

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation E-Rezept-Anwendung des Versicherten

Version:	1.1.1
Revision:	621720
Stand:	28.04.2023
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_eRp_AdV

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	23.02.2022		freigegeben	gematik
1.1.0	07.12.2022		Einarbeitung gemäß Änderungsliste E- Rezept_Maintenance_22.3	gematik
1.1.1	28.04.2023		redaktionelle Änderungen	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes	5
1.1 Zielsetzung	5
1.2 Zielgruppe	5
1.3 Geltungsbereich	5
1.4 Abgrenzungen	5
1.5 Methodik	6
1.5.1 Hinweis auf offene Punkte	6
2 Systemüberblick	7
3 Systemkontext.....	8
3.1 Akteure und Rollen	8
3.2 Nachbarsysteme	8
4 Übergreifende Festlegungen	10
4.1 Datenschutz und Sicherheit.....	10
4.1.1 Anforderungen zum Herstellungsprozess	12
4.1.2 Unterstützung von Audits	12
4.2 Benutzeroberfläche	12
4.3 Konfiguration der E-Rezept-AdV	12
4.4 Logging	13
5 Funktionsmerkmale	14
5.1 Allgemein	14
5.1.1 Session-Verwaltung.....	14
5.1.2 Kommunikation mit Diensten der TI	15
5.1.3 Authentisierung des Nutzers für Dienste der TI	16
5.1.4 Verschlüsselte Kommunikation zur VAU des E-Rezept-Fachdienstes.....	17
5.1.5 Zertifikatsprüfung	17
5.1.5.1 Zertifikatsprüfung von Zertifikaten der TI.....	18
5.1.5.2 Zertifikatsprüfung von Internet-Zertifikaten.....	19
5.2 E-Rezept Anwendungsfälle in der E-Rezept-AdV.....	20
5.2.1 Anwendungsfälle.....	20
5.2.1.1 E-Rezepte einsehen	20
5.2.1.2 E-Rezepte löschen	22
5.2.1.3 Protokolldaten anzeigen	24
5.2.1.4 Nachrichten empfangen	25
5.2.1.5 Nachrichten löschen	26
5.2.2 Fehlerbehandlung	27
6 Informationsmodell	28

7 Verteilungssicht.....	31
8 Anhang A – Verzeichnisse.....	32
8.1 Abkürzungen	32
8.2 Glossar	32
8.3 Abbildungsverzeichnis.....	33
8.4 Tabellenverzeichnis	33
8.5 Referenzierte Dokumente.....	33
8.5.1 Dokumente der gematik.....	33
8.5.2 Weitere Dokumente.....	34

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps E-Rezept-Anwendung des Versicherten.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller von Produkten des Produkttypen E-Rezept-Anwendung des Versicherten (gematik) sowie an Hersteller und Anbieter von weiteren Produkttypen der Fachanwendung E-Rezept.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastuktur 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. Produkttypsteckbrief, Leistungsbeschreibung, ...) festgelegt und bekanntgegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps E-Rezept-Anwendung des Versicherten verzeichnet.

Diese Spezifikation beschreibt Anforderungen zu den Aspekten Sicherheit, Interoperabilität und Funktionalität. Die konkrete Ausgestaltung der Benutzeroberfläche (GUI) und der Benutzerführung (UX) wird während der Entwicklung festgelegt und ist nicht Teil dieser Spezifikation.

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

In diesem Dokument werden auch Anforderungen aus dem Dokument Spezifikation E-Rezept-Frontend des Versicherten [gemSpec_eRp_FdV] referenziert. Sie sind im Titel mit "E-Rezept-FdV" bezeichnet. **Diese Anforderungen gelten sowohl für das E-Rezept-Frontend des Versicherten als auch für die E-Rezept-Anwendung des Versicherten.**

Anforderungen, die sich nur auf die E-Rezept-AdV beziehen, werden im Titel der Anforderungen mit "E-Rezept-AdV:" bezeichnet.

User Stories

Eine User Story ist eine in Alltagssprache formulierte Software-Anforderung. Sie ist bewusst kurz gehalten und umfasst in der Regel nicht mehr als zwei Sätze. User Stories werden im Rahmen der agilen Softwareentwicklung zusammen mit Akzeptanztests zur Spezifikation von Anforderungen eingesetzt. [Wikipedia:User Story]

Aus diesem Grund kann in den User Stories eine abweichende Terminologie genutzt werden, welche für den Leser nachvollziehbar (bspw. Patient = Versicherter) ist.

1.5.1 Hinweis auf offene Punkte

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

Beispiel für einen offenen Punkt.

2 Systemüberblick

Die E-Rezept-Anwendung des Versicherten (E-Rezept-AdV) ist eine Anwendung für den Versicherten, welche die für die Wahrnehmung der Rechte der informationelle Selbstbestimmung in der Fachanwendung E-Rezept notwendigen Funktionalitäten bündelt und dezentrale Fachlogik der Fachanwendung E-Rezept ausführt.

Ausführungsumgebung der E-Rezept-AdV ist ein stationäres Gerät des Versicherten (GdV). Es steht unter alleiniger Kontrolle des Versicherten. Dem Versicherten obliegt es, durch geeignete Maßnahmen die Sicherheit der Daten zu stärken.

Unterschiede zum E-Rezept-FdV bestehen in der Ausführungsumgebung und im reduzierten Umfang der für den Nutzer ausführbaren Anwendungsfälle.

3 Systemkontext

3.1 Akteure und Rollen

Im Systemkontext der E-Rezept-AdV interagieren verschiedene Akteure (aktive Komponenten) in unterschiedlichen Rollen mit der E-Rezept-AdV.

Tabelle 1 : TAB_AdVERP_001 – Akteure und Rollen

Akteur	Rolle	Beschreibung
Nutzer der E-Rezept-AdV	Versicherter	primärer Anwender, Ausführen von fachlichen Anwendungsfällen mit Zugriff auf den E-Rezept-Fachdienst
Ausführungsumgebung	Gerät des Versicherten	Betriebs-/Ablaufumgebung der E-Rezept-AdV ein stationäres Gerät
Hersteller E-Rezept-AdV (gematik)	organisatorisch, kein Akteur in der Ausführung von E-Rezept-Anwendungsfällen	Der Hersteller E-Rezept-AdV stellt im Handbuch Informationen bereit bezüglich: <ul style="list-style-type: none">Anforderungen an die Ausführungsumgebung Der Hersteller E-Rezept-AdV erfüllt sicherheitstechnische Anforderungen zum Herstellungsprozess.

3.2 Nachbarsysteme

Die von der E-Rezept-AdV direkt erreichbaren Produkttypen der TI sind

- Identity Provider (IDP)
- E-Rezept-Fachdienst
- elektronische Gesundheitskarte (eGK)

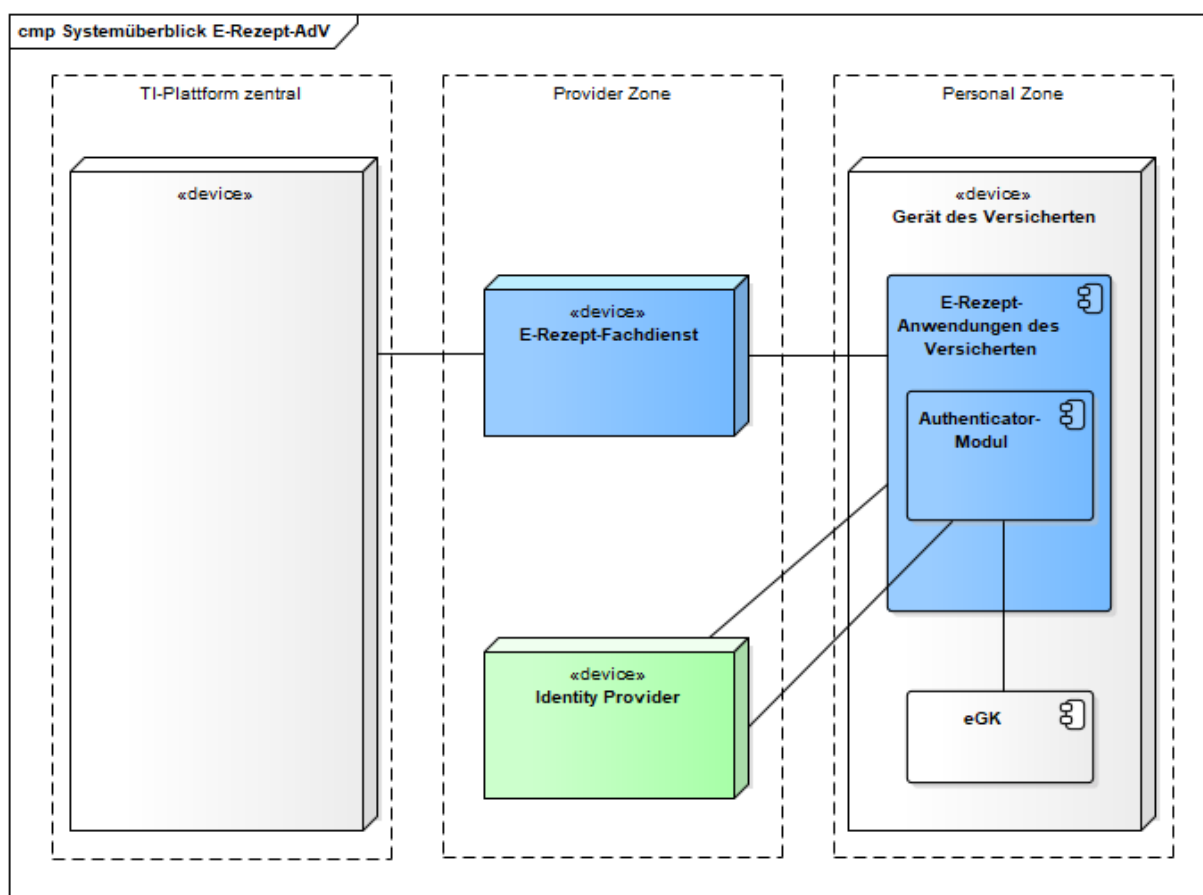


Abbildung 1 : Systemüberblick E-Rezept-AdV

Identity Provider

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

E-Rezept-Fachdienst

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

Authenticator-Modul

Das Authenticator-Modul ist eine logische Komponente in der E-Rezept-AdV. Das Authenticator-Modul kapselt funktionale Anteile des Authentifizierungsprozesses und die Kommunikation mit der Smart Card des Nutzers. Im Authentifizierungsprozess übernimmt das Authenticator-Modul die Rolle Authenticator-Modul und das E-Rezept-AdV die Rolle Anwendungsfrontend. Siehe [gemSpec_IDP_FD]. Für die Authentisierung mittels eGK greift die E-Rezept-AdV über die kontaktbehaftete Schnittstelle oder mittels des Funkstandards Near Field Communication (NFC) zur drahtlosen Datenübertragung auf die kontaktlose Schnittstelle auf die eGK zu. Das bedeutet für den Nutzer, dass er einen Kartenleser benötigt.

4 Übergreifende Festlegungen

4.1 Datenschutz und Sicherheit

In diesem Kapitel werden übergreifende Anforderungen beschrieben, die sich aus den Themenfeldern Datenschutz und Sicherheit ergeben.

A_19176 - E-Rezept-FdV – Nutzungshinweise

Der Hersteller bzw. der Anbieter des E-Rezept-FdV MUSS den Nutzer über die Annahmen und Anforderungen seines Produktes an das Gerät, auf dem das E-Rezept-FdV läuft, sowie über den Bezug des Produkts aus vertrauenswürdigen App Stores informieren. [<=]

A_21359 - E-Rezept-AdV – Vertrauenswürdige Bezugsquellen

Der Hersteller bzw. der Anbieter der E-Rezept-AdV MUSS es den Versicherten ermöglichen, die E-Rezept-AdV aus vertrauenswürdigen Quellen zu beziehen. [<=]

A_21364 - E-Rezept-AdV – Information über Bezugsquellen

Der Hersteller bzw. der Anbieter der E-Rezept-AdV MUSS die Versicherten darüber informieren, aus welchen vertrauenswürdigen Quellen sie die E-Rezept-AdV beziehen können und wie diese verifiziert werden können. [<=]

A_21365 - E-Rezept-AdV – Authentifizierung der Bezugsquelle bei Erstbezug

Der Hersteller bzw. der Anbieter der E-Rezept-AdV MUSS sicherstellen, dass der Versicherte bei Erstbezug einer E-Rezept-AdV die Authentizität der vertrauenswürdigen Bezugsquelle verifizieren kann. [<=]

Hinweis: Beim Erstbezug der E-Rezept-AdV kann die Prüfung der Authentizität der Quelle noch nicht durch die E-Rezept-AdV selbst erfolgen. Dies kann z.B. über eine TLS-Serverauthentifizierung der Bezugsquelle oder das Einstellen der E-Rezept-AdV in einen vertrauenswürdigen Store erreicht werden.

A_21366 - E-Rezept-AdV – Technische Authentifizierung der Update-Bezugsquellen

Die E-Rezept-AdV MUSS Updates ausschließlich von bekannten, vertrauenswürdigen und authentisierten Quellen laden. [<=]

A_21367 - E-Rezept-AdV - lokale Datenverarbeitung

Die E-Rezept-AdV MUSS sicherstellen, dass die Klartextverarbeitung aller personenbezogenen bzw. sicherheitsrelevanten Daten eines Versicherten lokal auf dem Gerät des Versicherten erfolgt. [<=]

A_21368 - E-Rezept-AdV – Ausführung nur von zugelassenen Code

Die E-Rezept-AdV MUSS sicherstellen, dass nur von der gematik zugelassener Code ausgeführt wird. Dies gilt auch für dynamisch geladenen Code. [<=]

A_21369 - E-Rezept-AdV – Berücksichtigung OWASP ASVS

Der Hersteller der E-Rezept-AdV MUSS die E-Rezept-AdV unter Berücksichtigung des jeweils aktuellen OWASP Application Security Verification Standard Level 3 entwickeln und für jede Anforderung dokumentieren, wie sie umgesetzt ist bzw. ob sie ggf. für die E-Rezept-AdV nicht zutrifft. [<=]

A_19480 - E-Rezept-FdV – Schutz der Session-Daten

Das E-Rezept-FdV DARF Session-Daten (bspw. ACCESS_TOKEN und ID_TOKEN) NICHT an Dritte, außer im Rahmen der in den Anwendungsfällen spezifizierten Kommunikation, weitergeben. [<=]

A_20184 - E-Rezept-FdV - Speicherung der Session-Daten

Das E-Rezept-FdV DARF NICHT Session-Daten (bspw. ACCESS_TOKEN und ID_TOKEN) unverschlüsselt auf permanenten Speichermedien ablegen. [≤]

A_20185 - E-Rezept-FdV - Session-Timeout

Das E-Rezept-FdV MUSS die Session nach einem angemessenen Session-Timeout, gemäß aktuellen Best-Practice-Empfehlungen, aktiv beenden. [≤]

A_20186 - E-Rezept-FdV - Session-Daten löschen

Das E-Rezept-FdV MUSS beim Beenden einer Session die Session-Daten (bspw. ACCESS_TOKEN und ID_TOKEN) sicher löschen. [≤]

A_19179 - E-Rezept-FdV – Qualität verwendeter Schlüssel

Das E-Rezept-FdV MUSS sicherstellen, dass die von ihm erzeugten Schlüssel eine ausreichende Qualität besitzen. [≤]

Für Festlegungen zur Schlüsselerzeugung siehe [gemSpec_Krypt#GS-A_4368].

Um die geforderte Entropie zu erreichen, können Informationen von zusätzlichen Quellen (bspw. Internet, Sensoren des Geräts) zusammengeführt werden.

A_19979 - E-Rezept-FdV – Kein Zugriff von Diensten Dritter auf personenbezogene medizinische Daten

Das E-Rezept-FdV DARF Diensten Dritter NICHT Zugriff auf personenbezogene medizinische Daten geben. [≤]

A_19181-01 - E-Rezept-FdV – Privacy bei default

Das E-Rezept-FdV MUSS bei Konfigurationsmöglichkeiten die Voreinstellung wählen, so dass nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. [≤]

A_19182 - E-Rezept-FdV – Sicherheitsrisiken von Software-Bibliotheken minimieren

Das E-Rezept-FdV MUSS Maßnahmen umsetzen, um die Auswirkung von unentdeckten Schwachstellen in benutzten Software-Bibliotheken zu minimieren. [≤]

Hinweis: Beispielsmaßnahmen sind in [OWASP Proactive Control#C2] zu finden. Das gewählte Verfahren muss die gleiche Wirksamkeit aufweisen wie die Kapselung gemäß [OWASP Proactive Control#C2 Punkt 4].

A_19980 - E-Rezept-FdV – Information über Datenweitergabe an Dienste Dritter

Das E-Rezept-FdV MUSS den Versicherten darauf hinweisen, dass durch die Nutzung von Diensten Dritter Daten an diese abfließen und welche Daten dies sind. [≤]

Hinweis: Dienste Dritter, an die andere Daten als personenbezogene medizinische Daten weitergeleitet werden können, sind z.B. Kartendienste oder der Arzneimitteldatenbanken. Näheres hierzu regelt die Rechtsverordnung nach § 360 (5) PDSG.

A_19981 - E-Rezept-FdV – Zustimmung über Datenweitergabe an Dienste Dritter

Das E-Rezept-FdV MUSS vor einer Weitergabe von Daten an Dienste von Dritten einmalig das Einverständnis des Versicherten einholen (OPT-IN). [≤]

A_19982 - E-Rezept-FdV – Rücknahme der Zustimmung über Datenweitergabe an Dienste Dritter

Das E-Rezept-FdV MUSS es dem Versicherten ermöglichen das Einverständnis zur Weitergabe von Daten an Dienste von Dritten zu widerrufen und ihn dabei über eventuelle Einschränkungen in der Funktionalität informieren. [≤]

Hinweis: Nach dem Widerruf darf das E-Rezept-AdV keine Daten mehr an Dienste von Dritten weitergeben.

A_19983 - E-Rezept-FdV – Keine Nutzung von Diensten Dritter mit bekannten Schwachstellen

Das E-Rezept-FdV DARF NICHT Dienste von Dritten nutzen, wenn diese bekannte Schwachstellen besitzen. [≤]

A_19984 - E-Rezept-FdV – Validierung eingehender Daten von Diensten Dritter

Das E-Rezept-FdV SOLL eingehende Daten von Diensten Dritter validieren. [≤]

A_19186 - E-Rezept-FdV – Sichere Speicherung lokaler Daten

Das E-Rezept-FdV MUSS Daten lokal sicher speichern, so dass keine andere App auf demselben Gerät unbefugt Zugriff auf die Daten hat. Insbesondere MUSS das E-Rezept-FdV Zugriffsschlüssel verschlüsselt ablegen. Außerdem MUSS das E-Rezept-FdV sicherstellen, dass vertrauliche Daten nicht vom Betriebssystem an anderen Ablageorten zwischengespeichert werden. [≤]

A_19187 - E-Rezept-FdV – Authentisierung vor Zugang zum Dienst

Das E-Rezept-FdV DARF NICHT eine Verbindung zum E-Rezept-Fachdienst aufbauen, wenn es keinen ACCESS_TOKEN vom IDP erhalten hat. [≤]

A_19188 - E-Rezept-FdV – Sichere Deinstallation

Das E-Rezept-FdV MUSS die von ihm verarbeiteten Daten so speichern, dass die Daten bei einer Deinstallation des E-Rezept-FdV mit gelöscht werden. [≤]

Hinweis: Zu diesen Daten gehören u.a. Session-Daten, Cashes, Schlüssel, E-Rezept-Inhaltsdaten.

4.1.1 Anforderungen zum Herstellungsprozess

Der Hersteller der E-Rezept-AdV muss die Anforderungen aus dem Abschnitt "Sicherer Softwareentwicklungsprozess" des Dokuments [gemSpec_DS_Hersteller] erfüllen.

4.1.2 Unterstützung von Audits

Der Hersteller der E-Rezept-AdV muss die Anforderungen aus dem Abschnitt "Unterstützung von Audits" des Dokuments [gemSpec_DS_Hersteller] erfüllen.

4.2 Benutzeroberfläche

Die Benutzeroberfläche, welche durch den Versicherten genutzt wird, um E-Rezept-Anwendungsfälle auszuführen, ist Teil der E-Rezept-AdV.

Ausführungen zur visuellen Darstellung, Usability und zu geltenden technischen Normen werden im Dokument [gemSpec_eRp_FdV] beschrieben.

Die konkrete Ausgestaltung der GUI und der Benutzerführung wird während der Entwicklung festgelegt und in diesem Dokument nicht weiter behandelt.

4.3 Konfiguration der E-Rezept-AdV

Im Folgenden sind Konfigurationsparameter der Anwendung beschrieben, deren Werte für die Nutzung der Schnittstellen benötigt werden. Darüber hinaus kann der Hersteller der E-Rezept-AdV zusätzliche Konfigurationsparameter definieren.

A_20647 - E-Rezept-AdV: Parameter speichern und laden

Die E-Rezept-AdV MUSS die Parameter aus TAB_AdVERP_002 persistent speichern und bei der Initialisierung laden.

Tabelle 2 : TAB_AdVERP_002 – Konfiguration E-Rezept-AdV

Parameter	Beschreibung	Wertebereich (Default Wert)
Option Card Access Number (CAN) zur Authentisierung	falls eine Authentifizierung mittels eGK über die NFC-Schnittstelle unterstützt wird: Wahlmöglichkeit, ob die CAN der eGK in der E-Rezept-AdV gespeichert werden soll	ja/nein Default: nein
Card Access Number	falls Option für Speichern der CAN aktiviert wurde	Default: leer
Option Usability Tracking	falls Usability Tracking durch die E-Rezept-AdV unterstützt werden kann: Wahlmöglichkeit, ob der Nutzer Usability Tracking unterstützen möchte	ja/nein Default: nein
Option Crash Reporting	falls Crash Reporting durch die E-Rezept-AdV unterstützt werden kann: Wahlmöglichkeit, ob der Nutzer Crash Reporting unterstützen möchte	ja/nein Default: nein

[<=]

A_20678 - E-Rezept-AdV: Konfigurationsparameter verwalten

Die E-Rezept-AdV MUSS es dem Nutzer ermöglichen, die Parameter aus TAB_AdVERP_002 zu verwalten (anzeigen, ändern, löschen).[<=]

4.4 Logging

Die E-Rezept-AdV kann Protokolldateien schreiben, die eine Analyse technischer Vorgänge erlauben. Diese Protokolldateien sind dafür vorgesehen, aufgetretene Fehler zu identifizieren, die Performance zu analysieren und interne Abläufe zu beobachten.

Ein Logging der E-Rezept-AdV auf Geräten des Versicherten ist im Betrieb nicht vorgesehen, da die Protokolldaten zur Auswertung nicht erreichbar sind. Die Protokollierung auf einem externen Dienst ermöglicht eine Auswertung und kann die Fehlersuche unterstützen (siehe Usability Tracking und Crash Reporting). Für Testzwecke soll ein Logging zur Fehleranalyse möglich sein.

A_19682 - E-Rezept-FdV - Kein Logging auf Geräten des Versicherten

Das E-Rezept-FdV MUSS für den Betrieb auf dem Gerät des Versicherten das Logging deaktiviert haben.[<=]

5 Funktionsmerkmale

5.1 Allgemein

5.1.1 Session-Verwaltung

Eine Authentisierung gegenüber der TI nach dem Start der Anwendung erfolgt automatisch.

Eine **TI-Session** bezeichnet den Zeitraum von der Authentisierung gegenüber der TI bis zum Ablauf der Authentisierung.

Die Authentisierung gegenüber der TI erfolgt über ein Authentisierungsmodul, welche Bestandteil der E-Rezept-AdV ist oder als eigenständige Komponente ebenfalls auf dem Gerät des Versicherten (GdV) installiert ist. Das Authentisierungsmodul unterstützt in der ersten Stufe eine Authentisierung des Versicherten mit der eGK, wobei der Versicherte die PIN eingeben muss.

Der Versicherte weist sich gegenüber der TI mit der Identität der eGK aus.

Die Anbindung der eGK an das GdV kann mittels kontaktloser NFC-Schnittstelle oder der kontaktbehafteten Schnittstelle erfolgen.

Die Authentisierung des Nutzers erfolgt mittels eGK, MRPIN.home und, falls die NFC Schnittstelle genutzt wird, der CAN.

Die Authentisierungsdauer einer TI-Session beträgt maximal 12 Stunden ab dem Zeitpunkt der Erstellung des Authentisierungstokens. Wird die Anwendung durch den Nutzer aktiv beendet, werden die Session-Daten gelöscht und eine erneute Authentisierung wird erforderlich.

A_20117 - E-Rezept-FdV: Authentisierung wenn kein gültiger ACCESS_CODE

Das E-Rezept-FdV MUSS, falls für den Aufruf des E-Rezept-Fachdienstes kein gültiger ACCESS_TOKEN sowie kein gültiger ACCESS_CODE vorliegt, die TI-Session starten.[<=]

A_20035 - E-Rezept-FdV: TI-Session starten

Das E-Rezept-FdV MUSS zum Start der TI-Session die Aktivität "Authentisierung des Nutzers gegenüber TI" ausführen.[<=]

Für die Aktivität "Authentisierung des Nutzers gegenüber TI" siehe Kapitel 5.1.3.

A_19481 - E-Rezept-FdV: Löschen der App-Session-Daten

Das E-Rezept-FdV MUSS zum Beenden der App-Session die ACCESS_TOKEN und den ACCESS_CODE sicher löschen.[<=]

A_19482 - E-Rezept-FdV: Beenden der TI-Session

Das E-Rezept-FdV MUSS zum Beenden der TI-Session

- bestehende TLS-Verbindungen zu den Diensten der TI abbauen,
- die Schlüssel für die sichere Verbindung zur VAU des E-Rezept-Fachdienstes löschen und
- alle ACCESS_TOKEN und ACCESS_CODE löschen.

[<=]

5.1.2 Kommunikation mit Diensten der TI

Die E-Rezept-AdV nutzt TLS-Verbindungen für die Kommunikation zu den Diensten der TI. Es verbindet sich mit dem E-Rezept-Fachdienst und einem Identity Provider.

A_19438-01 - E-Rezept-FdV: Adressierung E-Rezept-Fachdienst

Das E-Rezept-FdV MUSS für die Kommunikation mit dem E-Rezept-Fachdienst die vom E-Rezept-Fachdienst im Internet bereitgestellten Schnittstellen nutzen. [\leq]

Für die URLs der Schnittstellen siehe [gemSpec_FD_eRP#A_21782-*].

A_19747 - E-Rezept-FdV: Endpunkt Schnittstelle E-Rezept-Fachdienst

Das E-Rezept-FdV MUSS die URL für die Kommunikation mit dem E-Rezept-Fachdienst gemäß `https://<FQDN aus DNS Lookup>:443/<path>` bilden. [\leq]

Die Informationen zu den Endpunkten des Identity Providers ermittelt die E-Rezept-AdV aus dem Discovery Document. Siehe auch [[gemSpec_IDP_Frontend#A_20512 - Regelmäßiges Einlesen des Discovery Document](#)]. Das Discovery Document ist vom IDP-Dienst unter der URL `/.well-known/openid-configuration` abrufbar.

A_19215 - E-Rezept-FdV: Kommunikation über TLS-Verbindung

Das E-Rezept-FdV MUSS mit den Diensten der TI ausschließlich über TLS kommunizieren. [\leq]

Für Informationen zur Nutzung der TLS siehe [gemSpec_Krypt].

A_20206-01 - E-Rezept-FdV: Kommunikation über TLS-Verbindung mit Diensten Dritter

Das E-Rezept-FdV MUSS mit den Diensten Dritter ausschließlich über TLS kommunizieren. [\leq]

A_19216 - E-Rezept-FdV: Unzulässige TLS-Verbindungen ablehnen

Das E-Rezept-FdV MUSS bei jedem Verbindungsaufbau den Dienst der TI anhand seines TLS-Zertifikats authentifizieren und MUSS die Verbindungen ablehnen, falls die Authentifizierung fehlschlägt. [\leq]

A_20014-01 - E-Rezept-FdV: HTTP-Header user-agent

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

`<Produktname>/<Produktversion> <Herstellername>/<client_id>` gemäß der Produktidentifikation befüllen:

- `<client_id>` gemäß Registrierung bei der gematik.

[\leq]

Für Informationen zur Produktidentifikation siehe [gemSpec_OM].

A_21553 - E-Rezept-FdV: Organisatorische Registrierung

Der Hersteller des E-Rezept-FdV MUSS organisatorische Prozesse für API-KEYs für die Kommunikation zum E-Rezept-Fachdienst unterstützen. [\leq]

A_21554 - E-Rezept-FdV: API-KEY speichern

Das E-Rezept-FdV MUSS den von der gematik vergebenen API-KEY im E-Rezept-FdV verwahren. [\leq]

Der Wechsel des API-KEY erfolgt mit einer neuen Version der E-Rezept-AdV.

A_21555 - E-Rezept-FdV - Verwendung API-KEY

Das E-Rezept-FdV MUSS in allen HTTP-Requests an den E-Rezept-Fachdienst im äußeren HTTP-Request den HTTP-Header "X-api-key" mit dem von der gematik übermittelten API-KEY befüllen. [\leq]

Der HTTP-Header X-api-key wird im äußeren HTTP-Request, d.h. außerhalb der Verschlüsselung des VAU-Transports, gesendet.

A_21567 - E-Rezept-FdV: HTTP-Header X-erp-user

Das E-Rezept-FdV MUSS in alle Anfragen an den E-Rezept-Fachdienst im äußeren HTTP-Request den HTTP-Header "X-erp-user" mit dem Wert "v" einfügen. [<=]

A_21570 - E-Rezept-FdV: HTTP-Header X-erp-resource

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

Tabelle 3 : TAB_FdVERP_019 - HTTP-Header "X-erp-resource"

Operation	X-erp-resource
DELETE /Communication/<id>	Communication
GET /AuditEvent/	AuditEvent
GET /AuditEvent/<id>	AuditEvent
GET /Communication/	Communication
GET /Communication/<id>	Communication
GET /Device/	Device
GET /MedicationDispense/	MedicationDispense
GET /MedicationDispense/<id>	MedicationDispense
GET /metadata/	metadata
GET /Task/	Task
GET /Task/<id>	Task
POST /Task/<id>/\$abort	Task

5.1.3 Authentisierung des Nutzers für Dienste der TI

Der Nutzer authentisiert sich für Zugriffe auf Dienste der TI gegenüber der TI. Die E-Rezept-AdV erhält bei erfolgreicher Authentisierung einen Authentisierungstoken (ACCESS_TOKEN), welcher für die Authentisierung bei den Diensten der TI weitergeleitet wird.

A_20167 - E-Rezept-FdV: Authentisierung - Rolle Authenticator-Modul und Anwendungsfrontend

Das E-Rezept-FdV MUSS für den Zugriff auf Dienste der TI, wenn kein gültiger ACCESS_TOKEN vorliegt, sich gegenüber einem Identity Provider der TI in den Rollen Authenticator-Modul und Anwendungsfrontend Applikation authentisieren. [<=]

Für Informationen zum Ablauf der Authentisierung siehe [gemSpec_IDP_Dienst] und [gemSpec_IDP_Frontend].

5.1.4 Verschlüsselte Kommunikation zur VAU des E-Rezept-Fachdienstes

Die Kommunikation zum E-Rezept-Fachdienst wird zusätzlich zu TLS über einen sicheren Kanal zwischen die E-Rezept-AdV und der Vertrauenswürdigen Ausführungsumgebung (VAU) im E-Rezept-Fachdienst gesichert.

A_19740-01 - E-Rezept-FdV: Umsetzung sicherer Kanal zur VAU des E-Rezept-Fachdienstes

Das E-Rezept-FdV MUSS für alle Anfragen an den E-Rezept-Fachdienst für

- die Abfrage des capability statement
- den Zugriff auf `Task`, `MedicationDispense`, `AuditEvent` oder `Communication` Ressourcen

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

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

5.1.5 Zertifikatsprüfung

Die E-Rezept-AdV verwendet bei den in TAB_FdVERP_017 dargestellten Aktivitäten Zertifikate.

Tabelle 4 : TAB_FdVERP_017 – Zertifikatsnutzung

Aktivität	Zertifikat der TI	Zertifikatstyp	Rollen-OID	Nutzung
TLS-Verbindungsaufbau zum E-Rezept-Fachdienst	nein	TLS Internet Zertifikat	n/a	aktiv
TLS-Verbindungsaufbau zum IDP	nein	TLS Internet Zertifikat	n/a	aktiv

Aktivität	Zertifikat der TI	Zertifikatstyp	Rollen-OID	Nutzung
Aufbau sicherer Kanal zur VAU des E-Rezept-Fachdienstes	ja	C.FD.ENC	oid_erp_vau	aktiv
Signaturzertifikat Fachdienst	ja	C.FD.SIG	oid_erezept	aktiv

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

A_19739 - E-Rezept FdV: verpflichtende Zertifikatsprüfung

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

Das E-Rezept-FdV MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können. [≤]

"Ein Zertifikat aktiv verwenden" bedeutet im Sinne von A_19739, dass eine E-Rezept-AdV einen dort aufgeführten öffentlichen Schlüssel innerhalb einer kryptografischen Operation (Signaturprüfung, Verschlüsselung, Signaturprüfung von öffentlichen (EC)DH-Schlüsseln etc.) nutzt. Erhält die E-Rezept-AdV ein Datenobjekt, in dem Signaturen und Zertifikate enthalten sind und behandelt es dieses als opakes Datenobjekt, ohne die Zertifikate darin gesondert zu betrachten, dann verwendet die E-Rezept-AdV diese Zertifikate im Sinne von A_19739 passiv.

5.1.5.1 Zertifikatsprüfung von Zertifikaten der TI

In der folgenden Anforderung sind die Schritte zum Prüfen eines Zertifikates der TI beschrieben. In den Schritten werden TUC_PKI_* referenziert. Sie dienen als Rahmen für den Ablauf der Prüfschritte. Die TUC_PKI_* sind in dieser Afo nicht normativ umzusetzen.

A_20032-01 - E-Rezept-FdV: Prüfung TI-Zertifikate

Das E-Rezept-FdV MUSS bei der Prüfung von X.509-Zertifikaten der TI folgende Prüfschritte durchlaufen.

1. Prüfung der zeitlichen Gültigkeit des Zertifikats auf Basis der aktuellen Systemzeit (orientiert an [gemSpec_PKI#TUC_PKI_002])
2. Ist das Zertifikat kryptographisch (Signaturprüfung) rückführbar auf ein CA-Zertifikat aus einer authentischen und integeren und zeitlich gültigen, vertrauenswürdigen Zertifikatskette? (siehe Festlegungen in [gemSpec_Krypt#7.2.2] "Client-seitige Prüfung der E-Rezept-VAU-Identität")
3. Prüfung auf den für den Anwendungsfall korrekten Zertifikatstyp gemäß TAB_FdVERP_017. Die OID des Zertifikatstyps gemäß [gemSpec_OID] muss in der Extension CertificatePolicies enthalten sein.
4. Falls das Zertifikat für den Aufbau des sicheren Kanals zur VAU verwendet wird (VAU-Zertifikat innerhalb des VAU-Protokolls, vgl.

[gemSpec_Krypt#Kommunikationsprotokoll zwischen VAU und E-Rezept-Clients]], so MUSS die Rolle "oid_erp-vau" gemäß [\[gemSpec_OID#GS-A_4446\]](#) im EE-Zertifikat aufgeführt sein (analog [gemSpec_PKI#TUC_PKI_009]). Falls nein, MUSS das Zertifikat für den Aufbau des sicheren Kanals zur VAU abgelehnt werden.

5. Falls das Zertifikat ein EE-Zertifikat ist: Ermittlung der OCSP-Statusinformation. Ist das Zertifikat nicht gesperrt (Status "good" [RFC-6960#2.2 Response]) (vgl. A_15869)? Eine OCSP-Antwort KANN lokal maximal 4 Stunden gecacht und als Prüfgrundlage verwendet werden.
Die Prüfung ist analog gemSpec_PKI#TUC_PKI_006 mit den Parametern Referenzzeitpunkt=Systemzeit, OCSP-Graceperiod=4 Stunden.
6. Prüfung der Extensions KeyUsage und ExtendedKeyUsage auf die richtige Belegung gemäß dem Anwendungsfall (orientiert an [gemSpec_PKI#TUC_PKI_018] Schritt 2).

Führt einer der Prüfschritte nicht zu einem positiven Prüfergebnis, so MUSS das Zertifikat abgelehnt werden und die weitere Verarbeitung des Zertifikats oder der Attribute darin abgelehnt werden.

Das E-Rezept-FdV muss die referenzierten technischen Use Cases (TUC_PKI_*) aus [gemSpec_PKI] im Rahmen dieser Anforderung nicht normativ umsetzen. [≤]

Für die Prüfung des Online-Status von Zertifikaten der TI wird die Schnittstelle I_OCSP_Status_Information genutzt. Siehe [gemSpec_PKI#9]. Die Schnittstelle wird durch den E-Rezept-Fachdienst angeboten. Siehe auch [gemSpec_FD_eRp#A_20024 - E-Rezept-Fachdienst - Bereitstellung OCSP-Forwarder].

Der E-Rezept-Fachdienst stellt neben der TSL eine zweite Lösung bereit, im E-Rezept-AdV einen Vertrauensraum auf Basis eines Root-CA-Zertifikats aufzubauen. Diese Lösung besteht in einer JSON-Struktur, die eine Zertifikatskette (CA-Zertifikate, Cross-Zertifikate) hin zur dem E-Rezept-FdV bekannten Root-CA enthält. Die JSON-Struktur ist einfacher zu verarbeiten. Die Anforderungen und Schritte zum Aufbau dieser vertrauenswürdigen Zertifikatskette finden sich in der Spezifikation [gemSpec_Krypt] in Abschnitt 7.2.2 "Client-seitige Prüfung der E-Rezept-VAU-Identität".

5.1.5.2 Zertifikatsprüfung von Internet-Zertifikaten

Folgende Vorgaben gelten für die Prüfung von Internet-Zertifikaten.

A_20033 - E-Rezept-FdV: Prüfung Internet-Zertifikate

Das E-Rezept-FdV MUSS für die Prüfung des internetseitigen Zertifikats von Diensten der TI das Zertifikat auf ein CA-Zertifikat einer CA, die die "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (<https://cabforum.org/baseline-requirements-documents/>) erfüllt, kryptographisch (Signaturprüfung) zurückführen können. Ansonsten MUSS es das Zertifikat als "ungültig" bewerten.

Das E-Rezept-FdV MUSS die zeitliche Gültigkeit des Zertifikats prüfen. Falls diese Prüfung negativ ausfällt, muss es das Zertifikat als "ungültig" bewerten. [≤]

Hinweis: Der erste Teil von A_20033 ist gleichbedeutend damit, dass das CA-Zertifikat im Zertifikats-Truststore eines aktuellen Webbrowsers ist.

5.2 E-Rezept Anwendungsfälle in der E-Rezept-AdV

In diesem Kapitel wird die Umsetzung der im systemspezifischen Konzept [gemSysL_eRp] spezifizierten Anwendungsfälle in der E-Rezept-AdV beschrieben.

5.2.1 Anwendungsfälle

Die in diesem Kapitel aufgeführten User Stories schildern die Absichten des Nutzers in Verbindung mit der E-Rezept-AdV und dienen als Lesehilfe zu den fachlichen Anwendungsfällen. Die User Stories erheben keinen Anspruch auf Vollständigkeit.

5.2.1.1 E-Rezepte einsehen

User Stories:

- Als Patient möchte ich nach Authentisierung in der E-Rezept-AdV alle meine Verordnungen einsehen können, so dass ich einen Überblick über meine Verordnungen behalte.
- Als Patient möchte ich die relevanten Informationen aus einem E-Rezept lesen können, so dass ich weiß, was mir verschrieben wurde.
- Als Patient möchte ich alle E-Rezepte, die für mich verfügbar sind, sehen können, so dass ich entscheiden kann, was ich mit diesen E-Rezepten machen will.

Mit diesem Anwendungsfall kann sich der Nutzer (Versicherter) die Informationen zu allen seinen auf dem E-Rezept-Fachdienst hinterlegten E-Rezepten in seine E-Rezept-AdV herunterladen und speichern, um sie sich anschließend anzeigen zu lassen.

A_20576 - E-Rezept-AdV: E-Rezepte abrufen

Das E_Rezept-AdV MUSS den Anwendungsfall "UC 3.1 - E-Rezepte durch Versicherten abrufen" aus [gemSysL_eRp] gemäß TAB_AdVERP_009 umsetzen.

Tabelle 5: TAB_AdVERP_009 - E-Rezepte abrufen

Name	E-Rezepte abrufen
Auslöser	<ul style="list-style-type: none">• Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter
Vorbedingung	<ul style="list-style-type: none">• Authentisierung des Nutzers ggü. der TI ist erfolgt.
Nachbedingung	<ul style="list-style-type: none">• Die E-Rezepte können angezeigt werden.

Name	E-Rezepte abrufen
Standardablauf	<ol style="list-style-type: none">1. E-Rezepte herunterladen2. Für jedes E-Rezept:<ol style="list-style-type: none">a. E-Rezept decodierenb. Signatur prüfen3. Dispensierinformation herunterladen

[<=]

A_19347 - E-Rezept-FdV: E-Rezept herunterladen

Das E-Rezept-FdV MUSS im Anwendungsfall "E-Rezepte empfangen" zum Herunterladen alle E-Rezepte des Nutzers die HTTP-Operation `GET /Task` mit

- `ACCESS_TOKEN` im Authorization-Header

ausführen.[<=]

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

Falls E-Rezepte auf dem E-Rezept-Fachdienst für den Versicherten abgelegt sind, dann liefert der Response ein Set von `Task` Ressourcen. Für die Spezifikation der `Task` Ressource siehe [gemSpec_DM_eRp]. Jeder Task enthält u.a. die folgenden fachlichen Informationen:

- `Task-ID` (`Task.id`), mit dem der Task bei Aufrufen des E-Rezept-Fachdienstes referenziert wird
- E-Rezept-Bundle mit den Detailinformationen zum E-Rezept
- `signature` mit der durch den E-Rezept-Fachdienst erzeugten FHIR-Signatur des E-Rezept-Bundles

Das E-Rezept-FdV prüft die FHIR-Signatur des E-Rezept-Bundles. Hierzu wird das base64-kodierte `data` Element aus `signature` dekodiert. Es enthält eine JSON Web Signature mit Information zum Algorithmus, eine Referenz zum Zertifikat und die signierten Daten.

A_20053 - E-Rezept-FdV: FHIR-Signatur prüfen

Das E-Rezept-FdV MUSS die FHIR-Signatur des E-Rezept-Bundles aus dem vom E-Rezept-Fachdienst heruntergeladenen E-Rezept gemäß [RFC7515#5.2] prüfen und bei negativer Prüfung die Verarbeitung abbrechen.[<=]

Der Ablauf der Prüfung erfolgt in den folgenden Schritten:

1. JSON als String einlesen, Header.Payload.Signatur sind punktgetrennt, ohne Zeilenumbruch
2. Header Base64 decodieren
3. Header JSON-Syntax prüfen, passen „{“, etc nach JSON-RFC
4. Header prüfen, keine Dubletten-Attribute im Header
5. Header „Schema“ validieren (Implementierung muss Header-Inhalt verstehen)
6. Payload Base64 decodieren

7. Signatur Base64 decodieren
8. Signaturinput = „ASCII(BASE64URL(UTF8(JWS Protected Header))+'.'+BASE64URL(JWS Payload))“ für Prüfung gemäß Signaturverfahren wie im Header angegeben
9. 4-8 ggfs. wiederholen, falls mehrere Signaturen drin sind
10. Feststellung gültig/ungültig

A_20594 - E-Rezept-AdV: E-Rezepte einsehen - MedicationDispense herunterladen

Die E-Rezept-AdV MUSS im Anwendungsfall "E-Rezepte abrufen" die HTTP-Operation `GET /MedicationDispense` mit

- `ACCESS_TOKEN` im Authorization-Header

ausführen, um die die Dispensierinformation zu E-Rezepten mit dem Status "quittiert" abzufragen. [`<=`]

Für weitere Informationen siehe "Abgabeinformationen abrufen" in der API-Schnittstelle [E-Rezept API Dokumentation].

Falls auf dem E-Rezept-Fachdienst Informationen zur Abgabe durch die abgebende LEI hinterlegt wurden, liefert der Response ein `MedicationDispense` Ressource. Zur Spezifikation der `MedicationDispense` Ressource siehe [gemSpec_DM_eRp]. Diese beinhaltet u.a. die folgenden fachlichen Informationen zum abgegebenen Arzneimittel:

- bei Fertigarzneimitteln: Pharmazentralnummer (sofern vorhanden)
- Beschreibung des Arzneimittels

Mittels der Task-ID können die Dispensierinformationen den E-Rezepten zugeordnet werden.

A_20595 - E-Rezept-AdV: E-Rezepte im Frontend anzeigen

Die E-Rezept-AdV MUSS dem Nutzer die vom E-Rezept-Fachdienst heruntergeladenen E-Rezepte in geeigneter Weise anzeigen. [`<=`]

A_20036 - E-Rezept-FdV: Anzeige der Abgabeinformationen

Das E-Rezept-FdV MUSS dem Nutzer die Abgabeinformationen in geeigneter Weise anzeigen [`<=`]

5.2.1.2 E-Rezepte löschen

User Stories:

- Als Patient möchte ich nach Authentisierung in der E-Rezept-AdV einzelne Verordnungen löschen können, so dass ich E-Rezepte, die ich nicht benötige, permanent entfernen kann und diese nicht mehr einsehbar sind und ich mein Recht auf informationelle Selbstbestimmung ausüben kann.
- Als Patient möchte ich verstehen können, welche Konsequenzen das Löschen von E-Rezepten hat, so dass ich mir der Tragweite meines Handelns bewusst sein kann.
- Als Patient möchte ich, dass mich die E-Rezept-AdV davor bewahrt, ein E-Rezept aus Versehen zu löschen, so dass ich keine Fehler mache und damit meine Therapie gefährde.

- Als Patient möchte ich Rückmeldung darüber erhalten, wenn die ausgewählten E-Rezepte gelöscht worden sind, so dass ich sicher sein kann, dass die Daten auch wirklich nicht mehr vorliegen.
- Als Patient möchte ich eine Rückmeldung darüber erhalten, wenn das Löschen fehlgeschlagen ist, so dass ich auf anderem Wege eine Löschen einleiten kann.

Mit diesem Anwendungsfall kann der Nutzer (Versicherter) einzelne ausgewählte oder alle E-Rezepte, die auf dem E-Rezept-Fachdienst gespeichert sind, löschen.

A_19219 - E-Rezept-FdV: E-Rezepte löschen - E-Rezepte zum Löschen auswählen

Das E-Rezept-FdV MUSS es dem Nutzer ermöglichen, ein oder mehrere E-Rezepte aus der Übersicht aller E-Rezepte zum Löschen auf dem Fachdienst zu markieren. [**<=**]

A_19220 - E-Rezept-FdV: E-Rezept löschen - Bestätigung

Das E-Rezept-FdV MUSS vom Nutzer eine Bestätigung einholen, dass die selektierten E-Rezepte gelöscht werden sollen und die Möglichkeit geben, das Löschen abubrechen. [**<=**]

A_20575 - E-Rezept-AdV: E-Rezepte löschen

Das E-Rezept-AdV MUSS den Anwendungsfall "UC 3.2 - E-Rezept durch Versicherten löschen" aus [gemSysL_eRp] gemäß TAB_AdVERP_008 umsetzen.

Tabelle 6 : TAB_AdVERP_008 – E-Rezepte löschen

Name	E-Rezepte löschen
Auslöser	<ul style="list-style-type: none"> • Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter
Vorbedingung	<ul style="list-style-type: none"> • Der Nutzer hat ein oder mehrere E-Rezepte zum Löschen markiert und das Löschen bestätigt. • Der Nutzer hat sich gegenüber der TI authentisiert.
Nachbedingung	<ul style="list-style-type: none"> • Die ausgewählten E-Rezepte sind vom E-Rezept-Fachdienst unwiederbringlich gelöscht.
Standardablauf	<ol style="list-style-type: none"> 1. Für jedes E-Rezept: <ol style="list-style-type: none"> a. Task-ID des E-Rezepts bestimmen b. E-Rezept löschen

[**<=**]

A_20648 - E-Rezept-AdV: E-Rezept löschen - Löschrequest

Die E-Rezept-AdV MUSS im Anwendungsfall "E-Rezepte löschen" für jedes zu löschende E-Rezept die HTTP-Operation `POST /Task/<id>/$abort` des E-Rezept-Fachdienstes mit

- ACCESS_TOKEN im Authorization-Header
- Task-ID in URL `<id>`

ausführen [**<=**]

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

5.2.1.3 Protokolldaten anzeigen

User Stories:

- Als Patient möchte ich nach Authentisierung im E-Rezept-AdV die Zugriffsprotokolle einzelner oder aller Verordnungen einsehen können, um nachzuvollziehen wer darauf zugegriffen hat
- Als Patient möchte ich, dass mein Protokoll so dargestellt wird, dass ich mit den Informationen auch was anfangen kann, so dass die Protokolleinträge für mich nicht nutzlos oder sogar verwirrend sind.

Mit diesem Anwendungsfall kann der Nutzer (Versicherter) Einsicht in alle protokollierten Zugriffe in Verbindung mit seinen E-Rezepten nehmen.

A_19209 - E-Rezept-FdV: Protokolldaten anzeigen

Das E-Rezept-FdV MUSS den Anwendungsfall "UC 3.5 - Protokolldaten abrufen" aus [gemSysL_eRp] gemäß TAB_FdVERP_014 umsetzen.

Tabelle 7 : TAB_FdVERP_014 – Protokolldaten anzeigen

Name	Protokolldaten anzeigen
Auslöser	<ul style="list-style-type: none"> • Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter
Vorbedingung	Der Nutzer ist gegenüber der TI authentifiziert.
Nachbedingung	Die Protokolldaten werden angezeigt
Standardablauf	<ol style="list-style-type: none"> 1. Protokolleinträge vom E-Rezept-Fachdienst abrufen 2. Protokolleinträge anzeigen
Varianten / Alternativen	Als Alternative zur Abfrage aller Protokolleinträge können die Protokolleinträge zu einer spezifischen Task-ID abgefragt werden.

[<=]

A_19210 - E-Rezept-FdV: Protokolldaten anzeigen - Protokolleinträge abrufen

Das E-Rezept-FdV MUSS im Anwendungsfall "Protokolldaten anzeigen" zum Abrufen der Protokolleinträge vom E-Rezept-Fachdienst die HTTP-Operation `GET /AuditEvent` mit

- `ACCESS_TOKEN` im Authorization-Header

ausführen.[<=]

Für weitere Informationen siehe "Eingriff in das Zugriffsprotokoll" in der API-Schnittstelle [E-Rezept API Dokumentation].

Der Response beinhaltet ein Bundle mit einem `searchset` von `AuditEvent` Ressourcen. Eine `AuditEvent` Ressource beinhaltet die folgenden Informationen (Siehe auch [\[gemSpec_DM_eRp#A_19296-* - E-Rezept-Fachdienst - Inhalt Protokolleintrag \]](#)):

- ID des Datenobjektes, auf das zugegriffen wurde (`AuditEvent.entity.what`) Das entspricht der Task-ID oder MedicationDispense-ID
- lesbarer Beschreibung in einfacher Sprache (`AuditEvent.text`)
- Name des Zugreifenden (`AuditEvent.agent.who`)
- Zeitpunkt des Zugriffs (`AuditEvent.recorded`)
- Ergebnis der aufgerufenen Operation (`AuditEvent.outcome`)

A_19211 - E-Rezept-FdV: Protokolldaten anzeigen - Anzeigen

Das E-Rezept-FdV MUSS eine Anzeige für die Protokolldaten umsetzen, in der die Protokolleinträge übersichtlich dargestellt werden. [`<=`]

Die E-Rezept-AdV kann es dem Nutzer über einen Link in der Anzeige ermöglichen, die Details zum referenzierten E-Rezept anzuzeigen.

Die Protokolldaten sollen für den Nutzer sortierbar und filterbar über die Angabe von Filterkriterien wie z.B. Zeitraum, dargestellt werden.

A_19479 - E-Rezept-FdV: Filterfunktion

Das E-Rezept-FdV MUSS es dem Nutzer ermöglichen, die Suchergebnisse nach festgelegten Kriterien zu filtern. [`<=`]

5.2.1.4 Nachrichten empfangen

User Stories:

- Als Versicherter möchte ich, dass ich Nachrichten von meiner Apotheke empfangen kann.

Mit diesem Anwendungsfall kann der Nutzer (Versicherter) Nachrichten von der Apotheke oder anderen Versicherten empfangen und anzeigen lassen.

A_21527 - E-Rezept-AdV: Nachrichten empfangen

Die E-Rezept-AdV MUSS den Anwendungsfall "UC 3.4 - Nachrichten durch Versicherten empfangen" aus [gemSysL_eRp] gemäß TAB_AdVERP_010 umsetzen.

Tabelle 8 : TAB_AdVERP_010 - Nachrichten empfangen

Name	Nachrichten empfangen
Auslöser	<ul style="list-style-type: none"> • Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter
Vorbedingung	Der Nutzer ist gegenüber der TI authentifiziert.
Nachbedingung	Die Nachrichten stehen zur Anzeige bereit.
Standardablauf	1. Nachrichten herunterladen

[`<=`]

A_19205 - E-Rezept-FdV: Nachrichten anzeigen - Nachrichten herunterladen

Das E-Rezept-FdV MUSS im Anwendungsfall "Nachrichten von Apotheken anzeigen" zum Herunterladen von Nachrichten vom E-Rezept-Fachdienst die HTTP-Operation `GET /Communication` mit

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

ausführen. [`<=`]

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

Der Response liefert ein Bundle mit `Communication` Ressourcen.

Eine `Communication` Ressource beinhaltet u.a. die fachlichen Informationen:

- Absender-ID (Telematik-ID der Apotheke)
- Mitteilung
Für die strukturierten Informationen in der Mitteilung siehe [gemILF_PS_eRp]

A_19208 - E-Rezept-FdV: Nachrichten anzeigen - Anzeigen

Das E-Rezept-FdV MUSS die vom E-Rezept-Fachdienst heruntergeladenen Nachrichten in geeigneter Weise anzeigen. [`<=`]

5.2.1.5 Nachrichten löschen

User Stories:

- Als Versicherter möchte ich auf dem Fachdienst gespeicherte Nachrichten löschen können.

Mit diesem Anwendungsfall kann der Nutzer von ihm zuvor versandte Nachrichten auf dem E-Rezept-Fachdienst löschen.

A_21523 - E-Rezept-FdV: Nachrichten löschen - Nachrichten zum Löschen auswählen

Das E-Rezept-FdV MUSS es dem Nutzer ermöglichen, ein oder mehrere Nachrichten zum Löschen auf dem E-Rezept-Fachdienst zu markieren. [`<=`]

A_21524 - E-Rezept-FdV: Nachrichten löschen - Bestätigung

Das E-Rezept-FdV MUSS vom Nutzer eine Bestätigung einholen, dass die selektierten Nachrichten gelöscht werden sollen und die Möglichkeit geben, das Löschen abubrechen. [`<=`]

A_21525 - E-Rezept-FdV: Nachrichten löschen

Das E-Rezept-FdV MUSS den Anwendungsfall "UC 3.8 - Nachricht durch Versicherten löschen" aus [gemSysL_eRp] gemäß TAB_FdVERP_018 umsetzen.

Tabelle 9 : TAB_FdVERP_018 – Nachrichten löschen

Name	Nachrichten löschen
Auslöser	<ul style="list-style-type: none"> • Aufruf des Anwendungsfalls in der GUI

Name	Nachrichten löschen
Akteur	Versicherter
Vorbedingung	<ul style="list-style-type: none"> Der Nutzer hat ein oder mehrere Nachrichten zum Löschen markiert und das Löschen bestätigt. Der Nutzer ist gegenüber der TI authentifiziert.
Nachbedingung	Die Nachrichten sind im E-Rezept-Fachdienst unwiederbringlich gelöscht.
Standardablauf	<ol style="list-style-type: none"> Für jede Nachricht: <ol style="list-style-type: none"> Communication-ID der Nachricht bestimmen Nachricht löschen

[<=]

A_21526 - E-Rezept-FdV: Nachrichten löschen - Löschrequest

Das E-Rezept-FdV MUSS im Anwendungsfall "Nachrichten löschen" für jede zu löschende Nachricht die HTTP-Operation `DELETE /Communication/<id>` des E-Rezept-Fachdienstes mit

- ACCESS_TOKEN im Authorization-Header
- Communication-ID in URL `<id>`

ausführen.[<=]

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

5.2.2 Fehlerbehandlung

Tritt ein Fehler bei der Verarbeitung von Operationsaufrufen des E-Rezept-Fachdienstes auf, dann antwortet der E-Rezept-Fachdienst mit einer Fehlermeldung. Das Format und die verwendeten Fehlercodes sind in den Spezifikationen der Interfaces beschrieben. Weiterhin können Fehler in der lokalen Verarbeitung auftreten.

A_19560 - E-Rezept-FdV: Abbrechen des Anwendungsfalls

Das E-Rezept-FdV MUSS, wenn bei der Abarbeitung der Aktivitäten eines Anwendungsfalls ein Fehler auftritt und keine Fehlerbehandlung beschrieben ist, den Anwendungsfall abbrechen.[<=]

Die E-Rezept-AdV soll dem Nutzer nach einem Abbruch eine verständliche Fehlermeldung anzeigen.

Wenn die Möglichkeit besteht, dass der Nutzer das fehlerverursachende Problem selbst beheben kann, kann die E-Rezept-AdV den Nutzer auf die Lösung hinweisen.

A_19561 - E-Rezept-FdV: Anzeige von Handlungsmöglichkeiten im Fehlerfall

Das E-Rezept-FdV SOLL dem Nutzer im Fehlerfall einen Hinweis geben, wenn es für den Nutzer Handlungsmöglichkeiten dazu gibt.[<=]

6 Informationsmodell

Dienste der TI:

Datenfeld	Herkunft	Beschreibung
E-Rezept-Fachdienst - E-Rezept-Schnittstelle FQDN, Port	DNS-Abfrage	Lokalisierungsinformationen
E-Rezept-Fachdienst - OCSP-Status-Proxy FQDN, Port	DNS-Abfrage	Lokalisierungsinformationen
Identity Provider: FQDN, Port, Path	DNS-Abfrage	Lokalisierungsinformationen

Session-Daten (TI-Session)

Datenfeld	Herkunft	Beschreibung
ACCESS_TOKEN	IDP Token-Endpunkt	Authentisierungs-Token für den Zugriff auf Dienste der TI
ACCESS_CODE	IDP	

E-Rezept:

Datenfeld	Herkunft	Beschreibung
E-Rezept-ID	Task.identifizier mit NamingSystem "PrescriptionID" E-Rezept-Fachdienst (GET /Task)	https://simplifier.net/erezept-workflow/gemerxprescriptionid
Task-ID	E-Rezept-Fachdienst (GET /Task) alternativ: E-Rezept-Token (2D-Code scannen)	https://simplifier.net/erezept-workflow/gemerxprescriptionid
Einlösedatum	acceptDate E-Rezept-Fachdienst (GET /Task)	Datum, bis wann das E-Rezept zur Erstattung durch die Krankenkasse einlösbar ist https://simplifier.net/erezept-workflow/acceptdate

Datenfeld	Herkunft	Beschreibung
Gültig bis	expiryDate E-Rezept-Fachdienst (GET /Task)	Datum, an dem das E-Rezept seine Gültigkeit verliert https://simplifier.net/erezept-workflow/expirydate
E-Rezept-Bundle	E-Rezept-Fachdienst (GET /Task)	https://simplifier.net/erezept/kbvprerpbundle
FHIR signature	signature E-Rezept-Fachdienst (GET /Task)	durch den E-Rezept-Fachdienst erstellte FHIR-Signatur des E-Rezept-Bundles
MedicationDispense	E-Rezept-Fachdienst (GET /MedicationDispense)	https://simplifier.net/erezept-workflow/gemerxmedicationdispense
Protokolleinträge	E-Rezept-Fachdienst (GET /AuditEvent)	https://simplifier.net/erezept-workflow/gemerxauditevent

Weitere detaillierte Daten zum Informationsmodell der Verordnung sind im Datenmodell der KBV <https://simplifier.net/erezept/kbvprerpbundle> enthalten. Siehe [gemSpec_DM_eRp].

MedicationDispense

Datenfeld	Herkunft	Beschreibung
PZN	Medikamentinformationen	https://simplifier.net/erezept/kbvprerpmedikamentpzn
Beschreibung		
Darreichungsform		
Menge		
LEI, welche das Mittel abgegeben hat	performer	https://simplifier.net/erezept-workflow/gemerxorganization
ID des zugehörigen Task	supportingInformation	https://simplifier.net/erezept-workflow/gemerxtask

Protokolleintrag:

Datenfeld	Herkunft	Beschreibung
ID des Datenobjektes, auf das zugegriffen wurde	AuditEvent.entity	https://simplifier.net/erezept-workflow/gemerxauditevent
Rezept-ID	AuditEvent.entity.description	
lesbarer Beschreibung in einfacher Sprache	AuditEvent.text	
Name des Zugreifenden	AuditEvent.agent.name	
Zeitpunkt des Zugriffs	AuditEvent.recorded	
Ergebnis der aufgerufenen Operation	AuditEvent.outcome	

7 Verteilungssicht

Eine Darstellung der hardwareseitigen Verteilung des Produkttyps bzw. seiner Teilsysteme und der Einbettung in die physikalische Umgebung wird nicht benötigt.

8 Anhang A – Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
AdV	Anwendung des Versicherten
CAN	Card Access Number
DF.HCA	Gesundheitsanwendung, Health Care Application
eGK	elektronische Gesundheitskarte
eRp	E-Rezept (elektronisches Rezept)
FdV	Frontend des Versicherten
GdV	Gerät des Versicherten
GUI	graphical user interface, Benutzeroberfläche
IDP	Identity Provider
MRPIN.home	Multireferenz-PIN Das Geheimnis entspricht der Personal Identification Number Card Holder (PIN des Karteneigentümers)
NFC	Near Field Communication
UX	User Experience
VAU	Vertrauenswürdige Ausführungsumgebung

8.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

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

8.3 Abbildungsverzeichnis

Abbildung 1 : Systemüberblick E-Rezept-AdV.....	9
---	---

8.4 Tabellenverzeichnis

Tabelle 1 : TAB_AdVERP_001 – Akteure und Rollen	8
Tabelle 2 : TAB_AdVERP_002 – Konfiguration E-Rezept-AdV	13
Tabelle 3 : TAB_FdVERP_019 - HTTP-Header "X-erp-resource"	16
Tabelle 4 : TAB_FdVERP_017 – Zertifikatsnutzung	17
Tabelle 5: TAB_AdVERP_009 - E-Rezepte abrufen.....	20
Tabelle 6 : TAB_AdVERP_008 – E-Rezepte löschen	23
Tabelle 7 : TAB_FdVERP_014 – Protokolldaten anzeigen	24
Tabelle 8 : TAB_AdVERP_010 - Nachrichten empfangen	25
Tabelle 9 : TAB_FdVERP_018 – Nachrichten löschen	26

8.5 Referenzierte Dokumente

8.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemSpec_DS_Hersteller]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller

[Quelle]	Herausgeber: Titel
[gemSpec_eRp_FdV]	gematik: Spezifikation E-Rezept-Frontend des Versicherten
[gemSpec_FD_eRP]	gematik: Spezifikation E-Rezept-Fachdienst
[gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider - Dienst
[gemSpec_IDP_FD]	gematik: Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste
[gemSpec_IDP_Frontend]	gematik: Spezifikation Identity Provider - Frontend
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OM]	gematik: Übergreifende Spezifikation – Operations und Maintenance
[gemSpec_PKI]	gematik: Übergreifende Spezifikation – Spezifikation PKI

8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel