbedingungen

Die nachfolgenden Vorbedingungen müssen für alle Anwendungsfälle erfüllt sein, damit sie erfolgreich ausgeführt werden können. Wenn diese Vorbedingungen nicht erfüllt sind, so muss die Operation mit einer Fehlermeldung abbrechen.

A_18496 - Übergreifende Vorbedingung: Aufrufparameter gültig

Die Produkttypen der Fachanwendung E-Rezept MÜSSEN bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn notwendige Aufrufparameter unvollständig, ungültig oder inkonsistent sind. [<=]

A_18839 - Übergreifende Vorbedingung: Validierung von AuthN-Token

Jeder Produkttyp, der AuthN-Token als Aufrufparameter bei Operationen entgegennimmt und verarbeitet, MUSS den AuthN-Token (ID Token) gemäß [OIDC] validieren. Er MUSS die Operation mit einer qualifizierten Fehlermeldung abbrechen, falls die Validierung fehlschlägt.[<=]

3.3 Übergreifende Nachbedingungen

Der folgende Abschnitt beschreibt übergreifende Nachbedingungen, die für den erfolgreichen Abschluss fachlicher Anwendungsfälle gelten.

A_18497 - Protokollierung der Zugriffe auf medizinische Daten

Die Fachanwendung E-Rezept MUSS für jeden Aufruf einer Operation zum Einstellen, zur Statusänderung, zum Lesen oder Löschen eines E-Rezepts einen Protokolleintrag für den Versicherten erstellen. Der Eintrag MUSS dabei das aktuelle Datum, die aktuelle Uhrzeit und die Art des Zugriffs, einen lesbaren Namen des Zugreifenden, einen Identifier des Zugreifenden sowie einen Bezeichner des zugegriffenen Datenobjekts enthalten.[<=]

A_18498 - Für Nutzer verständliche Fehlermeldungen

Alle an den Anwendungsfällen der Fachanwendung E-Rezept beteiligten Produkttypen und Komponenten MÜSSEN interoperable Fehlermeldungen bereitstellen, die es den Versicherten bzw. den Mitarbeitern der Leistungserbringerinstitution ermöglichen, die Ursache des Fehlers über ihr jeweiliges Frontend zu identifizieren und mögliche Gegenmaßnahmen zu ergreifen.[<=]

3.4 E-Rezept ausstellen**3.4.1 E-Rezepte durch Verordnenden erzeugen**

Mit diesem Anwendungsfall signiert ein verordnender Leistungserbringer ein oder mehrere Verordnungsdatensätze. Vor dem Signieren wird im Verordnungsdatensatz eine über die TI bezogene Rezept-ID ergänzt. Dieser Anwendungsfall kann, da er eine qualifizierte elektronische Signatur beinhaltet, nur durch den Leistungserbringer, nicht jedoch durch einen Mitarbeiter der medizinischen Institution durchgeführt werden.

A_18502 - Anwendungsfall "E-Rezepte erzeugen"

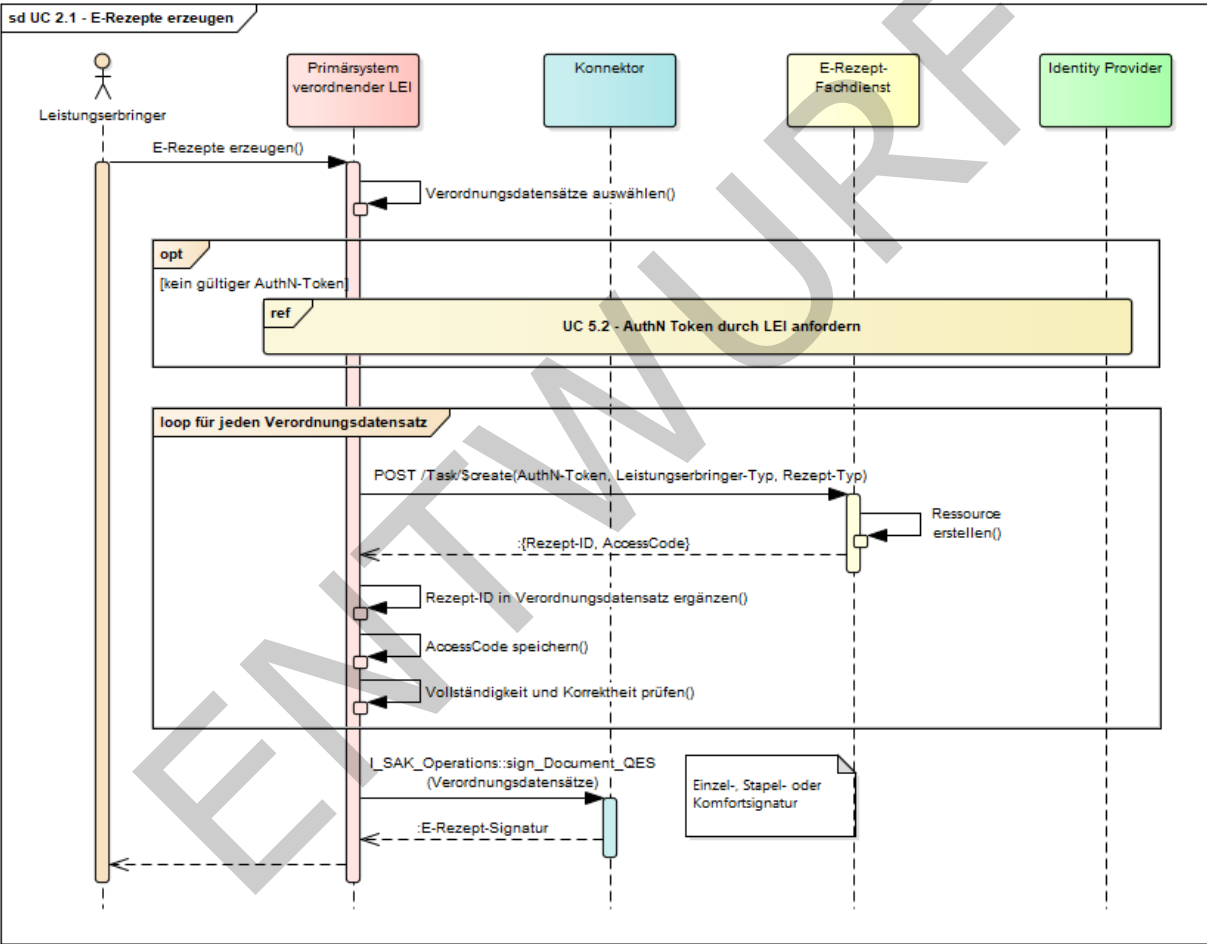
Alle am Anwendungsfall "E-Rezepte erzeugen" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 4: TAB_SYSLERP_005 Anwendungsfall E-Rezepte erzeugen

Name	UC 2.1 - E-Rezepte erzeugen
Vorbedingung	<ul style="list-style-type: none">• Der oder die Versicherten sind der LEI bekannt.• Ein oder mehrere Verordnungsdatensätze wurden für den bzw. die Versicherten im Primärsystem erstellt.• Der HBA ist für die QES gesteckt und freigeschaltet.
Kurzbeschreibung (Außenansicht)	Der verordnende Leistungserbringer wählt im Primärsystem einen oder mehrere Verordnungsdatensätze zum Signieren aus. Der Leistungserbringer wählt das Signaturverfahren aus.

	Das Primärsystem ruft für jedes E-Rezept vom E-Rezept-Fachdienst eine Rezept-ID ab und ergänzt diese im Verordnungsdatensatz. Anschließend werden die E-Rezepte mittels Konnektor mit einer QES signiert. Es kann die Einzel-, Stapel- oder Komfortsignatur genutzt werden.
Nachbedingung	Die erzeugten E-Rezepte beinhalten eine eindeutige Rezept-ID und haben eine QES. Der AccessCode für jedes E-Rezept ist im Primärsystem gespeichert. Die E-Rezepte sind im E-Rezept-Fachdienst angelegt und haben den Status "initialisiert".

644



645

646 [\leq]

647

648 **3.4.2 E-Rezept einstellen**

649

650

Mit diesem Anwendungsfall stellt eine verordnende Leistungserbringerinstitution ein E-Rezept auf den E-Rezept-Fachdienst ein und erzeugt den zugehörigen E-Rezept-Token.

651

A_18503 - Anwendungsfall "E-Rezept einstellen"

652

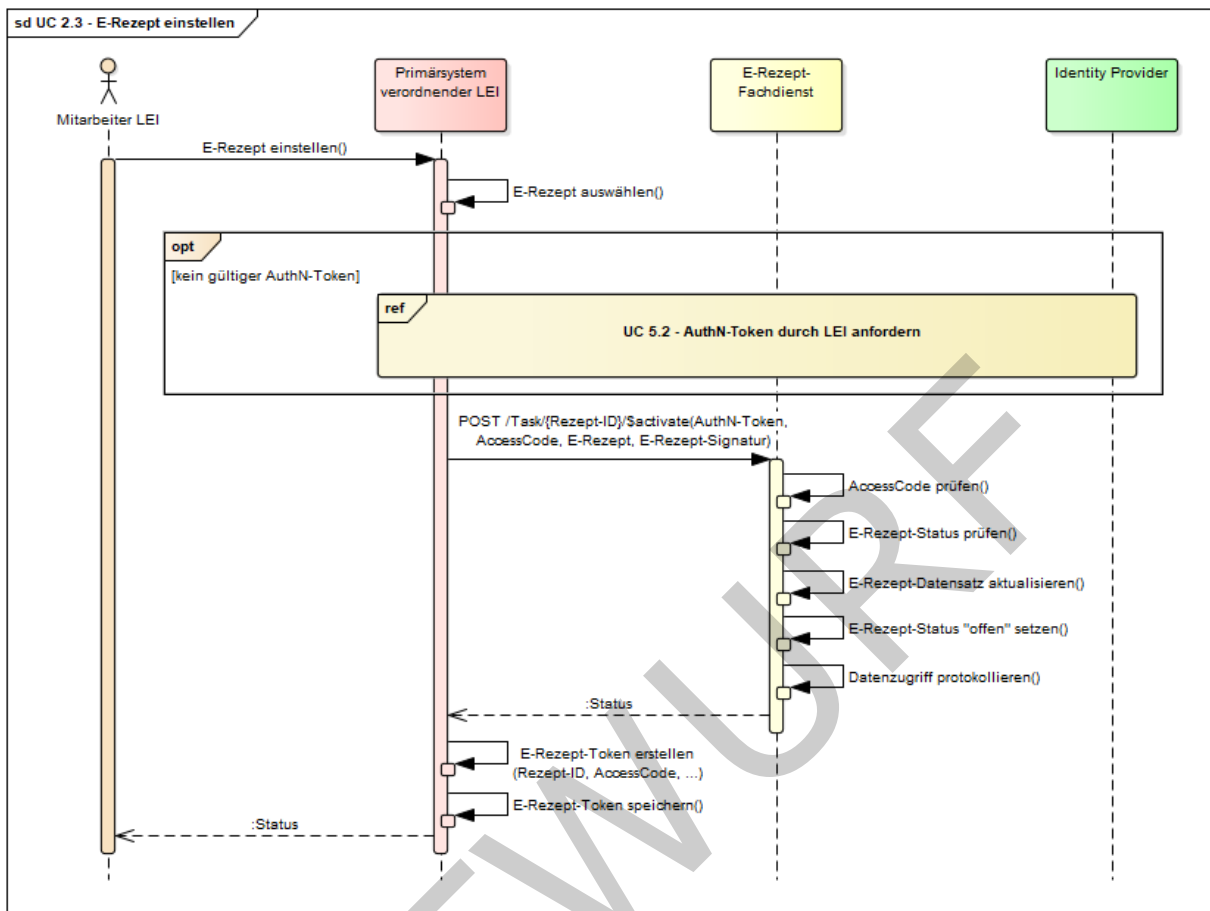
Alle am Anwendungsfall "E-Rezept einstellen" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

653

654 **Tabelle 5: TAB_SYSLERP_006 Anwendungsfall E-Rezept einstellen**

Name	UC 2.3 - E-Rezept einstellen
Vorbedingung	<ul style="list-style-type: none">• Der verordnende Leistungserbringer hat den Anwendungsfall "UC 2.1 - E-Rezepte erzeugen" ausgeführt. Ein E-Rezept und die zugehörige Signatur liegen im Primärsystem vor.• Die Rezept-ID und der AccessCode sind im Primärsystem bekannt.• Das E-Rezept im E-Rezept-Fachdienst hat den Status "initialisiert".
Kurzbeschreibung (Außenansicht)	<p>Der verordnende Leistungserbringer oder ein Mitarbeiter der medizinischen Institution wählt im Primärsystem ein E-Rezept zum Einstellen aus.</p> <p>Das Primärsystem aktualisiert das E-Rezept im E-Rezept-Fachdienst. Das Primärsystem erstellt einen E-Rezept-Token und speichert diesen..</p>
Nachbedingung	<p>Das E-Rezept ist im E-Rezept-Fachdienst gespeichert und hat den Status "offen".</p> <p>Das Einstellen ist im E-Rezept-Fachdienst protokolliert.</p> <p>Der E-Rezept-Token ist im Primärsystem gespeichert.</p>

655



656

657 [\leq]

658

659 3.4.3 E-Rezept-Token durch Verordnenden an Versicherten oder 660 Apotheker übermitteln

661 Nachdem ein Mitarbeiter der verordnenden LEI den Anwendungsfall "UC 2.3 - E-Rezept
662 einstellen" ausgeführt hat, kann der Versicherte sich das E-Rezept mit dem
663 Anwendungsfall "UC 3.1 - E-Rezepte durch Versicherten abrufen" auf sein FdV
664 herunterladen und einen E-Rezept-Token erstellen.

665 Wenn der Versicherte kein FdV nutzt, wird der E-Rezept-Token im Primärsystem erzeugt
666 und als 2D-Code ausgedruckt. Der Ausdruck wird dem Versicherten übergeben.
667 Ergänzend zum Ausdruck können zusätzliche technische Möglichkeiten bestehen, den 2D-
668 Code für den Versicherten zum Abfotografieren anzuzeigen.

669 Für Verordnungen von Sprechstundenbedarfen und von parenteralen Zubereitungen nach
670 §11 ApoG (Zytostatika) kann die verordnende LEI den E-Rezept-Token an eine Apotheke
671 übertragen und hierfür KOM-LE nutzen. Im Kontext eines Krankenhauses sind ggf. auch
672 weitere Übertragungswege innerhalb des KIS möglich.

673 3.4.4 E-Rezept durch Verordnenden löschen

674 Mit diesem Anwendungsfall kann ein Mitarbeiter einer verordnenden
 675 Leistungserbringerinstitution, den Status für ein zuvor durch die LEI für den Versicherten
 676 eingestelltes E-Rezept auf "gelöscht" setzen. Die Nutzer können auf ein E-Rezept mit
 677 dem Status "gelöscht" nicht mehr zugreifen.

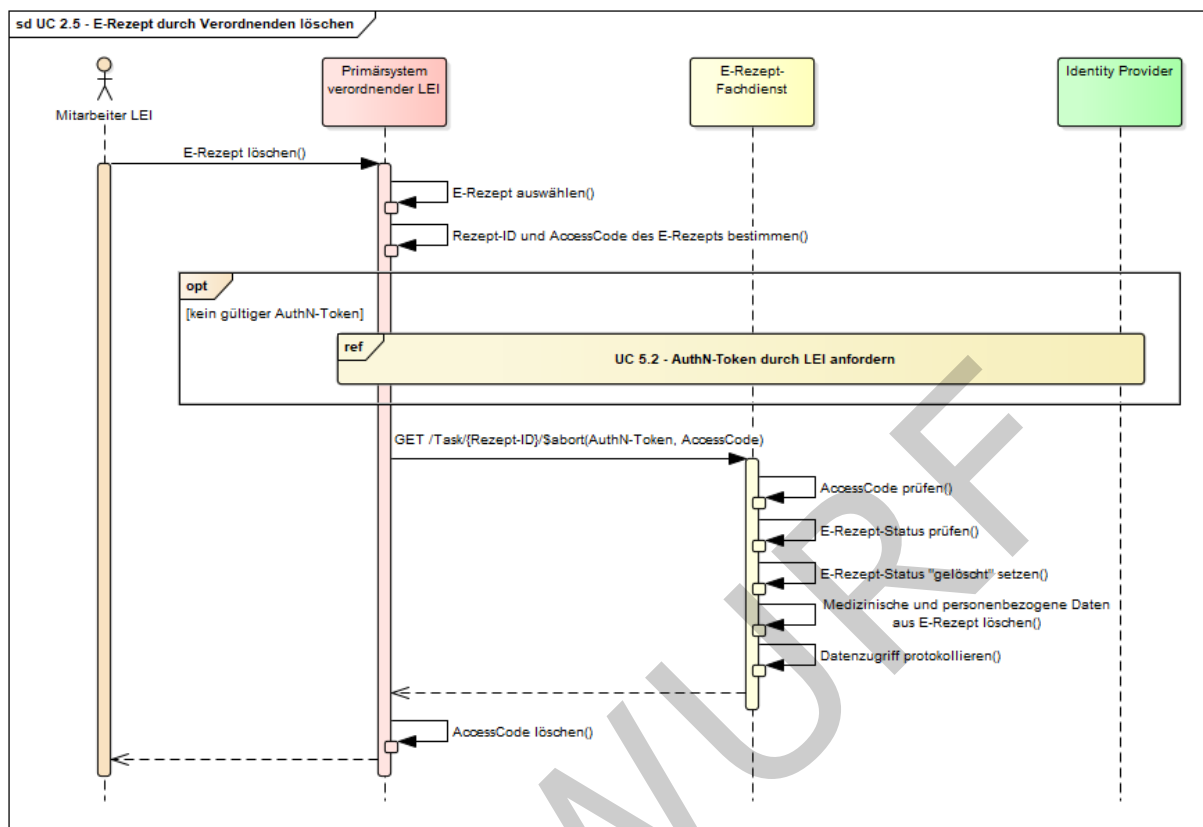
678 A_18505 - Anwendungsfall "E-Rezept durch Verordnenden löschen"

679 Alle am Anwendungsfall "E-Rezept durch Verordnenden löschen" beteiligten Produkttypen
 680 und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

681 **Tabelle 6: TAB_SYSLERP_008 Anwendungsfall E-Rezept durch Verordnenden löschen**

Name	UC 2.5 - E-Rezept durch Verordnenden löschen
Vorbedingung	<ul style="list-style-type: none"> • Ein Mitarbeiter der verordnenden LEI hat den Anwendungsfall "UC 2.3 - E-Rezept einstellen" ausgeführt. • Die Rezept-ID und der AccessCode sind im Primärsystem bekannt. • Das E-Rezept im E-Rezept-Fachdienst hat den Status "offen".
Kurzbeschreibung (Außenansicht)	<p>Ein Mitarbeiter der verordnenden LEI markiert über das PS ein durch die LEI verordnetes E-Rezept zum Löschen und bestätigt den Vorgang.</p> <p>Der Status des E-Rezepts im E-Rezept-Fachdienst wird geändert. Die personenbezogenen und medizinischen Daten im E-Rezept werden gelöscht.</p> <p>Der AccessCode wird im Primärsystem gelöscht.</p>
Nachbedingung	<p>Das E-Rezept im E-Rezept-Fachdienst hat den Status "gelöscht". Es beinhaltet keine personenbezogenen oder medizinischen Daten.</p> <p>Der Statuswechsel des E-Rezepts zum Status "gelöscht" ist im E-Rezept-Fachdienst protokolliert.</p>

682



683

684 [<=]

685

686 3.5 E-Rezept durch Versicherten verwalten

687 3.5.1 E-Rezepte durch Versicherten abrufen

688 Mit diesem Anwendungsfall kann ein Versicherter alle seine im E-Rezept-Fachdienst
 689 eingestellten E-Rezepte herunterladen, um Einsicht in die Daten dieser E-Rezepte zu
 690 nehmen oder einen E-Rezept-Token zu erstellen.

691 A_18506 - Anwendungsfall "E-Rezepte durch Versicherten abrufen"

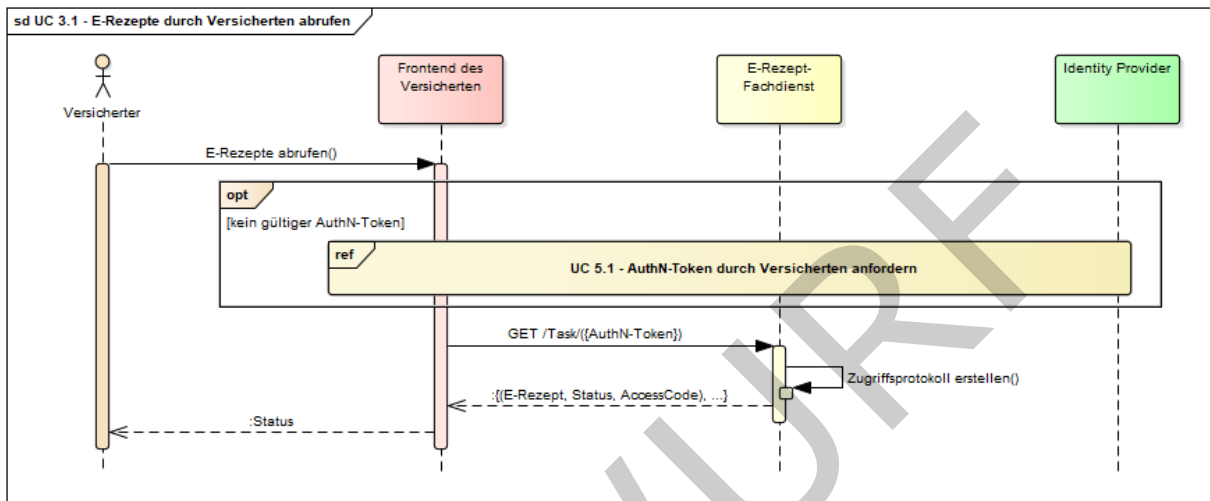
692 Alle am Anwendungsfall "E-Rezepte durch Versicherten abrufen" beteiligten Produkttypen
 693 und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

694 **Tabelle 7: TAB_SYSLERP_009 Anwendungsfall E-Rezepte durch Versicherten abrufen**

Name	UC 3.1 - E-Rezepte durch Versicherten abrufen
Vorbedingung	<ul style="list-style-type: none"> keine
Kurzbeschreibung (Außenansicht)	Ein Versicherter ruft über das Frontend des Versicherten alle seine im E-Rezept-Fachdienst eingestellten Rezepte ab. Der E-Rezept-Fachdienst identifiziert die E-Rezepte auf Basis der Versicherten-ID des Versicherten und liefert die E-Rezepte und die

	zugehörigen AccessCodes, Status und die Zeitpunkte, an denen die Status gesetzt wurden.
Nachbedingung	Im FdV stehen die E-Rezepte zur Anzeige sowie die Daten für das Erstellen eines E-Rezept-Tokens bereit. Der Abruf ist im E-Rezept-Fachdienst protokolliert.

695



696

697 [\leq]

698

699 3.5.2 E-Rezept durch Vertreter abrufen

700 Mit diesem Anwendungsfall kann ein Vertreter ein im E-Rezept-Fachdienst eingestelltes
 701 E-Rezept herunterladen, um Einsicht in die Daten des E-Rezepts zu nehmen.

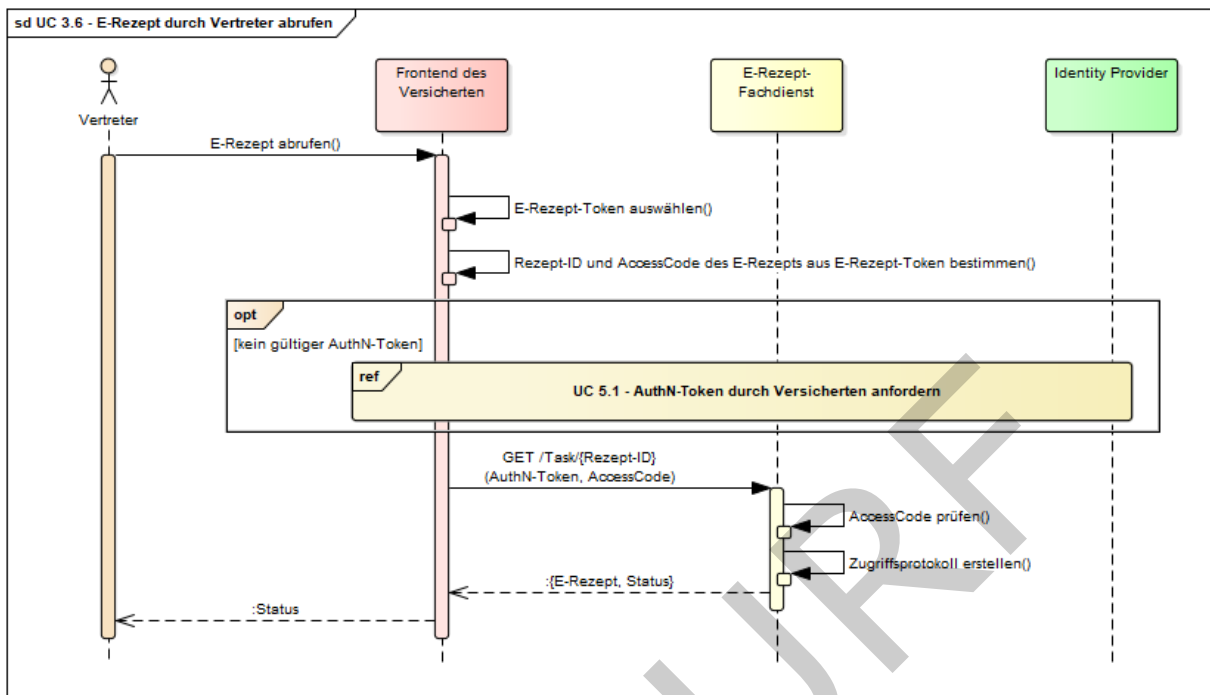
702 **A_18781 - Anwendungsfall "E-Rezept durch Vertreter abrufen"**

703 Alle am Anwendungsfall "E-Rezept durch Vertreter abrufen" beteiligten Produkttypen und
 704 Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

705 **Tabelle 8: TAB_SYSLERP_041 Anwendungsfall E-Rezept durch Vertreter abrufen**

Name	UC 3.6 - E-Rezept durch Vertreter abrufen
Vorbedingung	<ul style="list-style-type: none"> Der Vertreter hat den E-Rezept-Token vom Versicherten/Vertreter oder der verordnenden LEI empfangen. Der E-Rezept-Token ist im Frontend des Versicherten gespeichert.
Kurzbeschreibung (Außenansicht)	Ein Vertreter ruft über das Frontend des Versicherten ein im E-Rezept-Fachdienst eingestelltes Rezept ab. Der E-Rezept-Fachdienst liefert das E-Rezept, den Status und den Zeitpunkt, an dem der Status gesetzt wurde.
Nachbedingung	Im FdV steht das E-Rezept zur Anzeige sowie die Daten für das Erstellen eines E-Rezept-Tokens bereit. Der Abruf ist im E-Rezept-Fachdienst protokolliert.

706



707

708 [<=]

709

710 3.5.3 E-Rezept durch Versicherten löschen

711

712 Mit diesem Anwendungsfall kann der Versicherte den Status für ein für ihn eingestelltes
 713 E-Rezept auf "gelöscht" setzen. Die Nutzer können auf ein E-Rezept mit dem
 714 Status "gelöscht" nicht zugreifen.

715 Der Anwendungsfall kann nicht durch einen Vertreter ausgeführt werden.

716 A_18507 - Anwendungsfall "E-Rezept durch Versicherten löschen"

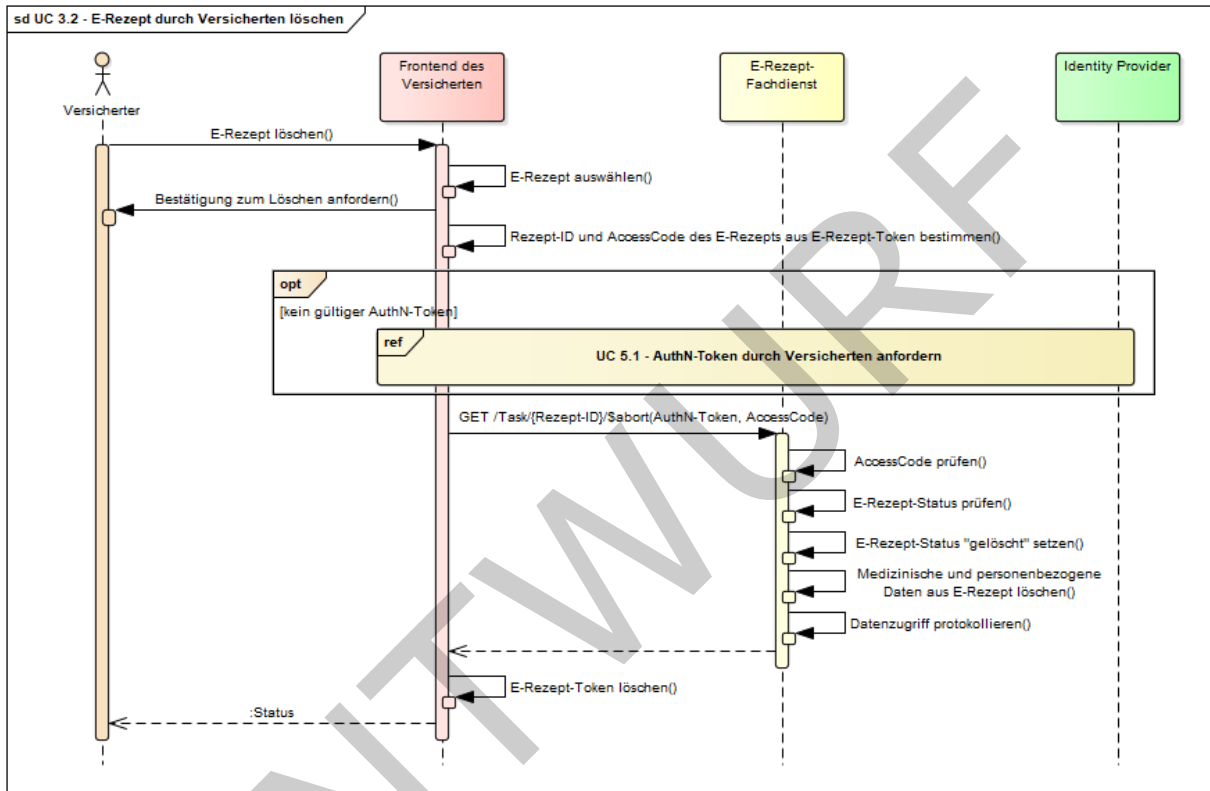
717 Alle am Anwendungsfall "E-Rezept durch Versicherten löschen" beteiligten Produkttypen
 718 und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

719 **Tabelle 9: TAB_SYSLERP_010 Anwendungsfall E-Rezept durch Versicherten löschen**

Name	UC 3.2 - E-Rezept durch Versicherten löschen
Vorbedingung	<ul style="list-style-type: none"> Der Versicherte hat den Anwendungsfall "UC 3.1 - E-Rezepte durch Versicherten abrufen" ausgeführt. Das E-Rezept hat einen Status ungleich "in Abgabe (gesperrt)"
Kurzbeschreibung (Außenansicht)	<p>Ein Versicherter wählt am FdV ein für ihn ausgestelltes E-Rezept aus, das gelöscht werden soll. Der Versicherte bestätigt das Löschen.</p> <p>Das FdV überträgt die Anforderung an den E-Rezept-Fachdienst. Der Status des E-Rezepts im E-Rezept-Fachdienst wird geändert. Die personenbezogenen und medizinischen Daten im E-Rezept</p>

	werden gelöscht. Abschließend wird der E-Rezept-Token im FdV gelöscht.
Nachbedingung	Das E-Rezept im E-Rezept-Fachdienst hat den Status "gelöscht". Es beinhaltet keine personenbezogenen oder medizinischen Daten. Der Statuswechsel des E-Rezepts zum Status "gelöscht" ist im E-Rezept-Fachdienst protokolliert.

720



721

722 [\leq]

723

724 3.5.4 Nachricht durch Versicherten an Abgebenden übermitteln

725 Mit diesem Anwendungsfall kann ein Versicherter oder Vertreter einen E-Rezept-Token
 726 oder eine Mitteilung an eine Apotheke seiner Wahl übermitteln, um das Rezept
 727 einzulösen oder eine Verfügbarkeitsanfrage zu dem Rezept zu stellen. Als Alternative
 728 steht die optische Übermittlung des E-Rezept-Tokens als 2D-Code zur Verfügung.

729 A_18508 - Anwendungsfall "Nachricht durch Versicherten übermitteln"

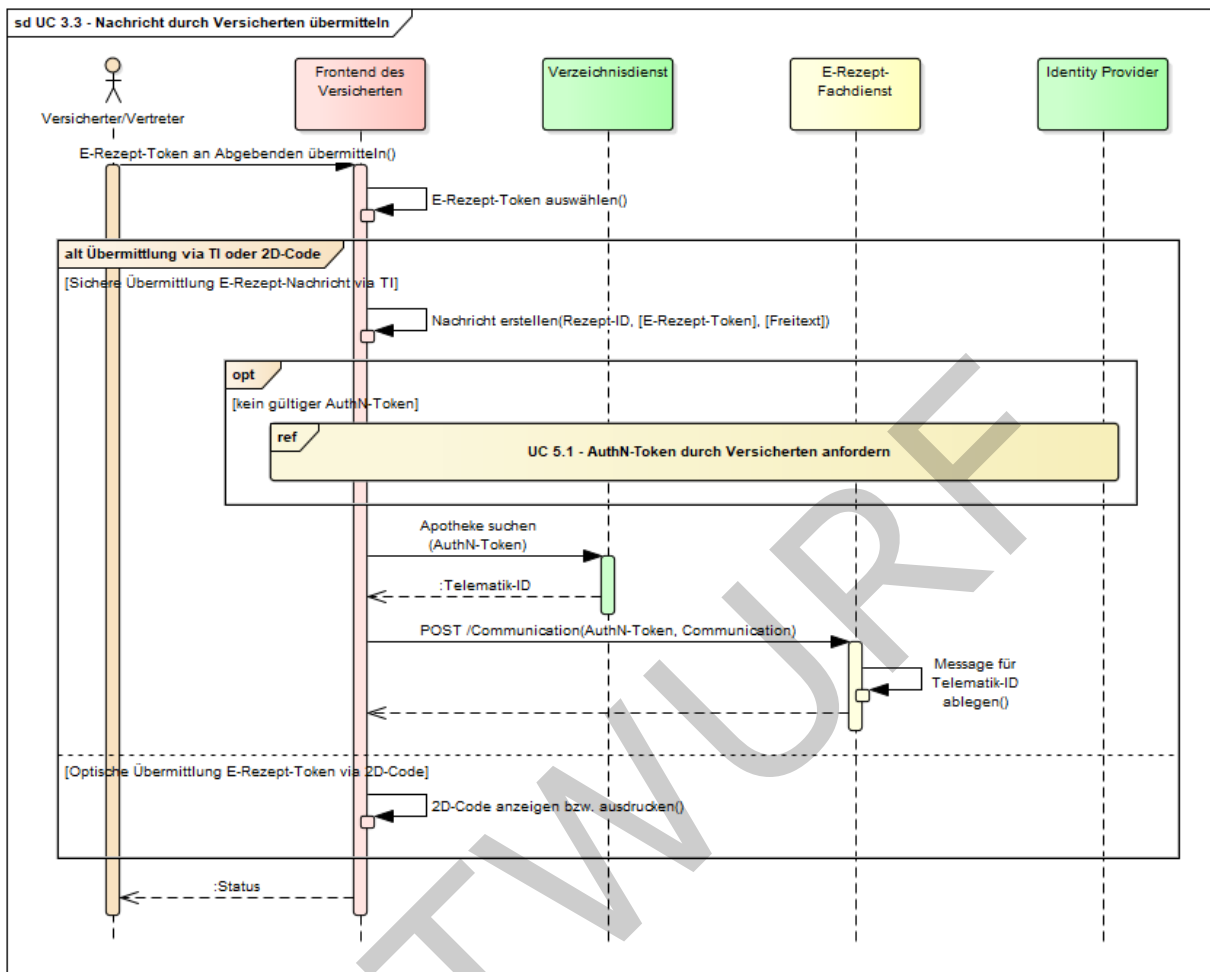
730 Alle am Anwendungsfall "Nachricht durch Versicherten übermitteln" beteiligten
 731 Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

732 **Tabelle 10: TAB_SYSLERP_011 Anwendungsfall Nachricht durch Versicherten**
 733 **übermitteln**

Name	UC 3.3 - Nachricht durch Versicherten übermitteln
------	---

Vorbedingung	<ul style="list-style-type: none">• Der Versicherte hat den Anwendungsfall "UC 3.1 - E-Rezepte durch Versicherten abrufen" ausgeführt. Das FdV hat einen E-Rezept-Token erstellt.• alternativ: Der Vertreter hat von einem Versicherten einen E-Rezept-Token erhalten. Ein E-Rezept-Token liegt im FdV vor.
Kurzbeschreibung (Außenansicht)	<p>Ein Versicherter/Vertreter wählt im FdV einen E-Rezept-Token aus und trifft dann die Entscheidung, ob der Versand über die TI oder alternativ optisch per 2D-Code stattfinden soll.</p> <p>Der sichere Versand über die TI erfolgt mithilfe des E-Rezept-Fachdienstes. Der Versicherte wählt im Verzeichnisdienst die Apotheke aus, an die die Nachricht übermittelt werden soll. Anschließend stellt das FdV die Nachricht im E-Rezept-Fachdienst für die Apotheke ein. Die Nachricht enthält einen E-Rezept-Token und/oder eine Textnachricht.</p> <p>Im Falle der Alternative wird der E-Rezept-Token in einen 2D-Code umgewandelt und dem Abgebenden entweder zum Scannen an einem Bildschirm gezeigt oder als Ausdruck übergeben.</p>
Nachbedingung	<p>Die Nachricht mit dem E-Rezept-Token liegt im E-Rezept-Fachdienst und kann von der ausgewählten LEI asynchron empfangen werden. Im Falle der Alternative kann der Abgebende den 2D-Code abscannen.</p>

734



735

736 [\leq]

737 3.5.5 E-Rezept-Token durch Versicherten an Vertreter übermitteln

738 Mit diesem Anwendungsfall kann ein Versicherter einen E-Rezept-Token an seinen
 739 Vertreter übermitteln, damit dieser das E-Rezept für den Versicherten einlöst. Da die
 740 Kommunikation von einem Versicherten zu einem anderen Versicherten (Vertreter) über
 741 den E-Rezept-Fachdienst nicht zulässig ist, wird der E-Rezept-Tokens als 2D-Code
 742 dargestellt. Er steht damit zum Abscannen, zum Ausdruck oder für eine sonstige
 743 Übertragung außerhalb der TI bereit.

744 3.5.6 Nachrichten durch Versicherten empfangen

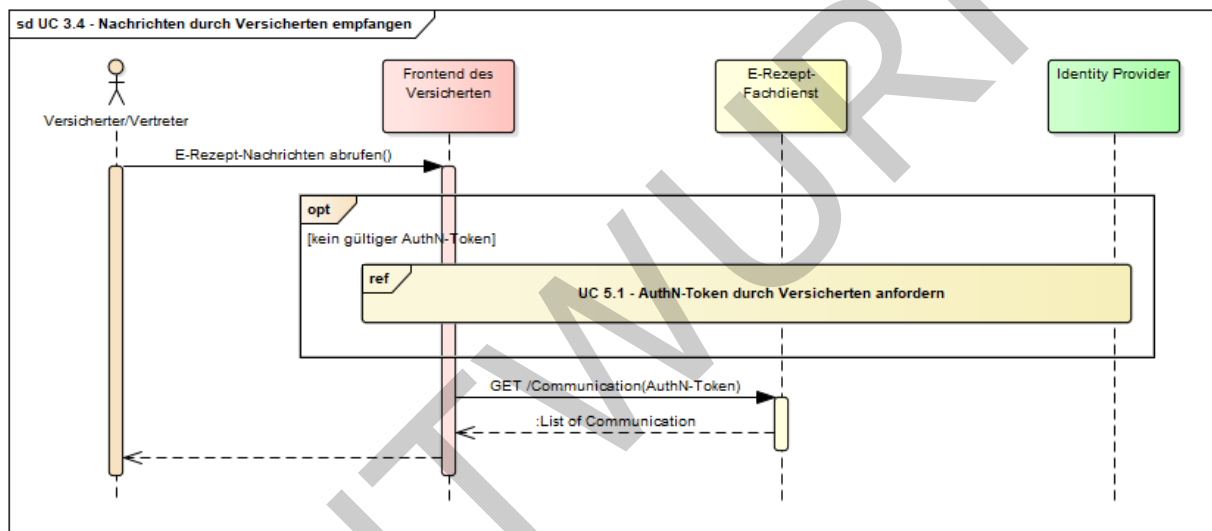
745 Mit diesem Anwendungsfall kann ein Versicherter oder Vertreter eine oder mehrere
 746 Nachrichten von abgebenden LEI zu E-Rezepten mittels der sicheren Übertragung über
 747 die TI empfangen.

748 A_18618 - Anwendungsfall "Nachrichten durch Versicherten empfangen"

749 Alle am Anwendungsfall "Nachrichten durch Versicherten empfangen" beteiligten
 750 Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 11: TAB_SYSLERP_037 Anwendungsfall Nachrichten durch Versicherten empfangen

Name	UC 3.4 - Nachrichten durch Versicherten empfangen
Vorbedingung	<ul style="list-style-type: none"> Ein Mitarbeiter der abgebenden LEI hat den Anwendungsfall "UC 4.7 - Nachricht durch Abgebenden übermitteln" ausgeführt.
Kurzbeschreibung (Außenansicht)	Das FdV fragt beim E-Rezept-Fachdienst an, ob neue Nachrichten für den Nutzer des FdV vorliegen und lädt diese herunter.
Nachbedingung	Die Nachrichten liegen im FdV zur Anzeige bereit.



[<=]

3.5.7 Protokolldaten durch Versicherten einsehen

Mit diesem Anwendungsfall nimmt der Versicherte Einsicht in das Zugriffsprotokoll. Darin ersichtlich sind das Einstellen von E-Rezepten für den Versicherten, alle folgenden Statuswechsel zu diesen E-Rezepten sowie das Löschen von E-Rezepten.

A_18510 - Anwendungsfall "Protokolldaten abrufen"

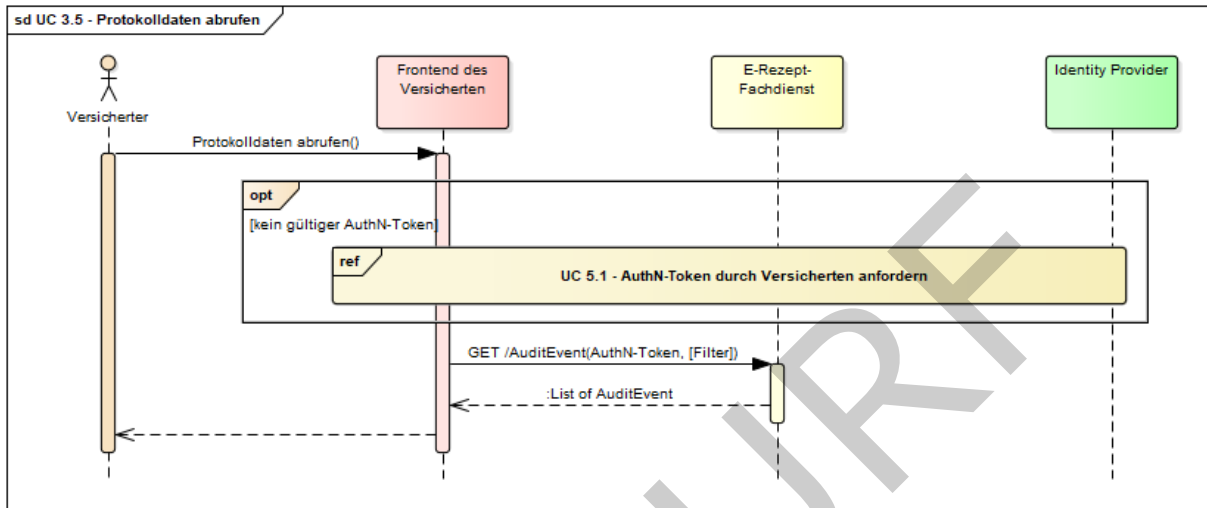
Alle am Anwendungsfall "Protokolldaten abrufen" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 12: TAB_SYSLERP_013 Anwendungsfall Protokolldaten abrufen

Name	UC 3.5 - Protokolldaten abrufen
Vorbedingung	<ul style="list-style-type: none"> keine
Kurzbeschreibung (Außenansicht)	Ein Versicherter ruft über das FdV alle Protokolleinträge zur Anzeige ab.

	Für die Abfrage können Filterkriterien, wie bspw. ein Zeitraum angegeben werden.
Nachbedingung	Die Protokolleinträge stehen zur Anzeige bereit.

765



766

767 [<=]

768

769 3.6 E-Rezept in Apotheke einlösen

770 3.6.1 Nachrichten durch Abgebenden empfangen

771 Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden
 772 Leistungserbringerinstitution Nachrichten vom E-Rezept-Fachdienst abrufen. Alternativ
 773 können E-Rezept-Token als 2D-Code im AVS eingescannt werden.

774 A_18617 - Anwendungsfall "Nachrichten durch Abgebenden empfangen"

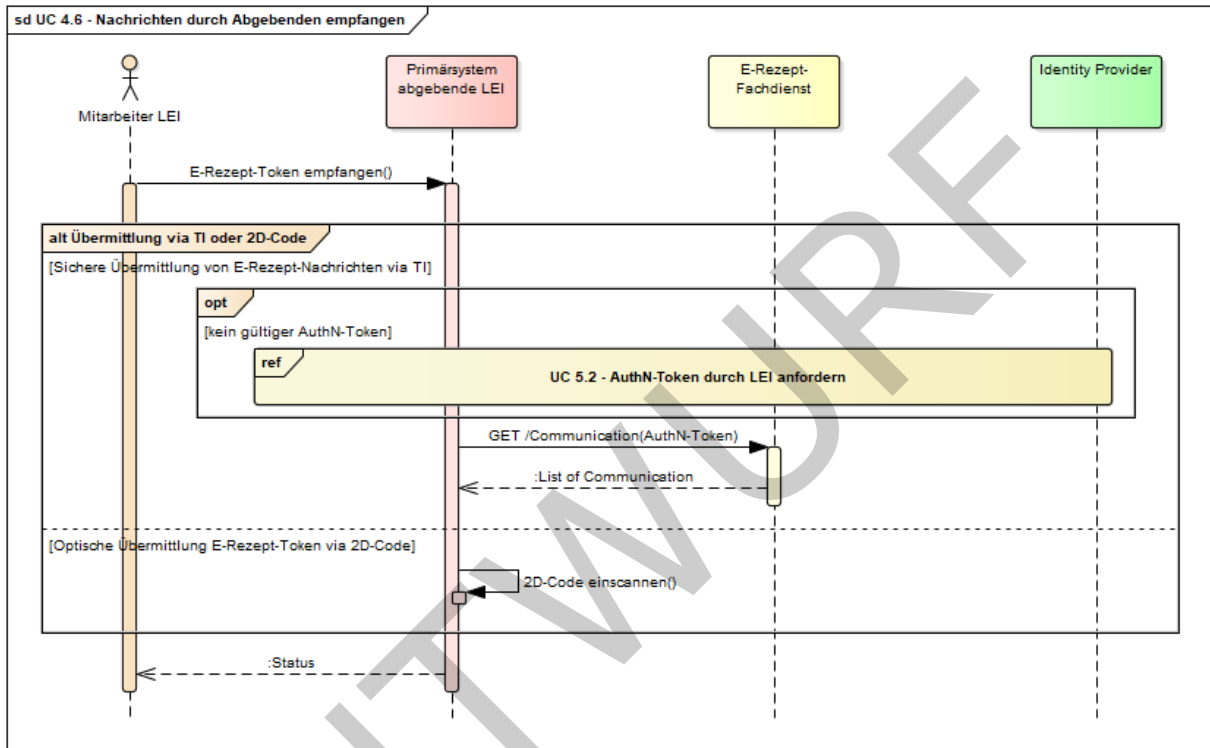
775 Alle am Anwendungsfall "Nachrichten durch Abgebenden empfangen" beteiligten
 776 Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

777 Tabelle 13: TAB_SYSLERP_036 Anwendungsfall Nachrichten durch Abgebenden 778 empfangen

Name	UC 4.6 - Nachrichten durch Abgebenden empfangen
Vorbedingung	<ul style="list-style-type: none"> Ein Versicherter oder Vertreter hat den Anwendungsfall "UC 3.3 - Nachricht durch Versicherten übermitteln" ausgeführt <p>Alternativ kann ein Versicherter oder Vertreter persönlich in der Apotheke den 2D-Code des E-Rezept-Tokens ausgedruckt oder als Anzeige in einem mobilen Gerät dem Abgebenden präsentieren.</p>
Kurzbeschreibung (Außenansicht)	<p>Der Mitarbeiter der abgebenden LEI wählt im PS aus, ob er einen E-Rezept-Token über die TI empfangen möchte oder der E-Rezept-Token als 2D-Code vorliegt.</p> <p>Das Empfangen über die TI erfolgt mithilfe des E-Rezept-</p>

	Fachdienstes. Das PS fragt beim E-Rezept-Fachdienstes an, ob für die Telematik-ID der LEI neue Nachrichten vorliegen und lädt diese herunter. Im Falle der Alternative über den 2D-Code wandelt das PS die optische Repräsentation in die Textform um.
Nachbedingung	Der E-Rezept-Token liegt im PS der abgebenden LEI vor.

779



780

781 [\leq]

782

783 3.6.2 Nachricht durch Abgebenden an Versicherten übermitteln

784 Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden
 785 Leistungserbringerinstitution auf ein mittels dem E-Rezept-Fachdienst übermittelten E-
 786 Rezept-Token reagieren und dem Absender eine Nachricht, bspw. über die
 787 Verfügbarkeit, übermitteln.

788 A_19013 - Anwendungsfall "Nachricht durch Abgebenden übermitteln"

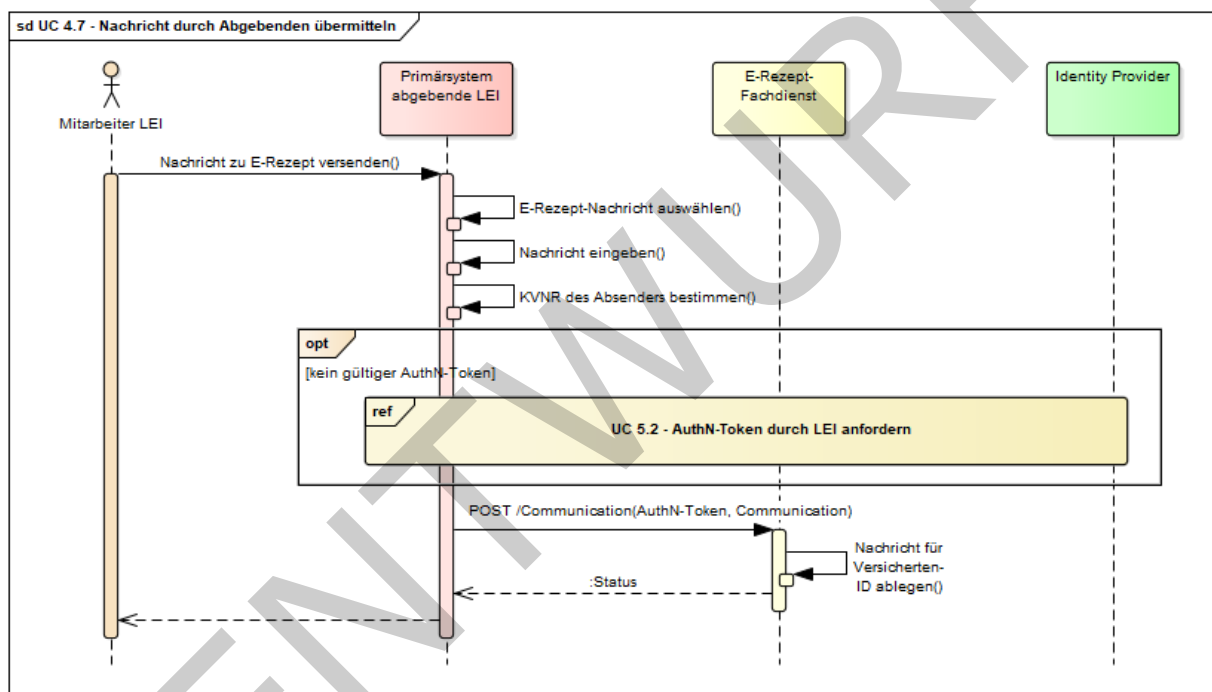
789 Alle am Anwendungsfall "Nachricht durch Abgebenden übermitteln" beteiligten
 790 Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

791 Tabelle 14: TAB_SYSLERP_055 Anwendungsfall Nachricht durch Abgebenden übermitteln

Name	UC 4.7 - Nachricht durch Abgebenden übermitteln
Vorbedingung	<ul style="list-style-type: none"> Ein Versicherter oder Vertreter hat den Anwendungsfall "UC 3.3 - Nachricht durch Versicherten übermitteln" ausgeführt. Ein Mitarbeiter der abgebenden LEI hat den Anwendungsfall

	"UC 4.6 - Nachrichten durch Abgebenden empfangen" durchgeführt.
Kurzbeschreibung (Außenansicht)	<p>Der Mitarbeiter der abgebenden LEI wählt im PS die Nachricht eines Versicherten bzw. Vertreters zu einem E-Rezept aus und erstellt eine Antwortnachricht.</p> <p>Der sichere Versand über die TI erfolgt mithilfe des E-Rezept-Fachdienstes. Als Empfänger wird der Absender der ursprünglichen Nachricht gesetzt.</p> <p>Das PS stellt die Nachricht in den E-Rezept-Fachdienst ein.</p>
Nachbedingung	Der Nachricht liegt im E-Rezept-Fachdienst und kann vom Versicherten bzw. Vertreter asynchron empfangen werden.

792



793

794

[<=]

795

796

3.6.3 E-Rezept durch Abgebenden abrufen

797

798

799

800

Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden Leistungserbringerinstitution ein E-Rezept auf Basis eines durch den Versicherten, einen Vertreter oder die verordnende LEI übermittelten E-Rezept-Tokens aus dem E-Rezept-Fachdienst abrufen.

801

A_18511 - Anwendungsfall "E-Rezept durch Abgebenden abrufen"

802

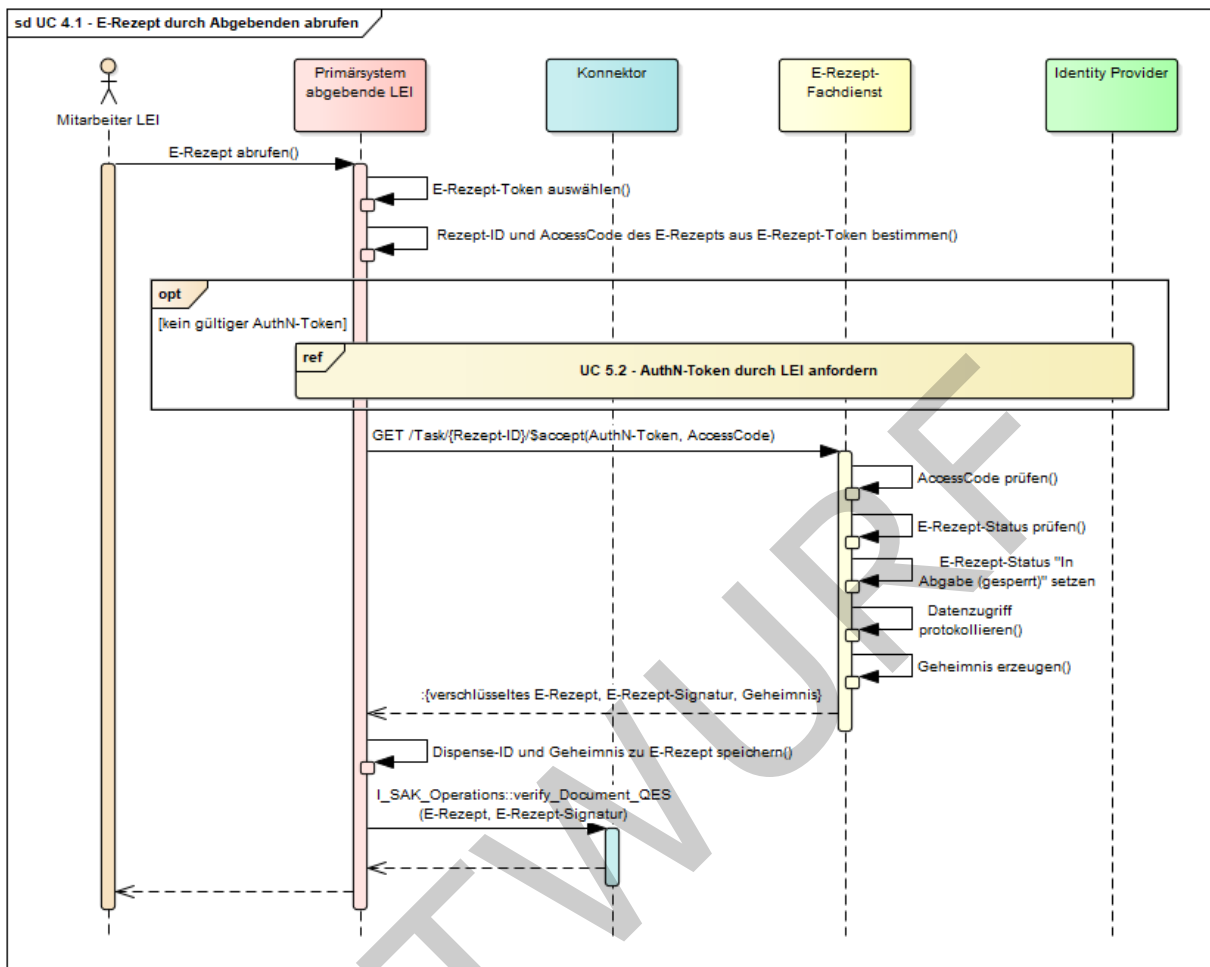
803

Alle am Anwendungsfall "E-Rezept durch Abgebenden abrufen" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

804 **Tabelle 15: TAB_SYSLERP_014 Anwendungsfall E-Rezept durch Abgebenden abrufen**

Name	UC 4.1 - E-Rezept durch Abgebenden abrufen
Vorbedingung	<ul style="list-style-type: none"> Ein Versicherter, ein Vertreter oder eine verordnende LEI haben der abgebenden LEI einen E-Rezept-Token übermittelt. Ein Mitarbeiter der abgebenden LEI hat den Anwendungsfall "UC 4.6 - Nachrichten durch Abgebenden empfangen" durchgeführt. Der E-Rezept-Token liegt im Primärsystem vor. Das E-Rezept im E-Rezept-Fachdienst hat den Status "offen".
Kurzbeschreibung (Außenansicht)	<p>Ein Mitarbeiter der abgebenden LEI wählt einen E-Rezept-Token zum Abruf im PS aus.</p> <p>Das PS ermittelt die Rezept-ID und den AccessCode aus dem E-Rezept-Token.</p> <p>Das PS ruft mit der Rezept-ID und dem AccessCode das E-Rezept vom E-Rezept-Fachdienst ab.</p> <p>Der Status des E-Rezepts im E-Rezept-Fachdienst wird auf "in Abgabe (gesperrt)" geändert.</p> <p>Der E-Rezept-Fachdienst erzeugt ein Geheimnis zur Statusänderung "in Abgabe (gesperrt)", welches im E-Rezept-Fachdienst gespeichert und dem PS zusammen mit dem E-Rezept übermittelt wird.</p> <p>Das PS prüft die Gültigkeit der QES des E-Rezepts mittels Konnektor.</p>
Nachbedingung	<p>Das E-Rezept hat im E-Rezept-Fachdienst den Status "in Abgabe (gesperrt)".</p> <p>Der Statuswechsel ist im E-Rezept-Fachdienst protokolliert.</p> <p>Das E-Rezept steht zur Anzeige im AVS bereit.</p> <p>Das Geheimnis zur Statusänderung "in Abgabe (gesperrt)" ist im PS gespeichert.</p>

805



806

807 [\leq]

808 3.6.4 E-Rezept durch Abgebenden zurückgeben

809 Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden
 810 Leistungserbringerinstitution, ein zuvor aus dem E-Rezept-Fachdienst abgerufenes E-
 811 Rezept zurückgeben, wenn die Abgabe des E-Rezepts nicht vollzogen werden kann oder
 812 soll.

813 A_18512 - Anwendungsfall "E-Rezept durch Abgebenden zurückgeben"

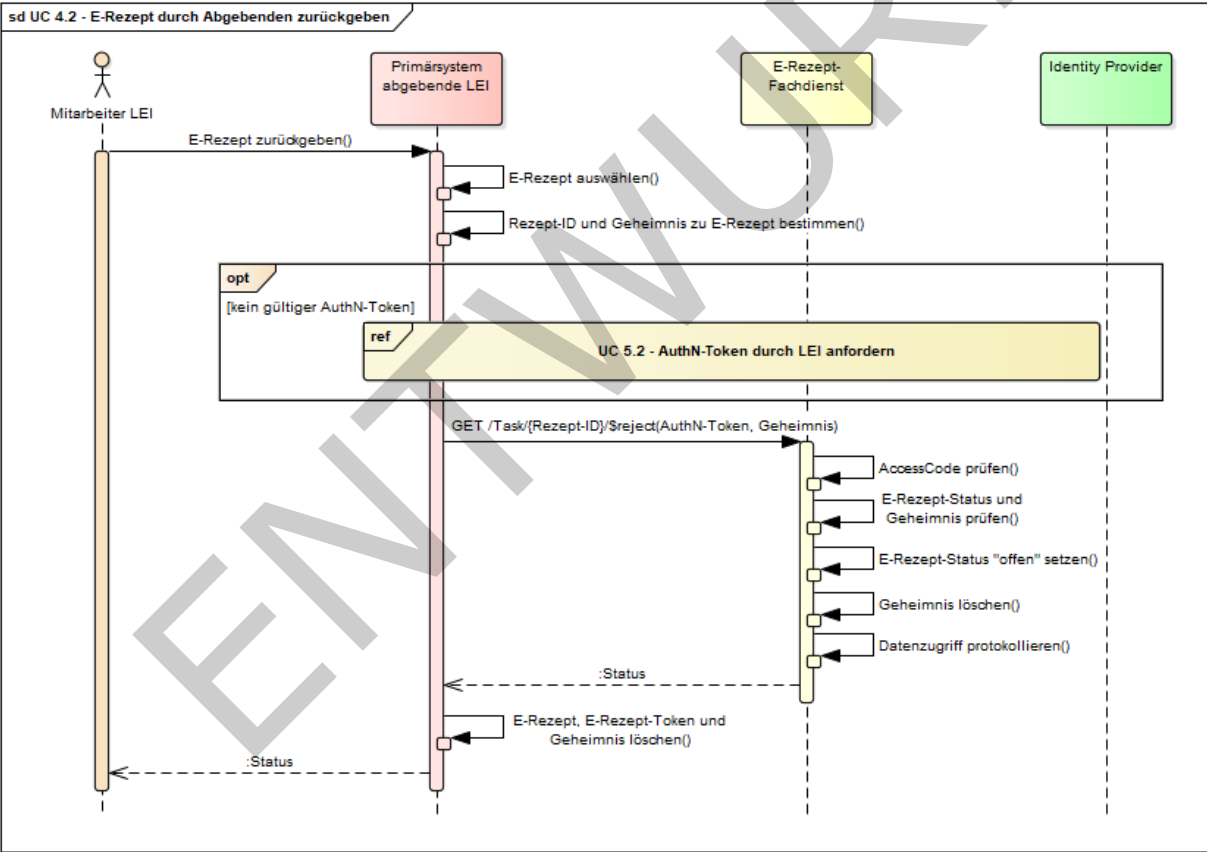
814 Alle am Anwendungsfall "E-Rezept durch Abgebenden zurückgeben" beteiligten
 815 Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

816 **Tabelle 16: TAB_SYSLERP_015 Anwendungsfall E-Rezept durch Abgebenden**
 817 **zurückgeben**

Name	UC 4.2 - E-Rezept durch Abgebenden zurückgeben
Vorbedingung	<ul style="list-style-type: none"> Ein Mitarbeiter der abgebenden LEI hat den Anwendungsfall "UC 4.1 - E-Rezept durch Abgebenden abrufen" durchgeführt. Die Rezept-ID, der AccessCode und das Geheimnis zur Statusänderung "in Abgabe (gesperrt)" sind im PS bekannt.

	<ul style="list-style-type: none">Das E-Rezept im E-Rezept-Fachdienst hat den Status "in Abgabe (gesperrt)".
Kurzbeschreibung (Außenansicht)	Ein Mitarbeiter der abgebenden LEI markiert über das PS ein E-Rezept zum Zurückgeben und bestätigt es. Das PS übermittelt beim Aufruf des E-Rezept-Fachdienstes die Rezept-ID, den AccessCode und das Geheimnis zur Statusänderung "in Abgabe (gesperrt)". Der Status des E-Rezepts im E-Rezept-Fachdienst wird geändert.
Nachbedingung	Das E-Rezept im E-Rezept-Fachdienst hat den Status "offen". Der Statuswechsel des E-Rezepts zum Status "offen" ist im E-Rezept-Fachdienst protokolliert. Das E-Rezept, der E-Rezept-Token und das Geheimnis zur Statusänderung "in Abgabe (gesperrt)" sind im PS gelöscht.

818



819

820 [\leq]

821

822 **3.6.5 E-Rezept durch Abgebenden löschen**

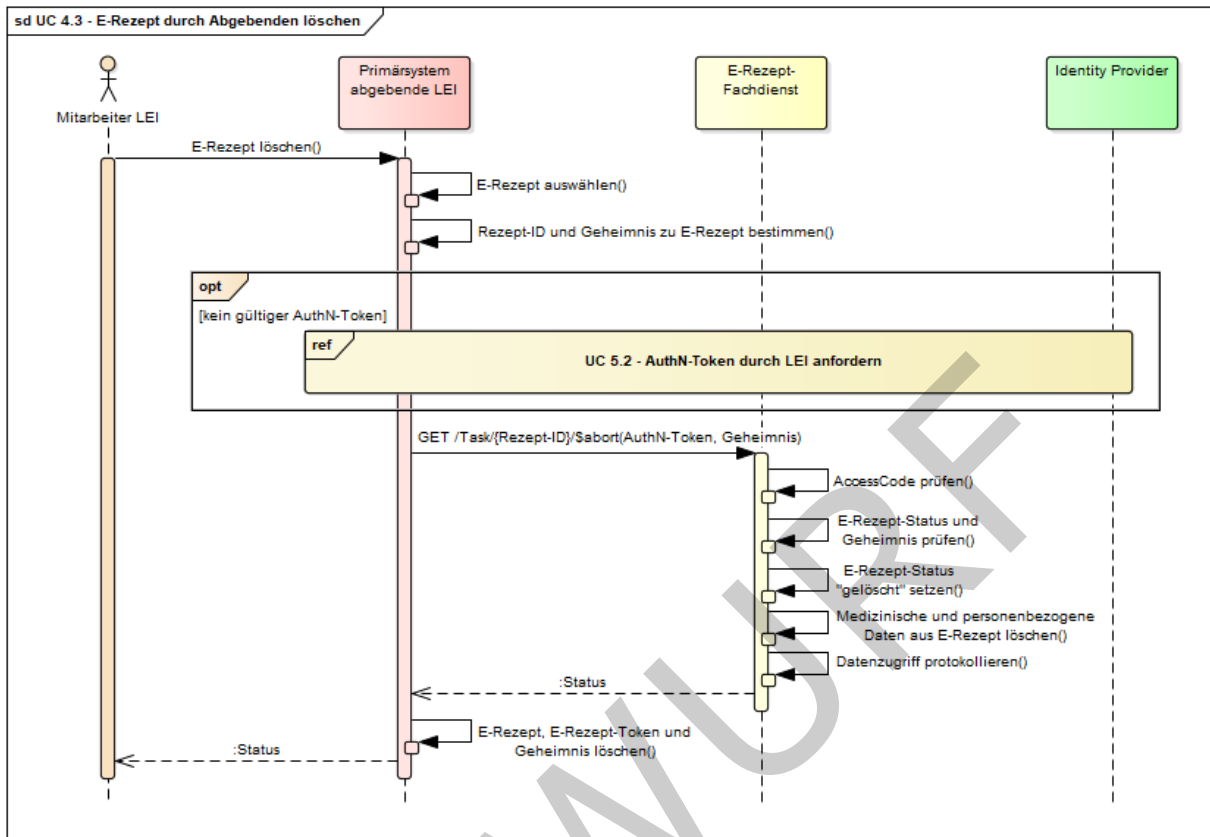
823 Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden
824 Leistungserbringerinstitution den Status für ein zuvor aus dem E-Rezept-Fachdienst
825 abgerufenes E-Rezept auf "gelöscht" setzen. Die Nutzer können auf ein E-Rezept mit dem
826 Status "gelöscht" nicht zugreifen.

827 **A_18513 - Anwendungsfall "E-Rezept durch Abgebenden löschen"**
 828 Alle am Anwendungsfall "E-Rezept durch Abgebenden löschen" beteiligten Produkttypen
 829 und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

830 **Tabelle 17: TAB_SYSLERP_016 Anwendungsfall E-Rezept durch Abgebenden löschen**

Name	UC 4.3 - E-Rezept durch Abgebenden löschen
Vorbedingung	<ul style="list-style-type: none"> • Ein Versicherter, ein Vertreter oder eine verordnende LEI hat der abgebenden LEI einen E-Rezept-Token übermittelt. • Der Versicherte hat der abgebenden LEI seinen Wunsch zum Löschen des E-Rezepts mitgeteilt • Ein Mitarbeiter der abgebenden LEI hat die Anwendungsfälle "UC 4.6 - Nachrichten durch Abgebenden empfangen" und "UC 4.1 - E-Rezept durch Abgebenden abrufen" durchgeführt. • Die Rezept-ID, der AccessCode und das Geheimnis zur Statusänderung "in Abgabe (gesperrt)" sind im PS bekannt. • Das E-Rezept im E-Rezept-Fachdienst hat den Status "in Abgabe (gesperrt)".
Kurzbeschreibung (Außenansicht)	<p>Ein Mitarbeiter der abgebenden LEI markiert über das PS ein Rezept zum Löschen und bestätigt es.</p> <p>Das PS übermittelt beim Aufruf des E-Rezept-Fachdienstes die Rezept-ID, den AccessCode und das Geheimnis zur Statusänderung "in Abgabe (gesperrt)".</p> <p>Der Status des E-Rezepts im E-Rezept-Fachdienst wird geändert. Die personenbezogenen und medizinischen Daten im E-Rezept werden gelöscht.</p>
Nachbedingung	<p>Das E-Rezept im E-Rezept-Fachdienst hat den Status "gelöscht". Es beinhaltet keine personenbezogenen oder medizinischen Daten.</p> <p>Der Statuswechsel des E-Rezepts zum Status "gelöscht" ist im E-Rezept-Fachdienst protokolliert.</p> <p>Das E-Rezept, der E-Rezept-Token und das Geheimnis sind im PS gelöscht.</p>

831



832

833 [\leq]

834 3.6.6 Quittung abrufen

835 Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden
 836 Leistungserbringerinstitution ein zuvor aus dem E-Rezept-Fachdienst abgerufenes E-
 837 Rezept nach der Abgabe des Mittels als "quittiert" kennzeichnen und erhält eine Quittung.

838 A_18514 - Anwendungsfall "Quittung abrufen"

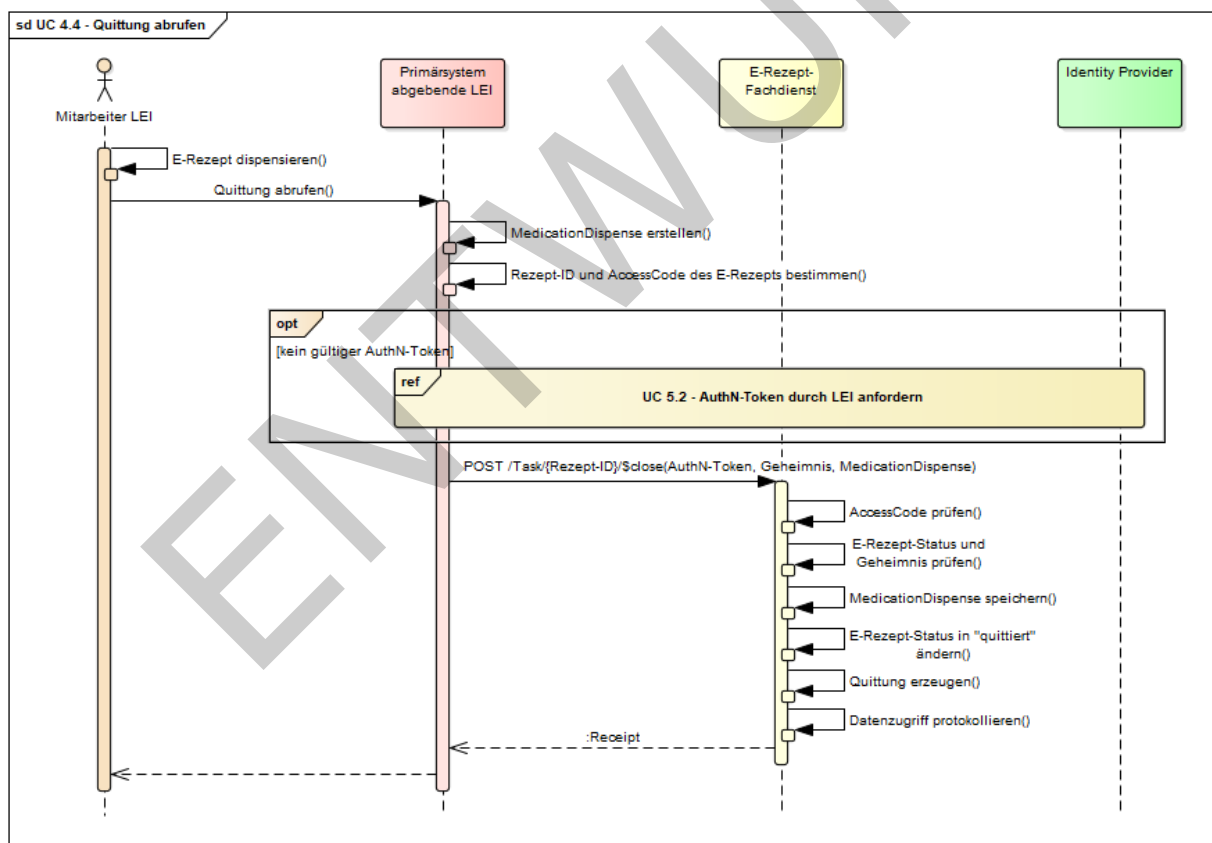
839 Alle am Anwendungsfall "Quittung abrufen" beteiligten Produkttypen und Komponenten
 840 MÜSSEN die nachfolgenden Festlegungen umsetzen.

841 **Tabelle 18: TAB_SYSLERP_017 Anwendungsfall Quittung abrufen**

Name	UC 4.4 - Quittung abrufen
Vorbedingung	<ul style="list-style-type: none"> Ein Mitarbeiter der abgebenden LEI hat den Anwendungsfall "UC 4.1 - E-Rezept durch Abgebenden abrufen" durchgeführt. Das Primärsystem hat die QES des E-Rezepts erfolgreich geprüft. Die QES des E-Rezepts ist gültig. Die Rezept-ID, der AccessCode und das Geheimnis zur Statusänderung "in Abgabe (gesperrt)" des E-Rezepts sind im PS bekannt.

	<ul style="list-style-type: none"> Das E-Rezept im E-Rezept-Fachdienst hat den Status "in Abgabe (gesperrt)".
Kurzbeschreibung (Außenansicht)	<p>Ein Mitarbeiter der abgebenden LEI hat ein E-Rezept dispensiert. Er markiert das E-Rezept über das PS als abgegeben und bestätigt es. Das PS übermittelt beim Aufruf des E-Rezept-Fachdienstes die Rezept-ID, den AccessCode und das Geheimnis zur Statusänderung "in Abgabe (gesperrt)" und die Informationen zur Abgabe. Der Status des E-Rezepts im E-Rezept-Fachdienst wird geändert. Der E-Rezept-Fachdienst erstellt eine Quittung und übermittelt diese an das PS.</p>
Nachbedingung	<p>Das E-Rezept im E-Rezept-Fachdienst hat den Status "quittiert". Die Information zur Abgabe liegen im E-Rezept-Fachdienst. Der Statuswechsel des E-Rezepts zum Status "quittiert" ist im E-Rezept-Fachdienst protokolliert. Im PS liegt eine Quittung vor, welche bspw. für die Abrechnung des E-Rezepts genutzt werden kann.</p>

842



843

844 [<=]

845 3.6.7 Quittung erneut abrufen

846 Falls beim Aufruf der Operation "UC 4.4 - Quittung abrufen" ein Fehler bei der
 847 Übertragung der Quittung an das AVS auftrat, hat die abgebende LEI die Möglichkeit, die
 848 zuvor erstellte Quittung noch einmal abzurufen.

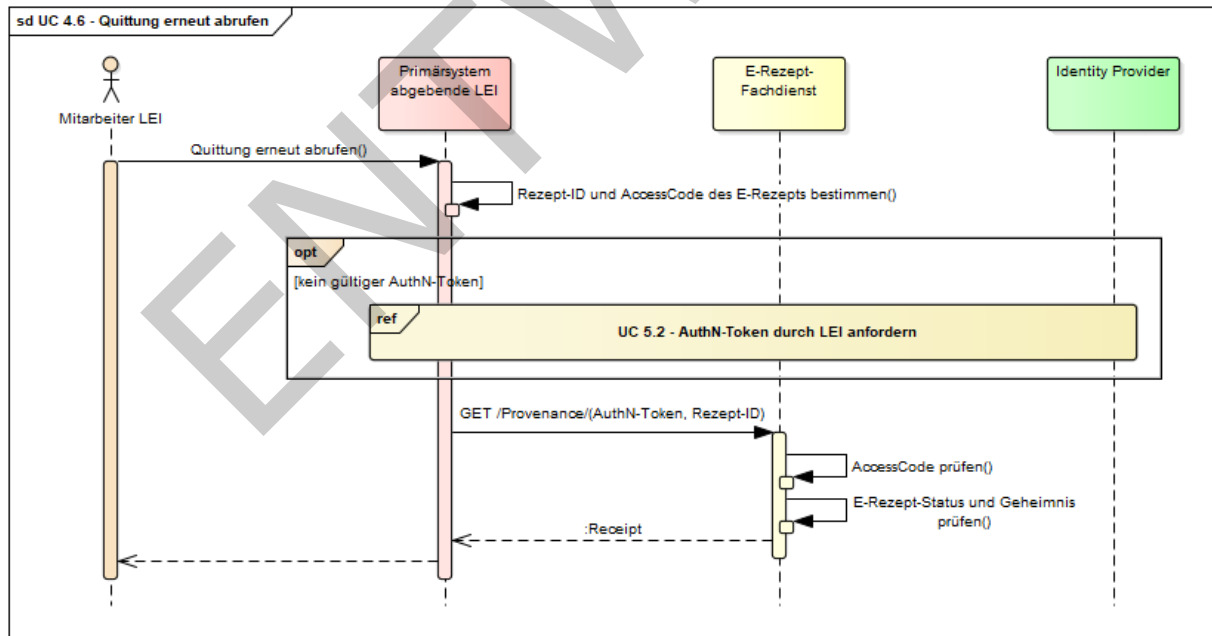
Der Anwendungsfall führt zu keiner Änderung am Status des E-Rezepts.

A_19117 - Anwendungsfall "Quittung erneut abrufen"

Alle am Anwendungsfall "Quittung erneut abrufen" beteiligten Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

Tabelle 19: TAB_SYSLERP_057 Anwendungsfall Quittung erneut abrufen

Name	UC 4.8 - Quittung erneut abrufen
Vorbedingung	<ul style="list-style-type: none"> Ein Mitarbeiter der abgebenden LEI hat den Anwendungsfall "UC 4.4 - Quittung abrufen" durchgeführt. Im PS liegt <u>keine</u> Quittung vor. Das E-Rezept im E-Rezept-Fachdienst hat den Status "quittiert".
Kurzbeschreibung (Außenansicht)	<p>Ein Mitarbeiter der abgebenden LEI wählt das E-Rezept über das PS aus, um erneut die Quittung abzurufen.</p> <p>Das PS übermittelt beim Aufruf des E-Rezept-Fachdienstes die Rezept-ID, den AccessCode und das Geheimnis zur Statusänderung "in Abgabe (gesperrt)".</p> <p>Der E-Rezept-Fachdienst übermittelt die im Anwendungsfall "UC 4.4 - Quittung abrufen" erstellte Quittung an das PS.</p>
Nachbedingung	Im PS liegt eine Quittung vor, welche bspw. für die Abrechnung des E-Rezepts genutzt werden kann.



[<=]

858 **3.6.8 Dispensierdatensatz durch Abgebenden signieren**

859 Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden
860 Leistungserbringerinstitution einen Dispensierdatensatz signieren. Erfolgt bei der
861 Belieferung des E-Rezepts eine Änderung der Verschreibung nach § 17 (5) ApoBetrO,
862 dann wird ein QES aufgebracht, anderenfalls wird fortgeschritten signiert.

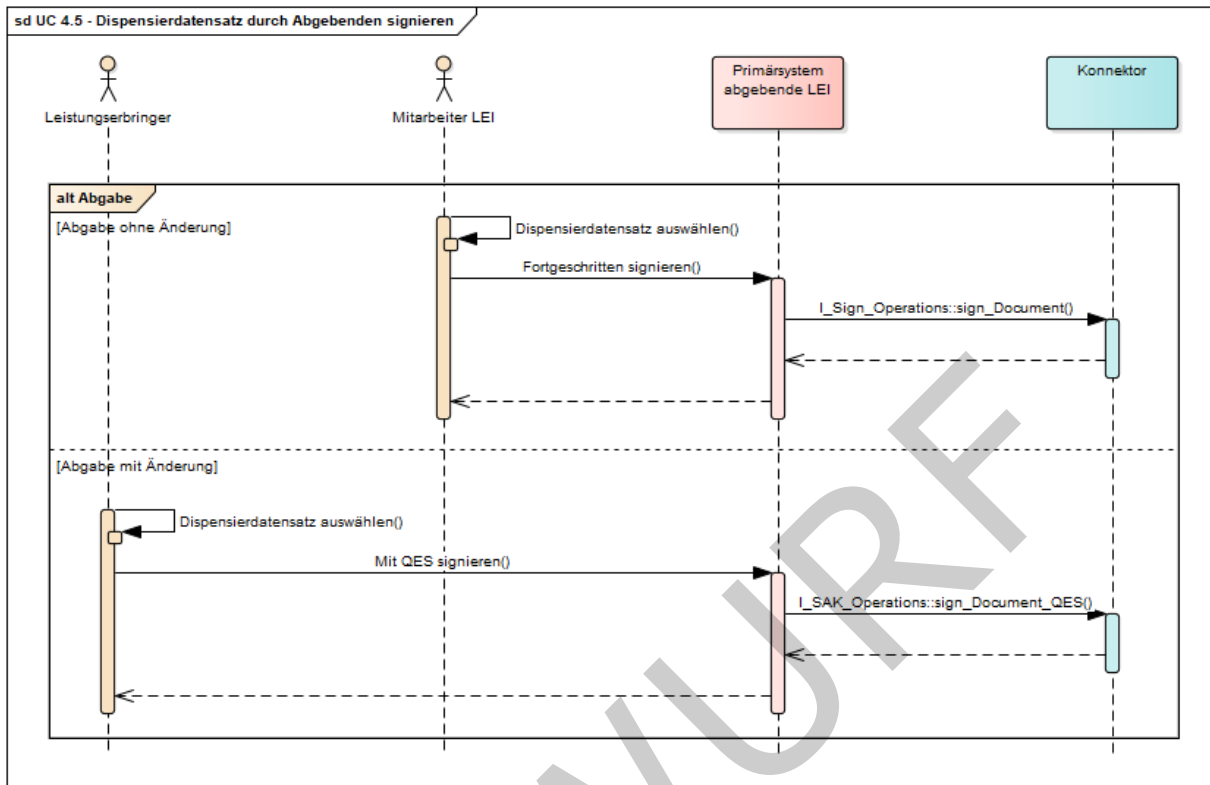
863 **A_18515 - Anwendungsfall "Dispensierdatensatz durch Abgebenden signieren"**

864 Alle am Anwendungsfall "Dispensierdatensatz durch Abgebenden signieren" beteiligten
865 Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

866 **Tabelle 20: TAB_SYSLERP_018 Anwendungsfall Dispensierdatensatz durch Abgebenden**
867 **signieren**

Name	UC 4.5 - Dispensierdatensatz durch Abgebenden signieren
Vorbedingung	<ul style="list-style-type: none">• Ein E-Rezept wurde dispensiert.• Der Dispensierdatensatz steht zum Signieren im PS bereit.• Der HBA bzw. eine SMC-B ist für das Signieren gesteckt und freigeschaltet.
Kurzbeschreibung (Außenansicht)	Falls die Abgabe ohne Änderung erfolgte, signiert ein Mitarbeiter der abgebenden LEI den Dispensierdatensatz mit einer fortgeschrittenen Signatur. Falls die Abgabe mit Änderung der Verschreibung nach § 17 (5) ApoBetrO erfolgte, signiert der abgebende Leistungserbringer den Dispensierdatensatz mit einer QES.
Nachbedingung	Der Dispensierdatensatz ist durch den Abgebenden signiert.

868



869

870 [\leq]

871 3.7 Anfordern von Identitätsbestätigungen

872 3.7.1 Identitätsbestätigung durch den Versicherten anfordern

873 Dieser Anwendungsfall betrifft die Anforderung eine Identitätsbestätigung (AuthN-Token)
 874 für den aktuellen Nutzer durch das FdV. Er ist Bestandteil aller Anwendungsfälle, die für
 875 einen Zugriff auf einen Dienst der TI (Ausnahme: Zugriff auf IdP) ein solches Token
 876 benötigen, siehe die Ablaufbeschreibungen (Sequenzdiagramme) der oben aufgeführten
 877 Anwendungsfälle.

878 A_18822 - Anwendungsfall "AuthN-Token durch Versicherten anfordern"

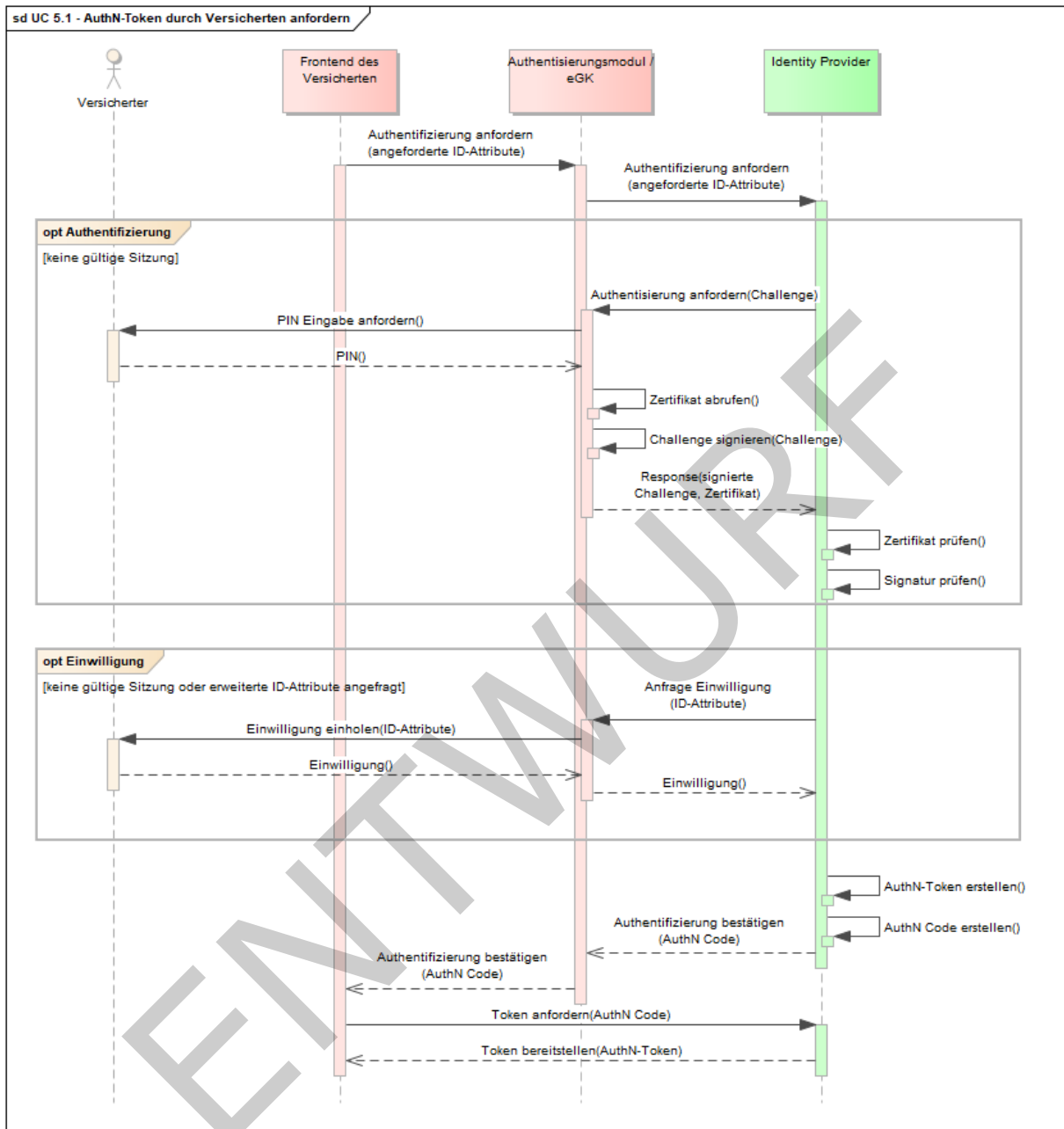
879 Alle am Anwendungsfall "AuthN-Token durch Versicherten anfordern" beteiligten
 880 Produkttypen und Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

881 Tabelle 21: TAB_SYSLERP_045 AuthN-Token durch Versicherten anfordern

Name	UC 5.1 - AuthN-Token durch Versicherten anfordern
Vorbedingung	<ul style="list-style-type: none"> Die eGK des Versicherten kann über Gerät des Nutzers gelesen werden Es liegt kein gültiger AuthN-Token vor (zeitlich nicht mehr gültig oder fehlende Identitätsattribute)

Kurzbeschreibung (Außensicht)	<ol style="list-style-type: none">1. Das FdV übergibt die Authentifizierungs-Anforderung mit den angeforderten Identitätsmerkmalen an das Authentisierungsmodul.2. Dieses leitet die Anforderung an den IdP weiter.3. <i>Falls beim IdP keine gültige Sitzung vorliegt:</i> Authentifizierung des Versicherten per Challenge/Response-Verfahren (eGK). Das Authentisierungsmodul greift dazu auf die AUT-Identität der eGK zu.4. <i>Falls beim IdP keine gültige Sitzung vorliegt oder erweiterte Identitätsattribute angefragt sind:</i> Einholen einer Einwilligung des Versicherten zur Bereitstellung der Identitätsattribute über das Authentisierungsmodul.5. Der IdP erstellt AuthN-Token mit den angefragten und bestätigten Identitätsattributen und einen zugehörigen AuthN Code.6. Der IdP übergibt den AuthN Code an das Authentisierungsmodul.7. Das Authentisierungsmodul übergibt den AuthN Code an das FdV.8. Das FdV fragt mittels des erhaltenen AuthN Codes den AuthN-Token beim IdP ab.9. Der IdP stellt dem FdV den AuthN-Token bereit.
Nachbedingung	Ein AuthN-Token mit den angeforderten Identitätsmerkmalen liegt im FdV vor.

882



883

884 [\leq]

885 3.7.2 Identitätsbestätigung durch LEI anfordern

886 Dieser Anwendungsfall betrifft die Anforderung eines AuthN-Tokens durch eine LEI über
 887 das Primärsystem. Er ist Bestandteil aller Anwendungsfälle, die für einen Zugriff auf
 888 einen Dienst der TI (Ausnahme: Zugriff auf IdP) ein solches Token benötigen, siehe die
 889 Ablaufbeschreibungen (Sequenzdiagramme) der oben aufgeführten Anwendungsfälle.

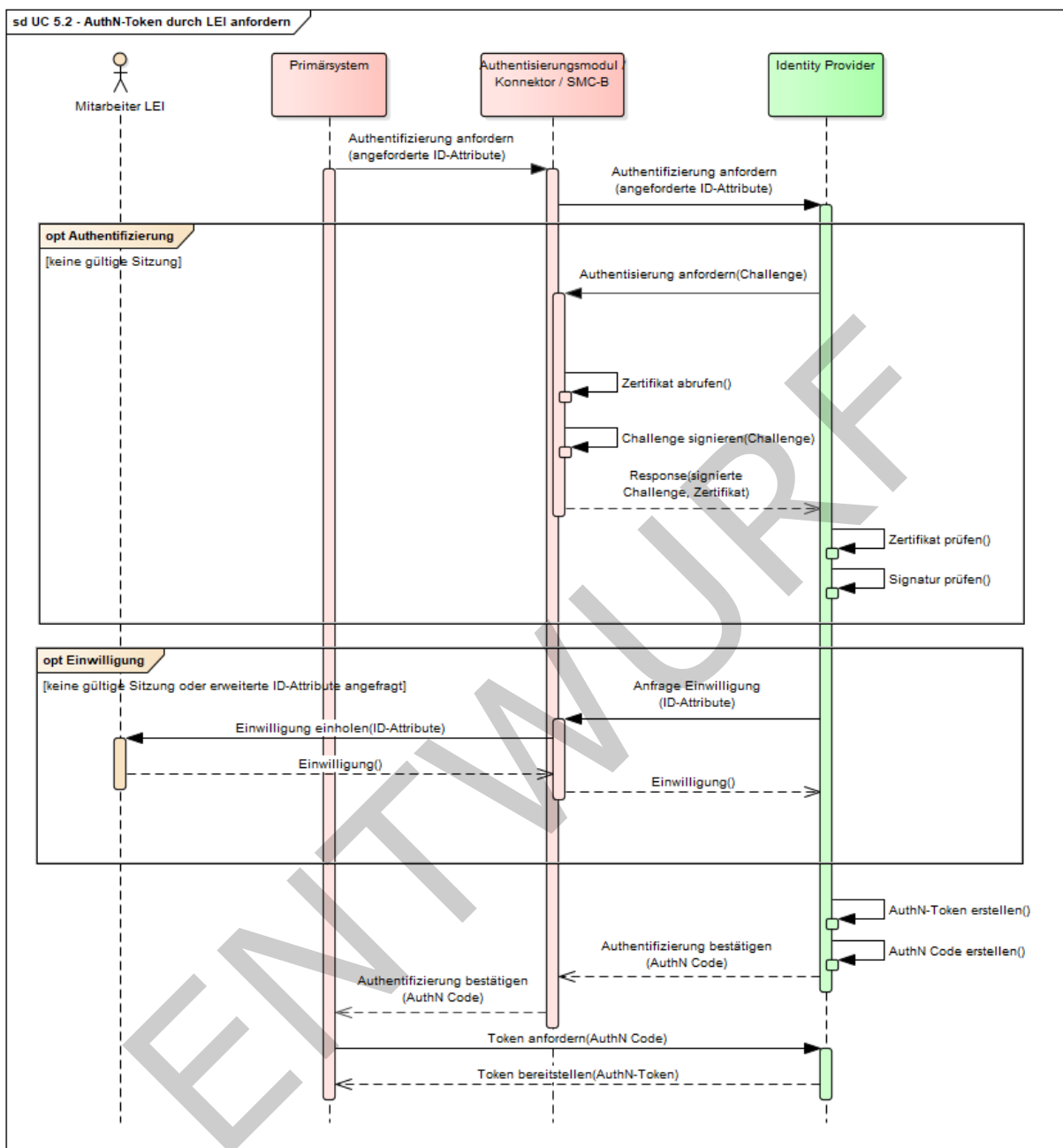
890 A_18827 - Anwendungsfall "AuthN-Token durch LEI anfordern"

891 Alle am Anwendungsfall "AuthN-Token durch LEI anfordern" beteiligten Produkttypen und
 892 Komponenten MÜSSEN die nachfolgenden Festlegungen umsetzen.

893 **Tabelle 22 TAB_SYSLERP_046 AuthN-Token durch LEI anfordern**

Name	UC 5.2 - AuthN-Token durch LEI anfordern
Vorbedingung	<ul style="list-style-type: none"> • SMC-B ist gesteckt und freigeschaltet • Es liegt kein gültiger AuthN-Token vor (zeitlich nicht mehr gültig oder fehlende Identitätsattribute).
Kurzbeschreibung (Außensicht)	<ol style="list-style-type: none"> 1. Das Client System (PS/AVS) übergibt die Authentifizierungs-Anforderung mit den angeforderten Identitätsmerkmalen an das Authentisierungsmodul. 2. Dieses leitet die Anforderung an den IdP weiter. 3. <i>Falls beim IdP keine gültige Sitzung vorliegt:</i> Authentifizierung der LEI per Challenge/Response-Verfahren (SMC-B). Das Authentisierungsmodul greift dazu über die Konnektorschnittstelle <code>I_Sign_Operations::external_authenticate</code> auf die AUT-Identität der SMC-B zu. 4. <i>Falls beim IdP keine gültige Sitzung vorliegt oder erweiterte Identitätsattribute angefragt sind:</i> Einholen einer Einwilligung des LEI-Mitarbeiters zur Bereitstellung der Identitätsattribute über das Authentisierungsmodul. 5. Der IdP erstellt AuthN-Token mit den angefragten und bestätigten Identitätsattributen und einen zugehörigen AuthN Code. 6. Der IdP übergibt den AuthN Code an das Authentisierungsmodul. 7. Das Authentisierungsmodul übergibt den Code an das Client System (PVS/AVS). 8. Das Client System (PVS/AVS) fragt mittels des erhaltenen AuthN Codes den AuthN-Token beim IdP ab. 9. Der IdP stellt dem Client System (PVS/AVS) den AuthN-Token bereit.
Nachbedingung	Ein AuthN-Token mit den angeforderten Identitätsmerkmalen liegt im Client System vor.

894



[<=]

895

896

897

4 Systemzerlegung (Deployment)

Die Fachanwendung E-Rezept realisiert die fachlichen Anwendungsfälle über das Zusammenspiel mehrerer Produkttypen in verschiedenen Zonen der TI. Die Systemzerlegung der Fachanwendung ist in der nachfolgenden Abbildung "Systemzerlegung E-Rezept" dargestellt. Sie ordnet die fachanwendungsspezifischen Produkttypen (blau dargestellt) und ihre Komponenten den Zonen gemäß Zonenmodell der TI-Plattform aus [gemKPT_Arch_TIP] zu.

Fachanwendungsübergreifende zentrale Produkttypen, für die sich mit der Einführung der Fachanwendung E-Rezept zusätzliche Anforderungen ergeben, sind grün dargestellt.

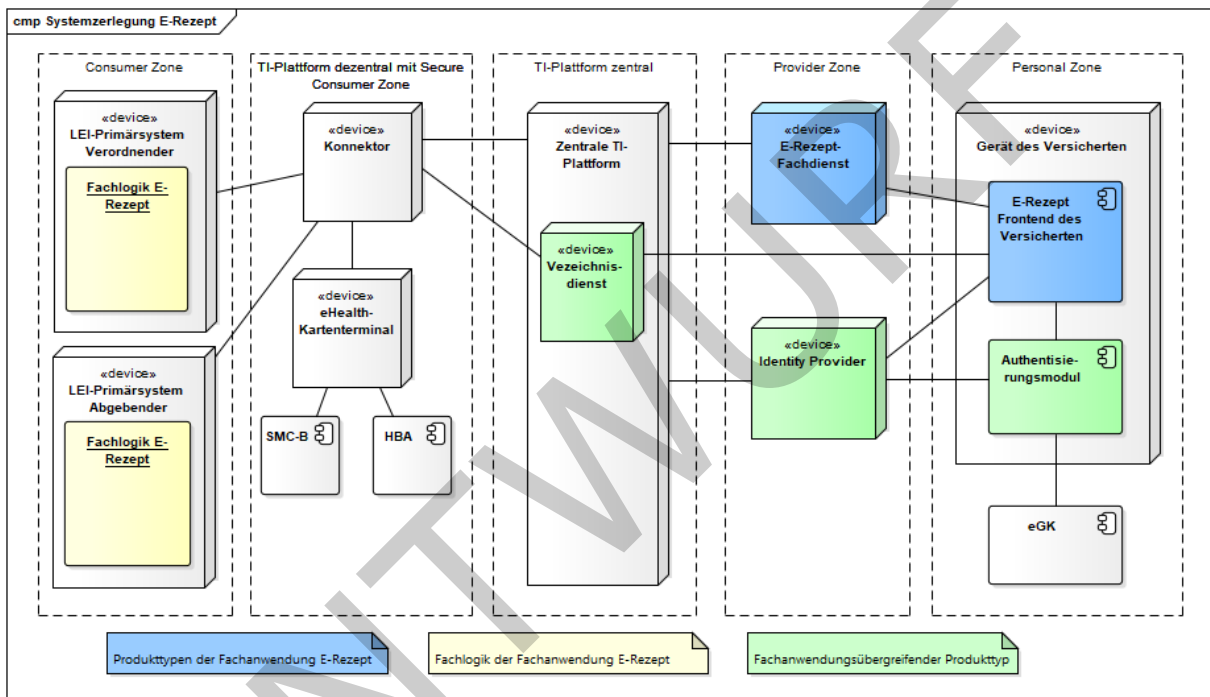


Abbildung 7: ABB_SYSLERP_006 Systemzerlegung E-Rezept

Der E-Rezept-Fachdienst verwaltet die durch die Verordnenden eingestellten E-Rezepte und stellt sicher, dass die Statusänderungen nur entsprechend dem Statusmodell durchgeführt werden. Der E-Rezept-Fachdienst erstellt und verwaltet die Zugriffsprotokolle für die E-Rezepte.

Der E-Rezept-Fachdienst ermöglicht die sichere Übertragung von E-Rezept-Token zwischen Versicherten, Vertretern und Abgebenden über die TI. Wenn der Empfänger eine Apotheke ist, kann diese im Verzeichnisdienst der TI ausgewählt werden. Die Übertragung erfolgt asynchron.

Folgende anwendungsübergreifenden Dienste der Provider Zone werden durch die fachanwendungsspezifischen Produkttypen und Komponenten genutzt.

Der Identity Provider authentifiziert Akteure und erstellt Identitätstoken, auf deren Basis die fachanwendungsspezifischen und fachanwendungsübergreifenden Dienste den Zugriff auf Ressourcen autorisieren.

Der Verzeichnisdienst der TI ermöglicht die Suche nach abgebenden LEIs für Versicherte, Vertreter und verordnende LEIs für die Übermittlung von E-Rezept-Token.

4.1 Produkttypen der Fachanwendung E-Rezept

Es besteht die Möglichkeit, dass E-Rezept-Token optisch übertragen werden. Dafür wird eine Darstellung von E-Rezept-Token als 2D-Code vorgesehen. Der bundeseinheitliche Medikationsplan (BMP) besitzt eine Darstellung als DataMatrix-Code, welcher durch die Primärsysteme der Leistungserbringer seit Oktober 2016 gedruckt und gescannt werden kann. Durch die weite Verbreitung bietet sich die Verwendung des gleichen Standards auch in der Fachanwendung E-Rezept an.

A_18516 - E-Rezept-Token als DataMatrix-Code unterstützen

Das Primärsystem und das Frontend des Versicherten MÜSSEN den E-Rezept-Token in seiner Kodierung als DataMatrix-Code gemäß ISO/IEC 16022 unterstützen. [<=]

Neben dem E-Rezept-Fachdienst bieten auch der Verzeichnisdienst und der Identity Provider, welche für die Anwendung E-Rezept genutzt werden, ihre Dienste im Internet an.

A_18792 - Sicherung der TI

Die durch die Fachanwendung E-Rezept genutzten Dienste, welche ihren Dienst im Internet anbieten, MÜSSEN die TI gegenüber dem Internet absichern. [<=]

Um ein Single Sign-On zu ermöglichen, werden die Nutzer von den Diensten mittels einer durch einen IdP ausgestellten Identitätsbestätigung authentifiziert.

A_18793 - Authentifizierung mittels AuthN-Token

Die durch die Fachanwendung E-Rezept genutzten Dienste, außer dem Identity Provider, MÜSSEN Leistungserbringerinstitutionen und Versicherte über einen durch einen Identity Provider der TI erstellte Identitätsbestätigung (AuthN-Token) authentifizieren. [<=]

A_18794 - Zugang zu Diensten nur nach Authentifizierung

Die Dienste der Fachanwendung E-Rezept MÜSSEN sicherstellen, dass nur nach erfolgreicher Authentifizierung der Zugang zum Dienst gewährt wird. [<=]

4.1.1 Produkttyp E-Rezept-Fachdienst

Der E-Rezept-Fachdienst ist ein offener fachanwendungsspezifischer Dienst in der TI zum Speichern der E-Rezepte. Er ist im Zonenmodell der TI-Plattform der Provider Zone zugeordnet.

Es gibt genau einen Anbieter für den E-Rezept-Fachdienst, d.h. alle Akteure greifen auf denselben Dienst zu.

A_18517 - E-Rezept-Fachdienst – Ressource E-Rezept

Der E-Rezept-Fachdienst MUSS die Ressourcen E-Rezept und Zugriffsprotokolleintrag verwalten und für die Ressourcen die Operationen gemäß TAB_SYSLERP_019 anbieten.

Tabelle 23: TAB_SYSLERP_019 Schnittstellen E-Rezept-Fachdienst

Ressource	Operation	Nutzer
E-Rezept	E-Rezept-ID abrufen E-Rezept einstellen E-Rezept durch Verordnenden löschen	Verordnender

E-Rezept	E-Rezept durch Abgebenden abrufen E-Rezept durch Abgebenden löschen E-Rezept durch Abgebenden zurückgeben Quittung abrufen Quittung erneut abrufen	Abgebender
E-Rezept	E-Rezepte durch Versicherten abrufen E-Rezept durch Versicherten löschen	Versicherter
Zugriffsprotokolleintrag	Zugriffsprotokolleinträge durch Versicherten abrufen	Versicherter
E-Rezept-Nachricht	E-Rezept-Nachricht einstellen E-Rezept-Nachrichten abrufen	Versicherter Vertreter Abgebender

960 [\leq]

961 **A_18519 - E-Rezept-Fachdienst – Rezept-ID erzeugen**

962 Der E-Rezept-Fachdienst MUSS Rezept-IDs erzeugen, welche mindestens über einen
963 Zeitraum von 10 Jahren eindeutig sind. [\leq]

964 Die Rezept-ID ist Teil des fachlichen Informationsmodells des E-Rezepts. Sie identifiziert
965 das E-Rezept über den gesamten Lebenszyklus, d.h. auch in den Abrechnungsprozessen.
966 Die Rezept-ID kann eine fortlaufende Nummer sein.

967 **A_18764 - E-Rezept-Fachdienst – Rezept-ID als Ressourcen-Identifizier**

968 Der E-Rezept-Fachdienst MUSS die Rezept-ID als Ressourcen-Identifizier für die Ressource
969 E-Rezept verwenden. [\leq]

970 Die Zugriffsautorisierung erfolgt u.a. auf Basis eines AccessCodes, welcher durch den E-
971 Rezept-Fachdienst für jedes Rezept erstellt wird.

972 **A_18520 - E-Rezept-Fachdienst – Eineindeutiger AccessCode des E-Rezepts**

973 Der E-Rezept-Fachdienst MUSS einen AccessCode mit ausreichend hoher Entropie
974 erzeugen. Der E-Rezept-Fachdienst MUSS sicherstellen, dass jedes im E-Rezept-
975 Fachdienst verwaltete E-Rezept einen eineindeutigen AccessCode besitzt. [\leq]

976 **A_18522 - E-Rezept-Fachdienst – E-Rezept-Statuswechsel**

977 Der E-Rezept-Fachdienst MUSS sicherstellen, dass ein mit einer Operation verbundener
978 Statuswechsel eines E-Rezepts zulässig ist und anderenfalls die Operation mit einem
979 Fehler abrechnen. Die Fehlermeldung an das aufrufende System muss eine Information
980 über den aktuellen Status des E-Rezepts beinhalten. [\leq]

981 Für einen Überblick der Status und der Statusübergänge siehe 2.4.6- Konzept Status E-
982 Rezept.

983 **A_18523 - E-Rezept-Fachdienst – Quittung beim Statusübergang zu "quittiert"**

984 Der E-Rezept-Fachdienst MUSS beim Übergang des Status eines E-Rezepts von "in
985 Abgabe (gesperrt)" zu "quittiert" eine E-Rezept-spezifische Quittung erstellen, mit seiner
986 PKI-Identität (ID.FD.SIG) signieren und dem abgebenden Leistungserbringer übergeben.
987 Die Quittung muss die Rezept-ID und das Datum des Statuswechsels beinhalten. [\leq]

Hinweis: Diese Quittung kann in Abrechnungsprozessen verwendet werden, um sicherzustellen, dass ein E-Rezept nur einmal abgerechnet wird.

A_18524 - E-Rezept-Fachdienst – Geheimnis zur Statusänderung "in Abgabe (gesperrt)"

Der E-Rezept-Fachdienst MUSS bei jedem Übergang des Status eines E-Rezepts von "offen" zu "in Abgabe (gesperrt)" ein E-Rezept-spezifisches und übergangsspezifisches Geheimnis mit ausreichend hoher Entropie erzeugen und dem abgebenden Leistungserbringer übermitteln, sowie dem E-Rezept zuordnen. [\leq]

Das Geheimnis zur Statusänderung "in Abgabe (gesperrt)" wird genutzt, um den exklusiven Zugriff und die Zulässigkeit des folgenden Statusüberganges sicherzustellen.

A_18820 - E-Rezept-Fachdienst – Inhalte löschen beim Statusübergang "gelöscht"

Der E-Rezept-Fachdienst MUSS bei jedem Übergang des Status eines E-Rezepts zu "gelöscht" alle personenbezogenen und medizinischen Inhalte aus dem E-Rezept-Datensatz löschen. [\leq]

A_18952 - E-Rezept-Fachdienst – Abfrage E-Rezept mit Status "gelöscht"

Der E-Rezept-Fachdienst MUSS die Abfrage eines E-Rezepts, welches den Status "gelöscht" hat, mit einem Fehler abbrechen, welcher dem Client den Status anzeigt. Wenn ein Versicherter alle seine E-Rezepte abrufen, dann werden Rezepte mit dem Status "gelöscht" nicht zurückgegeben. [\leq]

A_20055 - E-Rezept-Fachdienst – Prüfung Leistungserbringer-Typ

Der E-Rezept-Fachdienst MUSS bei der Abfrage eines E-Rezepts durch eine abgebende LEI den Leistungserbringer-Typ prüfen, ob die LEI für die Abgabe des Rezept-Typen berechtigt ist. [\leq]

Das Löschen eines E-Rezept-Datensatzes erfolgt automatisiert entsprechend einer Löschfrist durch den E-Rezept-Fachdienst.

A_18525 - E-Rezept-Fachdienst – E-Rezept-Datensatz löschen (Löschfristen)

Der E-Rezept-Fachdienst MUSS einen E-Rezept-Datensatz in Abhängigkeit von Gültigkeitszeitraum und Status löschen.

Tabelle 24: TAB_SYSLERP_021 Bedingungen zum Löschen von E-Rezepten

Status E-Rezept	Bedingung
initialisiert	1 Tage nach Statuswechsel zu "initialisiert"
offen	10 Tage nach "gültig bis (einlösbar)"
in Abgabe (gesperrt)	100 Tage nach Statuswechsel zu "in Abgabe (gesperrt)"
quittiert	100 Tage nach Statuswechsel zu "quittiert"
gelöscht	10 Tage nach Statuswechsel zu "gelöscht"

[\leq]

A_18788 - E-Rezept-Fachdienst – E-Rezept-Nachricht löschen (Löschfrist)

Der E-Rezept-Fachdienst MUSS eine E-Rezept-Nachricht 100 Tage nach dem Einstellen löschen. [\leq]

A_18526 - E-Rezept-Fachdienst – Einträge für Zugriffsprotokoll erstellen

Der E-Rezept-Fachdienst MUSS für das Einstellen eines E-Rezepts, für jeden Statuswechsel des E-Rezepts durch Leistungserbringer, das Abrufen durch Versicherte/Vertreter und für das Löschen des E-Rezepts einen Protokolleintrag erstellen. [\leq]

Für die Identifikation des E-Rezepts im Protokolleintrag wird die Rezept-ID verwendet.

A_18937 - E-Rezept-Fachdienst – Protokolleinträge für E-Rezept löschen (Löschfrist)

Der E-Rezept-Fachdienst MUSS sicherstellen, dass Protokolleinträge 3 Jahre nach ihrer Generierung gelöscht werden. [\leq]

A_18889 - E-Rezept-Fachdienst - Authentifizierung auf Basis Identitätsbestätigung des IdP

Der E-Rezept-Fachdienst MUSS den aufrufenden Nutzer anhand einer durch einen Identity Provider ausgestellten Identitätsbestätigung authentifizieren. [\leq]

A_18739 - E-Rezept-Fachdienst - Zugangsberechtigungen

Der E-Rezept-Fachdienst MUSS Zugangsberechtigungen für die Operationen auf Basis der Identitätsattribute der Identitätsbestätigung des Nutzers gemäß TAB_SYSLERP_040 umsetzen.

Tabelle 25: TAB_SYSLERP_040 Zugangsberechtigungen Operationen E-Rezept-Fachdienst

Operation	Zugang zulässig für folgende Rollen gemäß [gemKPT_Arch_TIP#Tab_ArchTIP_002]
E-Rezept-ID abrufen	Arzt, Zahnarzt, Mitarbeiter Arzt, Mitarbeiter Zahnarzt, Mitarbeiter Krankenhaus
E-Rezept einstellen	Arzt, Zahnarzt, Mitarbeiter Arzt, Mitarbeiter Zahnarzt, Mitarbeiter Krankenhaus
E-Rezept durch Verordnenden löschen	Arzt, Zahnarzt, Mitarbeiter Arzt, Mitarbeiter Zahnarzt, Mitarbeiter Krankenhaus
E-Rezept durch Abgebenden abrufen	Apotheker, Mitarbeiter Apotheke
E-Rezept durch Abgebenden löschen	Apotheker, Mitarbeiter Apotheke
E-Rezept durch Abgebenden zurückgeben	Apotheker, Mitarbeiter Apotheke
Quittung abrufen	Apotheker, Mitarbeiter Apotheke
Quittung erneut abrufen	Apotheker, Mitarbeiter Apotheke
E-Rezepte durch Versicherten abrufen	Versicherter

E-Rezept durch Vertreter abrufen	Versicherter
E-Rezept durch Versicherten löschen	Versicherter
Zugriffsprotokolleinträge durch Versicherten abrufen	Versicherter
E-Rezept-Nachricht einstellen	Versicherter, Apotheker, Mitarbeiter Apotheke
E-Rezept-Nachricht abrufen	Versicherter, Apotheker, Mitarbeiter Apotheke

1043 [\leq]

1044 **A_18936 - E-Rezept-Fachdienst - Transaktionssicherheit**

1045 Der E-Rezept-Fachdienst MUSS alle Aktivitäten zu einem Aufruf durch einen Client
1046 transaktionssicher durchführen.[\leq]

1047 **A_18795 - E-Rezept-Fachdienst - Erreichbarkeit im Internet**

1048 Der E-Rezept-Fachdienst MUSS im Internet erreichbar sein. Der E-Rezept-Fachdienst
1049 MUSS sicherstellen, dass ausschließlich Versicherte aus dem Internet zugreifen
1050 können.[\leq]

1051 **4.1.1.1 Vertrauenswürdige Ausführungsumgebung**

1052 Der E-Rezept-Fachdienst wird in einer Vertrauenswürdigen Ausführungsumgebung
1053 betrieben und garantiert damit den Ausschluss des Anbieters des Dienstes vom Zugriff
1054 auf die verarbeiteten Nutzdaten der E-Rezepte.

1055 **A_18823 - Umsetzung des E-Rezept-Fachdienstes in einer Vertrauenswürdigen
1056 Ausführungsumgebung (VAU)**

1057 Der E-Rezept-Fachdienst MUSS alle Komponenten, die an der Verarbeitung von E-
1058 Rezept-Daten im Klartext beteiligt sind, in einer Vertrauenswürdigen
1059 Ausführungsumgebung umsetzen.[\leq]

1060 Im Folgenden werden betrieblich-funktionalen Aspekte beschrieben, die bei der
1061 Umsetzung der VAU des E-Rezept-Fachdienstes zu berücksichtigen sind, um der Situation
1062 des Anbieters Ausschlusses Rechnung zu tragen. Die Sicherheitsmechanismen werden in
1063 Kapitel 5 behandelt.

1064 **A_18824 - Automatische Wiederherstellung eines konsistenten Zustands der
1065 VAU nach Systemfehlern**

1066 Die Vertrauenswürdige Ausführungsumgebung des E-Rezept-Fachdienstes MUSS nach
1067 Fehlern in der Datenverarbeitung automatisch, d. h. ohne administrative Eingriffe,
1068 die Klartextdaten berühren könnten, in einen konsistenten Systemzustand
1069 zurückkehren.[\leq]

1070 **A_18825 - Fehlererkennung für Anwender ermöglichen**

1071 Der E-Rezept-Fachdienst MUSS jeden Verarbeitungsvorgang eines Anwenders in solcher
1072 Weise durchführen, dass der Anwender erkennen kann, wenn der Abschluss seines
1073 Verarbeitungsvorgangs aufgrund von Systemfehlern gescheitert ist.[\leq]

1074 **A_18826 - Vorgangswiederholung nach Fehler gewährleisten**

1075 Der E-Rezept-Fachdienst MUSS die Wiederholung von aufgrund von Systemfehlern
1076 gescheiterten Verarbeitungsvorgängen ermöglichen und dies so umsetzen, dass die

1077 Vorgangswiederholung durch die Client-Anwendung in Form eines einfachen „erneut
1078 versuchen“ umgesetzt werden kann.[<=]

1079 4.1.1.2 Betriebliche Aspekte

1080 Der Anbieter E-Rezept-Fachdienst liefert Rohdaten zu Performance-Kennzahlen für die
1081 Überwachung der TI an die gematik. Die notwendigen Tätigkeiten im Rahmen der
1082 Serviceerbringung (Mitwirkungspflichten, Service Level) sowie die Teilnahme an den TI-
1083 ITSM-Prozessen ist in [gemKPT_Betr] und [gemRL_Betr_TI] geregelt.

1084 A_18741 - E-Rezept-Fachdienst - Anbieterschlüsse

1085 Der Anbieter E-Rezept-Fachdienst DARF NICHT Anbieter der folgenden Funktionen,
1086 Dienste oder Produkttypen gemäß [gemKPT_Arch_TIP] sein:

- 1087 • Identity Provider

1088 [<=]

1089 A_18687 - E-Rezept-Fachdienst – Verfügbarkeit

1090 Der Anbieter E-Rezept-Fachdienst MUSS die Hochverfügbarkeit des Dienstes
1091 sicherstellen.[<=]

1092 A_18743 - E-Rezept-Fachdienst - Maximales Rezeptaufkommen

1093 Der E-Rezept-Fachdienst MUSS in der Lage sein, mindestens die in TAB_SYSLERP_002
1094 und TAB_SYSLERP_003 genannten Maximalwerte der Rezeptaufkommen bewältigen zu
1095 können.

1096 **Tabelle 26: TAB_SYSLERP_002 Maximales Aufkommen nach Rezeptzeilen (Muster 16)**
1097 **2018 an ausgewählten Wochentagen**

	ausgestellt (max. Anzahl)	eingelöst (max. Anzahl)
Montag 17.12.2018	4.791.000	3.501.000
Dienstag 18.12.2018	4.023.000	3.683.000
Mittwoch	3.099.000	2.827.000
Donnerstag	3.607.000	3.401.000
Freitag	2.209.000	2.878.000
Samstag	119.000	883.000
Sonntag	95.000	302.000

1098 In 2018 war der 17.12. der Tag, an dem die meisten Rezepte ausgestellt wurden. Der
1099 Tag, an dem die meisten Rezepte in 2018 in einer Apotheke eingelöst wurden, war der
1100 18.12.

1101 **Tabelle 27: TAB_SYSLERP_003 Gesamtes Aufkommen nach Rezeptzeilen (Muster 16)**
1102 **2018 kumuliert nach Wochentagen**

	ausgestellt (Gesamtzahl)	eingelöst (Gesamtzahl)
--	--------------------------	------------------------

Montag	185.300.000	137.000.000
Dienstag	156.800.000	143.300.000
Mittwoch	105.600.000	113.400.000
Donnerstag	146.700.000	140.400.000
Freitag	91.700.000	121.300.000
Samstag	4.500.000	26.400.000
Sonntag	2.800.000	3.100.000
Gesamt	693.400.000	684.900.000

1103 [\leq]

1104 **A_18745 - E-Rezept-Fachdienst - Antwortzeiten**

1105 Der E-Rezept-Fachdienst MUSS alle Aufrufe seiner Schnittstellen so beantworten, dass in
1106 Primärsystemen und den FdV keine Verzögerungen in den übergeordneten Abläufen
1107 entstehen. [\leq]

1108 **A_19014 - Ende-zu-Ende-Verifikation bei Produkt-Changes**

1109 Der Anbieter E-Rezept-Fachdienst MUSS den Erfolg eines Produkt-Changes durch eine
1110 hinreichende Anzahl erfolgreich durchlaufener, dem Produkt-Change angemessener
1111 Anwendungsfälle oder Bearbeitungsvorgänge verifizieren. [\leq]

1112 Die Verifikationskriterien werden im Rahmen des betrieblichen Change-Prozesses in
1113 Zusammenarbeit mit dem Anbieter von der gematik festgelegt. Sie können auch das
1114 Erfordernis umschließen, den Nachweis mittels einer Ende-zu-Ende Verifikation zu
1115 erbringen.

1116 **4.1.2 Produkttyp E-Rezept-Frontend des Versicherten**

1117 Das E-Rezept-Frontend des Versicherten wird in der Versichertenumgebung, d.h. auf
1118 einem Gerät des Versicherten, genutzt. Das E-Rezept-Frontend des Versicherten führt die
1119 dezentrale Fachlogik der Fachanwendung E-Rezept aus. Es ermöglicht dem Versicherten
1120 die Verwaltung seiner E-Rezepte.

1121 Es gibt genau einen Anbieter für das E-Rezept-Frontend des Versicherten.

1122 Die E-Rezept-Frontend des Versicherten wird durch die gematik bereitgestellt.

1123 **A_18689 - Frontend des Versicherten – Zusätzliche Funktionalitäten**

1124 Das E-Rezept-Frontend des Versicherten KANN zusätzliche Funktionalität enthalten,
1125 sofern diese nicht den Schutz der personenbezogenen und medizinischen Daten des
1126 Versicherten in der Fachanwendung E-Rezept gefährdet. [\leq]

1127 Eine zusätzliche Funktionalität ist beispielsweise die Verfügbarkeitsabfrage der
1128 Verordnung in einem Warenwirtschaftssystem.

1129 **A_18528 - Frontend des Versicherten – GUI**

1130 Das E-Rezept-Frontend des Versicherten MUSS eine grafische Oberfläche (GUI) zum
1131 Ausführen der E-Rezept-Anwendungsfälle anbieten. [\leq]

1132 **A_18529 - Frontend des Versicherten – Barrierefreiheit**

1133 Das E-Rezept-Frontend des Versicherten SOLL Bedienungselemente der Barrierefreiheit
1134 umsetzen. [≤]

1135 **A_18533 - Frontend des Versicherten – Nutzung interoperabler Schnittstellen**
1136 Das E-Rezept-Frontend des Versicherten MUSS die interoperablen Schnittstellen gemäß
1137 TAB_SYSLERP_022 nutzen.

1138 **Tabelle 28: TAB_SYSLERP_022 Nutzung Schnittstellen eRp-FdV**

Ressource	Schnittstelle / Operation	Bereitstellende Komponente
E-Rezept	E-Rezepte durch Versicherten abrufen E-Rezept durch Vertreter abrufen E-Rezept durch Versicherten löschen	E-Rezept-Fachdienst
E-Rezept-Nachricht	E-Rezept-Nachricht einstellen E-Rezept-Nachrichten abrufen	E-Rezept-Fachdienst
Zugriffsprotokolleintrag	Zugriffsprotokolleinträge durch Versicherten abrufen	E-Rezept-Fachdienst
	Authentifizierung anfordern	Authentisierungsmodul
	I_Authenticate (AuthN-Token anfordern)	Identity Provider
	I_Directory_Query	Verzeichnisdienst der TI

1139 [≤]

1140 **A_18789 - Frontend des Versicherten – E-Rezept-Token erzeugen**

1141 Das E-Rezept-Frontend des Versicherten MUSS einen E-Rezept-Token mit den folgenden
1142 Inhalten auf Basis des E-Rezepts erzeugen:

- 1143 • Rezept-ID,
- 1144 • AccessCode

1145 [≤]

1146 **A_18534 - Frontend des Versicherten – E-Rezept-Token als DataMatrix-Code anzeigen**

1147 Das E-Rezept-Frontend des Versicherten MUSS einen E-Rezept-Token optisch als
1148 DataMatrix-Code gemäß ISO/IEC 16022 darstellen können. [≤]

1150 Ein DataMatrix-Code kann einen oder mehrere E-Rezept-Token beinhalten, um den
1151 Versicherten zu ermöglichen, mehrere E-Rezepte mit einem Abscann-Vorgang der
1152 Apotheke zuzuweisen.

1153 **A_18535 - Frontend des Versicherten – E-Rezept-Token einscannen**

1154 Das E-Rezept-Frontend des Versicherten MUSS einen DataMatrix-Code gemäß ISO/IEC
1155 16022 einscannen und den E-Rezept-Token dekodieren können. [≤]

1156 **A_18537 - Frontend des Versicherten – E-Rezept-Token importieren und**
1157 **exportieren**

1158 Das E-Rezept-Frontend des Versicherten KANN einen E-Rezept-Token aus
1159 Drittanwendungen importieren und in Drittanwendungen exportieren. [≤]

1160 Der Export kann bspw. durch das Weiterleiten mittels eines Messenger-Dienstes oder E-
1161 Mail erfolgen. Beim Export sind datenschutzrechtliche Anforderungen zu beachten.

1162 **A_18539 - Frontend des Versicherten – E-Rezept anzeigen**

1163 Das E-Rezept-Frontend des Versicherten MUSS die fachlichen Inhalte eines E-Rezepts
1164 anzeigen können. [≤]

1165 Wenn das FdV sich mit der TI verbindet, dann können alle Daten zu einem E-Rezept
1166 angezeigt werden. Wird das FdV ohne Verbindung zur TI genutzt und der E-Rezept-Token
1167 bspw. eingescannt, dann soll das FdV die beschreibenden Metadaten aus dem E-Rezept-
1168 Token anzeigen können.

1169 **A_18622 - Frontend des Versicherten – E-Rezept-Token anzeigen**

1170 Das E-Rezept-Frontend des Versicherten MUSS die beschreibenden Metadaten aus einem
1171 E-Rezept-Token anzeigen können. [≤]

1172 Bei den beschreibenden Metadaten handelt es sich um alle Daten aus dem E-Rezept-
1173 Token, außer dem AccessCode.

1174 **A_18540 - Frontend des Versicherten – Abgebende LEI im Verzeichnis suchen**

1175 Das E-Rezept-Frontend des Versicherten MUSS es dem Versicherten ermöglichen, eine
1176 abgebende LEI für den Versand des E-Rezept-Tokens aus dem Verzeichnisdienst der TI
1177 auszuwählen. [≤]

1178 Der Versicherte soll für die Suche im Verzeichnis Suchkriterien eingeben und über die
1179 Ergebnismenge filtern können. Filterkriterien können bspw. der Name, die Adresse oder
1180 Geoinformationen sein.

1181 Das Frontend soll den Nutzer bei der intuitiven Nutzung der Fachanwendung E-Rezept
1182 unterstützen. Beispielsweise:

- 1183 • Information über neu vorliegende Nachrichten durch Verordnende oder
1184 Abgebende,
- 1185 • automatische Information über Statusänderungen von E-Rezepten im E-Rezept-
1186 Fachdienst,
- 1187 • Ausdruck des DataMatrix-Code für einen E-Rezept-Token,
- 1188 • Filterfunktionen zur Auswahl abgebender LEI aus dem Verzeichnis,
- 1189 • Filterfunktionen für die Anzeige der Protokolleinträge.

1190 **4.1.3 Primärsysteme**

1191 Die Primärsysteme stellen das Frontend für Leistungserbringer dar. Hiermit greift der
1192 Leistungserbringer auf die Fachanwendung E-Rezept zu.

1193 Die Primärsysteme verwalten in einer lokalen Datenbasis die notwendigen Informationen
1194 zu Versicherten und der in der Fachanwendung E-Rezept eingesetzten SMC-Bs und HBAs.

1195 Für die Erzeugung einer fortgeschrittenen oder qualifizierten elektronischen Signatur
1196 sowie für die Prüfung einer qualifizierten elektronischen Signatur nutzt ein Primärsystem
1197 Schnittstellen der TI-Plattform, die die tatsächlichen kryptographischen Operationen
1198 durchführen.

1199 **A_18541 - Primärsystem - Signaturverfahren auswählen**

1200 Das Primärsystem MUSS es dem verordnenden und abgebenden Akteur ermöglichen, für
1201 Anwendungsfälle des E-Rezepts, welche das Signieren von Dokumenten beinhalten,

1202 zwischen Einzel-, Stapel- und Komfortsignatur auszuwählen. Eine Defaultauswahl soll
1203 konfigurierbar sein. [≤]

1204 Wenn das Primärsystem einer verordnenden oder abgebenden LEI eine Operation aufruft,
1205 mit der der Status eines E-Rezepts geändert werden soll, dann prüft der E-Rezept-
1206 Fachdienst die Zulässigkeit des Statuswechsels (vgl. A_18522).

1207 **A_18747 - Primärsystem - Hinweis unzulässiger Statuswechsel**

1208 Das Primärsystem MUSS, wenn ein Statuswechsel als unzulässig abgelehnt wird, dem
1209 verordnenden oder abgebenden Akteur einen Hinweis mit dem aktuellen Status des E-
1210 Rezepts geben. [≤]

1211 Bei der Verordnung und der Abgabe eines E-Rezepts kann es Wechselwirkungen mit
1212 anderen Fachanwendungen der TI (bspw. eMP/AMTS oder ePA) geben. Der
1213 Leistungserbringer soll dabei unterstützt werden, die Daten in mehreren Anwendungen
1214 zu nutzen, bspw. die Bereitstellung der Daten des E-Rezepts für die Aktualisierung des
1215 eMP.

1216 **A_18688 - Primärsystem - E-Rezept-Daten für medizinische Anwendungen 1217 nutzen**

1218 Das Primärsystem SOLL den verordnenden und abgebenden Akteur dabei unterstützen,
1219 die Daten des E-Rezepts für andere Anwendungen der TI zu nutzen. [≤]

1220 **4.1.3.1 Primärsystem verordnender Leistungserbringer**

1221 Das Primärsystem verordnender Leistungserbringer ist ein ärztliches bzw. zahnärztliches
1222 Praxisverwaltungssystem (PVS) oder ein Krankenhausinformationssystem (KIS).

1223 **A_18542 - Primärsystem verordnende LEI – Nutzung interoperabler 1224 Schnittstellen**

1225 Das Primärsystem der verordnenden Leistungserbringerinstitution MUSS die
1226 interoperablen Schnittstellen gemäß TAB_SYSLERP_023 nutzen.

1227 **Tabelle 29: TAB_SYSLERP_023 Nutzung Schnittstellen PS verordnende LEI**

Ressource	Schnittstelle	Bereitstellende Komponente
E-Rezept	E-Rezept-ID abrufen E-Rezept einstellen E-Rezept durch Verordnenden löschen E-Rezept durch Abgebenden abrufen	E-Rezept-Fachdienst
	Authentifizierung anfordern	Authentisierungsmodul
	I_Authenticate (AuthN-Token anfordern)	Identity Provider
	I_IP_Transport I_SAK_Operations	Konnektor

1228 [≤]

1229 **A_18544 - Primärsystem verordnende LEI – E-Rezept um Rezept-ID ergänzen**

1230 Das Primärsystem der verordnenden Leistungserbringerinstitution MUSS ein E-Rezept
1231 gemäß den Vorgaben des fachlichen Informationsmodells mit einer vom E-Rezept-
1232 Fachdienst bereitgestellten Rezept-ID ergänzen. [≤]

1233 **A_18545 - Primärsystem verordnende LEI – Rezept-ID einmalig verwenden**

1234 Das Primärsystem der verordnenden Leistungserbringerinstitution MUSS eine vom E-
1235 Rezept-Fachdienst bereitgestellten Rezept-ID für genau ein E-Rezept verwenden.[<=]

1236 **A_18612 - Primärsystem verordnende LEI – Verordnungsdatensatz prüfen**

1237 Das Primärsystem der verordnenden Leistungserbringerinstitution MUSS beim Erstellen
1238 des E-Rezepts die Korrektheit und Vollständigkeit des Verordnungsdatensatzes
1239 entsprechend des fachlichen Informationsmodells prüfen.[<=]

1240 **A_18613 - Primärsystem verordnende LEI – Kein E-Rezept unsigned einstellen**

1241 Das Primärsystem der verordnenden Leistungserbringerinstitution DARF ein E-Rezept
1242 NICHT in den E-Rezept-Fachdienst einstellen, wenn das Aufbringen der QES nicht
1243 erfolgreich durchgeführt wurde.[<=]

1244 **A_18614 - Primärsystem verordnende LEI – E-Rezept-Token erzeugen**

1245 Das Primärsystem der verordnenden Leistungserbringerinstitution MUSS einen E-Rezept-
1246 Token mit den folgenden Inhalten auf Basis eines E-Rezepts erzeugen:

- 1247 • Rezept-ID,
- 1248 • AccessCode

1249 [<=]

1250 Rezept-ID und AccessCode sind die Informationen, welche für den Zugriff auf ein E-
1251 Rezept notwendig sind.

1252 **A_18543 - Primärsystem verordnende LEI – E-Rezept-Token ausdrucken**

1253 Das Primärsystem der verordnenden Leistungserbringerinstitution MUSS E-Rezept-Token
1254 als DataMatrix-Code gemäß ISO/IEC 16022 ausdrucken können. [<=]

1255 Der durch das PS erzeugte DataMatrix-Code beinhaltet die Informationen von einem E-
1256 Rezept-Token.

1257 Neben der optischen Darstellung des E-Rezept-Tokens als DataMatrix-Code kann der
1258 Ausdruck weitere lesbare Informationen zum E-Rezept für den Empfänger enthalten. Die
1259 Ausgestaltung eines Formulars für den Ausdruck liegt nicht in der Regelungshoheit der
1260 gematik.

1261 **A_18615 - Primärsystem verordnende LEI – E-Rezept-Token anzeigen**

1262 Das Primärsystem der verordnenden Leistungserbringerinstitution KANN E-Rezept-Token
1263 optisch als DataMatrix-Code gemäß ISO/IEC 16022 anzeigen, um bspw. das Abscannen
1264 zu ermöglichen.[<=]

1265

1266 **A_18616 - Primärsystem verordnende LEI – E-Rezept-Token speichern**

1267 Das Primärsystem der verordnenden Leistungserbringerinstitution MUSS einen E-Rezept-
1268 Token für den Zeitraum, in dem das E-Rezept einlösbar ist, vorhalten.[<=]

1269 Ein Versand des E-Rezept-Token an den Versicherten ist nicht notwendig, da sich dieser
1270 die notwendigen Informationen mit seinem FdV vom E-Rezept-Fachdienst abrufen kann
1271 und den E-Rezept-Token im FdV erstellt.

1272 Die Übermittlung eines E-Rezept-Token an eine abgebende LEI ist entsprechend der
1273 gesetzlichen Grundlagen gemäß §11 ApoG zulässig. Hierfür kann KOM-LE genutzt
1274 werden.

1275 **4.1.3.2 Primärsystem abgebender Leistungserbringer**

1276 Das Primärsystem abgebender Leistungserbringer ist ein Apothekenverwaltungssystem
1277 (AVS).

A_18547 - Primärsystem abgebende LEI – Nutzung interoperabler Schnittstellen

Das Primärsystem der abgebenden Leistungserbringerinstitution MUSS die interoperablen Schnittstellen gemäß TAB_SYSLERP_024 nutzen.

Tabelle 30: TAB_SYSLERP_024 Nutzung Schnittstellen PS abgebende LEI

Ressource	Schnittstelle / Operation	Bereitstellende Komponente
E-Rezept	E-Rezept durch Abgebenden abrufen E-Rezept durch Abgebenden löschen E-Rezept durch Abgebenden zurückgeben Quittung abrufen Quittung erneut abrufen	E-Rezept-Fachdienst
E-Rezept-Nachricht	E-Rezept-Nachricht einstellen E-Rezept-Nachrichten abrufen	E-Rezept-Fachdienst
	Authentifizierung anfordern	Authentisierungsmodul
	I_Authenticate (AuthN-Token anfordern)	Identity Provider
	I_IP_Transport I_SAK_Operations	Konnektor

[<=]

A_18548 - Primärsystem abgebende LEI – DataMatrix-Code einscannen

Das Primärsystem der abgebenden Leistungserbringerinstitution MUSS E-Rezept-Token als DataMatrix-Code gemäß ISO/IEC 16022 einscannen können. [<=]

Ein DataMatrix-Code kann die Informationen von einem oder mehreren E-Rezept-Token enthalten.

A_18758 - Primärsystem abgebende LEI – E-Rezept-Token empfangen

Das Primärsystem der abgebenden Leistungserbringerinstitution MUSS einen E-Rezept-Token mittels des E-Rezept-Fachdienstes empfangen können. [<=]

A_18549 - Primärsystem abgebende LEI – E-Rezept-Token importieren

Das Primärsystem der abgebenden Leistungserbringerinstitution KANN Funktionalitäten anbieten, E-Rezept-Token aus Drittanwendungen zu importieren. [<=]

Das Primärsystem der abgebenden Leistungserbringerinstitution darf nur E-Rezepte bearbeiten, zu deren Abgabe es gemäß Metadaten berechtigt ist.

A_18551 - Primärsystem abgebende LEI – Signatur des E-Rezepts prüfen

Das Primärsystem der abgebenden Leistungserbringerinstitution MUSS die Signatur des E-Rezepts prüfen und eine Warnung anzeigen, falls die Prüfung nicht erfolgreich oder technisch nicht möglich war. [<=]

Das E-Rezept wird auch bei nicht erfolgreicher Prüfung der Signatur im Primärsystem angezeigt.

A_18552 - Primärsystem abgebende LEI – E-Rezept anzeigen

Das Primärsystem der abgebenden Leistungserbringerinstitution MUSS ein E-Rezept anzeigen können. [≤]

A_18791 - Primärsystem abgebende LEI – AccessCode speichern

Das Primärsystem der abgebenden Leistungserbringerinstitution MUSS den im E-Rezept-Token für ein E-Rezept übermittelten AccessCode speichern, um ihn beim Aufruf einer Operation an den E-Rezept-Fachdienst übermitteln zu können. [≤]

A_18553 - Primärsystem abgebende LEI – Geheimnis zur Statusänderung "in Abgabe (gesperrt)" speichern

Das Primärsystem der abgebenden Leistungserbringerinstitution MUSS das beim Abruf des E-Rezepts übermittelte Geheimnis zur Statusänderung "in Abgabe (gesperrt)" speichern und beim Aufruf der Operation zum Zurückgeben oder Löschen des E-Rezepts bzw. zum Abruf der Quittung zurück übermitteln. [≤]

4.2 Fachanwendungsübergreifende Produkttypen**4.2.1 Produkttyp 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. Die Bereitstellung von Authentifizierungsbestätigungen und Identitätsmerkmalen erfolgt in Form von Bearer Token (AuthN-Token). Der IdP bietet außerdem die Möglichkeit, bereits erfolgte Authentifizierungen eines Nutzers im Sinne eines Single Sign-on nachzunutzen. Als TIP-Nutzerdienst ist der Dienst der Provider Zone des TI-Zonenmodells zugeordnet. Der Dienst ist in der TI ggf. mehrfach vorhanden, wobei jeder einzelne IdP die Identitäten einer Gruppe von TI-Teilnehmern abdeckt.

Für die Fachanwendung E-Rezept werden IdPs für die nutzenden Leistungserbringerinstitutionen und die Versicherten genutzt. Deren Identitätsmerkmale bestimmen - zusammen mit den E-Rezept-Token - die Zugriffsberechtigungen auf Funktionen und Daten der Anwendung E-Rezept.

4.2.1.1 Funktionale Anforderungen**A_18797 - IdP - Umsetzung des IdP gemäß OpenID Connect**

Der IdP MUSS als OpenID Provider gemäß OpenID Connect 1.0, Protocol Suite "Complete", umgesetzt werden, siehe [OIDC]. Darin referenzierte Standards, wie z.B. OAuth 2.0 [OAUTH2], MÜSSEN beachtet werden. [≤]

A_18803 - IdP - Zulässige Client Profile

Der IdP MUSS die Authentifizierung von Nutzern gemäß demjenigen Client Profil durchführen, welches zum Frontend bzw. Primärsystem passt (siehe [OAUTH2], Section 2.1. "Client Types"):

- Frontend des Versicherten bzw. Primärsystem als native Applikation (allgemein: Ausführung der Fachlogik auf dem Gerät des Nutzers):
Client Profil "Native Application"
- Primärsystem als Web Applikation (Ausführung der Fachlogik serverseitig, in sicherer Umgebung):
Client Profil "Web Application"

Es sind keine weiteren Client Profile zulässig. [≤]

A_18815 - IdP - Zulässiger Protokollablauf bei der Bereitstellung von Token

Der IdP MUSS entsprechend A_18803 mit dem Authentisierungsmodul und dem Client (Relying Party) gemäß Grant Type "Authorization Code" interagieren. [≤]

A_18805 - IdP - Zulässige Clients

Der IdP MUSS seine Dienste ausschließlich den Anwendungen und Diensten der TI sowie weiteren Anwendungen gemäß [gemRL_NvTIWA] zur Verfügung stellen. [≤]

A_18811 - IdP - Nur registrierte Clients

Der IdP MUSS Requests einer unregistrierten Relying Party (Client) mit einem Fehler abweisen. [≤]

A_18812 - IdP - Client-Authentisierung

Der IdP MUSS eine Relying Party (Client) anhand der bei der Registrierung festgelegten Identifikationsmerkmale authentifizieren. [≤]

A_18838 - IdP - Ablehnung nicht erfolgreich authentifizierter Clients

Der IdP MUSS einen Client erfolgreich authentifizieren, bevor er dessen Request bearbeitet. Der IdP MUSS mit einem Fehler reagieren, falls er den Client nicht erfolgreich authentifizieren kann. [≤]

A_18799 - IdP - Authentisierung mittels Smart Cards der TI

Ein IdP MUSS für die von ihm verwalteten TI-Teilnehmer die Authentisierung mittels Smart Card ermöglichen, sofern dieser über eine Smart Card der TI verfügt. Die Authentifizierung erfolgt auf Basis des Nutzerzertifikats (AUT-Identität) im Challenge-Response-Verfahren. Der IdP MUSS dazu dem Authentisierungsmodul eine Challenge übergeben. [≤]

A_18914 - IdP - Schnittstelle für die Ressource signierte Challenge

Ein IdP MUSS für die Authentisierung mittels Smart Card dem Authentisierungsmodul eine Schnittstelle mit der logischen Operation "signierte Challenge übergeben" bereitstellen. [≤]

A_18865 - IdP - Einwilligung in die Nutzung von Identitätsattributen

Ein IdP MUSS für die von ihm verwalteten TI-Teilnehmer eine Einwilligung in die Nutzung von Identitätsattributen einholen, bevor diese erstmalig in einem AuthN-Token dem Client bereitgestellt werden. Der IdP MUSS dazu dem Authentisierungsmodul die angefragten Identitätsattribute bereitstellen. [≤]

A_18915 - IdP - Schnittstelle für die Ressource Einwilligung

Ein IdP MUSS für die Einwilligung in die Nutzung von Identitätsattributen dem Authentisierungsmodul eine Schnittstelle mit der logischen Operation "Einwilligung erteilen" bereitstellen. [≤]

A_19011 - IdP - Schnittstelle für die Anforderung des AuthN-Token

Ein IdP MUSS eine Schnittstelle I_Authenticate (AuthN-Token anfordern) bereitstellen, über die die Relying Party für einen übergebenen AuthN-Code einen AuthN-Token anfordern kann. Diese Schnittstelle entspricht dem Token Endpoint gemäß OAuth 2.0 [OAUTH2]. [≤]

A_18819 - IdP - Nutzung der PKI durch den IdP

Der IdP MUSS, wenn für einen TI-Teilnehmer Identitäten über die PKI der TI bereitgestellt werden, vorhandene Dienste der PKI verwenden, insbesondere bei der TLS- oder OCSP-Abfrage für die Zertifikatsprüfung. [≤]

A_18808 - IdP - Abdeckung der fachlichen Identitätsattribute PKI-basierter Identitäten

1394 Der IdP MUSS, wenn für einen TI-Teilnehmer Identitäten sowohl AuthN-Token vom IdP
1395 als auch Zertifikate durch die PKI bereitgestellt werden, mindestens die fachlichen
1396 Identitätsattribute unterstützen, die in den Zertifikaten enthalten sind. [<=]

1397 **A_18809 - IdP - Minimierung der Authentisierungsanfragen, komfortabler Single**
1398 **Sign-On**

1399 Der IdP MUSS Authentisierungsanfragen an bereits authentifizierte Nutzer auf solche
1400 Fälle beschränken, in denen eine erneute Authentisierung durch den Nutzer aus Gründen
1401 der Sicherheit erforderlich ist oder von der Anwendung explizit angefordert wird. [<=]

1402 **4.2.1.2 Betriebliche Aspekte**

1403 **A_18904 - IdP – Verfügbarkeit**

1404 Der Anbieter des IdP MUSS die Hochverfügbarkeit des Dienstes sicherstellen. [<=]

1405 Der Anbieter des IdP liefert Rohdaten zu Performance-Kennzahlen für die Überwachung
1406 der TI an die gematik. Die notwendigen Tätigkeiten im Rahmen der Serviceerbringung
1407 (Mitwirkungspflichten, Service Level) sowie die Teilnahme an den TI-ITSM-Prozessen ist
1408 in [gemKPT_Betr] und [gemRL_Betr_TI] geregelt.

1409 **A_18903 - IdP - Anbieterschluss**

1410 Der Anbieter des IdP DARF NICHT Anbieter der folgenden Funktionen, Dienste oder
1411 Produkttypen gemäß [gemKPT_Arch_TIP] sein:

- 1412 • E-Rezept-Fachdienst

1413 [<=]

1414 **A_18810 - IdP - Registrierung von Clients**

1415 Der Anbieter des IdP MUSS ein Verfahren bzw. eine Schnittstelle bereitstellen, über
1416 welche sich Dienste der TI als Relying Party (Clients) für die Nutzung des IdP registrieren
1417 können. [<=]

1418 **A_18801 - IdP - Widerspruchsfreiheit von IdP und PKI**

1419 Der Anbieter des IdP MUSS, wenn für einen TI-Teilnehmer Identitäten sowohl über die
1420 PKI als auch den IdP bereitgestellt werden, sicherstellen, dass sich die beiden Identitäten
1421 bezüglich der aktuellen Gültigkeit und der inhaltlichen Aussagen nicht
1422 widersprechen. [<=]

1423 **A_18802 - IdP - Widerspruchsfreiheit von IdP und Verzeichnisdienst**

1424 Der Anbieter des IdP MUSS, wenn für einen Teilnehmer Identitätsattribute sowohl über
1425 den Verzeichnisdienst als auch den IdP bereitgestellt werden, sicherstellen, dass sich die
1426 beiden Identitätsattribute bezüglich der aktuellen Gültigkeit und der inhaltlichen
1427 Aussagen nicht widersprechen. [<=]

1428 **A_18939 - IdP - Bereitstellung Authentisierungsmodul**

1429 Der Anbieter des IdP SOLL ein Authentisierungsmodul für die gängigen mobilen
1430 Betriebssysteme iOS und Android bereitstellen, das den Authentifizierungsvorgang des
1431 Nutzers über eine Schnittstelle zwischen IdP und dem Authentisierungsmodul auf dem
1432 Gerät des Nutzers steuert. [<=]

1433 **A_19016 - Verifikation von Produkt-Changes**

1434 Der Anbieter des IdP MUSS den Erfolg eines Produkt-Changes durch eine hinreichende
1435 Anzahl erfolgreich durchlaufener, dem Produkt-Change angemessener Anwendungsfälle
1436 oder Bearbeitungsvorgänge verifizieren. [<=]

1437 Die Verifikationskriterien werden im Rahmen des betrieblichen Change-Prozesses in
1438 Zusammenarbeit mit dem Anbieter von der gematik festgelegt. Sie können auch das
1439 Erfordernis umschließen, den Nachweis mittels einer Ende-zu-Ende-Verifikation zu
1440 erbringen.

4.2.2 Authentisierungsmodul

Das Authentisierungsmodul ergänzt den IdP, um auf dem Gerät des Nutzers den Zugriff auf die Smart Card des Nutzers (z.B. über Kartenleser, NFC, Konnektor) umzusetzen. Es ermöglicht die Interaktion mit dem Nutzer zwecks Authentisierung und Einwilligung (Consent) in die Bereitstellung von Identitätsattributen. Dem IdP stellt das Authentisierungsmodul die Einwilligung des Nutzers und die für die Authentifizierung des Nutzers erforderlichen Daten bereit. Das Authentisierungsmodul alleine speichert den IdP-Sitzungsschlüssel (Subject Session ID) und ermöglicht einen Single Sign-On für alle den IdP nutzenden Anwendungen auf dem Gerät des Nutzers.

A_18813 - Authentisierungsmodul - Umsetzung gemäß OpenID Connect

Das Authentisierungsmodul MUSS so umgesetzt werden, dass es dem User Agent gemäß OpenID Connect 1.0, Protocol Suite "Complete", entspricht, siehe [OIDC]. Darin referenzierte Standards, wie z.B. OAuth 2.0 [OAUTH2], MÜSSEN beachtet werden. [<=]

A_18814 - Authentisierungsmodul - Zulässiger Protokollablauf bei der Bereitstellung von Token

Das Authentisierungsmodul MUSS entsprechend A_18803 mit dem IdP und der Anwendung (Client, Relying Party) gemäß Grant Type "Authorization Code" interagieren. [<=]

A_18816 - Authentisierungsmodul - Authentisierung mit Smart Cards der TI

Das Authentisierungsmodul MUSS eine Authentisierung des Nutzers per Smart Card ermöglichen. Falls der IdP dazu eine Challenge an das Authentisierungsmodul übergibt, MUSS das Authentisierungsmodul das Zertifikat der AUT-Identität des Nutzers ermitteln, die Challenge mit dem zugehörigen Schlüssel signieren lassen und die signierte Challenge zusammen mit dem Zertifikat an den IdP übergeben. [<=]

Für das Signieren mit einer SMC-B bzw. eGK siehe A_18817 bzw. A_18818. Für die Übergabe der signierten Challenge siehe 4.3.4.

A_18917 - Authentisierungsmodul - Einwilligung in die Nutzung von Identitätsattributen

Das Authentisierungsmodul MUSS vom Nutzer eine Einwilligung in die Bereitstellung von Identitätsattributen durch den IdP an die Anwendung einholen. Falls der IdP dazu die angeforderten Identitätsattribute an das Authentisierungsmodul übergibt, MUSS das Authentisierungsmodul die Einwilligung des Nutzers einholen und an den IdP übergeben (siehe 4.3.5). [<=]

A_18817 - Authentisierungsmodul - Authentisierung mit SMC-B

Das Authentisierungsmodul MUSS für die Authentisierung von Leistungserbringerinstitutionen die Signaturfunktion `I_Sign_Operations::external_Authenticate` gemäß [gemKPT_Arch_TIP#A_5075](#) und die Zertifikatsabfrage der SMC-B (AUT-Identität) über die Client-Schnittstelle des Konnektors nutzen. [<=]

A_18818 - Authentisierungsmodul - Authentisierung mit eGK

Das Authentisierungsmodul MUSS für die Authentisierung von Versicherten mittels eGK die Signaturfunktion und die Zertifikatsabfrage der eGK (AUT-Identität) über einen Kartenleser/die NFC-Schnittstelle des Geräts des Nutzers nutzen. [<=]

Die Anbindung der eGK kann mittels eines Kartenlesegerätes Klasse 1 oder mittels Near Field Communication (NFC) erfolgen.

A_18940 - Authentisierungsmodul - Schnittstelle für Fachlogik-App

1488 Das Authentisierungsmodul MUSS einen Systemdienst auf der Betriebssystemplattform
1489 des Gerät des Nutzers mit einer Schnittstelle (Authentisierung anfordern) anbieten, über
1490 die das E-Rezept-Modul Frontend des Versicherten einen Authentifizierungsrequest an
1491 das Authentisierungsmodul zur Authentifizierung des Nutzers gegenüber dem IdP
1492 weiterleiten kann.[<=]

1493 **4.2.3 Produkttyp Verzeichnisdienst der TI**

1494 Der durch die Fachanwendung E-Rezept genutzt Produkttyp Verzeichnisdienst der TI
1495 basiert auf dem Online-Produktivbetrieb Stufe 3 [OPB3] spezifizierten Produkttypen.

1496 Folgende zusätzliche Anforderungen bestehen.

1497 **A_18867 - VZD - Authentifizierung auf Basis Identitätsbestätigung des IdP**

1498 Der Verzeichnisdienst MUSS es ermöglichen, dass sich der aufrufende Nutzer mittels
1499 einer durch einen Identity Provider ausgestellten Identitätsbestätigung
1500 authentifiziert.[<=]

1501 **A_18837 - VZD - Erreichbarkeit im Internet**

1502 Der Verzeichnisdienst MUSS im Internet erreichbar sein.[<=]

1503 **A_18941 - VZD - Einschränkung abfragbarer Informationen für Versicherte**

1504 Der Verzeichnisdienst MUSS die für Versicherte bereitgestellte Schnittstelle so
1505 einschränken, dass ausschließlich die für die Suche und Adressierung von abgebenden
1506 LEI notwendigen Informationen abgefragt werden können.[<=]

1507 Der Versicherte kann für die Suche bspw. folgende Parameter verwenden:
1508 Institutionsname, Straße, Postleitzahl, Ort, Geodaten.

1509 **4.3 Schnittstelle der Fachanwendung E-Rezept**

1510 Der folgende Abschnitt beschreibt die interoperablen Schnittstellen der Fachanwendung
1511 E-Rezept, die zwischen Primärsystem verordnender LEI und E-Rezept-Fachdienst,
1512 zwischen Primärsystem abgebender LEI und E-Rezept-Fachdienst sowie zwischen
1513 Frontend des Versicherten und E-Rezept-Fachdienst genutzt werden.

1514 Der folgende Abschnitt beschreibt die durch die Anwendung genutzten Ressourcen und
1515 zugehörigen Operationen, auf welche die Primärsysteme der verordnenden und
1516 abgebenden LEI und die FdV zugreifen können.

1517 **4.3.1 Schnittstelle für die Ressource E-Rezept**

1518 Die Ressource E-Rezept enthält alle Daten des fachlichen Informationsmodells und
1519 zusätzliche Informationen für die Verwaltung des E-Rezepts.

1520

1521 **A_18555 - Logische Operation "E-Rezept-ID abrufen"**

1522 Die Schnittstelle MUSS die logische Operation "E-Rezept-ID abrufen" implementieren.

1523 **Tabelle 31: TAB_SYSLERP_025 Operation E-Rezept-ID abrufen**

Kategorie	Name	Typ
Ressource	E-Rezept	

Operation	E-Rezept-ID abrufen	
Methode	POST	/Task/\$create
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Body)	Parameters (Leistungserbringer-Typ und Rezept-Typ)	JSON-Object
Attribut-Out (Body)	PrescriptionID	Ressourcen-ID in Task.id und Task.identifizier
Attribut-Out (Body)	AccessCode	external Identifier in Task.identifizier

1524 Mit dieser Operation kann ein Verordnender eine Rezept-ID abrufen. Die Operation muss
 1525 zur Autorisierung des Aufrufenden (`IdentityToken`) die Rolle prüfen. Als Aufruf-
 1526 Parameter der FHIR-Operation `$create` der Ressource `Task` wird ein strukturierter
 1527 Datensatz mit FHIR-Operationsparametern (Rezept-Typ, Leistungserbringer-Typ bei dem
 1528 der Versicherte das Rezept einlösen kann) übergeben, da das entsprechende E-Rezept
 1529 inkl. E-Rezept-ID im nächsten Schritt vom Konnektor signiert werden muss.
 1530 Die Operation liefert die Rezept-ID (`PrescriptionId`) als ID der angelegten Ressource
 1531 `Task` und generiert den `AccessCode` (`AccessCode`) als external Identifier in den
 1532 Datensatz, welcher den Zugriff auf das E-Rezept erlaubt. Der Task erhält den Status
 1533 "initialisiert" ("draft").[<=]

1534 **A_18556 - Logische Operation "E-Rezept einstellen"**

1535 Die Schnittstelle MUSS die logische Operation "E-Rezept einstellen" implementieren.

1536 **Tabelle 32: TAB_SYSLERP_026 Operation E-Rezept einstellen**

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept einstellen	
Methode	POST	/Task/{Rezept-ID}/\$activate
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	AccessCode	Header-Attribut String
Attribut-In (Body)	E-Rezept-FHIR-Bundle	JSON-Objekt
Attribut-In (Body)	signature	Base64-codiertes CMS-Objekt als selfcontained Binary in Bundle.signature

Mit dieser Operation kann eine verordnende LEI ein E-Rezept im E-Rezept-Fachdienst um den qualifiziert signierten Anteil ergänzen. Die Operation muss zur Autorisierung des Aufrufenden (`IdentityToken`) die Rolle prüfen. Der `AccessCode` muss dem beim Einstellen erzeugten Geheimnis entsprechen, mit dem der Versicherte den Zugriff auf das E-Rezept steuert.

Die Operation muss vor dem Statuswechsel prüfen, ob das E-Rezept den Status "initialisiert" ("draft") hat.

Die Operation prüft die Gültigkeit der QES (`signature`) und den Inhalt des übergebenen `FHIR-Bundles` und erzeugt bei Korrektheit aller Daten eine Signatur über das Bundle mit der Signaturidentität `ID.FD.SIG`, die als Provenance mit Verweis auf den Task zum Abruf durch den Versicherten abgelegt wird. Der Datensatz der QES wird als Binary-Objekt des `FHIR-Bundles` gespeichert. Sind alle Daten valide und die QES gültig erhält das E-Rezept (der Task) den Status "offen" ("ready"). [`<=`]

A_18557 - Logische Operation "E-Rezept durch Verordnenden löschen"

Die Schnittstelle MUSS die logische Operation "E-Rezept durch Verordnenden löschen" implementieren.

Tabelle 33: TAB_SYSLERP_027 Operation E-Rezept durch Verordnenden löschen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Verordnenden löschen	
Methode	POST	/Task/{Rezept-ID}/\$abort
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	AccessCode	Header-Attribut String

Mit dieser Operation kann eine verordnende LEI den Status des E-Rezepts im E-Rezept-Fachdienst auf "gelöscht" (Status des Task "`cancelled`") ändern. Die Operation löscht die personenbezogenen und medizinischen Daten aus dem E-Rezept-Datensatz.

Die Operation muss zur Autorisierung des Aufrufenden (`IdentityToken`) die Rolle prüfen. Der `AccessCode` muss dem beim Einstellen erzeugten `AccessCode` entsprechen, mit dem der Versicherte den Zugriff auf das E-Rezept steuert.

Die Operation muss vor dem Statuswechsel prüfen, ob das E-Rezept den Status "offen" ("ready") hat. Die Operation liefert neben dem http-Status-Code über den Erfolg der Operation keine weiteren Daten zurück. [`<=`]

A_18559 - Logische Operation "E-Rezept durch Abgebenden abrufen"

Die Schnittstelle MUSS die logische Operation "E-Rezept durch Abgebenden abrufen" implementieren.

Tabelle 34: TAB_SYSLERP_028 Operation E-Rezept durch Abgebenden abrufen

Kategorie	Name	Typ
Ressource	E-Rezept	

Operation	E-Rezept durch Abgebenden abrufen	
Methode	POST	/Task/{Rezept-ID}/\$accept
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (URL)	?ac={AccessCode}	URL-Parameter 'ac'
Attribut-Out (Body)	Bundle aus Task inkl. QES-Objekt und Provenance	JSON-Objekt
Attribut-Out (Body)	Secret	external Identifier in Task.identifier

1567 Mit dieser Operation kann eine abgebende LEI ein E-Rezept vom E-Rezept-Fachdienst
1568 abrufen.

1569 Die Operation muss zur Autorisierung des Aufrufenden (`IdentityToken`) die Rolle
1570 prüfen. Der `AccessCode` muss dem beim Erstellen des Task erzeugten `AccessCode`
1571 entsprechen, mit dem der Versicherte den Zugriff auf das E-Rezept steuert. Die
1572 Operation muss vor dem Statuswechsel zu "in Abgabe (gesperrt)" ("in-progress")
1573 prüfen, ob das E-Rezept den Status "offen" ("ready") hat.

1574 Die Operation erzeugt ein Geheimnis zur Statusänderung (`Secret`) im Task, mit der der
1575 abgebenden LEI nachfolgende Zugriffe auf die Ressource gewährt werden. In der
1576 Response wird der Task, die beim Einstellen erzeugte serverseitige Signatur und das
1577 QES-signierte FHIR-Bundle zurückgegeben. [`<=`]

1578 **A_18560 - Logische Operation "E-Rezept durch Abgebenden löschen"**

1579 Die Schnittstelle MUSS die logische Operation "E-Rezept durch Abgebenden
1580 löschen" implementieren.

1581 **Tabelle 35: TAB_SYSLERP_029 Operation E-Rezept durch Abgebenden löschen**

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Abgebenden löschen	
Methode	POST	/Task/{Rezept-ID}/\$abort
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	AccessCode	Header-Attribut String
Attribut-In (Header)	Secret	Header-Attribut String

1582 Mit dieser Operation kann eine abgebende LEI den Status (`Task.status`) des E-Rezepts
1583 im E-Rezept-Fachdienst auf "cancelled" ändern.

Die Operation muss zur Autorisierung des Aufrufenden (`IdentityToken`) die Rolle prüfen. Das `Secret` muss dem beim Abruf des Rezepts erzeugten Geheimnis entsprechen, der `AccessCode` muss dem beim Erstellen des Task erzeugten `AccessCode` entsprechen und der Task den Status "in-progress" haben. Die Operation löscht die personenbezogenen und medizinischen Daten aus dem E-Rezept-Datensatz und ändert den Status des referenzierten Task auf "cancelled".[<=]

A_18561 - Logische Operation "E-Rezept durch Abgebenden zurückgeben"

Die Schnittstelle MUSS die logische Operation "E-Rezept durch Abgebenden zurückgeben" implementieren.

Tabelle 36: TAB_SYSLERP_030 Operation E-Rezept durch Abgebenden zurückgeben

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Abgebenden zurückgeben	
Methode	POST	/Task/{Rezept-ID}/\$reject
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	Secret	Header-Attribut String

Mit dieser Operation kann eine abgebende LEI den Zugriff auf das E-Rezept wieder freigeben (der Status des Task wird auf "ready" gesetzt).

Die Operation muss zur Autorisierung des Aufrufenden (`IdentityToken`) die Rolle prüfen.

Die Operation muss vor dem Statuswechsel prüfen, ob der Task den Status "in-progress" hat und ob das übermittelte Geheimnis (`Secret`) dem beim Abrufen des E-Rezeptes im Task erzeugten Geheimnis entspricht.[<=]

A_18562 - Logische Operation "Quittung abrufen"

Die Schnittstelle MUSS die logische Operation "Quittung abrufen" implementieren.

Tabelle 37: TAB_SYSLERP_031 Operation Quittung abrufen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	Quittung abrufen	
Methode	POST	/Task/{Rezept-ID}/\$close
Attribut-In (Header)	IdentityToken	JSON Web Token

Attribut-In (Body)	MedicationDispense	JSON-Objekt
Attribut-In (Header)	Secret	Header-Attribut String
Attribut-Out (Body)	Receipt	signiertes JSON-Objekt Provenance über Task und MedicationDispense

Mit dieser Operation kann eine abgebende LEI den Status des E-Rezepts im E-Rezept-Fachdienst auf "quittiert" ("completed") ändern. Die Operation muss zur Autorisierung des Aufrufenden (`IdentityToken`) die Rolle prüfen. Mit der Aktualisierung der `Task` in den Status "completed" gesetzt. Der E-Rezept-Fachdienst prüft die übergebene `MedicationDispense` strukturell und erzeugt eine Signatur mit der Signaturidentität `ID.FD.SIG`, die als Provenance mit Verweis auf den Task und die `MedicationDispense` gespeichert und an den Aufrufenden zurückgegeben wird.

Die Operation muss vor dem Statuswechsel prüfen, ob der Task den Status "in-progress" hat und ob das übermittelte Geheimnis (`Secret`) dem beim Abrufen des E-Rezeptes im Task erzeugten Geheimnis entspricht.

Die Operation übermittelt im Response die signierte Quittung (`Receipt`) als Provenance-Ressource. [<=]

A_19125 - Logische Operation "Quittung erneut abrufen"

Die Schnittstelle MUSS die logische Operation "Quittung erneut abrufen" implementieren.

Tabelle 38: TAB_SYSLERP_031 Operation Quittung erneut abrufen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	Quittung erneut abrufen	
Methode	GET	/Provenance
Attribut-In (Header)	<code>IdentityToken</code>	JSON Web Token
Attribut-In (URL)	<code>Searchparameters</code> <code>?target:Task={Rezept-ID}</code>	Suchparameter als URL-Parameter Provenance mit Verweis auf das quittierte E-Rezept
Attribut-Out (Body)	<code>Receipt</code>	signiertes JSON-Objekt Provenance über Task und MedicationDispense

Mit dieser Operation kann eine abgebende LEI eine Quittung erneut abrufen. Dafür wird eine Suchanfrage auf die Ressource Provenance durchgeführt, der Suchparameter ist dabei die Rezept-ID, der E-Rezept-Fachdienst prüft intern zusätzlich die Rolle des Aufrufenden und ob die Identität (`IdentityToken`) gleich derjenigen `Provenance.agent` ist, für die die Provenance ursprünglich ausgestellt wurde. [<=]

1624 **A_18868 - Logische Operation "E-Rezepte durch Versicherten abrufen"**

1625 Die Schnittstelle MUSS die logische Operation "E-Rezepte durch Versicherten
1626 abrufen" implementieren.

1627 **Tabelle 39: TAB_SYSLERP_043 Operation E-Rezepte durch Versicherten abrufen**

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezepte durch Versicherten abrufen	
Methode	GET	/Task
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-Out	Bundle mit Task- und Provenance-Ressourcen	JSON-Objekt

1628 Mit dieser Operation kann ein Versicherter alle für ihn im E-Rezept-Fachdienst abgelegten
1629 E-Rezepte abrufen.

1630 Die Operation muss auf Basis der KVNR in der Identitätsbestätigung (`IdentityToken`) die
1631 E-Rezepte im E-Rezept-Fachdienst auswählen.

1632 Die Operation muss prüfen, ob die einzelnen E-Rezepte einen Status ungleich
1633 "initialisiert" ("draft") und "gelöscht" ("cancelled") haben. Die Ausgabe der Tasks erfolgt
1634 inkl. des QES-signierten FHIR-Bundles, mit der Anpassung, dass aus jedem signierten
1635 Bundle das Signatur-Attribut "Bundle.signature" entfernt wird. [`<=`]

1636 **A_18564 - Logische Operation "E-Rezept durch Vertreter abrufen"**

1637 Die Schnittstelle MUSS die logische Operation "E-Rezept durch Vertreter
1638 abrufen" implementieren.

1639 **Tabelle 40: TAB_SYSLERP_032 Operation E-Rezept durch Vertreter abrufen**

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Vertreter abrufen	
Methode	GET	/Task/{Rezept-ID}
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	AccessCode	Header-Attribut String (optional)
Attribut-Out (Body)	Bundle mit einer Task- und Provenance-Ressource	JSON-Objekt

Mit dieser Operation kann ein Versicherter oder Vertreter ein im E-Rezept-Fachdienst abgelegtes E-Rezept (Task) inkl. serverseitiger Signatur (Provenance) abrufen. Die Operation muss zur Autorisierung des Aufrufenden (IdentityToken) die Rolle prüfen. Der AccessCode muss dem beim Einstellen erzeugten Geheimnis entsprechen, mit dem der Versicherte den Zugriff auf das E-Rezept steuert. Ruft der Versicherte selbst ein einzelnes E-Rezept über die Rezept-ID ab, muss der AccessCode nicht übergeben werden.

Die Operation muss prüfen, ob das E-Rezept einen Status ungleich "initialisiert" ("draft") und "gelöscht" ("cancelled") hat. Die Ausgabe des Tasks erfolgt inkl. des QES-signierten FHIR-Bundles, mit der Anpassung, dass aus dem signierten Bundle das Signatur-Attribut "Bundle.signature" entfernt wird. [\leq]

A_18565 - Logische Operation "E-Rezept durch Versicherten löschen"

Die Schnittstelle MUSS die logische Operation "E-Rezept durch Versicherten löschen" implementieren.

Tabelle 41: TAB_SYSLERP_033 Operation E-Rezept durch Versicherten löschen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Versicherten löschen	
Methode	POST	/Task/{Rezept-ID}/\$abort
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	AccessCode	Header-Attribut String

Mit dieser Operation kann ein Versicherter ein für ihn abgelegtes E-Rezepts im E-Rezept-Fachdienst löschen ("cancelled"). Die Operation muss auf Basis der KVNR in der Identitätsbestätigung (IdentityToken) prüfen, ob das E-Rezept für den Versicherten erstellt wurde und ob das E-Rezept einen Status ungleich "in Abgabe (gesperrt)" ("in-progress") hat. DerAccessCode muss dem beim Einstellen erzeugten AccessCode entsprechen, mit dem der Versicherte den Zugriff auf das E-Rezept steuert. Die Operation löscht die personenbezogenen und medizinischen Daten aus dem E-Rezept-Datensatz. [\leq]

A_19140 - Logische Operation "Dispensierinformationen durch Versicherten abrufen"

Die Schnittstelle MUSS die logische Operation "Dispensierinformationen durch Versicherten abrufen" implementieren.

Tabelle 42: TAB_SYSLERP_054 Operation Dispensierinformationen durch Versicherten abrufen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	Dispensierinformationen durch Versicherten abrufen	

Methode	GET	/MedicationDispense
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	AccessCode	Header-Attribut String
Attribut-Out (Body)	MedicationDispense	JSON-Objekt

1669 Mit dieser Operation kann ein Versicherter die Dispensierinformationen für seine E-
 1670 Rezepte abrufen. Die Operation muss auf Basis der KVN in der Identitätsbestätigung
 1671 (`IdentityToken`) prüfen, ob die Dispensierinformationen für den Versicherten erstellt
 1672 wurden. Der `AccessCode` muss dem beim Erzeugen der Dispensierinformationen aus dem
 1673 zugrundeliegenden E-Rezept übernommenen `AccessCode` entsprechen, mit dem der
 1674 Versicherte den Zugriff auf das E-Rezept steuert. [`<=`]

1675 **A_19141 - Logische Operation "Dispensierinformation für ein einzelnes E-
 1676 Rezept abrufen"**

1677 Die Schnittstelle MUSS die logische Operation "Dispensierinformationen für ein einzelnes
 1678 E-Rezept durch Versicherten abrufen" implementieren.

1679 **Tabelle 43: TAB_SYSLERP_058 Operation Dispensierinformation für ein einzelnes E-
 1680 Rezept durch Versicherten oder Vertreter abrufen**

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	Dispensierinformation für ein einzelnes E-Rezept durch Versicherten oder Vertreter abrufen	
Methode	GET	/Task/{Rezept-ID}?_include=output
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	AccessCode	Header-Attribut String
Attribut-Out (Body)	Bundle aus Task und MedicationDispense	JSON-Objekt

1681 Mit dieser Operation kann ein Versicherter die Dispensierinformationen für ein einzelnes
 1682 E-Rezept abrufen. Die Operation muss zur Autorisierung des Aufrufenden
 1683 (`IdentityToken`) die Rolle prüfen. Der `AccessCode` muss dem beim Einstellen erzeugten
 1684 `AccessCode` entsprechen, mit dem der Versicherte den Zugriff auf das E-Rezept steuert.
 1685 Im Ergebnis wird das E-Rezept inklusive der Dispensierinformationen
 1686 zurückgegeben. [`<=`]

1687

4.3.2 Schnittstelle für die Ressource E-Rezept-Nachricht

Die Ressource E-Rezept-Nachricht enthält alle Daten zur Übermittlung eines E-Rezept-Tokens.

A_18869 - Logische Operation "E-Rezept-Nachricht einstellen"

Die Schnittstelle MUSS die logische Operation "E-Rezept-Nachricht einstellen" implementieren.

Tabelle 44: TAB_SYSLERP_044 Operation E-Rezept-Nachricht einstellen

Kategorie	Name	Typ
Ressource	Communication	
Operation	E-Rezept-Nachricht einstellen	
Methode	POST	/Communication
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Body)	Communication	JSON-Objekt

Mit dieser Operation kann der aufrufende Akteur eine E-Rezept-Nachricht einstellen. Die Nachricht als Communication-Objekt enthält den Identifikator des Empfängers als `Communication.recipient` (Telematik-ID oder Versicherten-ID) und die Operation übernimmt den Identifikator des Absenders aus dem `IdentityToken` (Versicherten-ID oder Telematik-ID als `Communication.sender`). Optional kann der Absender eine Referenz auf das in der Kommunikation referenzierte E-Rezept als URL auf die verordnete Medication in `Communication.payload.contentReference` einfügen. [<=]

A_18870 - Logische Operation "E-Rezept-Nachrichten abrufen"

Die Schnittstelle MUSS die logische Operation "E-Rezept-Nachrichten abrufen" implementieren.

Tabelle 45: TAB_SYSLERP_050 Operation E-Rezept-Nachrichten abrufen

Kategorie	Name	Typ
Ressource	Communication	
Operation	E-Rezept-Nachrichten abrufen	
Methode	GET	/Communication
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-Out (Body)	List of Messages	JSON-Objekt

Mit dieser Operation kann der aufrufende Akteur alle für ihn eingestellten E-Rezept-Nachrichten abrufen.

Die Operation wählt die Nachrichten auf Basis der Telematik-ID für Leistungserbringerinstitutionen bzw. KVNR für Versicherte in der Identitätsbestätigung

1711 (`IdentityToken`) aus (Telematik-ID bzw. Versicherten-ID muss gleich
1712 `Communication.recipient` sein).[<=]

1713 4.3.3 Schnittstelle für die Ressource Zugriffsprotokolleintrag

1714 Die Ressource Zugriffsprotokolleintrag enthält alle Daten zum Zugriff eines Akteurs auf
1715 die E-Rezept-Datensätze eines Versicherten.

1716 **A_18871 - Logische Operation "Zugriffsprotokolleinträge durch Versicherten 1717 abrufen"**

1718 Die Schnittstelle MUSS die logische Operation "Zugriffsprotokolleinträge durch
1719 Versicherten abrufen" implementieren.

1720 **Tabelle 46: TAB_SYSLERP_051 Operation Zugriffsprotokolleinträge durch Versicherten**
1721 **abrufen**

Kategorie	Name	Typ
Ressource	AuditEvent	
Operation	Zugriffsprotokolleinträge durch Versicherten abrufen	
Methode	GET	/AuditEvent
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (URL)	Filter	URL-Parameter für AuditEvent
Attribut-Out (Body)	List of AuditEvent	JSON-Objekt

1722 Mit dieser Operation kann ein Versicherter alle im Zugriffsprotokoll abgelegten Einträge
1723 (`AuditEvents`) abrufen.

1724 Die Operation wählt die Protokolleinträge auf Basis der KVN in der Identitätsbestätigung
1725 (`IdentityToken`) aus. Mittels URL-Parameter-Filter kann zusätzlich nach Ereignissen
1726 gefiltert werden (z.B. nicht älter als <date>).[<=]

1727 4.3.4 Schnittstelle für die Ressource signierte Challenge

1728 Für die Authentifizierung bei Verwendung von Smart Cards der TI im Challenge-
1729 Response-Verfahren wird eine Schnittstelle zwischen Authentisierungsmodul und IdP
1730 benötigt. Dazu wird hier eine Ressource definiert.

1731 **A_18887 - Logische Operation "signierte Challenge übergeben"**

1732 Die Schnittstelle MUSS die logische Operation "signierte Challenge übergeben"
1733 implementieren.

Kategorie	Name	Typ
-----------	------	-----

Ressource	signierte Challenge	
Operation	signierte Challenge übergeben	
Methode	POST	
Param-In	signierte Challenge	
Param-In	Zertifikat	
Param-Out	AuthN-Code oder Liste der angeforderten Identitätsattribute (falls Einwilligung erforderlich)	

1734 Mit dieser Operation kann das Authentisierungsmodul eine signierte Challenge,
 1735 zusammen mit dem Zertifikat des Nutzers, an den IdP übergeben (Signatur per AUT-
 1736 Identität der Smart Card). Die Challenge erhält das Authentisierungsmodul zuvor vom
 1737 IdP. [<=]

1738 4.3.5 Schnittstelle für die Ressource Einwilligung

1739 Für das Einholen einer Einwilligung (Consent) des Nutzers in die Verwendung angefragter
 1740 Identitätsattribute wird eine Schnittstelle zwischen Authentisierungsmodul und IdP
 1741 benötigt. Dazu wird hier eine Ressource definiert.

1742 A_18888 - Logische Operation "Einwilligung erteilen"

1743 Die Schnittstelle MUSS die logische Operation "Einwilligung erteilen" implementieren.

Kategorie	Name	Typ
Ressource	Einwilligung	
Operation	Einwilligung erteilen	
Methode	POST	
Param-In	Einwilligung	
Param-Out	AuthN-Code	

1744 Mit dieser Operation kann das Authentisierungsmodul die Einwilligung des Nutzers für die
 1745 Verwendung der Identitätsattribute (Consent) an den IdP übergeben. Die angeforderten
 1746 Identitätsattribute erhält das Authentisierungsmodul zuvor vom IdP. [<=]

1747

5 Datenschutz- und Sicherheitsaspekte

1748 Für die Akzeptanz der Fachanwendung E-Rezept durch die Nutzer ist die Gewährleistung
 1749 des Datenschutzes und - damit verbunden - die Sicherheit der personenbezogenen
 1750 medizinischen Daten ein unabdingbares Merkmal. Die Fachanwendung E-Rezept erreicht
 1751 dies durch das Aufstellen von Anforderungen an den Datenschutz und die
 1752 Informationssicherheit, das Prüfen der Einhaltung dieser Anforderungen in der Zulassung
 1753 und die Überprüfung der Einhaltung der Anforderungen im laufenden Betrieb durch den
 1754 Anbieter des E-Rezept-Fachdienstes selbst, aber auch durch Audits der gematik.

1755 Die aufgestellten Anforderungen des Datenschutzes und der Informationssicherheit
 1756 entsprechen dem Gebot der Angemessenheit dadurch, dass sie einerseits den
 1757 Schutzbedarf der zu verarbeitenden Daten und andererseits die Umsetzungsfähigkeit
 1758 durch den Hersteller des E-Rezept-Frontend des Versicherten und den Anbieter des E-
 1759 Rezept-Fachdienstes berücksichtigen. Die Angemessenheit der Anforderungen hinsichtlich
 1760 des Schutzbedarfs wird durch die Nutzung der Methoden zur Informationssicherheit und
 1761 des Datenschutzes der TI unter Beachtung der Risiko-Policy der TI erreicht. Die
 1762 Angemessenheit hinsichtlich der Umsetzbarkeit wird in den spezifizierten Technologien
 1763 berücksichtigt.

1764 Die Sicherheitsanforderungen an den E-Rezept-Fachdienst leiten sich zum einen vom
 1765 Schutzbedarf der verarbeiteten Daten und zum anderen von der potenziellen negativen
 1766 Beeinflussung der TI durch diesen Dienst ab.

1767 Hinsichtlich des maßgeblichen Schutzbedarfs wurden folgende Informationsobjekte
 1768 identifiziert:

1769 **Tabelle 47: TAB_SYSLERP_052 Schutzbedarf der maßgeblichen Informationsobjekte**

Informationsobjekt	Vertraulichkeit	Integrität	Authentizität
E-Rezept (Ohne Schutzmaßnahmen)	sehr hoch	sehr hoch	sehr hoch
E-Rezept (QES-signiert)	sehr hoch	normal	normal
E-Rezept-Token	sehr hoch	hoch	normal
Nachricht	sehr hoch	hoch	normal
Zusatzinformationen im Access-Token	normal	normal	normal
Quittung (vom E-Rezept-Fachdienst signiert)	normal	normal	normal
Protokolldaten	sehr hoch	sehr hoch	sehr hoch
Authentisierungs-Token (AuthN-Token des IdP, vom IdP signiert)	sehr hoch	sehr hoch	normal
Identitätsmerkmale der Nutzer im IdP	normal	sehr hoch	sehr hoch

1770 Die für die Verfügbarkeit maßgeblichen Prozesse sind:

1771 **Tabelle 48: TAB_SYSLERP_053 Schutzbedarf der maßgeblichen Prozesse**

Prozess	Verfügbarkeit
Anwendungsfall "UC 4.1 - E-Rezept durch Abgebenden abrufen"	hoch
Anwendungsfall "UC 5.2 - AuthN-Token durch LEI anfordern"	hoch

1772 Für die Aufrechterhaltung des Datenschutz- und Informationssicherheitsniveaus der TI ist
 1773 es erforderlich, dass die TI durch die Nutzung der Fachanwendung E-Rezept nicht negativ
 1774 beeinflusst wird. Eine Beeinträchtigung kann insbesondere über den Anschluss des E-
 1775 Rezept-Fachdienstes erfolgen. Um dies zu verhindern, werden dem Anbieter des E-
 1776 Rezept-Fachdienstes entsprechend dem Modularisierungskonzept in
 1777 [gemSpec_DS_Anbieter] Module der Informationssicherheit und des Datenschutzes
 1778 zugeordnet.

1779 Über diese Module bzw. die zugehörigen Anforderungen wird der Anbieter auch
 1780 verpflichtet, Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der
 1781 Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der
 1782 Sicherheit der Verarbeitung einzurichten.

1783 Aufgrund der Kritikalität des E-Rezept-Fachdienstes wird zudem eine Anforderung an die
 1784 Vertrauenswürdigkeit des Anbieters des E-Rezept-Fachdienstes gestellt:

1785 **A_19010 - Vertrauenswürdigkeit des Anbieters**

1786 Der Anbieter des E-Rezept-Fachdienstes MUSS für den Betrieb des E-Rezept-
 1787 Fachdienstes geeignet sein.

1788 Das heißt insbesondere, dass das Vertrauen in ihn gesetzt werden kann, dass er
 1789 organisatorische oder technische Schwachstellen im E-Rezept-Fachdienstes für
 1790 unberechtigte Zugriffe auf E-Rezepte ausnutzt. [≤]

1791 Beispiele für Kriterien des Nachweises der Vertrauenswürdigkeit sind, dass der Anbieter
 1792 in den letzten fünf Jahren bereits Anwendungen betreibt, in denen besonders
 1793 schützenswerte Daten nach Artikel 9 DSGVO (insbes. personenbezogene medizinische
 1794 Daten) verarbeitet wurden, oder dass der Anbieter in den letzten drei Jahren keine
 1795 meldepflichtigen Datenschutzvorfälle zu verzeichnen hatte. Eine weitere Möglichkeit wäre
 1796 die Sicherstellung von Datenschutz und Sicherheit beim Anbieter durch externe
 1797 Gutachter (z.B. im Rahmen von Zertifizierungen bzw. Prüfsiegeln) überprüfen und
 1798 bestätigen zu lassen.

1799 **5.1 Anforderungen an den E-Rezept-Fachdienst**

1800 Folgende Anforderungen müssen durch den E-Rezept-Fachdienst zudem umgesetzt
 1801 werden:

1802 **A_18566 - Schutz der Kommunikation**

1803 Der E-Rezept-Fachdienst MUSS sicherstellen, dass alle Komponenten des E-Rezept-
 1804 Fachdienstes vertraulich miteinander kommunizieren. [≤]

1805 **A_18567 - Transportverschlüsselte Übertragung von Daten**

1806 Der E-Rezept-Fachdienst MUSS sicherstellen, dass die vertrauliche E-Rezept-
 1807 Verarbeitung nur transportverschlüsselt mit Clients kommuniziert. [≤]

1808 Hinweis: für die Qualität der Transportverschlüsselung gelten die Anforderungen aus
1809 [gemSpec_Krypt].

1810 **A_18568 - Möglichkeit der Authentisierung gegenüber Clients**

1811 Der E-Rezept-Fachdienst MUSS sicherstellen, dass die vertrauliche E-Rezept-
1812 Verarbeitung sich gegenüber Clients, die mit ihr kommunizieren, authentisiert. [<=]

1813 **A_18851 - Kommunikation nur zwischen Berechtigten**

1814 Der E-Rezept-Fachdienst MUSS sicherstellen, dass er nur berechnigte
1815 Kommunikationsbeziehungen zulässt. [<=]

1816 **A_18569 - Ablegen und Abrufen von E-Rezepten nur durch berechnigte
1817 Leistungserbringer**

1818 Der E-Rezept-Fachdienst MUSS sicherstellen, dass nur zum Einstellen berechnigte
1819 Leistungserbringer E-Rezepte einstellen und nur zur Abgabe berechnigte
1820 Leistungserbringer E-Rezepte abrufen können. [<=]

1821 **A_18570 - Verbot der Auswertung von Beziehungen zwischen LE, LEI und
1822 Versicherten**

1823 Der E-Rezept-Fachdienst MUSS verhindern, dass eine Auswertung von Beziehungen
1824 zwischen LE, LEI und Versicherten möglich ist. [<=]

1825 **A_18571 - Verbot der Profilbildung**

1826 Der E-Rezept-Fachdienst MUSS verhindern, dass eine missbräuchliche Profilbildung
1827 möglich ist. [<=]

1828 **A_18844 - Schutzmaßnahmen gegen die OWASP Top 10 Risiken**

1829 Der E-Rezept-Fachdienst MUSS Maßnahmen zum Schutz vor der aktuellen Version der
1830 OWASP-Top-10-Risiken umsetzen. [<=]

1831 **A_18845 - Schutz der E-Rezepte**

1832 Der E-Rezept-Fachdienst MUSS sicherstellen, dass E-Rezepte während der Verarbeitung
1833 vor dem Zugriff durch den Anbieter technisch geschützt sind. [<=]

1834 **A_18846 - Speicherung von E-Rezepten nur verschlüsselt**

1835 Der E-Rezept-Fachdienst MUSS sicherstellen, dass E-Rezepte nur
1836 verschlüsselt persistent im E-Rezept-Fachdienst gespeichert werden. [<=]

1837 **A_18847 - Speicherung von Nachrichten nur verschlüsselt**

1838 Der E-Rezept-Fachdienst MUSS sicherstellen, dass Nachrichten nur verschlüsselt
1839 persistent im E-Rezept-Fachdienst gespeichert werden. [<=]

1840 **A_18841 - Erkennung Anomalien auf Netzwerkebene**

1841 Der E-Rezept-Fachdienst MUSS Anomalien auf Netzwerkebene erkennen und darauf
1842 reagieren können. [<=]

1843 **A_18842 - Erkennung Anomalien beim Einstellen von E-Rezepten**

1844 Der E-Rezept-Fachdienst MUSS Anomalien in der pro Zeiteinheit von einer
1845 Leistungserbringerinstitution eingestellten Menge von E-Rezepten erkennen und darauf
1846 reagieren können. [<=]

1847 **A_18843 - Erkennung Anomalien beim Abrufen von E-Rezepten**

1848 Der E-Rezept-Fachdienst MUSS Anomalien in der pro Zeiteinheit von einer
1849 Leistungserbringerinstitution abgerufenen Menge von E-Rezepten erkennen und darauf
1850 reagieren können. [<=]

1851 **A_18923 - Authentisierungsniveau für E-Rezept-Fachdienst mindestens "hoch"**

1852 Der E-Rezept-Fachdienst DARF NICHT AuthN-Token des IdP akzeptieren, die mit einem
1853 geringeren Authentisierungsniveau als "hoch" gemäß Verordnung (EU) Nr. 910/2014
1854 (eIDAS-Verordnung) ausgestellt wurden. [<=]

5.1.1 Anforderungen an die Vertrauenswürdige Ausführungsumgebung

In diesem Abschnitt werden die Anforderungen an den E-Rezept-Fachdienst zur Umsetzung einer Vertrauenswürdigen Ausführungsumgebung (VAU) gestellt. Die VAU dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten unverschlüsselten Daten innerhalb des E-Rezept-Fachdienstes. Die VAU stellt dazu einen Verarbeitungskontext bereit, in dem die Verarbeitung sensibler Daten unverschlüsselt erfolgen kann. Dieser Verarbeitungskontext ist entsprechend zu schützen.

A_18872 - Umsetzung des E-Rezept-Verwaltung in einer Vertrauenswürdigen Ausführungsumgebung (VAU)

Der E-Rezept-Fachdienst MUSS die Verarbeitung der fachlichen Operationen im Verarbeitungskontext einer Vertrauenswürdigen Ausführungsumgebung (VAU) umsetzen.[<=]

5.1.2 Verarbeitungskontext

Die Gesamtheit aus der für eine Verarbeitung der unverschlüsselten Daten erforderlichen Software, dem für diese Verarbeitung genutzten physikalischen System sowie den für die Integrität dieser Verarbeitung erforderlichen organisatorischen und physischen Rahmenbedingungen bildet den Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung.

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

Zur Vertrauenswürdigen Ausführungsumgebung gehören neben den Verarbeitungskontexten alle für ihre Erreichbarkeit und betriebliche Steuerung erforderlichen Komponenten. Sie dürfen nur soweit unbedingt erforderlich als Teil des Verarbeitungskontextes implementiert sein.

A_18873 - Verarbeitungskontext der VAU

Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sämtliche physikalischen Systemkomponenten sowie sämtliche Softwarekomponenten umfassen, deren Sicherheitseigenschaften sich auf den Schutz der personenbezogenen medizinischen Daten vor Zugriff durch Unbefugte bei ihrer unverschlüsselten Verarbeitung auswirken können.[<=]

A_18874 - Verschlüsselung von außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten

Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass sämtliche schützenswerten Daten vor einer Speicherung außerhalb der VAU verschlüsselt werden.[<=]

A_18875 - Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU

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

A_18876 - Verschlüsselung der E-Rezept-Daten und technischen Daten der VAU
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS für die Verschlüsselung aller E-Rezept-Daten sowie eigener technischer Daten den Persistenz-Schlüssel verwenden.[<=]

Als Persistenz-Schlüssel wird ein kryptographischer, symmetrischer Schlüssel verstanden, der folgende Eigenschaften aufweist:

- Er schützt durch Ver- und Entschlüsselung sämtliche schützenswerten E-Rezept-bezogenen Daten.
- Er wird an die Verarbeitungskontexte, die auf die verschlüsselte Datenspeicherung zugreifen müssen, für die Nutzung zur Ver- und Entschlüsselung gespeicherter Daten im Rahmen der Initialisierung der Verarbeitungskontexte sicher übermittelt.
- Er ist vor jedem Zugriff durch den Anbieter des E-Rezept-Fachdienstes geschützt gespeichert.

Eine ggf. erforderliche Umschlüsselung der durch einen Persistenz-Schlüssel geschützten Daten ist nur innerhalb des Verarbeitungskontextes der VAU oder innerhalb eines HSM und nach Autorisierung im "Mehr-Augen-Prinzip" zulässig.

A_19070 - Begrenzung der mit einem Persistenz-Schlüssel gesicherten Datenmenge

Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS den Persistenz-Schlüssel regelmäßig wechseln und damit sicherstellen, dass in den außerhalb der VAU gespeicherten Daten nur jeweils kleine Segmente mit einem Persistenz-Schlüssel verschlüsselt sind.[<=]

5.1.3 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld

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

A_18877 - Isolation der VAU von Datenverarbeitungsprozessen des Anbieters

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

A_18878 - Ausschluss von Manipulationen an der Software der VAU

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

A_18879 - Ausschluss von Manipulationen an der Hardware der VAU

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

A_18880 - Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU

Die VAU des E-Rezept-Fachdienstes MUSS den Ausschluss von Manipulationen an der für Verarbeitungskontexte eingesetzten Hardware und Software durch den Anbieter des E-

- 1947 Rezept-Fachdienstes mit Mitteln umsetzen, deren dauerhafte und kontinuierliche
1948 Wirksamkeit gewährleistet werden kann.[<=]
- 1949 **A_18881 - Kein physischer Zugang des Anbieters zu Systemen der VAU**
1950 Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln sicherstellen, dass
1951 niemand, auch nicht der Anbieter des E-Rezept-Fachdienstes, während der Verarbeitung
1952 personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme
1953 erlangen kann, auf denen Verarbeitungskontexte ausgeführt werden.[<=]
- 1954 **A_18882 - Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU**
1955 Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln sicherstellen, dass
1956 physischer Zugang zu Hardware-Komponenten der Verarbeitungskontexte nur erfolgen
1957 kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten extrahiert werden
1958 können.[<=]
- 1959 **A_18832 - Gute Prüfbarkeit der Sicherheitseigenschaften von Code in der VAU**
1960 Die VAU des E-Rezept-Fachdienstes MUSS die Verarbeitungslogik in
1961 Verarbeitungskontexten mittels Komponenten umsetzen, die ein hohes Maß an
1962 Gewissheit bei der Feststellung der Sicherheitseigenschaften der Anwendung ermöglichen
1963 und dazu auf Ebene des Codes (der Trusted Computing Base) möglichst kompakt
1964 gehalten werden.[<=]
- 1965 Die VAU des E-Rezept-Fachdienstes benötigt symmetrisches Schlüsselmaterial für die
1966 Speicherung der E-Rezept-Daten außerhalb der VAU, um für persistierte Daten den
1967 Anbieter vom Zugriff auszuschließen. Die Funktionen der Vorhaltung und Bereitstellung
1968 des Persistenz-Schlüssels wird von einem HSM ausgefüllt. Das HSM muss die Integrität
1969 der Verarbeitungskontexte feststellen können, bevor es einen Persistenz-Schlüssel an
1970 einen Verarbeitungskontext übermittelt.
- 1971 **A_18833 - Persistenz-Schlüssel der VAU von HSM bereitgestellt**
1972 Die VAU des E-Rezept-Fachdienstes MUSS den für die verschlüsselte Speicherung von E-
1973 Rezept-Daten außerhalb der Verarbeitungskontexte erforderlichen symmetrischen
1974 Persistenz-Schlüssel im Zuge des Startvorgangs jedes Verarbeitungskontextes aus einem
1975 HSM beziehen.[<=]
- 1976 Die VAU des E-Rezept-Fachdienstes muss sich gegenüber Nutzern mittels eines
1977 Dienstzertifikats ausweisen, welches die Vertrauenswürdigkeit des Dienstes repräsentiert.
1978 Die Nutzung des privaten Schlüssels dieses Dienstzertifikats muss an die
1979 Integritätsprüfung der Verarbeitungskontexte gebunden sein und darf ausschließlich
1980 innerhalb eines HSM erfolgen.
- 1981 **A_18834 - Integritätsprüfung der VAU**
1982 Das HSM des E-Rezept-Fachdienstes MUSS sicherstellen, dass es der VAU den benötigten
1983 Persistenz-Schlüssel erst zur Verfügung stellt bzw. Signaturen für die VAU im Rahmen
1984 des Verbindungsaufbaus von Clients zur VAU erst erstellt nachdem der
1985 Verarbeitungskontext seine Integrität gegenüber dem HSM nachgewiesen hat.[<=]
- 1986 **A_18883 - HSM-Kryptographieschnittstelle und Persistenz-Schlüssel verfügbar**
1987 **nur für Verarbeitungskontexte der VAU**
1988 Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln, die auch
1989 Manipulationen durch den Anbieter des E-Rezept-Fachdienstes ausschließen,
1990 gewährleisten, dass nur integere Verarbeitungskontexte der VAU Zugriff auf die
1991 Kryptographieschnittstelle des HSM zur Nutzung des privaten Schlüsselmaterials für ihr
1992 Dienstzertifikat und zum Bezug des Persistenz-Schlüssels erhalten kann.[<=]
- 1993 **A_18884 - Aktivierung des Verarbeitungskontextes der VAU**
1994 Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln gewährleisten, dass
1995 schützenswerte Nutzdaten im Verarbeitungskontext erst nach Bezug des Persistenz-
1996 Schlüssels entschlüsselt und verarbeitet werden können.[<=]

1997 **A_18885 - Keine Speicherung der Persistenz-Schlüssel in**
1998 **Verarbeitungskontexten der VAU**

1999 Die VAU des E-Rezept-Fachdienstes DARF den Persistenz-Schlüssel in
2000 Verarbeitungskontexten NICHT über einen Neustart hinaus speichern oder
2001 verwenden. [<=]

2002 **A_18886 - Datenschutzkonformes Logging und Monitoring des**
2003 **Verarbeitungskontextes der VAU**

2004 Die VAU des E-Rezept-Fachdienstes MUSS die für den Betrieb eines Fachdienstes
2005 erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben
2006 und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dem Anbieter des
2007 E-Rezept-Fachdienstes vertrauliche oder zur Profilbildung geeignete Daten zur Kenntnis
2008 gelangen. [<=]

2009 **A_18920 - Managementprozesse des HSM**

2010 Der E-Rezept-Fachdienst MUSS die Managementprozesse des HSM so gestalten, dass ein
2011 Missbrauch des Schlüsselmaterials durch den Betreiber des E-Rezept-Fachdienstes
2012 ausgeschlossen wird. [<=]

2013 **5.1.4 Trennung von Session- und Request-Kontexten**

2014 In jedem Verarbeitungskontext der VAU des E-Rezept-Fachdienstes werden Daten
2015 unverschlüsselt verarbeitet, die zu genau einem Akteur gehören und dementsprechend
2016 einer authentifizierten Client-Verbindung zuzuordnen sind. Innerhalb einer Client-Session
2017 kann z. B. der verordnende Arzt ein mehrzeiliges Rezept (in Form eines E-Rezepts pro
2018 Zeile) im E-Rezept-Fachdienst ablegen.

2019 Aus Gründen der Skalierbarkeit des Fachdienstes können Verarbeitungskontexte in
2020 verschiedenen Komponenten des Dienstes auf Basis verschiedener Methoden bzw.
2021 Technologien separiert werden.

2022 Ein grundlegender Faktor für die Bewertung der Qualität der Kontextseparation ist die
2023 Komplexität der in jeder Komponente umgesetzten Verarbeitung und damit die
2024 Möglichkeit zur belastbaren Feststellung der Zuverlässigkeit der Kontextseparation in der
2025 Komponente.

2026 **A_19001 - Isolation zwischen Datenverarbeitungsprozessen mehrerer**
2027 **Verarbeitungskontexte der VAU**

2028 Die VAU des E-Rezept-Fachdienstes MUSS die in ihr ablaufenden Verarbeitungen für die
2029 Daten eines Verarbeitungskontextes von den Verarbeitungen für die Daten anderer
2030 Verarbeitungskontexte in solcher Weise trennen, dass mit technischen Mitteln
2031 ausgeschlossen wird, dass die Verarbeitungen eines Verarbeitungskontextes schadhaft
2032 auf die Verarbeitungen eines anderen Verarbeitungskontextes einwirken können. [<=]

2033 **A_19002 - Verfügbarkeit des Persistenz-Schlüssels in der VAU**

2034 Die VAU des E-Rezept-Fachdienstes MUSS sicherstellen, dass der für die Speicherung von
2035 Daten außerhalb der VAU genutzte Persistenz-Schlüssel ausschließlich innerhalb von
2036 Verarbeitungskontexten der VAU verfügbar ist. [<=]

2037 **A_19003 - Schutz des Persistenz-Schlüssels der VAU**

2038 Die VAU des E-Rezept-Fachdienstes MUSS sicherstellen, dass kein Verarbeitungsvorgang
2039 zum Verlust von Vertraulichkeit oder Integrität des Persistenz-Schlüssels führen kann.
2040 Dies gilt auch im Falle von Manipulationsversuchen seitens authentifierter Akteure sowie
2041 im Falle von Verarbeitungsfehlern jeder Art. [<=]

2042 Aus Sicherheitsgründen und aus Gründen der betrieblichen Stabilität müssen
2043 Verarbeitungsvorgänge und in ihnen möglicherweise auftretende Fehlerzustände
2044 voneinander isoliert werden. Ein konsistenter Systemzustand des E-Rezept-Fachdienstes

2045 muss auch nach einem schwerwiegenden Fehler in der Datenverarbeitung (z. B. aufgrund
2046 eines Hardware-Fehlers) wiederhergestellt werden können, ohne dass die Verfügbarkeit
2047 des Dienstes wesentlich eingeschränkt wird.

2048 **A_19005 - Fault Isolation und Wiederherstellung**

2049 Der E-Rezept-Fachdienst MUSS sicherstellen, dass Fehler in Verarbeitungsvorgängen auf
2050 die Verarbeitung des jeweils in Verarbeitung befindlichen E-Rezepts begrenzt bleiben und
2051 dass die Wiederherstellung eines konsistenten Systemzustands aus den persistierten
2052 Daten immer möglich ist.[<=]

2053 **A_19006 - Zuordnung von Verarbeitungskontexten und persistenten** 2054 **Datenstrukturen**

2055 Der E-Rezept-Fachdienst SOLL die Struktur der persistenten Datenhaltung darauf
2056 ausrichten, dass im Rahmen der Wiederherstellung eines konsistenten Systemzustands
2057 nach einem Verarbeitungsfehler die Rekonstruktion nur des Verarbeitungskontextes des
2058 von dem Verarbeitungsfehler direkt betroffenen E-Rezepts aus dem persistenten
2059 Datenspeicher erforderlich ist.[<=]

2060 **5.2 Anforderungen an das E-Rezept-Frontend des Versicherten**

2061 Für das E-Rezept-Frontend des Versicherten gelten die Anforderungen aus
2062 [gemSpec_DS_Hersteller].

2063 Folgende Anforderungen müssen durch das E-Rezept-Frontend des Versicherten
2064 umgesetzt werden:

2065 **A_18572 - Information zur Einsatzumgebung**

2066 Das E-Rezept-Frontend des Versicherten MUSS sicherstellen, dass der Nutzer über die
2067 Annahmen und Anforderungen an die Einsatzumgebung des FdV informiert wird.[<=]

2068 **A_18573 - Anzeige von Protokolldaten**

2069 Das E-Rezept-Frontend des Versicherten MUSS es den Versicherten ermöglichen, die für
2070 die Fachanwendung für ihn erzeugten Protokolleinträge anzeigen zu können.[<=]

2071 **A_18574 - Schutz der sensiblen Daten im E-Rezept-Frontend des Versicherten**

2072 Das E-Rezept-Frontend des Versicherten MUSS Maßnahmen zum Schutz vor der
2073 aktuellen Version der OWASP-Mobile-Top-10-Risiken umsetzen.[<=]

2074 Hinweis: Die Best-Practice-Sicherheitsmaßnahmen sind abhängig von der Technologie,
2075 mit der das E-Rezept FdV vom Hersteller umgesetzt wird.

2076 **A_18575 - Verhindern von Session Hijacking im E-Rezept-Frontend des** 2077 **Versicherten**

2078 Das E-Rezept-Frontend des Versicherten MUSS sicherstellen, dass eine eRp-Session
2079 nicht von anderen Anwendungen auf dem Gerät übernommen werden kann.[<=]

2080 **5.3 Anforderungen an den Identity Provider**

2081 Dem Anbieter des IdP werden entsprechend dem Modularisierungskonzept in
2082 [gemSpec_DS_Anbieter] Module der Informationssicherheit und des Datenschutzes
2083 zugeordnet.

2084 Folgende Anforderungen müssen durch den IdP zudem umgesetzt werden:

2085 **A_18861 - Gewährleistung des Schutzbedarfs**

2086 Der IdP MUSS sicherstellen, dass die Prozesse zur Verwaltung der Identitätsmerkmale
2087 deren Schutzbedarf gewährleisten. [≤]

2088 Durch einen Missbrauch des IdP (z.B. durch einen Innentäter bei einem
2089 Authentifizierungsdienst) kann ein missbräuchlicher Zugriff auf die in Fachdiensten der TI
2090 gespeicherten personenbezogenen medizinischen Daten erfolgen, sofern der Fachdienst
2091 nicht weitere eigene Sicherheitsmaßnahmen einsetzt. Es sind daher durch den IdP
2092 geeignete Maßnahmen umzusetzen, die das Risiko eines solchen Missbrauchs verhindern.

2093 **A_18862 - Transportverschlüsselte Übertragung von AuthN-Token**

2094 Der IdP MUSS sicherstellen, dass er nur transportverschlüsselt mit Clients
2095 kommuniziert. [≤]

2096 Hinweis: für die Qualität der Transportverschlüsselung gelten die Anforderungen aus
2097 [gemSpec_Krypt].

2098 **A_18863 - Authentifizierungsverfahren mit Sicherheitsniveau hoch**

2099 Der IdP MUSS Authentifizierungsverfahren mit einem Sicherheitsniveau von hoch gemäß
2100 Artikel 8 Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) anbieten. [≤]

2101 **A_18864 - Sicherheitsbetrachtungen berücksichtigen**

2102 Der IdP MUSS die Sicherheitsbetrachtungen der eingesetzten Standards
2103 berücksichtigen. [≤]

2104 Für die durch den IdP genutzten kryptographische Verfahren, sind die Anforderungen aus
2105 [gemSpec_Krypt] einzuhalten.

2106 **A_18860 - Zeitliche Begrenzung AuthN-Token**

2107 Der IdP MUSS AuthN-Token zeitlich begrenzen. [≤]

2108 **A_18858 - Ungültigkeit AuthN-Token nach Logout**

2109 Der IdP MUSS sicherstellen, dass nach einer Abmeldung des Nutzers die AuthN-Token
2110 nicht mehr verwendbar sind. [≤]

2111 **A_18857 - Widerruf AuthN-Token durch Nutzer**

2112 Der IdP MUSS sicherstellen, dass ein Nutzer ein für ihn ausgestelltes AuthN-Token
2113 jederzeit für ungültig erklären kann. [≤]

2114 **A_18856 - Beschränkung auf erforderliche Informationen**

2115 Der IdP DARF NICHT mehr Identitätsmerkmale in einen Token eintragen, als durch den
2116 Nutzer angefordert werden. [≤]

2117 **A_18859 - Verbot der Profilbildung**

2118 Der IdP MUSS verhindern, dass eine missbräuchliche Profilbildung möglich ist. [≤]

2119 **5.4 Grenzen der Sicherheitsleistung der Fachanwendung E-Rezept**

2120 Nicht alle Sicherheitsleistungen, die von der Fachanwendung E-Rezept benötigt werden,
2121 werden von Produkttypen der Fachanwendung umgesetzt. Zum Teil werden solche
2122 Leistungen von der TI-Plattform bereitgestellt, zum Teil müssen Systeme außerhalb der
2123 TI diese Leistungen übernehmen.

2124 Leistungen, die durch die TI-Plattform erbracht werden:

- 2125 • die Identifikation von TI-Teilnehmern,
- 2126 • das Erstellen einer fortgeschrittenen und einer qualifizierten elektronischen
- 2127 Signatur und die Prüfung einer qualifizierten elektronischen Signatur.

2128 Leistungen, die nicht durch die TI erbracht werden:

- 2129
- 2130
- 2131
- 2132
- 2133
- 2134
- 2135
- 2136
- 2137
- 2138
- 2139
- 2140
- 2141
- 2142
- 2143
- 2144
- 2145
- 2146
- 2147
- 2148
- 2149
- 2150
- 2151
- 2152
- 2153
- E-Rezept-Token, die außerhalb der TI transportiert werden, können durch die TI nicht geschützt werden. Der Schutz dieser E-Rezept-Token liegt in der Verantwortung derjenigen, die diese Übermittlungsverfahren anwenden.
 - Die Verhinderung von Mehrfacheinlösungen und damit auch Mehrfachabrechnungen eines E-Rezepts muss durch die Prozesse und Systeme bei den abgebenden Leistungserbringern und Kostenträgern erfolgen. Nur für E-Rezepte, die über den E-Rezept-Fachdienst transportiert werden, stellt der E-Rezept-Fachdienst eine Quittung aus. Sollten E-Rezept-Dateien über andere Wege, als die TI transportiert werden, so kann die TI eine Mehrfacheinlösung nicht verhindern, sondern die Prozesse und Systeme bei den abgebenden Leistungserbringern und Kostenträgern müssen auf eine korrekte Quittung achten.
 - Die TI stellt nicht sicher, dass ein E-Rezept, das über den E-Rezept-Fachdienst transportiert wird, syntaktisch oder semantisch korrekt ist. Das E-Rezept-Frontend des Versicherten kann den Versicherten auf syntaktisch nicht korrekte E-Rezepte hinweisen – in diesen Fällen wird es die E-Rezepte auch nicht anzeigen können. Die Primärsysteme der verordnenden Leistungserbringer sind für die korrekte Erzeugung der E-Rezepte verantwortlich. Die Primärsysteme der abgebenden Leistungserbringer sollten in jedem Fall mit syntaktisch unkorrekten E-Rezepten umgehen können und sich zudem gegen Schadsoftware schützen.
 - Die TI kann eine missbräuchlichen Ausstellung von E-Rezepten in der Umgebung des verordnenden Leistungserbringers durch eine Übernahme der Kontrolle über alle dafür notwendigen Komponenten (inkl. ausgespäter PIN für eine QES-Erstellung mittels entwendeten HBAs) nicht verhindern.

2154

6 Informationsmodell

6.1 Technisches Informationsmodell

2156 Der E-Rezept-Fachdienst erzeugt eine eindeutige Rezept-ID, welche das E-Rezept, den
2157 zugehörige Dispensierdatensatz und die Quittung identifiziert, sowie einen AccessCode.

2158 Das E-Rezept wird durch den verordnenden Leistungserbringer auf den E-Rezept-
2159 Fachdienst hochgeladen. Zusammen mit dem E-Rezept werden folgende Metadaten im E-
2160 Rezept-Fachdienst im E-Rezept-Datensatz verwaltet:

- 2161 • Versicherten-ID des Versicherten, dem das E-Rezept verordnet wurde,
- 2162 • der Status des E-Rezepts,
- 2163 • das Datum der letzten Statusänderung,
- 2164 • AccessCode,
- 2165 • der Leistungserbringer-Typ, welcher zur Abgabe berechtigt ist,
- 2166 • gültig bis (einlösbar),
- 2167 • das Geheimnis zur Statusänderung "in Abgabe (gesperrt)" für die Prüfung von
2168 Statusübergängen und
- 2169 • Quittung.

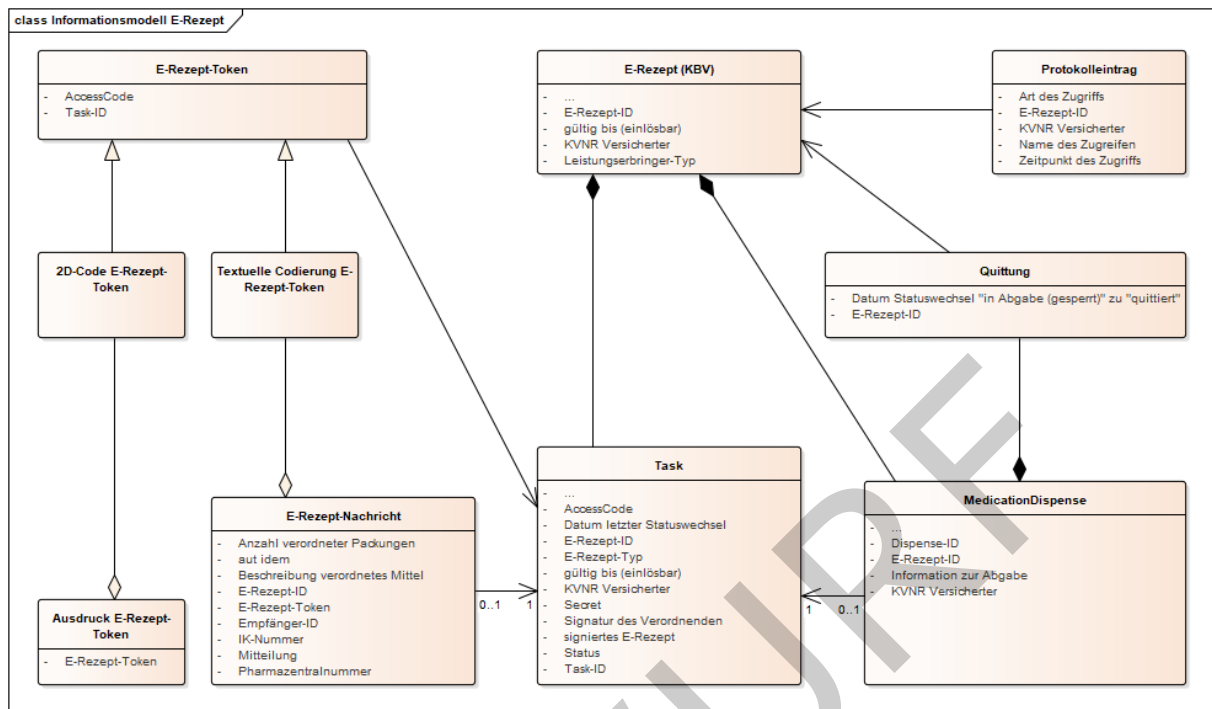
2170 Der E-Rezept-Token beinhaltet die Task-ID als Referenz für den zum E-Rezept
2171 zugehörigen Task im E-Rezept-Fachdienst und den AccessCode.

2172 Der E-Rezept-Token besitzt für die optische Übermittlung eine Darstellung als 2D-Code
2173 und für die elektronische Übermittlung und Verarbeitung eine textuelle Codierung. Auf
2174 dem Ausdruck eines E-Rezept-Tokens wird der 2D-Code sowie weitere Metadaten
2175 abgebildet.

2176 Die beim Statuswechsel von "in Abgabe (gesperrt)" zu "quittiert" erstellte Quittung
2177 beinhaltet das Datum des Statuswechsels und die Rezept-ID. Mittels Rezept-ID kann eine
2178 Quittung dem E-Rezept im Abrechnungsprozess zugeordnet werden.

2179 Die E-Rezept-Nachricht beinhaltet eine Text-Mitteilung und alternativ den E-Rezept-
2180 Token oder Informationen für eine Verfügbarkeitsanfrage.

2181



2182

2183

Abbildung 8: ABB_SYSLERP_008 Informationsmodell E-Rezept

2184 6.2 Fachliches Informationsmodell

2185 Die fachlichen Inhalte des Informationsmodells für die Fachanwendung E-Rezept, d.h.
 2186 den Daten, die durch den Verordnenden bereitgestellt werden, werden durch die
 2187 Bundesmantelvertragspartner im Benehmen mit dem Deutschen Apothekerverband
 2188 (DAV) festgelegt.

2189 Die fachlichen Inhalte des Informationsmodells zu den Dispensier- und
 2190 Abrechnungsdaten werden über den Rahmenvertrag § 129 Abs. 2 SGB V sowie über die
 2191 Vereinbarung nach § 300 Abs. 3 SGB V festgelegt.

2192 Diese fachlichen Inhalte sind nicht Teil des Scopes dieses Konzeptes.

2193

7 Anhang – Verzeichnisse

2194

7.1 Abkürzungen

Kürzel	Erläuterung
AMTS	Arzneimitteltherapiesicherheit
ApoBetrO	Verordnung über den Betrieb von Apotheken
AVS	Apothekenverwaltungssystem
BMP	bundeseinheitliche Medikationsplan
BtM	Betäubungsmittel
DAV	Deutschen Apothekerverband
DVO	Dienstleister vor Ort
eIDAS	<u>e</u> lectronic <u>I</u> dentification, <u>A</u> uthentication and trust <u>S</u> ervices
eMP	elektronischer Medikationsplan
ePA	elektronische Patientenakte
eRp	E-Rezept
FdV	Frontend des Versicherten
GUI	Graphical User Interface, Grafisches Benutzerinterface
HBA	Heilberufsausweis
IdP	Identity Provider
KIS	Krankenhausinformationssystem
KOM-LE	Kommunikation Leistungserbringer
KVNR	Krankenversichertennummer
LE	Leistungserbringer

LEI	Leistungserbringerinstitution
MVZ	Medizinisches Versorgungszentrum
NFC	Near Field Communication
OPB	Online-Produktivbetrieb
PS	Primärsystem, Oberbegriff für AVS, KIS und PVS
PVS	Praxisverwaltungssystem, ärztliches bzw. zahnärztliches
PZN	Pharmazentralnummer
QES	Qualifizierte elektronische Signatur
SGB	Sozialgesetzbuch
SM-B	Security Modul Typ B
SMC-B	Security Modul Card Typ B
TI	Telematikinfrastruktur
TIP	TI-Plattform, Plattform der Telematikinfrastruktur
URI	Uniform Resource Identifier
VAU	Vertrauenswürdige Ausführungsumgebung
VPN	Virtual Private Network

2195 7.2 Glossar

Begriff	Erläuterung
AccessCode	Ist ein für ein E-Rezept durch den E-Rezept-Fachdienst festgelegter Wert mit hoher Entropie. Ein Akteur (außer dem Versicherten, für den das E-Rezept ausgestellt wurde), welcher auf das E-Rezept zugreifen möchte, muss diesen AccessCode kennen. Der AccessCode wird im E-Rezept-Token übermittelt.
E-Rezept	Mit dem Aufbringen der QES auf einen Verordnungsdatensatz entsteht ein E-Rezept.
E-Rezept-Datensatz	Mit dem Einstellen des E-Rezepts in den E-Rezept-Fachdienst entsteht ein E-Rezept-Datensatz. Der E-Rezept-Datensatz

	enthält zusätzliche Informationen zur technischen Verarbeitung und Verwaltung des E-Rezepts.
E-Rezept-Token	Der E-Rezept-Token beinhaltet Informationen, wie auf den E-Rezept-Datensatz werden kann sowie weitere Metadaten, welche einem Versicherten ermöglichen soll, das E-Rezept zu verwalten. Der Besitz des E-Rezept-Tokens autorisiert den Zugriff auf das E-Rezept. Der E-Rezept-Token wird durch den Versicherten nach dem Abruf des E-Rezepts im FdV oder durch die verordnende LEI erstellt.
Identitätsbestätigung	Die Identifikationsbestätigung (AuthN-Token) wird durch den Identity Provider erstellt. Der Nutzer muss sich dafür gegenüber dem Identity Provider authentifizieren. Der Nutzer nutzt die Identifikationsbestätigung, um Zugang zu Diensten der TI zu erhalten.
Verordnungsdatensatz	Der Verordnungsdatensatz wird im Primärsystem der verordnenden Leistungserbringerinstitution erstellt. Er beinhaltet genau eine Verordnung, welche gemäß dem fachlichen Informationsmodell beschrieben ist.
Versicherten-ID	Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen Krankenversicherungsnummer (KVNR).

2196 Allgemeine Begriffe finden sich in [gemGlossar].

2197 7.3 Abbildungsverzeichnis

2198	Abbildung 1: ABB_SYSLERP_001 Übersicht der Fachanwendung E-Rezept	8
2199	Abbildung 2: ABB_SYSLERP_002 Fachliches Rollenmodell	11
2200	Abbildung 3: ABB_SYSLERP_003 Funktionale Zerlegung E-Rezept	15
2201	Abbildung 4 ABB_SYSLERP_009 Übersicht Identity Provider im Kontext E-Rezept	17
2202	Abbildung 5: ABB_SYSLERP_004 Statusübergänge E-Rezept	20
2203	Abbildung 6: ABB_SYSLERP_005 Anwendungsfälle E-Rezept	26
2204	Abbildung 7: ABB_SYSLERP_006 Systemzerlegung E-Rezept	55
2205	Abbildung 8: ABB_SYSLERP_008 Informationsmodell E-Rezept	95
2206		

2207 7.4 Tabellenverzeichnis

2208	Tabelle 1 : TAB_SYSLERP_048 Fachliche Rollen	11
------	--	----

2209	Tabelle 2: TAB_SYSLERP_001 Kryptografische Identitäten der Akteure und ihre jeweilige	
2210	Rolle	14
2211	Tabelle 3 : TAB_SYSLERP_006 Beschreibung Status Task	21
2212	Tabelle 4: TAB_SYSLERP_005 Anwendungsfall E-Rezepte erzeugen	27
2213	Tabelle 5: TAB_SYSLERP_006 Anwendungsfall E-Rezept einstellen	29
2214	Tabelle 6: TAB_SYSLERP_008 Anwendungsfall E-Rezept durch Verordnenden löschen...31	
2215	Tabelle 7: TAB_SYSLERP_009 Anwendungsfall E-Rezepte durch Versicherten abrufen ...32	
2216	Tabelle 8: TAB_SYSLERP_041 Anwendungsfall E-Rezept durch Vertreter abrufen.....33	
2217	Tabelle 9: TAB_SYSLERP_010 Anwendungsfall E-Rezept durch Versicherten löschen34	
2218	Tabelle 10: TAB_SYSLERP_011 Anwendungsfall Nachricht durch Versicherten übermitteln	
2219	35
2220	Tabelle 11: TAB_SYSLERP_037 Anwendungsfall Nachrichten durch Versicherten	
2221	empfangen	38
2222	Tabelle 12: TAB_SYSLERP_013 Anwendungsfall Protokolldaten abrufen.....38	
2223	Tabelle 13: TAB_SYSLERP_036 Anwendungsfall Nachrichten durch Abgebenden	
2224	empfangen	39
2225	Tabelle 14: TAB_SYSLERP_055 Anwendungsfall Nachricht durch Abgebenden übermitteln	
2226	40
2227	Tabelle 15: TAB_SYSLERP_014 Anwendungsfall E-Rezept durch Abgebenden abrufen ...42	
2228	Tabelle 16: TAB_SYSLERP_015 Anwendungsfall E-Rezept durch Abgebenden zurückgeben	
2229	43
2230	Tabelle 17: TAB_SYSLERP_016 Anwendungsfall E-Rezept durch Abgebenden löschen ...45	
2231	Tabelle 18: TAB_SYSLERP_017 Anwendungsfall Quittung abrufen.....46	
2232	Tabelle 19: TAB_SYSLERP_057 Anwendungsfall Quittung erneut abrufen	48
2233	Tabelle 20: TAB_SYSLERP_018 Anwendungsfall Dispensierdatensatz durch Abgebenden	
2234	signieren	49
2235	Tabelle 21: TAB_SYSLERP_045 AuthN-Token durch Versicherten anfordern	50
2236	Tabelle 22 TAB_SYSLERP_046 AuthN-Token durch LEI anfordern	53
2237	Tabelle 23: TAB_SYSLERP_019 Schnittstellen E-Rezept-Fachdienst.....56	
2238	Tabelle 24: TAB_SYSLERP_021 Bedingungen zum Löschen von E-Rezepten	58
2239	Tabelle 25: TAB_SYSLERP_040 Zugangsberechtigungen Operationen E-Rezept-Fachdienst	
2240	59
2241	Tabelle 26: TAB_SYSLERP_002 Maximales Aufkommen nach Rezeptzeilen (Muster 16)	
2242	2018 an ausgewählten Wochentagen	61
2243	Tabelle 27: TAB_SYSLERP_003 Gesamtes Aufkommen nach Rezeptzeilen (Muster 16)	
2244	2018 kumuliert nach Wochentagen.....	61
2245	Tabelle 28: TAB_SYSLERP_022 Nutzung Schnittstellen eRp-FdV	63
2246	Tabelle 29: TAB_SYSLERP_023 Nutzung Schnittstellen PS verordnende LEI	65
2247	Tabelle 30: TAB_SYSLERP_024 Nutzung Schnittstellen PS abgebende LEI.....	67
2248	Tabelle 31: TAB_SYSLERP_025 Operation E-Rezept-ID abrufen.....	72

2249	Tabelle 32: TAB_SYSLERP_026 Operation E-Rezept einstellen	73
2250	Tabelle 33: TAB_SYSLERP_027 Operation E-Rezept durch Verordnenden löschen	74
2251	Tabelle 34: TAB_SYSLERP_028 Operation E-Rezept durch Abgebenden abrufen	74
2252	Tabelle 35: TAB_SYSLERP_029 Operation E-Rezept durch Abgebenden löschen	75
2253	Tabelle 36: TAB_SYSLERP_030 Operation E-Rezept durch Abgebenden zurückgeben	76
2254	Tabelle 37: TAB_SYSLERP_031 Operation Quittung abrufen	76
2255	Tabelle 38: TAB_SYSLERP_031 Operation Quittung erneut abrufen	77
2256	Tabelle 39: TAB_SYSLERP_043 Operation E-Rezepte durch Versicherten abrufen	78
2257	Tabelle 40: TAB_SYSLERP_032 Operation E-Rezept durch Vertreter abrufen	78
2258	Tabelle 41: TAB_SYSLERP_033 Operation E-Rezept durch Versicherten löschen	79
2259	Tabelle 42: TAB_SYSLERP_054 Operation Dispensierinformationen durch Versicherten	
2260	abrufen	79
2261	Tabelle 43: TAB_SYSLERP_058 Operation Dispensierinformation für ein einzelnes E-	
2262	Rezept durch Versicherten oder Vertreter abrufen	80
2263	Tabelle 44: TAB_SYSLERP_044 Operation E-Rezept-Nachricht einstellen	81
2264	Tabelle 45: TAB_SYSLERP_050 Operation E-Rezept-Nachrichten abrufen.....	81
2265	Tabelle 46: TAB_SYSLERP_051 Operation Zugriffsprotokolleinträge durch Versicherten	
2266	abrufen	82
2267	Tabelle 47: TAB_SYSLERP_052 Schutzbedarf der maßgeblichen Informationsobjekte....	84
2268	Tabelle 48: TAB_SYSLERP_053 Schutzbedarf der maßgeblichen Prozesse	85
2269		

2270 7.5 Referenzierte Dokumente

2271 7.5.1 Dokumente der gematik

2272 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 2273 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der
 2274 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
 2275 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und
 2276 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
 2277 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer entnehmen Sie
 2278 bitte der aktuellen, auf der Internetseite der gematik veröffentlichten
 2279 Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemGlossar]	gematik: Glossar
[gemKPT_Arch_TIP]	gematik: Architekturkonzept der TI-Plattform
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI

[gemRL_NvTIwA]	gematik: Richtlinie Nutzungsvoraussetzungen der TI für weitere Anwendungen des Gesundheitswesens sowie für die Gesundheitsforschung
[gemSpec_DS_Anbieter]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter
[gemSpec_DS_Hersteller]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller
[OPB3]	Online-Produktivbetrieb https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/

2280 7.5.2 Weitere Dokumente

2281

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
DSGVO	Datenschutz-Grundverordnung
[FHIR]	FHIR - Resource MedicationRequest https://www.hl7.org/fhir/medicationrequest.html
[FHIR-Sig]	FHIR - Signature (JSON Signature rules for FHIR Resources) https://www.hl7.org/fhir/datatypes.html#Signature
[FHIR_MED_WORKFLOW]	FHIR - Workflow Module (siehe Common Use Cases für Workflow-Beschreibung) https://www.hl7.org/fhir/workflow-module.html https://www.hl7.org/fhir/task.html#statemachine (generischer Workflow)
[OAUTH2]	Internet Engineering Task Force (October 2012): RFC 6749 - The OAuth 2.0 Authorization Framework
[OIDC]	OpenID Foundation: OpenID Connect Core 1.0 incorporating errata set 1
[OWASP-CSC]	OWASP Cheat Sheet Series https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series
SGB V	Sozialgesetzbuch Fünftes Buch Gesetzliche Krankenversicherung

2282

2283