

Elektronische Gesundheitskarte und Telematikinfrastruktur

Systemspezifisches Konzept E-Rezept

Version:	1.1.0
Revision:	294962
Stand:	12.11.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSysL_eRp

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.06.2020		freigegeben	gematik
1.0.1	06.07.2020		Aktualisierung Hinweis zu Dispensierinformation	gematik
1.1.0	12.11.2020		Einarbeitung gemäß Änderungsliste P22.2 / Scope-Themen Systemdesign R4.0.1	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments	6
1.1 Zielsetzung	6
1.2 Zielgruppe	6
1.3 Geltungsbereich	6
1.4 Abgrenzung des Dokuments	6
1.5 Methodik	7
1.5.1 Anforderungen	7
1.5.2 Hinweis auf offene Punkte	7
2 Systemüberblick	8
2.1 Einführung	8
2.2 Übergeordnete Ziele	9
2.2.1 Sicherheit und Datenschutz	9
2.2.2 Datenhoheit und Flexibilität	9
2.2.3 Erweiterbarkeit	10
2.2.4 Betrieb	10
2.3 Akteure und Rollen	10
2.3.1 Fachliche Rollen	10
2.3.2 Technische Rollen	14
2.4 Funktionale Zerlegung	14
2.4.1 Konzept Identifikation und Zugang zum E-Rezept	16
2.4.2 Konzept Zugriffsberechtigung auf E-Rezepte	17
2.4.3 Konzept der E-Rezept-Ressourcenverwaltung	18
2.4.4 Konzept der Verschlüsselung des E-Rezepts	19
2.4.5 Konzept der Übermittlung eines E-Rezept-Tokens	19
2.4.6 Konzept Status E-Rezept	20
2.4.7 Unterstützung betrieblicher Prozesse	23
3 Anwendungsfälle	26
3.1 Übersicht der Anwendungsfälle	26
3.2 Übergreifende Vorbedingungen	27
3.3 Übergreifende Nachbedingungen	27
3.4 E-Rezept ausstellen	27
3.4.1 E-Rezepte durch Verordnenden erzeugen	27
3.4.2 E-Rezept einstellen	29
3.4.3 E-Rezept-Token durch Verordnenden an Versicherten oder Apotheker übermitteln	30
3.4.4 E-Rezept durch Verordnenden löschen	31
3.5 E-Rezept durch Versicherten verwalten	32
3.5.1 E-Rezepte durch Versicherten abrufen	32
3.5.2 E-Rezept durch Vertreter abrufen	33
3.5.3 E-Rezept durch Versicherten löschen	34

3.5.4 Nachricht durch Versicherten an Abgebenden oder einen Vertreter übermitteln	35
3.5.5 E-Rezept-Token durch Versicherten an Vertreter übermitteln	37
3.5.6 Nachrichten durch Versicherten empfangen	37
3.5.7 Nachricht durch Versicherten löschen	38
3.5.8 Protokolldaten durch Versicherten einsehen	40
3.6 E-Rezept in Apotheke einlösen	40
3.6.1 Nachrichten durch Abgebenden empfangen	40
3.6.2 Nachricht durch Abgebenden an Versicherten übermitteln	42
3.6.3 Nachricht durch Abgebenden löschen	43
3.6.4 E-Rezept durch Abgebenden abrufen	44
3.6.5 E-Rezept durch Abgebenden zurückgeben	46
3.6.6 E-Rezept durch Abgebenden löschen	47
3.6.7 Quittung abrufen	49
3.6.8 Quittung erneut abrufen	50
3.6.9 Dispensierdatensatz durch Abgebenden signieren	52
3.7 Anfordern von Identitätsbestätigungen	53
3.7.1 Identitätsbestätigung durch den Versicherten anfordern	53
3.7.2 Identitätsbestätigung durch LEI anfordern	55
4 Systemzerlegung (Deployment)	58
4.1 Produkttypen der Fachanwendung E-Rezept	59
4.1.1 Produkttyp E-Rezept-Fachdienst	59
4.1.1.1 Vertrauenswürdige Ausführungsumgebung	63
4.1.1.2 Betriebliche Aspekte	64
4.1.2 Produkttyp E-Rezept-Frontend des Versicherten	66
4.1.3 Primärsysteme	68
4.1.3.1 Primärsystem verordnender Leistungserbringer	69
4.1.3.2 Primärsystem abgebender Leistungserbringer	70
4.2 Fachanwendungsübergreifende Produkttypen	71
4.2.1 Produkttyp Identity Provider	71
4.2.1.1 Funktionale Anforderungen	72
4.2.1.2 Betriebliche Aspekte	73
4.2.2 Authentisierungsmodul	74
4.2.3 Produkttyp Verzeichnisdienst der TI	75
4.3 Schnittstelle der Fachanwendung E-Rezept	76
4.3.1 Schnittstelle für die Ressource E-Rezept	76
4.3.2 Schnittstelle für die Ressource E-Rezept-Nachricht	84
4.3.3 Schnittstelle für die Ressource Zugriffsprotokolleintrag	85
4.3.4 Schnittstelle für die Ressource signierte Challenge	86
4.3.5 Schnittstelle für die Ressource Einwilligung	87
5 Datenschutz- und Sicherheitsaspekte	88
5.1 Anforderungen an den E-Rezept-Fachdienst	89
5.1.1 Anforderungen an die Vertrauenswürdige Ausführungsumgebung	90
5.1.2 Verarbeitungskontext	91
5.1.3 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	92
5.1.4 Trennung von Session- und Request-Kontexten	94
5.2 Anforderungen an das E-Rezept-Frontend des Versicherten	95
5.3 Anforderungen an den Identity Provider	95

5.4 Grenzen der Sicherheitsleistung der Fachanwendung E-Rezept	96
6 Informationsmodell	98
6.1 Technisches Informationsmodell	98
6.2 Fachliches Informationsmodell.....	99
7 Anhang – Verzeichnisse	100
7.1 Abkürzungen	100
7.2 Glossar	101
7.3 Abbildungsverzeichnis.....	102
7.4 Tabellenverzeichnis	103
7.5 Referenzierte Dokumente	105
7.5.1 Dokumente der gematik.....	105
7.5.2 Weitere Dokumente.....	105

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

1.5 Methodik

1.5.1 Anforderungen

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

1.5.2 Hinweis auf offene Punkte

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

Beispiel für einen offenen Punkt.

2 Systemüberblick

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.

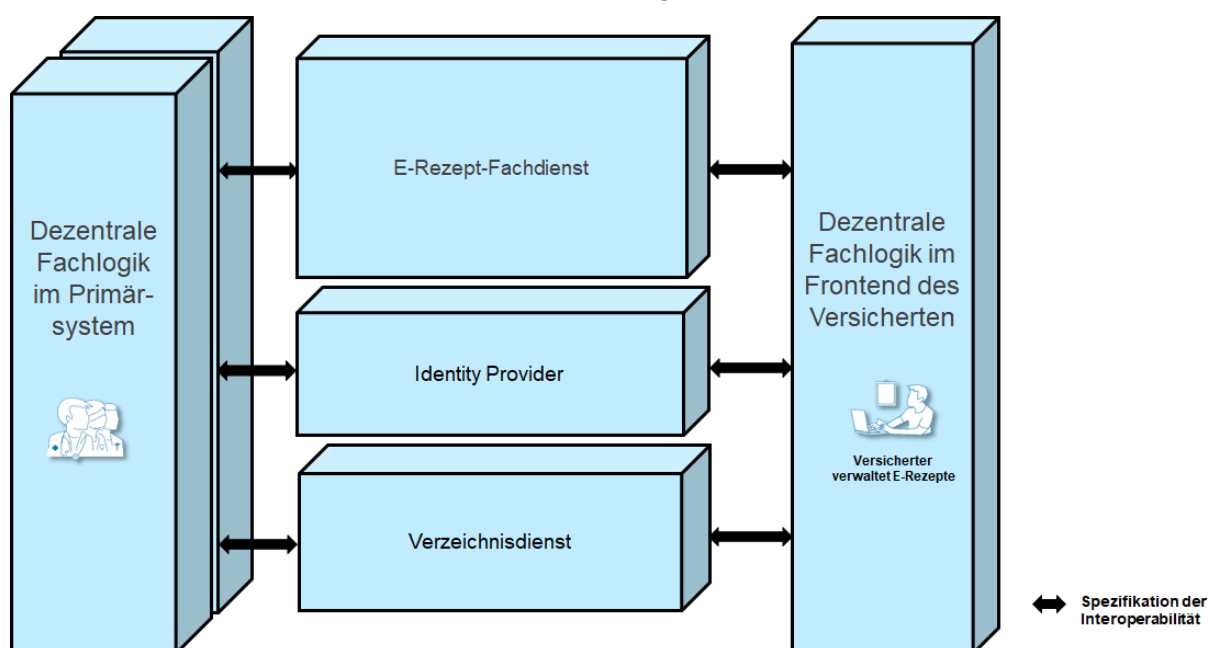


Abbildung 1: ABB_SYSLERP_001 Übersicht der Fachanwendung E-Rezept

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 des Versicherten auf seinem technischen Gerät verwaltet. Mit dem E-Rezept-Frontend des Versicherten 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 des Versicherten 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

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

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

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

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

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

Für den Zugang zur Telematikinfrastruktur nutzt der Versicherte seine eGK mit NFC-Schnittstelle, sodass eine Nutzung des E-Rezepts auch ohne weitere Hardware an den Geräten des Versicherten möglich ist.

2.2 Übergeordnete Ziele

2.2.1 Sicherheit und Datenschutz

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

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

2.2.2 Datenhoheit und Flexibilität

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

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

Versicherte müssen das E-Rezept auch ohne eigene technische Geräte und Softwarekomponenten einlösen können. Ein zusätzliches durch den Versicherten 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. Diese Erweiterungen erfolgen in Folgestufen.

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.

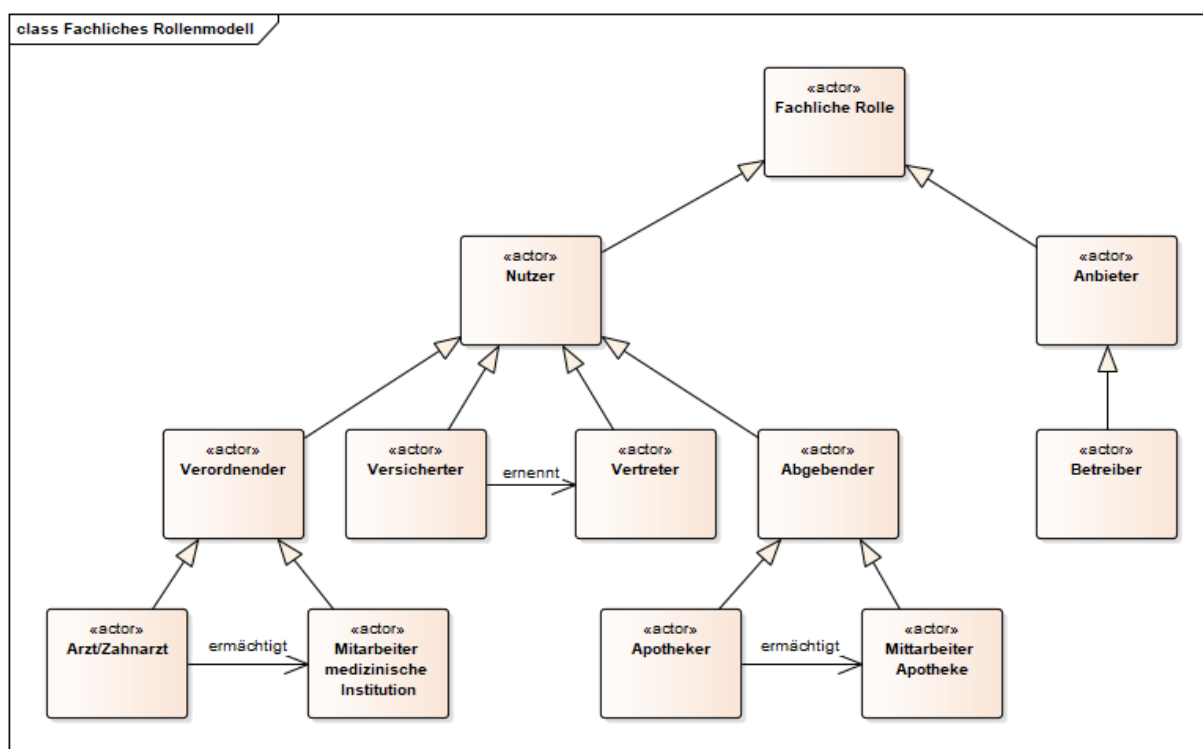


Abbildung 2: ABB_SYSLERP_002 Fachliches Rollenmodell

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 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 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 zu dokumentieren. In Abhängigkeit der arzneimittelrechtlichen Vorschriften und der Verträge nach § 129 SGB V erfolgt eine Signatur des Abgabedatensatzes und des Dispensierdatensatz fortgeschritten oder durch eine QES. • 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-/Filialapotheke), 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. • Ein „Mitarbeiter Apotheke (nicht abzeichnungsberechtigt)“ arbeitet in einer Apotheke (z.B. öffentliche Apotheke (Haupt-/Filialapotheke), 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.

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

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

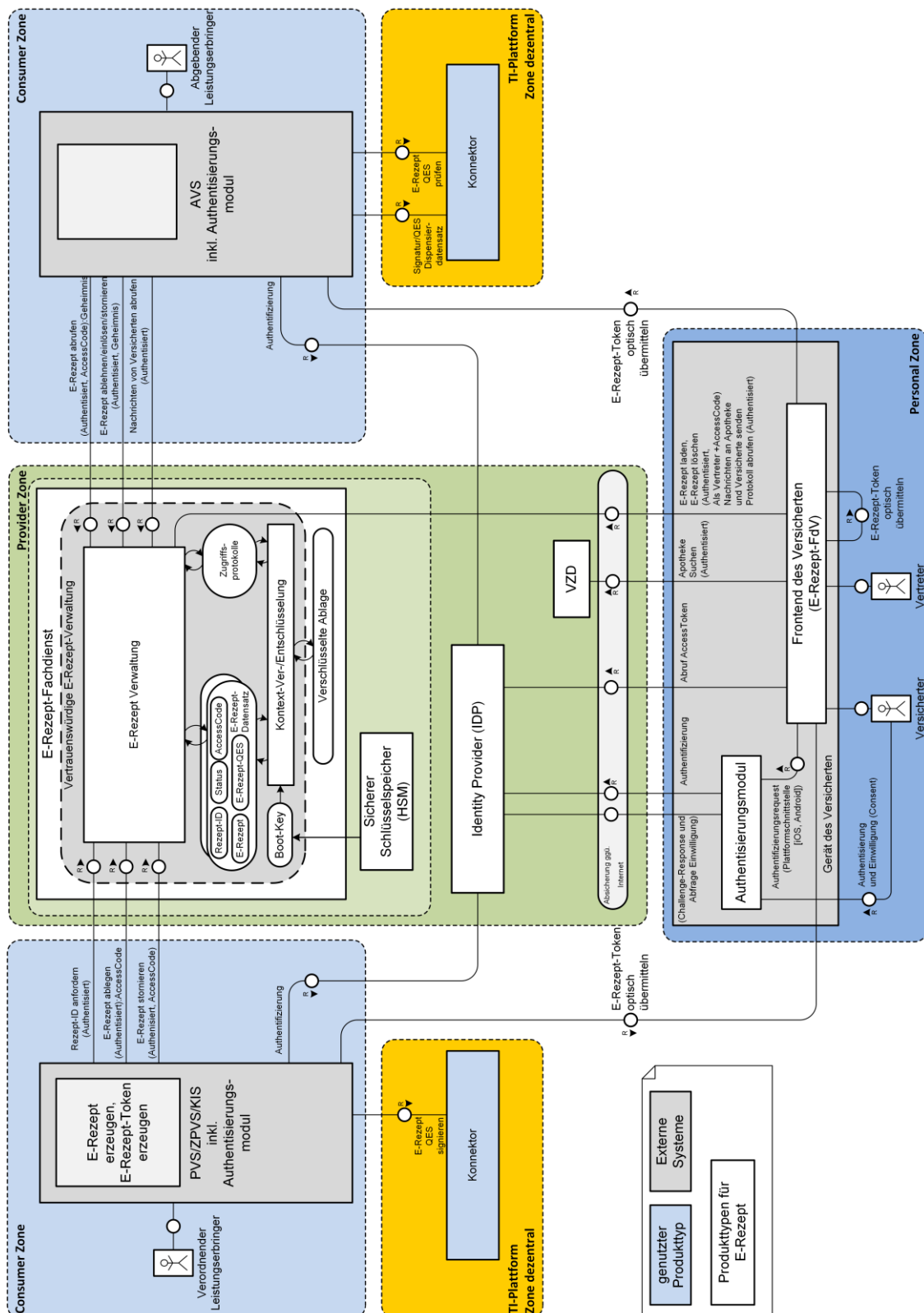
Komponente	Identität (gem. [gemKPT_Arch_TIP #Anhang B])	Rolle	Verwendungszweck	Prüfende Komponente
SMC-B	ID.HCI.AUT	Mitarbeiter LEI	Authentisierung der LEI	Identity Provider LE
	ID.HCI.OSIG		Fortgeschrittene Signatur der LEI für E-Rezept/Dispensierdatensatz	Konnektor, Komponenten außerhalb der TI
HBA	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.



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.

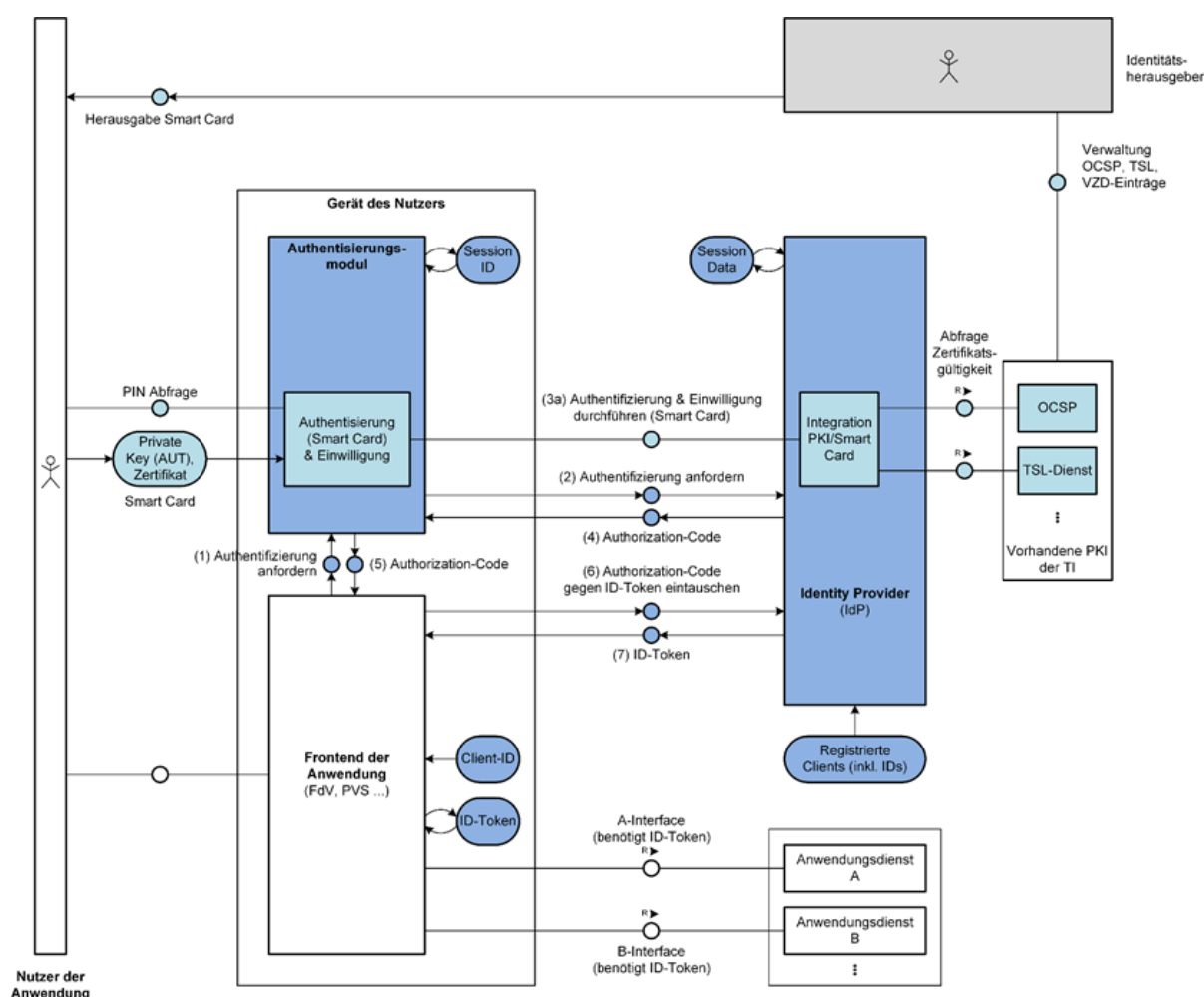


Abbildung 4: ABB_SYSLERP_009 Übersicht Identity Provider im Kontext E-Rezept

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 Zugriff 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 (Vor-Ort-Apotheke, Versandapotheke). 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-Rezepts 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 (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 der Arzneimittelverordnung ("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. Die konkrete Ausgestaltung der UserExperience mit der Definition entsprechender Schnittstellen und Ressourcen ergibt sich aus dem zu definierenden Zusammenspiel des E-Rezept-Fachdiensts für den Verordnungs-Prozess und der elektronischen Patientenakte für die Langzeitdokumentation medizinischer Daten.

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 schematisch 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 Krankenversicherungsnummer (KVNR)) 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 Leistungserbringerinstitution. E-Rezepte abrufen und die Abgabe vollziehen dürfen ausschließlich Apotheken, deren Rolle ebenfalls anhand der Identität der Apotheke als Leistungserbringerinstitution geprüft wird. Zusätzlich erfordert das Abrufen eines E-Rezepts durch eine Apotheke die Vorlage des vom Versicherten an den Apotheker übergebenen AccessCode, der beim Abruf des E-Rezepts mit dem am E-Rezept-Datensatz gespeicherten AccessCode übereinstimmen muss.

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

2.4.4 Konzept der Verschlüsselung des E-Rezepts

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

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

Anmerkung:

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

2.4.5 Konzept der Übermittlung eines E-Rezept-Tokens

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

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

Der 2D-Code kann in der einlösenden Apotheke vom Frontend abgescannt werden. Die Darstellung des Tokens als 2D-Code ist ein optisches Übertragungsverfahren.

Für den digitalen Versand des E-Rezept-Tokens an eine Apotheke und die weitere Kommunikation rund um den Einlösevorgang mit der Apotheke (Verfügbarkeit, Terminabsprache zum Abholen, ...) sowie die Weitergabe des E-Rezept-Tokens an einen Vertreter 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 bzw. der Vertreter rufen die an sie adressierte Nachricht vom E-Rezept-Fachdienst ab. Eine eventuelle Antwort der Apotheke wird vom AVS bzw. beim Vertreter durch das Frontend ebenfalls als strukturierte Nachricht in den E-Rezept-Fachdienst eingestellt.

Für Versorgungsprozesse in folgenden Ausbaustufen sind weitere Kommunikationsbeziehungen naheliegend:

- 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 KIM (ehemals KOM-LE), über welche dann auch die Kommunikationsbeziehungen Versicherter/Vertreter ==> Abgebender und Versicherter ==> Vertreter in einem einheitlichen Kommunikationsverfahren umgesetzt werden können.

2.4.6 Konzept Status E-Rezept

Ein E-Rezept durchläuft während seines Lebenszyklus verschiedene Status.

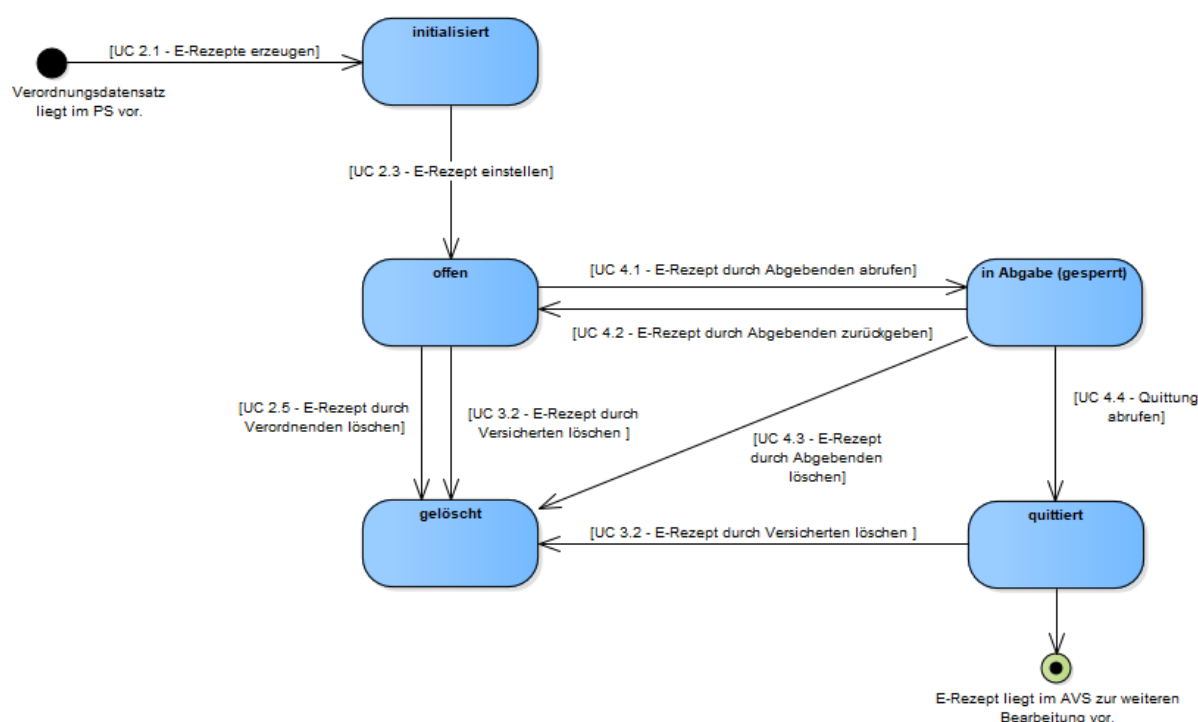


Abbildung 5: ABB_SYSLERP_004 Statusübergänge E-Rezept

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

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

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

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" (<i>ready</i>).
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" (<i>cancelled</i>). Der Abruf einer abgebenden LEI ändert den Status des Tasks auf "in Abgabe (gesperrt)" (<i>in-progress</i>). 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>).

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

2.4.7 Unterstützung betrieblicher Prozesse

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

A_18967 - Erhebung und Speicherung von Performance-Messdaten

Die an der Fachanwendung E-Rezept beteiligten Produkttypen E-Rezept-Fachdienst und Identity Provider 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.[<=]

A_18992 - Lieferung von Performance-Messdaten

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

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

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

A_18993 - Identity Provider - Erhebung von Performance-Messdaten

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

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

Die an den Anwendungsfällen der Fachanwendung E-Rezept beteiligten Produkttypen E-Rezept-Fachdienst, Identity Provider und deren Komponenten sowie die jeweiligen Frontend-Komponenten der Nutzer MÜSSEN zur Unterstützung des Endanwender-

Supports bei einer entstehenden Störung oder einem Abbruch, gleich aus welchem Grunde, eine eindeutige, aussagekräftige und interoperable Fehlermeldung bereitstellen, die es den Supporteinheiten ermöglichen, die Störungsursache und den oder die Lösungsverantwortlichen der Störung zu identifizieren und mögliche eigene Gegenmaßnahmen zu ergreifen. [<=]

A_18999 - Anzeige des E-Rezept-Betriebszustandes

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

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

A_18997 - Anbieter E-Rezept-Fachdienst - Supportverantwortung im TI-ITSM-Teilnehmersupport

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

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

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

A_18970 - Versichertensupport durch Anbieter Frontend des Versicherten

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

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

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

3 Anwendungsfälle

3.1 Übersicht der Anwendungsfälle

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

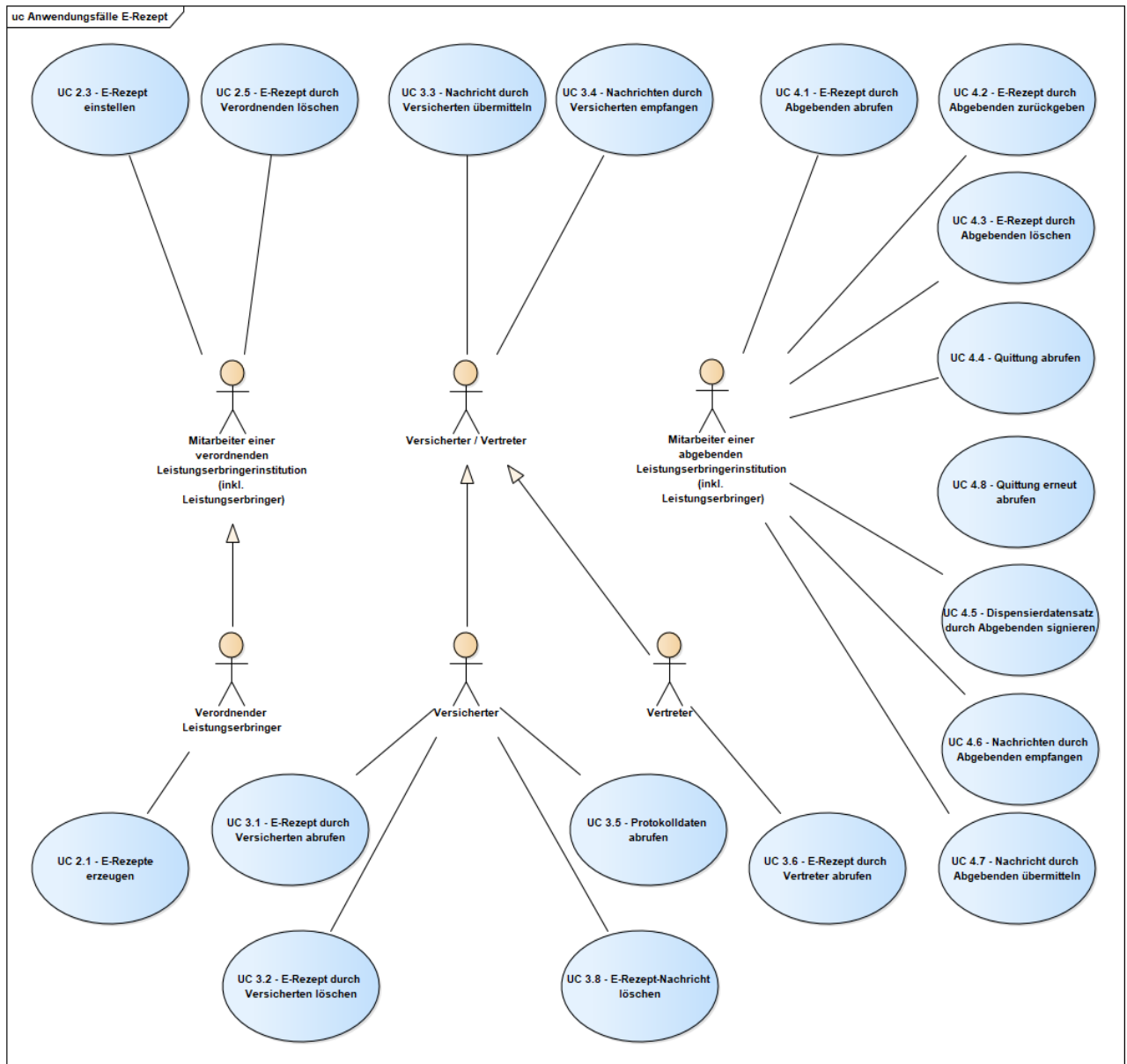


Abbildung 6: ABB_SYSLERP_005 Anwendungsfälle E-Rezept

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 zugriffenen 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

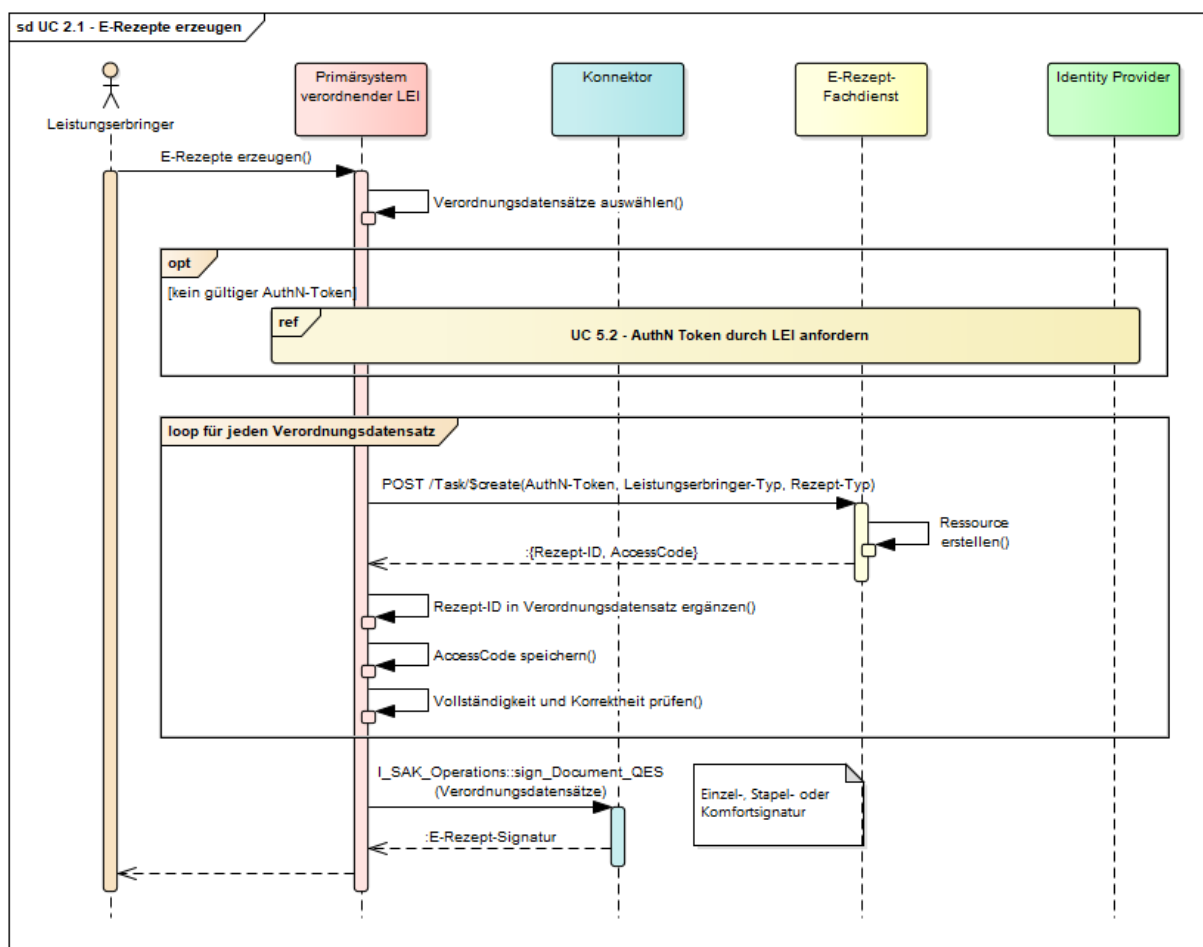
Mit diesem Anwendungsfall signiert ein verordnender Leistungserbringer ein oder mehrere Verordnungsdatensätze. Vor dem Signieren wird im Verordnungsdatensatz eine über die TI bezogene Rezept-ID ergänzt. Dieser Anwendungsfall kann, da er eine qualifizierte elektronische Signatur beinhaltet, nur durch 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)	<p>Der verordnende Leistungserbringer wählt im Primärsystem einen oder mehrere Verordnungsdatensätze zum Signieren aus. Der Leistungserbringer wählt das Signaturverfahren aus.</p> <p>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.</p>
Nachbedingung	<p>Die erzeugten E-Rezepte beinhalten eine eindeutige Rezept-ID und haben eine QES.</p> <p>Der AccessCode für jedes E-Rezept ist im Primärsystem gespeichert. Die E-Rezepte sind im E-Rezept-Fachdienst angelegt und haben den Status "initialisiert".</p>



[<=]

3.4.2 E-Rezept einstellen

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

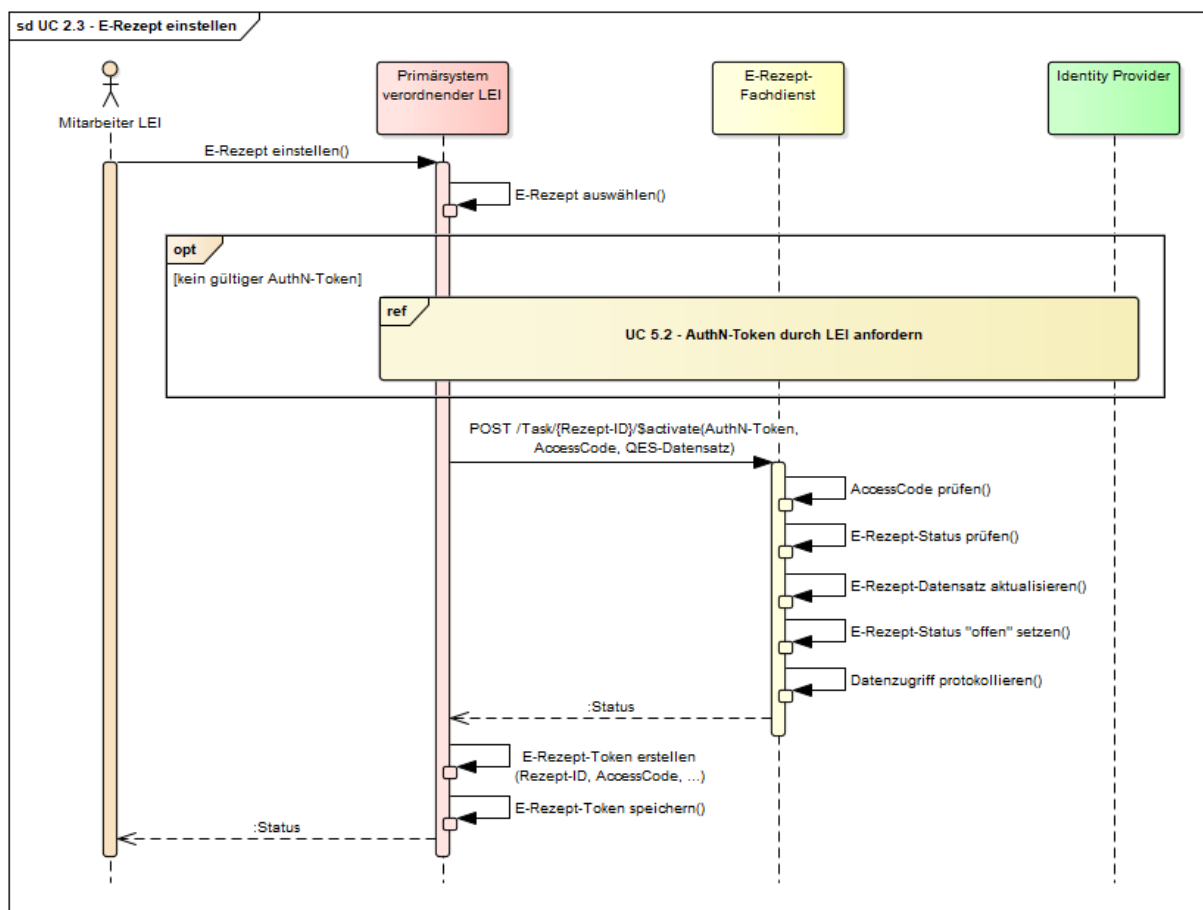
A_18503 - Anwendungsfall "E-Rezept einstellen"

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

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.

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



[<=]

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

Nachdem ein Mitarbeiter der verordnenden LEI den Anwendungsfall "UC 2.3 - E-Rezept einstellen" ausgeführt hat, kann der Versicherte sich das E-Rezept mit dem

Anwendungsfall "UC 3.1 - E-Rezepte durch Versicherten abrufen" auf sein FdV herunterladen und einen E-Rezept-Token erstellen.

Nur wenn der Versicherte kein FdV nutzt, wird der E-Rezept-Token im Primärsystem erzeugt und als 2D-Code ausgedruckt. Der Ausdruck wird dem Versicherten übergeben. Ergänzend zum Ausdruck können zusätzliche technische Möglichkeiten bestehen, den 2D-Code für den Versicherten zum Abfotografieren anzuzeigen. Die Inhalte und das Format des papierbasierten Token der Fachanwendung E-Rezept werden durch die Bundesmantelvertragspartner in Absprache mit dem Deutschen Apothekerverband (DAV) festgelegt.

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

3.4.4 E-Rezept durch Verordnenden löschen

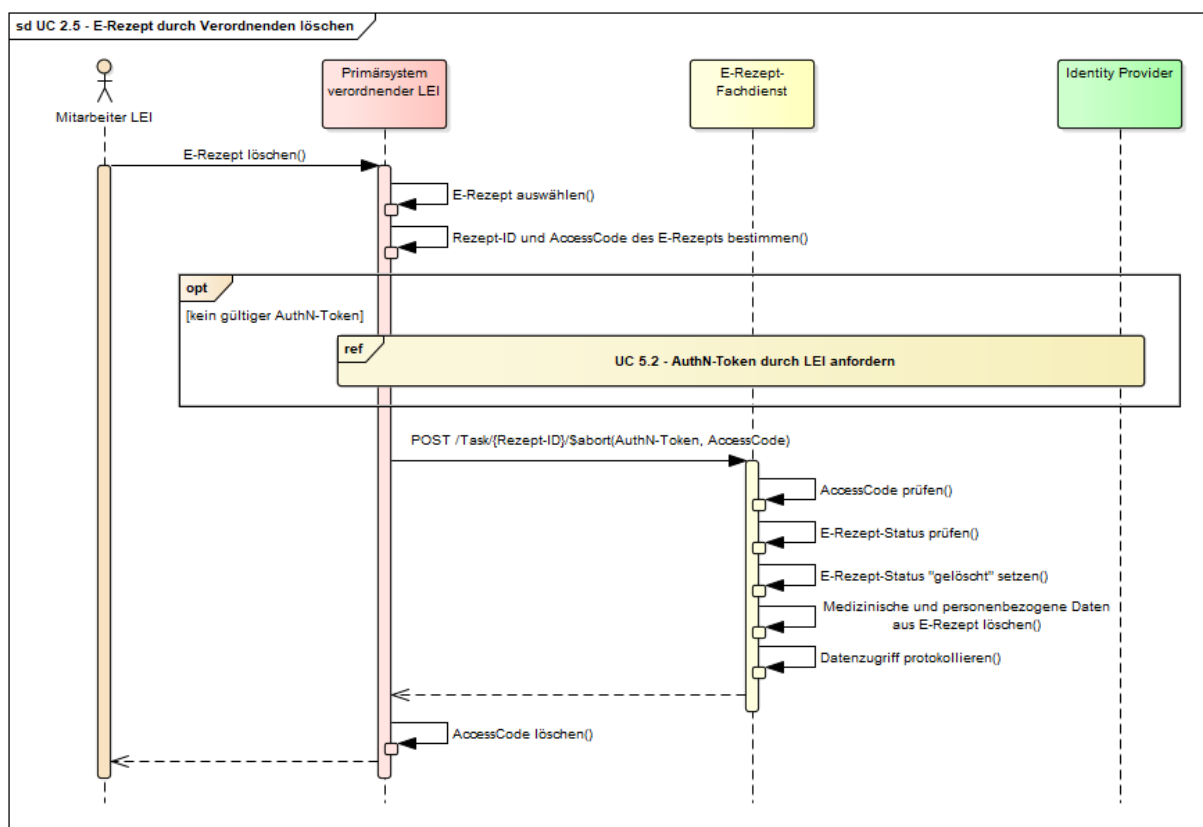
Mit diesem Anwendungsfall kann ein Mitarbeiter einer verordnenden Leistungserbringerinstitution, den Status für ein zuvor durch die LEI für den Versicherten eingestelltes E-Rezept auf "gelöscht" setzen. Die Nutzer können auf ein E-Rezept mit dem Status "gelöscht" nicht mehr zugreifen.

A_18505 - Anwendungsfall "E-Rezept durch Verordnenden löschen"

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

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>



[<=]

3.5 E-Rezept durch Versicherten verwalten

3.5.1 E-Rezepte durch Versicherten abrufen

Mit diesem Anwendungsfall kann ein Versicherter alle seine im E-Rezept-Fachdienst eingestellten E-Rezepte herunterladen, um Einsicht in die Daten dieser E-Rezepte zu nehmen. Die E-Rezepte werden ohne QES des verordnenden LE bereitgestellt, dafür erhält der dem Versicherten bereitgestellte Datensatz eine Serversignatur zum Nachweis der Integrität und Authentizität, dass die bereitgestellten Daten mit den Daten der QES-Signatur übereinstimmen.

Beim Abruf der E-Rezepte im E-Rezept-FdV übermittelt der E-Rezept-Fachdienst auch den AccessCode der E-Rezepte. Dies ermöglicht das Erstellen von E-Rezept-Token.

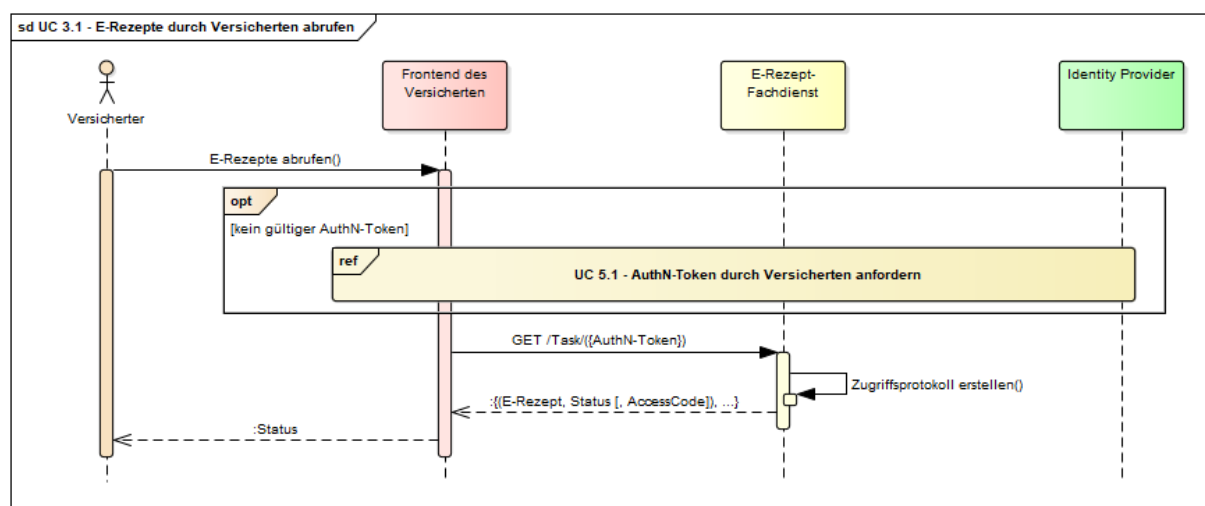
A_18506 - Anwendungsfall "E-Rezepte durch Versicherten abrufen"

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

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)	<p>Ein Versicherter ruft über ein FdV (E-Rezept-FdV) alle seine im E-Rezept-Fachdienst eingestellten Rezepte ab.</p> <p>Der E-Rezept-Fachdienst identifiziert die E-Rezepte auf Basis der Versicherten-ID des Versicherten und liefert die E-Rezepte, Status und die Zeitpunkte, an denen die Status gesetzt wurden. Die AccessCodes werden nur übermittelt, wenn der Abruf über ein E-Rezept-FdV erfolgt.</p>
Nachbedingung	<p>Im FdV stehen die E-Rezepte zur Anzeige sowie die Daten für das Erstellen eines E-Rezept-Tokens bereit.</p> <p>Der Abruf ist im E-Rezept-Fachdienst protokolliert.</p>



[<=]

3.5.2 E-Rezept durch Vertreter abrufen

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

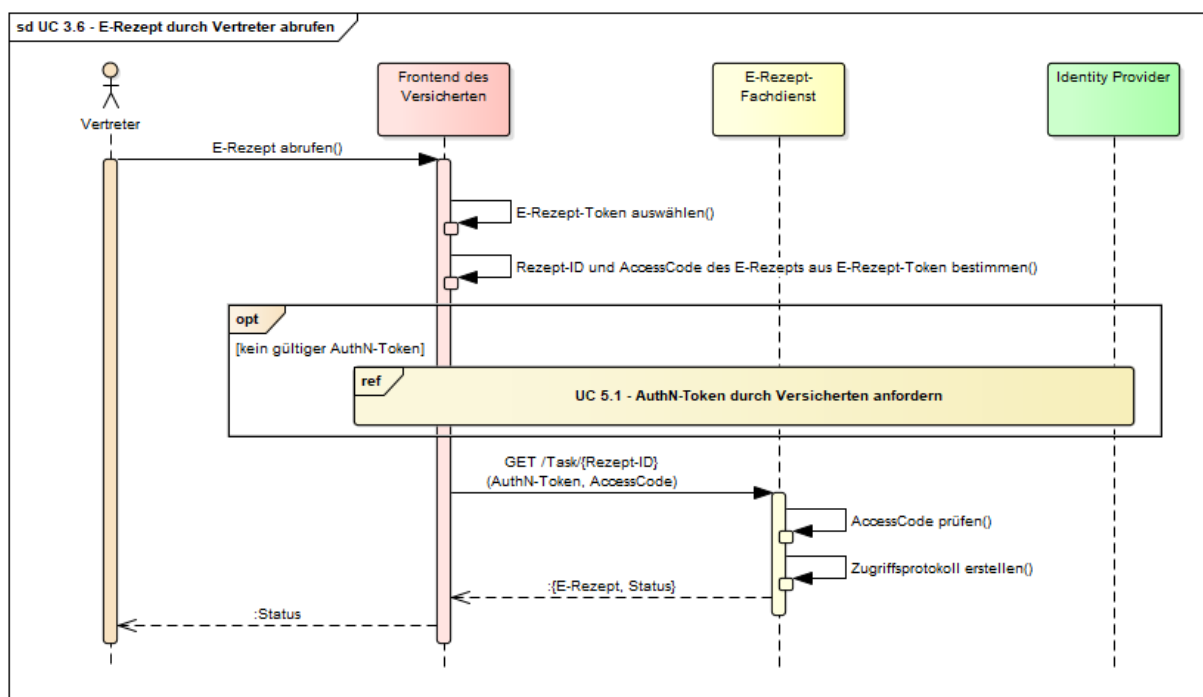
A_18781 - Anwendungsfall "E-Rezept durch Vertreter abrufen"

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

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 bereit. Der Abruf ist im E-Rezept-Fachdienst protokolliert.



[<=]

3.5.3 E-Rezept durch Versicherten löschen

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

Der Anwendungsfall kann nicht durch einen Vertreter ausgeführt werden.

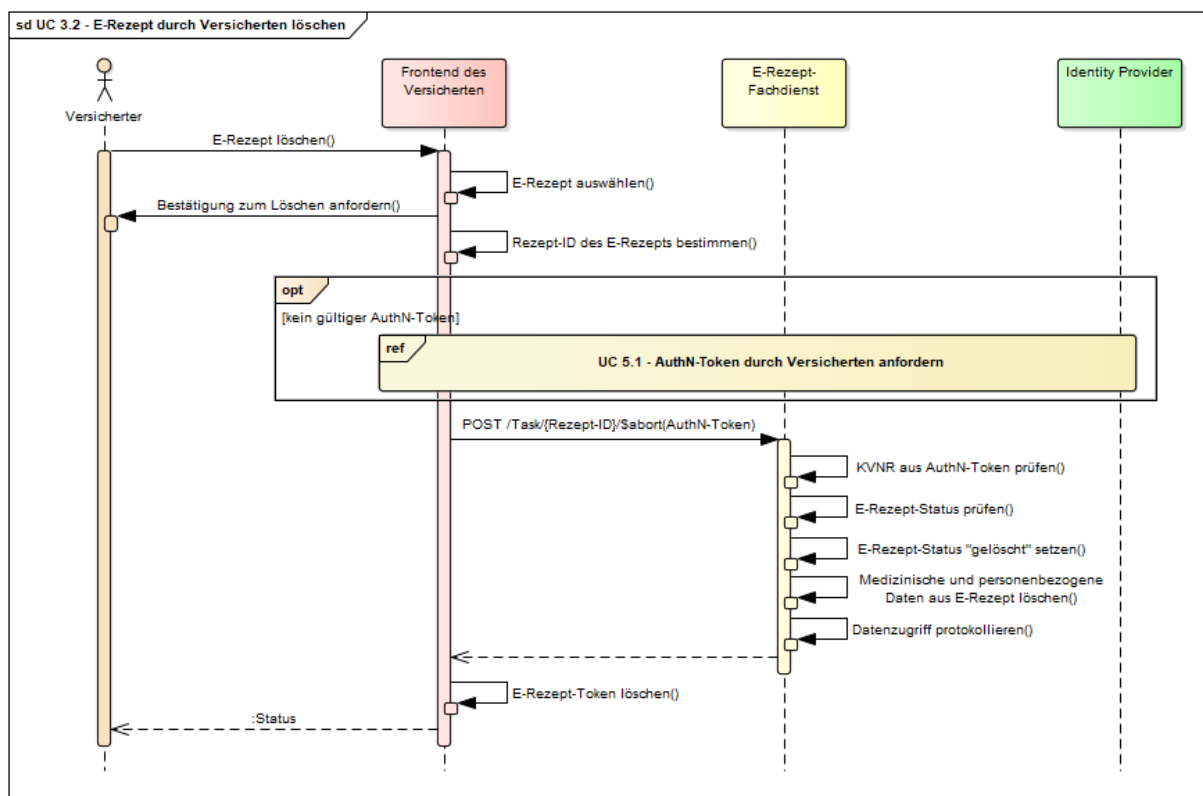
A_18507 - Anwendungsfall "E-Rezept durch Versicherten löschen"

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

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.

	<ul style="list-style-type: none"> Das E-Rezept hat einen Status ungleich "in Abgabe (gesperrt)"
Kurzbeschreibung (Außenansicht)	<p>Ein Versicherter wählt am FdV (E-Rezept-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 werden auf dem E-Rezept-Fachdienst gelöscht. Abschließend wird der E-Rezept-Token im E-Rezept-FdV gelöscht.</p>
Nachbedingung	<p>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.</p>



[<=]

3.5.4 Nachricht durch Versicherten an Abgebenden oder einen Vertreter übermitteln

Mit diesem Anwendungsfall kann ein Versicherter oder Vertreter einen E-Rezept-Token oder eine Mitteilung an eine Apotheke oder einen Vertreter seiner Wahl übermitteln, um das Rezept einzulösen oder eine Anfrage zur Belieferung des Rezepts durch die Apotheke

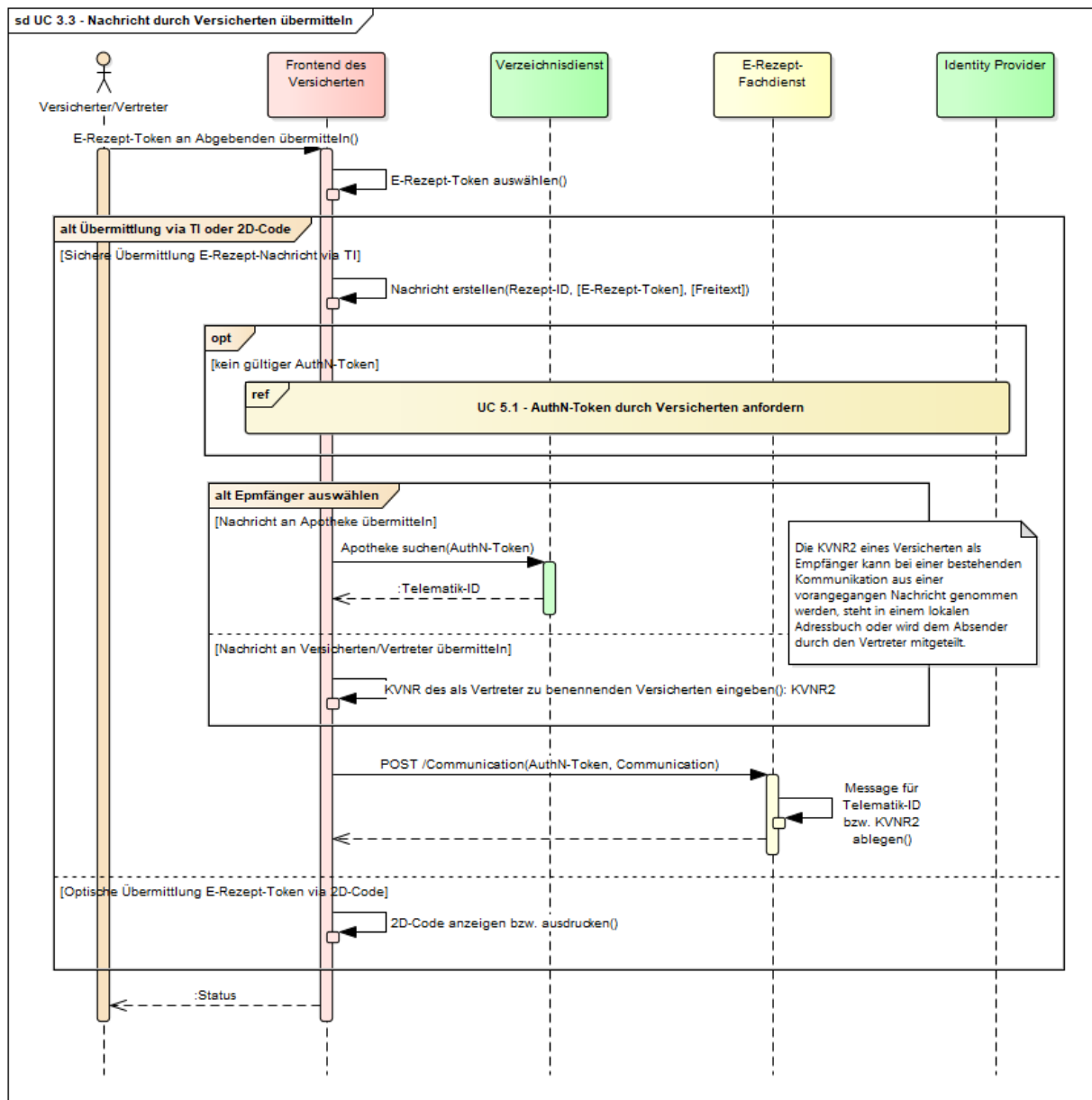
zu stellen. Als Alternative steht die optische Übermittlung des E-Rezept-Tokens als 2D-Code zur Verfügung.

A_18508 - Anwendungsfall "Nachricht durch Versicherten übermitteln"

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

Tabelle 10: TAB_SYSLERP_011 Anwendungsfall Nachricht durch Versicherten 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. Der sichere Versand über die TI erfolgt mithilfe des E-Rezept-Fachdienstes.</p> <p>Versand an Apotheke: Der Versicherte wählt im Verzeichnisdienst die Apotheke aus, an die die Nachricht übermittelt werden soll.</p> <p>Versand an einen Versicherten: Der Versicherte gibt die KVNR des Empfängers (KVNR2) in das FdV ein, diese hat ihm der Empfänger mitgeteilt oder ist dem FdV aus einer vorherigen Nachricht bekannt.</p> <p>Anschließend stellt das FdV die Nachricht im E-Rezept-Fachdienst für den Empfänger 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 oder Vertreter 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 vom Empfänger asynchron empfangen werden.</p> <p>Im Falle der Alternative kann der Empfänger den 2D-Code absキャンen.</p>



[<=]

3.5.5 E-Rezept-Token durch Versicherten an Vertreter übermitteln

Die Benennung eines Vertreters mit Mitteln der Telematikinfrastruktur erfolgt über den UseCase "UC 3.3 - Nachricht durch Versicherten übermitteln". Eine Übergabe des Tokens außerhalb der TI kann mittels Schnittstellen des E-Rezept-FdV erfolgen, welche in einer Rechtsverordnung zu § 360 Abs. 5 PDSG definiert werden.

3.5.6 Nachrichten durch Versicherten empfangen

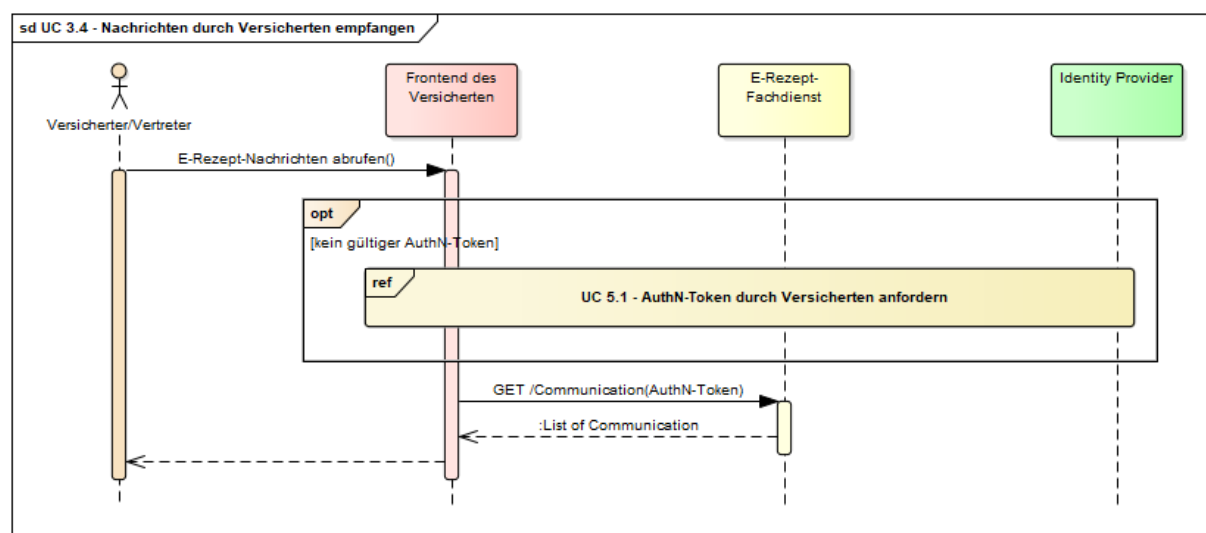
Mit diesem Anwendungsfall kann ein Versicherter oder Vertreter eine oder mehrere Nachrichten von abgebenden LEI zu E-Rezepten mittels der sicheren Übertragung über die TI empfangen.

A_18618 - Anwendungsfall "Nachrichten durch Versicherten empfangen"

Alle am Anwendungsfall "Nachrichten durch Versicherten empfangen" beteiligten 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. Ein Versicherter hat den Anwendungsfall "UC 3.3 - Nachricht durch Versicherten 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 Nachricht durch Versicherten löschen

Mit diesem Anwendungsfall kann der Versicherte von ihm übermittelte Nachrichten an Apotheken oder Versicherte löschen. Im Ergebnis der Löschanforderung wird dem Versicherten mitgeteilt, ob die Nachricht bereits vom Empfänger abgerufen wurde.

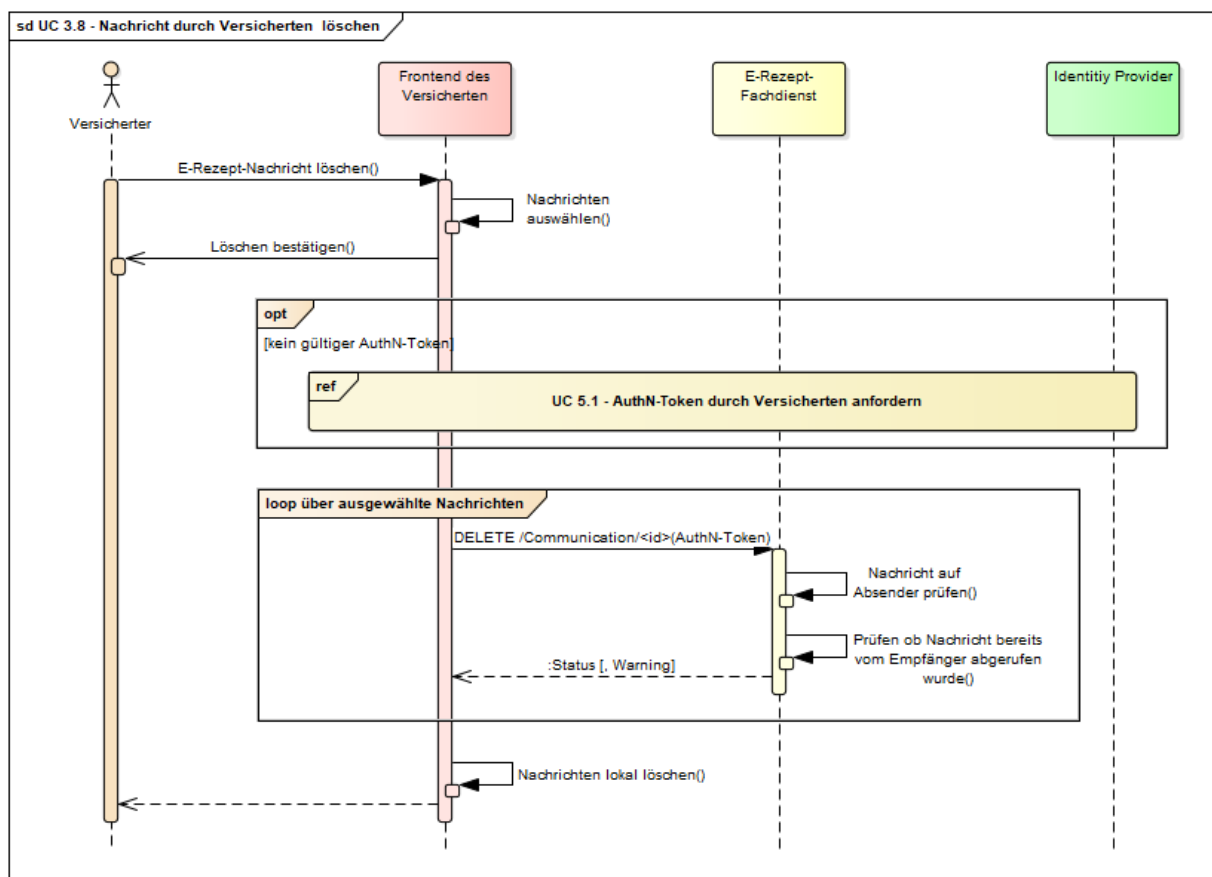
A_20260 - Anwendungsfall "Nachricht durch Versicherten löschen"

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

Tabelle 12: TAB_SYSLERP_061 Anwendungsfall Nachricht durch Versicherten löschen

Name	UC 3.8 - Nachricht durch Versicherten löschen
------	---

Vorbedingung	<ul style="list-style-type: none"> Ein Versicherter hat den Anwendungsfall "UC 3.3 - Nachricht durch Versicherten übermitteln" ausgeführt.
Kurzbeschreibung (Außenansicht)	<p>Der Versicherte wählt eine oder mehrere zuvor von ihm übermittelte Nachrichten zum Löschen aus.</p> <p>Der Versicherte bestätigt das Löschen.</p> <p>Das FdV überträgt für jede zu löschende Nachricht die Löschanforderung an den E-Rezept-Fachdienst.</p> <p>Die zu löschenden Nachrichten werden im E-Rezept-Fachdienst gelöscht.</p> <p>Der E-Rezept-Fachdienst übermittelt dem FdV eine Warning, wenn die Nachricht bereits durch den Empfänger abgerufen wurde.</p> <p>Abschließend werden die zu löschenden Nachrichten im FdV gelöscht.</p>
Nachbedingung	Die Nachrichten sind auf dem E-Rezept-Fachdienst und im FdV gelöscht.



[<=]

3.5.8 Protokolldaten durch Versicherten einsehen

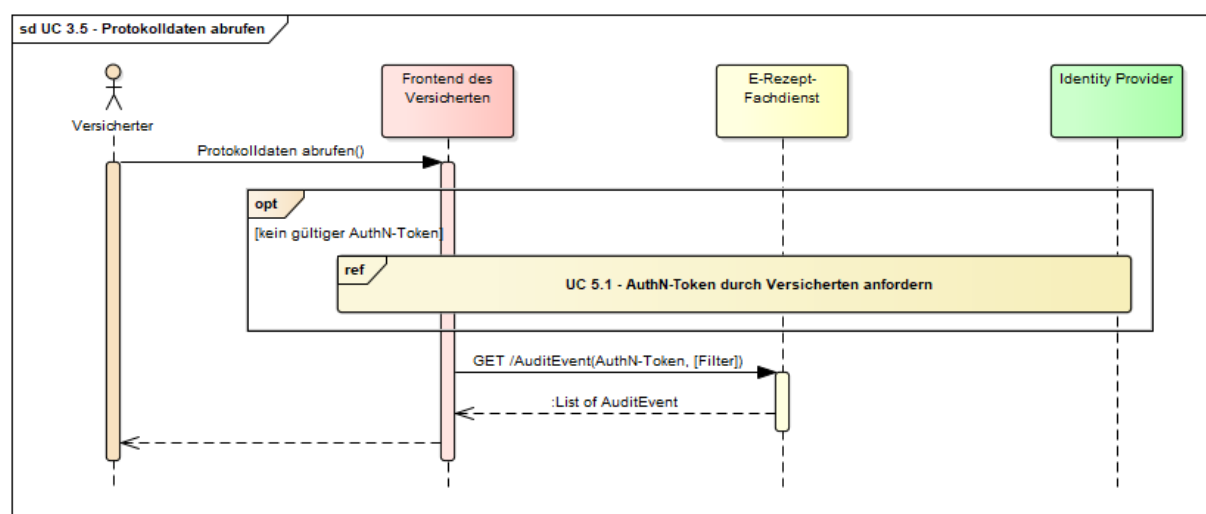
Mit diesem Anwendungsfall nimmt der Versicherte Einsicht in das Zugriffsprotokoll. Darin ersichtlich sind das Einstellen von E-Rezepten für den Versicherten, alle folgenden Statuswechsel zu diesen E-Rezepten sowie das Löschen von E-Rezepten.

A_18510 - Anwendungsfall "Protokolldaten abrufen"

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

Tabelle 13: 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 (E-Rezept-FdV) alle Protokolleinträge zur Anzeige ab. Für die Abfrage können Filterkriterien, wie bspw. ein Zeitraum angegeben werden.
Nachbedingung	Die Protokolleinträge stehen zur Anzeige bereit.



[<=]

3.6 E-Rezept in Apotheke einlösen

3.6.1 Nachrichten durch Abgebenden empfangen

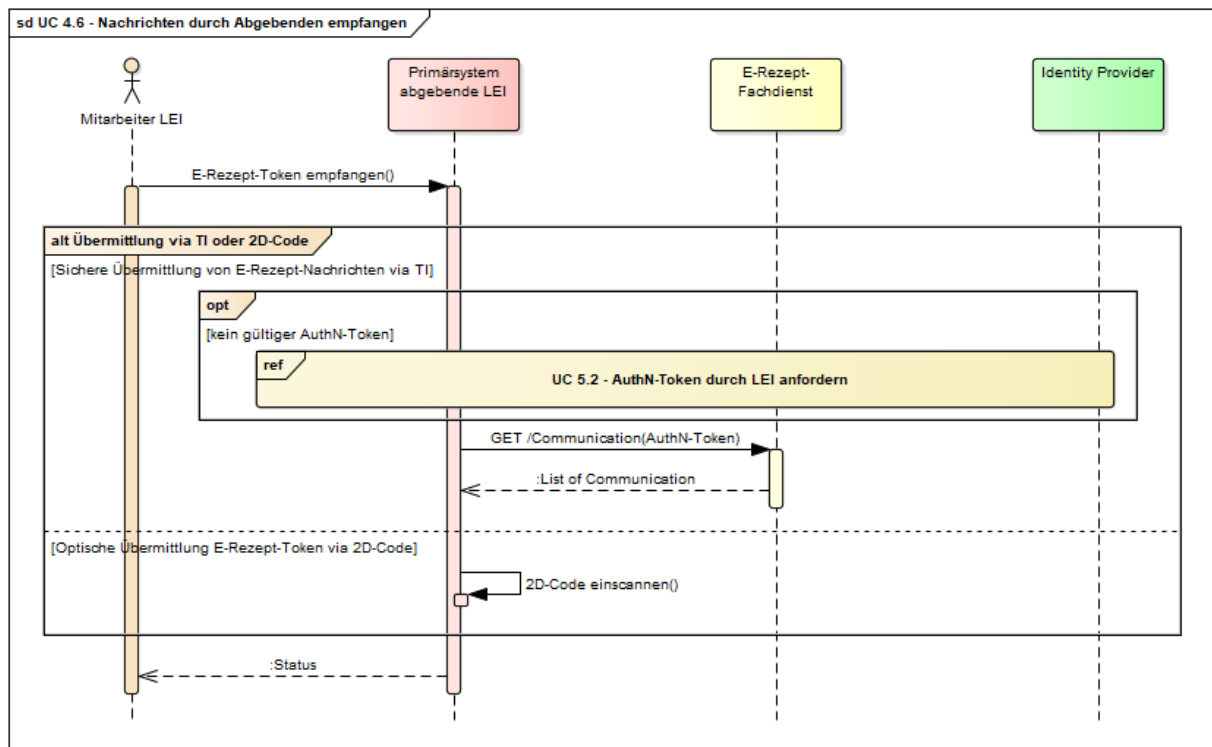
Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden Leistungserbringerinstitution Nachrichten vom E-Rezept-Fachdienst abrufen. Alternativ können E-Rezept-Token als 2D-Code im AVS eingescannt werden.

A_18617 - Anwendungsfall "Nachrichten durch Abgebenden empfangen"

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

Tabelle 14: TAB_SYSLERP_036 Anwendungsfall Nachrichten durch Abgebenden 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-Fachdienstes. Das PS fragt beim E-Rezept-Fachdienstes an, ob für die Telematik-ID der LEI neue Nachrichten vorliegen und lädt diese herunter.</p> <p>Im Falle der Alternative über den 2D-Code wandelt das PS die optische Repräsentation in die Textform um.</p>
Nachbedingung	Der E-Rezept-Token liegt im PS der abgebenden LEI vor.



[<=]

3.6.2 Nachricht durch Abgebenden an Versicherten übermitteln

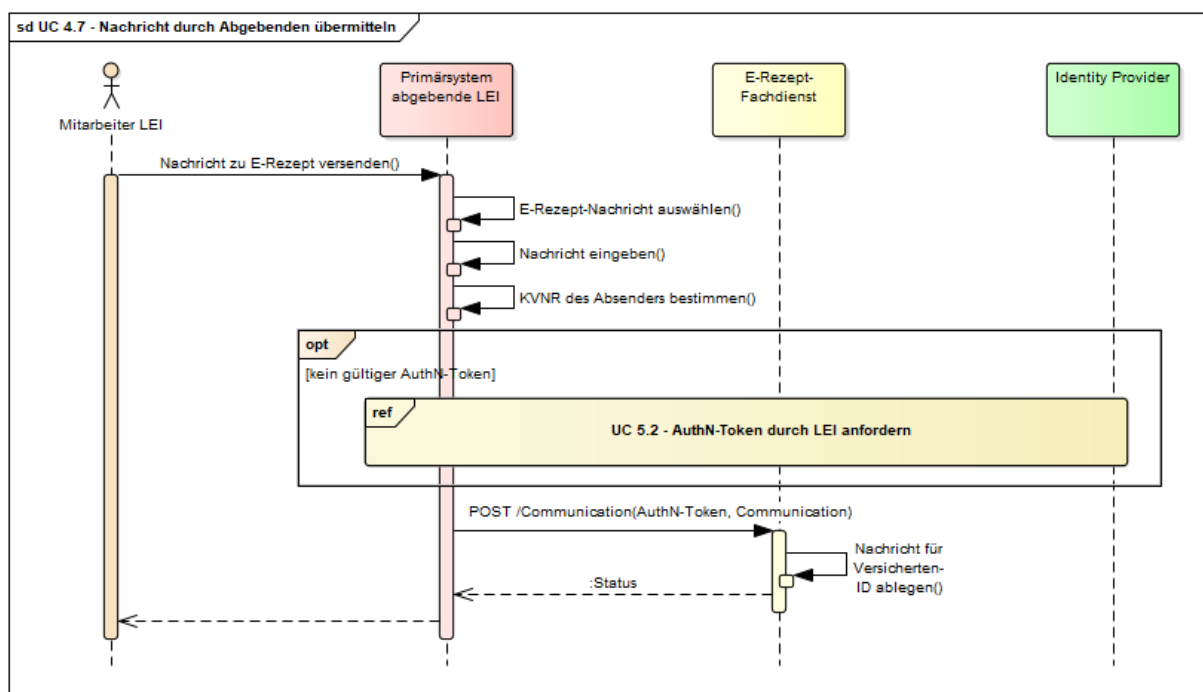
Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden Leistungserbringerinstitution auf ein mittels dem E-Rezept-Fachdienst übermittelten E-Rezept-Token reagieren und dem Absender eine Nachricht, bspw. über die Verfügbarkeit, übermitteln.

A_19013 - Anwendungsfall "Nachricht durch Abgebenden übermitteln"

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

Tabelle 15: 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.



[<=]

3.6.3 Nachricht durch Abgebenden löschen

Mit diesem Anwendungsfall kann der abgebende Leistungserbringer von ihm übermittelte Nachrichten an Versicherte löschen. Im Ergebnis der Löschanforderung wird dem Primärsystem des abgebenden Leistungserbringers mitgeteilt, ob die Nachricht bereits vom Empfänger abgerufen wurde.

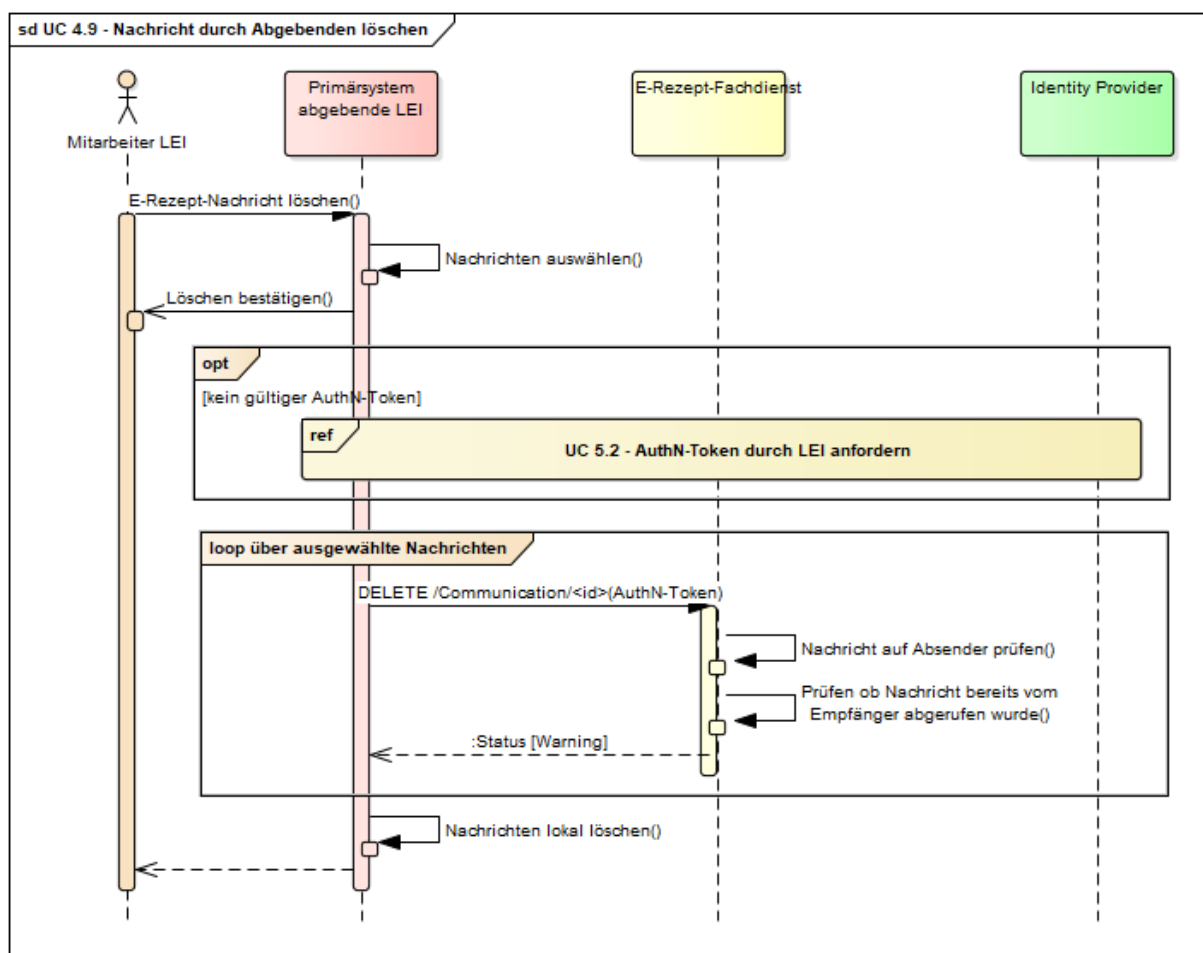
A_20776 - Anwendungsfall "Nachricht durch Abgebenden löschen"

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

Tabelle 16: TAB_SYSLERP_062 Anwendungsfall Nachricht durch Abgebenden löschen

Name	UC 4.9 - Nachricht durch Abgebenden löschen
Vorbedingung	<ul style="list-style-type: none"> Ein abgebender Leistungserbringer hat den Anwendungsfall "UC 4.7 - Nachricht durch Abgebenden übermitteln" ausgeführt.
Kurzbeschreibung (Außenansicht)	<p>Der Abgebende wählt eine oder mehrere zuvor von ihm übermittelte Nachrichten zum Löschen aus.</p> <p>Der Abgebende bestätigt das Löschen.</p> <p>Das Primärsystem des Abgebenden überträgt für jede zu löschende Nachricht die Löschanforderung an den E-Rezept-Fachdienst.</p> <p>Die zu löschenden Nachrichten werden im E-Rezept-Fachdienst gelöscht.</p> <p>Der E-Rezept-Fachdienst übermittelt dem Primärsystem eine Warnung, wenn die Nachricht bereits durch den Empfänger</p>

	abgerufen wurde. Abschließend werden die zu löschenden Nachrichten im Primärsystem gelöscht.
Nachbedingung	Die Nachrichten sind auf dem E-Rezept-Fachdienst und im FdV gelöscht.



[<=]

3.6.4 E-Rezept durch Abgebenden abrufen

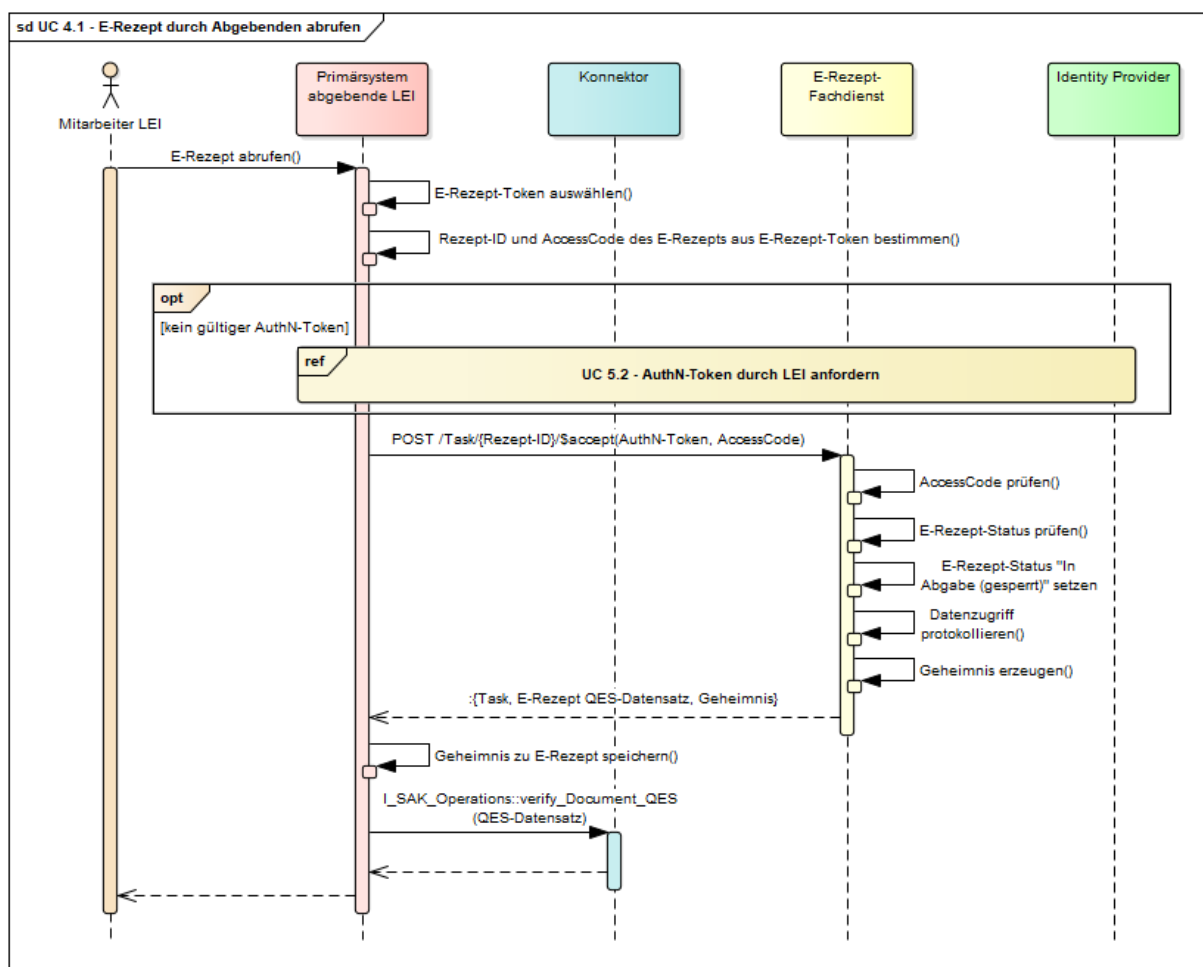
Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden Leistungserbringerinstitution ein E-Rezept auf Basis eines durch den Versicherten, einen Vertreter oder die verordnende LEI übermittelten E-Rezept-Tokens aus dem E-Rezept-Fachdienst abrufen.

A_18511 - Anwendungsfall "E-Rezept durch Abgebenden abrufen"

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

Tabelle 17: 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>



[<=]

3.6.5 E-Rezept durch Abgebenden zurückgeben

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

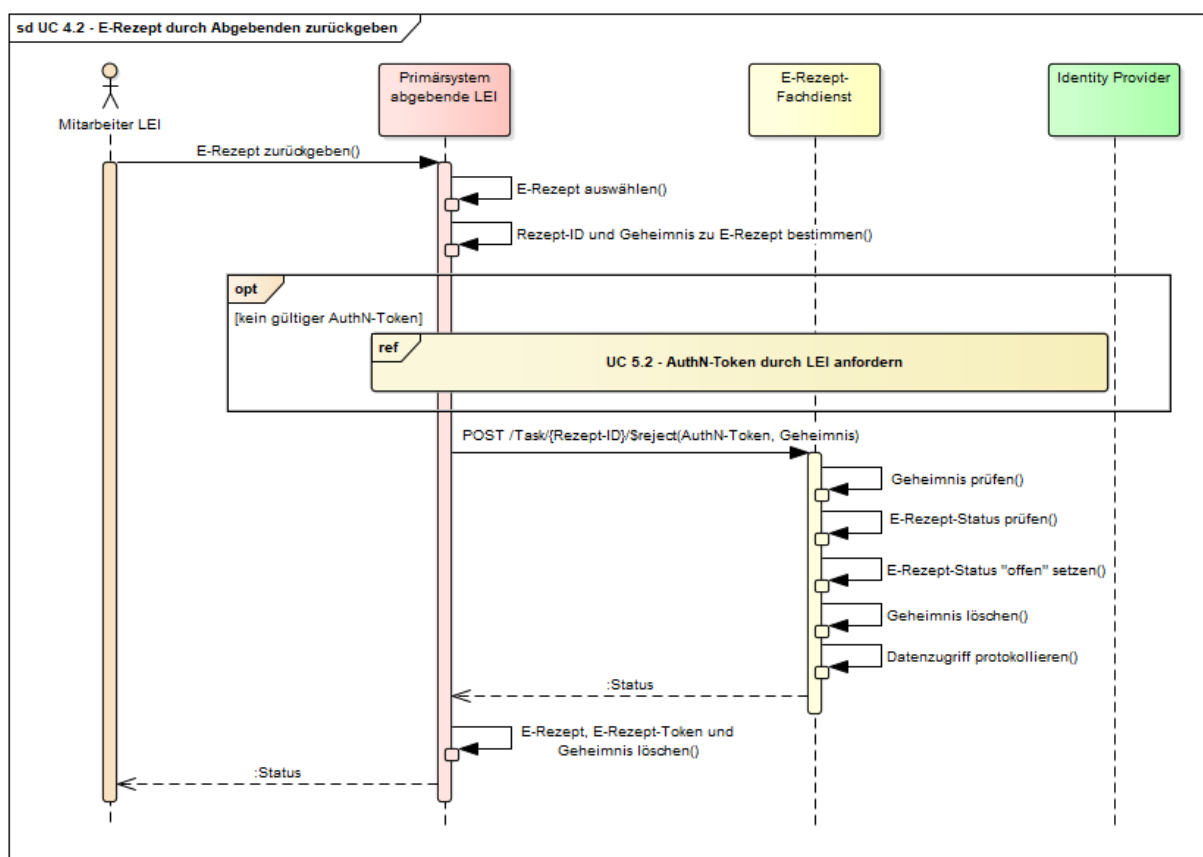
A_18512 - Anwendungsfall "E-Rezept durch Abgebenden zurückgeben"

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

Tabelle 18: TAB_SYSLERP_015 Anwendungsfall E-Rezept durch Abgebenden 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)	<p>Ein Mitarbeiter der abgebenden LEI markiert über das PS ein E-Rezept zum Zurückgeben 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.</p>
Nachbedingung	<p>Das E-Rezept im E-Rezept-Fachdienst hat den Status "offen".</p> <p>Der Statuswechsel des E-Rezepts zum Status "offen" ist im E-Rezept-Fachdienst protokolliert.</p> <p>Das E-Rezept, der E-Rezept-Token und das Geheimnis zur Statusänderung "in Abgabe (gesperrt)" sind im PS gelöscht.</p>



[<=]

3.6.6 E-Rezept durch Abgebenden löschen

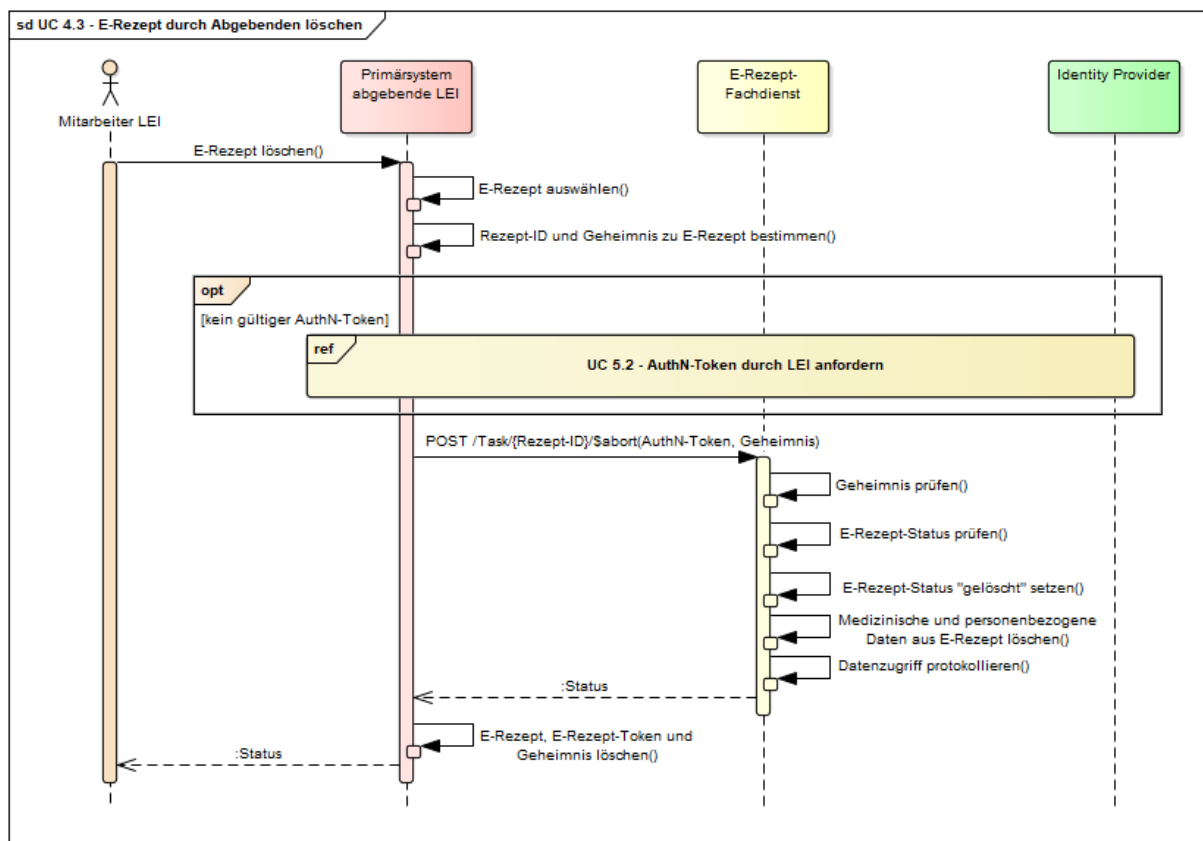
Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden Leistungserbringerinstitution den Status für ein zuvor aus dem E-Rezept-Fachdienst abgerufenes E-Rezept auf "gelöscht" setzen. Die Nutzer können auf ein E-Rezept mit dem Status "gelöscht" nicht zugreifen.

A_18513 - Anwendungsfall "E-Rezept durch Abgebenden löschen"

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

Tabelle 19: 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>



[<=]

3.6.7 Quittung abrufen

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

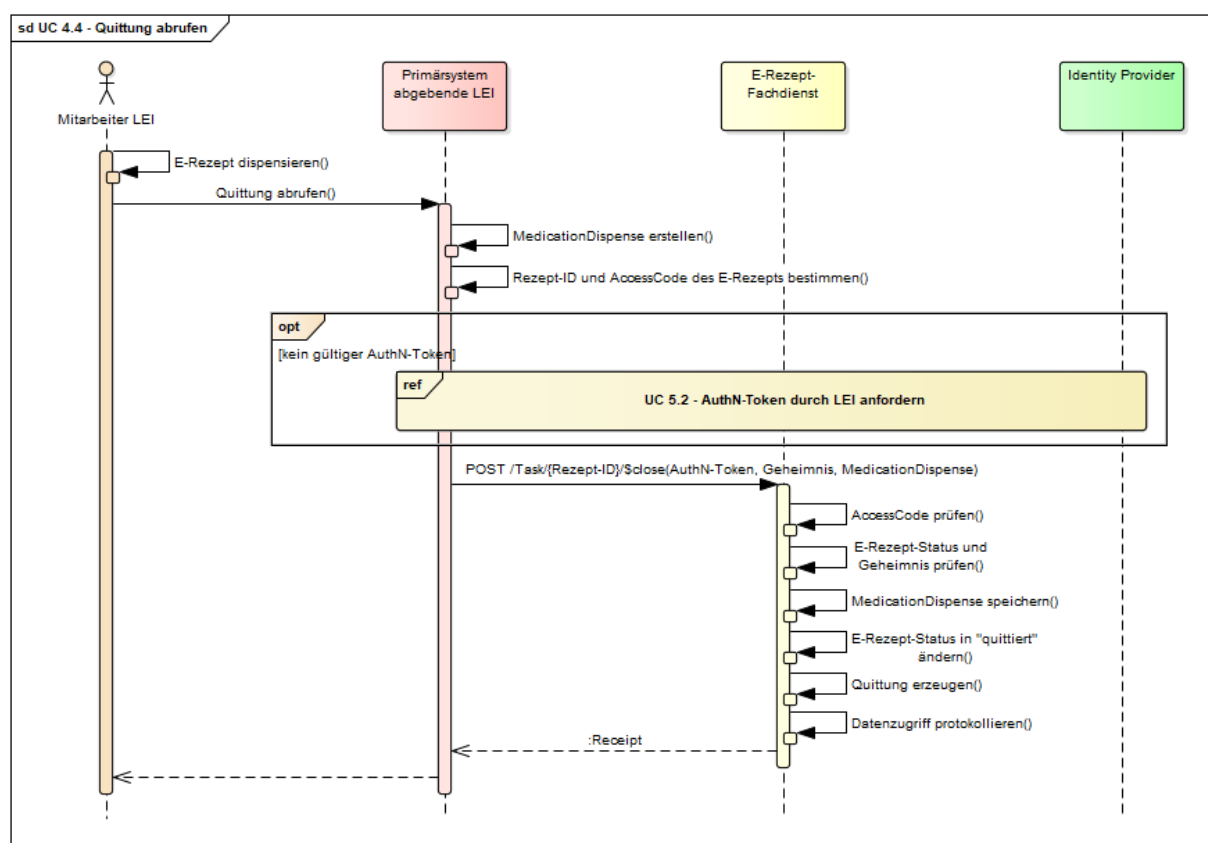
A_18514 - Anwendungsfall "Quittung abrufen"

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

Tabelle 20: 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>



[<=]

3.6.8 Quittung erneut abrufen

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

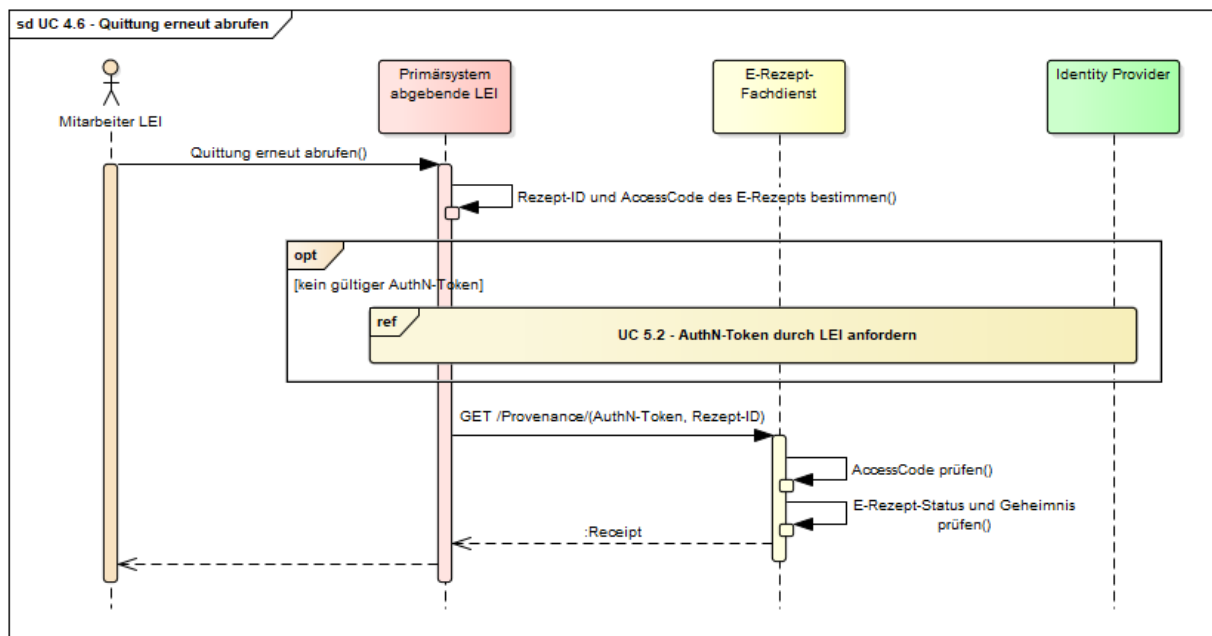
Der Anwendungsfall führt zu keiner Änderung am Status des E-Rezepts.

A_19117 - Anwendungsfall "Quittung erneut abrufen"

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

Tabelle 21: 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 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.



[<=]

3.6.9 Dispensierdatensatz durch Abgebenden signieren

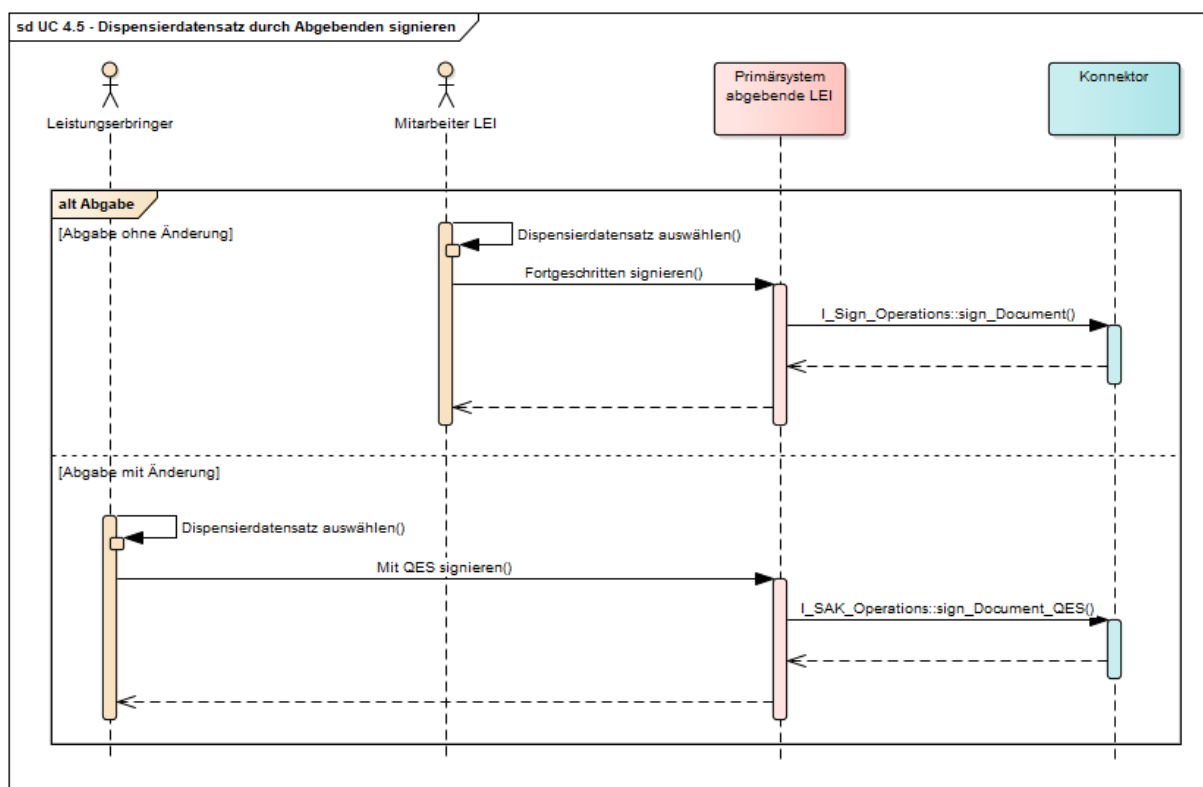
Mit diesem Anwendungsfall kann ein Mitarbeiter einer abgebenden Leistungserbringerinstitution einen Dispensierdatensatz signieren. In Abhängigkeit der arzneimittelrechtlichen Vorschriften und der Verträge nach § 129 SGB V wird dieser Datensatz qualifiziert (QES) bzw. fortgeschritten (nonQES) signiert.

A_18515 - Anwendungsfall "Dispensierdatensatz durch Abgebenden signieren"

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

Tabelle 22: TAB_SYSLERP_018 Anwendungsfall Dispensierdatensatz durch Abgebenden 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)	<p>Falls die Abgabe ohne Änderung erfolgte, signiert ein Mitarbeiter der abgebenden LEI den Dispensierdatensatz mit einer fortgeschrittenen Signatur.</p> <p>Falls die Abgabe mit Änderung der Verschreibung nach § 17 (5) ApoBetrO erfolgte, signiert der abgebende Leistungserbringer den Dispensierdatensatz mit einer QES.</p>
Nachbedingung	Der Dispensierdatensatz ist durch den Abgebenden signiert.



[<=]

3.7 Anfordern von Identitätsbestätigungen

3.7.1 Identitätsbestätigung durch den Versicherten anfordern

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

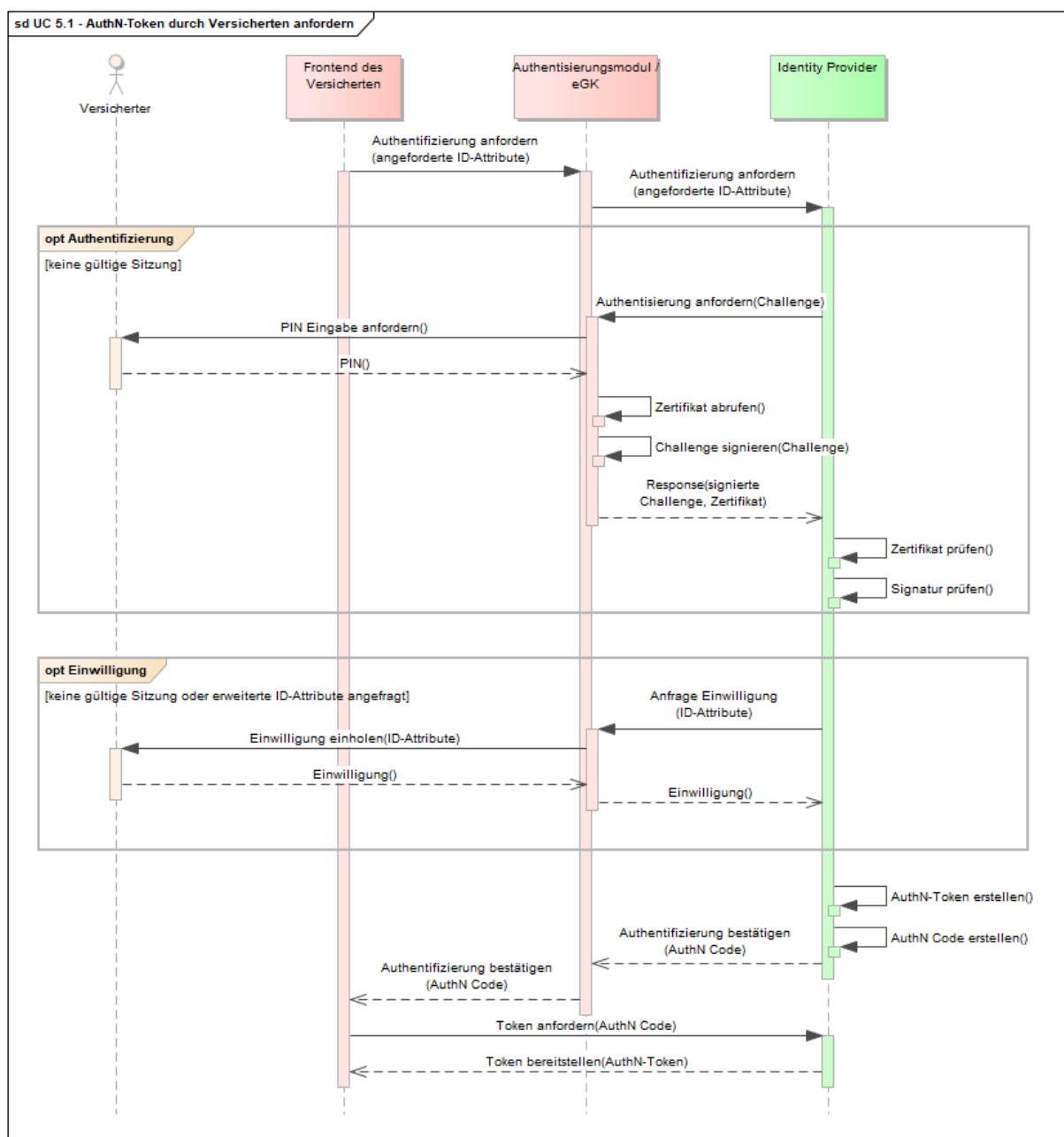
A_18822 - Anwendungsfall "AuthN-Token durch Versicherten anfordern"

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

Tabelle 23: 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.



[<=]

In Ausbaustufen des IDP bzw. mit der Förderung der IDPs zu einem umfassenden Identity Management sind weitere Authentifizierungsverfahren (ggfs. über alternative Identifikationsmittel) denkbar, sofern sie das jeweils aus dem Schutzniveau der Daten abgeleitete Sicherheitsniveau erfüllen (Sicherheitsniveau im E-Rezept: 'hoch').

3.7.2 Identitätsbestätigung durch LEI anfordern

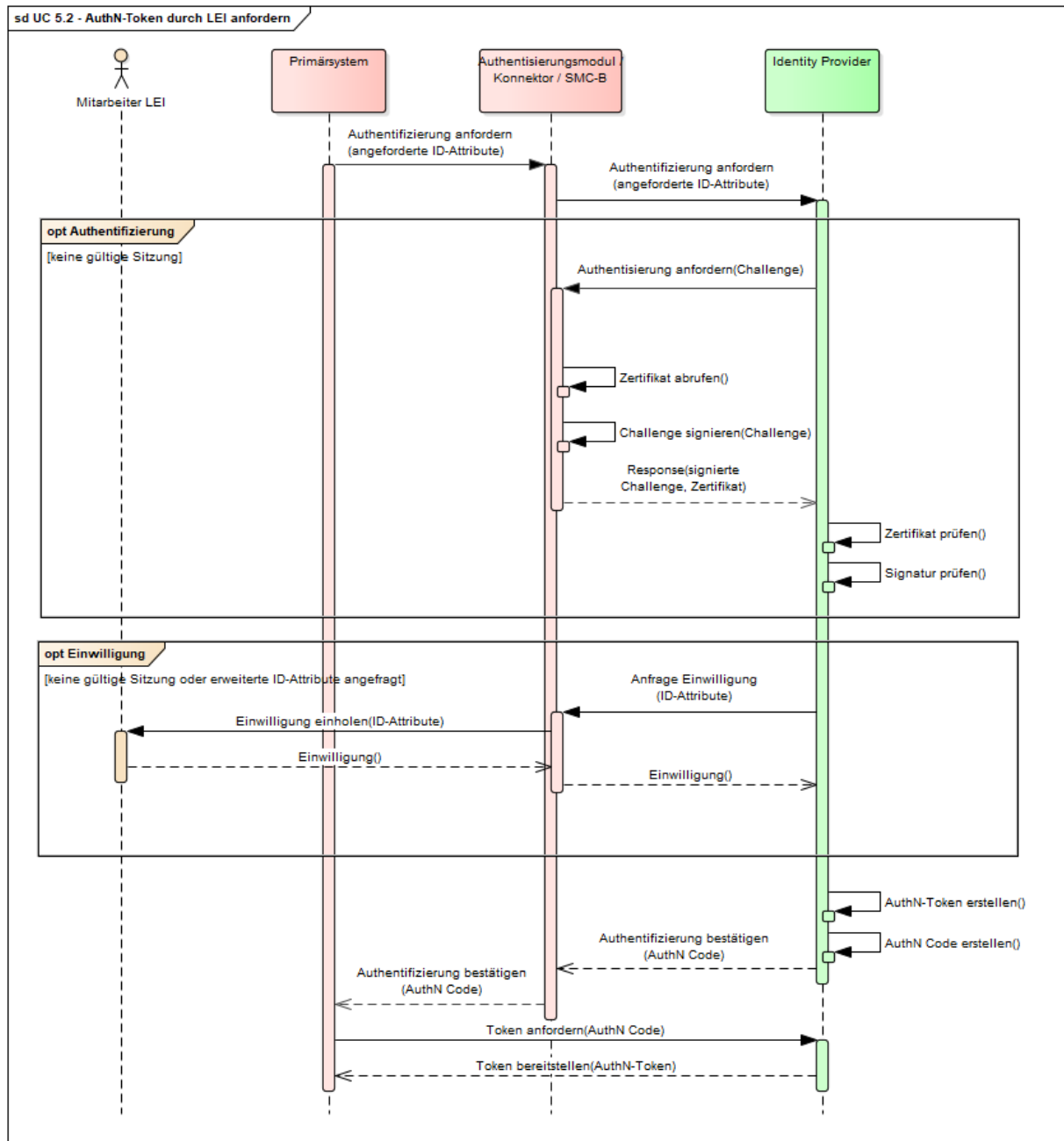
Dieser Anwendungsfall betrifft die Anforderung eines AuthN-Tokens durch eine LEI über das Primärsystem. Er ist Bestandteil aller Anwendungsfälle, die für einen Zugriff auf einen Dienst der TI (Ausnahme: Zugriff auf IDP) ein solches Token benötigen, siehe die Ablaufbeschreibungen (Sequenzdiagramme) der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

A_18827 - Anwendungsfall "AuthN-Token durch LEI anfordern"

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

Tabelle 24 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 I_Sign_Operations::external_authenticate 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.



[<=]

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.

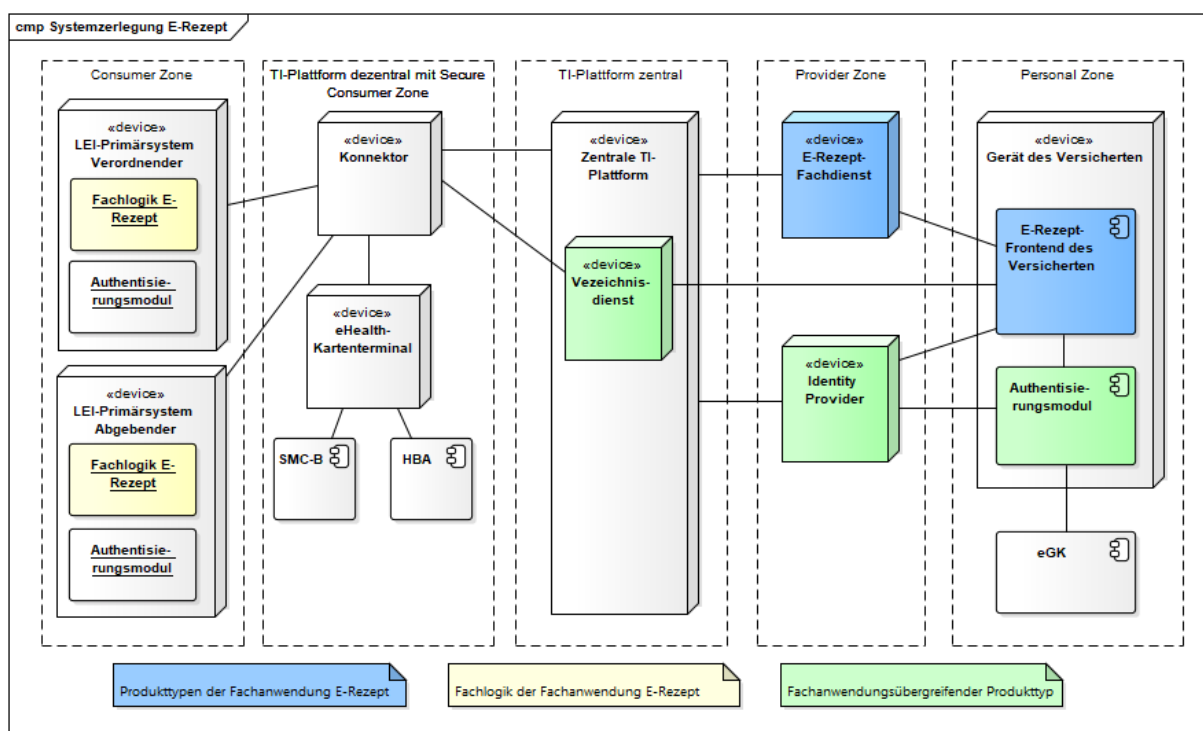


Abbildung 7: ABB_SYSLERP_006 Systemzerlegung E-Rezept

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 E-Rezept-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 25: TAB_SYSLERP_019 Schnittstellen E-Rezept-Fachdienst

Ressource	Operation	Nutzer
E-Rezept	E-Rezept-ID abrufen E-Rezept einstellen	Verordnender

	E-Rezept durch Verordnenden löschen	
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 E-Rezept-Nachricht löschen	Versicherter Vertreter Abgebender

[<=]

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

Der E-Rezept-Fachdienst MUSS Rezept-IDs erzeugen, welche mindestens über einen Zeitraum von 11 Jahren eindeutig sind. [<=]

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

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

Der E-Rezept-Fachdienst MUSS die Rezept-ID als Ressourcen-Identifizier für die Ressource E-Rezept verwenden. [<=]

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

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

Der E-Rezept-Fachdienst MUSS einen AccessCode mit ausreichend hoher Entropie erzeugen. Der E-Rezept-Fachdienst MUSS sicherstellen, dass jedes im E-Rezept-Fachdienst verwaltete E-Rezept einen eineindeutigen AccessCode besitzt. [<=]

A_18522 - E-Rezept-Fachdienst – E-Rezept-Statuswechsel

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

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

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

Der E-Rezept-Fachdienst MUSS beim Übergang des Status eines E-Rezepts von "in Abgabe (gesperrt)" zu "quittiert" eine E-Rezept-spezifische Quittung erstellen, mit seiner

PKI-Identität (ID.FD.SIG) signieren und dem abgebenden Leistungserbringer übergeben. 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 26: 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. [<=]

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

Der E-Rezept-Fachdienst MUSS sämtliche Zugriffe auf sowie Statuswechsel und das Löschen von E-Rezepten für den Versicherten nachvollziehbar protokollieren. [<=]

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. [<=]

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. [<=]

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 27: 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
E-Rezept-Nachricht löschen	Versicherter, Apotheker, Mitarbeiter Apotheke

Die Ausführung von Operationen durch Unberechtigte sowie hier nicht genannte Operationen MUSS vom E-Rezept-Fachdienst unterbunden werden. [<=]

A_18936 - E-Rezept-Fachdienst - Transaktionssicherheit

Der E-Rezept-Fachdienst MUSS alle Aktivitäten zu einem Aufruf durch einen Client transaktionssicher durchführen. [<=]

A_18795 - E-Rezept-Fachdienst - Erreichbarkeit im Internet

Der E-Rezept-Fachdienst MUSS im Internet erreichbar sein. Der E-Rezept-Fachdienst MUSS sicherstellen, dass ausschließlich Versicherte aus dem Internet zugreifen können. [<=]

Um eine missbräuliche Verwendung von eGK-Prüfkarten auszuschließen, prüft der E-Rezept-Fachdienst die Verwendung der eGK-Prüfkarte in den Anwendungsfällen der Vertreterkommunikation und des Vertreterzugriffs auf E-Rezepte.

A_20755 - E-Rezept-Fachdienst - Prüfkarte eGK in der Vertreterkommunikation

Der E-Rezept-Fachdienst MUSS eine Kommunikation von Versicherten einer Krankenkasse zu Nutzern einer Prüfkarte eGK verhindern. Der umgekehrte Kommunikationsweg MUSS vom E-Rezept-Fachdienst ebenfalls verhindert werden. [<=]

A_20756 - E-Rezept-Fachdienst - Prüfkarte eGK im Vertreterzugriff auf E-Rezepte

Der E-Rezept-Fachdienst MUSS einen Zugriff auf E-Rezepte von Versicherten einer Krankenkasse durch Nutzer einer Prüfkarte eGK verhindern. Ebenso MUSS der E-Rezept-Fachdienst verhindern, dass Versicherte einer Krankenkasse auf E-Rezepte zugreifen können, die für Nutzer einer Prüfkarte eGK ausgestellt wurden. [<=]

4.1.1.1 Vertrauenswürdige Ausführungsumgebung

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

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

Der E-Rezept-Fachdienst MUSS alle Komponenten, die an der Verarbeitung von E-Rezept-Daten im Klartext beteiligt sind, in einer Vertrauenswürdigen Ausführungsumgebung umsetzen. [<=]

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

A_18824 - Automatische Wiederherstellung eines konsistenten Zustands der VAU nach Systemfehlern

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

A_18825 - Fehlererkennung für Anwender ermöglichen

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

A_18826 - Vorgangswiederholung nach Fehler gewährleisten

Der E-Rezept-Fachdienst MUSS die Wiederholung von aufgrund von Systemfehlern gescheiterten Verarbeitungsvorgängen ermöglichen und dies so umsetzen, dass die Vorgangswiederholung durch die Client-Anwendung in Form eines einfachen „erneut versuchen“ umgesetzt werden kann. [<=]

4.1.1.2 Betriebliche Aspekte

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

A_18741 - E-Rezept-Fachdienst - Anbieterschlüsse

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

- Identity Provider

[<=]

A_18687 - E-Rezept-Fachdienst – Verfügbarkeit

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

A_18743 - E-Rezept-Fachdienst - Maximales Rezeptaufkommen

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

Tabelle 28: TAB_SYSLERP_002 Maximales Aufkommen nach Rezeptzeilen (Muster 16) 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

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

Tabelle 29: TAB_SYSLERP_003 Gesamtes Aufkommen nach Rezeptzeilen (Muster 16) 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

[<=]

A_18745 - E-Rezept-Fachdienst - Antwortzeiten

Der E-Rezept-Fachdienst MUSS alle Aufrufe seiner Schnittstellen so beantworten, dass in Primärsystemen und den FdV keine Verzögerungen in den übergeordneten Abläufen entstehen.[<=]

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

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

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

4.1.2 Produkttyp E-Rezept-Frontend des Versicherten

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

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

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

A_18689 - Frontend des Versicherten – Zusätzliche Funktionalitäten

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

Eine zusätzliche Funktionalität ist beispielsweise die Anfrage zur Belieferung durch eine Apotheke oder Download digitaler Beipackzettel.

A_20207 - Frontend des Versicherten - Makelverbot

Das E-Rezept-FdV DARF NICHT zusätzliche Funktionalitäten enthalten, die die berufs- oder gewerbsmäßige Zuweisung und das Makeln von E-Rezepten unterstützen oder den Nutzer in in seiner Entscheidung beeinflussen, welche elektronischen Verordnungen in welcher Apotheke eingelöst werden. [<=]

A_18528 - Frontend des Versicherten – GUI

Das E-Rezept-Frontend des Versicherten MUSS eine grafische Oberfläche (GUI) zum Ausführen der E-Rezept-Anwendungsfälle anbieten. [<=]

A_18529 - Frontend des Versicherten – Barrierefreiheit

Das E-Rezept-Frontend des Versicherten SOLL Bedienungselemente der Barrierefreiheit umsetzen. [<=]

A_18533 - Frontend des Versicherten – Nutzung interoperabler Schnittstellen

Das E-Rezept-Frontend des Versicherten MUSS die interoperablen Schnittstellen gemäß TAB_SYSLERP_022 nutzen.

Tabelle 30: 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-Nachricht löschen	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

[<=]

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

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

- Rezept-ID
- AccessCode

[<=]

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

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

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

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

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

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

Das E-Rezept-Frontend des Versicherten KANN einen E-Rezept-Token aus Drittanwendungen importieren und in Drittanwendungen exportieren. [<=]

Der Export kann bspw. durch das Weiterleiten mittels eines Messenger-Dienstes oder E-Mail erfolgen. Beim Export sind datenschutzrechtliche Anforderungen zu beachten. Näheres hierzu regelt die Rechtsverordnung nach § 360 Abs. 5 PDSG.

A_18539 - Frontend des Versicherten – E-Rezept anzeigen

Das E-Rezept-Frontend des Versicherten MUSS die fachlichen Inhalte eines E-Rezepts anzeigen können. [<=]

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

A_18540 - Frontend des Versicherten – Abgebende LEI im Verzeichnis suchen

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

A_20225 - Frontend des Versicherten – Neutralität in der Verzeichnissuche

Das E-Rezept-Frontend des Versicherten MUSS Such- und Filterkriterien wettbewerbsneutral ausgestalten (z.B. Sortierung nach Alphabet, nächster Standort, etc.) und das Ergebnis einer Such- bzw. Filterabfrage im VZD vollständig anzeigen, sodass keine Hervorhebung oder andere Art der Bevorzugung von Apotheken bei der Darstellung erfolgt. [<=]

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

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

- Information über neu vorliegende Nachrichten durch Abgebende,
- automatische Information über Statusänderungen von E-Rezepten im E-Rezept-Fachdienst,
- Ausdruck des DataMatrix-Code für einen E-Rezept-Token,
- Filterfunktionen zur Auswahl abgebender LEI aus dem Verzeichnis,
- Filterfunktionen für die Anzeige der Protokolleinträge.

4.1.3 Primärsysteme

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

Die Primärsysteme verwalten in einer lokalen Datenbasis die notwendigen Informationen zu den in der Fachanwendung E-Rezept eingesetzten SMC-Bs und HBAs. Praxisverwaltungssysteme verwalten zusätzlich die zur Verordnung notwendigen Versichertendaten (KVNR).

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

A_18541 - Primärsystem - Signaturverfahren auswählen

Das Primärsystem MUSS es dem verordnenden und abgebenden Akteur ermöglichen, für Anwendungsfälle des E-Rezepts, welche das Signieren von Dokumenten beinhalten, zwischen Einzel-, Stapel- und Komfortsignatur auszuwählen. Eine Defaultauswahl soll konfigurierbar sein. [<=]

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

A_18747 - Primärsystem - Hinweis unzulässiger Statuswechsel

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

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

A_18688 - Primärsystem - E-Rezept-Daten für medizinische Anwendungen nutzen

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

4.1.3.1 Primärsystem verordnender Leistungserbringer

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

A_18542 - Primärsystem verordnende LEI – Nutzung interoperabler Schnittstellen

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

Tabelle 31: 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-Fachdienst
	Authentifizierung anfordern	Authentisierungsmodul
	I_Authenticate (AuthN-Token anfordern)	Identity Provider
	I_IP_Transport I_SAK_Operations	Konnektor

[<=]

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

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

A_18545 - Primärsystem verordnende LEI – Rezept-ID einmalig verwenden

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

A_18612 - Primärsystem verordnende LEI – Verordnungsdatensatz prüfen

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

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

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

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

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

- Rezept-ID
- AccessCode

[<=]

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

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

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

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

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

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

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

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

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

4.1.3.2 Primärsystem abgebender Leistungserbringer

Das Primärsystem abgebender Leistungserbringer ist ein Apothekenverwaltungssystem (AVS).

A_18547 - Primärsystem abgebende LEI – Nutzung interoperabler Schnittstellen

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

Tabelle 32: 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-Profil

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-Profil 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

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

A_18809 - IDP - Minimierung der Authentisierungsanfragen, komfortabler Single Sign-On

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

4.2.1.2 Betriebliche Aspekte

A_18904 - IDP – Verfügbarkeit

Der Anbieter des IDP MUSS die Hochverfügbarkeit des Dienstes sicherstellen. [≤]

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

A_18903 - IDP - Anbieterausschlüsse

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

- E-Rezept-Fachdienst

[≤]

A_18810 - IDP - Registrierung von Clients

Der Anbieter des IDP MUSS ein Verfahren bzw. eine Schnittstelle bereitstellen, über welche sich Dienste der TI als Relying Party (Clients) für die Nutzung des IDP registrieren können. [≤]

A_18801 - IDP - Widerspruchsfreiheit von IDP und PKI

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

A_18802 - IDP - Widerspruchsfreiheit von IDP und Verzeichnisdienst

Der Anbieter des IDP MUSS, wenn für einen Teilnehmer Identitätsattribute sowohl über den Verzeichnisdienst als auch den IDP bereitgestellt werden, sicherstellen, dass sich die beiden Identitätsattribute bezüglich der aktuellen Gültigkeit und der inhaltlichen Aussagen nicht widersprechen. [≤]

A_18939 - IDP - Bereitstellung Authentisierungsmodul

Der Anbieter des IDP SOLL ein Authentisierungsmodul für die gängigen mobilen Betriebssysteme iOS und Android bereitstellen, das den Authentifizierungsvorgang des Nutzers über eine Schnittstelle zwischen IDP und dem Authentisierungsmodul auf dem Gerät des Nutzers steuert. [≤]

A_19016 - Verifikation von Produkt-Changes

Der Anbieter des IDP MUSS den Erfolg eines Produkt-Changes durch eine hinreichende Anzahl erfolgreich durchlaufener, dem Produkt-Change angemessener Anwendungsfälle oder Bearbeitungsvorgänge verifizieren. [≤]

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

Das Authentisierungsmodul MUSS einen Systemdienst auf der Betriebssystemplattform des Geräts des Nutzers mit einer Schnittstelle (Authentisierung anfordern) anbieten, über die ein Clientsystem einen Authentifizierungsrequest an das Authentisierungsmodul zur Authentifizierung des Nutzers gegenüber dem IDP weiterleiten kann.[<=]

4.2.3 Produkttyp Verzeichnisdienst der TI

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

Folgende zusätzliche Anforderungen bestehen.

A_18867 - VZD - Authentifizierung auf Basis Identitätsbestätigung des IDP

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

A_18837 - VZD - Erreichbarkeit im Internet

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

A_18941 - VZD - Einschränkung abfragbarer Informationen für Versicherte

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

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

4.3 Schnittstelle der Fachanwendung E-Rezept

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

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

4.3.1 Schnittstelle für die Ressource E-Rezept

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

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

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

Tabelle 33: 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 (Workflowidentifizier für Rezept-Typ)	FHIR-Object
Attribut-Out (Body)	PrescriptionID	Objekt-ID in Task.id, Rezept-ID in Task.identifizier
Attribut-Out (Body)	AccessCode	external Identifizier in Task.identifizier

Mit dieser Operation kann ein Verordnender eine Rezept-ID abrufen. Die Operation muss zur Autorisierung des Aufrufenden (`IdentityToken`) die Rolle prüfen. Als Aufruf-Parameter der FHIR-Operation `$create` der Ressource `Task` wird ein strukturierter Datensatz mit FHIR-Operationsparametern (Workflowidentifizier) übergeben, da das entsprechende E-Rezept inkl. E-Rezept-ID im nächsten Schritt vom Konnektor signiert werden muss.

Die Operation liefert die Rezept-ID (`PrescriptionId`) als ID der angelegten Ressource `Task` und generiert den `AccessCode` (`AccessCode`) als external Identifizier in den

Datensatz, welcher den Zugriff auf das E-Rezept erlaubt. Der Task erhält den Status "initialisiert" ("draft").[<=]

A_18556 - Logische Operation "E-Rezept einstellen"

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

Tabelle 34: TAB_SYSLERP_026 Operation E-Rezept einstellen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept einstellen	
Methode	POST	/Task/{ID}/\$activate
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	AccessCode	Header-Attribut String
Attribut-In (Body)	E-Rezept-FHIR-Parameter	FHIR-Objekt
Attribut-In (Body)	signature	Base64-codiertes CMS-Objekt als selfcontained Binary in PKCS#7-Datei

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 im QES-Datensatz enthaltenen `FHIR-Bundles` und erzeugt bei Korrektheit aller Daten eine Signatur über das Bundle mit der Signaturidentität ID.FD.SIG, die als Kopie für den Versicherten mit Zugriff auf den Task zum Abruf durch den Versicherten abgelegt wird. Der Datensatz der QES wird als Binary-Objekt 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 35: TAB_SYSLERP_027 Operation E-Rezept durch Verordnenden löschen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Verordnenden löschen	

Methode	POST	/Task/{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 36: TAB_SYSLERP_028 Operation E-Rezept durch Abgebenden abrufen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Abgebenden abrufen	
Methode	POST	/Task/{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	FHIR-Objekt
Attribut-Out (Body)	Secret	external Identifier in Task.identifier

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

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

Die Operation erzeugt ein Geheimnis zur Statusänderung (`Secret`) im Task, mit der der abgebenden LEI nachfolgende Zugriffe auf die Ressource gewährt werden. In der

Response wird der Task und der beim Einstellen des E-Rezepts hinterlegte QES-Datensatz in einem FHIR-Bundle zurückgegeben. [<=]

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

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

Tabelle 37: TAB_SYSLERP_029 Operation E-Rezept durch Abgebenden löschen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Abgebenden löschen	
Methode	POST	/Task/{ID}/\$abort
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (URL)	?secret={Secret}	URL-Parameter 'secret'

Mit dieser Operation kann eine abgebende LEI den Status (`Task.status`) des E-Rezepts 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 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 38: TAB_SYSLERP_030 Operation E-Rezept durch Abgebenden zurückgeben

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

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 39: TAB_SYSLERP_031 Operation Quittung abrufen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	Quittung abrufen	
Methode	POST	/Task/{ID}/\$close
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Body)	MedicationDispense	FHIR-Objekt
Attribut-In (URL)	?secret={Secret}	URL-Parameter 'secret'
Attribut-Out (Body)	Receipt	signiertes FHIR-Objekt Bundle über 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` als FHIR-Bundle, die am Task als Workflow-Output zum Abruf gespeichert und an ebenso den Aufrufenden zurückgegeben wird. Die `MedicationDispense` wird für den Versicherten zum Abruf gespeichert.

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 40: TAB_SYSLERP_031 Operation Quittung erneut abrufen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	Quittung erneut abrufen	

Methode	GET	/Task/{ID}
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (URL)	?secret={Secret}	URL-Parameter 'secret'
Attribut-Out (Body)	Task inkl. Receipt	Bundle FHIR-Objekt aus Task und signiertem FHIR-Bundle-Objekt über MedicationDispense

Mit dieser Operation kann eine abgebende LEI eine Quittung erneut abrufen. Dafür wird eine lesende Anfrage an den Task gestellt, zu dem die Apotheke das während der Belieferung erzeugte Geheimnis (`Secret`) kennt. Der E-Rezept-Fachdienst prüft intern zusätzlich die Rolle des Aufrufenden im `IdentityToken` und ob das während der Dispensierung erstellte Secret gleich dem übergebenen Parameter `Secret` entspricht. [<=]

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

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

Tabelle 41: 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 signierten FHIR-Bundles	FHIR-Objekt

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

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

Die Operation muss prüfen, ob die einzelnen E-Rezepte einen Status ungleich "initialisiert" ("draft") und "gelöscht" ("cancelled") haben. Die Ausgabe der Tasks erfolgt inkl. der serverseitig signierten FHIR-Bundles. [<=]

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

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

Tabelle 42: TAB_SYSLERP_032 Operation E-Rezept durch Vertreter abrufen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Vertreter abrufen	
Methode	GET	/Task/{ID}
Attribut-In (Header)	IdentityToken	JSON Web Token
Attribut-In (Header)	AccessCode	Header-Attribut String (optional)
Attribut-Out (Body)	Bundle mit einer Task- und signiertem FHIR-Bundle	FHIR-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 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 serverseitig-signierten FHIR-Bundles. [\leq]

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

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

Tabelle 43: TAB_SYSLERP_033 Operation E-Rezept durch Versicherten löschen

Kategorie	Name	Typ
Ressource	E-Rezept	
Operation	E-Rezept durch Versicherten löschen	
Methode	POST	/Task/{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 KVN 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. Der AccessCode 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. [<=]

A_19140 - Logische Operation "Dispensierinformationen durch Versicherten abrufen"

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

Tabelle 44: 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-Out (Body)	MedicationDispense	FHIR-Objekt

Mit dieser Operation kann ein Versicherter die Dispensierinformationen für seine E-Rezepte abrufen. Die Operation muss auf Basis der KVNR in der Identitätsbestätigung (`IdentityToken`) filtern, sodass nur die Dispensierinformationen zurückgegeben werden, die für den Versicherten erstellt wurden. [<=]

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

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

Tabelle 45: TAB_SYSLERP_058 Operation Dispensierinformation für ein einzelnes E-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/{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	FHIR-Objekt
---------------------	--	-------------

Mit dieser Operation kann ein Versicherter die Dispensierinformationen für ein einzelnes E-Rezept abrufen. 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. Im Ergebnis wird das E-Rezept inklusive der Dispensierinformationen zurückgegeben. [`<=`]

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 46: 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	FHIR-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 die verordnete Medication als Objekt in `Communication.about` oder eine Referenz auf den umzusetzenden Task in `Communication.basedOn` einfügen. [`<=`]

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

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

Tabelle 47: 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)	Bundle of Messages	FHIR-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. KVN für Versicherte in der Identitätsbestätigung (`IdentityToken`) aus (Telematik-ID bzw. Versicherten-ID muss gleich `Communication.recipient` sein).[<=]

A_20261 - Logische Operation "E-Rezept-Nachricht löschen"

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

Tabelle 48: TAB_SYSLERP_060 Operation E-Rezept-Nachricht löschen

Kategorie	Name	Typ
Ressource	Communication	
Operation	E-Rezept-Nachricht löschen	
Methode	DELETE	/Communication/{ID}
Attribut-In (Header)	IdentityToken	JSON Web Token

Mit dieser Operation kann der aufrufende Akteur eine von ihm eingestellte E-Rezept-Nachricht über die beim Einstellen erzeugte Ressourcen-ID {ID} löschen.

Die Operation prüft auf Basis der Telematik-ID für Leistungserbringerinstitutionen bzw. KVN für Versicherte in der Identitätsbestätigung (`IdentityToken`), ob der aufrufende Nutzer derjenige Absender der Nachricht ist, der in `Communication.sender` angegeben ist. Wurde die Nachricht vom Empfänger bereits abgerufen (Attribut `Communication.received` ungleich Null), meldet der E-Rezept-Fachdienst dies im http-Response-Header "Warning".[<=]

4.3.3 Schnittstelle für die Ressource Zugriffsprotokolleintrag

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

A_18871 - Logische Operation "Zugriffsprotokolleinträge durch Versicherten abrufen"

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

Tabelle 49: TAB_SYSLERP_051 Operation Zugriffsprotokolleinträge durch Versicherten 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)	Bundle of AuditEvent	FHIR-Objekt

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

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

4.3.4 Schnittstelle für die Ressource signierte Challenge

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

A_18887 - Logische Operation "signierte Challenge übergeben"

Die Schnittstelle MUSS die logische Operation "signierte Challenge übergeben" 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)	
-----------	---	--

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

4.3.5 Schnittstelle für die Ressource Einwilligung

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

A_18888 - Logische Operation "Einwilligung erteilen"

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	

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

5 Datenschutz- und Sicherheitsaspekte

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

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

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

Hinsichtlich des maßgeblichen Schutzbedarfs wurden folgende Informationsobjekte identifiziert:

Tabelle 50: 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

Die für die Verfügbarkeit maßgeblichen Prozesse sind:

Tabelle 51: 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

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

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

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

A_19010 - Vertrauenswürdigkeit des Anbieters

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

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

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

5.1 Anforderungen an den E-Rezept-Fachdienst

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

A_18566 - Schutz der Kommunikation

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

A_18851 - Kommunikation nur zwischen Berechtigten

Der E-Rezept-Fachdienst MUSS sicherstellen, dass er nur berechnigte Kommunikationsbeziehungen zulässt. [≤]

A_18569 - Ablegen und Abrufen von E-Rezepten nur durch berechtigte Leistungserbringer

Der E-Rezept-Fachdienst MUSS sicherstellen, dass nur zum Einstellen berechtigte Leistungserbringer E-Rezepte einstellen und nur zur Abgabe berechtigte Leistungserbringer E-Rezepte abrufen können. [≤]

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

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

A_18571 - Verbot der Profilbildung

Der E-Rezept-Fachdienst MUSS verhindern, dass eine Profilbildung durch den Anbieter des E-Rezept-Fachdienstes erfolgen kann. [≤]

A_18844 - Schutzmaßnahmen gegen die OWASP Top 10 Risiken

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

A_18845 - Schutz der E-Rezepte

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

A_18846 - Speicherung von E-Rezepten nur verschlüsselt

Der E-Rezept-Fachdienst MUSS sicherstellen, dass E-Rezepte nur verschlüsselt persistent im E-Rezept-Fachdienst gespeichert werden. [≤]

A_18847 - Speicherung von Nachrichten nur verschlüsselt

Der E-Rezept-Fachdienst MUSS sicherstellen, dass Nachrichten nur verschlüsselt persistent im E-Rezept-Fachdienst gespeichert werden. [≤]

A_18841 - Erkennung Anomalien auf Netzwerkebene

Der E-Rezept-Fachdienst MUSS Anomalien auf Netzwerkebene erkennen und darauf reagieren können. [≤]

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

Der E-Rezept-Fachdienst MUSS AuthN-Token des IDP ablehnen, die nicht mittels eines geeigneten technischen Verfahrens, das zur Authentifizierung einen hohen Sicherheitsstandard gewährleistet erstellt wurden. [≤]

A_20555 - Informationen zum Erstellen von E-Rezept-Token für E-Rezept-FdV

Der E-Rezept-Fachdienst MUSS sicherstellen, dass bei Clientsystemen des Versicherten nur das E-Rezept-FdV einen E-Rezept-Token erzeugen kann. [≤]

A_20556 - Identifikation Frontend des Versicherten

Der E-Rezept-Fachdienst MUSS Clientsysteme des Versicherten identifizieren können. [≤]

A_20557 - Zulässigkeit von Operationen für Clientsysteme des Versicherten

Der E-Rezept-Fachdienst MUSS sicherstellen, dass er für Clientsysteme des Versicherten ausschließlich die jeweils dafür spezifizierten Operationen ausführt. [≤]

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_18567 - Transportverschlüsselte Übertragung von Daten

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

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

A_18568 - Möglichkeit der Authentisierung gegenüber Clients

Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sich gegenüber Clients, die mit ihm kommunizieren, authentisieren. [≤]

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-Rezept-Fachdienstes mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann. [<=]

A_18881 - Kein physischer Zugang des Anbieters zu Systemen der VAU

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

A_18882 - Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU

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

A_18832 - Gute Prüfbarkeit der Sicherheitseigenschaften von Code in der VAU

Die VAU des E-Rezept-Fachdienstes MUSS die Verarbeitungslogik in Verarbeitungskontexten mittels Komponenten umsetzen, die ein hohes Maß an Gewissheit bei der Feststellung der Sicherheitseigenschaften der Anwendung ermöglichen und dazu auf Ebene des Codes (der Trusted Computing Base) möglichst kompakt gehalten werden. [<=]

Die VAU des E-Rezept-Fachdienstes benötigt symmetrisches Schlüsselmaterial für die Speicherung der E-Rezept-Daten außerhalb der VAU, um für persistierte Daten den Anbieter vom Zugriff auszuschließen. Die Funktionen der Vorhaltung und Bereitstellung des Persistenz-Schlüssels wird von einem HSM ausgefüllt. Das HSM muss die Integrität der Verarbeitungskontexte feststellen können, bevor es einen Persistenz-Schlüssel an einen Verarbeitungskontext übermittelt.

A_18833 - Persistenz-Schlüssel der VAU von HSM bereitgestellt

Die VAU des E-Rezept-Fachdienstes MUSS den für die verschlüsselte Speicherung von E-Rezept-Daten außerhalb der Verarbeitungskontexte erforderlichen symmetrischen Persistenz-Schlüssel im Zuge des Startvorgangs jedes Verarbeitungskontextes aus einem HSM beziehen. [<=]

Die VAU des E-Rezept-Fachdienstes muss sich gegenüber Nutzern mittels eines Dienstzertifikats ausweisen, welches die Vertrauenswürdigkeit des Dienstes repräsentiert. Die Nutzung des privaten Schlüssels dieses Dienstzertifikats muss an die Integritätsprüfung der Verarbeitungskontexte gebunden sein und darf ausschließlich innerhalb eines HSM erfolgen.

A_18834 - Integritätsprüfung der VAU

Das HSM des E-Rezept-Fachdienstes MUSS sicherstellen, dass es der VAU den benötigten Persistenz-Schlüssel erst zur Verfügung stellt bzw. Signaturen für die VAU im Rahmen des Verbindungsaufbaus von Clients zur VAU erst erstellt nachdem der Verarbeitungskontext seine Integrität gegenüber dem HSM nachgewiesen hat. [<=]

A_18883 - HSM-Kryptographieschnittstelle und Persistenz-Schlüssel verfügbar nur für Verarbeitungskontexte der VAU

Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln, die auch Manipulationen durch den Anbieter des E-Rezept-Fachdienstes ausschließen, gewährleisten, dass nur integre Verarbeitungskontexte der VAU Zugriff auf die Kryptographieschnittstelle des HSM zur Nutzung des privaten Schlüsselmaterials für ihr Dienstzertifikat und zum Bezug des Persistenz-Schlüssels erhalten kann. [<=]

A_18884 - Aktivierung des Verarbeitungskontextes der VAU

Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln gewährleisten, dass schützenswerte Nutzdaten im Verarbeitungskontext erst nach Bezug des Persistenz-Schlüssels entschlüsselt und verarbeitet werden können. [<=]

A_18885 - Keine Speicherung der Persistenz-Schlüssel in Verarbeitungskontexten der VAU

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

A_18886 - Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU

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

A_18920 - Managementprozesse des HSM

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

5.1.4 Trennung von Session- und Request-Kontexten

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

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

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

A_19001 - Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU

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

A_19002 - Verfügbarkeit des Persistenz-Schlüssels in der VAU

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

A_19003 - Schutz des Persistenz-Schlüssels der VAU

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

Aus Sicherheitsgründen und aus Gründen der betrieblichen Stabilität müssen Verarbeitungsvorgänge und in ihnen möglicherweise auftretende Fehlerzustände voneinander isoliert werden. Ein konsistenter Systemzustand des E-Rezept-Fachdienstes muss auch nach einem schwerwiegenden Fehler in der Datenverarbeitung (z. B. aufgrund eines Hardware-Fehlers) wiederhergestellt werden können, ohne dass die Verfügbarkeit des Dienstes wesentlich eingeschränkt wird.

A_19005 - Fault Isolation und Wiederherstellung

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

A_19006 - Zuordnung von Verarbeitungskontexten und persistenten Datenstrukturen

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

5.2 Anforderungen an das E-Rezept-Frontend des Versicherten

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

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

A_18572 - Information zur Einsatzumgebung

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

A_18573 - Anzeige von Protokolldaten

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

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

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

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

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

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

5.3 Anforderungen an den Identity Provider

Dem Anbieter des IDP werden entsprechend dem Modularisierungskonzept in [gemSpec_DS_Anbieter] Module der Informationssicherheit und des Datenschutzes zugeordnet.

Folgende Anforderungen müssen durch den IDP zudem umgesetzt werden:

A_18861 - Gewährleistung des Schutzbedarfs

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

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

A_18862 - Transportverschlüsselte Übertragung von AuthN-Token

Der IDP MUSS sicherstellen, dass er nur transportverschlüsselt mit Clients kommuniziert. [≤]

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

A_18863 - Authentifizierungsverfahren mit hohem Sicherheitsstandard

Der IDP MUSS Authentifizierungsverfahren mit einem hohen Sicherheitsstandard anbieten. [≤]

A_18864 - Sicherheitsbetrachtungen berücksichtigen

Der IDP MUSS die Sicherheitsbetrachtungen der eingesetzten Standards berücksichtigen. [≤]

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

A_18860 - Zeitliche Begrenzung AuthN-Token

Der IDP MUSS AuthN-Token zeitlich begrenzen. [≤]

A_18858 - Ungültigkeit AuthN-Token nach Logout

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

A_18857 - Widerruf AuthN-Token durch Nutzer

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

A_18856 - Beschränkung auf erforderliche Informationen

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

A_18859 - Verbot der Profilbildung

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

5.4 Grenzen der Sicherheitsleistung der Fachanwendung E-Rezept

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

Leistungen, die durch die TI-Plattform erbracht werden:

- die Identifikation von TI-Teilnehmern,

- das Erstellen einer fortgeschrittenen und einer qualifizierten elektronischen Signatur und die Prüfung einer qualifizierten elektronischen Signatur.

Leistungen, die nicht durch die TI erbracht werden:

- 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 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 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.

6 Informationsmodell

6.1 Technisches Informationsmodell

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

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

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

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

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

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

Die E-Rezept-Nachricht beinhaltet eine Text-Mitteilung und alternativ den E-Rezept-Token oder Informationen für eine Anfrage zur Belieferung der Verordnung durch eine Apotheke.

Die folgende Abbildung ABB_SYSLERP_008 gibt einen informativen Überblick der relationalen Zusammenhänge der in der Fachanwendung verarbeiteten Informationsobjekte.

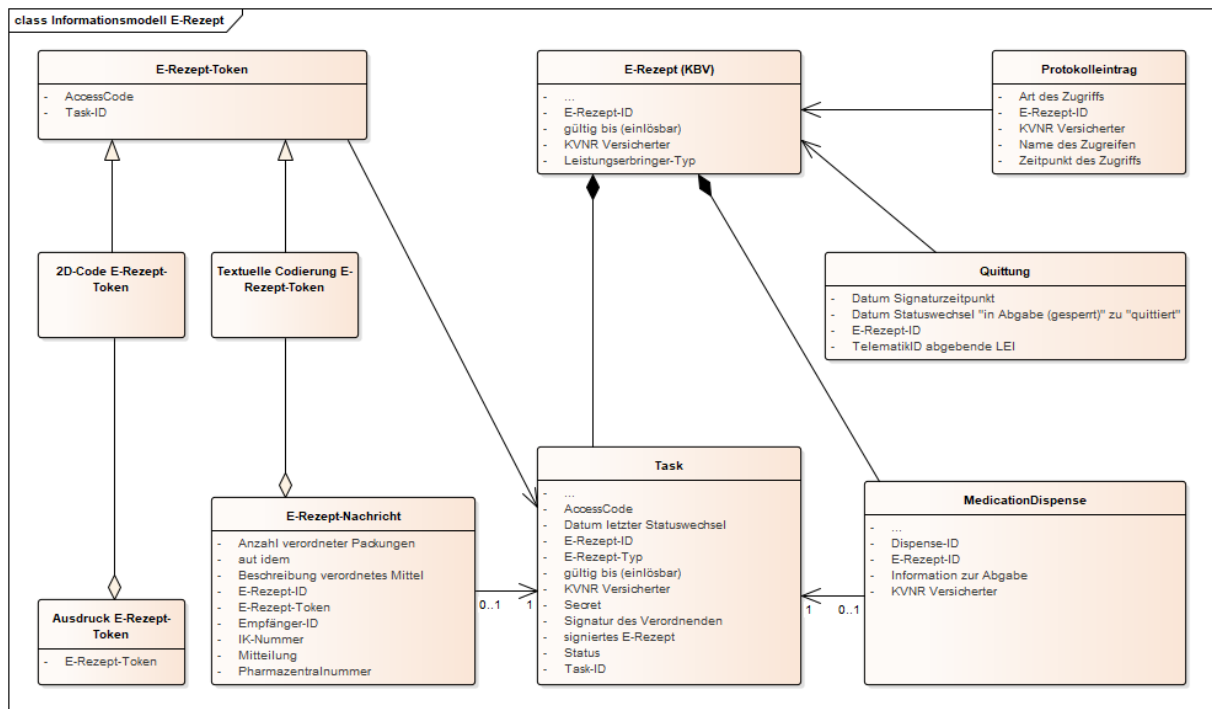


Abbildung 8: ABB_SYSLERP_008 Informationsmodell E-Rezept

6.2 Fachliches Informationsmodell

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

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

Diese fachlichen Inhalte sind nicht Teil des Scopes dieses Konzeptes.

7 Anhang – Verzeichnisse

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 Benutzeroberfläche
HBA	Heilberufsausweis
IDP	Identity Provider
KIM	Kommunikation im Medizinwesen
KIS	Krankenhausinformationssystem
KOM-LE	Kommunikation Leistungserbringer
KVNR	Krankenversichertennummer

LE	Leistungserbringer
LEI	Leistungserbringerinstitution
MVZ	Medizinisches Versorgungszentrum
NFC	Near Field Communication
OPB	Online-Produktivbetrieb
PDSG	Patientendaten-Schutz-Gesetz
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

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.

Dispensierinformation	Die Dispensierinformationen werden von der abgebenden LEI für den Versicherten über den E-Rezept-Fachdienst bereitgestellt. Sie enthalten Informationen über die Abgabe an den Versicherten. Diese können sich von den Informationen im Verordnungsdatensatz unterscheiden.
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 zugegriffen werden kann. 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 E-Rezept-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.
Quittung	Die Quittung ist ein durch den E-Rezept-Fachdienst erstellter und signierter Datensatz, welcher der abgebenden LEI eines E-Rezepts bereitgestellt wird. Sie dient als Nachweis, dass der Workflow ordnungsgemäß von dieser LEI abgeschlossen wurde.
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 Krankenversicherтенnummer (KVNR).

Allgemeine Begriffe finden sich in [gemGlossar].

7.3 Abbildungsverzeichnis

Abbildung 1: ABB_SYSLERP_001 Übersicht der Fachanwendung E-Rezept	8
Abbildung 2: ABB_SYSLERP_002 Fachliches Rollenmodell	11
Abbildung 3: ABB_SYSLERP_003 Funktionale Zerlegung E-Rezept	15

Abbildung 4: ABB_SYSLERP_009 Übersicht Identity Provider im Kontext E-Rezept.....	17
Abbildung 5: ABB_SYSLERP_004 Statusübergänge E-Rezept.....	21
Abbildung 6: ABB_SYSLERP_005 Anwendungsfälle E-Rezept	26
Abbildung 7: ABB_SYSLERP_006 Systemzerlegung E-Rezept	58
Abbildung 8: ABB_SYSLERP_008 Informationsmodell E-Rezept	99

7.4 Tabellenverzeichnis

Tabelle 1 : TAB_SYSLERP_048 Fachliche Rollen.....	11
Tabelle 2: TAB_SYSLERP_001 Kryptografische Identitäten der Akteure und ihre jeweilige Rolle.....	14
Tabelle 3 : TAB_SYSLERP_006 Beschreibung Status Task	22
Tabelle 4: TAB_SYSLERP_005 Anwendungsfall E-Rezepte erzeugen	28
Tabelle 5: TAB_SYSLERP_006 Anwendungsfall E-Rezept einstellen	29
Tabelle 6: TAB_SYSLERP_008 Anwendungsfall E-Rezept durch Verordnenden löschen...31	
Tabelle 7: TAB_SYSLERP_009 Anwendungsfall E-Rezepte durch Versicherten abrufen ...32	
Tabelle 8: TAB_SYSLERP_041 Anwendungsfall E-Rezept durch Vertreter abrufen.....33	
Tabelle 9: TAB_SYSLERP_010 Anwendungsfall E-Rezept durch Versicherten löschen	34
Tabelle 10: TAB_SYSLERP_011 Anwendungsfall Nachricht durch Versicherten übermitteln	36
Tabelle 11: TAB_SYSLERP_037 Anwendungsfall Nachrichten durch Versicherten empfangen	38
Tabelle 12: TAB_SYSLERP_061 Anwendungsfall Nachricht durch Versicherten löschen ..38	
Tabelle 13: TAB_SYSLERP_013 Anwendungsfall Protokolldaten abrufen.....40	
Tabelle 14: TAB_SYSLERP_036 Anwendungsfall Nachrichten durch Abgebenden empfangen	41
Tabelle 15: TAB_SYSLERP_055 Anwendungsfall Nachricht durch Abgebenden übermitteln	42
Tabelle 16: TAB_SYSLERP_062 Anwendungsfall Nachricht durch Abgebenden löschen...43	
Tabelle 17: TAB_SYSLERP_014 Anwendungsfall E-Rezept durch Abgebenden abrufen ...45	
Tabelle 18: TAB_SYSLERP_015 Anwendungsfall E-Rezept durch Abgebenden zurückgeben	46
Tabelle 19: TAB_SYSLERP_016 Anwendungsfall E-Rezept durch Abgebenden löschen ...48	
Tabelle 20: TAB_SYSLERP_017 Anwendungsfall Quittung abrufen.....49	
Tabelle 21: TAB_SYSLERP_057 Anwendungsfall Quittung erneut abrufen	51
Tabelle 22: TAB_SYSLERP_018 Anwendungsfall Dispensierdatensatz durch Abgebenden signieren	52
Tabelle 23: TAB_SYSLERP_045 AuthN-Token durch Versicherten anfordern	53

Tabelle 24: TAB_SYSLERP_046 AuthN-Token durch LEI anfordern	56
Tabelle 25: TAB_SYSLERP_019 Schnittstellen E-Rezept-Fachdienst.....	59
Tabelle 26: TAB_SYSLERP_021 Bedingungen zum Löschen von E-Rezepten	61
Tabelle 27: TAB_SYSLERP_040 Zugangsberechtigungen Operationen E-Rezept-Fachdienst	62
Tabelle 28: TAB_SYSLERP_002 Maximales Aufkommen nach Rezeptzeilen (Muster 16) 2018 an ausgewählten Wochentagen	64
Tabelle 29: TAB_SYSLERP_003 Gesamtes Aufkommen nach Rezeptzeilen (Muster 16) 2018 kumuliert nach Wochentagen	65
Tabelle 30: TAB_SYSLERP_022 Nutzung Schnittstellen eRp-FdV	66
Tabelle 31: TAB_SYSLERP_023 Nutzung Schnittstellen PS verordnende LEI	69
Tabelle 32: TAB_SYSLERP_024 Nutzung Schnittstellen PS abgebende LEI.....	70
Tabelle 33: TAB_SYSLERP_025 Operation E-Rezept-ID abrufen	76
Tabelle 34: TAB_SYSLERP_026 Operation E-Rezept einstellen.....	77
Tabelle 35: TAB_SYSLERP_027 Operation E-Rezept durch Verordnenden löschen	77
Tabelle 36: TAB_SYSLERP_028 Operation E-Rezept durch Abgebenden abrufen	78
Tabelle 37: TAB_SYSLERP_029 Operation E-Rezept durch Abgebenden löschen	79
Tabelle 38: TAB_SYSLERP_030 Operation E-Rezept durch Abgebenden zurückgeben	79
Tabelle 39: TAB_SYSLERP_031 Operation Quittung abrufen	80
Tabelle 40: TAB_SYSLERP_031 Operation Quittung erneut abrufen	80
Tabelle 41: TAB_SYSLERP_043 Operation E-Rezepte durch Versicherten abrufen	81
Tabelle 42: TAB_SYSLERP_032 Operation E-Rezept durch Vertreter abrufen	82
Tabelle 43: TAB_SYSLERP_033 Operation E-Rezept durch Versicherten löschen	82
Tabelle 44: TAB_SYSLERP_054 Operation Dispensierinformationen durch Versicherten abrufen	83
Tabelle 45: TAB_SYSLERP_058 Operation Dispensierinformation für ein einzelnes E- Rezept durch Versicherten oder Vertreter abrufen	83
Tabelle 46: TAB_SYSLERP_044 Operation E-Rezept-Nachricht einstellen	84
Tabelle 47: TAB_SYSLERP_050 Operation E-Rezept-Nachrichten abrufen.....	84
Tabelle 48: TAB_SYSLERP_060 Operation E-Rezept-Nachricht löschen	85
Tabelle 49: TAB_SYSLERP_051 Operation Zugriffsprotokolleinträge durch Versicherten abrufen	86
Tabelle 50: TAB_SYSLERP_052 Schutzbedarf der maßgeblichen Informationsobjekte	88
Tabelle 51: TAB_SYSLERP_053 Schutzbedarf der maßgeblichen Prozesse	89

7.5 Referenzierte Dokumente

7.5.1 Dokumente der gematik

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

7.5.2 Weitere Dokumente

[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