

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation E-Rezept-Fachdienst

| | |
|------------------|----------------|
| Version: | 1.6.0 |
| Revision: | 621719 |
| Stand: | 28.04.2023 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | gemSpec_FD_eRp |

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

| Version | Stand | Kap./ Seite | Grund der Änderung, besondere Hinweise | Bearbeitung |
|---------|------------|----------------|--|-------------|
| 1.0.0 | 30.06.2020 | | freigegeben | gematik |
| 1.0.1 | 06.07.2020 | | Aktualisierung Hinweis zu Dispensierinformation | gematik |
| 1.1.0 | 12.11.2020 | | Einarbeitung gemäß Änderungsliste P22.2 / Scope-Themen zu R4.0.1 | gematik |
| 1.1.1 | 13.11.2020 | | Einarbeitung gemäß Änderungsliste P22.4 | gematik |
| 1.2.0 | 19.02.2021 | | Einarbeitung gemäß Änderungsliste P22.5 | gematik |
| 1.3.0 | 07.10.2021 | | Einarbeitung gemäß Änderungslisten E-Rezept_Maintenance_21.1 und _21.2 | gematik |
| 1.4.0 | 09.08.2022 | | Einarbeitung gemäß Änderungslisten E- Rezept_Maintenance_21.3, _21.4, 22.1 und _22.2; Einarbeitung gemF_eRp_WF_LE, gemF_eRp_MVO und gemF_eRp_PKV | gematik |
| 1.5.0 | 07.12.2022 | | Einarbeitung gemäß Änderungsliste E- Rezept_Maintenance_22.3 | gematik |
| 1.6.0 | 28.04.2023 | | Einarbeitung gemäß Änderungsliste E- Rezept_Maintenance_22.5, E- Rezept_Maintenance_22.6 und gemF_eRp_Autorisierung_Apo | gematik |

Inhaltsverzeichnis

| | |
|---|-----------|
| 1 Einordnung des Dokumentes | 6 |
| 1.1 Zielsetzung | 6 |
| 1.2 Zielgruppe | 6 |
| 1.3 Geltungsbereich | 6 |
| 1.4 Abgrenzungen | 6 |
| 1.5 Methodik | 7 |
| 1.5.1 Hinweis auf offene Punkte | 7 |
| 2 Systemüberblick | 8 |
| 3 Systemkontext..... | 10 |
| 3.1 Nachbarsysteme | 10 |
| 3.2 Akteure und Rollen | 10 |
| 4 Zerlegung des Produkttyps | 12 |
| 5 Übergreifende Festlegungen | 13 |
| 5.1 Servicelokalisierung | 13 |
| 5.2 Authentifizierung von Nutzern..... | 14 |
| 5.2.1 Registrierung beim Identity Provider..... | 14 |
| 5.2.2 Claims der Identitätsbestätigung..... | 16 |
| 5.2.3 Verwaltung der Nutzersession..... | 17 |
| 5.3 Routing von Requests..... | 19 |
| 5.4 Fehlercodes | 19 |
| 5.5 Protokollierung..... | 23 |
| 5.6 Löschrufen | 27 |
| 5.7 Berechtigungen und Prozessparameter | 28 |
| 5.8 Sicherheit | 31 |
| 5.8.1 Allgemeine Sicherheitsanforderungen | 31 |
| 5.8.2 Identifikation des Clientsystems | 33 |
| 5.8.3 Vertrauensraum der TI | 34 |
| 5.8.4 Sicherheit der Netzübergänge..... | 35 |
| 5.8.5 Vertrauenswürdige Ausführungsumgebung | 37 |
| 5.8.5.1 Verarbeitungskontext..... | 37 |
| 5.8.5.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld | 39 |
| 5.8.5.3 Konsistenz des Systemzustands, Logging und Monitoring | 41 |
| 5.8.5.4 Client-Verbindungen zum Verarbeitungskontext | 41 |
| 5.9 Management VSDM HMAC-Schlüssel..... | 42 |
| 6 Funktionsmerkmale | 44 |
| 6.1 Ressource Task..... | 45 |

| | |
|--|-----------|
| 6.1.1 HTTP-Operation GET | 45 |
| 6.1.1.1 HTTP-Operation GET - Prüfung VSDM Prüfungsnachweis | 48 |
| 6.1.2 HTTP-Operation POST | 49 |
| 6.1.2.1 POST /Task/\$create | 50 |
| 6.1.2.2 POST /Task/<id>/\$activate | 51 |
| 6.1.2.2.1 POST /Task/<id>/\$activate - Mehrfachverordnung | 56 |
| 6.1.2.3 POST /Task/<id>/\$accept | 58 |
| 6.1.2.4 POST /Task/<id>/\$reject | 59 |
| 6.1.2.5 POST /Task/<id>/\$close | 60 |
| 6.1.2.6 POST /Task/<id>/\$abort | 62 |
| 6.2 Ressource MedicationDispense | 65 |
| 6.2.1 HTTP-Operation GET /MedicationDispense | 65 |
| 6.3 Ressource ChargeItem | 66 |
| 6.3.1 HTTP-Operation DELETE | 66 |
| 6.3.2 HTTP-Operation GET | 67 |
| 6.3.2.1 GET /ChargeItem | 67 |
| 6.3.2.2 GET /ChargeItem/<id> | 68 |
| 6.3.3 HTTP-Operation PATCH | 70 |
| 6.3.3.1 PATCH /ChargeItem/<id> | 70 |
| 6.3.4 HTTP-Operation POST | 71 |
| 6.3.4.1 POST /ChargeItem | 71 |
| 6.3.5 HTTP-Operation PUT | 75 |
| 6.3.5.1 PUT /ChargeItem/<id> | 75 |
| 6.4 Ressource Consent | 77 |
| 6.4.1 HTTP-Operation DELETE | 77 |
| 6.4.2 HTTP-Operation GET | 78 |
| 6.4.3 HTTP-Operation POST | 78 |
| 6.5 Ressource Communication | 79 |
| 6.5.1 HTTP-Operation GET | 79 |
| 6.5.1.1 GET /Communication/ | 80 |
| 6.5.2 HTTP-Operation POST | 80 |
| 6.5.2.1 POST /Communication/ | 80 |
| 6.5.3 HTTP-Operation DELETE | 84 |
| 6.5.3.1 DELETE /Communication/ | 84 |
| 6.6 Ressource AuditEvent | 85 |
| 6.6.1 HTTP-Operation GET /AuditEvent | 85 |
| 6.7 Ressource Device | 86 |
| 6.8 Ressource Subscription | 86 |
| 6.8.1 HTTP-Operation POST | 86 |
| 6.9 Subscription Service | 87 |
| 7 Informationsmodell | 89 |
| 8 Anhang A – Verzeichnisse | 91 |
| 8.1 Abkürzungen | 91 |
| 8.2 Glossar | 92 |
| 8.3 Abbildungsverzeichnis | 92 |

| | |
|--|-----------|
| 8.4 Tabellenverzeichnis | 92 |
| 8.5 Referenzierte Dokumente | 92 |
| 8.5.1 Dokumente der gematik..... | 92 |
| 8.5.2 Weitere Dokumente..... | 93 |

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) festgelegt 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

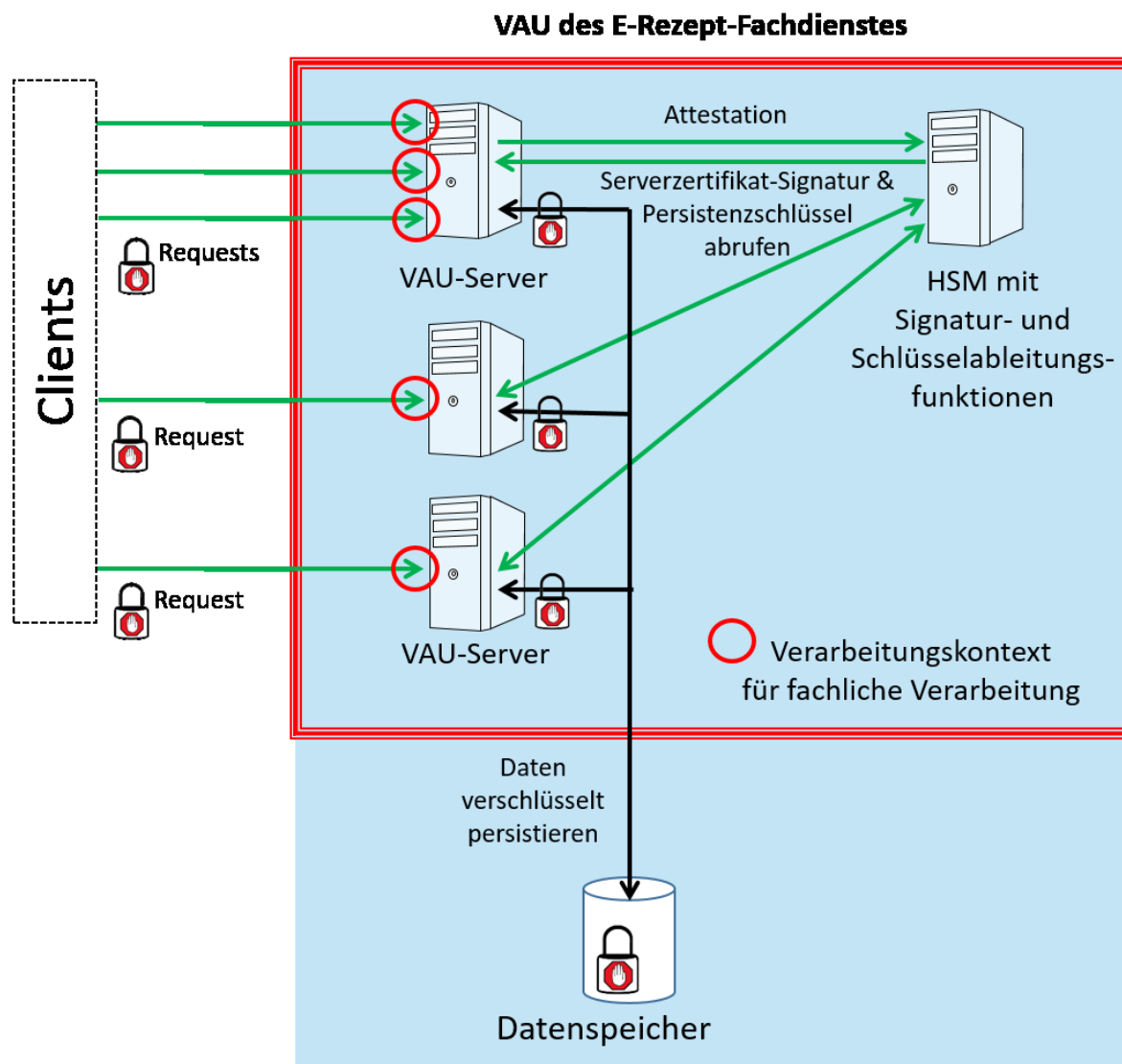
Themen, die noch intern geklärt werden müssen oder eine Entscheidung, sind wie folgt im Dokument gekennzeichnet:

Beispiel für einen offenen Punkt.

2 Systemüberblick

Der E-Rezept-Fachdienst verwaltet E-Rezepte in der Telematikinfrastuktur 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.

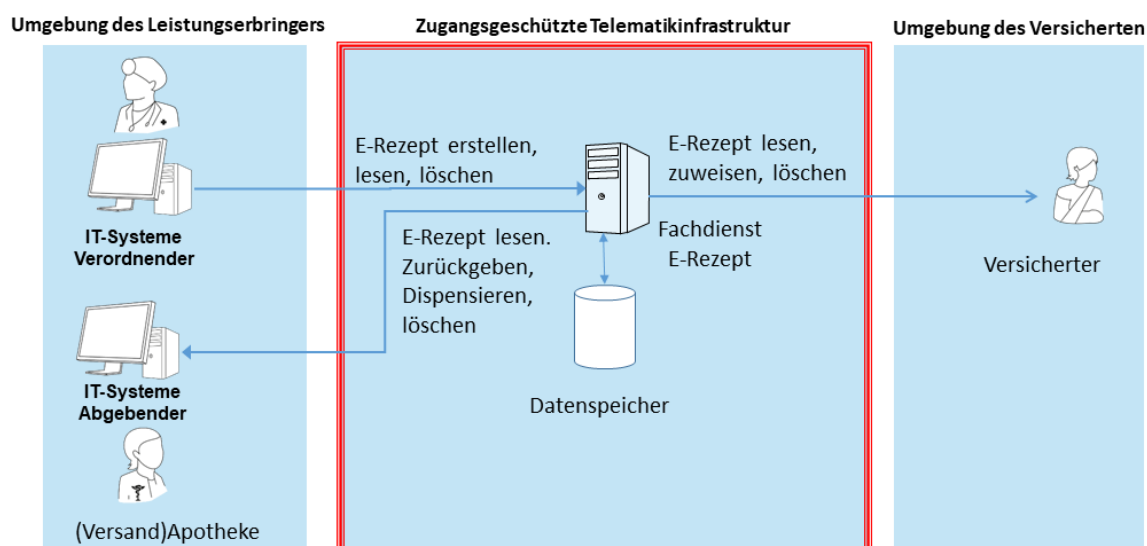


Abbildung 2: Systemkontext E-Rezept-Fachdienst

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, ACCESS_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 (ACCESS_TOKEN) aus, die sie von einem Identitätsprovider, z.B. SmartCard-IDP, beziehen. In diesen ACCESS_TOKEN ist ihre Rollen-OID sowie ihr Identitätskennzeichen Versicherten-ID (10-stelliger unveränderlicher 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_19412-03 - Anbieter E-Rezept-Fachdienst - Schnittstellenadressierung Primärsysteme

Der Anbieter des E-Rezept-Fachdienstes MUSS die den Primärsystemen angebotenen Schnittstellen des E-Rezept-Fachdienstes unter den folgenden URLs zur Verfügung stellen:

- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAU> - Schnittstelle E-Rezept
- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAUCertificate> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.zentral.erp.splitdns.ti-dienste.de/VAUCertificateOCSPResponse> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.zentral.erp.splitdns.ti-dienste.de/ocspf> - Schnittstelle OCSP-Forwarder
- <https://erp.zentral.erp.splitdns.ti-dienste.de/TSL.xml> - Schnittstelle Download TSL-Datei
- <https://erp.zentral.erp.splitdns.ti-dienste.de/TSL.sha2> - Schnittstelle Download Hashwert TSL-Datei
- <https://erp.zentral.erp.splitdns.ti-dienste.de/.well-known> - Schnittstelle well-known locations
- <https://erp.zentral.erp.splitdns.ti-dienste.de/CertList>
- <https://erp.zentral.erp.splitdns.ti-dienste.de/OCSPList>
- <https://erp.zentral.erp.splitdns.ti-dienste.de/random> - Schnittstelle für Zufallsdaten
- <https://subscription.zentral.erp.splitdns.ti-dienste.de> - Schnittstelle Subscription Service

[<=]

A_21782 - Anbieter E-Rezept-Fachdienst - Schnittstellenadressierung Internet

Der Anbieter des E-Rezept-Fachdienstes MUSS die im Internet angebotenen Schnittstellen des E-Rezept-Fachdienstes unter den folgenden URLs zur Verfügung stellen:

- <https://erp.app.ti-dienste.de/VAU> - Schnittstelle E-Rezept
- <https://erp.app.ti-dienste.de/VAUCertificate> - Schnittstelle VAU-Verschlüsselungsidentität

- <https://erp.app.ti-dienste.de/VAUCertificateOCSPResponse> - Schnittstelle VAU-Verschlüsselungsidentität
- <https://erp.app.ti-dienste.de/ocspf> - Schnittstelle OCSP-Forwarder
- <https://erp.app.ti-dienste.de/TSL.xml> - Schnittstelle Download TSL-Datei
- <https://erp.app.ti-dienste.de/TSL.sha2> - Schnittstelle Download Hashwert TSL-Datei
- <https://erp.app.ti-dienste.de/.well-known> - Schnittstelle well-known locations
- <https://erp.app.ti-dienste.de/CertList>
- <https://erp.app.ti-dienste.de/OCSPList>
- <https://erp.app.ti-dienste.de/random> - Schnittstelle für Zufallsdaten

[<=]

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 Statement gemäß [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 Identity Provider der Telematikinfrastruktur ACCESS_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 (ACCESS_TOKEN) festlegen. Die Umsetzung des IdentityManagements über Identity Provider startet mit einem einzelnen IDP (Smartcard-IDP), später werden weitere Identity Provider bei den verschiedenen identitätsbestätigenden Stellen realisiert. Verwaltet ein solcher IDP Identitäten von Nutzern der Telematikinfrastruktur und gilt als vertrauenswürdig für die Umsetzung von Use Cases unter Nutzung der Schnittstellen des E-Rezept-Fachdienstes, obliegt es dem E-Rezept-Fachdienst, sich bei diesem IDP als Relying Party zu registrieren.

A_19985-01 - 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 Identity Provider (IDP) der Telematikinfrastruktur als

Relying Party registrieren und die Bereitstellung der folgenden Claims in für Nutzer ausgestellte ACCESS_TOKEN mit dem IDP vereinbaren:

- professionOID
- given_name
- family_name
- organizationName
- idNummer
- acr
- aud

damit der E-Rezept-Fachdienst die Fachlogik der Autorisierung und Protokollierung auf diesen Attributen umsetzen kann. [\leq]

A_20706 - Anbieter E-Rezept-Fachdienst - Claims für ID_TOKEN für FdV

Der Anbieter des E-Rezept-Fachdienstes MUSS bei der Registrierung als Relying Party im IDP die Bereitstellung der folgenden Claims in für Nutzer ausgestellte ID_TOKEN mit dem IDP vereinbaren:

- professionOID
- given_name
- family_name
- organizationName
- idNummer
- acr

damit ein E-Rezept-Client diese Informationen bei Bedarf auswerten kann. [\leq]

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 ACCESS_TOKEN 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. [\leq]

A_20710 - Anbieter E-Rezept-Fachdienst - E-Rezept-Lebensdauer ACCESS_TOKEN

Der Anbieter des E-Rezept-Fachdienstes MUSS bei der Registrierung als Relying Party im IDP eine Lebensdauer von ausgestellten ACCESS_TOKEN durch den IDP für die Berechnung des Werts "`tokenTimeout`" von 300 Sekunden festlegen. [\leq]

A_19993 - E-Rezept-Fachdienst - Prüfung eingehender ACCESS_TOKEN

Der E-Rezept-Fachdienst MUSS jedes mit einem eingehenden HTTP-Request übergebene ACCESS_TOKEN gemäß der Festlegungen in [gemSpec_IDP_FD#Kapitel 6 ACCESS_TOKEN] prüfen und Fehler bzw. ungültige Token gemäß dieser Festlegungen und dem HTTP-Status-Code 401 abweisen. [\leq]

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 ACCESS_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 ACCESS_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='invalidACCESS_TOKEN'" abweisen, die ein unsigniertes oder ungültiges ACCESS_TOKEN im HTTP-Request-Header "Authorization" bereitstellen, 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 Identity Provider, 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 der Attribute "given_name", "family_name" und "organizationName" 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 "idNummer" im übergebenen IDP-Token im HTTP-Header "Authorization" feststellen und für die Protokollierung des Zugriffs auf personenbezogene medizinische Daten je Operationsaufruf verwenden. [≤]

A_19439-01 - 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 "gematik-ehealth-loa-high" mit dem HTTP-Status-Code 401 ablehnen. [<=]

5.2.3 Verwaltung der Nutzersession

Der Identity Provider übernimmt für den E-Rezept-Fachdienst als Relying Party die Verwaltung von Nutzersessions und stellt dem Client während der Gültigkeit der Nutzersession ACCESS_TOKEN für den Zugriff auf den E-Rezept-Fachdienst aus. Der E-Rezept-Fachdienst prüft diese ACCESS_TOKEN auf Gültigkeit gemäß der Festlegungen in [gemSpec_IDP_FD].

A_19992 - E-Rezept-Fachdienst - Blocklisting zu häufig verwendeter ACCESS_TOKEN

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

A_20158-02 - E-Rezept-Fachdienst - Prüfung Signaturzertifikat IDP

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

Tabelle 1: TAB_eRPFD_005 Parameter Prüfung Signaturzertifikat IDP

| Parameter | |
|--------------------------|--|
| Zertifikat | Signaturzertifikat des IDP PUK_IDP_SIG (wird im Discovery Document referenziert, siehe [gemSpec_IDP_Dienst#Kapitel 4]) |
| 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 ACCESS_TOKEN von einem vertrauenswürdigen IDP akzeptiert werden. [<=]

Das Signaturzertifikat C.FD.SIG des IDP kann über das Discovery Document des IDP unter <https://<FQDN des IDP>/auth/realms/idp/.well-known/openid-configuration> automatisch bezogen werden. Das Discovery Document ist als [JWT] aufgebaut und stellt im Claim "uri_puk_idp_sig" den Downloadpunkt auf ein JWK bereit. Darin ist das Signaturzertifikat über den key "kid"="puk_idp_sig" zu lokalisieren und liegt im Parameter "x5c" in Base64-DER-Codierung vor.

A_20974-01 - E-Rezept-Fachdienst - Prüfungsintervall Signaturzertifikat E-Rezept-Fachdienst

Der E-Rezept-Fachdienst MUSS mindestens einmal stündlich sein Signaturzertifikat C.FD.OSIG auf Gültigkeit prüfen. [<=]

A_20765-02 - E-Rezept-Fachdienst - Prüfung Signaturzertifikat E-Rezept-Fachdienst

Der E-Rezept-Fachdienst MUSS sein Signaturzertifikat gemäß [gemSpec_PKI#TUC_PKI_018] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 2: TAB_eRPFD_010 Parameter Prüfung Signaturzertifikat

| Parameter | |
|--------------------------|--|
| Zertifikat | Signaturzertifikat des E-Rezept-Fachdienstes C.FD.OSIG |
| PolicyList | oid_fd_osig |
| intendedKeyUsage | nonRepudiation |
| intendedExtendedKeyUsage | (leer) |
| OCSP-Graceperiod | 24 Stunden |
| Offline-Modus | nein |
| Prüfmodus | OCSP |

Der E-Rezept-Fachdienst MUSS das Signaturzertifikat anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig] befinden und eingehende HTTP-Requests, welche eine Signatur durch den E-Rezept-Fachdienst erfordern, andernfalls mit dem HTTP-Status-Code 503 ablehnen, damit sichergestellt wird, dass Signaturen mit einem gültigen Signaturzertifikat erstellt werden. [<=]

A_22221 - Anbieter E-Rezept-Fachdienst - Erneuerung Signaturzertifikat

Der Anbieter des E-Rezept-Fachdienstes MUSS das Signaturzertifikat des E-Rezept-Fachdienstes C.FD.OSIG jährlich im Januar erneuern. [<=]

5.3 Routing von Requests

Die Clients verwenden Http-Header im äußeren Http-Request, um dem E-Rezept-Fachdienst ein internes Routing zu ermöglichen.

A_21571 - E-Rezept-Fachdienst - Routing-Informationen X-erp-resource

Der Eingangspunkt des E-Rezept-Fachdienstes KANN eine Routingentscheidung zu einem Ressourcen-spezifischen Verarbeitungskontext anhand des Headers "X-erp-resource" mit Wertebereich gemäß der Ressourcennamen (bspw. Communication, Task) im äußeren http-Request treffen. [≤]

A_21572 - E-Rezept-Fachdienst - Routing-Informationen X-erp-user

Der Eingangspunkt des E-Rezept-Fachdienstes KANN eine Routingentscheidung zu einem nutzergruppenspezifischen Verarbeitungskontext anhand des Headers "X-erp-user" mit Wertebereich [l, v, k, s] im äußeren http-Request treffen. [≤]

Die Werte sollen von Clients des E-Rezepts wie folgt verwendet werden:

- l (kleines L) - Leistungserbringer
- v - Versicherte
- k - Kostenträger (aktuell nicht verwendet, da nicht zugriffsberechtigt)
- s - Sonstige (aktuell nicht verwendet)

5.4 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-Status-Codes [HTTP-STATUS-CODES] mitgeteilt. Die folgende Tabelle listet die vom E-Rezept-Fachdienst genutzten Http-Status-Codes auf.

A_19514-03 - E-Rezept-Fachdienst - Http-Status-Codes

Der E-Rezept-Fachdienst MUSS beim Aufruf einer Operation im Http-Response-Header einen HTTP-Status-Codes gemäß [RFC7231] zurückgeben. [≤]

Tabelle 3: 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 GET /notifications/opt-in GET /notifications/opt-out GET, etc für alle übrigen Operationen | Die Operation wurde erfolgreich bearbeitet. In der Rückgabe sind die erzeugten bzw. gelesenen Daten enthalten. |

| HTTP-Status-Code | Bedeutung | in welchen Operationen als Statuscode möglich | Bedingung |
|------------------|---|---|--|
| 201 | Neues Objekt wurde erfolgreich angelegt, in der Rückgabe ist das Objekt enthalten | POST /Task/\$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 DELETE /Communication/<id> | 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 GET /notifications/opt-in GET, POST, etc für alle übrigen Operationen | 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" |

| HTTP-Status-Code | Bedeutung | in welchen Operationen als Statuscode möglich | Bedingung |
|------------------|---|---|---|
| 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 POST /Task/<id>/\$abort POST /Communication | Gemäß Rollenprüfung in jedem Operationsaufruf sind nur bestimmte Operationen je aufrufendem Nutzer zulässig. |
| 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> GET /notifications/opt-out | 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> |

| HTTP-Status-Code | Bedeutung | in welchen Operationen als Statuscode möglich | Bedingung |
|------------------|---|--|---|
| 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 | Der Task des E-Rezepts hat einen Status, für den der gewünschte Zugriff unzulässig ist. Bspw.: 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 |

| HTTP-Status-Code | Bedeutung | in welchen Operationen als Statuscode möglich | Bedingung |
|------------------|-----------------------|--|--|
| 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 GET, POST, etc für alle übrigen Operationen | In allen Operationen, die aufgrund eines internen Fehlers nicht bearbeitet werden können. Die Rückgabe liefert keine weiteren Informationen. |

A_22103 - E-Rezept-Fachdienst - Fehlerdetails in OperationOutcome

Der E-Rezept-Fachdienst MUSS im Fehlerfall (http-Statuscodes ≥ 400) Hinweise zur Fehlerursache

- im der inneren http-Response-Body als FHIR-Ressource OperationOutcome
- falls keine innere VAU-Response existiert, in einem "äußeren" http-Response-Body in einer JSON-Struktur mit "x-request-id", (http-) "status", "error"-Text, "message"-Details

an den Client zurückgeben, ohne Implementierungsdetails (z.B. kein Stacktrace) preiszugeben und dabei sicherstellen, dass personenbezogene oder medizinische Daten, falls für die qualifizierte Fehlerbeschreibung notwendig, ausschließlich in der VAU-verschlüsselten inneren http-Response übertragen werden. [\leq]

Die Fehlermeldung beinhaltet bei fachlichen Fehlern einen VAU-verschlüsselten inneren http-Response. In diesem inneren Response werden ggf. ausschliesslich personenbezogene oder medizinische Daten an den aufrufenden Client übermittelt, welche bereits im VAU-verschlüsselten inneren http-Request, welcher zum Fehler führte, enthalten waren. Das kann bspw. bei Fehlern bei der Prüfung der FHIR Konformität von Datensätzen auftreten.

Treten Fehler beim VAU-Transport (bspw. innerer http-Request kann nicht entschlüsselt werden) auf, beinhaltet die Fehlermeldung keinen inneren http-Response.

5.5 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, personenbezieharen 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_19284-04 - 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/<id> | | |
| - | Versicherter, Vertreter | Patient/Versicherter/Vertreter hat das E-Rezept heruntergeladen |
| | Apotheker | Apotheke hat die E-Rezept-Quittung heruntergeladen |
| http GET /Task | | |

| Operation | Rolle des zugreifenden Nutzers | Beschreibung (ggfs. als Vorschlag für einen lesbaren Protokolleintrag in einfacher Sprache) |
|---|--------------------------------------|---|
| | Apotheker | im Erfolgsfall: Apotheke hat mit Ihrer eGK die Liste der offenen E-Rezepte abgerufen. im Fehlerfall: Apotheke konnte aufgrund eines Fehlerfalls nicht die Liste der offenen E-Rezepte mit Ihrer eGK abgerufen. |
| 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/<id> bzw. Zugriff via Suchparameter GET /MedicationDispense?<parameter>=... | | |
| | Versicherter, Vertreter | Patient/Versicherter hat Medikament-Informationen heruntergeladen |
| http DELETE /ChargeItem/<id> | Versicherter | Versicherter hat Abrechnungsinformation gelöscht |

| Operation | Rolle des zugreifenden Nutzers | Beschreibung (ggfs. als Vorschlag für einen lesbaren Protokolleintrag in einfacher Sprache) |
|---|--------------------------------|---|
| http GET /ChargeItem/<id> | Versicherter | Versicherter hat Abrechnungsinformation gelesen |
| | Apotheke | Apotheke hat Abrechnungsinformation gelesen |
| http POST /ChargeItem | Apotheke | Apotheke hat Abrechnungsinformation bereitgestellt |
| http PATCH /ChargeItem/<id> | Versicherter | Versicherter hat Markierung zu Abrechnungsinformation gespeichert |
| http PUT /ChargeItem/<id> | Apotheke | Apotheke hat PKV-Abgabedatensatz gespeichert |
| http POST /Consent | Versicherter | Versicherter hat Einwilligung erteilt |
| http DELETE /Consent | Versicherter | Versicherter hat Einwilligung widerrufen |
| 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 Communication | | Veraltete Nachrichten vom Fachdienst automatisch gelöscht |
| Ressource ChargeItem | | Veraltete Abrechnungsinformation vom E-Rezept-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. [<=]

A_22217 - E-Rezept-Fachdienst - Protokollierung - keine Angabe zu organizationName

Der E-Rezept-Fachdienst MUSS, wenn im ACCESS_TOKEN die Angabe zur "organizationName" mit NULL gefüllt ist, in der Protokollierung als agentname "unbekannt" verwenden. [<=]

5.6 Löschrufen

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_19252-02 - E-Rezept-Fachdienst - Löschrufen abgelaufener Rezepte

Der E-Rezept-Fachdienst MUSS einen Task nach Ablauf der Löschrufen gemäß der folgenden Festlegung in TAB_eRPFD_007 automatisch löschen und das Löschrufen in einem AuditEvent für den Versicherten nachvollziehbar protokollieren, damit nicht mehr benötigte Informationen gelöscht sind.

Tabelle 5: TAB_eRPFD_007 Löschrufen Task

| Task.status nach Statuswechsel | Löschrufen |
|--------------------------------|---------------------------------------|
| draft | 5 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 |

[<=]

A_19254 - E-Rezept-Fachdienst - Löschrufen referenzierter Bundles

Der E-Rezept-Fachdienst MUSS bei jedem Löschrufen 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 Löschrufen 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_22109 - E-Rezept-Fachdienst – Löschfrist ChargeItem

Der E-Rezept-Fachdienst MUSS ein ChargeItem innerhalb eines Monats nach Ablauf von 10 Jahren nach dem Erstellen der Ressource automatisch löschen und das Löschen in einem AuditEvent für den Versicherten nachvollziehbar protokollieren, damit nicht mehr benötigte Informationen gelöscht sind.

Der E-Rezept-Fachdienst MUSS bei jedem Löschen eines ChargeItems alle referenzierten Bundles (E-Rezept-Bundle, Quittungs-Bundle, PKV-Abgabedatensatz) ebenfalls löschen, damit die Informationen rund um ein gelöscht ChargeItem ebenfalls entfernt werden. [<=]

A_19253-01 - 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` ,
- mit einer Referenz auf einen Task in `Communication.basedOn` gemäß der Löschfrist in TAB_eRPFD_007 beim Löschen des Tasks ,
- mit einer Referenz auf einen ChargeItem in `Communication.basedOn` nach 100 Tagen ab ihrem Sendedatum `Communication.sent`

automatisch löschen, damit nicht mehr relevante Nachrichten ebenfalls gelöscht werden. [<=]

A_19256-01 - E-Rezept-Fachdienst - Löschfrist veraltete Protokolleinträge

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

5.7 Berechtigungen und Prozessparameter**A_21267 - Prozessparameter - Berechtigungen für Nutzer**

Der E-Rezept-Fachdienst MUSS die folgenden Zugriffserlaubnisse in Abhängigkeit der Rolle bzw. KVN/TelematikID des zugreifenden Nutzers, des Task.status, Task.flowType und Kenntnis um AccessCode bzw. Secret gewähren und andernfalls jeden Zugriff mit dem http-Status 403 als unautorisiert abweisen.

Tabelle 6: Zugriffserlaubnisse

| Operation | Rolle des zugreifenden Nutzers | Bedingung (Task.status, Task.flowType, AccesCode bzw. Secret) |
|---|--------------------------------|---|
| | | ggfs. Beschränkung der ausgegebenen Daten |
| http GET /Task bzw. http GET /Task/<id> | | |
| | | keine sonstigen Bedingungen |

| Operation | Rolle des zugreifenden Nutzers | Bedingung (Task.status, Task.flowType, AccessCode bzw. Secret) |
|-----------------|--|---|
| | | ggfs. Beschränkung der ausgegebenen Daten |
| | oid_versicherter (Task.for = KVNR in AccessToken) | Flowtype 160: alle Daten werden zurückgegeben Flowtype 169: AccessCode wird in Task.identifizier <u>nicht</u> herausgegeben |
| | oid_versicherter (Task.for != KVNR in AccessToken) | Flowtype 160: AccessCode in URL-Parameter "ac" oder http-Header "X-AccessCode" muss mit Task.identifizier für AccessCode übereinstimmen Flowtype 169: Versicherte kennen den AccessCode nicht |
| | | Flowtype 160: alle Daten werden zurückgegeben Flowtype 169: Task.for != KVNR in AccessToken werden keine Daten zurückgegeben, da AccessCode nicht prüfbar |
| | oid_oeffentliche_apotheke, oid_krankenhausapotheke | Secret in URL-Parameter "secret" muss mit Task.identifizier für Secret übereinstimmen, Task.status = completed |
| | | alle Daten des direkt adressierten Tasks werden zurückgegeben |
| http POST /Task | | |
| \$create | oid_praxis_arzt oid_zahnarztpraxis oid_praxis_psychotherapeut oid_krankenhaus | keine sonstigen Bedingungen |
| | | Flowtype 160: Rezept-ID wird generiert mit 160-beginnend Flowtype 169: Rezept-ID wird generiert mit 169-beginnend |
| \$activate | oid_praxis_arzt oid_zahnarztpraxis oid_praxis_psychotherapeut oid_krankenhaus | Präfix 16x der PrescriptionID im Identifizier des Verordnungsdatensatzes muss mit Flowtype des Task übereinstimmen QES des Verordnungsdatensatzes muss von Leistungserbringer mit einer der Rollen erstellt sein: oid_arzt, oid_zahnarzt |
| \$accept | oid_oeffentliche_apotheke, oid_krankenhausapotheke | AccessCode in URL-Parameter "ac" oder http-Header "X-AccessCode" muss mit Task.identifizier für AccessCode übereinstimmen |

| Operation | Rolle des zugreifenden Nutzers | Bedingung (Task.status, Task.flowType, AccessCode bzw. Secret) |
|------------------------------|--|---|
| | | ggfs. Beschränkung der ausgegebenen Daten |
| | | Secret als zusätzlichen Task.identifizier generieren |
| \$reject | oid_oeffentliche_apotheke, oid_krankenhausapotheke | Secret in URL-Parameter "secret" muss mit Task.identifizier für Secret übereinstimmen |
| | | Secret als zusätzlicher Task.identifizier muss gelöscht werden |
| \$close | oid_oeffentliche_apotheke, oid_krankenhausapotheke | Secret in URL-Parameter "secret" muss mit Task.identifizier für Secret übereinstimmen |
| \$abort | oid_versicherter (Task.for = KVNR in AccessToken) | Flowtype 160: Task.status ungleich "in-progress" Flowtype 169: nicht zulässig, wenn Task.status ungleich "completed" |
| | oid_versicherter (Task.for != KVNR in AccessToken) | Flowtype 160: AccessCode in URL-Parameter "ac" oder http-Header "X- AccessCode" muss mit Task.identifizier für AccessCode übereinstimmen Flowtype 169: nicht zulässig, Versicherte dürfen diese Operation nicht aufrufen |
| | oid_praxis_arzt oid_zahnarztpraxis oid_praxis_psychotherapeut oid_krankenhaus | AccessCode in URL-Parameter "ac" oder http-Header "X-AccessCode" muss mit Task.identifizier für AccessCode übereinstimmen Task.status ungleich "in-progress" |
| | oid_oeffentliche_apotheke, oid_krankenhausapotheke | Secret in URL-Parameter "secret" muss mit Task.identifizier für Secret übereinstimmen |
| http GET /MedicationDispense | | |
| | oid_versicherter | (MedicationDispense.identifizier = KVNR in AccessToken) |
| | | alle Daten werden zurückgegeben |
| http GET /Bundle/<id> | | |
| | | |

| Operation | Rolle des zugreifenden Nutzers | Bedingung (Task.status, Task.flowType, AccesCode bzw. Secret) |
|----------------|---|--|
| | | ggfs. Beschränkung der ausgegebenen Daten |
| | | |
| /Communication | | |
| http GET | oid_versicherter oid_oeffentliche_apotheke, oid_krankenhausapotheke | keine besonderen Zugriffsbedingungen |
| | | Filterung auf Communication.recipient = KVNR/TelematikID aus AccessToken |
| /Communication | | |
| http POST | oid_versicherter oid_oeffentliche_apotheke, oid_krankenhausapotheke | keine besonderen Zugriffsbedingungen |
| | | KVNR/TelematikID aus AccessToken wird in Communication.sender übernommen |
| /AuditEvent | | |
| http GET | oid_versicherter | keine besonderen Zugriffsbedingungen |
| | | Filterung auf AuditEvent.entity.name = KVNR aus AccessToken |

[<=]

5.8 Sicherheit

5.8.1 Allgemeine Sicherheitsanforderungen

A_19260 - E-Rezept-Fachdienst – Ausschluss unbekannter FdV-Versionennummern von der Kommunikation

Der E-Rezept-Fachdienst MUSS an der Schnittstelle zum Internet die Produktidentifikation (Produktbezeichnung, Produktversion) des Clients erkennen und nicht zugelassene Produkte oder bestimmte Produktversionen von der Kommunikation mit dem E-Rezept-Fachdienst ausschließen zu können. Der E-Rezept-Fachdienst MUSS in diesen Fällen eine entsprechende Fehlermeldung mit dem http-StatusCode 403 an den aufrufenden Client geben. [<=]

Hinweis: Der Ausschluss soll über ein Whitelisting gültiger Produktidentifikationen erfolgen.

A_19261-01 - E-Rezept-Fachdienst – Ausschluss von Client-Versionen

Der Anbieter des E-Rezept-Fachdienstes MUSS ausschließlich auf Anweisung der gematik Clients mit einer bestimmten Produktidentifikation für die Kommunikation mit dem E-Rezept-Fachdienst zulassen. [≤]

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. [≤]

Der E-Rezept-Fachdienst soll sich vor Anfragen, die nicht auf ein übliches Verhalten von Leistungserbringerinstitutionen und Versicherten während des Verordnungsprozesses schließen lassen, schützen. Diesen Anomalien wird mit einer Drosselung der Bearbeitungsgeschwindigkeit begegnet, um bspw. Brute-Force-Attacken auf das Erraten von AccessCodes für den Zugriff auf E-Rezept-Daten unattraktiv zu machen.

A_20703 - E-Rezept-Fachdienst - Drosselung Brute-Force-Anfragen

Der E-Rezept-Fachdienst MUSS jede Antwort auf einen Funktionsaufruf, der einen AccessCode oder Secret enthält

um den konfigurierbaren http-Response-Header "Warning" (default "999 Throttling active") ergänzt und um ein konfigurierbares Zeitintervall (default: 500 Millisekunden) verzögert zurückschicken, sofern der erwartete AccessCode bzw Secret nicht mit dem übergebenen AccessCode bzw. Secret übereinstimmt, um BruteForce-Angriffe durch einen hohen Zeitaufwand unattraktiv zu machen. [≤]

A_20704 - E-Rezept-Fachdienst - Drosselung Rezeptfälschungen

Der E-Rezept-Fachdienst MUSS jede Antwort auf den Funktionsaufruf zum Aktivieren eines Tasks mittels Übergabe des QES-signierten Datensatzes um den konfigurierbaren http-Response-Header "Warning" (default "999 Throttling active") ergänzt und um ein konfigurierbares Zeitintervall (default: 500 Millisekunden) verzögert zurückschicken, sofern die QES in der Prüfung während der Operation POST /Task/<id>/\$activate als ungültig erkannt wird, um Angriffe durch Rezeptfälschungen durch einen hohen Zeitaufwand unattraktiv zu machen. [≤]

A_20705 - Anbieter E-Rezept-Fachdienst - Konfiguration und Deaktivierung Drosselung

Der Anbieter des E-Rezept-Fachdienstes MUSS die Funktion der Drosselung sowie die Konfiguration auf Weisung der gematik aktivieren oder deaktivieren bzw. die Konfigurationsparameter anpassen, um die Wirksamkeit des Mechanismus im Feld bei Bedarf zu verbessern. [≤]

Die gematik stellt mit der Prüfkarte eGK eine elektronische Identität zur Überprüfung verschiedener Anwendungsfälle in der TI und wird vorrangig von Dienstleistern vor Ort (DVOs) genutzt. Die Prüfkarte eGK ist nicht für die Nutzung im regulären Versorgungsalltag von Leistungserbringern oder Versicherten vorgesehen. Die folgenden Anforderungen verhindern eine Vermischung von Prüfkartenaktivitäten mittels der Prüfkarte eGK und den Anwendungsfällen von Versicherten einer Krankenkasse.

A_20751 - E-Rezept-Fachdienst - Erkennen der Prüfidentität

Der E-Rezept-Fachdienst MUSS eine eGK-Prüfkartenidentität anhand der Bildungsregel in Card-G2-A_3820 (X0000nnnnP, mit nnnn aus der Menge {0001 .. 5000} und P = Prüfziffer) für die KVNR der Prüfkarte eGK erkennen. [≤]

A_20752 - E-Rezept-Fachdienst - Ausschluss Vertreterkommunikation von bzw. an Prüf-Identität

Der E-Rezept-Fachdienst MUSS das Einstellen einer Communication-Ressource mit dem http-Status-Code 400 ablehnen wenn diese in den Absender-und Empfänger-Informationen eine Kombination von KVNR der Prüfkarte eGK und KVNR von Versicherten enthält. [≤]

A_20753 - E-Rezept-Fachdienst - Ausschluss Vertreterzugriff auf bzw. mittels Prüf-Identität

Der E-Rezept-Fachdienst MUSS jeden Zugriff auf E-Rezepte mittels AccessCode (Vertreterzugriff) mit dem http-Status-Code 400 ablehnen, wenn sich aus dem Zugriff eine Kombination aus KVNR der Prüfkarte eGK und KVNR von Versicherten ergibt, d.h. Versicherte dürfen nicht auf Prüfrezeppte und mit Prüfkarte eGK darf nicht auf Rezepte von Versicherten zugegriffen werden. [<=]

5.8.2 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_20013-01 - 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 403 beantworten, damit in der Betriebsüberwachung des E-Rezept-Fachdienstes die Nutzung unzulässiger Frontends erkannt werden kann. [<=]

Beim Verbindungsaufbau zwischen Client und E-Rezept-Fachdienst an Schnittstellen zum Internet wird ein API-KEY übermittelt, welcher durch den E-Rezept-Fachdienst an der Web-Schnittstelle auf Zulässigkeit geprüft wird.

API-KEYs werden durch die gematik in ihrer Rolle als Gesamtverantwortlicher der TI erzeugt. Sie sind Zufallswerte mit hoher Entropie und produkt-spezifisch. Die Zulässigkeit von API-KEYs wird von der gematik über organisatorische Prozesse dem Betreiber des E-Rezept-Fachdienstes und den Herstellern von Clientsystemen mitgeteilt. Die Übermittlung muss vertraulichkeits- und integritätsgeschützt erfolgen. Die gematik muss bei der Übergabe des API-KEY sicherstellen, dass nur ein berechtigter Client-Hersteller einen für ihn erzeugten API-KEY erhält.

Die Veranlassung zur Sperrung eines API-KEYs erfolgt durch die gematik, bspw. wenn der Verdacht besteht, dass der API-KEY kompromittiert wurde (bspw. missbräuchliche Nutzung des API-KEYs durch Dritte). Hinweis: Betriebliche Sperrprozesse werden über user-agent gesteuert, da ggf der API-KEY Mechanismus gegen einen alternativen Mechanismus getauscht wird, welcher zusätzlich die Authentizität des Clients absichert.

A_21551 - E-Rezept-Fachdienst - Prozess zur Verwaltung von API-KEYs

Der Anbieter des E-Rezept-Fachdienstes MUSS organisatorische Prozesse mit der gematik zur Verwaltung von API-KEYs für die Schnittstellen des E-Rezept-Fachdienstes zum Internet unterstützen. [<=]

Mittels dieser Prozesse werden zulässige API-KEYs übermittelt und API-KEYs als ungültig erklärt.

A_21552 - E-Rezept-Fachdienst - Zuordnung Abfrageursprung Client

Der E-Rezept-Fachdienst MUSS jeden Zugriff über eine Schnittstelle im Internet mittels dem HTTP-Header "X-api-key" gegen die Liste zulässiger API-KEYs prüfen. Anfragen ohne HTTP-Header "X-api-key" oder einem nicht gültigen API-KEY MÜSSEN als nicht authentisiert (HTTP-Statuscode 401) abgelehnt werden. [≤=]

5.8.3 Vertrauensraum der TI

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_20024-01 - E-Rezept-Fachdienst - Bereitstellung OCSP-Forwarder

Der E-Rezept-Fachdienst MUSS folgende Vorgaben umsetzen:

1. Er MUSS unter der Adresse <FQDN>/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. **[<=]**

Als Alternative zur TSL-Verarbeitung stellt der E-Rezept-Fachdienst eine kurze Zertifikatskette in einer JSON-Struktur bereit, die sich in Plattformen mobiler Betriebssysteme leichter verarbeiten lässt. Diese Zertifikatskette muss regelmäßig aktualisiert und über einen Downloadpunkt für Primärsysteme und das E-Rezept-FdV zur Verfügung gestellt werden. Die normativen Festlegungen finden sich in der Spezifikation [gemSpec_Krypt] in Abschnitt 7.2.2 "Client-seitige Prüfung der E-Rezept-VAU-Identität".

5.8.4 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-Responser 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) initiiertes 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. [<=]

5.8.5 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. [<=]

5.8.5.1 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.ENC (oid_fd_enc) 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_19726-01 - 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) sicherstellen, 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.

[<=]

Dies kann durch Betrieb der Funktionalitäten auf jeweils getrennten physischen Servern oder durch Mechanismen des vorgelagerten Load Balancing realisiert werden.

5.8.5.2 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_19711-01 - 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:

- Privater Schlüssel (PrK.FD.ENC) des Schlüsselpaars zur Authentisierung des Verarbeitungskontextes gegenüber dem E-Rezept-Frontend des Versicherten und Primärsystemen (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 authentifizierte Verbindung zur Kryptographieschnittstelle 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.[<=]

5.8.5.3 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.[<=]

5.8.5.4 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.[<=]

5.9 Management VSDM HMAC-Schlüssel

A_23501 - E-Rezept-Fachdienst – VSDM HMAC-Schlüssel - Verarbeitung in VAU

Der E-Rezept-Fachdienst MUSS die Nutzung eines HMAC-Schlüssel im Klartext in einer Vertrauenswürdigen Ausführungsumgebung umsetzen.[<=]

Der Anbieter des E-Rezept-Fachdienstes erhält das Exportpaket eines Betreiber eines Fachdienstes VSDM über das TI-ITSM-System. Zur Struktur des Export-Paket siehe A_23466-*,

A_23482 - Anbieter E-Rezept-Fachdienst - Bereitstellung Exportpaket VSDM HMAC-Schlüssel

Der Anbieter des E-Rezept-Fachdienstes MUSS Exportpakete von Fachdienstbetreiber VSDM ausschließlich aus dem TI-ITSM-System entgegen nehmen.[<=]

Der Anbieter des E-Rezept-Fachdienstes darf das Exportpaket erst in die VAU einbringen, nachdem "empty_string_hmac" und die Betreiberkennung aus dem Export-Paket mit den Informationen, die die gematik vom Betreiber des Fachdienstes VSDM erhalten hat, abgeglichen wurden.

A_23483 - Anbieter E-Rezept-Fachdienst - Prüfung Exportpaket VSDM HMAC-Schlüssel

Der Anbieter des E-Rezept-Fachdienstes MUSS ausschließlich Exportpakete aus dem TI-ITSM-System in die VAU einbringen, die von der gematik bestätigt wurden.[<=]

A_23492 - E-Rezept-Fachdienst - VSDM HMAC-Schlüssel - Exportpaket einbringen

Der E-Rezept-Fachdienst MUSS für Einbringen des Exportpakets in der VAU den im Exportpaket übermittelte "encrypted_key" mit dem VAU-Zertifikat entschlüsseln und mit einer Zuordnung zu Betreiberkennung ("betreiberkennung") und Schlüsselversion ("version") speichern.[<=]

A_23493 - E-Rezept-Fachdienst - VSDM HMAC-Schlüssel - Prüfung

Der E-Rezept-Fachdienst MUSS das erfolgreiche Einbringen des Exportpaket in die VAU prüfen, indem der E-Rezept-Fachdienst den HMAC der leeren Bytefolge mit dem

importierten HMAC-Schlüssel berechnet und mit dem im Exportpaket übermittelten Wert "hmac_empty_string" vergleicht. [≤]

A_23484 - Anbieter E-Rezept-Fachdienst - Prüfung Exportpaket VSDM HMAC-Schlüssel - Information Fachdienstbetreiber VSDM

Der Anbieter des E-Rezept-Fachdienstes MUSS die gematik und den Fachdienstbetreiber VSDM von dem das Exportpaket stammt, unverzüglich informieren, falls das Einbringen eines Exportpakets in die VAU nicht möglich ist. [≤]

Die VAU des E-Rezept-Fachdienstes setzt die Gültigkeitszeiten nicht technisch durch. Stattdessen erfolgt das Entfernen von alten Schlüsseln (alten Version) manuell.

A_23485 - Anbieter E-Rezept-Fachdienst - Löschen VSDM HMAC-Schlüssel

Der Anbieter des E-Rezept-Fachdienstes MUSS ausschließlich auf Anforderung der gematik einen in der VAU vorhandenen HMAC-Schlüssel löschen. [≤]

Aus Gründen der Dokumentation und der Nachvollziehbarkeit führt der Anbieter des E-Rezept-Fachdienstes eine Liste von importierten Schlüsseln.

A_23486 - E-Rezept-Fachdienst - VSDM HMAC-Schlüssel - Ausgabe

Der E-Rezept-Fachdienst MUSS eine Liste der importierten Schlüsseln aus Exportpaketen ausgeben können, die alle Informationen aus den Exportpaketen enthält. Diese Liste DARF NICHT die Schlüssel im Klartext enthalten. [≤]

Die Schnittstelle wird nicht im Internet oder im zentralen Netz der TI bereitgestellt.

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 MediaType fhir+xml

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

A_19538 - E-Rezept-Fachdienst - RESTful API MediaType fhir+json

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

A_19539 - E-Rezept-Fachdienst - RESTful API MediaType Aufrufparameter

Der E-Rezept-Fachdienst MUSS in seinen Schnittstellen einen von der Standardfestlegung abweichenden MediaType 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> oder mittels des Accept-Attributs im HTTP-Request-Header als `application/fhir+xml` bzw. `application/fhir+json` 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, DELETE-Operation für das Senden, Empfangen und Löschen 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.[<=]

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_21558-01 - E-Rezept-Fachdienst - Task abrufen - Rollenprüfung Versicherter oder Apotheke liest Rezepte

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Task` sicherstellen, dass ausschließlich Versicherte und Leistungserbringer in der Rolle

- `oid_versicherter`
- `oid_oeffentliche_apotheke`

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

A_19113-01 - E-Rezept-Fachdienst - Rollenprüfung Versicherter oder Apotheker liest Rezept

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation 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 ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit E-Rezepte nicht durch Unberechtigte ausgelesen werden können.[<=]

A_19115-01 - E-Rezept-Fachdienst - Task abrufen - 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 ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, die inTask.for die entsprechende KVNR des begünstigten Patienten referenziert haben, damit ausschließlich Versicherte ihre eigenen E-Rezepte einsehen können.[<=]

A_19116-01 - E-Rezept-Fachdienst - Task abrufen - Prüfung AccessCode bei KVNR-Mismatch

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf einen einzelnen /Task/<id> und Ungleichheit der KVNR des Aufrufenden (KVNR des ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests UNGLEICH KVNR inTask.for) prüfen, ob der im HTTP-Request-Header "X-AccessCode" oder URL-Parameter "?ac=..." übergebene AccessCode gleich dem AccessCode inTask.identifizier ist, damit auch Vertreter in Kenntnis des AccessCodes ein einzelnes E-Rezept einsehen können.[<=]

A_19129-01 - E-Rezept-Fachdienst - Rückgabe Tasks im Bundle Versicherter

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task die gültige Ergebnisliste der Task-Ressourcen ohne die referenzierten, signierten E-Rezept-Bundle an den Aufrufer zurückgeben, damit der Versicherte eine Übersicht aller Tasks erhält.[<=]

A_21375-02 - E-Rezept-Fachdienst - Task abrufen - Rückgabe Task inkl. Bundles Versicherter

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf einen einzelnen /Task/<id> durch einen Versicherten die einzelne Task-Ressource um das referenzierte, serverseitig signierte E-Rezept-Bundle aus Task.input mit Codingsystem https://gematik.de/fhir/erp/CodeSystem/GEM_ERP_CS_DocumentType = 2 als search.include im Ergebnis-Bundle an den Aufrufer zurückgeben, damit der Versicherte eine vollständige Einsicht in den Task und den signierten Verordnungsdatensatz für eigene Dokumentationszwecke erhält.[<=]

A_21532-01 - E-Rezept-Fachdienst - Task abrufen - Kein Secret für Versicherte

Der E-Rezept-Fachdienst MUSS beim Aufruf der Operation GET /Task und GET /Task/<id> durch einen Versicherten oid_versicherter ein optional vorhandenesTask.identifizier:Secret als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Secret aus dem zurückgegebenen Task entfernen, sodass Versicherte nicht in Kenntnis des Secrets gelangen, welches die Prozesshoheit des Apothekers darstellt.[<=]

A_20702-02 - E-Rezept-Fachdienst - Task abrufen - Keine Einlöseinformationen in unbekannten Clients

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Task/<id>` ausschließlich solchen Clients die AccessCode Information (`Task.identifiziert` mit `system="`

https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_AccessCode") in den Task-Ressourcen zurückgeben, welche anhand der mitgeteilten, gültigen Produktidentifikation als hierfür zulässige Clients erkannt werden. [`<=`]

In E-Rezept-Stufe 1 ist ausschließlich das E-Rezept-FdV ein Client, welcher den AccessCode über die Operation GET `/Task/<id>` übermittelt bekommt.

A_21360-01 - E-Rezept-Fachdienst - Task abrufen - Flowtype 169 / 209 - keine Einlöseinformationen

Der E-Rezept-Fachdienst DARF den AccessCode beim Zugriff durch den Versicherten NICHT an das E-Rezept-Frontend des Versicherten herausgeben, wenn der Flowtype des Tasks den Wert für die Workflowsteuerung durch Leistungserbringer enthält (169, 209). [`<=`]

A_19226-01 - E-Rezept-Fachdienst - Task abrufen - 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/erp/CodeSystem/GEM_ERP_CS_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_19569-02 - E-Rezept-Fachdienst - Suchparameter Task

Der E-Rezept-Fachdienst MUSS das Eingrenzen einer Suchanfrage auf `/Task` gemäß <https://www.hl7.org/fhir/medicationdispense.html#search> mindestens für die Attribute

- `Task.status`,
- `Task.authoredOn` und
- `Task.lastModified`

unterstützen, sowie ein `_revinclude` der Ressource

`AuditEvent:entity.what` gemäß <https://www.hl7.org/fhir/search.html#revinclude> zulassen, sodass der Versicherte zu einem gesuchten Task alle zugehörigen Protokolleinträge abrufen kann. [`<=`]

A_23450 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - Prüfung Prüfungsnachweis

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Task` mit den URL-Parametern `pnw="..."` durch eine abgebende LEI, den im Parameter `pnw` übermittelten Prüfungsnachweis extrahieren, prüfen und bei Fehlen oder fehlerhafter

Prüfung mit dem Fehler 403 abbrechen, damit nur Clients die Operation aufrufen können, welche einen Anwesenheitsnachweis erfolgreich durchgeführt haben. [\leq]

A_23451 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - Zeitraum Akzeptanz Prüfungsnachweis

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task mit dem URL-Parameter `pnw="..."` durch eine abgebende LEI prüfen, dass die Differenz zwischen Zeitstempel aus der Prüfziffer des Prüfungsnachweises und dem aktuellen Zeitpunkt nicht größer als 30 Minuten (konfigurierbar) ist und bei fehlerhafter Prüfung mit dem Fehler 403 abbrechen. Im Fehlerfall ist die Meldung "Anwesenheitsnachweis konnte nicht erfolgreich durchgeführt werden (Zeitliche Gültigkeit des Anwesenheitsnachweis überschritten)." im OperationOutcome zu übermitteln. [\leq]

Eine mögliche Änderung der Konfiguration für den Zeitraum der Gültigkeit des Prüfungsnachweises erfolgt ausschließlich nach Anpassung von A_23451-* im Rahmen des Änderungsmanagement für Spezifikationen.

A_23452 - E-Rezept-Fachdienst - Rezepte lesen - Apotheke - VSDM - Filter KVNR

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /Task mit den URL-Parameter `pnw="..."` durch eine abgebende LEI, die Tasks nach `Task.status = "ready"` und `Task.for = KVNR` für die KVNR aus der Prüfziffer des Prüfungsnachweises filtern und in einem Bundle der gefundenen Tasks (ohne den signierte Anhang QES) zurückgeben, damit eine Apotheke alle zu einem Versicherten gehörenden E-Rezepte mit dem Status "offen" abrufen kann. [\leq]

Diese Operation führt nicht zu einer Statusänderung bei den zurück gelieferten Task Ressourcen.

6.1.1.1 HTTP-Operation GET - Prüfung VSDM Prüfungsnachweis

Der VSDM Prüfungsnachweis wird URL-codiert übertragen.

Das Informationsmodell des VSDM Prüfungsnachweises ist in [gemSysL_VSDM] beschrieben.

Die Struktur der VSDM Prüfziffer ist in A_23453-* (siehe Änderungseintrag C_11321) beschrieben.

Tabelle 7 : Struktur VSDM Prüfziffer

| Nr | Feld | Format | Länge |
|----|--|-----------------|-------|
| 1 | 10-stelliger unveränderlicher Teil der KVNR | alphanummerisch | 10 |
| 2 | aktueller Unix Timestamp | alphanummerisch | 10 |
| 3 | Grund des Updates U – Update Flag Service (UFS) Anfrage V – Versichertenstammdaten (VSD) Update C – Kartenmanagement (CMS) Update | alphanummerisch | 1 |
| 4 | Kennung des Betreibers Fachdienste VSDM gemäß Liste der gematik | alphanummerisch | 1 |
| 5 | Version des Hash-Schlüssels | alphanummerisch | 1 |

| Nr | Feld | Format | Länge |
|----|---|--------|-------|
| 6 | HMAC: ersten 24 Byte der Ausgabe der SHA-256 Hashfunktion mit dem betreiberspezifischen Schlüssel für die konkatenierten Felder 1-5 | binär | 24 |

A_23454 - E-Rezept-Fachdienst - Prüfung Prüfziffer

Der E-Rezept-Fachdienst MUSS die Prüfung des VSDM Prüfungsnachweises wie folgt umsetzen:

1. die Prüfziffer aus dem Prüfungsnachweis extrahieren
2. Falls eine Prüfziffer im Prüfungsnachweis enthalten ist:
 - a. HMAC-Schlüssel auf Basis Kennung des Betreibers (Feld 4) und Version des Hash-Schlüssels (Feld 5) ermitteln
 - b. HMAC über Felder 1-5 der übermittelten Prüfziffer berechnen
 - c. Berechneten HMAC mit dem in der Prüfziffer übermittelten HMAC auf Gleichheit prüfen

[<=]

Der Vergleich für die Ermittlung des HMAC-Schlüssel (2.a.) erfolgt case-sensitive.

A_23455 - E-Rezept-Fachdienst - Prüfung Prüfziffer - keine Prüfziffer

Der E-Rezept-Fachdienst MUSS prüfen, ob eine Prüfziffer im VSDM Prüfungsnachweis enthalten ist und falls nicht, die Prüfung mit einem Fehler abbrechen.

Im Fehlerfall ist die Meldung "Anwesenheitsnachweis konnte nicht erfolgreich durchgeführt werden (Prüfziffer fehlt im VSDM Prüfungsnachweis)." im OperationOutcome zu übermitteln.**[<=]**

Der E-Rezept-Fachdienst verwaltet HMAC-Schlüssel, welche durch die Betreiber der Fachdienste VSDM bereitgestellt werden. Ein HMAC-Schlüssel wird durch die Kennung des Betreibers des Fachdienstes VSDM und der Version des Schlüssels identifiziert.

A_23456 - E-Rezept-Fachdienst - Prüfung Prüfziffer - Berechnung HMAC der Prüfziffer

Der E-Rezept-Fachdienst MUSS für den HMAC der Prüfziffer die führenden 23 Byte der Prüfziffer (Felder 1-5) mittels SHA-256 Hashfunktion berechnen und für den nachfolgenden Vergleich die ersten 24 Byte verwenden.

Im Fehlerfall ist die Meldung "Anwesenheitsnachweis konnte nicht erfolgreich durchgeführt werden (Fehler bei Prüfung der HMAC-Sicherung)." im OperationOutcome zu übermitteln.**[<=]**

Die Ausgabelänge der SHA-256 Hashfunktion ist 32 Byte lang. Für die Prüfziffer werden die ersten 24 Byte verwendet. Die restlichen Bytes werden verworfen.

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 ACCESS_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_19257-01 - E-Rezept-Fachdienst - Task erzeugen - 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/erp/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_19019-01 - E-Rezept-Fachdienst - Task erzeugen - 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 Namenssystem https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_PrescriptionId dem Task hinzufügen und sicherstellen, dass diese Rezept-ID innerhalb von 11 Jahren nach ihrer Erzeugung nicht erneut vergeben wird, damit es innerhalb der

Aufbewahrungsfrist der Abrechnungsdaten bei den Krankenkassen zu keinen Dubletten kommt. [<=]

A_23227 - E-Rezept-Fachdienst - Task erzeugen - Task-ID=Rezept-ID

Der E-Rezept-Fachdienst MUSS beim Erzeugen eines neuen Tasks die Rezept-ID, welche mit Task an das verordnende Primärsystem übermittelt wird, als Task-ID verwenden. [<=]

A_19021-01 - E-Rezept-Fachdienst - Task erzeugen - 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.identifizier:AccessCode als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_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 ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit E-Rezepte nicht durch Unberechtigte eingestellt werden können. [<=]

**A_19024-02 - E-Rezept-Fachdienst - Task aktivieren - 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" oder URL-Parameter "?ac=..." übertragenen AccessCode gegen den im referenzierten Task

gespeicherten AccessCode Task.identifizier:AccessCode
als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_AccessCode und den Status des Tasks auf Task.status = draft 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_20159-02 - E-Rezept-Fachdienst - Task aktivieren - 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 8 : TAB_eRPF_D_006 Parameter Prüfung Signaturzertifikat QES des HBA

| Parameter | |
|-------------------|---|
| Zertifikat | Signaturzertifikat des HBA (eingebettet in Signatur-Objekt des QES-Datensatzes): <ul style="list-style-type: none"> • C.HP.QES (oid_hba_qes = 1.2.276.0.76.4.72 gemäß gemSpec_OID) • bzw. für HBA-Vorläuferkarten C.HP.ENC (oid_vk_eaa_enc = 1.3.6.1.4.1.24796.1.10 gemäß gemSpec_OID) Hinweis: die OID dieses Profil wird für Ärzte- und Zahnärzteschaft gleichermaßen genutzt |
| Referenzzeitpunkt | <Zeitpunkt der QES-Erstellung gemäß signingTime im QES-Datensatz> |
| Offline-Modus | nein |
| OCSP-Response | eingebettet in QES-Datensatz |

und darf die OCSP-Response für die Abfrage des Zertifikatsstatus für 12 Stunden zwischenspeichern.

Ist keine OCSP-Response eingebettet, MUSS der E-Rezept-Fachdienst die gecachte OCSP-Response verwenden oder eine OCSP-Response beim benannten TSP anfragen und die genutzte OCSP-Response nachträglich in den QES-Datensatz einbetten.

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_19025-02 - E-Rezept-Fachdienst - Task aktivieren - 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 das innerhalb des PKCS#7-Datensatz enveloping-enthaltene FHIR-Bundle einer umfänglichen FHIR-Validierung gegen die eRezept-Schema-Definition der KBV kbv.ita.erp unterziehen und bei Invalidität die Operation mit Status 400 abbrechen
- bzw. bei gültiger Signatur und validem FHIR den Datensatz als PKCS#7-Datei sicher speichern und in Task.input mit Codingsystem https://gematik.de/fhir/erp/CodeSystem/GEM_ERP_CS_Document_Type = 1 über eine interne, eindeutige UUID referenzieren,

damit der nachfolgende Workflow ausschließlich auf Basis medizinisch korrekter und vom Leistungserbringer mittels Signatur freigegebener Daten erfolgt. [<=]

Hinweis: Das Signaturzertifikat der ZOD-Karten (der Zahnärzteschaft) beinhalten die professionOID oid_zahnarzt.

A_23172 - E-Rezept-Fachdienst - Task aktivieren - Mimetype Signatur

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über /Task/<id>/\$activate die Angabe zum Mimetype des signierten Dokumentes prüfen und mit dem Fehler 400 abbrechen, wenn dieser ungleich "text/plain; charset=utf-8" ist. [<=]

A_21370 - E-Rezept-Fachdienst - Prüfung Rezept-ID und Präfix gegen Flowtype

Der E-Rezept-Fachdienst MUSS beim berechtigten Aufruf der Operation POST /Task/<id>/\$activate prüfen, dass die PrescriptionID des Tasks mit der PrescriptionID im übergebenen QES-Datensatz übereinstimmt und der Präfix der PrescriptionID gleich dem Flowtype des zu aktivierenden Tasks ist und andernfalls die Operation mit dem http-Fehlercode 400 abbrechen. [<=]

A_22487 - E-Rezept-Fachdienst - Task aktivieren - Prüfregel Ausstellungsdatum

Der E-Rezept-Fachdienst MUSS den Aufruf der http-POST-Operation /Task/<id>/\$activate mit einem Fehlercode 400 und Hinweis im OperationOutcome auf "Ausstellungsdatum und Signaturzeitpunkt weichen voneinander ab, müssen aber taggleich sein" als ungültig abweisen, wenn das Datum authoredOn zur Gültigkeitsberechnung des E-Rezepts nicht dem Datum in QES.Erstellung im Signaturobjekt entspricht. [<=]

A_22925 - E-Rezept-Fachdienst - Task aktivieren - Längenprüfung PZN

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 und einem Hinweis auf die Längenprüfung der PZN ("Länge PZN unzulässig (muss 8-stellig sein)") im OperationOutcome) abbrechen, wenn die PZN einer übergebenen PZN-Verordnung in KBV_PR_ERP_Medication_PZN.code.coding.code nicht 8-stellig ist. [<=]

Hinweis: PZNs können eine führende "0" enthalten.

A_22927 - E-Rezept-Fachdienst - Task aktivieren - Ausschluss unspezifizierter Extensions

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate den übergebenen Verordnungsdatensatz auf das

Vorhandensein von Extensions prüfen, die nicht in den FHIR-Profilen "kbv.ita.erp 1.0.2" explizit an den zu verwendenden Stellen spezifiziert sind und

1. für eine Dauer von 6 Wochen (konfigurierbar) mit dem abweichenden Http-Statuscode 202 Accepted ab dem PU-Release dieser Funktion als valide akzeptieren
2. diese Verordnungen (nach 6 Wochen nach Release) als ungültig und Fehlermeldung (Http-Statuscode 400, "unintendierte Verwendung von Extensions an unspezifizierter Stelle im Verordnungsdatensatz") ablehnen

damit undefiniertes Verhalten in Clientsystemen und widersprüchliche Angaben in der Verordnung verhindert werden. [<=]

Der E-Rezept-Fachdienst setzt damit eine Übergangsregelung "closed slicing light" um – bis zur Umsetzung in den FHIR-Profilen des Verordnungsdatensatzes.

A_22347-01 - E-Rezept-Fachdienst – Task aktivieren – Flowtype 200/209 - Prüfung Coverage Type

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task des Flowtype `Task.extension:flowType = 200` oder `209` mittels HTTP-POST-Operation über `/Task/<id>/$activate` prüfen, ob `Coverage.type.coding.code` mit dem Wert "PKV" belegt ist und im Fehlerfall die Operation mit Http-Fehlercode 400 abbrechen, um sicherzustellen, dass diese Workflows nur für E-Rezepte für PKV-Versicherte genutzt werden. [<=]

A_22231 - E-Rezept-Fachdienst - Task aktivieren - Ausschluss Betäubungsmittel und Thalidomid

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über `/Task/<id>/$activate` die Operation mit dem Fehlercode 400 und einem Hinweis auf den Ausschluss von Betäubungsmittel und T-Rezepten ("BTM und Thalidomid nicht zulässig" im `OperationOutcome`) abbrechen, wenn der übergebene QES-Datensatz als Betäubungsmittel- oder Thalidomid-Verordnung (`Bundle.Medication.extension:KBV_EX_ERP_Medication_Category:code` ungleich "00") gekennzeichnet ist. [<=]

Hinweis: Dieser Ausschluss erfolgt für alle aktuell spezifizierten FlowTypes (160, 169, 200). In einer späteren Ausbaustufe sollen Betäubungsmittel und Verordnungen nach AMVV § 3a Abs. 1 explizit unterstützt werden. Die konkreten Festlegungen dazu werden in einem Folgerelease getroffen.

A_22222 - E-Rezept-Fachdienst - Task aktivieren - Ausschluss weitere Kostenträger

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über `/Task/<id>/$activate` die Operation mit dem Fehlercode 400 und einem Hinweis auf den Ausschluss der Kostenträger ("Kostenträger nicht zulässig" im `OperationOutcome`) abbrechen, wenn der übergebene QES-Datensatz einen unzulässigen Kostenträger (`Bundle.Coverage.type:KBV_VS_FOR_Payor_type` ungleich [GKV, PKV, SEL, BG + `KBV_CS_FOR_Payor_Type_KBV:UK`]) enthält. [<=]

Dieser Ausschluss erfolgt temporär, in einer späteren Version können weitere Kostenträger explizit unterstützt werden. Die konkreten Festlegungen dazu werden in einem Folgerelease getroffen.

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_19127-01 - E-Rezept-Fachdienst - Task aktivieren - 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/sid/gkv/kvid-10> bzw. <http://fhir.de/sid/pkv/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 System <http://fhir.de/sid/gkv/kvid-10> bzw. <http://fhir.de/sid/pkv/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 `StatusTask.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_19029-05 - E-Rezept-Fachdienst - Task aktivieren - Serversignatur Rezept aktivieren

Der E-Rezept-Fachdienst MUSS das bei der Operation `/Task/<id>/$activate` 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 beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Task/<id>` zurückliefern.

Der E-Rezept-Fachdienst MUSS für diesen

- einen neuen, eindeutigen Identifier für die [Bundle.id](#) als UUID generieren,
- das Bundle entsprechend der Kanonisierungsregeln <http://hl7.org/fhir/canonicalization/json#static> normalisieren (Bundle.text und Bundle.meta im "root-Element" entfernen) und
- mit der Signaturidentität des Fachdienstes ID.FD.OSIG gemäß [FHIR-Sig] signieren und
- das signierte Bundle mit Referenz in Task.input mit Codingsystem https://gematik.de/fhir/erp/CodeSystem/GEM_ERP_CS_DocumentType = 2 zurück liefern,

damit der Versicherte einen Nachweis über die Integrität der gespeicherten Daten einsehen kann. [`<=`]

Die Festlegungen in [FHIR-Sig] sind in Teilen unspezifisch, konkrete Beispiele finden sich in der gematik-API-Beschreibung für das E-Rezept auf <https://github.com/gematik/api-erp>

Die Signatur soll als JSON Web Signature [JWS] detached erstellt werden, dementsprechend bleibt das `data`-Feld der JWS-Struktur leer. Im JWS-Header muss das

Zertifikat C.FD.SIG eingebettet werden, mit dessen zugehörigen privaten Signaturschlüssel signiert wurde. Als Wert für targetFormat ist der MimeType `application/fhir+json` und für sigFormat ist der MimeType `application/jose` zu verwenden.

6.1.2.2.1 POST /Task/<id>/\$activate - Mehrfachverordnung

A_22627-01 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - zulässige Flowtype

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung als Mehrfachverordnung

(`MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = true`) gekennzeichnet und der Flowtype ungleich 160, 169, 200 oder 209 ist, weil Mehrfachverordnungen nur für die Verordnungen von apothekenpflichtigen Arzneimittel (kein BtM, kein T-Rezept) zulässig sind. [`<=`]

A_22628 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - Numerator-Denominator kleiner 5

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung als Mehrfachverordnung

(`MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = true`) gekennzeichnet und der Numerator oder Denominator größer als 4 ist, weil eine Mehrfachverordnungen aus maximal 4 Teilverordnungen bestehen darf. [`<=`]

A_22704 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - Numerator größer 0

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung als Mehrfachverordnung

(`MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = true`) gekennzeichnet und der Numerator kleiner als 1 ist. [`<=`]

A_22629 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - Denominator größer 1

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung als Mehrfachverordnung

(`MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = true`) gekennzeichnet und der Denominator kleiner als 2 ist, weil eine Mehrfachverordnungen aus mindestens 2 Teilverordnungen bestehen muss. [`<=`]

A_22630 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - Numerator kleiner / gleich Denominator

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung als Mehrfachverordnung

(`MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = true`) gekennzeichnet und der Numerator größer als der Denominator ist. [`<=`]

A_22631 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - Unzulässige Angaben

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung nicht als Mehrfachverordnung

(MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = false) gekennzeichnet ist, aber eine Extension Nummerierung oder Zeitraum enthält, weil normale Verordnungen keine MVO-Angaben enthalten dürfen.[<=]

A_22632 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - kein Entlassrezept

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung als Mehrfachverordnung

(MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = true) und als Entlassrezept (code="04" oder "14" in

Extension https://fhir.kbv.de/StructureDefinition/KBV_EX_FOR_Legal_basis in Bundle.Composition.extension:rechtsgrundlage) gekennzeichnet ist, weil für Entlassrezepte keine Mehrfachverordnungen zulässig sind.[<=]

A_22633 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - keine Ersatzverordnung

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung als Mehrfachverordnung

(MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = true) und als Ersatzverordnung (code="10" oder "11" oder "17" in

Extension https://fhir.kbv.de/StructureDefinition/KBV_EX_FOR_Legal_basis in Bundle.Composition.extension:rechtsgrundlage) gekennzeichnet ist, weil für Ersatzverordnungen keine Mehrfachverordnungen zulässig sind.[<=]

A_22634 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - Beginn Einlösefrist-Pflicht

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung als Mehrfachverordnung

(MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = true) gekennzeichnet ist und der Beginn der Einlösefrist

(MedicationRequest.extension:Mehrfachverordnung.extension:Zeitraum.value[x]:valuePeriod.start) nicht angegeben ist, weil die Information des Beginns der Einlösefrist notwendig ist, um den Gültigkeitszeitraum zu ermitteln.[<=]

Hinweis: Ist das Gültigkeitsende-

Datum (MedicationRequest.extension:Mehrfachverordnung.extension:Zeitraum.value[x]:valuePeriod.end) nicht angegeben, kann die Teilverordnung bis zum Tag [Ausstellungsdatum + 365] eingelöst und für E-Rezepte des Workflow-Typen 160 zu Lasten der GKV abgerechnet werden.

A_23164 - E-Rezept-Fachdienst - Task aktivieren - Mehrfachverordnung - Endedatum nicht vor Startdatum

Der E-Rezept-Fachdienst MUSS beim Aktivieren eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$activate die Operation mit dem Fehlercode 400 abbrechen, wenn die Verordnung als Mehrfachverordnung

(MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen =

true) gekennzeichnet, ein

Endedatum (`MedicationRequest.extension:Mehrfachverordnung.extension:Zeitraum.value[x]:valuePeriod.end`) angegeben ist und das Endedatum vor dem Startdatum (`MedicationRequest.extension:Mehrfachverordnung.extension:Zeitraum.value[x]:valuePeriod.start`) liegt. [`<=`]

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 ACCESS_TOKEN im HTTP-RequestHeader "`Authorization`" feststellen, damit E-Rezepte nicht durch Unberechtigte abgerufen werden können. [`<=`]

A_19167-03 - E-Rezept-Fachdienst - Task akzeptieren - Prüfung AccessCode

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über `/Task/<id>/$accept` den im HTTP-Header "`X-AccessCode`" oder URL-Parameter "`?ac=...`" übertragenen AccessCode gegen den im referenzierten Task gespeicherten AccessCode `Task.identifizier:AccessCode`

als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_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 `StatusTask.status = completed`, `Task.status = in-progress` oder `Task.status = draft` ist, damit ein bereits in Abgabe befindliches oder beliefertes E-Rezept nicht durch eine zweite Apotheke bearbeitet werden kann. [`<=`]

A_19169-01 - E-Rezept-Fachdienst - Task akzeptieren - 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.identifizier:Secret` als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Secret hinzufügen und den Task im Bundle mit dem in `Task.input` mit Codingsystem https://gematik.de/fhir/erp/CodeSystem/GEM_ERP_CS_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_22110 - E-Rezept-Fachdienst – Task akzeptieren – Flowtype 200/209 - Einwilligung ermitteln

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task des Flowtype `Task.extension:flowType = 200` oder `209` mittels HTTP-POST-Operation über `/Task/<id>/$accept`, wenn für die KVNR des begünstigten Versicherten (`Task.for`) eine Consent Ressource mit `Consent.patient.identifier = KVNR` und `Consent.category.coding.code = "CHARGCONS"` existiert, das Response Bundle um die Consent Ressource ergänzen, um der abgebenden LEI die Information zu übermitteln, ob der Versicherte eine Einwilligung zum Speichern der Abrechnungsinformationen auf dem E-Rezept-Fachdienst erteilt hat. [≤]

A_19149-01 - E-Rezept-Fachdienst - Task akzeptieren - 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/erp/StructureDefinition/GEM_ERP_PR_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. [≤]

A_22635-01 - E-Rezept-Fachdienst - Task akzeptieren - Mehrfachverordnung - Beginn Einlösefrist prüfen

Der E-Rezept-Fachdienst MUSS beim Zugriff auf einen Task mittels HTTP-POST-Operation über `/Task/<id>/$accept` die Operation mit dem Fehlercode 403 abbrechen, wenn die Verordnung als Mehrfachverordnung (`MedicationRequest.extension:Mehrfachverordnung.extension:Kennzeichen = true`) gekennzeichnet ist und der Beginn der Einlösefrist (`MedicationRequest.extension:Mehrfachverordnung.extension:Zeitraum.value[x]:valuePeriod.start`) zu einem späteren Zeitpunkt als das aktuelle Datum liegt, da Teilverordnungen von Mehrfachverordnungen erst ab Beginn der Einlösefrist abgerufen werden dürfen. Im Falle dieses Fehlers ist im `OperationOutcome` des Response der Beginn der Einlösefrist wie folgt anzugeben: „Teilverordnung ab <Datum> einlösbar.“, wobei <Datum> der Wert `<MedicationRequest.extension:Mehrfachverordnung.extension:Zeitraum.value[x]:valuePeriod.start>` im Format "dd.mm.yyyy" ist. [≤]

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_19170-01 - E-Rezept-Fachdienst - Rollenprüfung Abgebender weist zurück

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 ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit das E-Rezept nicht durch einen Unberechtigten zurückgewiesen werden kann.[<=]

A_19171-02 - E-Rezept-Fachdienst - Task zurückweisen - Prüfung Secret

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.identifizier:Secret als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Secret und auf Task.status = in-progress 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_19172-01 - E-Rezept-Fachdienst - Task zurückweisen - Secret löschen und Status setzen

Der E-Rezept-Fachdienst MUSS beim Zurückweisen eines Tasks mittels HTTP-POST-Operation über /Task/<id>/\$reject die externe ID inTask.identifizier:Secret als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_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 ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit der E-Rezept-Workflow nicht durch einen Unberechtigten abgeschlossen werden kann.[<=]

A_19231-01 - E-Rezept-Fachdienst - Task schließen - Prüfung Secret

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.identifizier:Secret als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Secret und auf Task.status = in-progress 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_19248-02 - E-Rezept-Fachdienst - Task schließen - 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/erp/StructureDefinition/GEM_ERP_PR_MedicationDispense prüfen, insbesondere

- die Korrektheit der Rezept-ID https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_PrescriptionId als `MedicationDispense.identifier`,
- die KVN-R des Versicherten im referenzierten Task (`Task.for`) gegen KVN-R in `MedicationDispense.subject.identifier` und
- ob die Telematik-ID der Apotheke gemäß `ACCESS_TOKEN` mit dem Wert in `MedicationDispense.performer.actor.identifier` übereinstimmt.

Der E-Rezept-Fachdienst MUSS die Referenz auf den aufgerufenen Task `/Task/<id>` als `MedicationDispense.supportingInformation` übernehmen und die MedicationDispense für den Abruf durch den Versicherten speichern. [≤]

A_22073 - E-Rezept-Fachdienst - Task schließen - Datum MedicationDispense whenHandedOver

Der E-Rezept-Fachdienst MUSS bei der Validierung der MedicationDispense das Feld `whenHandedOver` (und sofern vorhanden das Feld `whenPrepared`) übergangsweise als Datum entweder mit Uhrzeitangabe oder ausschließlich als Datum (10-stellig: "yyyy-mm-dd") gemäß des FHIR-Datentyps `dateTime` akzeptieren. [≤]

In einem Folgerelease der FHIR-Profildefinition für MedicationDispense wird ein Constraint für das 10-stellige Datum eingeführt, sodass ab dessen Gültigkeitsbeginn der Fachdienst in den Feldern `whenHandedOver` und `whenPrepared` ausschließlich Werte im 10-stelligen Datumsformat akzeptiert.

A_22069 - E-Rezept-Fachdienst - Task schließen - Speicherung mehrerer MedicationDispenses

Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels `/Task/<id>/$close` auch die Übergabe mehrerer MedicationDispense-Objekte in einem validen Standard-FHIR-Bundle im http-Body des Requests ermöglichen und die zweite, dritte usw. MedicationDispense für den Abruf unter einer einzelnen ID (z.B. `MedicationDispense/<prescriptionID> + "suffix"`) durch den Versicherten speichern. [≤]

Hinweis: Als Suffix kann ein Zähler "-1", "-2", etc. an die PrescriptionID angehängen werden, um für jede MedicationDispense eine eindeutige ID zu erzeugen.

A_19232 - E-Rezept-Fachdienst - Status beenden

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

A_20513 - E-Rezept-Fachdienst - nicht mehr benötigte Einlösekommunikation

Der E-Rezept-Fachdienst MUSS bei erfolgreicher Beendigung eines Tasks mittels `/Task/<id>/$close`-Operation alle Communication-Ressourcen löschen, die eine Referenz auf diesen Task in `Communication.baseOn` enthalten, damit nicht mehr benötigte

Informationen über die Kommunikation zur Einlösung des E-Rezepts vom E-Rezept-Fachdienst entfernt werden. [≤]

A_19233-05 - E-Rezept-Fachdienst - Task schliessen - Quittung erstellen

Der E-Rezept-Fachdienst MUSS beim Beenden eines Tasks mittels `/Task/<id>/$close` ein Quittungsbundle gemäß des FHIR-

Profils https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Bundle mit folgenden Informationen erstellen:

- Telematik-ID der aufrufenden Apotheke als `Beneficiary` in die `erxComposition`
- Zeitstempel des Statuswechsel des Tasks "in-progress" in `event.period.start`
- aktueller Zeitstempel in `event.period.end`
- Identifier `PrescriptionID` des Task als identifier des Quittungs-Bundle
- Device-Ressource mit Fachdienstinformationen als Autor der Signatur
- Base64Binary-Ressource mit `Binary.data` = <base64-codierter Hashwert aus der QES-Signatur des dem Task zugrunde liegenden Verordnungsdatensatzes> und `contentType` = "application/octet-stream"

und dieses Quittungs-Bundle mit der Signaturidentität des Fachdienstes `ID.FD.OSIG` gemäß [RFC5652] mit Profil `CAdES-BES` ([`CAdES`]) im Enveloping signieren.

In die Signatur wird die letzte OCSP-Antwort der regelmäßigen Statusprüfung des Signaturzertifikats `C.FD.OSIG` eingebettet.

Das Signatur-Ergebnis wird als `dss:Base64Signature`-Objekt in `Bundle.signature` eingebettet und dieses Quittungs-Bundle mit Referenz in `Task.output` mit

Codingsystem https://gematik.de/fhir/erp/CodeSystem/GEM_ERP_CS_DocumentType =

3 gespeichert 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. [≤]

A_22919 - E-Rezept-Fachdienst - Task schließen - OCSP-Response nicht älter als 24 h

Der E-Rezept-Fachdienst MUSS, falls keine OCSP-Response für das Signaturzertifikat der Quittung vorliegt bzw. die letzte vorliegende OCSP-Response älter als 24 h ist, die Operation mit dem Fehler 503 abbrechen. [≤]

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 dem Versicherten, für den das E-Rezept erstellt wurde, sowie allen Nutzern in Kenntnis des AccessCodes (verordnende und abgebende Leistungserbringer, 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 ACCESS_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_22102-01 - E-Rezept-Fachdienst - E-Rezept löschen - Flowtype 169 / 209 - Versicherter - Statusprüfung

Der E-Rezept-Fachdienst MUSS das Löschen eines E-Rezepts mit dem Flowtype 169 oder 209 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 "completed" ist und die Rolle des aufrufenden Nutzers der folgenden Rollen entspricht:

- oid_versicherter

damit kein Versicherter ein E-Rezept aus einem Workflow mit Workflowsteuerung durch Leistungserbringer (169, 209) löscht, das nicht bereits beliefert wurde. [≤]

A_20546-03 - E-Rezept-Fachdienst - E-Rezept löschen - Prüfung KVNR, Versicherter löscht Rezept

Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts durch einen Versicherten, wenn der HTTP-Request keinen HTTP-Header "X-AccessCode" oder URL-Parameter "?ac=..." enthält, den Versicherten anhand der KVNR aus dem ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, diese gegen die in `Task.for` hinterlegte KVNR des begünstigten Patienten prüfen und bei Mismatch den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich der begünstigte Patient als Berechtigter ohne Kenntnis des AccessCodes ein E-Rezept löscht. [≤]

A_19120-03 - E-Rezept-Fachdienst - E-Rezept löschen - Verordnender - Prüfung AccessCode und Status

Der E-Rezept-Fachdienst MUSS beim Löschen eines E-Rezepts über den mittels der `<id> adressierten/Task/<id>/$abort` durch verordnende Leistungserbringer den im HTTP-Header "X-AccessCode" gegen den im referenzierten Task enthaltenen AccessCode prüfen und bei Mismatch oder Fehlen im HTTP-Header oder wenn der `Task.Status` ungleich "ready" ist, den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich die verordnende Leistungserbringerinstitution in Kenntnis des AccessCodes als Berechtigte 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 in `Task.identifizier` prüfen und bei Mismatch 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_19027-03 - E-Rezept-Fachdienst - E-Rezept löschen - Medizinische und personenbezogene Daten löschen

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

- `Task.input` --> löschen (inkl. aller referenzierten Elemente)
- `Task.output` --> löschen (inkl. aller referenzierten Elemente)
- `Task.identifizier (AccessCode)` --> löschen
- `Task.identifizier (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. [≤]

Hinweis: Die KVNR in `Task.for` wird nicht gelöscht, damit der Versicherte den Status des Task mit dem E-Rezept-FdV abrufen 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_19405-01 - 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 `/MedicationDispense/<id>` sicherstellen, dass ausschließlich Versicherte in der Rolle

- `oid_versicherter`

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

A_19406-01 - E-Rezept-Fachdienst - MedicationDispense abrufen - 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 ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, die in `MedicationDispense.subject` die entsprechende KVNR des begünstigten Patienten referenziert haben, damit ausschließlich Versicherte ihre eigenen Dispensierinformationen einsehen können. [`<=`]

A_19518-01 - 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> mindestens für die Attribute

- MedicationDispense.whenHandedOver,
- MedicationDispense.whenPrepared und
- MedicationDispense.performer.actor

erlauben, damit Versicherte eine Suche und Sortierung nach Ausgabedatum sowie der aufgesuchten Apotheke durchführen können. [\leq]

A_22070-01 - E-Rezept-Fachdienst - MedicationDispense abrufen - Rückgabe mehrerer MedicationDispenses

Der E-Rezept-Fachdienst MUSS das Suchergebnis mit mehreren MedicationDispense-Objekten anhand der PrescriptionID (?identifier=|<PrescriptionID>) und bei Vorhandensein mehrerer MedicationDispense-Objekte zu einem beendeten Task, die MedicationDispense-Objekte in einem Bundle an den Aufrufenden zurückgeben. [\leq]

Der Fachdienst soll eine mögliche Konstellation von Bundles im Ergebnis-Bundle auflösen, sodass das Ergebnisbundle ausschließlich MedicationDispense-Objekte enthält, unabhängig davon, ob ein oder mehrere dieser Objekte zu je einem Task gehören.

6.3 Ressource ChargeItem

A_22111 - E-Rezept-Fachdienst – ChargeItem - unzulässige Operationen

Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource ChargeItem mittels der HTTP-Operationen HEAD unterbinden, damit keine unzulässigen Operationen auf die Informationen zu Abrechnungsinformationen ausgeführt werden können. [\leq]

6.3.1 HTTP-Operation DELETE

Die FHIR-Operation führt zum Löschen der unter <Prescription-ID> gespeicherten Abrechnungsinformation. Diese Operation steht dem Versicherten, für den das E-Rezept erstellt wurde, zur Verfügung.

A_22112 - E-Rezept-Fachdienst – Abrechnungsinformation löschen - alles Löschen verbieten

Der E-Rezept-Fachdienst MUSS den Aufruf der Operation DELETE /ChargeItem ohne Angabe einer konkreten über <id> adressierte ChargeItem Ressource mit dem HTTP-Fehlercode 405 ablehnen, um das Löschen mehrerer Ressourcen über einen Request zu verhindern. [\leq]

A_22113 - E-Rezept-Fachdienst – Abrechnungsinformation löschen - Rollenprüfung

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-DELETE-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource sicherstellen, dass ausschließlich Nutzer in der Rolle

- oid_versicherter

die Operation am E-Rezept-Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit eine Abrechnungsinformation nicht durch Unberechtigte gelöscht werden können. [\leq]

A_22114 - E-Rezept-Fachdienst – Abrechnungsinformation löschen – Prüfung KVNR

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-DELETE-Operation auf eine konkrete über <id> adressierte/ChargeItem/<id> Ressource durch einen Versicherten, den Versicherten anhand der KVNR aus dem ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, diese gegen die in "ChargeItem.subject.identifizier" hinterlegte KVNR des begünstigten Versicherten prüfen und bei Ungleichheit den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich der begünstigte Versicherte als Berechtigter eine Abrechnungsinformation löscht.[<=]

A_22117-01 - E-Rezept-Fachdienst - Abrechnungsinformation löschen - zu löschende Ressourcen

Der E-Rezept-Fachdienst MUSS beim Löschen einer ChargeItem-Ressource auch

- die in ChargeItem.supportingInformation referenzierten Ressourcen des Verordnungsdatensatzes, des PKV-Abgabedatensatzes und der Quittung,
- alle Communication mit Communication.basedOn = ChargeItem.id,

löschen.[<=]

6.3.2 HTTP-Operation GET**6.3.2.1 GET /ChargeItem**

Mit dieser Operation kann eine Liste von ChargeItem-IDs abgefragt werden, für deren Zugriff der Anfragende berechtigt ist.

A_22118 - E-Rezept-Fachdienst – Abrechnungsinformationen abrufen - Rollenprüfung Versicherter

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /ChargeItem sicherstellen, dass ausschließlich Nutzer in der Rolle

- oid_versicherter

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

A_22119 - E-Rezept-Fachdienst – Abrechnungsinformationen abrufen – Versicherter – Filter KVNR

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /ChargeItem durch einen Versicherten, den Versicherten anhand der KVNR aus dem ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren und die ChargeItems danach filtern, damit der Versicherte nur Abrechnungsinformationen abrufen, bei denen er der Begünstigte ist.[<=]

A_22121-01 - E-Rezept-Fachdienst – Abrechnungsinformationen abrufen - Suchkriterien

Der E-Rezept-Fachdienst MUSS das Eingrenzen einer Suchanfrage auf /ChargeItem über die URL-Parameter

gemäß <https://www.hl7.org/fhir/chargeitem.html#search> mindestens für die Attribute

- ChargeItem.enteredDate
- ChargeItem.meta.__lastUpdated

erlauben, damit Versicherte eine Suche nach neuen Abrechnungsinformations-Einträgen durchführen können. [≤]

A_22122 - E-Rezept-Fachdienst – Abrechnungsinformationen abrufen – Response

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt /ChargeItem eine Liste von ChargeItem Ressourcen ohne die in supportingInformation referenzierten Datensätze entsprechend der Filterung und Suchkriterien übermitteln. [≤]

A_22123 - E-Rezept-Fachdienst – Abrechnungsinformationen abrufen - Paging

Der E-Rezept-Fachdienst KANN beim Aufruf der HTTP-GET-Operation auf den Endpunkt /ChargeItem das Suchergebnis in einem Paging-Mechanismus auf mehrere Ergebnis-Bundle aufteilen, damit der Nutzer eine komfortable Navigationsmöglichkeit in seinen Abrechnungsinformationen erhält. [≤]

6.3.2.2 GET /ChargeItem/<id>

Mit dieser Operation können die Details zu einem ChargeItem abgefragt werden. Ein Versicherter ist berechtigt auf eine ChargeItem Ressourcen zuzugreifen, wenn er der Begünstigte ist. Eine Apotheke ist berechtigt auf eine ChargeItem Ressource zuzugreifen, wenn sie diese dem Versicherten bereitgestellt hat und wenn sie den vom Versicherten bereitgestellten AccessCode übermitteln kann.

A_22124 - E-Rezept-Fachdienst – Abrechnungsinformation abrufen - Rollenprüfung Versicherter oder Apotheker

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf eine konkrete über <id> adressierte/ChargeItem/<id> Ressource sicherstellen, dass ausschließlich Versicherte oder Apotheken in einer der Rollen

- oid_versicherter
- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am E-Rezept-Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit E-Rezepte nicht durch Unberechtigte ausgelesen werden können. [≤]

A_22125 - E-Rezept-Fachdienst – Abrechnungsinformation abrufen – Versicherter – Prüfung KVNR

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf eine konkrete über <id> adressierte/ChargeItem/<id> Ressource durch einen Versicherten, den Versicherten anhand der KVNR aus dem ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, diese gegen die in "ChargeItem.subject.identifizier" hinterlegte KVNR des begünstigten Versicherten prüfen und bei Ungleichheit den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich der begünstigte Versicherte als Berechtigter eine Abrechnungsinformation abrufen kann. [≤]

A_22126 - E-Rezept-Fachdienst – Abrechnungsinformation abrufen – Apotheke – Prüfung Telematik-ID

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf eine konkreten über <id> adressierte/ChargeItem/<id> Ressource durch eine abgebende

Leistungserbringerinstitution, die LEI anhand der Telematik-ID aus dem ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, diese gegen die in "ChargeItem.enterer.identifizier" hinterlegte Telematik-ID der einstellenden LEI prüfen und bei Ungleichheit den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich die LEI eine Abrechnungsinformation abrufen kann, welche die Abrechnungsinformation im E-Rezept-Fachdienst bereitgestellt hat. [<=]

A_22611-01 - E-Rezept-Fachdienst – Abrechnungsinformation abrufen – Apotheke – Prüfung AccessCode

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf eine konkreten über <id> adressierte /ChargeItem/<id> Ressource durch eine abgebende Leistungserbringerinstitution, den im URL-Parameter "?ac=..." übertragenen AccessCode gegen den im referenzierten ChargeItem gespeicherten

AccessCodeChargeItem.identifizier:AccessCode

als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_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_22127-01 - E-Rezept-Fachdienst – Abrechnungsinformation abrufen – Versicherte – Signieren

Der E-Rezept-Fachdienst MUSS beim Aufruf der Operation GET /ChargeItem/<id> durch einen Versicherten zusätzlich zum ChargeItem die folgenden Datensätze im JSON-Format in einem Responsebundle zurück liefern und dafür in jedem Aufruf

- den Verordnungsdatensatz im XML-Format mit der Signaturidentität des E-Rezept-Fachdienstes ID.FD.OSIG gemäß [RFC5652] mit Profil CAdES-BES ([CAdES]) Enveloping signieren (QES wird dabei entfernt),
- den PKV-Abgabedatensatz im XML-Format mit der Signaturidentität des E-Rezept-Fachdienstes ID.FD.OSIG gemäß [RFC5652#section-11.4] mit Profil CAdES-BES ([CAdES]) Enveloping im gegensignieren
- die Quittung im XML-Format mit der Signaturidentität des E-Rezept-Fachdienstes ID.FD.OSIG gemäß [RFC5652] mit Profil CAdES-BES ([CAdES]) Enveloping signieren und
- in jede Fachdienstsignatur die letzte OCSP-Antwort der regelmäßigen Statusprüfung des Signaturzertifikats C.FD.OSIG einbetten (jedes Signatur-Ergebnis wird als dss:Base64Signature-Objekt in Bundle.signature des jeweiligen JSON-Objekts eingebettet),

damit der Versicherte die Daten für die Abrechnung an Kostenträger weiterleiten kann. [<=]

Hinweis: Außer ChargeItem sind die zurückgegebenen FHIR-Ressourcen vom Typ Bundle und jedes Bundle trägt "seine" Signatur im jeweiligen Attribut Bundle.signature im CAdES-Enveloping-Format. Die signierten Daten sind dadurch doppelt vorhanden, das erspart jedoch die fehleranfällige Normalisierung und Kanonisierung in der Signaturprüfung.

Hinweis: Der Verordnungsdatensatz, der PKV-Abgabedatensatz und die Quittung werden zum Abrufzeitpunkt signiert, um die Möglichkeit der Prüfung der Signaturzertifikate im nachfolgenden Abrechnungsprozess sicherzustellen.

Hinweis: Es ist geplant, das Signaturzertifikat C.FD.OSIG durch ein eIDAS Siegel zu ersetzen, um eine Prüfung der Signatur außerhalb der TI mit Standardtools zu ermöglichen.

A_22128 - E-Rezept-Fachdienst – Abrechnungsinformation abrufen – Apotheke – kein AccessCode und Quittung

Der E-Rezept-Fachdienst DARF beim Aufruf der Operation `GET /ChargeItem/<id>` durch eine abgebende Leistungserbringerinstitution das in

"ChargeItem.supportingInformation" referenzierte

Element `ChargeItem.supportingInformation:receipt` und den

Identifizier `Task.identifizier:AccessCode` NICHT in den Response übernehmen, sodass die abgebende LEI nur den Verordnungsdatensatz und durch sie änderbaren PKV-Abgabedatensatz erhält. [`<=`]

Hinweis: Der Verordnungsdatensatz wird mit QES des Verordnenden an die Apotheke zurück geliefert.

6.3.3 HTTP-Operation PATCH

Die FHIR-Operation führt zum Aktualisieren einer unter `<Prescription-ID>` gespeicherten `ChargeItem` Ressource.

Diese Operation steht dem Versicherten für das Aktualisieren der Markierungen zur Verfügung.

6.3.3.1 PATCH /ChargeItem/<id>**A_22879 - E-Rezept-Fachdienst – Abrechnungsinformation ändern (PATCH) - alles Ändern verbieten**

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-Operation PATCH auf den Endpunkt `/ChargeItem` ohne Angabe einer `<id>` für eine konkrete Ressource mit dem HTTP-Fehlercode 405 ablehnen, um das Ändern mehrerer Ressourcen über einen Request zu verhindern. [`<=`]

Hinweis: Auf die Prüfung, ob die Einwilligung zum Speichern der Abrechnungsinformationen vorliegt, kann verzichtet werden, weil bei einem zwischenzeitlichen Widerruf alle Abrechnungsinformationen des Versicherten vom E-Rezept-Fachdienst gelöscht wurden. Beim Aufruf der Operation PATCH `/ChargeItem/<id>` wird der HTTP-Fehlercode 404 (Not found) zurückgegeben.

A_22875 - E-Rezept-Fachdienst – Abrechnungsinformation ändern (PATCH) – Rollenprüfung

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-PATCH-Operation auf eine konkrete über `<id>` adressierte `/ChargeItem/<id>` Ressource sicherstellen, dass ausschließlich Nutzer in der Rolle

- `oid_versicherter`

die Operation am E-Rezept-Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im `ACCESS_TOKEN` im HTTP-RequestHeader "Authorization" feststellen, damit eine Abrechnungsinformation nicht durch Unberechtigte aktualisiert werden kann. [`<=`]

A_22877 - E-Rezept-Fachdienst – Abrechnungsinformation ändern (PATCH) – Versicherter - Prüfung KVNR

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-PATCH-Operation auf eine konkrete über `<id>` adressierte `/ChargeItem/<id>` Ressource durch einen Versicherten, den Versicherten anhand der KVNR aus dem `ACCESS_TOKEN` im "Authorization"-Header des HTTP-Requests identifizieren, diese gegen die im gespeicherten Datensatz in `"ChargeItem.subject.identifizier"` hinterlegte KVNR des begünstigten Versicherten prüfen und bei Ungleichheit den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit

ausschließlich der begünstigte Versicherte als Berechtigter eine Abrechnungsinformation ändert. [<=]

A_22878 - E-Rezept-Fachdienst - Abrechnungsinformation ändern (PATCH) – Zulässige Felder

Der E-Rezept-Fachdienst MUSS die im HTTP-PATCH-Operation auf die Ressource ChargeItem übertragenen Attribute gegen das FHIR-Profil ChargeItem prüfen, auf die Zulässigkeit der änderbaren Felder prüfen:

| | |
|--------------|---|
| Versicherter | darf nur Markierungen (extension ChargeItem.extension:markingFlag) ändern |
|--------------|---|

und bei fehlerhafter Prüfung die Operation mit dem http-Status-Code 400 und einem Hinweis auf unzulässige Änderung gesperrter Attribute in OperationOutcome abbrechen, damit kein Schadcode und keine "fachfremden" Daten in den E-Rezept-Fachdienst hochgeladen werden. [<=]

6.3.4 HTTP-Operation POST

Die FHIR-Operation führt zum Einstellen einer neuen Abrechnungsinformation.

Diese Operation steht für das Einstellen den Apotheken zur Verfügung.

6.3.4.1 POST /ChargeItem

A_22129 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen - Rollenprüfung

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt /ChargeItem sicherstellen, dass ausschließlich Nutzer in der Rolle

- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am E-Rezept-Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit eine Abrechnungsinformation nicht durch Unberechtigte eingestellt werden kann. [<=]

A_22130 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen - Prüfung Parameter Task

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt /ChargeItem sicherstellen, dass ein URL-Parameter "task=..." übermittelt wurde und bei Fehlen des URL-Parameters die Operation mit dem HTTP-Fehlercode 400 abbrechen. [<=]

A_22131 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen - Prüfung Existenz Task

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt /ChargeItem sicherstellen, dass zu der im URL-Parameter "task=..." übertragene Task-ID eine Task Ressource mit dem Status Task.status = completed existiert und bei fehlgeschlagener Prüfung mit dem HTTP-Fehlercode 409 abbrechen, damit nur eine Abrechnungsinformation für E-Rezepte mit dem Status „quittiert“ angelegt wird. [<=]

Aus der Details der Fehlerbeschreibung in OperationOutcome soll für den Nutzer (Angehöriger einer abgebenden LEI) durch eine verständliche Darstellung im Primärsystem hervorgehen, warum die Abgabeinformation nicht bereitgestellt werden kann, damit der Grund dem Versicherten übermittelt werden kann.

A_22132-01 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – Prüfung Secret Task

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt `/ChargeItem` das im URL-Parameter "`secret=...`" übertragene Secret gegen das im referenzierten Task gespeicherte `SecretTask.identifizier:Secret` als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_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 die berechtigten Apotheke in Kenntnis des Secrets erfolgt. [`<=`]

A_22731 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – Prüfung Flowtype Task

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt `/ChargeItem` sicherstellen, dass der im URL-Parameter "`task=...`" referenzierte Task den Flowtype `Task.extension:flowType = 200` oder `209` besitzt und bei fehlgeschlagener Prüfung mit dem HTTP-Fehlercode 400 abbrechen, damit nur eine Abrechnungsinformation für E-Rezepte mit zulässigen Flowtype angelegt wird. [`<=`]

A_22133 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – Prüfung Einwilligung

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt `/ChargeItem` sicherstellen, dass zu der in `ChargeItem.subject.identifizier` übermittelten KVNR ein Consent Datensatz mit `Consent.patient.identifizier = KVNR` und `Consent.category.coding.code = CHARGCONS` existiert und bei fehlgeschlagener Prüfung die Operation mit dem HTTP-Fehlercode 403 abbrechen, damit nur eine Abrechnungsinformation für Versicherte gespeichert wird, die eine Einwilligung erteilt haben. [`<=`]

Aus der Details der Fehlerbeschreibung in `OperationOutcome` soll für den Nutzer (Angehöriger einer abgebenden LEI) durch eine verständliche Darstellung im Primärsystem hervorgehen, warum die Abgabeform nicht bereitgestellt werden kann, damit der Grund dem Versicherten übermittelt werden kann.

A_22136-01 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – FHIR-Validierung ChargeItem

Der E-Rezept-Fachdienst MUSS die im HTTP-POST-Operation auf die Ressource `ChargeItem` übertragene `ChargeItem` Ressource gegen das FHIR-Profil `ChargeItem` prüfen und

- die Korrektheit der Rezept-ID https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_PrescriptionId im referenzierten Task als `ChargeItem.identifizier`,
- die Korrektheit der Versicherten-ID des Versicherten im referenzierten Task (`Task.for`) gegen `ChargeItem.subject.identifizier`
- und die Korrektheit der Telematik-ID der Apotheke gemäß `ACCESS_TOKEN` mit dem Wert in `ChargeItem.enterer.identifizier`

prüfen und bei Nicht-Konformität das Anlegen der Ressource im E-Rezept-Fachdienst mit dem http-Status-Code 400 ablehnen, damit nur FHIR-valide Ressourcen in den E-Rezept-Fachdienst hochgeladen werden. [`<=`]

Der PKV-Abgabedatensatz wird `containedbinary` im Aufruf übermittelt.

A_22137 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – PKV-Abgabedatensatz übernehmen

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt /ChargeItem den im containedbinary übermittelten PKV-Abgabedatensatz herauslösen und entfernen, die Ressource zur ChargeItem Ressource speichern und in ChargeItem.supportingInformation:dispenseItem die Referenz hinzufügen. [<=]

A_22138 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – FHIR-Validierung PKV-Abgabedatensatz

Der E-Rezept-Fachdienst MUSS die im HTTP-POST-Operation auf die Ressource ChargeItem übertragene PKV-Abgabedatensatz Ressource gegen das FHIR-Profil <http://fhir.abda.de/eRezeptAbgabedaten/StructureDefinition/DAV-PKV-PR-ERP-AbgabedatenBundle> prüfen und bei Nicht-Konformität das Anlegen der Ressource im E-Rezept-Fachdienst mit dem http-Status-Code 400 ablehnen, damit nur FHIR-valide Ressourcen in den E-Rezept-Fachdienst hochgeladen werden. [<=]

A_22139 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – Signaturprüfung PKV-Abgabedatensatz

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt /ChargeItem die Signatur des PKV-Abgabedatensatzes gemäß [ETSI_QES] prüfen, und bei fehlender oder nicht gültiger Signatur mit Status 400 abrechnen, um ausschließlich authentische Daten zu verwalten. [<=]

Der PKV-Abgabedatensatz hat QES eines HBAs des Apothekers oder eine nonQES einer SMC-B der Apotheke. Die Zertifikate QES bzw. nonQES werden anhand ihres Zertifikatstyps (Policy-OID) unterschieden.

A_22140 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – Prüfung Signaturzertifikat PKV-Abgabedatensatz

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt /ChargeItem das Signaturzertifikats des PKV-Abgabedatensatzes prüfen. Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig] befunden werden und der Aufruf anderenfalls mit Status 400 abgebrochen werden, um ausschließlich authentische Daten zu verwalten. [<=]

Die Vorgaben für die Prüfung eines QES Zertifikates sind in A_20159-* beschrieben.

A_22141 - E-Rezept-Fachdienst – Signaturzertifikat SMC-B prüfen

Der E-Rezept-Fachdienst MUSS ein Signatur-Zertifikat einer nonQES-Signatur eine Leistungserbringerinstitution gemäß [gemSpec_PKI#TUC_PKI_018] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 9: TAB_eRPFD_xxx Parameter Prüfung Signaturzertifikat SMC-B

| Parameter | |
|--------------------------|-------------------------------|
| Zertifikat | Signaturzertifikat aus nonQES |
| PolicyList | oid_smc_b_osig |
| intendedKeyUsage | nonRepudiation |
| intendedExtendedKeyUsage | (leer) |
| OCSP-Graceperiod | 12 Stunden |

| Parameter | |
|---------------|------|
| Offline-Modus | nein |
| Prüfmodus | OCSP |

Der E-Rezept-Fachdienst darf die OCSP-Response für die Abfrage des Zertifikatsstatus für 12 Stunden zwischenspeichern. [≤]

A_22134 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – Verordnungsdatensatz übernehmen

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt /ChargeItem das E-Rezept-Bundle vom Profil

https://fhir.kbv.de/StructureDefinition/KBV_PR_ERP_Bundle ohne die Signatur zur im URL-Parameter "task=..." übertragenen Task-ID identifizieren und zur ChargeItem Ressource mit dem Identifier PrescriptionID speichern und in ChargeItem.supportingInformation:prescriptionItem die Referenz hinzufügen. [≤]

Für den übernommenen Verordnungsdatensatz gelten nicht die Löschfristen des Tasks, aus dem der Verordnungsdatensatz übernommen wurde.

A_22135-01 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – Quittung übernehmen

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt /ChargeItem das Quittung-Bundle vom

Profil https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Bundle ohne die Signatur zur im URL-Parameter "task=..." übertragenen Task-ID identifizieren und zur ChargeItem Ressource mit dem Identifier PrescriptionID speichern und in ChargeItem.supportingInformation:receipt die Referenz hinzufügen. [≤]

Für die übernommene Quittung gelten nicht die Löschfristen des Tasks, aus dem die Quittung übernommen wurde.

A_22614-01 - E-Rezept-Fachdienst - Abrechnungsinformation bereitstellen - Generierung AccessCode

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf den Endpunkt /ChargeItem eine 256-Bit-Zufallszahl mit einer Mindestentropie von 120 Bit erzeugen, hexadezimal kodieren ([0-9a-f]{64}) und diese im zu speichernden

ChargeItem als externe ID in ChargeItem.identifier:AccessCode als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_AccessCode hinzufügen, damit nachfolgende Zugriffe auf diesen Datensatz nur durch Berechtigte in Kenntnis des AccessCodes erfolgen. [≤]

A_22143 - E-Rezept-Fachdienst – Abrechnungsinformation bereitstellen – ChargeItem befüllen

Der E-Rezept-Fachdienst MUSS beim Erzeugen eines ChargeItem mittels HTTP-POST-Operation die folgenden Elemente schreiben:

- ChargeItem.enteredDate: aktueller Zeitstempel

[≤]

6.3.5 HTTP-Operation PUT

Die FHIR-Operation führt zum Aktualisieren einer unter <Prescription-ID> gespeicherten ChargeItem Ressource.

Diese Operation steht der Apotheke, welche die Abrechnungsinformation bereitgestellt hat, für das Aktualisieren des PKV-Abgabedatensatzes zur Verfügung.

6.3.5.1 PUT /ChargeItem/<id>

A_22144 - E-Rezept-Fachdienst – Abrechnungsinformation ändern – Rollenprüfung

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-PUT-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource sicherstellen, dass ausschließlich Nutzer in der Rolle

- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am E-Rezept-Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit eine Abrechnungsinformation nicht durch Unberechtigte aktualisiert werden kann. [**<=**]

A_22215 - E-Rezept-Fachdienst – Abrechnungsinformation ändern – Prüfung Einwilligung

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-PUT-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource sicherstellen, dass zu der in ChargeItem.subject.identifizier übermittelten KVN ein Consent Datensatz mit Consent.patient.identifizier = KVN und Consent.category.coding.code = CHARGCONS existiert und bei fehlgeschlagener Prüfung die Operation mit dem HTTP-Fehlercode 403 abbrechen, damit nur eine Abrechnungsinformation für Versicherte gespeichert wird, die eine Einwilligung erteilt haben. [**<=**]

A_22146 - E-Rezept-Fachdienst – Abrechnungsinformation ändern – Apotheke - Prüfung Telematik-ID

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-PUT-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource durch eine abgebende Leistungserbringerinstitution (Apotheke), diese anhand der Telematik-ID aus dem ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, diese gegen die im gespeicherten Datensatz in "ChargeItem.enterer.identifizier" hinterlegte Telematik-ID prüfen und bei Ungleichheit den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich die Apotheke, welche die Abrechnungsinformation bereitgestellt hat, als Berechtigte eine Abrechnungsinformation ändert. [**<=**]

A_22616-01 - E-Rezept-Fachdienst – Abrechnungsinformation ändern – Apotheke – Prüfung AccessCode

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-PUT-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource durch eine abgebende Leistungserbringerinstitution (Apotheke), den im URL-Parameter "?ac=..." übertragenen AccessCode gegen den im referenzierten ChargeItem gespeicherten AccessCode ChargeItem.identifizier:AccessCode als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_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_22148 - E-Rezept-Fachdienst – Abrechnungsinformation ändern – Apotheke – PKV-Abgabedatensatz übernehmen

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-PUT-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource durch eine abgebende LEI, den im containedbinary übermittelten PKV-Abgabedatensatz herauslösen und entfernen, die Ressource zur ChargeItem Ressource speichern und in ChargeItem.supportingInformation:dispenseItem die Referenz hinzufügen. [`<=`]

A_22149 - E-Rezept-Fachdienst – Abrechnungsinformation ändern – Apotheke – FHIR-Validierung PKV-Abgabedatensatz

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-PUT-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource durch eine abgebende LEI, die im HTTP-PUT-Operation auf die Ressource ChargeItem übertragene PKV-Abgabedatensatz Ressource gegen das FHIR-Profil PKV-Abgabedatensatz prüfen und bei Nicht-Konformität das Anlegen der Ressource im E-Rezept-Fachdienst mit dem http-Status-Code 400 und einem Hinweis auf die FHIR-Invalidität in OperationOutcome ablehnen, damit nur FHIR-valide Ressourcen in den E-Rezept-Fachdienst hochgeladen werden. [`<=`]

A_22150 - E-Rezept-Fachdienst – Abrechnungsinformation ändern - Apotheke – Signaturprüfung PKV-Abgabedatensatz

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-PUT-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource durch eine abgebende LEI, die Signatur des PKV-Abgabedatensatzes gemäß [ETSI_QES] prüfen, und bei fehlender oder nicht gültiger Signatur mit Status 400 und einem Hinweis auf den die ungültige Signatur in OperationOutcome abrechnen, um ausschließlich authentische Daten zu verwalten. [`<=`]

A_22151 - E-Rezept-Fachdienst – Abrechnungsinformation ändern – Apotheke – Prüfung Signaturzertifikat PKV-Abgabedatensatz

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-PUT-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource durch eine abgebende LEI, das Signaturzertifikats des PKV-Abgabedatensatzes prüfen. Das Signaturzertifikat muss anhand der Zertifikatsprüfung für [mathematisch gültig UND zeitlich gültig UND online gültig] befunden werden und der Aufruf anderenfalls mit Status 400 und einem Hinweis auf das abgelaufene/gesperrte Signaturzertifikat in OperationOutcome abgebrochen werden, um ausschließlich authentische Daten zu verwalten. [`<=`]

Die Vorgaben für die Prüfung eines QES Zertifikates sind in A_20159-* beschrieben. Die Vorgaben für die Prüfung eines nonQES Zertifikates sind in A_22141-* beschrieben.

A_22152 - E-Rezept-Fachdienst - Abrechnungsinformation ändern – FHIR-Validierung ChargeItem

Der E-Rezept-Fachdienst MUSS die im HTTP-PUT-Operation auf die Ressource ChargeItem übertragene ChargeItem Ressource gegen das FHIR-Profil ChargeItem prüfen, auf die Zulässigkeit der änderbaren Felder prüfen:

| | |
|---------------|-------------------------------------|
| abgebende LEI | darf nur PKV-Abgabedatensatz ändern |
|---------------|-------------------------------------|

und bei fehlerhafter Prüfung die Operation mit dem http-Status-Code 400 und einem Hinweis auf unzulässige Änderung gesperrter Attribute in OperationOutcome abrechnen, damit kein Schadcode und keine "fachfremden" Daten in den E-Rezept-Fachdienst hochgeladen werden. [`<=`]

A_22615-01 - E-Rezept-Fachdienst - Abrechnungsinformation ändern - Apotheke - Generierung AccessCode

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-PUT-Operation auf eine konkrete über <id> adressierte /ChargeItem/<id> Ressource durch eine abgebende LEI eine 256-Bit-Zufallszahl mit einer Mindestentropie von 120 Bit erzeugen, hexadezimal kodieren ([0-9a-f]{64}) und diese im zu speichernden ChargeItem als externe ID in ChargeItem.identifizier:AccessCode als https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_AccessCode überschreiben, damit nachfolgende Zugriffe auf diesen Datensatz nur durch Berechtigte in Kenntnis des AccessCodes erfolgen.[<=]

6.4 Ressource Consent

Für das Speichern der Abrechnungsinformationen eines Versicherten im E-Rezept-Fachdienst muss der Versicherte vorab eine Einwilligung erteilen. Für die Übermittlung der Einwilligung wird die FHIR Ressource Consent verwendet.

A_22153 - E-Rezept-Fachdienst - unzulässige Operationen Consent

Der E-Rezept-Fachdienst MUSS alle Zugriffe auf die Ressource Consent mittels der HTTP-Operationen PUT, PATCH, oder HEAD unterbinden, damit keine unzulässigen Operationen auf die Informationen zur Einwilligung ausgeführt werden können.[<=]

6.4.1 HTTP-Operation DELETE

Die Operation führt zum Löschen der für den Versicherten gespeicherten Einwilligung. Diese Operation steht dem Versicherten, der die Einwilligung erteilt hat, zur Verfügung.

A_22154 - E-Rezept-Fachdienst – Consent löschen - alles Löschen verbieten

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-Operation DELETE auf den Endpunkt /Consent ohne Angabe ?category mit dem HTTP-Fehlercode 405 ablehnen, um das Löschen mehrerer Ressourcen über einen Request zu verhindern. [<=]

A_22155 - E-Rezept-Fachdienst - Consent löschen - Rollenprüfung Versicherter

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-Operation DELETE auf den Endpunkt /Consent die Rolle "professionOID" des Aufrufers im ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen und sicherstellen, dass ausschließlich Versicherte in der Rolle oid_versicherter die Operation am E-Rezept-Fachdienst aufrufen dürfen, damit die Information zur Einwilligung nicht durch Unberechtigte gelöscht werden kann.[<=]

A_22874-01 - E-Rezept-Fachdienst - Consent löschen - Prüfung category

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-Operation DELETE auf den Endpunkt /Consent prüfen, dass der für ?category angegebene Wert im System https://gematik.de/fhir/erpchrg/CodeSystem/GEM_ERPCHRG_CS_ConsentType enthalten ist und bei fehlerhafter Prüfung den Request mit dem Fehler 400 abbrechen, damit nur Löschrequests für definierte Consent Typen ausgeführt werden.[<=]

A_22157 - E-Rezept-Fachdienst - Consent löschen - Löschen der bestehenden Abrechnungsinformationen

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-Operation DELETE auf den Endpunkt /Consent mit ?category=CHARGCONS alle dem Versicherten zugeordneten ChargeItem-Ressourcen (ChargeItem.subject.identifizier) anhand der KVNR des

Versicherten im ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren und löschen. [≤]

Für das Löschen der Abrechnungsinformationen ist "A_22117-* - E-Rezept-Fachdienst - Abrechnungsinformation löschen - zu löschende Ressourcen" zu beachten.

A_22158 - E-Rezept-Fachdienst - Consent löschen - Löschen der Consent

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-Operation DELETE auf den Endpunkt `/Consent` die Ressource löschen, bei der `Consent.patient.identifizier` der KVNR aus dem ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests sowie `Consent.category.coding.code` dem in `?category` übermittelten Wert entspricht. [≤]

6.4.2 HTTP-Operation GET

Mit der FHIR-Operation kann die Consent Ressource für die im ACCESS_TOKEN angegebene KVNR abgerufen werden. Diese Operation steht Versicherten zur Verfügung.

A_22159 - E-Rezept-Fachdienst - Consent lesen - Rollenprüfung Versicherter

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Consent` sicherstellen, dass ausschließlich Versicherte in der Rolle `oid_versicherter` die Operation am E-Rezept-Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit die Information zur Einwilligung nicht durch Unberechtigte ausgelesen werden kann. [≤]

A_22160 - E-Rezept-Fachdienst - Consent lesen - Filter Consent auf KVNR des Versicherten

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Consent` die dem Versicherten zugeordneten Consent-Ressourcen anhand der KVNR des Versicherten im ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren und in den Response aufnehmen, die in `Consent.Patient.identifizier` die entsprechende KVNR des begünstigten Versicherten referenziert haben, damit ausschließlich Versicherte ihre eigenen Information zu Einwilligungen einsehen können. [≤]

6.4.3 HTTP-Operation POST

Die FHIR-Operation führt zum Schreiben einer neuen Einwilligung. Diese Operation steht Versicherten zur Verfügung.

A_22161 - E-Rezept-Fachdienst - Consent schreiben - Rollenprüfung Versicherter

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-POST-Operation auf den Endpunkt `/Consent` sicherstellen, dass ausschließlich Versicherte in der Rolle `oid_versicherter` die Operation am E-Rezept-Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit eine Einwilligung nicht durch Unberechtigte erteilt werden kann. [≤]

A_22289 - E-Rezept-Fachdienst - Consent schreiben - Prüfung KVNR

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-POST-Operation auf den Endpunkt `/Consent` sicherstellen, dass die KVNR im ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests und die KVNR in `Consent.patient.identifizier` übereinstimmen, damit eine Einwilligung für einen Versicherten nicht durch Dritte erteilt werden kann. Im Fehlerfall muss der Http-Request mit dem Http-Fehlercode 403 abgewiesen werden. [≤]

A_22351 - E-Rezept-Fachdienst - Consent schreiben - FHIR-Validierung

Der E-Rezept-Fachdienst MUSS die im HTTP-POST-Operation auf die Ressource Consent übertragene Consent Ressource gegen das FHIR-Profil Consent prüfen und bei Nicht-Konformität das Anlegen der Ressource im E-Rezept-Fachdienst mit dem http-Status-Code 400 ablehnen, damit nur FHIR-valide Ressourcen in den E-Rezept-Fachdienst hochgeladen werden. [≤]

A_22162 - E-Rezept-Fachdienst - Consent schreiben – nur eine Einwilligung CHARGCONS pro KVNR

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-POST-Operation auf den Endpunkt /Consent sicherstellen, dass noch keine Consent Ressource für die KVNR im ACCESS_TOKEN und `Consent.category.coding.code = CHARGCONS` gespeichert ist, um maximal eine Einwilligung für den Versicherten zu speichern. Im Fehlerfall muss der Http-Request mit dem Http-Fehlercode 409 abgewiesen werden. [≤]

A_22350 - E-Rezept-Fachdienst - Consent schreiben – Persistieren

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-POST-Operation auf den Endpunkt /Consent – falls bei den Prüfungen keine Fehler aufgetreten sind, welche zum Abbruch der Operation führen – die übermittelte Ressource persistieren. [≤]

6.5 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 und HEAD unterbinden, damit keine unzulässigen Operationen auf den Kommunikationsnachrichten ausgeführt werden können. [≤]

A_19446-01 - E-Rezept-Fachdienst - Rollenprüfung Versicherter oder Apotheker nutzt Nachrichten

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-GET, DELETE und POST-Operation auf den Endpunkt `/Communication` bzw. `/Communication/<id>` 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 ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit der Nachrichtenaustausch nicht zwischen Unbefugten erfolgt. [≤]

6.5.1 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 ACCESS_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.

6.5.1.1 GET /Communication/

A_19520-01 - E-Rezept-Fachdienst - Nachrichten abrufen - 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` oder `Communication.sender` mit dem entsprechenden Identifier <https://gematik.de/fhir/sid/telematik-id> für Apotheken bzw. <http://fhir.de/sid/gkv/kvid-10> oder <http://fhir.de/sid/pkv/kvid-10> für Versicherte den gleichen Typ und den identischen Wert haben wie im Attribut "idNummer" des übergebenen ACCESS_TOKEN im HTTP-Header "Authorization" für Versicherten-ID 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 Filtermöglichkeit auf "neue Nachrichten" haben. [<=]

A_19522-01 - 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> mindestens für die Attribute

- `Communication.sent`,
- `Communication.received`,
- `Communication.recipient` und
- `Communication.sender` erlauben,

damit Versicherte eine Suche nach neuen Nachrichten, Sende- bzw. Empfangsrichtung und eine Sortierung nach Sende- und Empfangsdatum durchführen können. [<=]

A_19534-01 - E-Rezept-Fachdienst - Rückgabe Communication im Bundle Paging

Der E-Rezept-Fachdienst KANN beim Aufruf der HTTP-GET-Operation auf den Endpunkt `/Communication` das Suchergebnis in einem Paging-Mechanismus auf mehrere Ergebnis-Bundle aufteilen, damit der Nutzer eine komfortable Navigationsmöglichkeit in seinen Nachrichten erhält. [<=]

6.5.2 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.

6.5.2.1 POST /Communication/

A_19447-04 - 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 10: TAB_eRPFD_008 Nachrichtentyp zu Kommunikationsbeziehung

| sender | recipient | zusätzliche Bedingung | Schema |
|-------------|-------------|---|---|
| KVNR | TelematikID | Communication.basedOn referenziert Task | https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_DispReq |
| KVNR | TelematikID | Communication.about referenziert Medication Communication.basedOn referenziert Task | https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_InfoReq |
| TelematikID | KVNR | Communication.basedOn referenziert Task | https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_Reply |
| KVNR | KVNR | Communication.basedOn referenziert Task | https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_Representative |
| KVNR | TelematikID | Communication.basedOn referenziert ChargeItem | https://gematik.de/fhir/erpchrg/StructureDefinition/GEM_ERPCHRG_PR_Communication_ChargChangeReq |
| TelematikID | KVNR | Communication.basedOn referenziert ChargeItem | https://gematik.de/fhir/erpchrg/StructureDefinition/GEM_ERPCHRG_PR_Communication_ChargChangeReply |

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

A_19448-01 - 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 "idNummer" des übergebenen IDP-Token im HTTP-Header "Authorization" mit dem

entsprechenden System <https://gematik.de/fhir/sid/telematik-id> für Apotheken bzw. <http://fhir.de/sid/gkv/kvid-10> oder <http://fhir.de/sid/pkv/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_20229-01 - E-Rezept-Fachdienst - Nachricht einstellen - Nachrichtenzähler bei Versicherter-zu-Versichertem-Kommunikation

Der E-Rezept-Fachdienst MUSS die zulässige Anzahl der Communication-Ressourcen des Schemas https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_Representative 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 außerhalb der Vertretung in der Einlösung von E-Rezepten benutzen. [`<=`]

A_20511 - E-Rezept-Fachdienst - Nachrichtenzähler zweckgebunden

Der E-Rezept-Fachdienst DARF die Anzahl der Communication-Ressourcen je referenziertem Task für die Versicherter-zu-Versichertem-Kommunikation NICHT zu anderen Zwecken verwenden, als für die Beschränkung der Anzahl auf den maximalen Wert. [`<=`]

A_20230-01 - E-Rezept-Fachdienst - Nachricht einstellen - Einlösbare E-Rezepte für Versicherter-zu-Versichertem-Kommunikation

Der E-Rezept-Fachdienst MUSS beim Einstellen einer Nachricht des Schemas https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_Representative 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 "idNummer" des übergebenen IDP-Token im HTTP-Header "Authorization" ist, damit irreführende Kommunikationsbeziehungen nicht zu einer vermeidbaren Mehrbelastung des E-Rezept-Fachdienstes führen. [`<=`]

A_19450-01 - 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
- in von Versicherten eingestellten Nachrichten in `Communication.payload` eine externe URLs enthält oder
- ein Attachment mit MimeType "application/*" enthält,

damit über den E-Rezept-Fachdienst kein Schadcode verteilt wird.
[<=]

A_20885-03 - E-Rezept-Fachdienst - Nachricht einstellen - Versicherte - Prüfung Versichertenbezug und Berechtigung

Der E-Rezept-Fachdienst MUSS das Einstellen einer Nachricht des Profils "https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_DispReq", "https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_InfoReq" oder "https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_Representative" durch einen Versicherten über die http-Operation POST auf den Endpunkt/*Communication* mit dem http-Status-Code 400 abbrechen, wenn

- die KVN-Nummer des in *Communication.basedOn* referenzierten Tasks *Task.for* ungleich der KVN-Nummer des Einstellenden in "*idNummer*" des übergebenen *ACCESS_TOKEN*

und

- der http-Header "X-AccessCode" fehlt oder der im http-Header "X-AccessCode" übergebene *AccessCode* ungleich dem *AccessCode-Identifizierer* des referenzierten Tasks

ist, um irreführende Testnachrichten zu unterbinden, die eine vermeidbare Mehrbelastung für den E-Rezept-Fachdienst darstellen. [≤]

A_21371-02 - E-Rezept-Fachdienst - Nachricht einstellen - Prüfung Existenz Task

Der Fachdienst E-Rezept MUSS beim Einstellen einer Nachricht des Profils "https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_DispReq", "https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_InfoReq", "https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_Reply" oder "https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_Representative" über die http-Operation POST auf den Endpunkt/*Communication* mit dem http-Status-Code 400 abbrechen, wenn das Pflichtfeld *Communication.basedOn* einen Task referenziert, der nicht existiert, um Spam und nicht-rezeptbezogene Kommunikation zu verhindern. [≤]

A_22734-01 - E-Rezept-Fachdienst - Nachricht einstellen - Prüfung Existenz ChargeItem

Der Fachdienst E-Rezept MUSS beim Einstellen einer Nachricht des Profils "https://gematik.de/fhir/erpchrg/StructureDefinition/GEM_ERPCHRG_PR_Communication_ChargChangeReq" oder "https://gematik.de/fhir/erpchrg/StructureDefinition/GEM_ERPCHRG_PR_Communication_ChargChangeReply" über die http-Operation POST auf den Endpunkt/*Communication* mit dem http-Status-Code 400 abbrechen, wenn das Pflichtfeld *Communication.basedOn* einen *ChargeItem* referenziert, der nicht existiert, um Spam und nicht-rezeptbezogene Kommunikation zu verhindern. [≤]

A_22367-02 - E-Rezept-Fachdienst - Nachricht einstellen - Notification Apotheke

Der E-Rezept-Fachdienst MUSS beim Einstellen einer Nachricht des Profils "https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_DispReq", "https://gematik.de/fhir/erp/StructureDefinition/GEM_ERP_PR_Communication_InfoReq" oder "https://gematik.de/fhir/erpchrg/StructureDefinition/GEM_ERPCHRG_PR_Communication_ChargChangeReq" zur Versicherter-zu-Apotheken-Kommunikation über die http-Operation POST auf den Endpunkt/*Communication* prüfen, ob für die Telematik-ID des Empfängers Subscriptions registriert sind und für Registrierungen über den Subscription Service eine Notification (ping : subscription-id) senden.[<=]

6.5.3 HTTP-Operation DELETE

Mit der HTTP-Operation DELETE kann ein Nutzer eine verschickte Kommunikationsnachricht als Absender löschen, um bspw. einen Irrläufer zurückzurufen. Der E-Rezept-Fachdienst prüft, ob die Nachricht bereits abgerufen wurde. Das Löschen einer ungelesenen Nachricht erfolgt sofort, das Löschen einer bereits abgerufenen Nachricht wird vom E-Rezept-Fachdienst mit einer Warnung umgesetzt, um darauf hinzuweisen, dass die Nachricht als Kopie im Clientsystem des Empfängers vorliegt und das Löschen nicht vor unberechtigter Einsichtnahme schützt.

Um den Schutz vor unberechtigter Einsichtnahme in persönliche Daten durchzusetzen, ist es ratsam bei bereits gelesenen Nachrichten den referenzierten E-Rezept-Task zu löschen. Für eine geeignete Nutzerführung auf Clientseite ergänzt der E-Rezept-Fachdienst die http-Response um das Header-Attribut "Warning" mit einem entsprechenden Hinweis. Das Löschen des Task führt direkt auch zum Löschen aller Kommunikationsnachrichten, die auf diesen Task verweisen. Damit kann ein fälschlich adressierter Vertreter eines Versicherten keine Einsicht in die Daten des E-Rezepts mehr nehmen bzw. das E-Rezept in keiner Apotheke mehr einlösen.

6.5.3.1 DELETE /Communication/

A_20258 - E-Rezept-Fachdienst - Communication löschen auf Basis Absender-ID

Der E-Rezept-Fachdienst MUSS beim Aufruf der HTTP-DELETE-Operation auf /*Communication*/*<id>* die über *<id>* identifizierte Communication-Ressource anhand der KVN- bzw. Telematik-ID des aufrufenden Nutzers im ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests über das Absender-Attribut *Communication.sender* lokalisieren und löschen, damit Nutzer irrtümlich versendete oder nicht mehr gewünschte Nachrichten vom E-Rezept-Fachdienst entfernen können.[<=]

A_20259 - E-Rezept-Fachdienst - Communication löschen mit Warnung wenn vom Empfänger bereits abgerufen

Der E-Rezept-Fachdienst MUSS beim Löschen einer Communication-Ressource der http-Response das http-Header-Feld "Warning" mit dem Zeitpunkt des Nachrichtenabrufs durch den Empfänger ergänzen (z.B. "Warning: 'Deleted message delivered at 2020-07-01 10:30:00'"), wenn die Nachricht bereits durch den Empfänger abgerufen wurde (*Communication.received* ungleich NULL, bzw. enthält Datum des Abrufs), um dem Absender einen Hinweis anzeigen zu können.[<=]

6.6 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. 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, DELETE und POST unterbinden, damit keine unzulässigen Operationen auf den Protokolldaten ausgeführt werden können. [<=]

6.6.1 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 `ACCESS_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 `ACCESS_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 Zugriffsprotokoll erhält. [<=]

6.7 Ressource Device

Gemäß CapabilityStatement und FHIR-Profilierung stellt der E-Rezept-Fachdienst statische Informationen über seine Produkttypversion zur Verfügung. Mit diesen erhalten Clients eine entsprechende Auskunft und bei Bedarf das Signaturzertifikat C.FD.OSIG für die Signaturprüfung, für welches der E-Rezept-Fachdienst serverseitige Signaturen für die E-Rezept-Quittung, PKV-Abgabeinformationen und den E-Rezept-Datensatz für Versicherte erstellt.

A_20744 - E-Rezept-Fachdienst - Selbstauskunft Device-Informationen

Der E-Rezept-Fachdienst MUSS über die http-Operation GET /Device dem aufrufenden Clientsystem eine statische Auskunft gemäß der Profilierung der Device-Ressource bereitstellen. [<=]

6.8 Ressource Subscription

6.8.1 HTTP-Operation POST

A_22362 - E-Rezept-Fachdienst – Subscription registrieren – Rollenprüfung Apotheke

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf die /Subscription Ressource sicherstellen, dass ausschließlich Nutzer in der Rolle

- oid_oeffentliche_apotheke
- oid_krankenhausapotheke

die Operation am E-Rezept-Fachdienst aufrufen dürfen und die Rolle "professionOID" des Aufrufers im ACCESS_TOKEN im HTTP-RequestHeader "Authorization" feststellen, damit eine Subscription nicht durch Unberechtigte registriert werden kann. [<=]

A_22363 - E-Rezept-Fachdienst – Subscription registrieren – Prüfung Telematik-ID

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf die /Subscription Ressource durch eine abgebende Leistungserbringerinstitution (Apotheke), diese anhand der Telematik-ID aus dem ACCESS_TOKEN im "Authorization"-Header des HTTP-Requests identifizieren, diese gegen die in der Ressource im Element `criteria` Attribut `recipient` hinterlegte Telematik-ID prüfen und bei Ungleichheit den Aufruf mit dem HTTP-Fehlercode 403 abweisen, damit ausschließlich die Apotheke für sich selbst eine Subscription registrieren kann. [<=]

A_22364 - E-Rezept-Fachdienst – Subscription registrieren – Response

Der E-Rezept-Fachdienst MUSS beim Aufruf der Http-POST-Operation auf die /Subscription Ressource mit einem Response antworten, welcher eine Subscription Ressource mit

- Pseudonym der Telematik-ID in `id`
- aktueller Timestamp + 12 h in `end`
- Bearer Token in `Authorization`

enthält. [<=]

Beispiel:

```
<Subscription>
  <id
```

```
value="838dabe4e05416c776d60256c511558f6831f679c613f203d30b58b05555618a"/>
  <status value="active"/>
  <end value="2021-01-01T00:00:00Z"/>
  <criteria value="Communication?received=null&recipient=3-
05.2.1001000000.381"/>
  <channel>
    <type value="websocket"/>
    <header value="Authorization: Bearer secret-token-abc-123"/>
  </channel>
</Subscription>
```

Hinweis: Der Header wird beim Web Socket Upgrade durch den Client an den Subscription Service übermittelt.

A_22365 - E-Rezept-Fachdienst – Subscription registrieren – Pseudonym der Telematik-ID

Der E-Rezept-Fachdienst MUSS das Pseudonym innerhalb der VAU mittels eines 128-Bit-AES-CMAC-Schlüssels erstellen und hexadezimal kodieren (32 Byte lang) (vgl gemSpec_Krypt#A_20163).[<=]

A_22383-01 - E-Rezept-Fachdienst – Generierungsschlüssel – Pseudonym der Telematik-ID

Der E-Rezept-Fachdienst MUSS den AES-CMAC-Schlüssel zur Pseudonymgenerierung regelmäßig mindestens alle 3 Monate ändern.

[<=]

A_22366 - E-Rezept-Fachdienst – Subscription registrieren – Barrier-Token

Der E-Rezept-Fachdienst MUSS für die Registrierung der Subscription einen Bearer-Token mit den Claims

- subscriptionid: Pseudonym der Telematik-ID
- iAt: Timestamp wann Subscription erstellt wurde
- exp: Timestamp Ablauf der Subscription

erstellen und mit einer Identität des E-Rezept-Fachdienstes signieren (Signature Algorithm: ES256).[<=]

Hinweise:

Das Signaturzertifikat muss nicht aus der Komponenten-PKI der TI abgeleitet werden.

Es wird kein fester Turnus festgelegt, in dem der Schlüssel gewechselt wird. Ein Wechsel kann über betriebliche Prozesse initiiert werden.

Der Schlüssel für die Signatur muss sicher gespeichert, jedoch nicht zwingend im HSM abgelegt werden.

6.9 Subscription Service

Der Subscription Service wird außerhalb der VAU betrieben.

A_22368 - E-Rezept-Fachdienst - Subscription Service - Webschnittstelle

Der E-Rezept-Fachdienst MUSS eine Webschnittstelle anbieten, welche Websocket-Verbindungen mit einer Dauer von bis zu 12 h unterstützt.[<=]

A_22369 - E-Rezept-Fachdienst - Subscription Service - Prüfung Bearer-Token

Der E-Rezept-Fachdienst MUSS an der Webschnittstelle des Subscription Service beim Verbindungsaufbau prüfen, dass der Client einen zeitlich und kryptographisch gültigen Bearer-Token der Schnittstelle `GET /Subscription` übermittelt und bei nicht-erfolgreicher Prüfung die Verbindung mit dem Fehler 403 ablehnen. [`<=`]

A_22370 - E-Rezept-Fachdienst - Subscription Service - Upgrade

Der E-Rezept-Fachdienst MUSS an der Webschnittstelle des Subscription Service beim Verbindungsaufbau ein Upgrade durchführen. [`<=`]

A_22371 - E-Rezept-Fachdienst - Subscription Service - abgelaufene Verbindungen schließen

Der E-Rezept-Fachdienst MUSS an der Webschnittstelle des Subscription Service sicherstellen, dass Verbindungen nach Überschreiten des Timestamp Ablauf der Subscription geschlossen werden. [`<=`]

A_22378 - E-Rezept-Fachdienst - Subscription Service - Verbot Profilbildung

Der E-Rezept-Fachdienst DARF in der Verbindung zum Subscription Service anfallende Metadaten (Client-IP-Adresse, etc.) NICHT für eine unbefugte Profilbildung der verbundenen Clients verwenden. [`<=`]

Hinweis: Eine Verwendung zur Sicherung der Schnittstelle (DDoS-Schutz, Fehleranalyse in sehr eingeschränktem Maß) ist zulässig (im Sinne einer befugten Profilbildung).

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 Leistungserbringereinstitution (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.

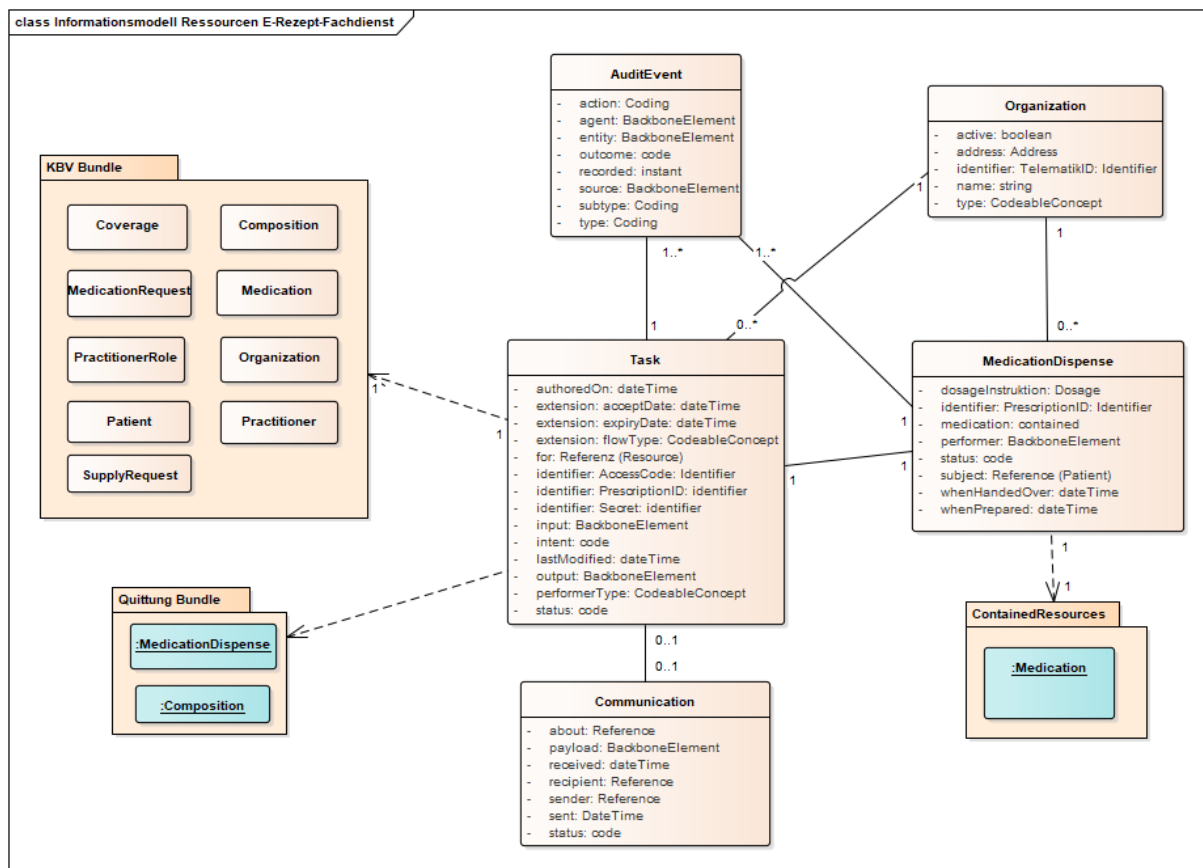


Abbildung 3: Informationsmodell FHIR-Ressourcen E-Rezept-Fachdienst

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 | Telematikinfrastuktur |
| 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 | 9 |
| Abbildung 2: Systemkontext E-Rezept-Fachdienst | 10 |
| Abbildung 3: Informationsmodell FHIR-Ressourcen E-Rezept-Fachdienst | 90 |

8.4 Tabellenverzeichnis

| | |
|---|----|
| Tabelle 1: TAB_eRPFD_005 Parameter Prüfung Signaturzertifikat IDP | 17 |
| Tabelle 2: TAB_eRPFD_010 Parameter Prüfung Signaturzertifikat | 18 |
| Tabelle 3: TAB_eRPFD_003 Übersicht HTTP-Statuscodes | 19 |
| Tabelle 4: TAB_eRPFD_004 Versichertenprotokoll | 24 |
| Tabelle 5: TAB_eRPFD_007 Löschrufen Task | 27 |
| Tabelle 6: Zugriffserlaubnisse | 28 |
| Tabelle 7 : Struktur VSDM Prüfziffer | 48 |
| Tabelle 8 : TAB_eRPFD_006 Parameter Prüfung Signaturzertifikat QES des HBA..... | 52 |
| Tabelle 9: TAB_eRPFD_009 Parameter Prüfung Signaturzertifikat SMC-B | 73 |
| Tabelle 10: TAB_eRPFD_008 Nachrichtentyp zu Kommunikationsbeziehung | 81 |

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 |
| [gemSpec_DM_eRp] | gematik: Spezifikation Datenmodell E-Rezept |
| [gemSpec_eRp_FdV] | gematik: Spezifikation E-Rezept-Frontend des Versicherten |
| [gemSpec_IDP_Dienst] | gematik: Spezifikation Identity Provider-Dienst |
| [gemSpec_IDP_FD] | gematik: Spezifikation Identity Provider – Nutzungsspezifikation für Fachdienste |
| [gemSpec_Krypt] | gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur |
| [gemSpec_OID] | gematik: Spezifikation Festlegung von OIDs |
| [gemSpec_Perf] | gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform |
| [gemSpec_PKI] | gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform |
| [gemSpec_TSL] | gematik: Spezifikation TSL-Dienst |

8.5.2 Weitere Dokumente

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
|------------|---|
| [BÄK_G0] | Zertifikatsprofile für X.509 Basiszertifikate, Version 2.3.2, Bundesärztekammer Revisions-Datum.: 16.05.2011 https://docplayer.org/13121506-Zertifikatsprofile-fuer-x-509-basiszertifikate-version-2-3-2.html |
| [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 |

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
|---------------------|---|
| [RFC5652] | Cryptographic Message Syntax (CMS), RFC 5652 (September 2009) https://tools.ietf.org/html/rfc5652 |
| [CAAdES] | 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 Ressourcen Versionierung https://www.hl7.org/fhir/valueset-versioning-policy.html |
| [HTTP-STATUS-CODES] | HTTP-Status-Code 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 |