Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
E-Rezept-Fachdienst

Version:	1.0.1
Revision:	241866
Stand:	06.07.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_FD_eRp

Dokumentinformationen

Hinweis:

Die Speicherung von Dispensierinformationen im E-Rezept ist noch nicht abschließend geklärt. Ggf. notwendige Anpassungen werden mit dem Folgerelease 4.0.1 veröffentlicht.

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.06.2020		freigegeben	gematik
			Aktualisierung Hinweis zu Dispensierinformation	gematik
1.0.1	06.07.20		freigegeben	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 9

3.1 Nachbarsysteme 9

3.2 Akteure und Rollen 9

4 Zerlegung des Produkttyps 11

5 Übergreifende Festlegungen 12

5.1 Servicelokalisierung 12

5.2 Authentifizierung von Nutzern 14

5.2.1 Registrierung beim Identity Provider 14

5.2.2 Claims der Identitätsbestätigung 15

5.2.3 Verwaltung der Nutzersession 16

5.3 Fehlercodes 17

5.4 Protokollierung 20

5.5 Löschfristen 23

5.6 Sicherheit 24

5.6.1 Allgemeine Sicherheitsanforderungen 24

5.6.2 Identifikation des Clientsystems 24

5.6.3 TSL und OCSP-Status 25

5.6.4 Sicherheit der Netzübergänge 26

5.6.5 Vertrauenswürdige Ausführungsumgebung 28

5.6.5.1 Verarbeitungskontext 28

5.6.5.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld 30

5.6.5.3 Konsistenz des Systemzustands, Logging und Monitoring 32

5.6.5.4 Client-Verbindungen zum Verarbeitungskontext 32

6 Funktionsmerkmale 34

6.1 Ressource Task 35

6.1.1 HTTP-Operation GET 35

6.1.2 HTTP-Operation POST 36

6.1.2.1 POST /Task/$create 36

6.1.2.2 POST /Task/<id>/$activate 38

6.1.2.3 POST /Task/<id>/$accept ... 40
6.1.2.4 POST /Task/<id>/$reject ... 41
6.1.2.5 POST /Task/<id>/$close ... 42
6.1.2.6 POST /Task/<id>/$abort ... 43
6.2 Ressource MedicationDispense ... 45
6.2.1 HTTP-Operation GET /MedicationDispense ... 45
6.3 Ressource Communication ... 46
6.3.1 HTTP-Operation GET ... 46
6.3.1.1 GET /Communication/ ... 47
6.3.2 HTTP-Operation POST ... 47
6.3.2.1 POST /Communication/ ... 47
6.4 Ressource AuditEvent ... 49
6.4.1 HTTP-Operation GET /AuditEvent ... 49
7 Informationsmodell ... 51
8 Anhang A – Verzeichnisse ... 53
8.1 Abkürzungen ... 53
8.2 Glossar ... 53
8.3 Abbildungsverzeichnis ... 54
8.4 Tabellenverzeichnis ... 54
8.5 Referenzierte Dokumente ... 54
8.5.1 Dokumente der gematik ... 54
8.5.2 Weitere Dokumente ... 55

1 Einordnung des Dokumentes

1.1 Zielsetzung

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

1.2 Zielgruppe

Das Dokument richtet sich an den Hersteller des E-Rezept-Fachdienstes, sowie an Hersteller und Anbieter von weiteren Produkttypen der Fachanwendung E-Rezept.

1.3 Geltungsbereich

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

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

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A5).

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

Nicht Bestandteil des vorliegenden Dokumentes sind die informativen Ergänzungen zur Nutzung der Schnittstellen des E-Rezept-Fachdienstes in der separaten API-Dokumentation, sowie zur Profilierung der verwendeten FHIR-Ressourcen.

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

1.5.1 Hinweis auf offene Punkte

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

Beispiel für einen offenen Punkt.

2 Systemüberblick

Der E-Rezept-Fachdienst verwaltet E-Rezepte in der Telematikinfrastruktur als ein zentraler Ressourcenserver auf Basis des FHIR-Standards mit einer RESTful API. Die Rezepte werden dabei über eine eindeutige Ressourcen-ID (Rezept-ID) adressiert. Zusätzlich protokolliert der E-Rezept-Fachdienst alle Zugriffe auf ein E-Rezept für den Versicherten und verwaltet die Statusübergänge eines E-Rezepts. Für einen Nachrichtenaustausch zwischen Apotheken und Versicherten über die Verfügbarkeit von Medikamenten, die Belieferung von E-Rezepten und der Vertretung beim Einlösen eines E-Rezepts ist zusätzlich eine Kommunikation über den E-Rezept-Fachdienst möglich.

Der E-Rezept-Fachdienst realisiert die Vertraulichkeit und Integrität der verarbeiteten Daten über das Konzept der vertrauenswürdigen Ausführungsumgebung (VAU), die eine durchgängige Verschlüsselung der E-Rezepte und der dazu gehörigen Daten aus einer Kombination kryptografischer Verfahren während des Transports, der vertrauenswürdigen Verarbeitung und in der verschlüsselten Persistierung der Daten sicherstellt.

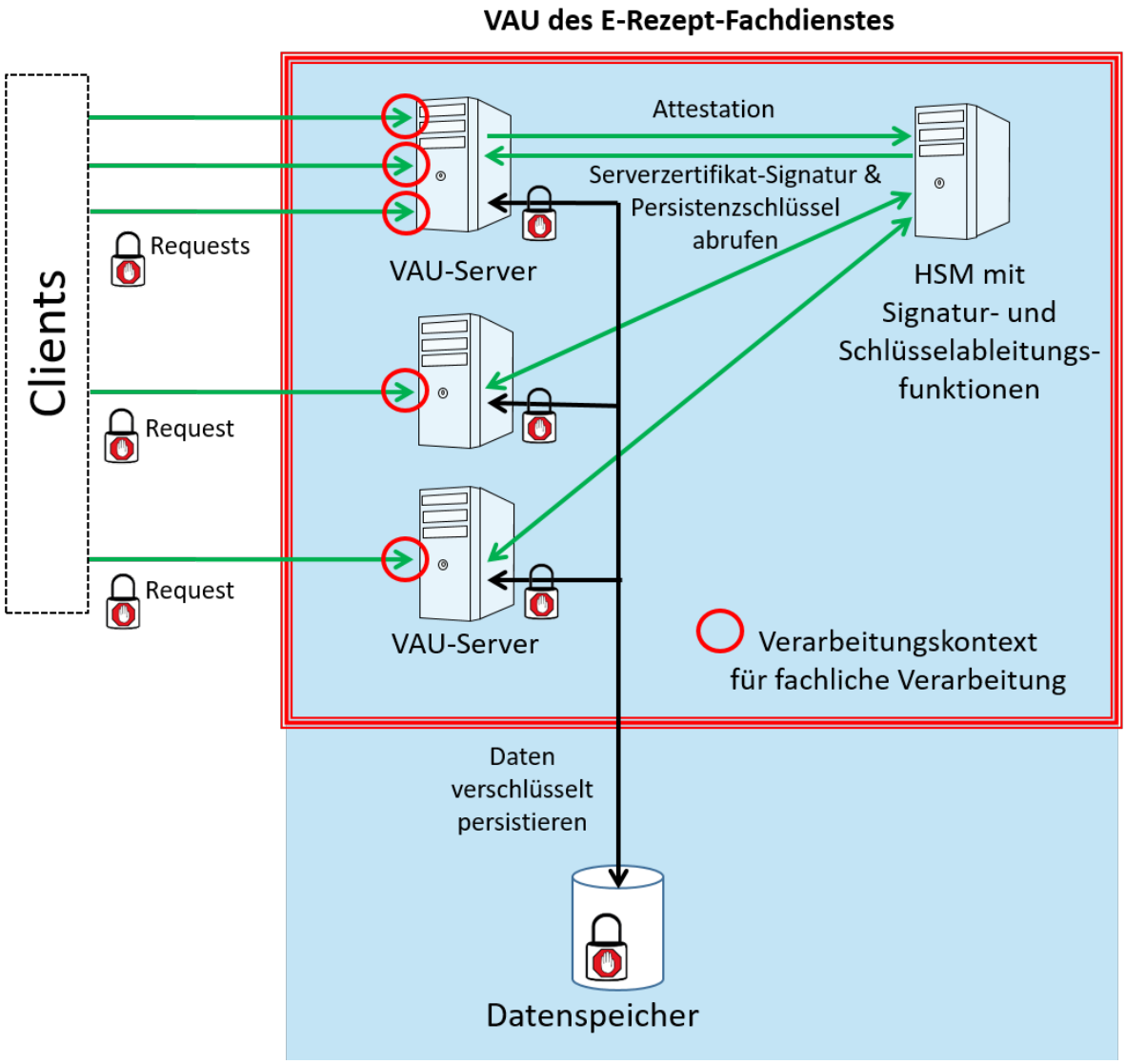


Abbildung 1 Systemüberblick

3 Systemkontext

Der E-Rezept-Fachdienst stellt Schnittstellen für die Verwaltung von E-Rezepten und für den Nachrichtenaustausch bereit. Diese werden von Leistungserbringerorganisationen und Versicherten genutzt, die über ihre jeweiligen Clientsysteme auf den E-Rezept-Fachdienst zugreifen.

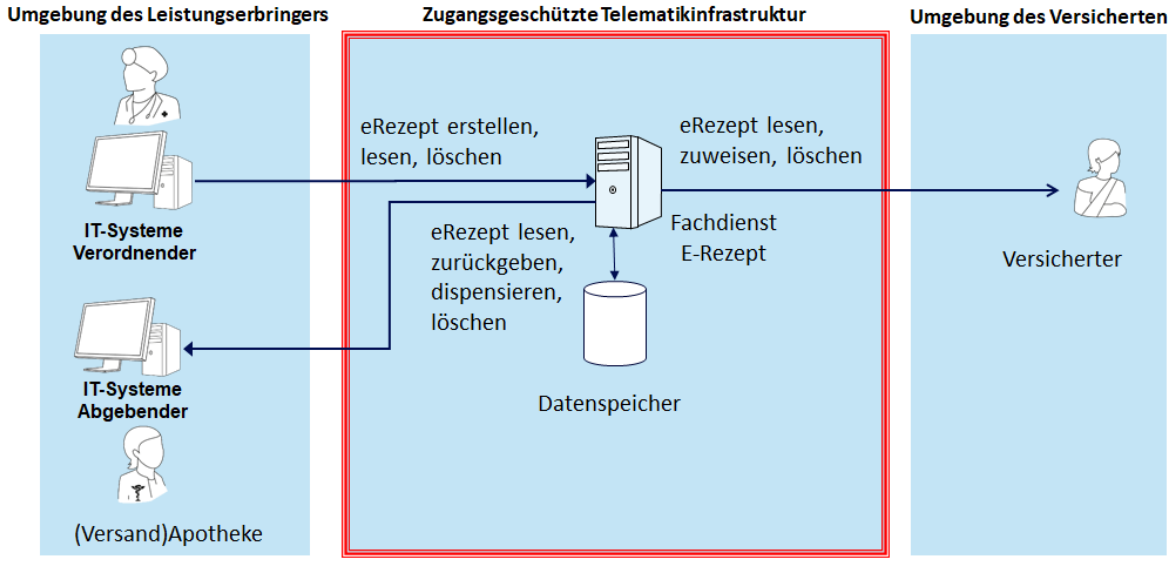


Abbildung 2 Systemkontext E-Rezept-Fachdienst

3.1 Nachbarsysteme

Die Schnittstellen des E-Rezept-Fachdienstes werden durch die Praxisverwaltungs- und Krankenhausinformationssysteme der verordnenden Leistungserbringer im Verordnungsprozess genutzt. Die Apothekenverwaltungssysteme nutzen die Schnittstellen des E-Rezept-Fachdienstes im Rahmen der Dispensierung. Außerdem werden sie vom E-Rezept-Frontend des Versicherten (E-Rezept-FdV) aufgerufen. Als Fachdienst der Telematikinfrastruktur bedient sich der E-Rezept-Fachdienst der weiteren Infrastrukturdienste wie TSP für die Gültigkeitsabfrage für Signaturzertifikate, des HBA (für QES-Prüfung) und des IdentityManagements, bei dem ein IdP Identitätsbestätigungen (ID-Token) für Nutzer im Rahmen eines Sessionmanagements für das Single Sign-On ausstellt.

3.2 Akteure und Rollen

Leistungserbringerinstitutionen und Versicherte weisen sich gegenüber dem E-Rezept-Fachdienst mit einer Identitätsbestätigung (ID_TOKEN) aus, die sie von einem Identitätsprovider, z.B. SmartCard-IdP, beziehen. In diesen ID-Token ist ihre Rollen-OID sowie ihr Identitätskennzeichen Versicherten-ID (10-stelliger Anteil der KVNR) bzw. Telematik-ID enthalten. Anhand der jeweiligen Rolle wird die Zulässigkeit einer aufgerufenen Operation geprüft. Das Identitätskennzeichen wird für die Protokollierung

von Zugriffen sowie die Zuordnung von Datensätzen, insbesondere bei E-Rezepten zu Versicherten, genutzt.

4 Zerlegung des Produkttyps

Der E-Rezept-Fachdienst verwaltet E-Rezepte über einen medizinischen Workflow. Dabei muss er die Vertraulichkeit und Integrität der verarbeiteten Daten sicherstellen. Daraus ergeben sich Sicherheitsanforderungen an die Betriebsumgebung, an die Fachlogik der Prozessverarbeitung sowie an die Ausführungsumgebung des Programmcodes.

A_19586 - Anbieter E-Rezept-Fachdienst Speicherung Schlüsselmaterial in HSM
Der Anbieter des E-Rezept-Fachdienstes MUSS das private Schlüsselmaterial für kryptografische Verfahren (Entschlüsselung, Signaturen) in einem HSM speichern, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria, ITSEC oder Federal Information Processing Standard (FIPS) in Frage.
Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3,
2. Common Criteria EAL 4+ mit hohem Angriffspotenzial oder
3. ITSEC E3 der Stärke „hoch" entsprechen.

[<=]

Eine über die Schlüsselspeicherung in einem Hardware Security Module (HSM) hinausgehende Anforderung an die Zerlegung des E-Rezept-Fachdienstes gibt es aus funktionaler Sicht nicht.

5 Übergreifende Festlegungen

Der folgende Abschnitt beschreibt übergreifende Anforderungen an den E-Rezept-Fachdienst zur Unterstützung der Fachlogik.

5.1 Servicelokalisierung

Die Schnittstellen des E-Rezept-Fachdienstes werden über verschiedene Netzsegmente von Leistungserbringern und Versicherten aufgerufen. Dafür müssen diese Schnittstellen über DNS-Abfragen lokalisierbar sein.

A_19410 - Anbieter E-Rezept-Fachdienst - PTR für Anbieterliste (RFC Service-Discovery)
Der Anbieter des E-Rezept-Fachdienstes MUSS DNS PTR, SRV und TXT Resource Records im Namensraum der TI gemäß folgender Tabelle verwalten.

Tabelle 1: TAB_eRPFD_001 Service Discovery

Resource Record Bezeichner	Resource Record Type	Beschreibung
_erp._tcp.erp.telematik	PTR	Ermittlung der E-Rezeptschnittstelle <erp_service_name>
<erp_service_name>	SRV und TXT	SRV Resource Record zur Ermittlung des FQDN des E-Rezept-Dienstes TXT Resource Record zur Ermittlung des Pfades der URL zum E-Rezept-Dienst "path=<Bezeichner der Schnittstelle als Pfadbestandteil (ohne /) >"

[<=]

Der Eintrag <erp_service_name> ist als Variable zu verstehen und kann zum Beispiel für die Namensauflösung durch die Primärsysteme folgende Ausprägung besitzen:

```
_erp._tcp.erp.telematik 86400 IN PTR _erp-fd._tcp.erp.telematik

_erp-fd._tcp.erp.telematik 86400 IN SRV 5 10 443 erp-
srv.zentral.erp.telematik

_erp-fd._tcp.erp.telematik 86400 IN TXT „txtvers=1“ „path=/“
```

A_19411 - Anbieter E-Rezept-Fachdienst - Resource Records FQDN eRP
Der Anbieter des E-Rezept-Fachdienstes MUSS im Namensraum der TI und in den Nameservern Internet die Ressource Records gemäß nachstehender Tabelle verwalten.

Tabelle 2: TAB_eRPFD_002 FQDN

Resource Record Bezeichner	Resource Record Type	Beschreibung

erp-srv.zentral.erp.telematik	A Record	A Resource Records zur Namensauflösung von FQDN des E-Rezept-Fachdienstes in IP-Adressen im Namensraum der TI
erp-srv.zentral.erp.ti-dienste.de	A Record	A Resource Records zur Namensauflösung von FQDN des E-Rezept-Fachdienstes in IP-Adressen im Namensraum Internet
erp-srv.zentral.erp.ti-dienste.de	AAAA Record	AAAA Resource Records zur Namensauflösung von FQDN des E-Rezept-Fachdienstes in IP-Adressen im Namensraum Internet
_erp._tcp.erp.ti-dienste.de	TXT	TXT Resource Records zur Ermittlung der Aufruf-Schnittstelle des E-Rezept-Fachdienstes. Der für die Adressierung benötigte Resource Record MUSS bereitgestellt werden. Das in den Klammern angegebene Kürzel MUSS verwendet werden. • E-Rezept-Schnittstelle (erp) • OCSP-Status-Proxy (ocspf) Das key/value-Paar des TXT-Records hat folgende Struktur (die spitzen Klammern dienen der Abgrenzung eines Wertes): "erp=<Schnittstelle E-Rezept>"

[<=]

Exemplarisch können die DNS-Einträge im Namensraum Internet für den E-Rezept-Fachdienst wie folgt aussehen:

```
_erp._tcp.erp.ti-dienste.de 86400 IN TXT „txtvers=1“ „path=/“
erp-srv.zentral.erp.ti-dienste.de IN A 10.28.2.42
erp-srv.zentral.erp.ti-dienste.de IN AAAA
```

A_19412 - Anbieter E-Rezept-Fachdienst - Schnittstellenadressierung
Der Anbieter des E-Rezept-Fachdienstes MUSS die im Internet angebotene Schnittstelle des E-Rezept-Fachdienstes unter der folgenden URL zur Verfügung stellen:
`https://<FQDN aus DNS Lookup>:443/<Aufrufschnittstelle aus TXT Record "path">`

`z.B. erp.zentral.erp.ti-dienste.de/`
[<=]

Um Benutzern den Umgang mit E-Rezepten zu erleichtern, wird die Nutzung der Endnutzeranwendung E-Rezept-FdV als App auf ihrem privaten Smartphone empfohlen. Der E-Rezept-Fachdienst unterstützt dabei die App-Nutzung durch Digital Asset Links (für Android) [DAL_ANDROID] und Universal Links (für iOS/macOS) [UL_APPLE].

A_19695 - E-Rezept-Fachdienst - Android Digital Asset Link
Der E-Rezept-Fachdienst MUSS ein Asset Link Statementgemäß [DAL_ANDROID] mit der Liste der Hashwerte der aktuell zugelassenen Android-Versionen des E-Rezept-FdV für den Wert "`sha256_cert_fingerprints`" unter der Internetadresse`https://<FQDN für`

`DNS Lookup>/.well-known/assetlinks.json` veröffentlichen und pflegen, damit Versicherte mit einem Android-Smartphone E-Rezepte standardmäßig mit dem E-Rezept-FdV verwalten können.**[<=]**

5.2 Authentifizierung von Nutzern

Die Identifikation von Nutzern erfolgt nach dem Standard OpenID-Connect, hierfür stellt ein IdentityProvider der Telematikinfrastruktur ID_TOKEN für Nutzer aus, die er anhand ihrer identifizierenden Merkmale (z.B. eGK, SMC-B) authentifiziert.

5.2.1 Registrierung beim Identity Provider

Der E-Rezept-Fachdienst delegiert die Authentifizierung von Nutzern an einen Identity Provider. Für diesen Zweck muss er sich bei diesem als Relying Party registrieren und die für die Fachlogik notwendigen Attribute in den Identitätsbestätigungen (ID_TOKEN) festlegen. Die Umsetzung des IdentityManagements über IdentityProvider startet mit einem einzelnen IdP (SmartCard-IdP), später werden weitere IdentityProvider bei den verschiedenen identitätsbestätigenden Stellen realisiert. Verwaltet ein solcher IdP Identitäten von Nutzern der Telematikinfrastruktur und gilt als vertrauenswürdig für die Umsetzung von UseCases unter Nutzung der Schnittstellen des E-Rezept-Fachdienstes, obliegt es dem E-Rezept-Fachdienst, sich bei diesem IdP als RelyingParty zu registrieren.

A_19985 - Anbieter E-Rezept-Fachdienst - Registrierung beim IdP als Relying Party
Der Anbieter des E-Rezept-Fachdienstes MUSS sich über einen organisatorischen Prozess bei einem vertrauenswürdigen IdentityProvider (IdP) der Telematikinfrastruktur als Relying Party registrieren und die Bereitstellung der folgenden Claims in für Nutzer ausgestellte ID_TOKEN mit dem IdP vereinbaren:

- `professionOID`
- `name`
- `sub`
- `acr`

damit der E-Rezept-Fachdienst die Fachlogik der Autorisierung und Protokollierung auf diesen Attributen umsetzen kann.**[<=]**

A_19986 - Anbieter E-Rezept-Fachdienst - E-Rezept-Sessiondauer im IdP
Der Anbieter des E-Rezept-Fachdienstes MUSS bei der Registrierung als Relying Party im IdP die Ausstellung von RefreshToken für Authentifizierte Nutzer für die maximale Dauer von 12 Stunden erlauben, sodass der IdP spätestens 12 Stunden nach `auth_time` eine Re-Authentifizierung des Nutzers erzwingt.**[<=]**

A_19987 - Anbieter E-Rezept-Fachdienst - URI für öffentl. Schlüssel Tokenverschlüsselung
Der Anbieter des E-Rezept-Fachdienstes MUSS bei der Registrierung als Relying Party im IdP die beiden URI bzw. FQDN der Schnittstellen im Namensraum der TI und im Internet sowie die Abrufadresse des öffentlichen Schlüssels PUK_FD mit Angabe des zu verwendenden Algorithmus für die Verschlüsselung des ID_TOKEN dem IdentityProvider bekannt machen.**[<=]**

A_19993 - E-Rezept-Fachdienst - Entschlüsselung eingehender ID_TOKEN
Der E-Rezept-Fachdienst MUSS jedes mit einem eingehenden HTTP-Request übergebene ID_TOKEN mit dem zum veröffentlichten öffentlichen Schlüssel PUK_FD gehörenden privaten Schlüssel entschlüsseln und unverschlüsselt eingehende ID_TOKEN mit dem HTTP-Status-Code 401 abweisen.**[<=]**

5.2.2 Claims der Identitätsbestätigung

A_19130 - E-Rezept-Fachdienst - Authentifizierung erforderlich LEI-Endpunkt
Der E-Rezept-Fachdienst MUSS alle eingehenden HTTP-Requests über den Endpunkt für Leistungserbringerinstitutionen mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "`WWW-Authenticate: Bearer realm='prescriptionserver.telematik'`

scope=openid profile prescriptionservice.lei"abweisen, die kein ID_TOKEN als JSON-Web-Token-Format gemäß [JWT] im HTTP-Request-Header "Authorization" bereitstellen, damit ausschließlich authentifizierte Nutzer Zugriff auf die HTTP-Schnittstelle des E-Rezept-Fachdienstes erhalten.**[<=]**

A_19389 - E-Rezept-Fachdienst - Authentifizierung erforderlich Vers-Endpunkt
Der E-Rezept-Fachdienst MUSS alle eingehenden HTTP-Requests über den Endpunkt für den Zugriff für Versicherte mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "`WWW-Authenticate: Bearer realm='prescriptionserver.telematik'`

scope=openid profile prescriptionservice.vers"abweisen, die kein ID_TOKEN als JSON-Web-Token-Format gemäß [JWT] im HTTP-Request-Header "Authorization" bereitstellen, damit ausschließlich authentifizierte Nutzer Zugriff auf die HTTP-Schnittstelle des E-Rezept-Fachdienstes erhalten.**[<=]**

A_19131 - E-Rezept-Fachdienst - Authentifizierung ungültig
Der E-Rezept-Fachdienst MUSS alle eingehenden HTTP-Requests mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "`WWW-Authenticate: Bearer realm='prescriptionserver.telematik', error='invalid_token'`"abweisen, die ein unsigniertes oder ungültiges ID_TOKEN im HTTP-Request-Header "Authorization" bereitstellen, damit ausschließlich authentifizierte Nutzer Zugriff auf die HTTP-Schnittstelle des E-Rezept-Fachdienstes erhalten.**[<=]**

A_19902 - E-Rezept-Fachdienst - Authentifizierung abgelaufen
Der E-Rezept-Fachdienst MUSS alle eingehenden HTTP-Requests mit dem HTTP-Fehlercode 401 und dem HTTP-Response-Header "`WWW-Authenticate: Bearer realm='prescriptionserver.telematik', error='invalid_token'`"abweisen, die ein ID_TOKEN im HTTP-Request-Header "Authorization" bereitstellen, dessen Gültigkeitsendezeitpunkt "`exp`" älter als die aktuelle Systemzeit oder dessen Ausstellzeitpunkt "`iat`" älter als die aktuelle Systemzeit - 5 Minuten ist, damit ausschließlich authentifizierte Nutzer Zugriff auf die HTTP-Schnittstelle des E-Rezept-Fachdienstes erhalten.**[<=]**

A_19132 - E-Rezept-Fachdienst - Authentifizierung Signaturprüfung
Der E-Rezept-Fachdienst MUSS die Signatur jedes im HTTP-Header "Authorization" eines eingehenden HTTP-Requests übergebenen JSON-Web-Tokens gemäß [JWS] prüfen und bei Ungültigkeit oder bei Signatur durch einen IdentityProvider, bei dem der E-Rezept-Fachdienst nicht als Relying Party registriert ist, den HTTP-Request mit dem HTTP-Fehlercode 401 abweisen.**[<=]**

A_19390 - E-Rezept-Fachdienst - Authentifizierung Nutzerrolle
Der E-Rezept-Fachdienst MUSS die fachliche Rolle eines Nutzers in jedem Operationsaufruf anhand des Attributs "`professionOID`" im übergebenen IdP-Token im

HTTP-Header "Authorization" feststellen und für die nachfolgende Rollenprüfung je Operationsaufruf verwenden.**[<=]**

A_19391 - E-Rezept-Fachdienst - Authentifizierung Nutzername
Der E-Rezept-Fachdienst MUSS den Namen eines Nutzers in jedem Operationsaufruf anhand des Attributs "`name`" im übergebenen IdP-Token im HTTP-Header "Authorization" feststellen und für die Protokollierung des Zugriffs auf personenbezogene medizinische Daten je Operationsaufruf verwenden.**[<=]**

A_19392 - E-Rezept-Fachdienst - Authentifizierung Nutzerkennung
Der E-Rezept-Fachdienst MUSS die Nutzerkennung (10-stelliger Teil der KVNR, Telematik-ID für Leistungserbringerinstitutionen) eines Nutzers in jedem Operationsaufruf anhand des Attributs "`sub`" im übergebenen IdP-Token im HTTP-Header "Authorization" feststellen und für die Protokollierung des Zugriffs auf personenbezogene medizinische Daten je Operationsaufruf verwenden.**[<=]**

A_19439 - E-Rezept-Fachdienst - Authentifizierung Authentifizierungsstärke
Der E-Rezept-Fachdienst MUSS die Authentifizierungsstärke des übergebenen IdP-Token anhand des Attributs "`acr`" im übergebenen IdP-Token im HTTP-Header "Authorization" auf dem Authentifizierungsniveau "hoch" feststellen und einen anderen Wert als bzw. ein Authentifizierungsniveau unterhalb von "`http://eidas.europa.eu/LoA/high`" mit dem HTTP-Status-Code 401 ablehnen. **[<=]**

5.2.3 Verwaltung der Nutzersession

Der IdentityProvider übernimmt für den E-Rezept-Fachdienst als Relying Party die Verwaltung von Nutzersessions. Um neben der kryptografischen Gültigkeit von übergebenen ID_TOKENs auch gegen die Laufzeit der Nutzersession zu prüfen, nutzt der E-Rezept-Fachdienst die Möglichkeit der Token Introspection beim Identity Provider. Das heißt, die Gültigkeit des vom Nutzer vorgelegten ID_TOKEN wird beim erstmaligen Vorlegen und nach der Hälfte der angegebenen Laufzeit des ID_TOKEN beim Identity Provider abgefragt.

A_19991 - E-Rezept-Fachdienst - Regelmäßige Token Introspection
Der E-Rezept-Fachdienst MUSS ein erstmalig sowie ein nach der Hälfte der spezifizierten Gültigkeitsdauer (iat - exp / 2) vom Nutzer übergebenes ID_TOKEN auf Gültigkeit gemäß [gemSpec_IDP_FD#Token Introspection Request] beim Identity Provider prüfen und bei einer Token Introspection Response mit `"active": "false"` gemäß [RFC7662#SECTION-2.2] den eingegangenen HTTP-Request mit dem HTTP-Status-Code 401 ablehnen, damit eine zwischenzeitlich im Identity Provider beendete Nutzersession nicht durch Weiterbenutzung des ID_TOKEN fortgeführt wird.**[<=]**

A_19992 - E-Rezept-Fachdienst - Blacklisting zu häufig verwendeter ID_TOKEN
Der E-Rezept-Fachdienst MUSS ein während einer konfigurierbaren Dauer vielfach vorgelegtes ID_TOKEN (z.B. mehr als 10 mal innerhalb einer Sekunde) für den Rest der angegebenen Gültigkeitsdauer auf einer Blacklist führen und eingehende HTTP-Requests mit diesem ID_TOKEN mit dem HTTP-Status-Code 429 ablehnen, damit ein Überlastungsangriff (DOS-Attacke) auf den E-Rezept-Fachdienst unterbunden werden kann.**[<=]**

A_20158 - E-Rezept-Fachdienst - Prüfung Signaturzertifikat IdP
Der E-Rezept-Fachdienst MUSS mindestens einmal täglich das Signatur-Zertifikat des IdP-Dienstes für die Signatur von ID_TOKEN gemäß [gemSpec_PKI#TUC_PKI_018] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 3 : TAB_eRPFD_005 Parameter Prüfung Signaturzertifikat IdP

Parameter	
Zertifikat	Signaturzertifikat des IdP (eingebettet in ID_TOKEN) C.FD.SIG
PolicyList	oid_fd_sig
intendedKeyUsage	nonRepudiation
intendedExtendedKeyUsage	(leer)
OCSP-Graceperiod	60 Minuten
Offline-Modus	nein
Prüfmodus	OCSP

Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig] befunden werden und der HTTP-Request andernfalls mit dem HTTP-Status-Code 401 abgelehnt werden, damit sichergestellt wird dass, ausschließlich ID_TOKEN von einem vertrauenswürdigen IdP akzeptiert werden.**[**<=**]**

5.3 Fehlercodes

Der E-Rezept-Fachdienst stellt eine http-Schnittstelle für den Aufruf durch Clientsysteme bereit. Das Ergebnis der Operation wird in der Verwendung von http-StatusCodes [HTTP-STATUS-CODES] mitgeteilt. Die folgende Tabelle listet die vom E-Rezept-Fachdienst genutzten http-StatusCodes auf.

A_19514 - E-Rezept-Fachdienst - Http-Status-Codes
Der E-Rezept-Fachdienst MUSS die in der folgenden Tabelle aufgelisteten HTTP-Status-Codes im http-Response-Header der aufgerufenen Operation gemäß der angegebenen Bedingung zurückgeben.

Table 1 TAB_eRPFD_003 Übersicht HTTP-Statuscodes

HTTP-Status-Code	Bedeutung	in welchen Operationen als Statuscode möglich	Bedingung
200	Operation erfolgreich beendet, in der Rückgabe ist ggfs. das Ergebnis der Operation enthalten	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/<id>/$activate POST /Task/<id>/$accept POST /Task/<id>/$close	Die Operation wurde erfolgreich bearbeitet. In der Rückgabe sind die erzeugten bzw. gelesenen Daten enthalten.

201	Neues Objekt wurde erfolgreich angelegt, in der Rückgabe ist das Objekt enthalten	POST /Task/<id>/$create POST /Communication	Der E-Rezept-Fachdienst hat die Ressource in der angeforderten Operation erzeugt.
204	Die Operation liefert keinen Rückgabewert	POST /Task/<id>/$abort POST /Task/<id>/$reject	Das Löschen eines E-Rezepts löscht alle personenbezogenen und medizinischen Daten, daher gibt es keine Daten in der Rückgabe der Operation. Das Zurückweisen eines Rezepts bedeutet die Nicht-Bearbeitung durch eine Apotheke, daher sind hier keine Rückgabedaten erforderlich.
400	Bad Request, der Operationsaufruf enthält ungültige Daten.	POST /Task/$create POST /Task/<id>/$activate POST /Task/<id>/$accept POST /Task/<id>/$reject POST /Task/<id>/$close POST /Task/<id>/$abort POST /Communication	In der aufgerufenen Operation werden vom Client Daten für die Verarbeitung erwartet. Entsprechen sie nicht dem erwarteten FHIR-Profil oder sind sie ungültig (bspw. Signatur), werden sie vom E-Rezept-Fachdienst zurückgewiesen.
401	Der Nutzer konnte nicht authentifiziert werden	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/$create POST /Task/<id>/$activate POST /Task/<id>/$accept POST /Task/<id>/$reject POST /Task/<id>/$close POST /Task/<id>/$abort POST /Communication	Der Aufruf enthält keine oder abgelaufene oder ungültige Authentifizierungsinformationen im HTTP-Request-Header "`Authorization`"
403	Der Nutzer ist nicht berechtigt, die aufgerufene Operation anzufordern	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/$create POST /Task/<id>/$activate POST /Task/<id>/$accept POST /Task/<id>/$reject POST /Task/<id>/$close	Gemäß Rollenprüfung in jedem Operationsaufruf sind nur bestimmte Operationen je aufrufendem Nutzer zulässig.

		POST /Task/<id>/$abort POST /Communication	
404	Die adressierte Ressource wurde nicht gefunden.	GET /Task/<id> POST /Task/<id>/$activate POST /Task/<id>/$accept POST /Task/<id>/$reject POST /Task/<id>/$close POST /Task/<id>/$abort GET /AuditEvent/<id> GET /Communication/<id> GET /MedicationDispense/<id>	Die über die <id> adressierte Ressource existiert nicht, d.h. wurde auch nicht zwischenzeitlich gelöscht (siehe Code 410).
405	Die Anfrage ist gültig, jedoch in Kombination mit anderen Aufrufparametern nicht gültig	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/$create POST /Task/<id>/$activate POST /Task/<id>/$accept POST /Task/<id>/$reject POST /Task/<id>/$close POST /Task/<id>/$abort POST /Communication	In der Operation wird eine unzulässige Kombination aus http-Operation auf eine bestimmte Ressource ggfs. in Verbindung mit einer FHIR-Operation aufgerufen, z.B. POST /AuditEvent POST /Task/$activate POST /Task/<id>/$create PUT /<Ressource>/ HEAD /<Ressource> DELETE /<Ressource/> PATCH /<Ressource>
408	Request Timeout. Die Anfrage konnte innerhalb der erwarteten Zeit nicht beantwortet werden	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/$create POST /Task/<id>/$activate POST /Task/<id>/$accept POST /Task/<id>/$reject POST /Task/<id>/$close POST /Task/<id>/$abort POST /Communication	Der E-Rezept-Fachdienst ist überlastet und kann die Anfrage innerhalb der Wartezeit des Clients (PVS, AVS, FdV) nicht beantworten
409	Konflikt im Aufruf verschiedener Nutzer um das gleiche Objekt	POST /Task/<id>/$accept POST /Task/<id>/$abort	Das E-Rezept befindet sich bereits in Belieferung durch einen Apotheker. Daher kann es vom Verordnenden und Versicherten nicht gelöscht werden ($abort) und von keinem anderen Apotheker

			heruntergeladen werden ($accept)
410	Das aufgerufene Objekt wurde zwischenzeitlich gelöscht	GET /Task/<id> POST /Task/<id>/$accept POST /Task/<id>/$abort	Der Client (PVS, AVS, FdV) versucht ein E-Rezept zu lesen, das zwischenzeitlich gelöscht wurde
429	Der Client hat zu viele Aufrufe innerhalb einer festgelegten Zeitspanne getätigt	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/$create POST /Task/<id>/$activate POST /Task/<id>/$accept POST /Task/<id>/$reject POST /Task/<id>/$close POST /Task/<id>/$abort POST /Communication	Der Client (PVS, AVS, FdV) hat innerhalb des konfigurierten Zeitabschnitts zu viele Requests geschickt
500	Interner Serverfehler	GET /Task GET /Task/<id> GET /AuditEvent/ GET /Communication GET /MedicationDispense POST /Task/$create POST /Task/<id>/$activate POST /Task/<id>/$accept POST /Task/<id>/$reject POST /Task/<id>/$close POST /Task/<id>/$abort POST /Communication	In allen Operationen, die aufgrund eines internen Fehlers nicht bearbeitet werden können. Die Rückgabe liefert keine weiteren Informationen.

[<=]

5.4 Protokollierung

Der E-Rezept-Fachdienst soll Protokolldateien schreiben, die eine Analyse technischer Vorgänge erlauben. Diese Protokolldateien sind dafür vorgesehen, aufgetretene Fehler zu identifizieren und die Performance zu analysieren. Für diese Zwecke führt der E-Rezept-Fachdienst ein Systemprotokoll, mit dem der Anbieter des Dienstes jederzeit den Betriebszustand des Systems kontrollieren kann.

A_19282 - E-Rezept-Fachdienst - Systemprotokoll für Betriebszustand
Der E-Rezept-Fachdienst MUSS ein Systemprotokoll über durchgeführte Operationen und deren Erfolg/Misserfolg führen, um dem Anbieter des Dienstes jederzeit eine Übersicht über den aktuellen Betriebszustand zu ermöglichen.**[<=]**

A_19283 - E-Rezept-Fachdienst - Systemprotokoll ohne personenbezogene und ohne medizinische Daten

Der E-Rezept-Fachdienst MUSS in jedem zu tätigenden Systemprotokolleintrag alle personenbezogenen, personenbeziehbaren und medizinischen Informationen vor der Speicherung entfernen, damit vom administrativen Personal keine personenbezogenen Daten der Versicherten oder Leistungserbringer eingesehen werden können. **[<=]**

A_19678 - E-Rezept-Fachdienst -Systemprotokoll Verfügbarkeit interner Logdaten
Der Betreiber des E-Rezept-Fachdienstes MUSS im Rahmen von Testmaßnahmen dem Testbetriebsverantwortlichen auf Anforderung die Log-Dateien des Systemprotokolls übermitteln.**[<=]**

A_20001 - E-Rezept-Fachdienst -Systemprotokoll zu Ergebnis einer aufgerufenen Operation
Der E-Rezept-Fachdienst MUSS ein Systemprotokoll über durchgeführte Operationen und deren Erfolg/Misserfolg führen. **[<=]**

Der E-Rezept-Fachdienst führt außerdem Zugriffsprotokolle für Versicherte, in denen alle Zugriffe auf die personenbezogenen und medizinischen Daten eines Versicherten für den Versicherten einsehbar sind. Diese Zugriffsprotokolle sind unabhängig vom Systemprotokoll und stehen ausschließlich dem Versicherten zur Wahrnehmung seiner Betroffenenrechte zur Einsicht zur Verfügung.

A_19284 - E-Rezept-Fachdienst - Versichertenprotokoll zu Operationen
Der E-Rezept-Fachdienst MUSS jeden Aufruf der folgenden Operationen protokollieren:

Tabelle 4 TAB_eRPFD_004 Versichertenprotokoll

Operation	**Rolle des zugreifenden Nutzers**	**Beschreibung (ggfs. als Vorschlag für einen lesbaren Protokolleintrag in einfacher Sprache)**
http GET /Task bzw. http GET /Task/<id>		
-	Versicherter, Vertreter	Patient/Versicherter/Vertreter hat das E-Rezept heruntergeladen
	Apotheker	Apotheke hat die E-Rezept-Quittung heruntergeladen
http POST /Task		
$activate	Arzt-/Zahnarztpraxis/Krankenhaus	Arzt-/Zahnarztpraxis/Krankenhaus hat das E-Rezept bereitgestellt
$accept	Apotheke	Apotheke hat das E-Rezept heruntergeladen
$reject	Apotheke	Apotheke hat das E-Rezept zurückgegeben
$close	Apotheke	Apotheke hat das E-Rezept beliefert

$abort	Versicherter, Vertreter	Patient/Versicherter/Vertreter hat das E-Rezept gelöscht
	Arzt-/Zahnarztpraxis/Krankenhaus	Arzt-/Zahnarztpraxis/Krankenhaus hat das E-Rezept gelöscht
	Apotheke	Apotheke hat das E-Rezept gelöscht
http GET /MedicationDispense		
	Versicherter, Vertreter	Patient/Versicherter hat Medikament-Informationen heruntergeladen
Automatisches Löschen durch den Fachdienst		
Ressource Task	E-Rezept-Fachdienst	Veraltete E-Rezepte vom Fachdienst automatisch gelöscht
Ressource MedicationDispense		Veraltete Medikament-Informationen vom Fachdienst automatisch gelöscht
Ressource AuditEvent		Veraltete Protokolleinträge vom Fachdienst automatisch gelöscht
Ressource Communication		Veraltete Nachrichten vom Fachdienst automatisch gelöscht

und die gelesene bzw. geschriebene Ressource im Protokolleintrag `AuditEvent.entity.what` als Referenz hinzufügen, sowie die KVNR des betroffenen Versicherten in `AuditEvent.entity.name` speichern.

Mit diesen Informationen kann der Versicherte die Zugriffe auf seine Daten nachvollziehen und bei einem unberechtigten Zugriff ggfs. intervenieren.**[<=]**

A_19302 - E-Rezept-Fachdienst -Protokolleintrag Versichertenprotokoll leicht verständlich
Der E-Rezept-Fachdienst MUSS in jedem zu tätigenden Eintrag des Protokolls für Versicherte einen lesbaren Text in einfacher Sprache (deutsch und englisch) erzeugen, der mindestens den Namen des Zugreifenden, die auslösende Operation und das Ergebnis der Operation umfasst, damit Versicherte ohne technisches Vorwissen den Inhalt des Zugriffsprotokolls verstehen können.**[<=]**

5.5 Löschfristen

Der E-Rezept-Fachdienst soll eine Datensparsamkeit realisieren. Dafür werden nicht mehr benötigte Ressourcen, abgelaufene E-Rezepte und veraltete Kommunikationsnachrichten automatisch nach einer festen Frist gelöscht.

A_19252 - E-Rezept-Fachdienst - Löschfrist abgelaufener Rezepte
Der E-Rezept-Fachdienst MUSS einen Task nach Ablauf der Löschfrist gemäß der folgenden Festlegung in TAB_eRPFD_007

Tabelle 5 TAB_eRPFD_007 Löschfristen

Task.status nach Statuswechsel	Löschfrist
draft	1 Tage nach Statuswechsel
ready	10 Tage nach Datum in `Task.expiryDate`
in-progress	100 Tage nach Statuswechsel
completed	100 Tage nach Statuswechsel
cancelled	10 Tage nach Statuswechsel

automatisch löschen und das Löschen in einem AuditEvent für den Versicherten nachvollziehbar protokollieren, damit nicht mehr benötigte Informationen gelöscht sind. **[<=]**

A_19254 - E-Rezept-Fachdienst - Löschen referenzierter Bundles
Der E-Rezept-Fachdienst MUSS bei jedem Löschen eines Tasks alle referenzierten Bundles (QES-Datensatz, Quittungs-Bundle) ebenfalls löschen, damit die Informationen rund um ein gelöschtes E-Rezept ebenfalls entfernt werden. **[<=]**

A_19255 - E-Rezept-Fachdienst Löschen veralteter MedicationDispense
Der E-Rezept-Fachdienst MUSS eine gespeicherte Ressource MedicationDispense nach 100 Tagen ab ihrem Erzeugungsdatum `MedicationDispense.whenHandedOver` automatisch löschen, damit Informationen zu veralteten und gelöschten Rezepten ebenfalls entfernt werden.**[<=]**

A_19253 - E-Rezept-Fachdienst - Löschfrist veraltete Nachrichten
Der E-Rezept-Fachdienst MUSS eine gespeicherte Ressource Communication ohne eine Referenz auf einen Task in `Communication.basedOn` nach 100 Tagen ab ihrem Sendedatum `Communication.sent` und solche mit einer Referenz auf einen Task gemäß der Löschfrist in TAB_eRPFD_007 beim Löschen des Tasks automatisch löschen, damit nicht mehr relevante Nachrichten zu gelöschten Rezepten ebenfalls gelöscht werden. **[<=]**

A_19256 - E-Rezept-Fachdienst - Löschfrist veraltete Protokolleinträge
Der E-Rezept-Fachdienst MUSS eine gespeicherte Ressource AuditEvent nach 3 Jahren ab dem Erzeugungsdatum `AuditEvent.recorded` löschen, damit veraltete Einträge nach Ende der regulären Aufbewahrungsfrist entfernt werden.**[<=]**

5.6 Sicherheit

5.6.1 Allgemeine Sicherheitsanforderungen

A_19260 - E-Rezept-Fachdienst – Ausschluss bestimmter FdV-Versionsnummern von der Kommunikation
Der E-Rezept-Fachdienst MUSS die von dem E-Rezept-FdV mitgeteilte Versionsnummer erkennen und festgelegte Versionsnummern von einer Kommunikation mit dem E-Rezept-Fachdienst ausschließen können. Der E-Rezept-Fachdienst MUSS in diesen Fällen eine entsprechende Fehlermeldung an das FdV geben.**[**<=**]**

Hinweis: Der Ausschluss kann z.B. über ein Whitelisting oder ein Blacklisting erfolgen.

A_19261 - E-Rezept-Fachdienst – Ausschluss von FdV-Versionen
Der Anbieter des E-Rezept-Fachdienstes MUSS ausschließlich auf Anweisung der gematik E-Rezept-FdVs mit bestimmten Versionsnummern von einer Kommunikation mit dem E-Rezept-Fachdienst ausschließen.**[**<=**]**

A_19266 - E-Rezept-Fachdienst - Berücksichtigung OWASP-Top-10-Risiken
Der E-Rezept-Fachdienst MUSS Maßnahmen zum Schutz vor den OWASP-Top-10-Risiken in der aktuellen Version umsetzen.**[**<=**]**

A_19111 - E-Rezept-Fachdienst - Versionierung von Ressourcen
Der E-Rezept-Fachdienst MUSS eine Versionierung der FHIR-Ressource Task gemäß des Versionierungskonzepts [FHIR-ResVers] des FHIR-Standards umsetzen und in seinem CapabilityStatement ausweisen, damit für den Versicherten Zustandsänderungen nachvollziehbar und in der Versionshistorie des Tasks einsehbar sind.**[**<=**]**

5.6.2 Identifikation des Clientsystems

Der E-Rezept-Fachdienst verwaltet und steuert den Einlöseprozess für elektronische Verordnungen. Damit kommt ihm eine Relevanz in der Medikamentenversorgung zu, die sich zum einen in einer hohen Verfügbarkeit und zum anderen in einem hohen Angriffspotential widerspiegelt. Zur Unterstützung der betrieblichen Überwachung des E-Rezept-Fachdienstes wird die Nutzung der im Feld befindlichen Clientsysteme protokolliert. Dabei ist der Zugriff auf die Schnittstellen des E-Rezept-Fachdienstes nur durch Primärsysteme der Leistungserbringer und zugelassene E-Rezept-FdVs zulässig. Der E-Rezept-Fachdienst erkennt die Clientsysteme anhand des User-Agent-Header eingehender HTTP-Requests und protokolliert diesen Wert.

A_20013 - E-Rezept-Fachdienst - Erkennung Clientsystem User-Agent
Der E-Rezept-Fachdienst MUSS das vom aufrufenden Nutzer verwendete Clientsystem anhand des im HTTP-Request enthaltenen Header-Feld "`User-Agent`" gemäß [RFC7231] erkennen und in den Einträgen zur Performance-Rohdatenerfassung gemäß [gemSpec_Perf] protokollieren. Der E-Rezept-Fachdienst MUSS bei fehlendem`User-Agent`-Header den Request mit dem HTTP-Status-Code 400 beantworten, damit in der Betriebsüberwachung des E-Rezept-Fachdienstes die Nutzung unzulässiger Frontends erkannt werden kann. **[**<=**]**

5.6.3 TSL und OCSP-Status

Der E-Rezept-Fachdienst muss das E-Rezept-Frontend des Versicherten (E-Rezept-FdV) bei den Aufgaben unterstützen, regelmäßig die TSL-Aktualisierung vorzunehmen [gemSpec_eRp_FdV#A_20028] und Sperrinformationen für Zertifikate zu ermitteln [gemSpec_eRp_FdV#A_20032]. Die OCSP-Responder und der TSL-Dienst haben deutlich höhere SLAs in Bezug auf die Verfügbarkeit innerhalb der TI. Manche OCSP-Responder besitzen keine direkte Anbindung an das Internet (Komponenten-PKI, Kontext: Prüfung Identität vertrauenswürdige Ausführungsumgebung). Es wird damit auch möglich, bessere Aussagen über die Verfügbarkeit von E-Rezept-Anwendungsfällen zu treffen, weil weniger nicht-SLA-belegte Datenverbindungen für die Anwendungsfälle notwendig sind. (Wenn eine funktionierende Datenverbindung zwischen E-Rezept-FdV und E-Rezept-Fachdienst besteht, dann kann eine in [gemSpec_Perf] definierte Verfügbarkeit garantiert werden.) Aufgrund der Verwendung der Schnittstellen-Funktionalität über die schon etablierte TLS-Verbindung sind OCSP-Requests des E-Rezept-FdV nicht im Klartext im Internet sichtbar.

A_20023 - E-Rezept-Fachdienst - Bereitstellung TSL
Der E-Rezept-Fachdienst MUSS folgende Vorgaben umsetzen:

1. Er MUSS mindestens einmal täglich aus der TI (TI-interne Verbindung) die "TSL(ECC-RSA)" und deren zugehörigen Hashwert aus der TI herunterladen.
2. Er MUSS unter dem Pfadnamen "/TSL.xml" über das vom E-Rezept-FdV genutzte HTTPS-Interface die "TSL(ECC-RSA)" der TI zur Verfügung stellen (HTTP-GET, HTTP Content-Type: text/xml).
3. Er MUSS unter dem Pfadnamen "/TSL.sha2" über das vom E-Rezept-FdV genutzte HTTPS-Interface den vom TSL-Dienst heruntergeladenen SHA-256 Hashwert der Datei TSL.xml aus Spiegelstrich 2 zur Verfügung stellen (HTTP Content-Type: text/plain, Hashwert als hexdump kodiert (64 Byte + Newline))

[<=]

Hinweise:

1. "TI-interne Verbindung" hat den Hintergrund, dass dort über SLAs eine ausreichende Verfügbarkeit gewährleistet ist.
2. Hashwert der TSL.xml bedeutet der Hashwert der Datei TSL.xml, so wie sie vom TSL-Dienst der TI bereitgestellt wird und als wenn man die Datei als Binärdatei interpretiert (vgl. [gemSpec_TSL]).

A_20024 - E-Rezept-Fachdienst - Bereitstellung OCSP-Forwarder
Der E-Rezept-Fachdienst MUSS folgende Vorgaben umsetzen:

1. Er MUSS unter dem in A_19411 in Tabelle: TAB_eRPFD_002 FQDN angegeben Pfadnamen für den key "ocspf" eine Möglichkeit zur Statusabfrage über das vom E-Rezept-FdV genutzte HTTPS-Interface zur Verfügung stellen (HTTP-POST, vgl. auch [RFC-6960, Appendix [gemSpec_PKI]).
2. Er MUSS über die Schnittstelle aus Spiegelstrich 1 OCSP-Requests [RFC-6960] entgegen nehmen.
3. Aus einem solchen OCSP-Request MUSS er aus dem issuerKeyHash [RFC-6960] die URL des entsprechenden OCSP-Responders in der TI ermitteln (Datengrundlage ist die TSL der TI) und den OCSP-Request an diese ermittelte URL weiterleiten.
4. Er MUSS die erhaltenen OCSP-Response an das die OCSP-Anfrage stellende E-Rezept-FdV unverändert weiterreichen.

[<=]

Auf Anfrage stellt die gematik eine Beispielimplementierung für A_20024 Spiegelstrich 3 bereit.

A_20025 - E-Rezept-Fachdienst - Caching OCSP-Antworten
Der E-Rezept-Fachdienst KANN OCSP-Antworten aus A_20024 bis zu 4 Stunden cachen und bei einer entsprechend passenden OCSP-Anfrage, anstatt neu den OCSP-Responder anzufragen, die im Cache befindliche OCSP-Antwort ausliefern.**[<=]**

A_20026 - E-Rezept-Fachdienst - OCSP-Stapling
Der E-Rezept-Fachdienst MUSS an der HTTPS-Schnittstelle zum Internet OCSP-Stapling [RFC-6066] unterstützen.**[<=]**

5.6.4 Sicherheit der Netzübergänge

Der E-Rezept-Fachdienst wird für Versicherte über das Internet erreichbar gemacht und für Leistungserbringer über das Netz der TI. Die folgenden Anforderungen beschreiben die für diese Netzübergänge erforderlichen Sicherheitsmechanismen. Für den Netzübergang aus dem Internet als Transportnetz zum E-Rezept-Fachdienst ist ein Paketfilter erforderlich.

A_19813 - E-Rezept-Fachdienst – Sicherung zum Transportnetz Internet durch Paketfilter
Der E-Rezept-Fachdienst MUSS zum Transportnetz Internet durch einen Paketfilter (ACL) gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der Paketfilter des E-Rezept-Fachdienstes MUSS frei konfigurierbar sein auf der Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.**[<=]**

A_19814 - E-Rezept-Fachdienst – Platzierung des Paketfilters Internet
Der Paketfilter des E-Rezept-Fachdienstes, zum Schutz in Richtung Transportnetz Internet, DARF NICHT physisch auf Systemen der VAU des E-Rezept-Fachdienstes oder dem vorgeschalteten TLS-terminierenden Load Balancer implementiert werden.**[<=]**

A_19815 - E-Rezept-Fachdienst – Richtlinien für den Paketfilter zum Internet
Der Paketfilter des E-Rezept-Fachdienstes MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

1. HTTPS, und
2. OCSP-Zugriffe für das OCSP-Stapling nach A_20026 (vgl. Hinweis nach A_19815), ggf. notwendige DNS Anfragen (und Antworten)

Ein Verbindungsaufbau aus dem E-Rezept-Fachdienst in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 . **[<=]**

Hinweis zu A_19815:

Der Anbieter des E-Rezept-Fachdienstes muss für seine HTTPS-Schnittstelle ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-Zertifikat also über einen aktuellen Webbrowser prüfbar ist, vgl. A_19823). Für dieses TLS-Zertifikat fragt der E-Rezept-Fachdienst regelmäßig für das OCSP-Stapling nach A_20026 den OCSP-Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält der E-Rezept-Fachdienst eine OCSP-Response. Diese wird nach A_20022 geprüft und anschließend von der HTTPS-Schnittstelle verwendet (vgl. https://tools.ietf.org/html/rfc6066#section-8 und bspw. http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling).

Um dies zu ermöglichen muss der Paketfilter entsprechende stateful-Firewall-Regeln gemäß A_19815 und A_20022 definieren.

A_20022 - E-Rezept-Fachdienst - OCSP-Status für das OCSP-Stapling
Der Paketfilter des E-Rezept-Fachdienstes MUSS bezüglich des OCSP-Stapling gemäß A_20026 folgende Vorgaben umsetzen:

1. Für das vom Anbieter des E-Rezept-Fachdienstes erworbene TLS-Zertifikat (vgl. Hinweis zu A_19815) MUSS der E-Rezept-Fachdienst initial die IP-Adresse (ggf. die IP-Adressen) des entsprechenden OCSP-Responsers ermitteln.
2. Diese IP-Adresse(n) MÜSSEN gemäß A_19815 per stateful-Firewalling Verbindungen von der HTTPS-Schnittstelle an den OCSP-Responder erlaubt werden (Whitelisting).
3. Gemäß OCSP-Stapling (https://tools.ietf.org/html/rfc6066#section-8) MUSS der E-Rezept-Fachdienst regelmäßig eine OCSP-Response vom entsprechenden OCSP-Responder beziehen (Die Regelmäßigkeit wird vom zertifikatsausgebenden TSP und der Gültigkeitsdauer dessen OCSP-Responses bestimmt).
4. Die OCSP-Responses MÜSSEN vom E-Rezept-Fachdienst geprüft werden (Signaturprüfung, CertID in der OCSP-Response passt zum angefragten Zertifikat). Falls eine der Prüfungen ein nicht-positives Ergebnis liefert so MUSS die erhaltene OCSP-Response verworfen werden.
5. Sollte die letzte im E-Rezept-Fachdienst vorhandene OCSP-Response zeitlich nicht mehr gültig sein (bspw. der OCSP-Responder im Internet war länger nicht erreichbar), so MUSS diese OCSP-Response verworfen werden und ein von einem Klienten (E-Rezept-FdV) initiierter TLS-Verbindungsaufbau der HTTPS-Schnittstelle ohne OCSP-Stapling durchgeführt werden.

[<=]

A_19824 - E-Rezept-Fachdienst – Verhalten bei Vollauslastung
Der Paketfilter des E-Rezept-Fachdienstes MUSS so konfiguriert sein, dass bei Vollauslastung der Systemressourcen im E-Rezept-Fachdienst keine weiteren Verbindungen angenommen werden.**[<=]**

Durch die Zurückweisung von Verbindungen wird sichergestellt, dass Clients einen Verbindungsaufbau mit einer anderen Instanz des Fachdienstes versuchen, bei dem die erforderlichen Ressourcen zur Verfügung stehen.

Da der E-Rezept-Fachdienst die Verarbeitung der fachlichen Operationen in einer VAU ausführt, ist der Zugang zum Schutz dieser VAU zweistufig. Der E-Rezept-Fachdienst verfügt über einen Eingangspunkt (einen Load Balancer), an dem die TLS-Verbindung terminiert wird. Der Eingangspunkt wertet dann den HTTP-Header aus, um aus der Ziel-URL des Requests den für die Verarbeitung zu adressierenden Verarbeitungskontext zu ermitteln. An diesen Verarbeitungskontext wird der Request durch den Eingangspunkt weitergeleitet. In umgekehrter Richtung sendet der Eingangspunkt die Response des Verarbeitungskontextes über die TLS-Verbindung an den Client.

A_19720 - E-Rezept-Fachdienst – Verbindungen von Clients zu Verarbeitungskontexten der VAU über den Eingangspunkt
Der Eingangspunkt des E-Rezept-Fachdienstes MUSS Verbindungen von Clients (Internet oder TI) ausschließlich über TLS akzeptieren. Er MUSS die TLS-Verbindung terminieren und HTTP Requests und Responses zwischen dem Client und dem für die jeweilige Sitzung zugeordneten Verarbeitungskontext der VAU vermitteln.**[<=]**

A_19823 - E-Rezept-Fachdienst – Richtlinien zum TLS-Verbindungsaufbau

Der Eingangspunkt des E-Rezept-Fachdienstes MUSS sich beim TLS-Verbindungsaufbau über das Transportnetz gegenüber dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren. Das Zertifikat MUSS an die jeweilige Schnittstelle des Eingangspunkts für Primärsysteme und Frontends der Versicherten des E-Rezept-Fachdienstes gebunden werden, damit Clientsysteme beim TLS-Verbindungsaufbau eine vereinfachte Zertifikatsprüfung mit TLS-Standardbibliotheken durchführen können. **[<=]**

5.6.5 Vertrauenswürdige Ausführungsumgebung

In diesem Abschnitt werden die Anforderungen an den E-Rezept-Fachdienst zur Umsetzung einer Vertrauenswürdigen Ausführungsumgebung (VAU) dargestellt. Die VAU dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten Klartextdaten innerhalb des E-Rezept-Fachdienstes sowie dem technischen Ausschluss der Profilbildung durch den Anbieter bzw. Betreiber. Die VAU stellt dazu Verarbeitungskontexte (d. h. Instanzen der VAU) bereit, in denen die Verarbeitung sensibler Daten im Klartext erfolgen kann. Diese Verarbeitungskontexte sind entsprechend zu schützen.

A_19683 - E-Rezept-Fachdienst – Umsetzung der fachlichen Operationen in einer Vertrauenswürdigen Ausführungsumgebung (VAU)
Der E-Rezept-Fachdienst MUSS die Verarbeitung aller fachlichen Operationen des Fachdienstes in einer Vertrauenswürdigen Ausführungsumgebung umsetzen.**[<=]**

5.6.5.1 Verarbeitungskontext

Die Gesamtheit aus der für eine Klartextverarbeitung erforderlichen Software, dem für eine Klartextverarbeitung genutzten physikalischen System sowie den für die Integrität einer Klartextverarbeitung erforderlichen organisatorischen und physischen Rahmenbedingungen bildet den Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung.

Zur Vertrauenswürdigen Ausführungsumgebung gehören neben den Verarbeitungskontexten alle für ihre Erreichbarkeit und betriebliche Steuerung erforderlichen Komponenten.

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

A_19684 - E-Rezept-Fachdienst – Verarbeitungskontext der VAU
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sämtliche physikalischen Systemkomponenten sowie sämtliche Softwarekomponenten umfassen, deren Sicherheitseigenschaften sich auf den Schutz der personenbezogenen medizinischen Daten vor Zugriff durch Unbefugte bei ihrer Verarbeitung im Klartext auswirken können. **[<=]**

A_19688 - E-Rezept-Fachdienst – Verschlüsselung von außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass sämtliche schützenswerten Daten vor einer Speicherung außerhalb der VAU verschlüsselt werden. Der Verarbeitungskontext MUSS dazu Schlüssel für nur jeweils ein individuelles E-Rezept

(inkl. aller mit diesem E-Rezept verbundenen Daten) verwenden oder mindestens einmal pro Sekunde den verwendeten Schlüssel wechseln, so dass nur die innerhalb einer Sekunde neu angelegten E-Rezepte mit einem Schlüssel verschlüsselt werden.**[<=]**

A_19699 - E-Rezept-Fachdienst – Ableitung der Persistenzschlüssel durch ein HSM
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS die zur Verschlüsselung der persistierten E-Rezept-Daten verwendeten Schlüssel von einem HSM innerhalb der VAU abrufen.**[<=]**

A_19700 - E-Rezept-Fachdienst - Ableitung der Persistenzschlüssel aus Merkmal der E-Rezepte
Das HSM der VAU des E-Rezept-Fachdienstes MUSS eine Schnittstelle zur Ableitung von symmetrischen Schlüsseln für die Persistierung von E-Rezept-Daten bereitstellen. Das HSM der VAU des E-Rezept-Fachdienstes MUSS zur Ableitung des jeweiligen Schlüssels ein nach der ersten Erstellung unveränderliches Merkmal des E-Rezept-Datensatzes als Ableitungsparameter verwenden (z. B. den Zeitstempel der Registrierung von Rezept-ID und Access Code oder den Access Code selbst).**[<=]**

A_19694 - E-Rezept-Fachdienst – Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass sämtliche schützenswerten Daten ausschließlich über sichere Verbindungen an autorisierte Nutzer weitergegeben werden.**[<=]**

A_19262 - E-Rezept-Fachdienst - Transportverschlüsselte Übertragung von Daten mit PVS
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass er nur transportverschlüsselt mit dem PVS kommuniziert. **[<=]**

A_19263 - E-Rezept-Fachdienst - Transportverschlüsselte Übertragung von Daten mit AVS
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass er nur transportverschlüsselt mit dem AVS kommuniziert. **[<=]**

A_19264 - E-Rezept-Fachdienst - Transportverschlüsselte Übertragung von Daten mit FdV
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass er nur transportverschlüsselt mit dem FdV kommuniziert. **[<=]**

A_19265 - E-Rezept-Fachdienst – vertrauliche Kommunikation
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sicherstellen, dass er nur transportverschlüsselt mit Komponenten außerhalb des Verarbeitungskontextes kommuniziert. **[<=]**

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

A_19267 - E-Rezept-Fachdienst - Authentisierung gegenüber Clients
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sich gegenüber Clients, die mit ihm kommunizieren, mittels der Fachdienstidentität oid_erp_vau mit Zertifikatsprofil C.FD.AUT (oid_fd_aut) ausweisen. **[<=]**

A_19702 - E-Rezept-Fachdienst – Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU
Die VAU des E-Rezept-Fachdienstes MUSS die in ihr ablaufenden Verarbeitungen für die Daten eines Verarbeitungskontextes von den Verarbeitungen für die Daten anderer Verarbeitungskontexte in solcher Weise trennen, dass mit technischen Mitteln

ausgeschlossen wird, dass die Verarbeitungen eines Verarbeitungskontextes schadhaft auf die Verarbeitungen eines anderen Verarbeitungskontextes einwirken können.**[**<=**]**

Hinweis: Da der Verarbeitungskontext der VAU des E-Rezept-Fachdienstes für jede fachliche Operation neu aufgebaut werden muss, ist ein Low-Level-Mechanismus zur Kontextseparation aus Gründen der Performance bzw. Skalierung nicht zwingend vorgeschrieben. Der hier geforderte Separationsmechanismus kann daher auch als Server-Thread, Worker, o. Ä. ausgeführt sein, solange für den dadurch gebildeten Verarbeitungskontext die geforderte Separation nachgewiesen werden kann. Dies setzt voraus, dass die Umsetzung der Verarbeitungskontexte und der in ihnen ablaufenden Verarbeitungsvorgänge technisch möglichst einfach und nachvollziehbar gestaltet ist.

A_19726 - E-Rezept-Fachdienst – Unabhängige Skalierung der Dienst-Ressourcen für verschiedene Anwendergruppen
Die VAU des E-Rezept-Fachdienstes MUSS für die Anwendergruppen Leistungserbringer (E-Rezepte ausstellen, E-Rezepte einlösen) und Versicherte (E-Rezepte einsehen, zuweisen und löschen) auf jeweils getrennten physischen Servern betrieben werden, so dass eine Überlastung aufgrund außergewöhnlich hoher Aktivität einer Anwendergruppe (primär der Versicherten) keine Beeinträchtigung der Arbeitsfähigkeit der anderen Anwendergruppen (primär der Ärzte und Apotheker) zur Folge hat.**[**<=**]**

5.6.5.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld

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

A_19704 - E-Rezept-Fachdienst – Isolation der VAU von Datenverarbeitungsprozessen des Anbieters
Die VAU des E-Rezept-Fachdienstes MUSS die in ihren Verarbeitungskontexten ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters trennen und damit gewährleisten, dass der Anbieter des E-Rezept-Fachdienstes vom Zugriff auf die in der VAU verarbeiteten schützenswerten Daten ausgeschlossen ist. **[**<=**]**

Hinweis: Für die Separation zwischen Verarbeitungskontexten und Verarbeitungsprozessen des Anbieters, die der betrieblichen Steuerung des Systems dienen, ist eine Low-Level Separation anzustreben, da - im Unterschied zur Separation zwischen Verarbeitungskontexten - hier technisch sehr verschiedene Aspekte getrennt werden müssen.

A_19706 - vE-Rezept-Fachdienst – Ausschluss von Manipulationen an der Software der VAU
Die VAU des E-Rezept-Fachdienstes MUSS eine Manipulation der eingesetzten Software erkennen und eine Ausführung der manipulierten Software verhindern.**[**<=**]**

A_19707 - E-Rezept-Fachdienst – Ausschluss von Manipulationen an der Hardware der VAU
Die VAU des E-Rezept-Fachdienstes MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter des E-Rezept-Fachdienstes ausschließen.**[**<=**]**

A_19708 - E-Rezept-Fachdienst – Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU
Die VAU des E-Rezept-Fachdienstes MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter des E-Rezept-Fachdienstes mit Mitteln

umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann.**[<=]**

A_19709 - E-Rezept-Fachdienst – Kein physischer Zugang des Anbieters zu Systemen der VAU
Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter des E-Rezept-Fachdienstes, während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.**[<=]**

A_19710 - E-Rezept-Fachdienst – Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU
Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln sicherstellen, dass physischer Zugang zu Hardware-Komponenten der Verarbeitungskontexte nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten extrahiert werden können.**[<=]**

A_19711 - E-Rezept-Fachdienst – Private Schlüssel von Dienstzertifikaten im HSM
Der E-Rezept-Fachdienst MUSS die folgenden privaten Schlüssel in einem Hardware Security Module (HSM) erzeugen und anwenden:

- TI-Fachdienst-Identität zur Authentisierung des Dienstes gegenüber dem Primärsystem des Leistungserbringers (TLS)
- TI-Fachdienst-Identität zur Authentisierung des Verarbeitungskontextes gegenüber dem Primärsystem des Leistungserbringers (sicherer Kanal auf Anwendungsebene),
- Privater Schlüssel des Schlüsselpaars zur Authentisierung des Verarbeitungskontextes gegenüber dem E-Rezept-Frontend des Versicherten (sicherer Kanal auf Anwendungsebene).

Die Prüftiefe des HSM MUSS dabei den in [A_19712] angegebenen Standards entsprechen.**[<=]**

Hinweis: Die TLS-TI-Fachdienst-Identität kann z. B. auf einem außerhalb der VAU betriebenen Load Balancer mit TLS-Terminierung verwendet werden. Hierfür muss dann ein HSM außerhalb der VAU verwendet werden.

A_19712 - E-Rezept-Fachdienst – Einsatz zertifizierter HSM
Der Anbieter des E-Rezept-Fachdienstes MUSS beim Einsatz eines HSM sicherstellen, dass dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria, ITSEC oder Federal Information Processing Standard (FIPS) in Frage.
Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3,
2. Common Criteria EAL 4+ mit hohem Angriffspotenzial oder
3. ITSEC E3 der Stärke „hoch" entsprechen.

[<=]

A_19713 - E-Rezept-Fachdienst – HSM-Kryptographieschnittstelle verfügbar nur für Instanzen der VAU
Die VAU des E-Rezept-Fachdienstes MUSS mit technischen Mitteln, die auch Manipulationen durch den Anbieter des E-Rezept-Fachdienstes ausschließen, gewährleisten, dass nur Instanzen der VAU Zugriff auf die Kryptographieschnittstelle des

HSM zur Nutzung des privaten Schlüsselmaterials für ihre Dienstzertifikate erhalten können.**[<=]**

Hinweis: Falls die Verarbeitungskontexte als Threads, Workers, o. Ä. umgesetzt sind und daher gemeinsam in einem übergreifenden Anwendungsprozess ausgeführt werden, kann dieser Anwendungsprozess eine authentisierte Verbindung zur Kryptograhieschnittstelle des HSM herstellen und aufrecht erhalten, um darüber die Kryptographieschnittstelle des HSM den Verarbeitungskontexten (und nur diesen) lokal zur Verfügung zu stellen.

A_19714 - E-Rezept-Fachdienst – Sicherer Kanal vom Client zum Verarbeitungskontext der VAU
Die VAU des E-Rezept-Fachdienstes MUSS den Aufbau eines vertraulichen und integritätsgeschützten Kommunikationskanals gemäß [gemSpec_Krypt#3.16] und [gemSpec_Krypt#7] zwischen einem Client und einem Verarbeitungskontext erzwingen, bevor der Verarbeitungskontext seine fachlichen Schnittstellen für den Client nutzbar macht.**[<=]**

5.6.5.3 Konsistenz des Systemzustands, Logging und Monitoring

A_19715 - E-Rezept-Fachdienst – Konsistenter Systemzustand des Verarbeitungskontextes der VAU
Die VAU des E-Rezept-Fachdienstes MUSS sicherstellen, dass ein konsistenter Zustand des Verarbeitungskontextes auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw. wiederhergestellt werden kann.**[<=]**

A_19716 - E-Rezept-Fachdienst – Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU
Die VAU des E-Rezept-Fachdienstes MUSS die für den Betrieb eines Fachdienstes erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dem Anbieter des E-Rezept-Fachdienstes oder Dritten vertrauliche oder zur Profilbildung geeignete Daten zur Kenntnis gelangen. **[<=]**

5.6.5.4 Client-Verbindungen zum Verarbeitungskontext

Um Verbindungen vom E-Rezept-Frontend des Versicherten nach [gemSpec_eRp_FdV] zum Verarbeitungskontext zu ermöglichen, ist ein der VAU vorgelagertes Routing ausgehend von einem netztechnischen Eingangspunkt (z. B. in Form eines TLS-terminierenden Load Balancers) erforderlich. Der Eingangspunkt ist im Netzwerk der TI für das Primärsystem unter mindestens einer IP-Adresse/Port-Kombination erreichbar, die im Namensdienst der TI registriert sein muss. Der Eingangspunkt vermittelt die Verbindungen zwischen dem Client und dem jeweils benötigten Verarbeitungskontext.

A_19719 - E-Rezept-Fachdienst – Verarbeitungskontexte der VAU über gemeinsame Host-Adressen erreichbar
Die VAU des E-Rezept-Fachdienstes MUSS ihre Verarbeitungskontexte über gemeinsame IP-Adressen und Ports des Eingangspunkts des Fachdienstes erreichbar machen.**[<=]**

A_19724 - E-Rezept-Fachdienst – Identität des Verarbeitungskontextes für Clients
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS sich gegenüber Clients mittels der Fachdienstidentität `oid_erp_vau` mit Zertifikatsprofil `C.FD.ENC` ausweisen.**[<=]**

A_19721 - E-Rezept-Fachdienst – Sicherer Kanal zum Verarbeitungskontext der VAU auf Inhaltsebene

Der Eingangspunkt des E-Rezept-Fachdienstes MUSS Clients den Aufbau eines sicheren Kanals auf Inhaltsebene, d. h. einen Verbindungsaufbau gemäß [gemSpec_Krypt#3.16] und [gemSpec_Krypt#7] , zum Verarbeitungskontext ermöglichen.**[<=]**

A_19722 - E-Rezept-Fachdienst – Automatisierter Abbau des sicheren Kanals
Der Verarbeitungskontext des E-Rezept-Fachdienstes MUSS den sicheren Kanal zu einem Client nach Abschluss einer fachlichen Operation (die aus mehreren Requests bestehen kann) abbauen, sodass anschließend keine Zugriffe dieses Clients auf den Verarbeitungskontext mehr möglich sind, ohne dass eine neue Verbindung aufgebaut wird.**[<=]**

6 Funktionsmerkmale

In diesem Abschnitt werden die vom E-Rezept-Fachdienst verwalteten Ressourcen mit ihren zulässigen Operationen und der Workflow des E-Rezepts spezifiziert. Dabei werden sowohl die relevanten HTTP-Operationen als auch die möglichen FHIR-Operationen auf Ressourcen-Endpunkte bzw. konkrete über eine <id> referenzierte Instanz vorgestellt. Die HTTP-Operationen dienen dabei der Zugriffssteuerung gemäß HTTP-Protokoll, um mit GET Daten von einem Server abzurufen und mittels POST Daten an einen Server zu schicken. Die FHIR-Operationen setzen in Kombination mit den HTTP-Operationen die Workflow-Steuerung um, wobei die entsprechenden FHIR-Operationen jeweils Zustandsänderungen triggern und bei den HTTP-Operationen POST vom Client Übergabeparameter erwarten und bei HTTP-GET ohne Übergabeparameter funktionieren.

A_19536 - E-Rezept-Fachdienst - RESTful API
Der E-Rezept-Fachdienst MUSS seine Schnittstellen für alle Zugriffe auf alle Datenobjekte und alle Ressourcen in einer RESTful API gemäß der FHIR-Spezifikation in http://hl7.org/fhir/http.html der Version v4.0.1 R4 umsetzen.**[<=]**

A_19537 - E-Rezept-Fachdienst - RESTful API MimeType fhir+xml
Der E-Rezept-Fachdienst MUSS in seinen Schnittstellen für die Zugriffe durch Leistungserbringer und Leistungserbringerinstitutionen standardmäßig den MimeType `application/fhir+xml` akzeptieren und in Responses verwenden.**[<=]**

A_19538 - E-Rezept-Fachdienst - RESTful API MimeType fhir+json
Der E-Rezept-Fachdienst MUSS in seinen Schnittstellen für die Zugriffe durch Versicherte standardmäßig den MimeType `application/fhir+json` akzeptieren und in Responses verwenden.**[<=]**

A_19539 - E-Rezept-Fachdienst - RESTful API MimeType Aufrufparameter
Der E-Rezept-Fachdienst MUSS in seinen Schnittstellen einen von der Standardfestlegung abweichenden MimeType umsetzen, wenn der jeweilige Client eine entsprechende Anforderung in der Aufrufschnittstelle über den URL-Parameter `_format=fhir+xml` bzw. `_format=fhir+json` gemäß http://hl7.org/fhir/http.html#general anfordert, damit Clientsysteme ein für sie leichter verarbeitbares Format in der Antwort erhalten können.**[<=]**

A_20171 - E-Rezept-Fachdienst - RESTful API CapabilityStatement
Der E-Rezept-Fachdienst MUSS an seinen Schnittstellen eine http-GET-Operation auf den Endpunkt /metadata erlauben, in welcher er ein CapabilityStatement gemäß https://www.hl7.org/fhir/capabilitystatement.html veröffentlicht, welches die vom E-Rezept-Fachdienst verarbeiteten Ressourcen mit den zugehörigen http-Operationen der angebotenen REST-Schnittstelle auflistet:

- Task – GET-, POST-Operation, FHIR-Operations für die Workflow-Steuerung und Einsicht durch den Versicherten
- MedicationDispense – GET-Operation für das Einsehen der Medikamentinformationen durch den Versicherten
- Communication – GET-, POST-Operation für das Senden und Empfangen von Nachrichten
- AuditEvent – GET-Operation für die Einsicht in Protokolleinträge durch den Versicherten
- Device – GET-Operation mit statischen Informationen zur serverseitigen Signatur

damit der Client eine Information über die FHIR-Kompatibilität zum Fachdienst erhält. **[<=]**

Offener Punkt:

Der E-Rezept-Fachdienst muss sich als Sender von Push-Notifications in der Firebase Cloud Messaging (FCM) Plattform und im Apple Push Notification Service (APNs) registrieren.

6.1 Ressource Task

Die FHIR-Resource Task [FHIR-TASK] bildet den Workflow für ein E-Rezept ab. Diese wird vom verordnenden Leistungserbringer mittels FHIR-Operationen `$create` und `$activate` im E-Rezept-Fachdienst erstellt. Der Versicherte kann die Ressource einsehen bzw. herunterladen und auf Wunsch mittels einer FHIR-Operation `$abort` löschen, die den Workflow abbricht. Die abgebende Apotheke greift ebenso wie der Verordnende ausschließlich über FHIR-Operationen `$accept` und `$close` zur Workflow-Steuerung auf einen Task zu.

A_19030 - E-Rezept-Fachdienst - unzulässige Operationen Task
Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource Task mittels der HTTP-Operationen PUT, PATCH, HEAD und DELETE sowie POST ohne die Angabe einer gültigen FHIR-Operation unterbinden, damit keine unzulässigen Operationen auf den Rezeptdaten ausgeführt werden können.**[<=]**

6.1.1 HTTP-Operation GET

Der Zugriff mittels der HTTP-Operation GET steht ausschließlich für die Einsichtnahme in E-Rezepte durch den Versicherten bzw. einen Vertreter mit Wissen um den AccessCode bzw. einen Apotheker mit Wissen um das Secret zur Verfügung. Die GET-Operation ohne Referenz einer FHIR-Operation führt zu keiner Statusänderung.

A_19113 - E-Rezept-Fachdienst - Rollenprüfung Versicherter oder Apotheker liest Rezept
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Task` und auf einen konkreten über <id> adressierten`/Task/<id>` (ohne die Referenz einer FHIR-Operation) sicherstellen, dass ausschließlich Versicherte oder Apotheken in einer der Rollen

- oid_versicherter
- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am Fachdienst aufrufen dürfen und die Rolle "`professionOID`" des Aufrufers im ID_TOKEN im HTTP-RequestHeader "`Authorization`" feststellen, damit E-Rezepte nicht durch Unberechtigte ausgelesen werden können. **[<=]**

A_19115 - E-Rezept-Fachdienst - Filter Tasks auf KVNR des Versicherten
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Task` die dem Versicherten zugeordneten Task-Ressourcen anhand der KVNR des Versicherten aus dem ID_TOKEN im "`Authorization`"-Header des HTTP-Requests identifizieren, die in`Task.for` mit dem Value-Set http://fhir.de/NamingSystem/gkv/kvid-10 die entsprechende KVNR des

begünstigten Patienten referenziert haben, damit ausschließlich Versicherte ihre eigenen E-Rezepte einsehen können.**[<=]**

A_19116 - E-Rezept-Fachdienst - Prüfung AccessCode bei KVNR-Missmatch
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf einen einzelnen `/Task/<id>` und Ungleichheit der KVNR des Aufrufenden (KVNR des ID_TOKEN im "`Authorization`"-Header des HTTP-Requests UNGLEICH KVNR in`Task.for` mit Value-Set http://fhir.de/NamingSystem/gkv/kvid-10) prüfen, ob der im HTTP-Request-Header "`X-AccessCode`" oder URL-Parameter "?ac=..." übergebene AccessCode gleich dem AccessCode in`Task.identifier` ist, damit auch Vertreter in Kenntnis des AccessCodes ein einzelnes E-Rezept einsehen können. **[<=]**

A_19129 - E-Rezept-Fachdienst - Rückgabe Task inkl. Bundle im Bundle Versicherter
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Task` oder auf einen einzelnen /Task/<id> die gültige Ergebnisliste der Task-Ressourcen um das jeweils referenzierte, serverseitig signierte E-Rezept-Bundle aus`Task.input` mit Codingsystem `https://gematik.de/fhir/CodeSystem/Documenttype = 2` und sofern vorhanden aus `Task.output` als `search.include` im Ergebnis-Bundle ergänzen und die Ergebnismenge Task[s] + E-Rezept-Bundle[s] an den Aufrufer zurückgeben, damit der Versicherte eine vollständige Einsicht in den Task und den signierten Verordnungsdatensatz und bei Vorhandensein die Quittung für eigene Dokumentationszwecke erhält. **[<=]**

A_19226 - E-Rezept-Fachdienst - Rückgabe Task inkl. Bundle im Bundle Apotheker
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf einen einzelnen Task mittels "`/Task/<id>?secret=...`" durch einen Apotheker den Task, sofern er den Status "`completed`" hat, um das referenzierte, serverseitig signierte Quittungs-Bundle aus`Task.output` mit Codingsystem `https://gematik.de/fhir/CodeSystem/Documenttype = 3` als `search.include` im Ergebnis-Bundle ergänzen und die Ergebnismenge Task + Quittungs-Bundle an den Apotheker zurückgeben, damit ein Apotheker, der ein konkretes E-Rezept beliefert hat, bei Bedarf genau dieses belieferte E-Rezept inkl. der Quittung erneut abrufen kann.**[<=]**

A_19569 - E-Rezept-Fachdienst - Suchparameter Task
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Task` eine Suche nach einem Task mit einer konkreten Task.id und `_revinclude` der Ressource `AuditEvent:entity:what` gemäß https://www.hl7.org/fhir/search.html#revinclude und https://www.hl7.org/fhir/task.html#search zulassen, sodass der Versicherte zu einem Task alle zugehörigen Protokolleinträge abrufen kann. **[<=]**

6.1.2 HTTP-Operation POST

Der Zugriff auf einen Task mittels der HTTP-Operation POST erfolgt immer in Verbindung mit dem Aufruf einer FHIR-Operation, die den Workflow des Tasks steuert. Je nach Anwendungsfall erfolgt der POST-Aufruf auf den Ressourcen-Endpunkt /Task oder eine konkrete über die ID referenzierte Task-Ressource /Task/<id>.

6.1.2.1 POST /Task/$create

Die FHIR-Operation $create erzeugt einen neuen FHIR-Task für ein E-Rezept. Diese Operation steht ausschließlich verordnenden Leistungserbringern zur Verfügung.

A_19018 - E-Rezept-Fachdienst - Rollenprüfung Verordnender stellt Rezept ein
Der E-Rezept-Fachdienst MUSS beim Erzeugen eines Tasks mittels HTTP-POST/$create-Operation die Rolle "`professionOID`" des Aufrufenden im ID_TOKEN im HTTP-RequestHeader "`Authorization`" feststellen und sicherstellen, dass ausschließlich verordnende Leistungserbringer in der Rolle

- oid_arzt
- oid_zahnarzt
- oid_praxis_arzt
- oid_zahnarztpraxis
- oid_praxis_psychotherapeut
- oid_krankenhaus

die Operation im Fachdienst aufrufen dürfen, damit E-Rezepte nicht durch zur Verordnung Unberechtigte eingestellt werden können.**[<=]**

A_19257 - E-Rezept-Fachdienst - Schemavalidierung Rezept anlegen
Der E-Rezept-Fachdienst MUSS die im Body der HTTP-POST-Operation auf die Ressource Task übertragenen Parameter gegen das Schema http://gematik.de/fhir/OperationDefinition/CreateOperationDefinition prüfen und bei Nicht-Konformität das Anlegen der Ressource im Fachdienst mit dem http-Status-Code 400 beantworten, damit kein Schadcode und keine "fachfremden" Daten in den E-Rezept-Fachdienst hochgeladen werden.**[<=]**

A_19112 - E-Rezept-Fachdienst - Parametrierung Task für Workflow-Typ
Der E-Rezept-Fachdienst MUSS beim Erzeugen eines Tasks mittels HTTP-POST/$create-Operation den Parameter workFlowType (Rezepttyp) aus dem HTTP-Body des POST-Requests entnehmen, als Attribut `Task.extension:flowType` des zu erstellenden Tasks verwenden und bei Fehlen bzw. Nicht-Konformität des Parameters den Request als unzulässig abweisen, damit auf Basis dieser Parameter ausschließlich gültige Workflows gestartet werden können und dem Versicherten bei Einsicht des Tasks der Weg in entweder eine Apotheke oder ein Sanitätshaus oder eine andere zuständige Einrichtung gewiesen werden kann.**[<=]**

A_19214 - E-Rezept-Fachdienst - Ergänzung Performer-Typ für Einlöseinstitutstyp
Der E-Rezept-Fachdienst MUSS beim Erzeugen eines Tasks das Feld `Task.performerType` aus dem übergebenen, gültigen Parameter `Task.extension:flowType` gemäß der Prozessparameter [gemSpec_DM_eRp#19445] übernehmen.**[<=]**

A_19019 - E-Rezept-Fachdienst - Generierung Rezept-ID
Der E-Rezept-Fachdienst MUSS beim Anlegen eines neuen Tasks eine Rezept-ID gemäß der Bildungsregel [gemSpec_DM_eRp#19217] generieren und als Identifier mit Namingsystem https://gematik.de/fhir/NamingSystem/PrescriptionID dem Task hinzufügen und sicherstellen, dass diese Rezept-ID innerhalb von 10 Jahren nach ihrer Erzeugung nicht erneut vergeben wird, damit es innerhalb der Aufbewahrungsfrist der Abrechnungsdaten bei den Krankenkassen zu keinen Dubletten kommt.**[<=]**

A_19021 - E-Rezept-Fachdienst - Generierung AccessCode
Der E-Rezept-Fachdienst MUSS beim Erzeugen eines Tasks mittels HTTP-POST/$create-Operation eine 256 Bit Zufallszahl mit einer Mindestentropie von 120 Bit erzeugen, hexadezimal kodieren ([0-9a-f]{64}) und diese im zu speichernden Task als

externe ID in Task.identifier:AccessCode
als https://gematik.de/fhir/Namingsystem/accessCode hinzufügen, damit nachfolgende Zugriffe auf diesen Datensatz nur durch Berechtigte in Kenntnis des AccessCodes erfolgen. **[<=]**

A_19114 - E-Rezept-Fachdienst - Status draft
Der E-Rezept-Fachdienst MUSS die zulässige Anlage eines Tasks mittels HTTP-POST/$create-Operation im Status `Task.status = draft` vollziehen und beim erfolgreichen Abschluss der Operation die angelegte Ressource Task im HTTP-Body der HTTP-Response zurückgeben, damit der verordnende Leistungserbringer die generierte Rezept-ID für die QES verwenden kann.**[<=]**

6.1.2.2 POST /Task/<id>/$activate

Die FHIR-Operation $activate startet einen E-Rezept-Workflow eines zuvor unter einer <id> angelegten neuen Tasks. Diese Operation steht ausschließlich verordnenden Leistungserbringern zur Verfügung.

A_19022 - E-Rezept-Fachdienst - Rollenprüfung Verordnender aktiviert Rezept
Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks für ein E-Rezept mittels HTTP-POST/$activate-Operation auf den in der URL referenzierten `/Task/<id>` sicherstellen, dass ausschließlich verordnende Leistungserbringer in der Rolle

- oid_arzt
- oid_zahnarzt
- oid_praxis_arzt
- oid_zahnarztpraxis
- oid_praxis_psychotherapeut
- oid_krankenhaus

die Operation am Fachdienst aufrufen dürfen und die Rolle "`professionOID`" des Aufrufers im ID_TOKEN im HTTP-RequestHeader "`Authorization`" feststellen, damit E-Rezepte nicht durch Unberechtigte eingestellt werden können.**[<=]**

A_19024 - E-Rezept-Fachdienst - Prüfung AccessCode Rezept aktualisieren
Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/$activate den im HTTP-RequestHeader "`X-AccessCode`" übertragenenen AccessCode gegen den im referenzierten Task gespeicherten AccessCode Task.identifier:AccessCode als https://gematik.de/fhir/Namingsystem/accessCode prüfen und bei Ungleichheit oder Fehlen des HTTP-Headers die Operation mit dem HTTP-Fehlercode 403 abbrechen, damit Zugriffe auf diesen Datensatz nur durch Berechtigte in Kenntnis des AccessCodes erfolgen.**[<=]**

A_19020 - E-Rezept-Fachdienst - Schemavalidierung Rezept aktivieren
Der E-Rezept-Fachdienst MUSS den im Aufrufparameter der HTTP-POST-Operation `/Task/<id>/$activate` übergebenen FHIR-Operationsparameter des QES-Datensatzes als PKCS#7-Datei einer Enveloping CAdES-Signatur entgegennehmen und verarbeiten und bei Fehlen oder ungültiger ASN.1 Datenstruktur die Weiterverarbeitung im Fachdienst mit dem http-Status-Code 400 beantworten, damit kein Schadcode und keine "fachfremden" Daten in den E-Rezept-Fachdienst hochgeladen werden. **[<=]**

A_19025 - E-Rezept-Fachdienst - QES prüfen Rezept aktualisieren
Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/$activate die qualifizierte Signatur des QES-Datensatzes gemäß

[ETSI_QES] prüfen und bei nicht gültiger qualifizierter Signatur die Operation mit Status 400 abbrechen bzw. bei gültiger Signatur den Datensatz als PKCS#7-Datei sicher speichern und in`Task.input` mit Codingsystem https://gematik.de/fhir/CodeSystem/Documenttype = 1 über eine interne, eindeutige UUID referenzieren, damit der nachfolgende Workflow ausschließlich auf Basis medizinisch korrekter und vom Leistungserbringer mittels Signatur freigegebener Daten erfolgt. **[<=]**

A_20159 - E-Rezept-Fachdienst - QES Prüfung Signaturzertifikat des HBA
Der E-Rezept-Fachdienst MUSS das QES-Signaturzertifikat C.HP.QES in der Signatur des übergebenen QES-Datensatzes gemäß [gemSpec_PKI#TUC_PKI_030] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 6 : TAB_eRPFD_006 Parameter Prüfung Signaturzertifikat QES des HBA

Parameter	
Zertifikat	Signaturzertifikat des HBA (eingebettet in Signatur-Objekt des QES-Datensatzes) C.HP.QES
Referenzzeitpunkt	<Zeitpunkt der QES.Erstellung gemäß`signingTime` im QES-Datensatz>
Offline-Modus	nein
OCSP-Response	(leer)

und darf die OCSP-Response für die Abfrage des Zertifikatsstatus für 12 Stunden zwischenspeichern.
Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig] befunden werden und der HTTP-Request andernfalls mit dem HTTP-Status-Code 400 abgelehnt werden, damit sichergestellt wird, dass ausschließlich E-Rezepte verwaltet werden die von einer gültigen, nicht gesperrten Heilberufsidentität eines HBA signiert wurden.
[<=]

A_19225 - E-Rezept-Fachdienst - QES durch berechtigte Berufsgruppe
Der E-Rezept-Fachdienst MUSS die Aktivierung eines E-Rezept-Tasks mit dem HTTP-Status-Code 400 abbrechen, wenn die QES gemäß der professionOID des Signaturzertifikats des Signierers nicht von einer Berufsgruppe ausgestellt wurde, die der folgenden professionOID entspricht:

- oid_arzt
- oid_zahnarzt

damit nur solche Leistungserbringer ein signiertes E-Rezept einstellen, die zur Verordnung von Medikamenten ermächtigt sind.**[<=]**

A_19999 - E-Rezept-Fachdienst - Ergänzung PerformerTyp für Einlöseinstitutstyp
Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks aus dem Feld `Task.performerType` die Prozessparameter des Tasks gemäß [gemSpec_DM_eRp#19445] ableiten und befüllen.**[<=]**

A_19127 - E-Rezept-Fachdienst - Übernahme der KVNR des Patienten

Der E-Rezept-Fachdienst MUSS im Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/$activate und bei gültiger qualifizierter elektronischer Signatur die KVNR des Patienten dem Identifier http://fhir.de/NamingSystem/gkv/kvid-10 der Patient-Ressource im signierten E-Rezept-Bundle gemäß https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle des QES-Datensatzes entnehmen und diese als `Identifier` mit dem Value-Set http://fhir.de/NamingSystem/gkv/kvid-10 dem Task in `Task.for` hinzufügen, damit ausschließlich eine gültige, vom Arzt signierte Patientenreferenz im Workflow verwendet wird. **[<=]**

A_19128 - E-Rezept-Fachdienst - Status aktivieren
Der E-Rezept-Fachdienst MUSS die zulässige Aktivierung eines Tasks mittels /Task/<id>/$activate-Operation im Status`Task.status = ready` vollziehen und bei erfolgreichem Abschluss der Operation die Ressource Task im HTTP-Body der HTTP-Response zurückgeben, damit der verordnende Leistungserbringer über den erfolgreichen Abschluss der Operation in Kenntnis gesetzt wird.**[<=]**

A_19029 - E-Rezept-Fachdienst - Serversignatur Rezept aktivieren
Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels /Task/<id>/$activate das im QES-Datensatz enthaltene FHIR-E-Rezept-Bundle vom Profil https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle in ein Bundle gleichen Typs in JSON-Repräsentation transformieren, einen neuen Identifier für `Bundle.id` als UUID generieren, das Bundle entsprechend der Kanonisierungsregeln http://hl7.org/fhir/canonicalization/json#static normalisieren und mit der Signaturidentität des Fachdienstes ID.FD.SIG gemäß [FHIR-Sig] signieren und das signierte Bundle mit Referenz in `Task.input` mit Codingsystem `https://gematik.de/fhir/CodeSystem/Documenttype = 2` speichern, damit der Versicherte einen Nachweis über die Integrität der gespeicherten Daten einsehen kann. **[<=]**

Offener Punkt:

Der E-Rezept-Fachdienst muss beim Aktivieren eines Tasks für einen Versicherten an die für diesen Versicherten registrierte Geräte-ID eine Push-Notification "neues E-Rezept erhalten" über den entsprechenden Notification-Service (FCM oder APNs) verschicken.

6.1.2.3 POST /Task/<id>/$accept

Die FHIR-Operation $accept weist ein E-Rezept einem abgebenden Leistungserbringer (bzw. der Apotheke als Leistungserbringerinstitution) als "in Abgabe" befindlich über die <id> referenzierten Tasks zu. Diese Operation steht ausschließlich abgebenden Leistungserbringern in Kenntnis des AccessCodes zur Verfügung.

A_19166 - E-Rezept-Fachdienst - Rollenprüfung Abgebender ruft Rezept ab
Der E-Rezept-Fachdienst MUSS beim Abrufen eines Tasks für ein E-Rezept mittels HTTP-POST/$accept-Operation auf den in der URL referenzierten `/Task/<id>` sicherstellen, dass ausschließlich abgebende Leistungserbringer in der Rolle

- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am Fachdienst aufrufen dürfen und die Rolle "`professionOID`" des Aufrufers im ID_TOKEN im HTTP-RequestHeader "`Authorization`" feststellen, damit E-Rezepte nicht durch Unberechtigte abgerufen werden können. **[<=]**

A_19167 - E-Rezept-Fachdienst - Prüfung AccessCode Rezept abrufen

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/$accept den im URL-Parameter "`?ac=...`" übertragenen AccessCode gegen den im referenzierten Task gespeicherten AccessCode `Task.identifier:AccessCode` als https://gematik.de/fhir/Namingsystem/accessCode prüfen und bei Ungleichheit oder Fehlen des URL-Parameters die Operation mit dem HTTP-Fehlercode 403 abbrechen, damit Zugriffe auf diesen Datensatz nur durch Berechtigte in Kenntnis des AccessCodes erfolgen. **[<=]**

A_19168 - E-Rezept-Fachdienst - Rezept bereits in Abgabe oder Bearbeitung
Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/$accept die Operation mit dem HTTP-Fehlercode 409 abbrechen, wenn der Status`Task.status = in-progress` oder `Task.status = draft` ist, damit ein bereits in Abgabe befindliches E-Rezept nicht durch eine zweite Apotheke bearbeitet werden kann.**[<=]**

A_19169 - E-Rezept-Fachdienst - Generierung Secret, Statuswechsel in Abgabe und Rückgabewert
Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/$accept den Status des Tasks auf`Task.status = in-progress` setzen, eine 256 Bit Zufallszahl mit einer Mindestentropie von 120 Bit erzeugen, hexadezimal kodieren ([0-9a-f]{64}) und diese im zu speichernden Task als externe ID in `Task.identifier:Secret` als https://gematik.de/fhir/Namingsystem/Secret hinzufügen und den Task im Bundle mit dem in `Task.input` mit Codingsystem `https://gematik.de/fhir/CodeSystem/Documenttype = 1` referenzierten QES-Datensatz als Binary-Ressource https://www.hl7.org/fhir/binary.html an den Aufrufer zurückgeben, damit das E-Rezept für die nachfolgende Bearbeitung durch den abrufenden Apotheker reserviert ist. **[<=]**

A_19149 - E-Rezept-Fachdienst - Prüfung Datensatz zwischenzeitlich gelöscht
Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/$accept die Operation mit dem HTTP-Fehlercode 410 abbrechen, wenn der referenzierte /Task/<id> existiert, jedoch kein AccessCode im Task.identifier:AccessCode als https://gematik.de/fhir/Namingsystem/accessCode vorhanden ist oder der Status `Task.status = cancelled` ist, damit ein Apotheker den Versicherten über die zwischenzeitliche Löschung des Datensatzes in Kenntnis setzen kann.**[<=]**

6.1.2.4 POST /Task/<id>/$reject

Die FHIR-Operation $reject nutzt die abgebende LEI, um ein E-Rezept zurück zu geben. Anschließend kann das E-Rezept von einer anderen Apotheke in Kenntnis des AccessCodes und der ID des Tasks wieder abgerufen werden oder der Versicherte das E-Rezept bei Bedarf löschen.

A_19170 - E-Rezept-Fachdienst - Rollenprüfung Abgebender ruft Rezept ab
Der E-Rezept-Fachdienst MUSS beim Zurückweisen eines Tasks für ein E-Rezept mittels HTTP-POST/$reject-Operation auf den in der URL referenzierten `/Task/<id>` sicherstellen, dass ausschließlich abgebende Leistungserbringer in der Rolle

- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ID_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit das E-Rezept nicht durch einen Unberechtigten zurückgewiesen werden kann. **[<=]**

A_19171 - E-Rezept-Fachdienst - Prüfung Secret Rezept zurückweisen
Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/$reject das im URL-Parameter "?secret=..." übertragene Secret gegen das im referenzierten Task gespeicherte SecretTask.identifier:Secret als https://gematik.de/fhir/Namingsystem/Secret prüfen und bei Ungleichheit oder Fehlen des URL-Parameters die Operation mit dem HTTP-Fehlercode 403 abbrechen, damit der Zugriff auf diesen Datensatz nur durch den Berechtigten in Kenntnis des Secrets erfolgt.**[<=]**

A_19172 - E-Rezept-Fachdienst - Löschung Secret und Status
Der E-Rezept-Fachdienst MUSS beim Zurückweisen eines Tasks mittels HTTP-POST-Operation über /Task/<id>/$reject die externe ID inTask.identifier:Secret als https://gematik.de/fhir/Namingsystem/Secret löschen und den Status des referenzierten Tasks auf Task.status = ready setzen, damit nachfolgende Zugriffe auf diesen Datensatz durch Berechtigte in Kenntnis des AccessCodes erfolgen können. **[<=]**

6.1.2.5 POST /Task/<id>/$close

Die FHIR-Operation $close beendet den E-Rezept-Workflow des unter der <id> geführten Tasks, erzeugt eine Quittung als Signatur über das vom abgebenden Leistungserbringer eingestellte MedicationDispense und speichert die vom Apotheker übermittelten Dispensierinformationen für den Versicherten. Diese Operation steht ausschließlich abgebenden Leistungserbringern in Kenntnis eines generierten Secrets zur Verfügung.

A_19230 - E-Rezept-Fachdienst - Rollenprüfung Abgebender vollzieht Abgabe des Rezepts
Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks für ein E-Rezept mittels HTTP-POST/$close-Operation auf den in der URL referenzierten /Task/<id> sicherstellen, dass ausschließlich abgebende Leistungserbringer in der Rolle

- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ID_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit der E-Rezept-Workflow nicht durch einen Unberechtigten abgeschlossen werden kann. **[<=]**

A_19231 - E-Rezept-Fachdienst - Prüfung Secret Rezept beenden
Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels HTTP-POST-Operation über /Task/<id>/$close das im URL-Parameter "?secret=..." übertragene Secret gegen das im referenzierten Task gespeicherte SecretTask.identifier:Secret als https://gematik.de/fhir/Namingsystem/Secret prüfen und bei Ungleichheit oder Fehlen des URL-Parameters die Operation mit dem HTTP-Fehlercode 403 abbrechen, damit der Zugriff auf diesen Datensatz nur durch den Berechtigten in Kenntnis des Secrets erfolgt. **[<=]**

A_19248 - E-Rezept-Fachdienst - Schemaprüfung und Speicherung MedicationDispense
Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels /Task/<id>/$close das im http-Body des Requests enthaltene MedicationDispense-Objekt gegen das Profil https://gematik.de/fhir/StructureDefinition/erxMedicationDispense prüfen und bei Gültigkeit die Rezept-ID https://gematik.de/fhir/NamingSystem/PrescriptionID als zusätzlichen MedicationDispense.identifier , die

KVNR http://fhir.de/NamingSystem/gkv/kvid-10 des Versicherten aus dem referenzierten Task in `MedicationDispense.subject:identifier` und die TelematikID der Apotheke gemäß ID_TOKEN in `MedicationDispense.performer.actor:identifier` sowie die Referenz auf den aufgerufenen Task `/Task/<id>` als `MedicationDispense.supportingInformation` übernehmen und die MedicationDispense für den Abruf durch den Versicherten speichern. **[<=]**

A_19232 - E-Rezept-Fachdienst - Status beenden
Der E-Rezept-Fachdienst MUSS die zulässige Beendigung eines Tasks mittels /Task/<id>/$close-Operation im Status`Task.status = completed` vollziehen, damit der Workflow für den Versicherten als beendet und das E-Rezept somit als eingelöst dargestellt wird.**[<=]**

A_19233 - E-Rezept-Fachdienst - Serversignatur Rezept beenden (Quittung erstellen)
Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels /Task/<id>/$close die übergebene Ressource MedicationDispense in ein Quittungsbundle des FHIR-Profils https://gematik.de/fhir/StructureDefinition/erxReceipt einbetten, dieses Quittungs-Bundle in XML-Darstellung gemäß http://hl7.org/fhir/canonicalization/xml#static kanonisieren und mit der Signaturidentität des Fachdienstes ID.FD.SIG gemäß [RFC5652] mit Profil CAdES-BES ([CAdES]) im Enveloping signieren, das Signatur-Ergebnis in der Codierung als `dss:Base64Signature`-Objekt in `Bundle.signature` einbetten und dieses Quittungs-Bundle mit Referenz in `Task.output` mit Codingsystem https://gematik.de/fhir/CodeSystem/Documenttype `= 3` speichern sowie als Response des http-Requests an den Aufrufer zurückgeben, damit der Apotheker einen Nachweis über den ordnungsgemäßen Abschluss des E-Rezept-Workflows als Quittung erhält. **[<=]**

6.1.2.6 POST /Task/<id>/$abort

Die FHIR-Operation $abort bricht einen unter der <id> angelegten Task als aktiven E-Rezept-Workflow ab und führt zum Löschen aller personenbezogenen und medizinischen Daten. Diese Operation steht allen Nutzern in Kenntnis des AccessCodes (verordnende und abgebende Leistungserbringer, Versicherte, Vertreter) zur Verfügung.

A_19026 - E-Rezept-Fachdienst - Rollenprüfung Nutzer löscht Rezept
Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der <id> adressierten`/Task/<id>/$abort` sicherstellen, dass ausschließlich Nutzer in der Rolle

- oid_versicherter
- oid_arzt
- oid_zahnarzt
- oid_praxis_arzt
- oid_zahnarztpraxis
- oid_praxis_psychotherapeut
- oid_krankenhaus
- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ID_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit E-Rezepte nicht durch Unberechtigte gelöscht werden können. **[<=]**

A_19145 - E-Rezept-Fachdienst - Statusprüfung Apotheker löscht Rezept
Der E-Rezept-Fachdienst MUSS das Löschen eines E-Rezepts über den mittels der <id> adressierten/Task/<id>/$abort verhindern und die Operation mit dem HTTP-Fehlercode 403 abweisen, wenn der Status des adressierten Tasks gleich "in-progress" ist und die Rolle des aufrufenden Nutzers einer der folgenden Rollen entspricht:

- oid_versicherter
- oid_arzt
- oid_zahnarzt
- oid_praxis_arzt
- oid_zahnarztpraxis
- oid_praxis_psychotherapeut
- oid_krankenhaus

damit Nutzer außerhalb der Apotheke keine Rezepte löschen, die sich aktuell in Belieferung befinden.**[<=]**

A_19146 - E-Rezept-Fachdienst - Statusprüfung Nutzer (außerhalb Apotheke) löscht Rezept
Der E-Rezept-Fachdienst MUSS das Löschen eines E-Rezepts über den mittels der <id> adressierten/Task/<id>/$abort verhindern und die Operation mit dem HTTP-Fehlercode 403 abweisen, wenn der Status des adressierten Tasks ungleich "in-progress" ist und die Rolle des aufrufenden Nutzers einer der folgenden Rollen entspricht:

- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

damit kein Apotheker ein Rezept löscht, das ihm nicht ausdrücklich zugewiesen wurde. **[<=]**

A_19120 - E-Rezept-Fachdienst - Prüfung AccessCode Nutzer löscht Rezept
Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der <id> adressierten/Task/<id>/$abort durch Versicherte oder verordnende Leistungserbringer den im HTTP-Header "X-AccessCode" gegen den im referenzierten Task enthaltenen AccessCode prüfen und bei Missmatch oder Fehlen im HTTP-Header den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich Nutzer in Kenntnis des AccessCodes als Berechtigte (inkl. des betroffenen Versicherten) ein E-Rezept löschen.**[<=]**

A_19224 - E-Rezept-Fachdienst - Prüfung Secret Apotheker löscht Rezept
Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der <id> adressierten/Task/<id>/$abort durch abgebende Leistungserbringer (Apotheken) das im URL-Parameter "?secret=..." übertragene Geheimnis gegen das im referenzierten Task enthaltene Secret inTask.identifier prüfen und bei Missmatch oder Fehlen des URL-Parameters den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich Apotheker in Kenntnis des Secret als Berechtigte ein E-Rezept löschen.**[<=]**

A_19027 - E-Rezept-Fachdienst - Rezept löschen
Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der <id> adressierten/Task/<id>/$abort alle personenbezogenen medizinischen Daten aus dem referenzierten Task entfernen. Dies gilt insbesondere für:

- Task.for (KVNR des Patienten)--> löschen
- Task.input --> löschen (inkl. aller referenzierten Elemente)
- Task.output --> löschen (inkl. aller referenzierten Elemente)
- Task.identifier (AccessCode) --> löschen
- Task.identifier (Secret, falls vorhanden) --> löschen
- MedicationDispense --> die in MedicationDispense.supportingInformation auf Task.id verweist
- Communication --> die in Communication.basedOn auf Task.id verweist

damit dem Betroffenenrecht auf Löschen durch den Versicherten entsprochen wird und beim Löschen durch den Verordnenden dem Versicherten eine aussagekräftige Fehlermeldung durch einen Apotheker vermittelt werden kann.**[<=]**

A_19121 - E-Rezept-Fachdienst - Finaler Status cancelled
Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der <id> adressierten`/Task/<id>/$abort` den Status des Tasks `Task.status` auf den Wert "`cancelled`" setzen, damit das E-Rezept nicht weiter bearbeitet werden kann.**[<=]**

6.2 Ressource MedicationDispense

Dem Versicherten werden über die Ressource MedicationDispense Informationen über ein eingelöstes E-Rezept bereitgestellt. Im MedicationDispense ist dabei die Referenz auf das abgegebene Medikament enthalten. Diese Informationen unterstützen den Versicherten im Versorgungsprozess, indem ihm bspw. mittels dieser Informationen ein digitaler Beipackzettel oder weitere Informationen wie Applikationsanleitungen zur Verfügung gestellt werden können. Der Zugriff auf die Ressource MedicationDIspense erfolgt ausschließlich lesend über die http-GET-Operation. Das Löschen erfolgt indirekt über das Löschen des der MedicationDispense zugrunde liegenden Tasks.

A_19400 - E-Rezept-Fachdienst - unzulässige Operationen MedicationDispense
Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource MedicationDispense mittels der HTTP-Operationen PUT, PATCH, HEAD und DELETE sowie POST unterbinden, damit keine unzulässigen Operationen auf den Rezeptdaten ausgeführt werden können.**[<=]**

6.2.1 HTTP-Operation GET /MedicationDispense

A_19405 - E-Rezept-Fachdienst - Rollenprüfung Versicherter liest MedicationDispense
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/MedicationDispense` und auf einen konkreten über <id> adressierten`/MedicationDispenses/<id>` sicherstellen, dass ausschließlich Versicherte in der Rolle

- oid_versicherter

die Operation am Fachdienst aufrufen dürfen und die Rolle "`professionOID`" des Aufrufers im ID_TOKEN im HTTP-RequestHeader "`Authorization`" feststellen, damit Dispensierinformationen nicht durch Unberechtigte ausgelesen werden können.**[<=]**

A_19406 - E-Rezept-Fachdienst - Filter MedicationDispense auf KVNR des Versicherten

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/MedicationDispense` die dem Versicherten zugeordneten MedicationDispense-Ressourcen anhand der KVNR des Versicherten im ID_TOKEN im "`Authorization`"-Header des HTTP-Requests identifizieren, die in`MedicationDispense.identifier` mit Codesystem http://fhir.de/NamingSystem/gkv/kvid-10 die entsprechende KVNR des begünstigten Patienten referenziert haben, damit ausschließlich Versicherte ihre eigenen Dispensierinformationen einsehen können.**[<=]**

A_19518 - E-Rezept-Fachdienst - Suchparameter für MedicationDispense
Der E-Rezept-Fachdienst MUSS das Eingrenzen einer Suchanfrage auf`/MedicationDispense` über die URL-Parameter gemäß https://www.hl7.org/fhir/medicationdispense.html#search für die Attribute MedicationDispense.whenHandedOver und MedicationDispense.performer.actor erlauben, damit Versicherte eine Suche und Sortierung nach Ausgabedatum sowie der aufgesuchten Apotheke durchführen können.**[<=]**

6.3 Ressource Communication

Der E-Rezept-Fachdienst ermöglicht eine direkte Kommunikation zwischen Versicherten und Apotheken über die Belieferung von E-Rezepten über den Endpunkt `<Fachdienst-URL>/Communication` gemäß der FHIR-Definition in https://www.hl7.org/fhir/communication.html .

A_19401 - E-Rezept-Fachdienst - unzulässige Operationen Communication
Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource Communication mittels der HTTP-Operationen PUT, PATCH, HEAD und DELETE unterbinden, damit keine unzulässigen Operationen auf den Kommunikationsnachrichten ausgeführt werden können.**[<=]**

A_19446 - E-Rezept-Fachdienst - Rollenprüfung Versicherter oder Apotheker liest Rezept
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET und POST-Operation auf den Endpunkt `/Communication` sicherstellen, dass ausschließlich Versicherte und Apotheken in der Rolle

- oid_versicherter
- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am Fachdienst aufrufen dürfen und die Rolle "`professionOID`" des Aufrufers im ID_TOKEN im HTTP-RequestHeader "`Authorization`" feststellen, damit der Nachrichtenaustausch nicht zwischen Unbefugten erfolgt. **[<=]**

6.3.1 HTTP-Operation GET

Die HTTP-Operation GET wird für den Nachrichtenabruf verwendet. Dabei werden alle Anfragen auf Basis der KVNR bzw. Telematik-ID im übergebenen ID_TOKEN gefiltert, um die Nachrichten des jeweiligen Empfängers zu finden. Zusätzliche Filteranfragen für den Abruf ungelesener Nachrichten oder eine Sortierung nach Sendedatum sind zusätzlich möglich.

6.3.1.1 GET /Communication/

A_19520 - E-Rezept-Fachdienst - Nachrichten für Empfänger filtern
Der E-Rezept-Fachdienst MUSS beim Abrufen von Nachrichten über die http-Operation GET auf den Endpunkt `/Communication` bzw. beim Abruf einer einzelnen Nachricht über `/Communication/<id>` ausschließlich die Nachrichten an den Aufrufer zurückgeben, die im Attribut Communication.recipient mit dem entsprechenden NamingSystem https://gematik.de/fhir/Namingsystem/TelematikID für Apotheken bzw. http://fhir.de/NamingSystem/gkv/kvid-10 für Versicherte den gleichen Typ und den identischen Wert haben wie im Attribut "`sub`" des übergebenen IdP-Token im HTTP-Header "`Authorization`" für KVNR bzw. Telematik-ID, damit keine Nachrichten an Dritte unrechtmäßig ausgelesen werden. **[<=]**

A_19521 - E-Rezept-Fachdienst - Nachrichten als abgerufen markieren
Der E-Rezept-Fachdienst MUSS beim Abrufen von Nachrichten über die http-Operation GET auf den Endpunkt `/Communication` bzw. beim Abruf einer einzelnen Nachricht über `/Communication/<id>` den Wert des Attributs Communication.received = <aktuelle Systemzeit> setzen, wenn dieser Wert zum Zeitpunkt des Abrufs der Nachrichten`NULL` ist, damit Nutzer eine Filtermöglicheit auf "neue Nachrichten" haben.**[<=]**

A_19522 - E-Rezept-Fachdienst - Nachrichtenabruf Suchparameter
Der E-Rezept-Fachdienst MUSS das Eingrenzen einer Suchanfrage auf `/Communication` über die URL-Parameter gemäß https://www.hl7.org/fhir/communication.html#search für die Attribute Communication.sent und Communication.received erlauben, damit Versicherte eine Suche nach neuen Nachrichten und eine Sortierung nach Sende- und Empfangsdatum durchführen können.**[<=]**

A_19534 - E-Rezept-Fachdienst - Rückgabe Communication im Bundle Paging
Der E-Rezept-Fachdienst KANN beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Communication` die Ergebnisliste der Communication-Ressourcen bei mehr als 50 Einträgen das Suchergebnis in einem Paging-Mechanismus auf mehrere Ergebnis-Bundle aufteilen, damit der Nutzer eine komfortable Navigationsmöglichkeit in seinen Nachrichten erhält.**[<=]**

6.3.2 HTTP-Operation POST

Mit der HTTP-Operation POST erfolgt der Versand einer Kommunikationsnachricht an eine Identität der Telematikinfrastruktur, welche über ihre systemweit eindeutige Identifikationsnummer Telematik-ID bzw. Versicherten-ID (10-stelliger Anteil der KVNR) adressiert wird.

6.3.2.1 POST /Communication/

A_19447 - E-Rezept-Fachdienst - Nachricht einstellen Schemaprüfung
Der E-Rezept-Fachdienst MUSS beim Einstellen einer Nachricht über die http-Operation POST auf den Endpunkt `/Communication` die im http-Request-Body übergebene Communications-Ressource gegen das aus der Kommunikationsbeziehung ableitbare, zulässige Schema gemäß TAB_eRPFD_008

Tabelle 7 TAB_eRPFD_008 Nachrichtentyp zu Kommunikationsbeziehung

sender	recipient	zusätzliche Bedingung	Schema

KVNR	TelematikID	Communication.basedOn referenziert Task	https://gematik.de/fhir/StructureDefinition/erxCommunicationDispReq
KVNR	TelematikID	Communication.about referenziert Medication	https://gematik.de/fhir/StructureDefinition/erxCommunicationInfoReq
TelematikID	KVNR	-	https://gematik.de/fhir/StructureDefinition/erxCommunicationReply
KVNR	KVNR	-	https://gematik.de/fhir/StructureDefinition/erxCommunicationRepresentative

prüfen und den Aufruf bei Nicht-Konformität mit dem http-Status-Code 400 ablehnen, damit ausschließlich konforme E-Rezept-Nachrichten ausgetauscht werden. **[<=]**

A_19448 - E-Rezept-Fachdienst - Nachricht einstellen Absender und Sendedatum
Der E-Rezept-Fachdienst MUSS beim Einstellen einer Nachricht über die http-Operation POST auf den Endpunkt `/Communication` die Absenderidentifikation aus dem Attribut "`sub`" des übergebenen IdP-Token im HTTP-Header "`Authorization`" mit dem entsprechenden NamingSystem https://gematik.de/fhir/Namingsystem/TelematikID für Apotheken bzw. http://fhir.de/NamingSystem/gkv/kvid-10 für Versicherte übernehmen sowie das Absendedatum `Communication.sent` auf die aktuelle Systemzeit des E-Rezept-Fachdienstes setzen, damit Absender und Sendezeitpunkt für den Empfänger eindeutig sind. **[<=]**

A_20229 - E-Rezept-Fachdienst - Nachrichtenzähler bei Versicherter-zu-Versichertem-Kommunikation
Der E-Rezept-Fachdienst MUSS die zulässige Anzahl der Communication-Ressourcen des Schemas https://gematik.de/fhir/StructureDefinition/erxCommunicationRepresentative zur Versicherter-zu-Versichertem-Kommunikation auf einen konfigurierbaren Maximalwert (Default: 10) je referenziertem Task beschränken und bei Überschreiten des Maximalwerts das Einstellen einer Nachricht mit dem http-Status-Code 429 abbrechen, damit Versicherte den E-Rezept-Fachdienst nicht für beliebige Kommunikation missbrauchen. **[<=]**

A_20230 - E-Rezept-Fachdienst - Einlösbare E-Rezepte für Versicherter-zu-Versichertem-Kommunikation
Der E-Rezept-Fachdienst MUSS beim Einstellen einer Nachricht des Schemas https://gematik.de/fhir/StructureDefinition/erxCommunicationRepresentative zur Versicherter-zu-Versichertem-Kommunikation über die http-Operation POST auf den Endpunkt `/Communication` mit dem http-Status-Code 400 abbrechen, wenn der referenzierte Task nicht im Zustand "ready" oder "in-progress" ist, damit die Weitergabe des Zugriffs auf E-Rezepte ausschließlich auf einlösbare bzw. in Arbeit befindliche Verordnungen beschränkt wird. **[<=]**

A_20231 - E-Rezept-Fachdienst - Ausschluss Nachrichten an Empfänger gleich Absender
Der E-Rezept-Fachdienst MUSS das Einstellen einer Nachricht über die http-Operation POST auf den Endpunkt `/Communication` mit dem http-Status-Code 400 abbrechen,

wenn der Empfänger `Communication.recipient` gleich der Absenderidentifikation im Attribut "`sub`" des übergebenen IdP-Token im HTTP-Header "`Authorization`" ist, damit irreführende Kommunikationsbeziehungen nicht zu einer vermeidbaren Mehrbelastung des E-Rezept-Fachdienstes führen. **[<=]**

A_19450 - E-Rezept-Fachdienst - Nachricht einstellen Schadcodeprüfung
Der E-Rezept-Fachdienst MUSS das Einstellen einer Nachricht über die http-Operation POST auf den Endpunkt `/Communication` mit dem http-Status-Code 400 abbrechen, wenn der Nachrichteninhalt `Communication.payload` größer als 10 kByte ist oder externe URLs enthält oder ein `Attachment` mit MimeType "`application/*`" enthält, damit über den E-Rezept-Fachdienst kein Schadcode verteilt wird.**[<=]**

Offener Punkt:

Der E-Rezept-Fachdienst muss beim Einstellen einer Communication-Ressource für einen Versicherten an die für diesen Versicherten registrierte Geräte-ID eine Push-Notification "neue Nachricht zum E-Rezept erhalten" über den entsprechenden Notification-Service (FCM oder APNs) verschicken.

6.4 Ressource AuditEvent

Der E-Rezept-Fachdienst protokolliert alle Zugriffe auf personenbezogene und medizinische Daten der E-Rezepte von Versicherten. Über den Endpunkt `<Fachdienst-URL>/AuditEvent` stehen diese für den Abruf durch den jeweils betroffenen Versicherten zur Verfügung. Ein manuelles Löschen der Protokolleinträge ist nicht möglich, die Protokolleinträge werden gemäß der Löschfrist im E-Rezept-Fachdienst gespeichert und nach Ablauf dieser Frist automatisch gelöscht.

A_19402 - E-Rezept-Fachdienst - unzulässige Operationen AuditEvent
Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource AuditEvent mittels der HTTP-Operationen PUT, PATCH, HEAD und DELETE sowie POST unterbinden, damit keine unzulässigen Operationen auf den Protokolldaten ausgeführt werden können.**[<=]**

6.4.1 HTTP-Operation GET /AuditEvent

A_19395 - E-Rezept-Fachdienst - Rollenprüfung Versicherter liest AuditEvent
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/AuditEvent` und auf einen konkreten über <id> adressierten`/AuditEvent/<id>` sicherstellen, dass ausschließlich Versicherte in der Rolle

- oid_versicherter

die Operation am Fachdienst aufrufen dürfen und die Rolle "`professionOID`" des Aufrufers im ID_TOKEN im HTTP-RequestHeader "`Authorization`" feststellen, damit E-Rezept-Protokolleinträge nicht durch Unberechtigte ausgelesen werden können.**[<=]**

A_19396 - E-Rezept-Fachdienst - Filter AuditEvent auf KVNR des Versicherten
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/AuditEvent` die dem Versicherten zugeordneten AuditEvent-Ressourcen anhand der KVNR des Versicherten im ID_TOKEN im "`Authorization`"-Header des HTTP-Requests identifizieren, die in`AuditEvent.entity.name` die entsprechende KVNR des begünstigten Patienten referenziert haben, damit ausschließlich Versicherte ihre eigenen E-Rezept-Protokolleinträge einsehen können.**[<=]**

A_19399 - E-Rezept-Fachdienst - Suchparameter AuditEvent
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/AuditEvent` eine Sortierung über die Attribute der Protokolleinträge "`date`", "`agent`" und "`subType`" gemäß der Festlegungen für die Ressource AuditEvent https://www.hl7.org/fhir/auditevent.html#search in den URL-Parametern zulassen, damit sich Versicherte in ihrem Zugriffsprotokoll besser zurecht finden.**[<=]**

A_19397 - E-Rezept-Fachdienst - Rückgabe AuditEvents im Bundle
Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/AuditEvent` die Ergebnisliste der AuditEvent-Ressourcen bei mehr als einem Eintrag als Ergebnis-Bundle an den Aufrufer zurückgeben, damit der Versicherte eine vollständige Einsicht in das Zugriffsprotokoll erhält.**[<=]**

A_19398 - E-Rezept-Fachdienst - Rückgabe AuditEvents im Bundle Paging
Der E-Rezept-Fachdienst KANN beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/AuditEvent` die Ergebnisliste der AuditEvent-Ressourcen bei mehr als 50 Einträgen das Suchergebnis in einem Paging-Mechanismus auf mehrere Ergebnis-Bundle aufteilen, damit der Versicherte eine komfortable Navigationsmöglichkeit in seinem Zugriffprotokoll erhält.**[<=]**

7 Informationsmodell

Der E-Rezept-Fachdienst verwaltet E-Rezepte mittels der HL7-FHIR-Workflow-Ressource Task. Die Statusübergänge im Task werden durch verschiedene FHIR-Operationen der Ressource Task getriggert. Als Payload eines Tasks werden verschiedene E-Rezept-Bundles als Nutzdaten transportiert bzw. fachdienstseitig erzeugt.

- E-Rezept-Bundle, enveloping in QES-Datensatz enthalten (Task.input),
  Enthält die eigentlichen Verordnungsdaten, inkl. qualifizierter elektronischer Signatur des Arztes bzw. Zahnarztes
- Kopie des E-Rezept-Bundles (Task.input),
  Kopie der Verordnungsdaten für die Einsicht durch den Versicherten, inkl. serverseitiger Signatur
- Quittungs-Bundle (Task.output),
  Zusammenstellung aus QES-signierten Verordnungsdaten und Workflowdaten, inkl. serverseitiger Signatur

Für die Nachvollziehbarkeit der Medikamentenabgabe an den Versicherten erwartet der E-Rezept-Fachdienst zum Abschluss des Workflows die Übergabe einer MedicationDispense-Ressource von der abgebenden Leistungserbringerinstitution (Apotheke), die das abgegebene Medikament in einer Medication-Ressource dokumentiert. Die Verbindung zwischen MedicationDispense und Task erfolgt über MedicationDispense.supportingInformation.

Über den Zugriff auf personenbezogene medizinische Daten des Tasks und der MedicationDispenses führt der E-Rezept-Fachdienst ein Zugriffsprotokoll mittels der Ressource AuditEvent zum Abruf durch den Versicherten. Das Attribut AuditEvent.entity speichert dabei die Referenz des betroffenen Datenobjekts und die KVNR des Versicherten.

Über die Ressource Communication steht Versicherten und Apotheken ein Nachrichtenaustausch zur Verfügung. Communication-Einträge können dabei vom Versicherten eingestellt an Apotheken adressiert werden, Apotheken können Communication-Einträge für Versicherte bereitstellen. Mit der Communication-Ressource stellt der E-Rezept-Fachdienst keine vollwertige Messenger-Plattform zur Verfügung. Nachrichten von Versicherten an Versicherte sind im begrenzten Rahmen (Referenz eines Tasks und maximale Anzahl Nachrichten zu einem Task) zulässig, die Größe transportierbarer Communications-Einträge ist bewusst auf wenige Kilobytes begrenzt, um den Transport von Schadcode zu erschweren und den Nachrichtenaustausch auf die Belieferung von E-Rezepten zu beschränken. Um verschiedene Kommunikationsbeziehungen [Versicherter - Apotheke, Apotheke - Versicherter, Versicherter - Versicherter] abzubilden, werden dezidierte Profile für die Communication-Ressource definiert. Mit diesen Profilen werden Nachrichtentypen realisiert, um die jeweiligen Restriktionen für Verfügbarkeitsanfrage, Einlöseauftrag und Vertreterkommunikation abzubilden.

Der E-Rezept-Fachdienst speichert und verwaltet keine Patient-, Practitioner und Organization-Ressourcen. Sämtliche Bezüge zu verordnenden und abgebenden Leistungserbringern, Praxen und Apotheken sowie Versicherten erfolgen über logische Referenzen. Somit wird der Aufbau einer zentralen Patienten-Kartei und Liste verordnender Ärzte im E-Rezept-Fachdienst unnötig. Zudem löscht der E-Rezept-Fachdienst regelmäßig veraltete Daten, um die Verfügbarkeit der für den Workflow notwendigen Daten auf ein Minimum zu beschränken.

Der E-Rezept-Fachdienst startet einen E-Rezept-Workflow ausschließlich bei einer gültigen Verordnung, das heißt, das E-Rezept-Bundle muss über eine gültige QES eines zur Verordnung berechtigten Leistungserbringers verfügen. Zudem wird die Patientenreferenz (KVNR) aus genau diesem Datensatz verwendet, um dem Patienten, dem diese Verordnung gemäß ärztlicher Signatur gilt, die Hoheit über das E-Rezept einzuräumen.

Die nachfolgende Abbildung gibt eine Übersicht der verwalteten FHIR-Ressourcen.

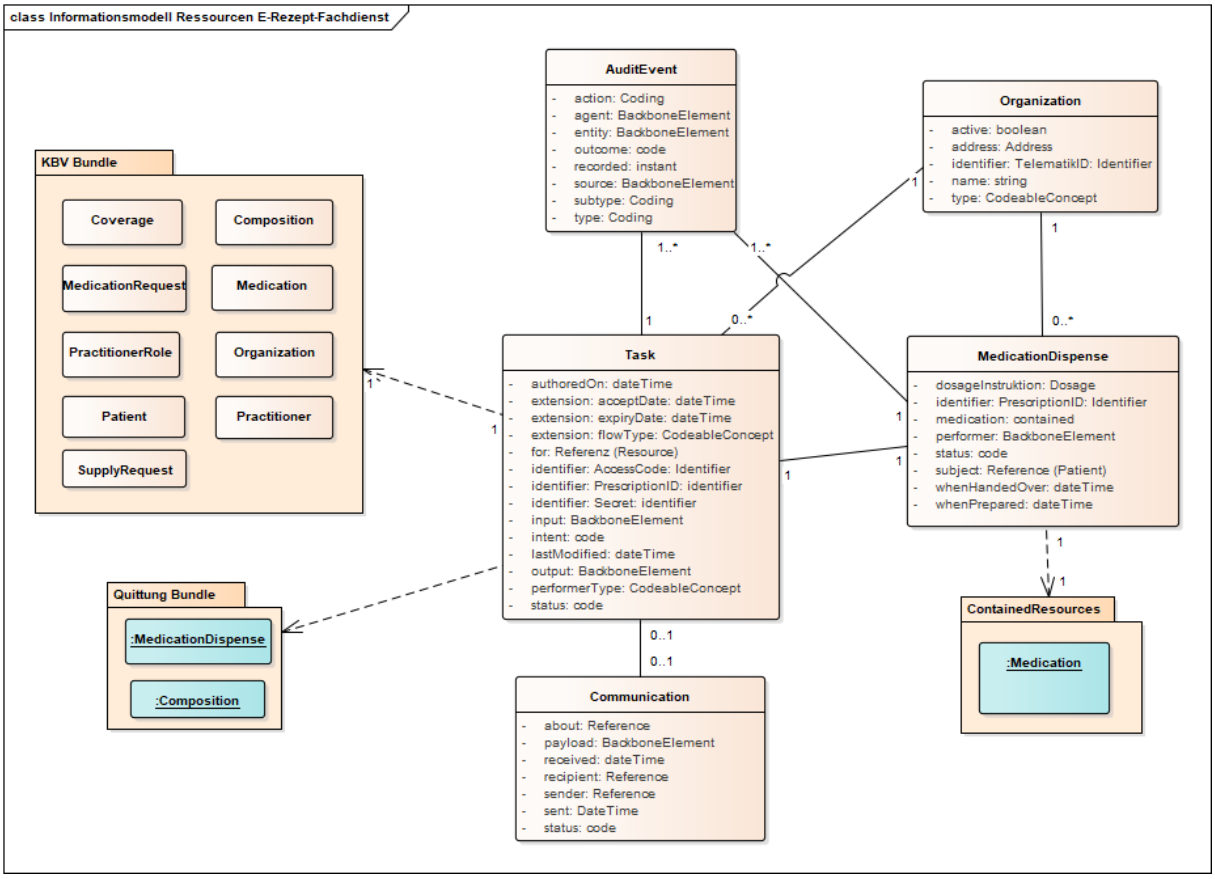


Abbildung 3 Informationsmodell FHIR-Ressourcen E-Rezept-Fachdienst

8 Anhang A – Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
AVS	Apothekenverwaltungssystem
FdV	Frontend des Versicherten
FHIR	Fast Healthcare Interoperable Resources
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
KVNR	Krankenversichertennummer
LEI	Leistungserbringerinstitution
OCSP	Online Certificate Status Protocol
OWASP	Open Web Application Security Project
PVS	Praxisverwaltungssystem
QES	Qualifizierte Elektronische Signatur
SLA	Service Level Agreement
SMC-B	Security Module Card Typ B, Institutionenkarte
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust Service Status List
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 8
Abbildung 2 Systemkontext E-Rezept-Fachdienst 9
Abbildung 3 Informationsmodell FHIR-Ressourcen E-Rezept-Fachdienst 52

8.4 Tabellenverzeichnis

Tabelle 1: TAB_eRPFD_001 Service Discovery 12
Tabelle 2: TAB_eRPFD_002 FQDN 12
Tabelle 3 : TAB_eRPFD_005 Parameter Prüfung Signaturzertifikat IdP 17
Tabelle 4 TAB_eRPFD_004 Versichertenprotokoll 21
Tabelle 5 TAB_eRPFD_007 Löschfristen 23
Tabelle 6 : TAB_eRPFD_006 Parameter Prüfung Signaturzertifikat QES des HBA 39
Tabelle 7 TAB_eRPFD_008 Nachrichtentyp zu Kommunikationsbeziehung 47

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: Glossar der Telematikinfrastruktur

8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[rfc6902]	Definition JSON Patch-Operation https://tools.ietf.org/html/rfc6902
[ETSI_QES]	DEN/ESI-0019122 Electronic Signatures and Infrastructures (ESI); CAdES digital signatures ETSI EN 319 102-1 Procedures for Creation and Validation of AdES Digital Signatures
[RFC5652]	Cryptographic Message Syntax (CMS), RFC 5652 (September 2009) http://tools.ietf.org/html/rfc5652
[CAdES]	ETSI: Electronic Signature Formats, Electronic Signatures and Infrastructures (ESI) – Technical Specification, ETSI TS 101 733 V2.2.1, via http://www.etsi.org
[FHIR-Sig]	FHIR - Signature (JSON Signature rules for FHIR Resources) https://www.hl7.org/fhir/datatypes.html#Signature
[FHIR-TASK]	FHIR Ressource Task https://www.hl7.org/fhir/task.html
[FHIR-ResVers]	FHIR Policy für RessourcenVersionierung https://www.hl7.org/fhir/valueset-versioning-policy.html
[HTTP-STATUS-CODES]	HTTP-StatusCode gemäß RFC-2616 https://tools.ietf.org/html/rfc2616
[JWT]	JSON Web Token (JWT) https://tools.ietf.org/html/rfc7519
[JWS]	JSON Web Signature (JWS) https://tools.ietf.org/html/rfc7515

[DAL_ANDROID]	Asset Owners Guide - Use statements to enable App Linking, declare default app handlers, ... https://developers.google.com/digital-asset-links/v1/getting-started
[RFC7231]	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content https://tools.ietf.org/html/rfc7231
[UL_APPLE]	Allowing Apps and Websites to Link to Your Content https://developer.apple.com/documentation/uikit/inter-process_communication/allowing_apps_and_websites_to_link_to_your_content