Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature:

Einlösen ohne Anmeldung am E-Rezept-Fachdienst im E-Rezept-FdV

Version:	1.0.0 CC
Revision:	451085
Stand:	04.04.2022
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemF_eRp_altern_Zuweisung

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 CC	04.04.2022		zur Abstimmung freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments 5
1.1 Zielsetzung 5
1.2 Zielgruppe 5
1.3 Abgrenzungen 5
1.4 Methodik 5
2 Epic und User Stories 7
2.1 User Stories 7
2.1.1 Versicherter 7
2.1.2 Apotheke 8
3 Einordnung in die Telematikinfrastruktur 9
4 Fachliches Konzept 10
5 Technisches Konzept 12
5.1 Apothekenstammdaten im APOVZD 12
5.2 Pflege der URLs im APOVZD 12
5.3 Bereitstellung Zusatzinformationen für das E-Rezept-FdV 14
5.3.1 Verschlüsselungszertifikate 14
5.3.2 URL für Belieferungsoptionen 15
5.4 Verschlüsselung Kommunikation E-Rezept-FdV zu Apothekensystem 16
5.4.1 Transportverschlüsselung 16
5.4.2 Verschlüsselung der Nachricht des Versicherten 16
5.5 Lokalisierung SMC-B und Entschlüsselung 18
5.6 Zuweisungsinformationen 19
6 Spezifikation 20
6.1 Anforderungen an das Apothekenverzeichnis 20
6.2 Anforderungen an das Apothekensystem 22
6.3 Anforderungen an das Primärsystem der abgebenden LEI 23
6.3.1 Verwalten der Zuweisungsadresse 23
6.3.2 Nachricht von Apothekendienstleister empfangen 25
6.4 Anforderungen an das E-Rezept-FdV 25
6.5 Daten- und Informationsmodell 27
6.5.1 Stammdatensatz der Apotheke 27
6.5.2 Message an die Apotheke 28
6.6 Datenschutz und Sicherheit 31
6.7 Betrieb 31

7 Dokumentenhaushalt 32
7.1 Übersicht betroffener Dokumente 32
7.2 Übersicht Produkt- und Anbietertypen 32
8 Anhang A – Verzeichnisse 33
8.1 Abkürzungen 33
8.2 Referenzierte Dokumente 33
8.2.1 Dokumente der gematik 33
8.2.2 Weitere Dokumente 34

1 Einordnung des Dokuments

Dieses Dokument beschreibt ein Feature, welches den Versicherten ermöglicht, ein mit dem E-Rezept-FdV eingescannten E-Rezept-Token einer Apotheke zuzuweisen.

Das Feature umfasst das Konzept, die Beschreibung der Schnittstelle für die Übermittlung der Nachricht sowie die Beschreibung der Schnittstelle für die Bereitstellung der für die Übermittlung notwendigen Informationen durch die Apotheke.

1.1 Zielsetzung

Die Beschreibung des Funktionsumfangs als Feature erleichtert das Verständnis und die Nachvollziehbarkeit der Lösung, ausgehend von der Darstellung der Nutzersicht auf Epic-Ebene, über das technische Konzept bis zur Spezifikation der technischen Details. Mit den hier aufgestellten Anforderungen sollen Hersteller in der Lage sein, den zusätzlichen Funktionsumfang ihrer verantworteten Komponente bzw. Produkttyp bewerten und umsetzen zu können.

1.2 Zielgruppe

Das Dokument richtet sich an den Hersteller des Produkttyps E-Rezept-Frontend des Versicherten, Apothekendienstleister sowie Hersteller von Apothekenverwaltungssystemen.

1.3 Abgrenzungen

Die Festlegungen zur Kommunikation zwischen Versicherten und Apotheke zum Zuweisen von E-Rezepten oder zu Verfügbarkeitsanfragen, deren Nachrichten über den E-Rezept-Fachdienst übermittelt werden, sind nicht Gegenstand dieses Dokuments. Die Ausführung dieses Dokumentes ergänzen die bisherigen Festlegungen.

1.4 Methodik

Anforderungen

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.

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen." die Phrase „DARF NICHT" semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen." verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anforderungen werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>

Text / Beschreibung
[<=]

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

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.

2 Epic und User Stories

Die bisherige Umsetzung im E-Rezept-FdV sieht für eine Zuweisung eines E-Rezeptes an eine Apotheke die Nutzung des E-Rezept-Fachdienstes vor – zum Beispiel zur verbindlichen Reservierung bzw. zur Bestellung via Versand. Beide Nutzer, Versicherter wie Apotheke, müssen hierfür authentifizierte Teilnehmer der Telematikinfrastruktur sein.

Es ist zum jetzigen Zeitpunkt, Anfang Januar 2022, absehbar, dass nur eine geringe Anzahl Versicherte eine Authentisierung durchführen können, da sich die Ausgabe der zur Authentifizierung benötigten NFC-fähigen elektronischer Gesundheitskarten (eGK) und zugehöriger PIN über mehrere Jahre strecken wird. Ferner ist die NFC-Kommunikation zwischen Smartphone und eGK zum Teil schwierig und erreicht nicht die notwendige Akzeptanz bei allen Versicherten.

Da für den digitalen Empfang eines E-Rezepts diese Authentisierung notwendig ist, werden die Versicherten daher zunächst in großer Zahl weiterhin Papierausdrucke zum E-Rezept erhalten. Diese können zwar mit dem E-Rezept-FdV „fotografiert" und gespeichert werden (technisch wird der DataMatrix-Code, der auf dem Papierausdruck abgebildet ist, ausgelesen). Einen Nutzwert außer der digitalen Ablage und damit möglicher Einlösung via App in der Apotheke hat das „Fotografieren" aber bisher nicht.

Um den Versicherten dennoch einen Mehrwert durch das E-Rezept und dem dazugehörige E-Rezept-FdV bieten zu können, sollen schnellstmöglich die wichtigsten Funktionen (zumindest übergangsweise) auch ohne Authentisierung ermöglicht werden.

Die Nutzung dieser Funktionalität ist zeitlich beschränkt, bis die Voraussetzungen im Feld geschaffen sind, dass sich der Versicherte ohne größere Hürden mit dem E-Rezept-FdV gegenüber dem E-Rezept-Fachdienst authentisieren kann. Bspw. durch die großflächige Verbreitung von NFC-fähiger eGK und PIN bei den Versicherten oder durch Nutzung von elektronischen Identitäten für die Authentisierung der Versicherten gegenüber der TI. Die erste Prüfung der Voraussetzung ist in Absprache mit dem BSI für Ende 2022 vorgesehen.

2.1 User Stories

Die User Stories beschreiben die Erwartungen der Nutzer.

2.1.1 Versicherter

Als Versicherter möchte ich:

- meine E-Rezepte (oder die E-Rezepte von Angehörigen) auch ohne aufwendige Anmeldung in der E-Rezept-App digital an eine Apotheke zuweisen können, sodass ich mir Wege dorthin sparen kann.
- eine Rückmeldung zu der Zuweisung von der Apotheke erhalten, damit ich weiß, ob alles geklappt hat und wann ich mein Medikament erhalte.
- sehen können, welche Apotheken die Zuweisung ohne Anmeldung akzeptieren, damit ich mein E-Rezept nicht einer „falschen" Apotheke zuweise.
- verstehen, dass es jederzeit die Alternative zur Anmeldung gibt und sie mir Vorteile bringt (z.B. neue digitale E-Rezepte empfangen).

- dass das Einlösen ohne Anmeldung genauso einfach ist wie nach der Anmeldung, damit ich keine Nachteile dadurch habe.
- dass die Übermittlung von meinem E-Rezept-Token an die Apotheke sicher ist, auch wenn ich nicht an der Telematikinfrastruktur angemeldet bin.
- alle Serviceoptionen nutzen können (Reservieren, Botendienst, Versand).
- dass ich diese komfortable Einlöse-Möglichkeit ohne Anmeldung sowohl für Vor-Ort Apotheken als auch für EU-Versandapotheken nutzen kann.

2.1.2 Apotheke

Als Apotheker möchte ich:

- entscheiden können, ob ich auch E-Rezepte digital annehme, wenn der Versicherte in der App nicht angemeldet ist.
- im Warenwirtschaftssystem erkennen können, ob das E-Rezept über die TI oder außerhalb der TI zugewiesen wurde, damit ich weiß, über welchen Kanal ich meinem Kunden eine Rückmeldung geben kann.
- meinen Kunden erreichen können, auch wenn er mir das E-Rezept außerhalb der TI zugewiesen hat, um Rückfragen zum E-Rezept stellen zu können oder ihn beraten zu können.
- keinen Mehraufwand bei der Bearbeitung der E-Rezepte haben, wenn mir diese außerhalb der TI zugewiesen wurden (im Vergleich zu einer Zuweisung über die TI).

3 Einordnung in die Telematikinfrastruktur

Das Einlösen ohne Anmelden am E-Rezept-Fachdienst im E-Rezept-FdV soll es dem Versicherten ermöglichen, einen eingescannten E-Rezept-Token über das E-Rezept-FdV an eine Apotheke digital zu übersenden und somit das E-Rezept aus der Distanz dort einzulösen.

Eine unauthentisierte Nutzung des E-Rezept-Fachdienstes ist nicht zulässig. Von daher wird eine Nachricht vom E-Rezept-FdV über das Internet an die Zuweisungsadresse der für die Belieferung ausgewählte Apotheke – ohne Nutzung des E-Rezept-Fachdienstes oder des zentralen Netzes der TI – übermittelt.

4 Fachliches Konzept

Das Einlösen ohne Anmelden am E-Rezept-Fachdienst im E-Rezept-FdV soll es dem Versicherten ermöglichen, einen eingescannten E-Rezept-Token über das E-Rezept-FdV an eine Apotheke digital zu übersenden und somit das E-Rezept aus der Distanz dort einzulösen.

Vorbereitende Maßnahmen:

- Die Apotheke schafft die technischen Voraussetzungen für die Unterstützung der Funktionalität, bspw. durch Beauftragung eines Apothekendienstleisters.
- Die Serviceinformationen der Apotheke sind im APOVZD erfasst. Für die Erfassung wird durch den Betreiber des APOVZD eine Schnittstelle für die AVS bereitgestellt. Die Serviceinformation besteht aus URLs (je eine URL für die durch die Apotheke unterstützten Belieferungsoptionen). Unter den URLs ist ein REST-Service (des Apothekendienstleisters) erreichbar. Diese Schnittstelle akzeptiert Nachrichten des E-Rezept-FdVs.

Es sind drei Belieferungsoptionen vorgesehen:

- Abholung in Apotheke
- Lieferung zum Versicherten durch Vor-Ort-Apotheke
- Versand zum Versicherten durch Online-Apotheke

Ablauf:

- Ein Arzt erstellt ein E-Rezept für einen Versicherten.
- Der Versicherte erhält einen Ausdruck für das E-Rezept vom Arzt.
- Der Versicherte nutzt das E-Rezept-FdV ohne Anmelden am E-Rezept-Fachdienst.
- Der Versicherte scannt den Datamatrix-Code auf dem Ausdruck mit dem E-Rezept-FdV ein. Der E-Rezept-Token liegt im E-Rezept-FdV vor.
- Der Versicherte sieht im E-Rezept-FdV eine Liste aller Apotheken mit ihren Belieferungsoptionen. Die Apotheken, die diese Zuweisungsoption für keine Belieferungsoption anbieten, werden gekennzeichnet (bspw. ausgegraut). Das E-Rezept-FdV bezieht die Informationen zu den Apotheken aus dem APOVZD.
- Der Versicherte wählt eine Apotheke, der das E-Rezept zugewiesen werden soll, und die gewünschte Belieferungsoption aus. Er kann optional einen Freitext an die Apotheke erfassen.
- Der Versicherte überprüft die angegebenen Kontaktdaten (Telefonnummer und/oder E-Mail) und ggf. abweichende Lieferadresse. Er muss mindestens eine Kontaktinformation an die Apotheke übergeben. Eine abweichende Lieferadresse kann er optional mit der App erfassen. Im Folgenden werden Kontaktdaten und Lieferadresse zusammengefasst als "begleitete Attribute" bezeichnet.
- Das E-Rezept-FdV erzeugt eine UUID (128-bit, gemäß RFC-4122) zur eindeutigen Identifikation der Transaktion.
- Das E-Rezept-FdV erstellt einen Nachricht. Dieser enthält
  - für die Apotheke verschlüsselt: die Information des E-Rezept-Token begleitende Attribute und UUID,

241 • unverschlüsselt: die UUID (redundant zu dem verschlüsselten Teil) und die
242 Ziel-Apotheke.

243 • Das E-Rezept-FdV sendet die Nachricht an die adressierte Apotheke. Der hierfür
244 bereitgestellte Dienst kann von einem Dienstleister im Auftrag der Apotheke
245 betrieben werden. Die gematik nimmt keinen Einfluss auf diese Ausgestaltung.
246 Der Dienst übermittelt die Nachricht an das Apothekenverwaltungssystem (AVS)
247 der Apotheke

248 • Die Apotheke entschlüsselt die Nachricht des Versicherten mit dem Konnektor.

249 • Der E-Rezept-Token, die Kontaktdaten des Versicherten und der Freitext liegen in
250 der Apotheke vor.

251 • Die Apotheke kann mit der Kenntnis des E-Rezept-Token, das E-Rezept vom E-
252 Rezept-Fachdienst abzurufen.

253 • Die Apotheke kann den Versicherten über die angegebenen Kontaktdaten
254 erreichen, z.B. für Bestellbestätigung, Liefertermin, etc.

255

256 Die Funktionalität steht Vor-Ort- und Online-Apotheken zur Verfügung. Das Anbieten der
257 Funktionalität ist für die Apotheken optional.
258

5 Technisches Konzept

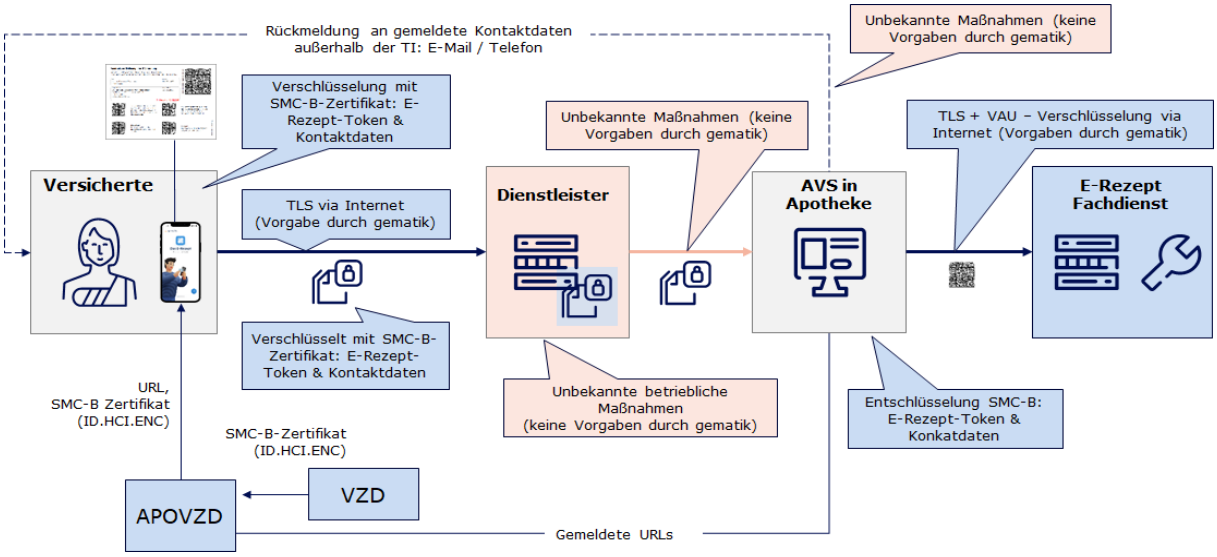

Abbildung 1: Schema Einlösen ohne Anmelden in der App

5.1 Apothekenstammdaten im APOVZD

Die Apothekenstammdaten im APOVZD werden um folgende Informationen erweitert:

- ein oder mehrere Verschlüsselungszertifikate der Apotheke (C.HCI.ENC)
- je eine URL für jede Belieferungsoption

Das APOVZD synchronisiert die Verschlüsselungszertifikate aus dem VZD der TI.

Die URLs werden durch das AVS übermittelt.

Unter der URL ist ein REST-Service erreichbar. Die Apotheke signalisiert durch Angabe der URL, dass sie die entsprechende Belieferungsoperation unterstützt.

5.2 Pflege der URLs im APOVZD

Die Pflege der Informationen zu den URLs im APOVZD erfolgt über die AVS (nach einer Information an die bzw. nach einer Freigabe durch die Apotheke) primär durch den AVS Hersteller. Es besteht die Möglichkeit, dass die Informationen durch die Apotheke editiert werden.

Mit dem Setzen mindestens einer der möglichen URLs gilt die Apotheke als "E-Rezept-ready" und wird im E-Rezept-FdV so dargestellt.

Die URLs können die folgenden Platzhalter beinhalten:

Tabelle 1 : Platzhalter in URL

Platzhalter	Bedeutung
<ti_id>	Telematik-ID der adressierten Apotheke
<transactionID>	Transaktions-ID der Zuweisung

Die Platzhalter werden beim Aufruf der URL durch das E-Rezept-FdV mit den konkreten Werten belegt.

Das AVS erstellt einen Datensatz mit den URLs.

```
{
  "shipment": "https://beispielurlVersand.de/<ti_id>?req=<transactionID>",
  "delivery": "https://beispielurlBote.de/",
  "onPremise": "https://beispielurlAbholung.de/",
}
```

Siehe auch [ADAS-A2B-eRezept].

Das AVS signiert den Datensatz mit dem Konnektor und der zugehörigen SMC-B. Mit der im Signaturzertifikat enthaltenen Telemantik-ID wird der zugehörige Eintrag im APOVZD zugeordnet.

Die Signatur des Datensatzes erfolgt mit dem Konnektor mit der Signaturidentität der SMC-B C.HCI.OSIG gemäß [RFC5652] mit Profil CAdES-BES ([CAdES]) als Enveloping-Signatur.

Das APOVZD stellt eine Schnittstelle (Upload-Container) bereit.

Das AVS authentifiziert sich gegenüber dem Upload-Container über einen durch den NGDA bereitgestellten Authentisierungsendpunkt, der der Systematik der Authentifizierung für den securPharm-Prozess entspricht. Es werden zwei abweichende Parameter verwendet:

```
clientId=urn-ngda-clients-erxti-m2m
scope=urn-ngda-services-pharmacy
```

Das Ergebnis der Authentifizierung ist ein Bearer Token, der bei Aufrufen des AVS an den Upload-Container im Header übergeben werden muss.

Das AVS übermittelt den signierten Datensatz.

Das APOVZD prüft das Vorhandensein eines Eintrages mit der Telematik-ID im APOVZD und die Signatur des übermittelten Datensatzes. Bei erfolgreicher Prüfung wird auf Basis der Telematik-ID aus dem Signaturzertifikat die übermittelten URLs den Einträgen im APOVZD zugeordnet.

Das Synchronisieren vom Upload-Container in das APOVZD erfolgt täglich zwischen 0 und 6 Uhr. Spätestens ab 6 Uhr ist die Änderung für das E-Rezept-FdV verfügbar.

Für die europäischen Versandapotheken erfolgt die Pflege der URLs im APOVZD mittels des Pflegetools der gematik.

5.3 Bereitstellung Zusatzinformationen für das E-Rezept-FdV

Das E-Rezept-FdV ruft die Informationen zu den Apotheken vom APOVZD ab. Das Datenmodell wird erweitert.

Die Zusatzinformationen Verschlüsselungszertifikate und URL für Belieferungsoptionen werden als Erweiterung der Location-Ressource transportiert.

5.3.1 Verschlüsselungszertifikate

Die Verschlüsselungszertifikate C.HCI.ENC jeder Apotheken bezieht das APOVZD aus dem Verzeichnisdienst der TI (VZD). Bsp.:

```
cn: gematik006

organization: gematik

userCertificate;binary:: MIIFcDCCBFigAwIBAgIDOlcOMA0GCSq...
userCertificate;binary:: MIIFUTCCBDmgAwIBAgIDQNF0MA0GCqG...
```

In der Location-Ressource wird eine neue Extension eingeführt, die eine Referenz auf eine Binary-Ressource transportiert. Die lokale Referenz verweist dann auf eine contained-Binary-Ressource innerhalb der Location-Ressource. Ist mehr als ein Zertifikat für eine Apotheke vorhanden (Anzahl entsprechend der für das KIM-Verfahren hinterlegten SMC-Bs), sind entsprechend der Anzahl viele Extensions und contained Binary-Ressourcen in der Location vorhanden.

Extension:

```
{
  "url": "http://ngda.de/fhir/extensions/PharmacyCertificateBase64",
  "valueReference": {
    "reference": "#123",
    "display": "Apothekenzertifikat1"
  }
}
```

Contained FHIR-Ressource Binary mit Zertifikat (Base64-String gekürzt):

```
{
  "id": "123",
  "resourceType": "Binary",
  "contentType": "application/pkix-cert",
  "data": "MIIFcDCCBFigAwIBAgIDOlcOMA0GCSq..."
}
```

5.3.2 URL für Belieferungsoptionen

Die URLs der angebotenen Belieferungsoptionen pflegen Apotheken in ihren eigenen Einträgen im APOVZD entsprechend der Vorgaben ihrer Warenwirtschaft bzw. ihres Dienstleisters.

Dem E-Rezept-FdV werden die URLs innerhalb der LocationRessource als weitere telecom-Attribute mitgeteilt. Die zu verwendenden Kontaktinformationen (Webseite, Telefon, E-Mail) erhalten einen niedrigen "rank" für eine hohe Priorität. Die bis zu 3 Belieferungsoptionen werden mit dem "system": "other" und folgenden Prioritäten festgelegt:

- 100 = URL für Belieferungsoption "Abholung in der Apotheke"
- 200 = URL für Belieferungsoption "Lieferung zum Versicherten durch Vor-Ort-Apotheke" (Botendienst)
- 300 = URL für Belieferungsoption "Versand zum Versicherten durch Online-Apotheke"

Beispiel:

```
"telecom": [
  {
    "system": "phone",
    "value": "030/400410",
    "rank": 1
  },
  {
    "system": "other",
    "value": "https://www.megaaoptheke.de/reservierung",
    "use": "mobile",
    "rank": 100
  },
  {
    "system": "other",
    "value": "https://www.megaapotheke.de/botendienst",
    "use": "mobile",
    "rank": 200
  }
]
{
  "shipment": "https://beispielurlVersand.de/<ti_id>?req=<transactionID>",
  "delivery": "https://beispielurlBote.de/",
  "onPremise": "https://beispielurlAbholung.de/",
}
```

5.4 Verschlüsselung Kommunikation E-Rezept-FdV zu Apothekensystem

5.4.1 Transportverschlüsselung

Die Übermittlung der Message vom E-Rezept-FdV zum Apothekensystem erfolgt über eine TLS-Verbindung. Es gelten die übergreifenden TLS Vorgaben der gematik (siehe [gemSpec_Krypt]).

5.4.2 Verschlüsselung der Nachricht des Versicherten

Die Nachricht des Versicherten wird für die Übermittlung zwischen E-Rezept-FdV und Apotheke verschlüsselt. Das E-Rezept-FdV verschlüsselt die Nachricht hybrid mit allen Verschlüsslungszertifikaten (C.HCI.ENC) der SMC-Bs der Apotheke. In jeden verschlüsselten Datensatz müssen dabei die Empfängerinformationen zur Identifikation der richtigen SMC-B durch das Apothekensystem eingetragen werden. Diese erfolgt analog zur Anwendung Kommunikation im Medizinwesen (KIM) über die Seriennummer des verwendeten Zertifikats in der Verschlüsselung.

Das Zielformat der Verschlüsselung ist ein CMS-Objekt, in das zusätzliche (unsafe = unverschlüsselt) Attribute für die Unterstützung der Entschlüsselung eingebettet werden. Diese werden unter der OID `oid_komle-recipient-emails` gemäß [gemSpec_OID] gespeichert.

Die Einbettung der Attribute erfolgt in eine ASN.1-Struktur analog zum KIM-Verfahren. Anstelle der im KIM-Verfahren verwendeten E-Mail-Adresse des Empfängers wird die Telematik-ID der adressierten Apotheke eingetragen.

```
id-recipientEmails OBJECT IDENTIFIER ::= {1.2.276.0.76.4.173}
Recipient-emails Attributwerte sind vom ASN.1 Typ RecipientEmails:
RecipientEmails ::= SET SIZE (1..MAX) OF RecipientEmail
RecipientEmail ::= SEQUENCE {
         telematikID IA5String, rid RecipientIdentifier }
```

Diese ASN.1-Struktur muss Base64-DER codiert im Aufruf der Verschlüsselungsoperation übergeben werden.

Das folgende beispielhafte Kommando verschlüsselt einen Datensatz für ein ENC-Zertifikat inkl. Einbettung der unsafe-Attribute (kotlin-Code).

```
val info = ASN1EncodableVector().apply {
    recipientCerts.forEach { recipientCert ->
        add(
            DERSequence(
                ASN1EncodableVector().apply {
                    add(DERIA5String("musterempfaenger@komle.de", true))
                    add(RecipientIdentifier(IssuerAndSerialNumber(JcaX509C
ertificateHolder(recipientCert).toASN1Structure())))
                }
            )
        )
    }
}
//
// ...
```

```
//
recipientCerts.forEach { recipientCert ->
    if (recipientCert.sigAlgOID == oidEcdsaWithSHA256) {
        edGen.addRecipientInfoGenerator(
            JceKeyAgreeRecipientInfoGenerator(
                CMSAlgorithm.ECDH_SHA256KDF,
                kp.private,
                kp.public,
                CMSAlgorithm.AES256_GCM
            )
                .setProvider(BCProvider)
                .addRecipient(recipientCert)
        )
    } else {
        edGen.addRecipientInfoGenerator(
            JceKeyTransRecipientInfoGenerator(
                recipientCert,
                JceAsymmetricKeyWrapper(
                    OAEPParameterSpec("SHA-256", "MGF1",
MGF1ParameterSpec.SHA256, PSource.PSpecified.DEFAULT),
                    recipientCert.publicKey
                )
            ).setProvider(BCProvider)
        )
    }
}
```

Der erhaltene CMS-Datensatz enthält unter der genannten OID die Entschlüsselungsinformationen für den Empfänger:

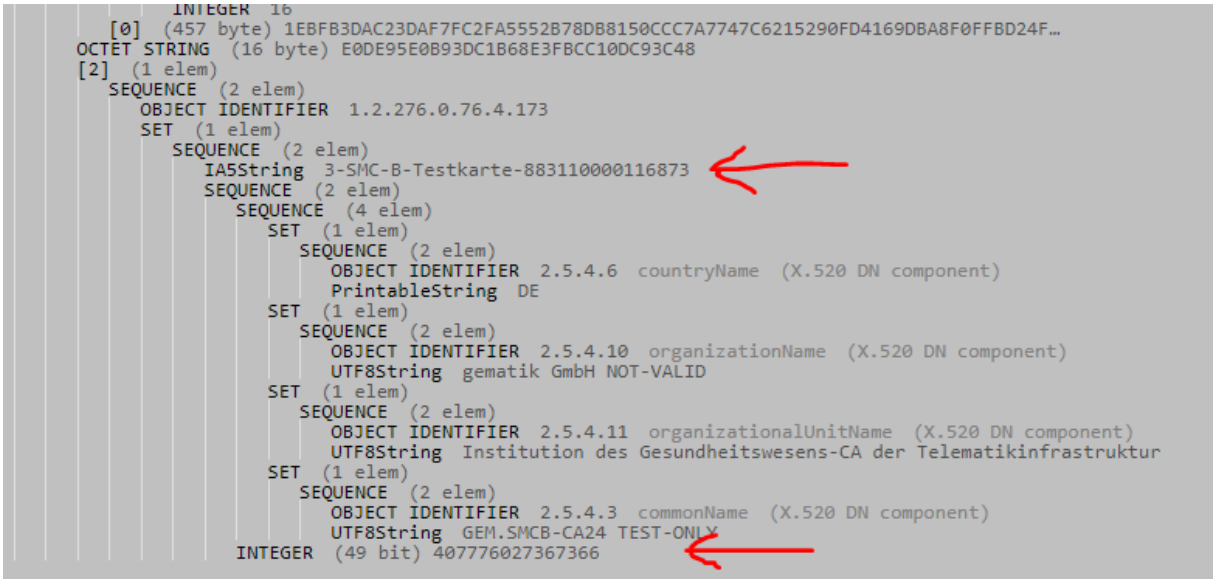

Abbildung 2: Ausschnitt recipient-mails-Informationen im CMS-Datensatz

Im Bild ist die Telematik-ID der Empfänger-Apotheke (3-SMC-B-Testkarte-883110000116873) und die Seriennummer des in der Verschlüsselung verwendeten SMC-B-Zertifikats (407776027367366) angegeben. Mit diesen Informationen kann durch

Auslesen der Karteninformationen über den Konnektor der Apotheke die richtige SMC-B für die Entschlüsselung identifiziert werden.

5.5 Lokalisierung SMC-B und Entschlüsselung

Die Lokalisierung der SMC-B zum Entschlüsseln und das Entschlüsseln der Nachricht erfolgt durch das Apothekenverwaltungssystem (AVS). Da eine Apotheke mehrere SMC-Bs in Benutzung haben kann (Redundanz, Lastverteilung, verschiedene Einsatzzwecke), muss das AVS wissen, mit welcher Karte der empfangene Datensatz entschlüsselt werden kann. Die oben in der Verschlüsselung eingebetteten Informationen helfen dabei.

Um die Anzahl der Zugriffe auf die Schnittstellen des Konnektors zu reduzieren, empfiehlt sich ein lokaler Cache im AVS, der Zuordnungen zwischen Telematik-ID, Zertifikats-Seriennummer und ICCSN von HBA/SM-B speichert. Die gespeicherten Zertifikats-Seriennummern sind dabei im ASN.1-Format in `IssuerAndSerialNumber` enthalten.

Das AVS geht dabei wie folgt vor:

1. Die über den Konnektor verfügbaren (gesteckten) Karten werden über die Operation `GetCards` ermittelt. Diese liefert je Karte ein CardHandle und die ICCSN der Karte zurück. Im Folgenden wird die jeweilige Karte über das CardHandle adressiert
2. Die Zertifikate je Karte werden über die Konnektoroperation `ReadCardCertificate` abgerufen. Mit dem Parameter `CertRefList = "C.ENC"` werden nur die Zertifikate Verschlüsselungsidentität abgerufen. In der Rückgabe ist die Seriennummer des Zertifikats in `IssuerAndSerialNumber` enthalten.
3. Mit dieser Suche wird fortgefahren, bis eine passende Karte gefunden ist, dessen ENC-Zertifikats-Seriennummer mit der Seriennummer in den ungeschützten (unsafe) Attributen im verschlüsselten Datensatz übereinstimmt. Mit dieser Karte kann der Datensatz entschlüsselt werden.

Das Entschlüsseln mittels der gefundenen Karte erfordert den Einsatz des PIN-geschützten privaten Schlüssels auf der Karte. Die Konnektoroperation fragt nicht automatisch nach dem PIN. Ist der PIN-Status dem AVS unbekannt, kann über die Konnektoroperationen `GetPinStatus` geprüft werden, ob eine PIN-Abfrage erforderlich ist. Die Konnektoroperation `VerifyPin` startet die PIN-Abfrage am Kartenterminal. Siehe auch [gemILF_PS]

Anschließend kann der Datensatz mit der Operation `DecryptDocument` des Konnektors und den Parametern `CardHandle` für die gefundene Karte und `Document` (die verschlüsselten Daten) entschlüsselt werden. Die übrigen Parameter (Verschlüsselungsalgorithmus, Kurvenparameter etc.) entnimmt der Konnektor dem Verschlüsselungscontainer.

```
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">   <SOAP-
ENV:Header/>   <S:Body>     <ns5:DecryptDocument
xmlns="http://ws.gematik.de/tel/error/v2.0"
xmlns:ns2="http://ws.gematik.de/conn/ConnectorCommon/v5.0"
xmlns:ns3="urn:oasis:names:tc:dss:1.0:core:schema"
xmlns:ns4="http://www.w3.org/2000/09/xmldsig#"
```

```
xmlns:ns5="http://ws.gematik.de/conn/EncryptionService/v6.1"
xmlns:ns6="http://ws.gematik.de/conn/ConnectorContext/v2.0"
xmlns:ns7="urn:oasis:names:tc:SAML:1.0:assertion">       <ns6:Context>
<ns2:MandantId>Mandant1</ns2:MandantId>
<ns2:ClientSystemId>CS1</ns2:ClientSystemId>
<ns2:WorkplaceId>AP1</ns2:WorkplaceId>
<ns2:UserId>user</ns2:UserId>       </ns6:Context>
<ns5:PrivateKeyOnCard>         <ns2:CardHandle>SMC-B-73</ns2:CardHandle>
<ns5:KeyReference/>       </ns5:PrivateKeyOnCard>       <ns2:Document>
<ns3:Base64Data
MimeType="text/plain">MIAGCyqGSIb3DQEJE...</ns3:Base64Data>
</ns2:Document>     </ns5:DecryptDocument>   </S:Body> </S:Envelope>
```

412

413 5.6 Zuweisungsinformationen

414 Für die direkte Zuweisung werden die Referenz auf das einzulösende E-Rezept, die
415 Zugriffsberechtigung (AccessCode) und Kontaktinformationen des Versicherten
416 verschlüsselt an die Apotheke geschickt. Die folgende Datenstruktur transportiert die
417 benötigten Informationen, wie im folgenden Beispiel angegeben:

```
{
"version": "2",
"supplyOptionsType": "delivery",
"name": "Dr. Maximilian von Muster",
"address": ["Bundesallee", "312", "12345", "Berlin"],
"hint": "Bitte im Morsecode klingeln: -.-.",
"text": "123456",
"phone": "004916094858168",
"mail": "max@musterfrau.de",
"transaction": "ee63e415-9a99-4051-ab07-257632faf985",
"taskID": "160.123.456.789.123.58",
"accessCode":
"777bea0e13cc9c42ceec14aec3ddee2263325dc2c6c699db115f58fe423607ea"
}
```

6 Spezifikation

Dieses Kapitel beschreibt die technische Umsetzung der beschriebenen Konzepte an die verschiedenen Produkt- und Anbietertypen. In den jeweiligen Produkt- und Anbietertypsteckbriefen sind zu den Anforderungen ("Blattanforderungen") die jeweiligen Prüfverfahren angegeben.

Dargestellt sind die zusätzlichen Anforderungen an die Produkttypen des E-Rezepts, die bestehende Anforderungslage für bereits eingeführte Funktionalitäten, wie bspw. der Zuweisung von E-Rezepten über die Kommunikation des E-Rezept-Fachdienstes bleibt hiervon unberührt.

6.1 Anforderungen an das Apothekenverzeichnis

A_22752 - Apothekenverzeichnis - Attribute Zuweisungsadresse
Das Apothekenverzeichnis MUSS im Stammdatensatz einer Apotheke drei Zuweisungsadresse (eine Zuweisungsadresse pro Belieferungsoption) verwalten können.**[**APOVZD, funkt. Eignung: Herstellererklärung, <=**]**

In den Attributen kann jeweils eine URL, z.B. https://urlDerApotheke.de/12345, hinterlegt werden.

Es sind drei Belieferungsoptionen spezifiziert:

- Reservierung
- Botendienst
- Versand

Hinweis: Für die Anzeige der möglichen Belieferungsoptionen im E-Rezept-FdV werden die bestehenden Flags im Stammdatensatz genutzt.

A_22753 - Apothekenverzeichnis - Pflege Attribute Zuweisungsadresse
Das Apothekenverzeichnis MUSS es den Apotheken ermöglichen, die Attribute der Zuweisungsadressen zu pflegen.**[**APOVZD, funkt. Eignung: Herstellererklärung, <=**]**

Zu diesem Zweck stellt das Apothekenverzeichnis einen Upload-Container bereit, welcher eine Schnittstelle zu den AVS anbietet.

Der beigestellte Upload-Container stellt im Internet einen REST-Service gemäß [ADAS-A2B-eRezpt] unter der folgenden URL zur Verfügung, welcher die POST-Operation zur Einlieferung der Endpunkte durch das AVS unterstützt:

https://datahub.ngda.de/erx2gem/<version>/configuration/erx2url/?n_id=<N-ID>

mit
<version> - Versionsnummer der Schnittstellenspezifikation (gepflegt durch ADAS als openAPI Spec in SwaggerHub
<N-ID> - N-ID der Apotheke als Identifier

Der Identifier N-ID ist dem AVS aus der Authentifizierungsmethodik der NGDA bekannt.

457 Beispiel für den Aufruf der POST-Operation:

```
{
  "meta": {
    "client_id": "APO1234567",
    "client_system_name": "System ABC der Firma XYZ",
    "client_system_version": "1.1.0",
    "user_id": "PM",
    "user_name": "Peter Mustermann",
    "ctid": "753d4e7f-a12b-89a4-f123-B25a45c78d9f"
  },
  "data": [
    {
      "coid": "1234567890abcdef",
      "type": "GMU",
      "contenttype": "application/pkcs7-mime",
      "data": "string"
    }
  ]
}
```

458 Die Metainformationen basieren auf Werten, die in der Standard-ADAS-Schnittstelle bei
459 allen Requests gegeben sind.
460 Der Type GMU definiert, dass es sich um ein Konfigurationsobjekt für die gematik
461 handelt.
462 Das Attribut "pkcs7" beinhaltet die eigentliche Information für das Verzeichnis in einem
463 base64-codierten PKCS7-Container.

464 Der Betreiber des Apothekenverzeichnisses stellt die Informationen zur API den AVS-
465 Hersteller zur Verfügung. Die AVS authentisieren sich ggü. dem Upload-Container mittels
466 des etablierten im securPharm-Prozess genutzten Vorgehen. Das AVS übermittelt einen
467 mit der zur Telematik-ID zugehörigen SMC-B signierten Datensatz mit den
468 Endpunktinformationen der Apotheke.

469 Das Apothekenverzeichnis MUSS die von den AVS übermittelten URL Datensätze aus dem
470 Upload-Container mit den Einträgen im APOVZD synchronisieren.

471 **A_22754 - Apothekenverzeichnis - Signatur-Prüfung der Datensatz-**
472 **Endpunktinformationen**
473 Das Apothekenverzeichnis MUSS die Gültigkeit der Signatur des durch das AVS
474 übermittelten Datensatzes prüfen und die Übernahme abbrechen, falls die Prüfung
475 fehlschlägt.**[**APOVZD, funkt. Eignung: Herstellererklärung, <=**]**

476 **A_22755 - Apothekenverzeichnis - Attribute Verschlüsselungszertifikate**
477 Das Apothekenverzeichnis MUSS im Stammdatensatz einer Apotheke bis zu 100
478 Verschlüsselungszertifikate verwalten können.**[**APOVZD, funkt. Eignung:
479 Herstellererklärung, <=**]**

480 **A_22756 - Apothekenverzeichnis - Extension Verschlüsselungszertifikate**
481 Das Apothekenverzeichnis MUSS bei Vorhandensein mindestens einer Zuweisungsadresse
482 alle Verschlüsselungszertifikate der Apotheke mittels einer optionalen Extension

```
{
  "url": "http://ngda.de/fhir/extensions/PharmacyCertificateBase64",
  "valueReference": {
    "reference": "#123",
    "display": "Apothekenzertifikat1"
```

```
   }
}
```

und einer contained Binary-Ressource je Zertifikat in der Location-Ressource bereitstellen.**[**APOVZD, funkt. Eignung: Test Produkt/FA, <=**]**

A_22757 - Apothekenverzeichnis - Synchronisation Verschlüsselungszertifikate im VZD
Das Apothekenverzeichnis MUSS beim Abruf der Apothekeninformationen aus dem VZD alle von der Apotheke im VZD hinterlegten Verschlüsselungszertifikate herunterladen und mit den Verschlüsselungszertifikaten im Stammdatensatz der Apotheke synchronisieren, wenn für die Apotheke mindestens eine Zuweisungsadresse angegeben ist. **[**APOVZD, funkt. Eignung: Test Produkt/FA, <=**]**

6.2 Anforderungen an das Apothekensystem

Das Apothekensystem bezeichnet ein System, welches den Empfang und die Verarbeitung der Nachricht umsetzt. Die genaue Architektur wird nicht vorgegeben. Ein Teil der Funktionalitäten muss nicht durch das Primärsystem der abgebenden Leistungserbringerinstitution (AVS) erbracht werden, sondern kann an einen Dienstleister ausgelagert werden. Anforderungen, welche durch das AVS umgesetzt werden müssen und nicht ausgelagert werden dürfen, werden an das PS der abgebenden LEI adressiert.

A_22758 - Apothekensystem - Schnittstelle bereitstellen
Das Apothekensystem MUSS eine Schnittstelle für das E-Rezept-FdV im Internet anbieten.**[**, , <=**]**

A_22759 - Apothekensystem - Schnittstelle TLS-Verbindung
Das Apothekensystem MUSS am Eingangspunkt Verbindungen von Clients ausschließlich über TLS akzeptieren.**[**, , <=**]**

Das Apothekensystem MUSS für die Übertragung mittels TLS mindestens die TLS-Version 1.2 unterstützen. Für Details zu den TLS-Versionen 1.2 und 1.3 siehe gemSpec_Krypt#3.3.2 TLS-Verbindungen.

A_22760 - Apothekensystem - REST Service
Das Apothekensystem MUSS an der Schnittstelle einen REST Service anbieten.**[**, , <=**]**

Der REST Service kann weitere Operationen anbieten, d.h. er muss nicht exklusiv für die Schnittstelle zum E-Rezept-FdV angeboten werden.

A_22761 - Apothekensystem - POST-Operation
Das Apothekensystem MUSS im REST Service eine POST-Operation unterstützen, welche die Nachrichten entgegennimmt.**[**, , <=**]**

Beispiel für den Aufruf der POST-Operation:

```
curl-XPOST "https://www.megaapotheke.de/botendienst?ti_id=<TI-
ID>&transactionID=<UUID>" --header "Content-Type: application/pkcs7-mime"
--data @blob.p7c
```

Der Aufruf beinhaltet, falls in der URL der Platzhalter <transactionID> verwendet wurde, eine Transaktions-ID ("UUID [(pseudo-)zufällig gemäß Version 4]"). Der Aufruf

beinhaltet, falls in der URL der Platzhalter <ti_id> verwendet wurde, die Telematik-ID der adressierten Apotheke, welche zum Routing genutzt wird.

Die Nachricht beinhaltet einen verschlüsselten Inhalt. Die Telematik-ID der adressierten Apotheke steht ebenfalls in den unsafe-Attributes des verschlüsselten Inhalts. Die Transaction-ID ist auch Bestandteil des verschlüsselten Inhalts.

A_22762 - Apothekensystem - Returncode für erfolgreiche Annahme der Nachricht
Das Apothekensystem MUSS die erfolgreiche Entgegennahme mit dem Returncode 200 quittieren.**[**, , <=**]**

A_22763 - Apothekensystem - Weiterleiten der Nachricht an die adressierte Apotheke
Das Apothekensystem MUSS die Nachricht an das PS der abgebenden LEI, welche SMC-Bs zur Telematik-ID verwaltet, weiterleiten.**[**, , <=**]**

6.3 Anforderungen an das Primärsystem der abgebenden LEI

A_22764 - PS der abgebenden LEI: Feature Einlösen ohne Anmelden am E-Rezept-Fachdienst im E-Rezept-FdV
Das PS der abgebenden LEI KANN die Funktionalitäten zum Feature "Einlösen ohne Anmelden am E-Rezept-Fachdienst im E-Rezept-FdV" unterstützen.**[**PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

Die folgenden Anforderungen gelten, wenn das AVS das Feature "Einlösen ohne Anmelden am E-Rezept-Fachdienst im E-Rezept-FdV" unterstützt.

6.3.1 Verwalten der Zuweisungsadresse

Das PS der abgebenden LEI muss die URL der Schnittstelle im Apothekenverzeichnis verwalten. Die Verwaltung der IP-Adresse anstatt der URL ist nicht zulässig.

A_22765 - PS der abgebenden LEI: Einlösen ohne Anmelden – Zuweisungsadresse erfassen
Das PS der abgebenden LEI MUSS es dem Nutzer ermöglichen, je eine URL pro unterstützter Belieferungsoption zu erfassen.**[**PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

Die Verwaltung der IP-Adresse anstatt der URL ist nicht zulässig.

A_22766 - PS der abgebenden LEI: Einlösen ohne Anmelden – Zuweisungsadresse übermitteln
Das PS der abgebenden LEI MUSS den Anwendungsfall "Zuweisungsadresse übermitteln" aus [gemSysL_eRp] gemäß TAB_ILFERP_006 umsetzen.

Tabelle 2 : TAB_ILFERP_xxx – Zuweisungsadresse übermitteln

Name	Zuweisungsadresse übermitteln

Auslöser	• Aufruf des Anwendungsfalls in der GUI
Akteur	Mitarbeiter der abgebenden LEI, DVO
Vorbedingung	• Die Information der Zuweisungsadressen ist im PS erfasst • Das PS ist am Upload-Container authentifiziert
Nachbedingung	• Die Informationen sind in den Upload-Container übermittelt und stehen zur Synchronisation in das APOVZD bereit
Standardablauf	1. Datensatz erstellen 2. Datensatz mit Konnektor signieren 3. Nachricht erstellen 4. Nachricht übermitteln

[PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

A_22767 - PS der abgebenden LEI: Zuweisungsadresse übermitteln - Datensatz erstellen
Das PS der abgebenden LEI MUSS im Anwendungsfall "Zuweisungsadresse übermitteln" einen Datensatz mit den URLs der unterstützen Belieferungsoptionen im Format

```
{
  "shipment": "<URL für die Bereitstellungsoption Versand>",
  "delivery": "<URL für die Bereitstellungsoption Botendienst>",
  "onPremise": "<URL für die Bereitstellungsoption Abholung>"
}
```

erstellen.**[**PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

Die URLs können die Platzhalter `<ti_id>` für die Telematik-ID der Apotheke und den Platzhalter `<transactionID>` für die Übermittlung einer Transaktions-ID enthalten.

Für nicht unterstützte Belieferungsoptionen wird ein Leerstring übermittelt.

A_22768 - PS der abgebenden LEI: Zuweisungsadresse übermitteln - Datensatz mit Konnektor signieren
Das PS der abgebenden LEI MUSS im Anwendungsfall "Zuweisungsadresse übermitteln" den Datensatz mit dem Konnektor signieren. Hierbei ist die SMC-B mit der Telematik-ID der LEI auszuwählen.**[**PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

A_22769 - PS der abgebenden LEI: Zuweisungsadresse übermitteln - Nachricht erstellen
Das PS der abgebenden LEI MUSS im Anwendungsfall "Zuweisungsadresse übermitteln" eine Nachricht gemäß [ADAS-A2B-eRezept] mit

- dem signierten und base64-kodierten Datensatz in `pkcs7`

erstellen.**[**PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

A_22770 - PS der abgebenden LEI: Zuweisungsadresse übermitteln - Nachricht übermitteln
Das PS der abgebenden LEI MUSS im Anwendungsfall "Zuweisungsadresse übermitteln" die Nachricht mittels `POST`-Operation gemäß [ADAS-A2B-eRezept] an den Upload-Container übermitteln.**[**PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

6.3.2 Nachricht von Apothekendienstleister empfangen

A_22771 - PS der abgebenden LEI: Einlösen ohne Anmelden - Nachrichten entgegennehmen
Das PS der abgebenden LEI MUSS die verschlüsselte Nachricht entgegennehmen.**[**PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

A_22772 - PS der abgebenden LEI: Einlösen ohne Anmelden - Nachricht entschlüsseln
Das PS der abgebenden LEI MUSS die Nachricht mit der Operation `DecryptDocument` des `EncryptionService` des Konnektors entschlüsseln.**[**PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

Siehe [gemILF_PS#4.4.5.2 Entschlüsseln].

A_22773 - PS der abgebenden LEI: Einlösen ohne Anmelden - Versicherten kontaktieren
Das PS der abgebenden LEI KANN eine Nachricht an die übermittelten Kontaktinformationen (SMS, E-Mail) senden, um den Eingang der der Nachricht zu bestätigen oder weitere Absprachen zur Belieferung zu treffen.**[**PS_E-Rezept_abgebend, funkt. Eignung: Herstellererklärung, <=**]**

6.4 Anforderungen an das E-Rezept-FdV

A_22774 - E-Rezept-FdV - Einlösen ohne Anmelden - Nachricht erfassen
Das E-Rezept-FdV MUSS dem Nutzer die Möglichkeit geben, die in der Nachricht übermittelten Informationen zu erfassen.**[**eRp_FdV, funkt. Eignung: Herstellererklärung, <=**]**

A_22775 - E-Rezept-FdV - Einlösen ohne Anmelden - Kontaktdaten bei Botendienst oder Versand
Das E-Rezept-FdV MUSS sicherstellen, dass der Nutzer, falls die Belieferungsoption Botendienst oder Versand ausgewählt wurde, das Kontaktdatenfeld "E-Mail" oder "Telefon" befüllt hat.**[**eRp_FdV, funkt. Eignung: Herstellererklärung, <=**]**

A_22776 - E-Rezept-FdV - Einlösen ohne Anmelden – Transaktions-ID
Das E-Rezept-FdV MUSS eine Transaktions-ID gemäß [RFC4122] für jede Mitteilung erstellen.**[**eRp_FdV, funkt. Eignung: Herstellererklärung, <=**]**

A_22777 - E-Rezept-FdV - Zuweisen ohne Fachdienst - Nachricht erstellen
Das E-Rezept-FdV MUSS auf Basis der vom Nutzer erfassten Informationen eine Nachricht erstellen.**[**eRp_FdV, funkt. Eignung: Test Produkt/FA, <=**]**

Für die Struktur der Nachricht siehe A_22784 - E-Rezept - Einlösen ohne Anmelden - Datenstruktur Nachricht .

A_22778 - E-Rezept-FdV - Einlösen ohne Anmelden - Verschlüsselung mit C.HCI.ENC
Das E-Rezept-FdV MUSS die Nachricht des Versicherten mit allen bereitgestellten C.HCI.ENC Zertifikaten (inkl. der verschiedenen kryptografischen Verfahren) der adressierten Apotheke (Verschlüsselungszertifikat der SMC-B C.HCI.ENC) verschlüsseln.**[**eRp_FdV, Sich.techn. Eignung: Produktgutachten, <=**]**

Das Profil des C.HCI.ENC Zertifikats wird in [gemSpec_PKI] beschrieben. Die Verwendung anderer Zertifikate zur Verschlüsselung von Nachrichten ist nicht zulässig.

Eine Apotheke kann mehrere SMC-Bs mit gleicher Telematik-ID im Einsatz haben, auf jeder SMC-B befinden sich aktuell Verschlüsselungsidentitäten für das kryptografische RSA und das ECC-Verfahren.

A_22779 - E-Rezept-FdV - Zuweisen ohne Fachdienst - Nachricht verschlüsseln
Das E-Rezept-FdV MUSS die Daten ausschließlich als PKCS#1 verschlüsselten Datensatz (CMS) bereitstellen.**[**eRp_FdV, Sich.techn. Eignung: Produktgutachten, <=**]**

GS-A_4389 - Symmetrischer Anteil der hybriden Verschlüsselung binärer Daten
Produkttypen, die die hybride Verschlüsselung binärer Daten durchführen, MÜSSEN für den symmetrischen Anteil der Verschlüsselung die folgenden Vorgaben berücksichtigen:

- Als symmetrische Block-Chiffre muss AES [FIPS-197] mit einer Schlüssellänge von 256 Bit im Galois/Counter Mode (GCM) gemäß [NIST-SP-800-38D] mit der Tag-Länge von 128 Bit verwendet werden.
- Die IVs dürfen sich bei gleichem Schlüssel nicht wiederholen (vgl. [NIST-SP-800-38D#S.25] und [BSI-TR-02102-1#S.24]). Der IV soll eine Bitlänge von 96 Bit besitzen, seine Länge muss mindestens 96 Bit sein. Es wird empfohlen den IV zufällig zu wählen (vgl. [gemSpec_Krypt#GS-A_4367]).
- Hinweis: Im Normalfall ist davon auszugehen, dass für die Sicherung der Integrität und Authentizität der zu verschlüsselnden Daten zudem noch eine Signatur dieser Daten notwendig ist.

[Aktensystem_ePA, Konnektor Highspeed, Konnektor PTV4, Konnektor PTV5, Konnektor PTV5Plus, eRp_FdV, IDP-D, Konnektor PTV4Plus, eRp_FD, KTR-AdV, Konnektor eHealth, Sich.techn. Eignung: CC-Evaluierung, funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie AdV-App, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle, <=**]**

GS-A_4390 - Asymmetrischer Anteil der hybriden Verschlüsselung binärer Daten
Produkttypen, die die hybride Verschlüsselung binärer Daten durchführen, MÜSSEN für den asymmetrischen Anteil der Verschlüsselung die folgenden Vorgaben berücksichtigen:

- Als asymmetrisches Verschlüsselungsverfahren MUSS RSAES-OAEP gemäß [PKCS#1, Kapitel 7.1] verwendet werden.
- Als Mask-Generation-Function für die Verwendung in RSAES-OAEP MUSS MGF 1 mit SHA-256 als Hash-Funktion gemäß [PKCS#1, Anhang B.2.1] verwendet werden.

[Aktensystem_ePA, Konnektor Highspeed, Konnektor PTV4, Konnektor PTV5, Konnektor PTV5Plus, eRp_FdV, IDP-D, Konnektor PTV4Plus, eRp_FD, KTR-AdV, Konnektor eHealth, Sich.techn. Eignung: CC-Evaluierung, funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Zertifizierung nach Technischer Richtlinie AdV-App, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle, <=**]**

A_22780 - E-Rezept-FdV - Einlösen ohne Anmelden - Platzhalter in URL ersetzen
Das E-Rezept-FdV MUSS, falls die für die gewählte Belieferungsoption verwendete URL Platzhalter enthält, die Platzhalter mit den entsprechenden Werten ersetzen.**[**eRp_FdV, funkt. Eignung: Test Produkt/FA, <=**]**

Für Liste der Platzhalter siehe Tabelle "Platzhalter in URL".

A_22781 - E-Rezept-FdV - Einlösen ohne Anmelden - Nachricht versenden
Das E-Rezept-FdV MUSS den verschlüsselten Datensatz an die für die gewählte Belieferungsoption verwendete URL per http-POST-Operation und dem Content-Type: application/pkcs7-mime versenden.**[**eRp_FdV, funkt. Eignung: Test Produkt/FA, <=**]**

Das folgende curl-Kommando zeigt, wie die Daten an die Schnittstelle des Apothekensystems übergeben werden:

```
curl-XPOST "https://www.megaapotheke.de/botendienst?ti_id=<TI-
ID>&transactionID=<UUID>" --header "Content-Type: application/pkcs7-mime"
--data @blob.p7c
```

A_22782 - E-Rezept-FdV - Einlösen ohne Anmelden - Returncode ungleich 200
Das E-Rezept-FdV MUSS alle Returncodes des Apothekensystems ungleich 200 als „nicht erfolgreich übertragen" interpretieren.**[**eRp_FdV, funkt. Eignung: Herstellererklärung, <=**]**

A_22783 - E-Rezept-FdV - Einlösen ohne Anmelden - Protokollierung
Das E-Rezept-FdV MUSS alle Zuweisungen, die nicht über den E-Rezept-Fachdienst erfolgen, protokollieren und für den Nutzer des E-Rezept-FdV zur Einsicht bereitstellen. Ein Protokolleintrag MUSS mindestens die E-Rezept-ID, den Namen der Empfänger-Apotheke, das Datum der Zuweisung und den Status der Zuweisung (erfolgreich, nicht erfolgreich) beinhalten.**[**eRp_FdV, funkt. Eignung: Test Produkt/FA, <=**]**

6.5 Daten- und Informationsmodell

6.5.1 Stammdatensatz der Apotheke

Der Stammdatensatz der Apotheke wird erweitert.

Attribut	verpflichtend	Beschreibung	zulässige Werte	Beispiel

telecom	nein	Zuweisungsadresse für die Belieferungsoption Abholung in Apotheke	Text, max. 1900 Zeichen	"Bundesallee 312, 12345 Berlin"
telecom	nein	Zuweisungsadresse für die Belieferungsoption Lieferung zum Versicherten durch Vor-Ort-Apotheke	Text, max. 1900 Zeichen	"Bundesallee 312, 12345 Berlin"
telecom	nein	Zuweisungsadresse für die Belieferungsoption Versand zum Versicherten durch Online-Apotheke	Text, max. 1900 Zeichen	"Bundesallee 312, 12345 Berlin"
Extension	nein	Referenz auf eine lokale FHIR-Ressource Binary, die in der Location-Ressource contained transportiert wird.	lokale Referenz	#123
contained	nein	FHIR-Ressource Binary mit CHCI.ENC-Zertifikat in Base64-DER-Codierung	Binary	

6.5.2 Message an die Apotheke

Die Message beinhaltet folgende Informationen

- Telematik-ID der adressierten Apotheke
- Transaktions-ID
- verschlüsselte Nachricht des Versicherten

Die Nachricht des Versicherten enthält folgende Informationen:

A_22784 - E-Rezept - Einlösen ohne Anmelden - Datenstruktur Nachricht
Das E-Rezept-FdV und das PS der abgebenden LEI MÜSSEN für den Anwendungsfall "Einlösen ohne Anmelden am E-Rezept-Fachdienst im E-Rezept-FdV" Nachrichten mit der folgenden Datenstruktur unterstützen.

Tabelle 3 : Einlösen ohne Anmelden - Datenstruktur Nachricht

Attribut	verpflichtend	Beschreibung	zulässige Werte	Beispiel
version	ja	Gibt die Version des JSON an. Aktuell immer 1. Kann im weiteren Lebenszyklus verändert werden.	nummerisch, bis zu 6 Stellen	1

Attribut	verpflichtend	Beschreibung	zulässige Werte	Beispiel
supplyOptionsType	ja	Wird gemäß des Servicerequests gesetzt, den der Nutzer wählt. Die für den Nutzer zur Auswahl stehenden Services gibt die Apotheke vor, indem sie den servicespezifischen Zuweisungs-Endpunkt angibt, oder nicht.	onPremise, shipment, delivery	shipment
name	nein	Das E-Rezept-FdV erlaubt dem Nutzer bei supplyOptionsType shipment oder delivery die Angabe eines alternativen Namen. Ansonsten gilt der Name auf dem E-Rezept.	Text und Ziffern 50 Stellen UTF-8	Max Müller
address	nein	Das E-Rezept-FdV erlaubt dem Nutzer bei supplyOptionsType shipment oder delivery die Angabe einer alternativen Belieferungsadresse. Ansonsten gilt die Adresse auf dem E-Rezept. Der Array enthält Straße, Hausnummer, PLZ, Ort	Text und Ziffern je Teil: 50 Stellen UTF-8	"Bundesallee", "312", "12345", "Berlin"
hint	nein	Optionale Angaben, die der Nutzer unterstützt durch das E-Rezept-FdV tätigen kann, die bei der Auslieferung hilfreich sind.	Text 500 Stellen UTF-8	Bitte im Morsecode klingeln: -.-.

Attribut	verpflichtend	Beschreibung	zulässige Werte	Beispiel
		Nur bei supplyOptionsType shipment oder delivery		
text	nein	Freitext, den der Nutzer App-unterstützt eingeben kann.	Text 500 Stellen UTF-8	Bitte zusätzlich Wicky Hustensaft, 500ml
phone	nein, siehe Beschreibung	Telefonnummer des Versicherten Das E-Rezept-FdV stellt sicher, dass bei supplyOptionsType shipment oder delivery mindestens eine Kontaktinformation (E-Mail oder Telefon) übermittelt wird	25 Stellen UTF-8	004916094858168
mail	nein, siehe Beschreibung	E-Mail-Adresse des Versicherten Das E-Rezept-FdV stellt sicher, dass bei supplyOptionsType shipment oder delivery mindestens eine Kontaktinformation (E-Mail oder Telefon) übermittelt wird	RFC-5322-konforme E-Mail-Adresse	max@musterfrau.de
transactionID	ja	Eindeutige ID zur Identifikation der Transaktion für Fehleranalyse und ggf. spätere Funktionserweiterung	RFC 4122	ee63e415-9a99-4051-ab07-257632faf985
taskID	ja	TaskID	500 Stellen UTF-8	160.123.456.789.123.58

Attribut	verpflichtend	Beschreibung	zulässige Werte	Beispiel
accessCode	ja	AccessCode	25 Stellen UTF-8	777bea0e13cc9c42ceec14aec3ddee2263325dc2c6c699db115f58fe423607ea

[PS_E-Rezept_abgebend, eRp_FdV, funkt. Eignung: Herstellererklärung, funkt. Eignung: Test Produkt/FA, <=**]**

Ein Beispiel für die ausgetauschte JSON-Struktur findet sich oben in Abschnitt 5.

6.6 Datenschutz und Sicherheit

Die in diesem Dokument spezifizierte Lösung trägt der Situation Rechnung, dass die Anmeldung am E-Rezept-Fachdienst mittels NFC-fähiger eGK und PIN-Eingabe aus verschiedenen Gründen für viele Versicherte eine große Hürde darstellt.

Diese Lösung trägt also bis zur Einführung einer komfortabel nutzbaren elektronischen Identität für Versicherte und wird dann obsolet.

Obwohl es sich also um eine Übergangslösung handelt, besteht das Ziel, die Lösung sicher zu gestalten. Dementsprechend wird der zu übermittelnde E-Rezept-Token mit einem (SMC-B)-Zertifikat verschlüsselt, dessen zugehöriger privater Schlüssel in alleiniger Hoheit der Empfänger-Apotheke liegt. Der in der Kommunikation zwischen E-Rezept-FdV und Apotheke geschaltete Dienstleister kann somit nicht auf den E-Rezept-Token in Klartext zugreifen. Gleiches gilt für die damit verbundene Nachricht des Versicherten an die Apotheke und die darin ggf. befindlichen personenbezogenen Daten.

Insofern muss der zwischengeschaltete Dienstleister auch keine Nachweise über seine (betrieblichen) Sicherheitsmaßnahmen erbringen. Dieser Dienstleister liegt mit seiner Technik, seinen Prozessen und seiner Verbindung zu den Apotheken außerhalb der Grenzen der Sicherheitsleistung der TI.

Da die Kommunikation vom E-Rezept-FdV zur Apotheke nicht über den E-Rezept-Fachdienst läuft, kann letzterer hierfür auch keine Protokolleinträge (Audit-Log) erstellen. Dies erfolgt lokal im E-Rezept-FdV - mit der Folge, dass die Protokolleinträge nicht von der E-Rezept-AdV oder einem E-Rezept-FdV auf einem anderen mobilen Gerät des Versicherten eingesehen werden können.

6.7 Betrieb

Die Kommunikation des Versicherten muss im Fehlerfall in Richtung der Apotheke gelenkt werden, da nur diese den Support in Richtung des durch sie genutzten AVS herstellen kann. Das E-Rezept-FdV muss durch entsprechende Hinweise in der Benutzerführung den Versicherten diesbezüglich anleiten. Der TI-Service-Desk (TISD) muss den Versicherten bei Kontaktaufnahme ebenfalls in die Richtung des abgebenden Leistungserbringers lenken.

Alle teilnehmenden AVS-Hersteller sollen am IT-Service-Management der TI (TI-ITSM) teilnehmen, damit auftretende Probleme im Zusammenspiel mit dem E-Rezept-FdV abgewickelt werden können.

7 Dokumentenhaushalt

7.1 Übersicht betroffener Dokumente

Dieses Dokument beschreibt das Feature als geschlossene funktionale Einheit. Mit der Freigabe zur Umsetzung werden die hier getroffenen Festlegungen in einem nachgelagerten Wartungsrelease in die jeweiligen Produkt- und Anbietertypspezifikationen überführt.

Dokument	Titel
[gemILF_PS_eRp]	gematik: Spezifikation Implementierungsleitfaden Primärsysteme – E-Rezept
[gemSpec_eRp_APOVZD]	gematik: Spezifikation Apothekenverzeichnis im E-Rezept
[gemSpec_eRp_FdV]	gematik: Spezifikation E-Rezept Frontend des Versicherten

7.2 Übersicht Produkt- und Anbietertypen

<Optional: Eine Übersicht neuer / betroffener Produkt und Anbietertypen>

8 Anhang A – Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
ADAS	Bundesverband Deutscher Apothekensoftwarehäuser e.V.
APOVZD	Apothekenverzeichnis im E-Rezept
AVS	Apothekenverwaltungssystem
DVO	Dienstleister vor Ort
FdV	Frontend des Versicherten
KIM	Kommunikation im Medizinwesen
NGDA	Netzgesellschaft Deutscher Apotheker
PIN	Personal Identification Number
SMC-B	Security Module Card Typ B, Institutionenkarte
TI	Telematikinfrastruktur
TI-ITSM	IT-Service-Management der TI
TISD	TI-Service-Desk
TLS	Transport Layer Security
VZD	Verzeichnisdienst der TI

8.2 Referenzierte Dokumente

8.2.1 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

783 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der
784 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die
785 vorliegende Version aufgeführt wird.

786

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemILF_PS]	Implementierungsleitfaden Primärsysteme – Telematikinfrastruktur (TI)
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs

787

788 8.2.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC4122]	Network Working Group https://www.ietf.org/rfc/rfc4122.txt
[ADAS-A2B-eRezept]	ADAS - A2B - eRezept - Services https://app.swaggerhub.com/apis/ADAS-A2B-Services/adas-a2b-erezept/1.0.0

789