

Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation E-Rechnung Fachdienst

Version: 1.1.0\_CC  
Revision: 1151311  
Stand: 03.03.2025  
Status: zur Abstimmung  
freigegeben  
Klassifizierung: öffentlich\_Entwurf  
Referenzierung: gemSpec\_eRg\_FD

---

## 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
			aufgrund der Technikanpassung wurde V1.0.0 erweitert auf V1.1.0	gematik
1.1.0_CC	03.03.2025		<ul style="list-style-type: none"><li>- Berücksichtigung des aktuellen Standes der Zero Trust Architektur der TI (ZETA).</li><li>- Platzierung des Rechnungstoken als 2D Barcode auf jeder Seite des Rechnungs-PDF</li><li>- Unterstützung elektronischer Zahlungen</li></ul>	gematik

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Dokumentes.....</b>	<b>5</b>
1.1 Zielsetzung.....	5
1.2 Zielgruppe.....	5
1.3 Geltungsbereich.....	5
1.4 Abgrenzungen.....	5
1.5 Methodik.....	6
<b>2 Systemüberblick.....</b>	<b>7</b>
<b>3 Systemkontext.....</b>	<b>9</b>
3.1 Zugang zum Fachdienst in der TI.....	9
3.2 Autorisierte Nutzergruppen und Rollen.....	9
3.2.1 Claims.....	10
3.2.2 Scopes.....	10
<b>4 Zerlegung des Produkttyps.....</b>	<b>12</b>
<b>5 Übergreifende Festlegungen.....</b>	<b>13</b>
<b>5.1 Datenschutz und Informationssicherheit.....</b>	<b>13</b>
5.1.1 Protokollierung für die Versicherten.....	15
5.1.2 Löschfristen.....	15
5.1.2.1 Nutzerkonten.....	15
5.1.2.2 Rechnungen und Dokumente.....	16
5.1.3 Vertrauenswürdige Ausführungsumgebung.....	16
5.1.3.1 Verarbeitungskontext.....	17
5.1.3.2 Verarbeitung schützenswerter Daten.....	17
5.1.3.3 Persistierung schützenswerter Daten.....	18
5.1.3.4 Transport schützenswerter Daten.....	18
5.1.3.5 Schutz der Integrität der VAU.....	19
5.1.3.6 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld.....	21
5.1.3.7 Einbinden des ZETA Guard der gematik.....	22
5.1.3.8 Konsistenz des Systemzustands, Logging und Monitoring.....	24
5.1.4 Dateigrößen.....	24
5.1.5 Dokumentenformate.....	25
5.1.6 Nutzerprotokoll.....	25
5.1.6.1 Rechnungen.....	25
5.1.6.2 Berechtigungen.....	26
5.1.6.3 Markierungen.....	26
5.1.6.4 Nutzerkonten.....	26
<b>5.2 RESTful API.....</b>	<b>26</b>
<b>5.3 FHIR-Ressourcen.....</b>	<b>27</b>
<b>5.4 FHIR-Endpunkte und -Operations.....</b>	<b>28</b>
5.4.1 RE-PS als Akteur.....	28

5.4.1.1 Abfrage Rechnungsempfänger und dessen Einwilligung zum Rechnungsversand.....	28
5.4.1.2 Rechnung validieren und einreichen.....	28
5.4.1.3 Rechnung validieren/einreichen (Bulk).....	29
5.4.1.4 Abfrage von Daten zu Rechnungen und Dokumenten per Token.....	29
5.4.1.5 Abfrage von angereicherten PDFs per Token (Bulk).....	30
5.4.2 FdV als Akteur.....	30
5.4.2.1 Abrufen/Suchen von Rechnungen.....	30
5.4.2.2 Abfrage von Daten zu Rechnungen und Dokumenten per Token.....	30
5.4.2.3 Statuswechsel.....	31
5.4.2.4 Markieren von Rechnungen und Dokumenten.....	31
5.4.2.5 Löschen eines Rechnungsvorgangs.....	32
5.4.2.6 Nutzerprotokoll einsehen.....	32
5.4.3 KTR als Akteur.....	32
5.4.3.1 Abfrage von Daten zu Rechnungen und Dokumenten per Token.....	32
<b>5.5 Weitere REST-Endpunkte.....</b>	<b>33</b>
<b>5.6 Nutzerregistrierung.....</b>	<b>33</b>
5.6.1 Institutionen.....	33
5.6.2 Versicherte.....	34
<b>5.7 Benachrichtigungen.....</b>	<b>34</b>
<b>5.8 Interne Fehlercodes.....</b>	<b>34</b>
<b>6 Informationsmodell.....</b>	<b>37</b>
6.1 FHIR-Ressourcen.....	37
6.2 Zugriffsprotokoll.....	37
6.3 Rechnungs- oder Dokumenten-Token.....	38
6.3.1 Zufallswert.....	38
6.3.2 Darstellung als Barcode.....	39
6.4 Angereichertes PDF.....	39
6.5 Signatur.....	40
<b>7 Verteilungssicht.....</b>	<b>41</b>
<b>8 Anhang A - Verzeichnisse.....</b>	<b>42</b>
8.1 Abkürzungen.....	42
8.2 Glossar.....	42
8.3 Abbildungsverzeichnis.....	43
8.4 Tabellenverzeichnis.....	43
8.5 Referenzierte Dokumente.....	43
8.5.1 Dokumente der gematik.....	43
8.5.2 Weitere Referenzen.....	44

---

## 1 Einordnung des Dokumentes

---

### 1.1 Zielsetzung

Die vorliegende Spezifikation definiert die fachlichen Anforderungen zur Herstellung des Produkttyps E-Rechnung Fachdienst. Sie dient als Ergänzung und Detaillierung der konzeptionellen Beschreibung der Anwendung E-Rechnung im Feature Dokument [gemF\_E-Rechnung].

### 1.2 Zielgruppe

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

### 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. gemPTV\_ATV\_Festlegungen, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekanntgegeben.

#### Schutzrechts-/Patentrechtshinweis

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

### 1.4 Abgrenzungen

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 8).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, u.a. zu den Bereichen Infrastruktur und Betrieb sowie Authentifizierung und Autorisierung über Zero Trust Komponenten. Diese werden in dem Produkttypsteckbrief des Produkttyps eRg FD verzeichnet, der zu einem späteren Zeitpunkt zur Verfügung gestellt wird.

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum Themenbereich des Frontend der Versicherten der Anwendung E-Rechnung (eRg FdV). Hierzu wird zu einem späteren Zeitpunkt ein weiteres Spezifikationsdokument sowie ein Produkttypsteckbrief für den Produkttyp eRg FdV erstellt.

## 1.5 Methodik

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

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

Anwendungsfälle und Anforderungen werden im Dokument wie folgt dargestellt:

**<AF-ID> - <Titel des Anwendungsfalles>**

Text / Beschreibung

[<=]

bzw.

**<AFO-ID> - <Titel der Afo>**

Text / Beschreibung

[<=]

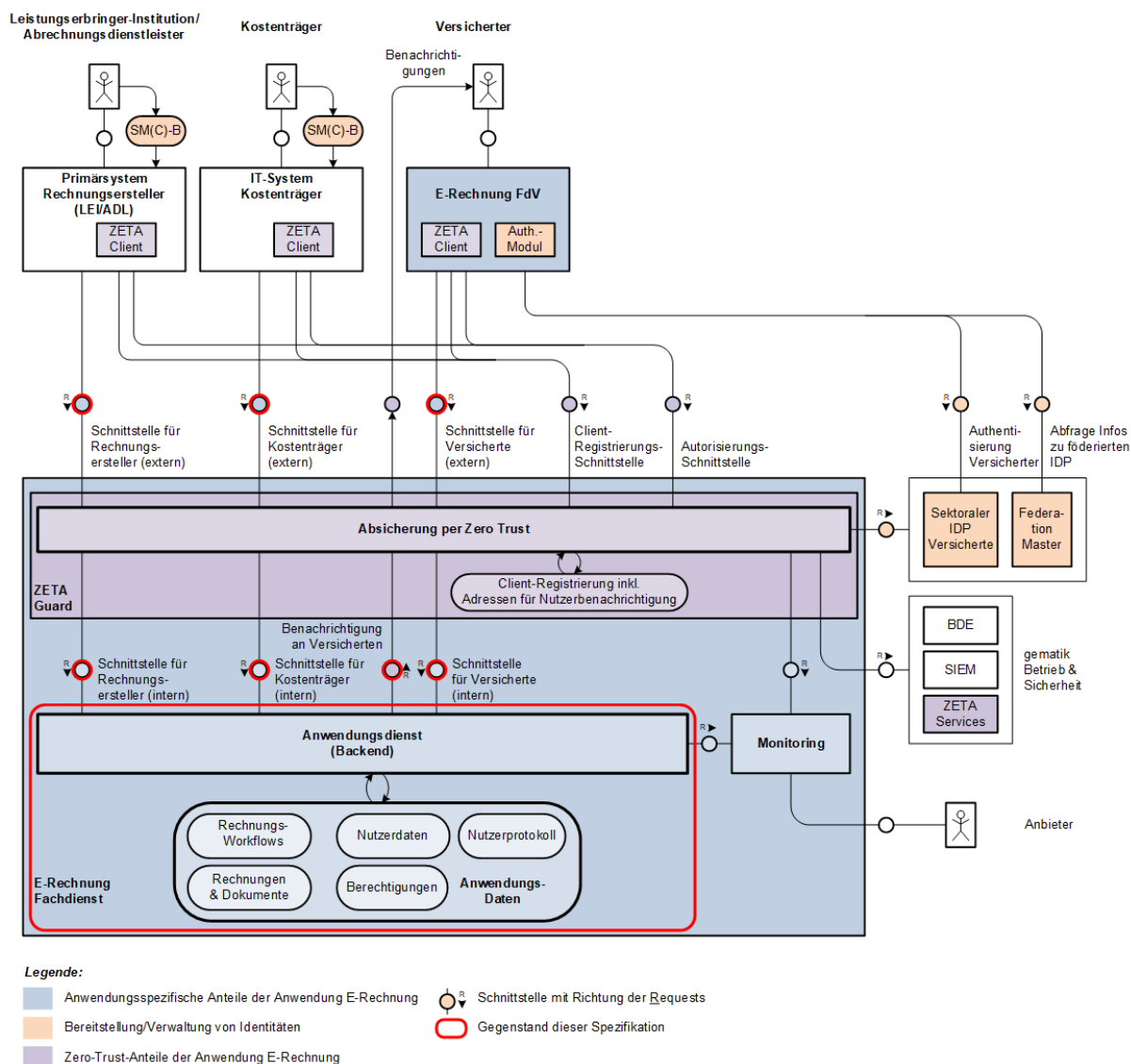
Dabei umfasst der Anwendungsfall bzw. die Anforderung sämtliche zwischen ID und Textmarke [<=] angeführten Inhalte.

### FHIR Spezifikation

Des Weiteren wird im Dokument über AFOs auf die Spezifikation der Operationen und Datenstrukturen in FHIR referenziert. Die referenzierten Festlegungen zu FHIR sind auf [simplifier.net](https://www.simplifier.net) [Simplifier eRg] verfügbar und dort über einen Implementation Guide dokumentiert. Sie werden während der Auftragsvergabe und Umsetzung zusammen mit dem Auftragnehmer im Rahmen der jeweils geltenden Anforderungslage weiterentwickelt und stellen in der aktuellen Version mitgeltende Bestandteile der vorliegenden Spezifikation dar.

## 2 Systemüberblick

Das folgende Bild zeigt die funktionale Aufteilung des Fachdienstes sowie die Schnittstellen zu den Client-Systemen und weiteren benötigten Diensten (siehe auch [gemF\_E-Rechnung#5.1 Zerlegung des Fachdienstes]).



**Abbildung 1 Funktionaler Aufbau der Anwendung E-Rechnung**

Des Weiteren ist dargestellt, welche funktionalen Anteile und Schnittstellen des E-Rechnung Fachdienstes im Rahmen dieser Spezifikation beschrieben werden. Nur die rot umrandeten Anteile des Fachdienstes sind Gegenstand dieser Spezifikation, d.h. Anforderungen an folgende Gegenstände werden hier nicht oder nur teilweise erfasst. Dies betrifft

- betriebliche Anforderungen wie z.B. das Betriebsdaten-Monitoring,

- die Absicherung des Fachdienstes per Zero Trust-Architektur (ZETA) und
- Anforderungen an die sichere, vertrauenswürdige Ausführungsumgebung.

Anforderungen zu den oben aufgeführten Gegenständen ergeben sich aus referenzierten Dokumenten bzw. den Anforderungen aus mitgeltenden Dokumenten gemäß Produkttypsteckbrief des Fachdienstes.



---

## 3 Systemkontext

---

Entsprechend der Beteiligung der Nutzergruppen der E-Rechnung sind die jeweils genutzten IT-Systeme in die Gesamtlösung zu integrieren (für mehr Details siehe [gemF\_E-Rechnung#3]).

### 3.1 Zugang zum Fachdienst in der TI

Der Zugang für die Nutzergruppen und die von ihnen genutzten Client-Systeme wird auf unterschiedliche Weise umgesetzt:

#### Institutionen (Rechnungsersteller und Kostenträger)

Der Zugriff erfolgt über das Internet, abgesichert nach dem Zero Trust-Ansatz, siehe [gemSpec\_ZETA]. Da die Authentisierung der Institutionen in der ersten Version der E-Rechnung mit der SMC-B bzw. HSM-B erfolgt, müssen diese über eine Anbindung mittels zugelassener dezentraler Komponenten verfügen:

- Konnektor oder
- Basis-Consumer oder
- TI Gateway (mit High Speed Konnektor)

Für die Anwendung E-Rechnung (eRg) ist kein Fachmodul für den Konnektor oder den Basis-Consumer vorgesehen.

Eine Zusammenstellung der verschiedenen möglichen TI-Zugangslösungen findet sich in [gemF\_E-Rechnung#Anhang A].

#### Versicherte

Der Zugriff erfolgt über das Internet, abgesichert nach dem Zero Trust-Ansatz, siehe [gemSpec\_ZETA].

### 3.2 Autorisierte Nutzergruppen und Rollen

Leistungserbringerinstitutionen (LEI), Abrechnungsdienstleister (ADL), Kostenträger (KTR) und Versicherte, die auf den E-Rechnung Fachdienst zugreifen möchten, müssen zuvor autorisiert werden. Dabei erfolgt eine rollenbasierte Berechtigungsprüfung durch den Autorisierungsdienst des Fachdienstes, wobei nur bestimmten Nutzergruppen der Zugriff in der jeweils zulässigen Rolle auf die Anwendung eRg gewährt wird. Diese Prüfung basiert auf der OID (Object Identifier) des Nutzers, die bei der Anmeldung mittels GesundheitsID (Versicherte) oder SM(C)-B (Institutionen) ermittelt wird.

#### A\_26020 - E-Rechnung Fachdienst - Erlaubte Nutzergruppen und Rollen

Der E-Rechnung Fachdienst MUSS sicherstellen, dass bei der Autorisierung ausschließlich die in der Tabelle angegebenen Nutzergruppen und OIDs Zugriff erhalten dürfen und darauf basierend die folgenden Rollen zugewiesen werden müssen.

**Tabelle 1 Erlaubte Nutzergruppen und Rollen**

Nutzergruppe	OID <sup>1</sup> (gemäß [gemSpec_OID])	Rolle
--------------	--	-------

Versicherter	oid_versicherter	Rechnungsempfänger, Rechnungseinreicher
Leistungserbringereinstitution	oid_zahnarztpraxis oid_praxis_arzt oid_oeffentliche_apotheke	Rechnungsersteller
Abrechnungsdienstleister	oid_abrechnungsdienstleister	Rechnungsersteller
Kostenträger	oid_kostentraeger	Kostenträger

<sup>1</sup>Die Auflistung der zulässigen OIDs ist abschließend, wird jedoch ggf. bei weiteren Ausbaustufen erweitert, um die autorisierten Nutzergruppen zu erweitern. [≤]

### 3.2.1 Claims

#### A\_26026 - E-Rechnung Fachdienst - Autorisierte Nutzergruppen und Rollen - Claims

Der E-Rechnung Fachdienst MUSS die Claims verwenden, die in [gemF\_E-Rechnung] beschrieben sind. [≤]

### 3.2.2 Scopes

Der E-Rechnung Fachdienst verwendet Scopes, die sich im Aufbau an den Empfehlungen von [SMART on FHIR] orientieren. Diese bestehen aus dem Namen des Datenobjekts, gefolgt von einem "." und eine Liste an Berechtigungen. Die Liste der Berechtigungen besteht in der Reihenfolge aus den Buchstaben "c" = "create", "r" = "read", "u" = "update", "d" = "delete" und "s" = "search", sofern zutreffend. Ein Scope, der das Lesen und Aktualisieren einer Rechnung erlaubt, würde wie folgt lauten:

invoiceDoc.ru

#### A\_26027 - E-Rechnung Fachdienst - Autorisierte Nutzergruppen und Rollen - Scopes

Der E-Rechnung Fachdienst MUSS zur Prüfung der Autorisierung bei Aufrufen die Scopes verwenden, welche wie folgt den Rollen zugeordnet sind:

**Tabelle 2: Rollen und Scopes**

Rolle	Zugriffsberechtigung	Scope
Rechnungsersteller	Daten des Rechnungsempfängers lesen	insurantAccount.rs
	E-Rechnungen (mit Dokumenten) anlegen	invoiceDoc.c
	Angereichertes Dokument abrufen	invoiceDoc.r
	Eigenes Nutzerkonto anlegen, lesen, bearbeiten und löschen	practitionerAccount.crud
Rechnungsempfänger	E-Rechnungen (mit Dokumenten) lesen, bearbeiten <sup>1</sup> , löschen und	invoiceDoc.ruds

	suchen	
	Angereichertes Dokument abrufen	invoiceDoc.r
	Eigenes Nutzerkonto anlegen, lesen, bearbeiten und löschen	insurantAccount.crud
	Einträge des Nutzerprotokolls lesen und suchen	auditEvent.rs
	Berechtigungen lesen, bearbeiten und löschen	permission.rud
Kostenträger	E-Rechnungen (mit Dokumenten) lesen	invoiceDoc.r
	Angereichertes Dokument abrufen	invoiceDoc.r
	Eigenes Nutzerkonto anlegen, lesen, bearbeiten und löschen	insuranceAccount.crud

[&lt;=]

**Hinweise:**

<sup>1</sup> Das "Bearbeiten" von Dokumenten und E-Rechnungen beschränkt sich auf die Bearbeitung von ergänzenden Metadaten, z.B. eine Markierung als ungelesen oder gelesen. Die eigentlichen E-Rechnungen und Dokumente werden unverändert gespeichert und übertragen.

---

## 4 Zerlegung des Produkttyps

---

Eine weitere Untergliederung der Aufbaustruktur des Produkttyps ist nicht erforderlich.

---

## 5 Übergreifende Festlegungen

---

### 5.1 Datenschutz und Informationssicherheit

Dieser Abschnitt enthält die anwendungsfallübergreifenden Datenschutz- und Sicherheitsanforderungen an den E-Rechnung Fachdienst bzw. seinen Hersteller sowie Anbieter/Betreiber.

#### Allgemeine Anforderungen

Der Hersteller des E-Rechnung Fachdienstes muss die Anforderungen aus dem Abschnitt "Sicherer Softwareentwicklungsprozess" sowie die Anforderungen aus dem Abschnitt "Unterstützung von Audits" des Dokuments [gemSpec\_DS\_Hersteller] erfüllen. Die konkreten Anforderungen sind im Produkttypsteckbrief aufgeführt.

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

#### A\_25907 - E-Rechnung Fachdienst - Umgang mit Prüfidentitäten

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Prüfidentitäten nicht auf Daten von echten Personen oder Institutionen zugreifen können und dass echte Personen oder Institutionen nicht auf Daten von Prüfidentitäten zugreifen können. [≤=]

Hinweis: Eine eGK-Prüfkartenidentität kann anhand der Bildungsregel X0000nnnnP, mit nnnn aus der Menge {0001 .. 5000} und P = Prüfziffer für die KVNR der Prüfkarte eGK erkannt werden.

Für die Gesamtsicherheit der Anwendung E-Rechnung ist es bedeutsam, dass der E-Rechnung Fachdienst nur zugelassene – und damit sicherheitsgeprüfte – Frontends des Versicherten (FdVs) den Zugriff auf Daten ermöglicht. Dies wird durch Komponenten der Zero Trust-Architektur sichergestellt.

Die Gliederung der folgenden Anforderungen orientiert sich an den Schutzzielen des Datenschutzes und der Informationssicherheit.

#### Vertraulichkeit

Die Vertraulichkeit der im E-Rechnung Fachdienst verarbeiteten personenbezogenen medizinischen Daten wird durch

- die Verschlüsselung der Daten beim Transport in den E-Rechnung Fachdienst und aus dem E-Rechnung Fachdienst sowie zwischen den Komponenten des Fachdienstes (data in motion),
- die vertrauliche Verarbeitung im E-Rechnung Fachdienst (data in use, siehe Anforderungen zur VAU in Abschnitt 5.1.3- Vertrauenswürdige Ausführungsumgebung),
- und die verschlüsselte Speicherung im E-Rechnung Fachdienst (data at rest, siehe Anforderungen zur VAU in Abschnitt 5.1.3- Vertrauenswürdige Ausführungsumgebung)

gewährleistet. Die kryptographischen Vorgaben für die umzusetzenden Maßnahmen (insbes. TLS) sind in [gemSpec\_Krypt] formuliert.

### **A\_25911 - Umsetzung der fachlichen Operationen in einer VAU**

Der E-Rechnung Fachdienst MUSS die Verarbeitung aller fachlichen Operationen des Fachdienstes in einer VAU umsetzen. [≤]

### **Integrität**

Die von LE bzw. Abrechnungsdienstleistern (ADL) eingestellten Rechnungen werden nach der Übertragung in den Fachdienst mit der Identität des E-Rechnung Fachdienstes signiert. Ein Client, der Dokumente abrufen kann, kann damit im Nachhinein die Integrität einer Rechnung prüfen. Details zur Signatur finden sich im Abschnitt 6.5- Signatur.

### **Verfügbarkeit**

Die Verfügbarkeit des E-Rechnung Fachdienstes wird über die betrieblichen Anforderungen geregelt.

### **Transparenz**

Der E-Rechnung Fachdienst führt Zugriffsprotokolle für die Versicherten, in denen alle Zugriffe auf die personenbezogenen (medizinischen) Daten eines Versicherten für den Versicherten einsehbar sind. Die Protokolleinträge müssen enthalten, wer wann in welchem Use Case (auf was) zugegriffen hat. Die Einträge müssen in einer leicht verständlichen Sprache formuliert sein.

Die Anforderungen zur Protokollierung sind in Abschnitt 6.2 formuliert.

### **Nichtverkettbarkeit**

### **A\_25914 - E-Rechnung Fachdienst - Verbot unbefugter Profilbildung aus personenbezogenen Daten**

Der Anbieter des E-Rechnung Fachdienstes DARF im E-Rechnung Fachdienst verarbeitete personenbezogene Daten NICHT für eine unbefugte Profilbildung verwenden. [≤]

Diese Anforderung gilt explizit auch für Verbindungsdaten, die durch die Kommunikation von Clients der Nutzer mit dem Fachdienst entstehen.

### **A\_25913 - E-Rechnung Fachdienst - Verbot unbefugter Profilbildung aus Verbindungsdaten**

Der Anbieter des E-Rechnung Fachdienstes DARF anfallende Verbindungsdaten (Client-IP-Adresse, etc.) NICHT für eine unbefugte Profilbildung der verbundenen Clients bzw. ihrer Nutzer verwenden. [≤]

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

### **Intervenierbarkeit**

Die Nutzung der Anwendung E-Rechnung ist für alle Beteiligten freiwillig. Die Versicherten geben ihre Einwilligung in die Nutzung der Anwendung über das FdV und der Fachdienst muss diese Information speichern.

### **A\_25918 - E-Rechnung Fachdienst - Anlegen Nutzerkonto nur bei Einwilligung**

Der E-Rechnung Fachdienst DARF NICHT ein Nutzerkonto für einen Nutzer anlegen, wenn ihm dessen Einwilligung in die Nutzung der Anwendung E-Rechnung nicht vorliegt. [≤]

### **A\_25919 - E-Rechnung Fachdienst - Einwilligung speichern**

Der E-Rechnung Fachdienst MUSS die Einwilligung eines Nutzers in die Nutzung der Anwendung E-Rechnung speichern. [≤]

Widerruft ein Nutzer die Einwilligung zur Nutzung der Anwendung, muss sein Nutzerkonto und die damit verbundenen Daten im Fachdienst gelöscht werden. Andersherum ist

die Löschung eines Nutzerkontos durch den Nutzer gleichbedeutend mit dem Widerruf der Einwilligung in die Anwendung E-Rechnung.

### **A\_25920 - E-Rechnung Fachdienst - Daten löschen bei Widerrufung der Einwilligung**

Der E-Rechnung Fachdienst MUSS alle Daten von und über einen Nutzer löschen, wenn ein Nutzer die Einwilligung in die Nutzung der Anwendung E-Rechnung widerruft. [≤]

Versicherte haben die Möglichkeit für sie im Fachdienst gespeicherte Rechnungen zu löschen.

### **A\_25921 - E-Rechnung Fachdienst - Löschen von Rechnungen durch den Versicherten**

Der E-Rechnung Fachdienst MUSS es Versicherten ermöglichen, ihre Rechnungen im E-Rechnung Fachdienst zu löschen. [≤]

### **Datenminimierung**

### **A\_25915 - E-Rechnung Fachdienst - Zweckbestimmte Verarbeitung von Daten**

Der E-Rechnung Fachdienst DARF NICHT Daten verarbeiten, die nicht dem rechtmäßigen Zweck der Anwendung dienen. [≤]

Die Anforderungen zu Löschrufen sind im Abschnitt 5.1.2 formuliert.

## **5.1.1 Protokollierung für die Versicherten**

Der E-Rechnung Fachdienst führt Zugriffsprotokolle für die Versicherten, in denen alle Zugriffe auf die personenbezogenen (medizinischen) Daten eines Versicherten für den Versicherten einsehbar sind. Diese Zugriffsprotokolle sind unabhängig von technischen Protokollen und stehen ausschließlich dem Versicherten zur Wahrnehmung seiner Betroffenenrechte zur Einsicht zur Verfügung.

Die Anforderungen zum Nutzerprotokoll sind im Abschnitt 5.1.6 formuliert.

## **5.1.2 Löschrufen**

Der E-Rechnung Fachdienst soll datensparsam umgesetzt werden. Das bedeutet, dass personenbezogene Daten und nicht mehr benötigte Daten nach folgend definierten Fristen gelöscht werden.

### **A\_27457 - E-Rechnung Fachdienst - Löschrufen - Möglichkeit der Konfiguration**

Der E-Rechnung Fachdienst MUSS die Möglichkeit bieten, Löschrufen dynamisch konfigurieren zu können, d.h. ohne dass ein erneutes Deployment erforderlich ist. [≤]

### **5.1.2.1 Nutzerkonten**

### **A\_25675 - E-Rechnung Fachdienst - Löschrufen - Nutzerkonten - Löschrufen inaktiver Nutzerkonten**

Der E-Rechnung Fachdienst MUSS Nutzerkonten sowie deren verknüpften Daten, Dokumente, Workflows und Protokolle automatisch zum Ende des laufenden Monats löschen, wenn diese 1 Jahr inaktiv waren. [≤]

### **A\_25676 - E-Rechnung Fachdienst - Löschrufen - Nutzerkonten - Benachrichtigung vor Löschrufen**

Der E-Rechnung Fachdienst MUSS den Nutzer automatisch 3 Monate vor der Löschrufen des Nutzerkontos per Benachrichtigung über diese informieren, so dass dieser sich anmelden kann, um die Löschrufen zu vermeiden. [≤]

### **A\_25682 - E-Rechnung Fachdienst - Löschrufen - Nutzerkonten - Erinnerung vor Löschrufen**

Der E-Rechnung Fachdienst MUSS den Nutzer automatisch 2 Wochen vor der Löschung des Nutzerkontos per Benachrichtigung an die bevorstehende Löschung erinnern. [≤]

### 5.1.2.2 Rechnungen und Dokumente

#### **A\_25677 - E-Rechnung Fachdienst - Löschfristen - Rechnungen und Dokumente - Papierkorb für OFFEN**

Der E-Rechnung Fachdienst MUSS Rechnungen 3 Jahre nach der Rechnungserstellung automatisch zum nächsten Jahresende in den Status PAPIERKORB ändern. [≤]

#### **A\_25678 - E-Rechnung Fachdienst - Löschfristen - Rechnungen und Dokumente - Verlängerung**

Der E-Rechnung Fachdienst MUSS Rechnungen 3 Jahre nach Wechsel in den Status OFFEN zum nächsten Jahresende automatisch in den Status PAPIERKORB ändern. [≤]

#### **A\_26132 - E-Rechnung Fachdienst - Löschfristen - Rechnungen und Dokumente - Papierkorb für ERLEDIGT**

Der E-Rechnung Fachdienst MUSS Rechnungen ein Jahr nach Wechsel in den Status ERLEDIGT zum nächsten Monatsende automatisch in den Status PAPIERKORB ändern. [≤]

#### **A\_25833 - E-Rechnung Fachdienst - Löschfristen - Rechnungen und Dokumente - Gesamtaufbewahrungsdauer**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Rechnungen trotz Verlängerungen der Löschfrist spätestens 10 Jahre nach Erstellung automatisch endgültig gelöscht werden. [≤]

#### **A\_25679 - E-Rechnung Fachdienst - Löschfristen - Rechnungen und Dokumente - Löschen**

Der E-Rechnung Fachdienst MUSS Rechnungen sowie die verknüpften, strukturierten Daten und Dokumente 3 Monate nach dem Wechsel in den Status PAPIERKORB zum nächsten Monatsende automatisch löschen. [≤]

#### **A\_25694 - E-Rechnung Fachdienst - Löschfristen - Rechnungen und Dokumente - Benachrichtigung vor Löschung**

Der E-Rechnung Fachdienst MUSS den Nutzer bei einem Wechsel in den Status PAPIERKORB per Benachrichtigung über diese informieren, so dass dieser die Löschfrist verlängern kann. [≤]

#### **A\_25695 - E-Rechnung Fachdienst - Löschfristen - Rechnungen und Dokumente - Erinnerung vor Löschung**

Der E-Rechnung Fachdienst MUSS den Nutzer automatisch 2 Wochen vor der Löschung von Rechnungen in dem Status PAPIERKORB per Benachrichtigung an die bevorstehende Löschung erinnern. [≤]

### 5.1.3 Vertrauenswürdige Ausführungsumgebung

In diesem Abschnitt werden die Anforderungen an den E-Rechnung Fachdienst (eRg FD) zur Umsetzung einer Vertrauenswürdigen Ausführungsumgebung (VAU) dargestellt. Die VAU dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten Klartextdaten innerhalb des eRg FD 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.



### 5.1.3.1 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 VAU 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-Rechnung-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\_27407 - E-Rechnung Fachdienst - Verarbeitungskontext der VAU**

Der Verarbeitungskontext des E-Rechnung 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. [≤]

### 5.1.3.2 Verarbeitung schützenswerter Daten

#### **A\_27464 - E-Rechnung Fachdienst - Klartext-Datenverarbeitung ausschließlich im Verarbeitungskontext**

Der E-Rechnung Fachdienst MUSS technisch sicherstellen, dass eine Klartext-Verarbeitung von schützenswerten Daten ausschließlich innerhalb eines Verarbeitungskontextes erfolgt. [≤]

#### **A\_27465 - E-Rechnung Fachdienst - Isolation zwischen Datenverarbeitungsprozessen**

Der E-Rechnung Fachdienst MUSS technisch sicherstellen, dass Datenverarbeitungsprozesse einer Client-Session keinen Zugriff auf Datenverarbeitungsprozesse einer anderen Client-Session ermöglichen können und je nach gewählter Form der Umsetzung von Client-Sessions (bspw. als Thread eines http-Servers) eine entsprechend gehärtete Implementierung einsetzen. [≤]

#### **A\_27466 - E-Rechnung Fachdienst - Löschen aller schützenswerten Daten beim Beenden eines Verarbeitungskontextes**

Der Verarbeitungskontext des E-Rechnung Fachdienstes MUSS sicherstellen, dass beim Beenden eines Verarbeitungskontextes sämtliche schützenswerten Daten dieses Verarbeitungskontextes aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [≤]

### 5.1.3.3 Persistierung schützenswerter Daten

#### **A\_27408 - E-Rechnung Fachdienst - Verschlüsselung von außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten**

Der Verarbeitungskontext des E-Rechnung Fachdienstes MUSS sicherstellen, dass sämtliche schützenswerten Daten vor einer Speicherung außerhalb der VAU verschlüsselt werden. Der Verarbeitungskontext MUSS dazu mindestens einmal pro Sekunde den verwendeten Schlüssel wechseln, so dass nur die innerhalb einer Sekunde neu angelegten E-Rechnungen mit einem Schlüssel verschlüsselt werden. [≤]

**A\_27409 - E-Rechnung Fachdienst - Ableitung der Persistenzschlüssel durch ein HSM**

Der Verarbeitungskontext des E-Rechnung Fachdienstes MUSS die zur Verschlüsselung der persistierten E-Rechnungsdaten verwendeten Schlüssel von einem HSM abrufen, in dem mindestens eine Partition ausschließlich für die Verwendung mit der VAU des E-Rechnung Fachdienstes konfiguriert ist.

[<=]

**A\_27410 - E-Rechnung Fachdienst - Ableitung der Persistenzschlüssel aus Merkmal der E-Rechnungen**

Das HSM der VAU des E-Rechnung Fachdienstes MUSS eine Schnittstelle zur Ableitung von symmetrischen Schlüsseln für die Persistierung von E-Rechnungsdaten bereitstellen. Das HSM der VAU des E-Rechnung Fachdienstes MUSS zur Ableitung des jeweiligen Schlüssels einen bei der ersten Erstellung im Verarbeitungskontext ermittelten und anschließend unveränderlichen Zeitstempel des jeweiligen zu speichernden Datensatzes als Ableitungsparameter verwenden.[<=]

**5.1.3.4 Transport schützenswerter Daten****A\_25908 - E-Rechnung Fachdienst - Schutz der in die VAU des Fachdienstes transportierten Daten**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass die Kommunikation zwischen Clients und dem E-Rechnung Fachdienst ausschließlich authentisiert, vertraulich und integritätsgeschützt erfolgt.[<=]

Für den Ausschluss des Anbieters/Betreibers des E-Rechnung Fachdienstes vom Zugriff auf die zwischen Clients und E-Rechnung Fachdienst transportierten personenbezogenen medizinischen Daten muss der Endpunkt dieser Kommunikation in der Vertrauenswürdigen Ausführungsumgebung (VAU) des E-Rechnung Fachdienstes liegen.

**A\_25909 - E-Rechnung Fachdienst - Endpunkt der Transportsicherung in der VAU des Fachdienstes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass der Endpunkt der transportgeschützten Kommunikation zwischen Clients und dem E-Rechnung Fachdienst in der VAU liegt.[<=]

**A\_25910 - E-Rechnung Fachdienst - Schutz der innerhalb des Fachdienstes transportierten Daten**

Der Anbieter des E-Rechnung Fachdienstes MUSS die zwischen den Komponenten des E-Rechnung Fachdienstes auszutauschenden Daten vertraulich und integritätsgeschützt übertragen.[<=]

**A\_25912 - E-Rechnung Fachdienst - Umsetzung der Operationen für das Protokoll der Versicherten in einer VAU**

Der E-Rechnung Fachdienst MUSS die Verarbeitung aller Operationen des Fachdienstes für das Protokoll der Versicherten in einer VAU umsetzen.[<=]

*Hinweis: für die Qualität der Transportverschlüsselung gelten die Anforderungen aus [gemSpec\_Krypt].*

**A\_27422 - E-Rechnung Fachdienst - Sicherer Kanal vom Client zum Verarbeitungskontext der VAU**

Die VAU des E-Rechnung 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.[<=]

**A\_27411 - E-Rechnung Fachdienst - Authentisierung gegenüber Clients**

Der Verarbeitungskontext des E-Rechnung Fachdienstes MUSS sich gegenüber Clients, die mit ihm kommunizieren, mittels der Fachdienstidentität `oid_erg-vau` mit Zertifikatsprofil C.FD.ENC (`oid_fd_enc`) ausweisen. [≤]

## **A\_27412 - E-Rechnung Fachdienst - Isolation zwischen Datenverarbeitungsprozessen der VAU**

Die VAU des E-Rechnung Fachdienstes MUSS die in ihr ablaufenden Verarbeitungen für die Daten einer Client-Session von den Verarbeitungen für die Daten anderer Client-Sessions in solcher Weise trennen, dass mit technischen Mitteln ausgeschlossen ist, dass aus einer (ggf. kompromittierten) Client-Session auf Daten einer anderen Client-Session zugegriffen werden kann. [≤]

Um Verbindungen vom E-Rechnung Client 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 vermittelt die Verbindungen zwischen dem Client und dem jeweils benötigten Verarbeitungskontext.

## **A\_27425 - E-Rechnung Fachdienst - Verarbeitungskontexte der VAU über gemeinsame Host-Adressen erreichbar**

Die VAU des E-Rechnung Fachdienstes MUSS ihre Verarbeitungskontexte über gemeinsame IP-Adressen und Ports des Eingangspunkts des Fachdienstes erreichbar machen. [≤]

## **A\_27427 - E-Rechnung Fachdienst - Automatisierter Abbau des sicheren Kanals**

Der Verarbeitungskontext des E-Rechnung 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. [≤]

### **5.1.3.5 Schutz der Integrität der VAU**

#### **A\_27454 - E-Rechnung Fachdienst - Remote Attestation beim Start eines Verarbeitungskontextes**

Der Verarbeitungskontext des E-Rechnung Fachdienstes MUSS unmittelbar nach seinem Start gegenüber einem Attestationsdienst der VAU nachweisen, dass er aus einem autorisierten und unveränderten VAU-Image initialisiert wurde. [≤]

*Hinweis: Der Verarbeitungskontext wird als ein "VAU-Image" geladen. Hierbei kann es sich um ein VM-Image oder einen Container o. Ä. handeln. Ein VAU-Image kann nur erfolgreich attestiert werden, wenn seine Attestationsmesswerte (Hashwert des Images im Arbeitsspeicher, bestimmte Konfigurationseinstellungen des Hosts bzw. der CPU, Signer-ID der CPU bzw. des TPM, etc.) zuvor beim Attestationsdienst als gültige Referenzwerte registriert wurden.*

#### **A\_27471 - E-Rechnung Fachdienst - Betreiber-unabhängiger Root of Trust for Measurement**

Der Betreiber der Infrastruktur des E-Rechnung Fachdienstes MUSS attestationsfähige Server-Hardware einsetzen, die erzeugte Attestation-Reports mit in der Hardware verankertem Schlüsselmaterial signiert, das nicht in der Hoheit des Betreibers liegt. [≤]

*Hinweis: Dies können Schlüssel in den CPUs der Server handeln (z. B. Intel Root of Trust for Measurement) oder in TPMs sein.*

#### **A\_27472 - E-Rechnung Fachdienst - Kontrollierte Lieferkette für VAU-Server**

Der Betreiber der Infrastruktur des E-Rechnung Fachdienstes MUSS Server einsetzen, für die eine Kompromittierung der Hardware, der Firmware oder des integrierten Schlüsselmaterials ausgeschlossen werden kann. [≤]

**A\_27455 - E-Rechnung Fachdienst - Erfolgreiche Attestation als Vorbedingung für Zugriff des Verarbeitungskontextes auf Schlüsselmaterial**

Der Remote Attestation Mechanismus des E-Rechnung Fachdienstes MUSS gewährleisten, dass Verarbeitungskontexte erst nach erfolgreichem Nachweis ihrer Autorisierung und Integrität gegenüber dem Attestationsdienst die Möglichkeit zum Zugriff auf das für die Authentisierung als E-Rechnung Fachdienst gegenüber Clients oder das Ver- bzw. Entschlüsseln der schützenswerten persistenten Daten erforderliche Schlüsselmaterial erlangen.[<=]

**A\_27467 - E-Rechnung Fachdienst - Sichere Verbindung zwischen Verarbeitungskontext und Attestationsdienst**

Die VAU des E-Rechnung Fachdienstes MUSS technisch sicherstellen, dass zwischen einem Verarbeitungskontext der VAU und dem Attestationsdienst eine beidseitig authentifizierte und vertrauliche Verbindung besteht, die auch gegen Zugriffe durch den Anbieter des Fachdienstes bzw. den Betreiber der Infrastruktur schützt.[<=]

**A\_27468 - E-Rechnung Fachdienst - Sichere Verbindung zwischen Verarbeitungskontext und HSM**

Die VAU des E-Rechnung Fachdienstes MUSS technisch sicherstellen, dass Verbindungen zwischen einem Verarbeitungskontext der VAU und dem HSM, die für die Nutzung von für den Verarbeitungskontext erforderlichem Schlüsselmaterial benötigt werden, beidseitig authentifziert und vertraulich sind und auch gegen Zugriffe durch den Anbieter des Fachdienstes bzw. den Betreiber der Infrastruktur schützen.[<=]

**A\_27469 - E-Rechnung Fachdienst - Sichere Verbindung zwischen Attestationsdienst und HSM**

Die VAU des E-Rechnung Fachdienstes MUSS technisch sicherstellen, dass nur der im Rahmen der Einrichtung der VAU im 4-Augen-Prinzip mit der gematik autorisierte Attestationsdienst Zugriff auf das für ihn erforderliche Schlüsselmaterial im HSM erhalten kann.[<=]

**A\_27456 - E-Rechnung Fachdienst - Registrierung von Referenzwerten im 4-Augen Prinzip**

Der Anbieter des E-Rechnung Fachdienstes MUSS die Registrierung von Referenzwerten für die Attestation von Verarbeitungskontexten unter Beteiligung der gematik in solcher Weise durchführen, dass unautorisierte Veränderungen seitens des Betreibers oder des Herstellers der VAU-Images ausgeschlossen sind.[<=]

**A\_27470 - E-Rechnung Fachdienst - Regelmäßiger Neustart von Verarbeitungskontexten**

Der E-Rechnung Fachdienst MUSS Instanzen des Verarbeitungskontextes der VAU spätestens eine Stunde nach ihrem jeweiligen Start neu starten, um die Attestation zu erneuern.[<=]

**5.1.3.6 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld**

Der Schutzbedarf der im Verarbeitungskontext 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\_27413 - E-Rechnung Fachdienst - Isolation der VAU von Datenverarbeitungsprozessen des Anbieters und des Betreibers**

Die VAU des E-Rechnung Fachdienstes MUSS die in ihren Verarbeitungskontexten ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters und des Betreibers der zugrundeliegenden Infrastruktur trennen und damit gewährleisten, dass der Anbieter und der Betreiber des

E-Rechnung Fachdienstes vom Zugriff auf die in der VAU verarbeiteten schützenswerten Daten ausgeschlossen ist. [ $\leq$ ]

*Hinweis: Für die Separation zwischen Verarbeitungskontexten und Verarbeitungsprozessen des Anbieters und des Bertreibers, 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\_27414 - E-Rechnung Fachdienst - Ausschluss von Manipulationen an der Software der VAU**

Die VAU des E-Rechnung Fachdienstes MUSS eine Manipulation der eingesetzten Software erkennen und eine Ausführung der manipulierten Software verhindern. [ $\leq$ ]

## **A\_27415 - E-Rechnung Fachdienst - Ausschluss von Manipulationen an der Hardware der VAU**

Die VAU des E-Rechnung Fachdienstes MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter des E-Rechnung-Fachdienstes ausschließen. [ $\leq$ ]

## **A\_27416 - E-Rechnung Fachdienst - Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU**

Die VAU des E-Rechnung Fachdienstes MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter des E-Rechnung Fachdienstes mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann. [ $\leq$ ]

## **A\_27417 - E-Rechnung Fachdienst - Kein physischer Zugang des Anbieters zu Systemen der VAU**

Die VAU des E-Rechnung Fachdienstes MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter des E-Rechnung-Fachdienstes oder der Betreiber der den Fachdienst ausführenden Infrastruktur, während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird. [ $\leq$ ]

## **A\_27418 - E-Rechnung Fachdienst - Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU**

Die VAU des E-Rechnung 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. [ $\leq$ ]

## **A\_27419 - E-Rechnung Fachdienst - Private Schlüssel von Dienstzertifikaten im HSM**

Der E-Rechnung 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-Rechnung Frontend des Versicherten (eRg FdV) und Primärsystemen (sicherer Kanal auf Anwendungsebene).

Die Prüftiefe des HSM MUSS dabei den in A\_27420 angegebenen Standards entsprechen. [ $\leq$ ]

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

## **A\_27420 - E-Rechnung Fachdienst - Einsatz zertifizierter HSM**

Der Anbieter des E-Rechnung 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\_27421 - E-Rechnung Fachdienst - HSM-Kryptographieschnittstelle verfügbar nur für Instanzen der VAU**

Die VAU des E-Rechnung Fachdienstes MUSS mit technischen Mitteln, die auch Manipulationen durch den Anbieter des E-Rechnung 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.*

### **5.1.3.7 Einbinden des ZETA Guard der gematik**

Der E-Rechnung Fachdienst verwendet als TI 2.0-Service die Mechanismen des Zero Trusts für die Zugriffskontrolle. Dazu wird von der gematik zentral ein Software-Image für den ZETA Guard bereitgestellt, der von den Diensten der TI 2.0 eingebunden wird.

Da der von der gematik bereitgestellte ZETA Guard ein reines Docker-Image ist, muss es vom Hersteller Proof of Patient Presence (PoPP) in die Lage versetzt werden, als VAU-Image in der VAU des PoPP-Service importiert werden zu können und dort lauffähig zu sein.

Der ZETA Guard ist also so im Build-Prozess zu berücksichtigen, dass dieser ohne manuelle Anpassungen am Code automatisiert integriert werden kann. Da häufige Updates des ZETA Guard zu erwarten sind (insbesondere schnelle Patches bei neuen, relevanten CVE), ist ein manueller Anpassungsprozess zur Herstellung der Kompatibilität des ZETA Guard zur VAU des PoPP-Service inakzeptabel.

Im Folgenden wird das System, dass den Prozess zur Erzeugung von VAU-Images umsetzt und dabei automatisiert den ZETA Guard einbindet VAU-Image-Build-Pipeline genannt.

### **A\_27583 - E-Rechnung Fachdienst - Bereitstellung VAU-Image-Build-Pipeline und automatisiertes Einbinden des ZETA Guard**

Der Hersteller des E-Rechnung Fachdienst MUSS eine VAU-Image-Build-Pipeline bereitstellen und nutzen, von der:

1. das seitens gematik bereitgestellte ZETA Guard-Image entgegengenommen wird, wobei:
  - a. die gematik-Signatur des Images gegen den als vertrauenswürdig hinterlegten gematik-Signatur-Prüf Schlüssel verifiziert wird und
  - b. das Image genau nur bei erfolgreicher Signaturprüfung übernommen wird, und anschließend automatisiert:
1. entweder aus der E-Rechnung Fachdienst-Logik und dem ZETA Guard-Image ein gemeinsames VAU-Image erzeugt wird



2. oder aus jeweils E-Rechnung Fachdienst-Logik und ZETA Guard-Image ein eigenes VAU-Image erzeugt wird, wobei in jedes VAU-Image ein Vertrauensanker für die Authentifizierung anderer Verarbeitungskontexte hinterlegt wird, und anschließend automatisiert:
  1. zu jedem VAU-Image der signierte Attestierungswert mit der gleichen Methodik/Technik ermittelt wird, wie sie auch in der VAU im Betrieb verwendet wird und
  2. das/die VAU-Image(s) und die dazugehörigen signierten Attestierungswerte ausgegeben werden.

**[<=]**

*Hinweis: Der in der zweiten Variante ("oder") genannte Vertrauensanker wird bei der gegenseitigen Authentifizierung bei der Kommunikation Verarbeitungskontext-zu-Verarbeitungskontext verwendet. Die Identitäten des jeweiligen Verarbeitungskontextes und die ausstellende CA sind auf dem HSM der VAU gespeichert [A\_26610\*] und werden bei der initialen Zeremonie [A\_26623\*] erzeugt. Dabei wird der öffentliche Schlüssel der CA exportiert, der dann als Vertrauensanker in die VAU-Images eingebracht wird. Die Authentifizierung eines anderen Verarbeitungskontext ist in ersterer Variante ("entweder") nicht notwendig, da die Kommunikation ZETA Guard<=>E-Rechnung Fachdienst-Logik dort innerhalb des Verarbeitungskontext stattfindet.*

*Ggf. ist zudem der Import eines Vertrauensankers für die Kommunikation zum HSM (Authentifizierung des HSM durch den Verarbeitungskontext) notwendig. Es kann hier dieselbe Certification Authority (CA) verwendet werden (so ist es im Hinweis unter [A\_26623\*] beschrieben). Grundsätzlich sind aber auch andere Methoden zur Etablierung eines beidseitig authentisierten Kanals zwischen Verarbeitungskontext und HSM möglich, solange der Verarbeitungskontext das HSM eindeutig authentifizieren kann.*

*Die VAU-Image-Build-Pipeline muss im Rahmen der Produkt-Begutachtung des E-Rechnung Fachdienstes geprüft werden. Der ZETA Guard selbst hat einen von der gematik abgenommenen Sicherheitsnachweis (Produktgutachten). Daher muss dieser bei dem beschriebenen Vorgehen nicht noch einmal sicherheitstechnisch betrachtet werden.*

## **A\_27584 - E-Rechnung Fachdienst - Sichere VAU-Image-Erzeugung (Prozess)**

Der Hersteller des E-Rechnung Fachdienst MUSS einen sicheren Gesamtprozess zur VAU-Image-Erzeugung umsetzen und dabei:

1. die geprüfte VAU-Image-Build-Pipeline nutzen,
2. im 4-Augen-Prinzip abgesichert den gematik-Signaturprüf Schlüssel für den ZETA Guard in die VAU-Image-Build-Pipeline einbringen und
3. Abwehrmaßnahmen gegen Manipulationen der VAU-Image-Build-Pipeline durch einen Innentäter umsetzen, was auch das Verhindern des unberechtigten Einbringens von Signatur-Prüf Schlüsseln umfasst.

**[<=]**

## **5.1.3.8 Konsistenz des Systemzustands, Logging und Monitoring**

### **A\_27423 - E-Rechnung Fachdienst - Konsistenter Systemzustand des Verarbeitungskontextes der VAU**

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

**A\_27424 - E-Rechnung Fachdienst - Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU**

Die VAU des E-Rechnung 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-Rechnung Fachdienstes oder Dritten vertrauliche oder zur Profilbildung geeignete Daten zur Kenntnis gelangen. [≤]

**A\_25815 - E-Rechnung Fachdienst - Funktionsmerkmale - Transaktionen**

Der E-Rechnung Fachdienst MUSS eine Information zur Verfügung stellen, falls die erneute Übermittlung von Dokumenten und Informationen zu Duplikaten führt. [≤]

**A\_27458 - E-Rechnung Fachdienst - Funktionsmerkmale - Vermeidung von Duplikaten aufgrund technischer Fehler**

Falls der Rechnungsersteller ein Dokument an den E-Rechnung Fachdienst übersendet und der Fachdienst die erfolgreiche Übermittlung aus technischen Gründen nicht bestätigen kann, dann MUSS der Fachdienst verhindern, dass durch das erneute Übertragen von Dokumenten Duplikate entstehen. [≤]

### 5.1.4 Dateigrößen

Beim Austausch und Speicherung von Dokumenten müssen Dateigrößenbeschränkungen eingehalten werden. Diese gelten sowohl für einzelne Dokumente als auch die Kombination von Rechnungen und ihren ergänzenden Dokumenten.

**A\_25975 - E-Rechnung Fachdienst - Dateigrößen - Maximale Größe einzelnes Dokument**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass einzelne Rechnungsdokumente und sonstige Dokumente nur bis zu einer maximalen Dateigröße von 10 MB in Übertragungen akzeptiert und gespeichert werden. [≤]

**A\_25976 - E-Rechnung Fachdienst - Dateigrößen - Maximale Größe zusammengehörige Dokumente**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Kombinationen aus Rechnungsdokument und dessen ergänzenden Dokumente nur bis zu einer maximalen Dateigröße von 50 MB in Übertragungen akzeptiert und gespeichert werden. [≤]

### 5.1.5 Dokumentenformate

**A\_25731 - E-Rechnung Fachdienst - Dokumentenformate - Dokumente**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass NUR Dokumente im Format PDF/A-1 und PDF/A-2 nach [ISO 19005] akzeptiert werden. Der E-Rechnung Fachdienst MUSS das Dokumentenformat validieren und bei Validierungsfehlern ablehnen. [≤]

**A\_25736 - E-Rechnung Fachdienst - Dokumentenformate - Angereichertes PDF**

Der E-Rechnung Fachdienst MUSS das angereicherte PDF im PDF/A-3 Format nach [ISO 19005] Abschnitt ISO 19005-3 erstellen. [≤]

Das Format PDF/A-3 wird für die Einreichung beim Kostenträger per Frontend (z.B. "Teilen"-Funktion) benötigt, da dieses die Einbettung der strukturierten Rechnungsdaten ermöglicht.

### 5.1.6 Nutzerprotokoll

Der E-Rechnung Fachdienst muss verschiedene Arten von Zugriffen protokollieren, so dass diese zu einem späteren Zeitpunkt von betroffenen Versicherten abgefragt werden können. Allgemein gefasst sind die Art des Zugriffs, der Zeitpunkt, der zugreifende



Akteur, das Ergebnis des Zugriffs, welche Ressourcen betroffen sind und der Protokolleintragsersteller zu protokollieren.

### **A\_25980 - E-Rechnung Fachdienst - Nutzerprotokoll - Zugriffszeit**

Der E-Rechnung Fachdienst MUSS bei jedem Zugriff den Zeitpunkt festhalten, zu dem dieser erfolgte.【<=】

#### **5.1.6.1 Rechnungen**

Für verschiedene Zugriffsarten müssen verschiedene Informationen protokolliert werden. Nachfolgend sind die zu protokollierenden Informationen beschrieben.

### **A\_25981 - E-Rechnung Fachdienst - Nutzerprotokoll - Rechnungen - Übermittlung**

Der E-Rechnung Fachdienst MUSS beim Übermitteln einer Rechnung das Erstellen, den Rechnungsersteller und die übermittelte Rechnung und, sofern vorhanden, die ergänzenden Dokumente protokollieren.【<=】

### **A\_25982 - E-Rechnung Fachdienst - Nutzerprotokoll - Rechnungen - Weitergabe an den Kostenträger**

Der E-Rechnung Fachdienst MUSS bei Weitergabe von Rechnungen und ergänzenden Dokumenten über das FdV an das IT-System des Kostenträgers die Weitergabe, den Rechnungseinreicher und die weitergegebenen Dokumente protokollieren.【<=】

Automatische Aktionen des E-Rechnung Fachdienstes müssen ebenfalls protokolliert werden. Diese Aktionen sind beispielsweise das automatische Verschieben von Rechnungen in den Papierkorb oder das automatische Löschen.

### **A\_25983 - E-Rechnung Fachdienst - Nutzerprotokoll - Rechnungen - Automatische Aktionen**

Der E-Rechnung Fachdienst MUSS bei automatischen Aktionen durch den Fachdienst selbst

- die Aktion (das Aktualisieren bzw. Löschen),
- sich selbst als Akteur und
- die betroffenen Dokumente

protokollieren.【<=】

#### **5.1.6.2 Berechtigungen**

Die Erstellung und Veränderung von Berechtigungen muss ebenfalls durch den Fachdienst protokolliert werden.

### **A\_25984 - E-Rechnung Fachdienst - Nutzerprotokoll - Berechtigungen - Erstellen**

Der E-Rechnung Fachdienst MUSS bei Erstellung von Berechtigungen die Erstellung, den entsprechenden Initiator und die erstellten Berechtigungen protokollieren.【<=】

### **A\_25985 - E-Rechnung Fachdienst - Nutzerprotokoll - Berechtigungen - Bestätigung/Widerruf**

Der E-Rechnung Fachdienst MUSS bei Bestätigung oder Widerruf von Berechtigungen die Aktualisierung dieser, den entsprechenden Bestätiger und die aktualisierten Berechtigungen protokollieren.【<=】

### **A\_25986 - E-Rechnung Fachdienst - Nutzerprotokoll - Berechtigungen - Abfrage**

Der E-Rechnung Fachdienst MUSS bei der Abfrage von Berechtigungen das Lesen, die Abfragenden und die abgefragten Berechtigungen protokollieren.【<=】

### 5.1.6.3 Markierungen

#### **A\_25987 - E-Rechnung Fachdienst - Nutzerprotokoll - Markierungen - Hinzufügen/Verändern**

Der E-Rechnung Fachdienst MUSS beim Hinzufügen oder Verändern von Markierungen das Aktualisieren, die betroffenen Dokumente und die Entitäten, die für die Veränderung verantwortlich sind, protokollieren. [≤]

### 5.1.6.4 Nutzerkonten

#### **A\_25988 - E-Rechnung Fachdienst -Nutzerprotokoll - Nutzerkonten - Erstellen**

Der E-Rechnung Fachdienst MUSS beim Erstellen von Nutzerkonten die Erstellung, den betreffenden Nutzer und das betreffende Nutzerkonto protokollieren. [≤]

## 5.2 RESTful API

#### **A\_25847 - E-Rechnung Fachdienst - RESTful API - Schnittstelle**

Der E-Rechnung Fachdienst MUSS seine Schnittstellen für alle Zugriffe auf alle Datenobjekte und alle Ressourcen in einer RESTful API gemäß der FHIR-Spezifikation in <https://hl7.org/fhir/r4/http.html> der Version v4.0.1 umsetzen. [≤]

#### **A\_25896 - E-Rechnung Fachdienst - RESTful API - FHIR Search**

Der E-Rechnung Fachdienst MUSS in seinen Schnittstellen Suchanfragen mittels FHIR-Search gemäß der FHIR-Spezifikation in <https://www.hl7.org/fhir/r4/search.html> der Version v4.0.1 in dem für die Anwendungsfälle (siehe [gemF\_E-Rechnung]) benötigten Umfang umsetzen. [≤]

#### **A\_25906 - E-Rechnung Fachdienst - RESTful API - FHIR Operations**

Der E-Rechnung Fachdienst MUSS in seinen Schnittstellen FHIR-Operations gemäß der FHIR-Spezifikation in <https://hl7.org/fhir/r4/operations.html> der Version v4.0.1 in dem für die Anwendungsfälle (siehe [gemF\_E-Rechnung]) benötigten Umfang umsetzen. [≤]

#### **A\_25845 - E-Rechnung Fachdienst - RESTful API - Konsumierende Formate**

Der E-Rechnung Fachdienst MUSS in seinen Schnittstellen für Zugriffe die MimeTypes application/fhir+json und application/fhir+xml akzeptieren und verarbeiten. [≤]

#### **A\_25846 - E-Rechnung Fachdienst - RESTful API - Produzierende Formate**

Der E-Rechnung Fachdienst MUSS in seinen Schnittstellen für Zugriffe entsprechend des HTTP-Request-Headers Accept entweder den Mime-Type application/fhir+json oder application/fhir+xml in Responses verwenden. [≤]

#### **A\_25848 - E-Rechnung Fachdienst - RESTful API - CapabilityStatement**

Der E-Rechnung Fachdienst MUSS eine HTTP-Route namens /metadata anbieten, bei der auf einem GET-Aufruf ein CapabilityStatement gemäß <https://www.hl7.org/fhir/capabilitystatement.html> zurückgeliefert werden muss, welches die vom E-Rechnung Fachdienst beschriebenen Ressourcen und Operations auflistet. [≤]

## 5.3 FHIR-Ressourcen

#### **A\_26053 - E-Rechnung Fachdienst - FHIR-Ressourcen - Dokument-Objekt**

Der E-Rechnung Fachdienst MUSS für den Austausch von Dokument-Objekten, bestehend aus Visualisierungen und strukturierten Daten, den FHIR-Ressource-Typ DocumentReference mit dem Profil <https://gematik.de/fhir/erg/StructureDefinition/erg-dokumentenmetadaten> verwenden. [≤]

**A\_26054 - E-Rechnung Fachdienst - FHIR-Ressourcen - Rechnungsdaten**

Der E-Rechnung Fachdienst MUSS für den Austausch von strukturierten Rechnungsdaten den FHIR-Ressource-Typ Invoice mit dem Profil

<https://gematik.de/fhir/erg/StructureDefinition/erg-rechnung> verwenden.[<=]

**A\_26062 - E-Rechnung Fachdienst - FHIR-Ressourcen - Rechnungsdokument**

Der E-Rechnung-Fachdienst MUSS für den Austausch des Base64-kodierten Rechnungsdokuments den FHIR-Ressource-Typ Binary mit dem Profil

<https://gematik.de/fhir/erg/StructureDefinition/erg-rechnungsdokument> verwenden.[<=]

**A\_26055 - E-Rechnung Fachdienst - FHIR-Ressourcen - Rechnungsposition**

Der E-Rechnung Fachdienst MUSS für den Austausch von Rechnungspositionen den FHIR-Ressource-Typ ChargeItem mit dem Profil

<https://gematik.de/fhir/erg/StructureDefinition/erg-rechnungsposition> verwenden.[<=]

**A\_26063 - E-Rechnung Fachdienst - FHIR-Ressource - Rechnungsdiagnose**

Der E-Rechnung Fachdienst MUSS für den Austausch von Diagnosen in Rechnungen den FHIR-Ressource-Typ Condition mit dem Profil

<https://gematik.de/fhir/erg/StructureDefinition/erg-rechnungsdiagnose> verwenden.[<=]

**A\_26056 - E-Rechnung Fachdienst - FHIR-Ressourcen - Versicherte**

Der E-Rechnung Fachdienst MUSS für den Austausch von Informationen über Versicherten den FHIR-Ressource-Typ Patient mit dem Profil

<https://gematik.de/fhir/erg/StructureDefinition/erg-versicherteperson> verwenden.[<=]

**A\_26057 - E-Rechnung Fachdienst - FHIR-Ressourcen - Leistungserbringer**

Der E-Rechnung Fachdienst MUSS für den Austausch von Informationen über Leistungserbringer den FHIR-Ressource-Typ Practitioner mit dem Profil

<https://gematik.de/fhir/erg/StructureDefinition/erg-leistungserbringer> verwenden.[<=]

**A\_26058 - E-Rechnung Fachdienst - FHIR-Ressourcen - Leistungserbringer-Institution**

Der E-Rechnung Fachdienst MUSS für den Austausch von Informationen über Leistungserbringer-Institutionen den FHIR-Ressource-Typ Organization mit dem Profil

<https://gematik.de/fhir/erg/StructureDefinition/erg-leistungserbringer-organisation> verwenden.[<=]

**A\_26059 - E-Rechnung Fachdienst - FHIR-Ressourcen - Nutzerprotokolleintrag**

Der E-Rechnung Fachdienst MUSS für den Austausch von Einträgen des Nutzerprotokolls den FHIR-Ressource-Typ AuditEvent mit dem Profil

<https://gematik.de/fhir/erg/StructureDefinition/erg-nutzungsprotokoll> verwenden.[<=]

## 5.4 FHIR-Endpunkte und -Operations

Der E-Rechnung Fachdienst muss für verschiedene Aktionen FHIR-Endpunkte und FHIR-Operations anbieten. Diese sind nachfolgend beschrieben.

### 5.4.1 RE-PS als Akteur

Nachfolgend beschrieben sind Anforderungen für Anwendungsfälle, in denen die Rechnungsersteller-Primärsysteme (RE-PS) die Akteure sind.

#### 5.4.1.1 Abfrage Rechnungsempfänger und dessen Einwilligung zum Rechnungsversand

##### **A\_25852 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Abfrage Rechnungsempfänger und dessen Einwilligung zum Rechnungsversand - Aufruf**

Der E-Rechnung Fachdienst MUSS die Abfrage eines Rechnungsempfängers mittels der HTTP-GET-Methode auf dem Endpunkt /Patient unterstützen, wie unter [IG eRg RE-PS#R0] beschrieben. [≤]

##### **A\_25879 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Abfrage Rechnungsempfänger und dessen Einwilligung zum Rechnungsversand - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-GET-Anfragen auf dem Endpunkt /Patient mit Status-Codes antworten, wie unter [IG eRg RE-PS#R0] beschrieben. [≤]

##### **A\_26028 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Abfrage Rechnungsempfänger und dessen Einwilligung zum Rechnungsversand - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Abfrage eines Rechnungsempfängers einen Claim mit der Telematik-ID des Nutzers und den Scope `insurantAccount.rs` enthalten und andernfalls diese abweisen. [≤]

#### 5.4.1.2 Rechnung validieren und einreichen

##### **A\_25849 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Rechnung validieren und einreichen - Aufruf**

Der E-Rechnung Fachdienst MUSS das Einreichen und Validieren von Rechnungen mittels HTTP-POST-Methode als FHIR-Operation `$rechnung-submit` mit der Definition <https://gematik.de/fhir/erg/OperationDefinition/Submit> auf dem Endpunkt /Patient/<id>/ unterstützen, wie unter [IG eRg RE-PS#R1] beschrieben. [≤]

##### **A\_25880 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Rechnung validieren und einreichen - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-POST-Anfragen auf dem Endpunkt /Patient/<id>/ mit der Operation `$rechnung-submit` mit Status-Codes antworten, wie unter [IG eRg RE-PS#R1] beschrieben. [≤]

##### **A\_26029 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Rechnung validieren und einreichen - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zum Einreichen und Validieren von Rechnungen einen Claim mit der Telematik-ID des Nutzers und den Scope `invoiceDoc.c` enthalten und andernfalls diese abweisen. [≤]

#### 5.4.1.3 Rechnung validieren/einreichen (Bulk)

##### **A\_25853 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Rechnung validieren/einreichen (Bulk) - Aufruf**

Der E-Rechnung Fachdienst MUSS die Validierung und Einreichen von Rechnungen als Bulk-Operation mittels HTTP-POST-Methode auf dem Endpunkt / unterstützen, wie unter [IG eRg RE-PS#R2] beschrieben. [≤]

##### **A\_25881 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Rechnung validieren/einreichen (Bulk) - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-POST-Anfragen auf dem Endpunkt / zum Einreichen und Validieren von Rechnungen als Bulk-Operation mit Status-Codes antworten, wie unter [IG eRg RE-PS#R2] beschrieben. [≤]

##### **A\_26030 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Rechnung validieren/einreichen (Bulk) - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zum Einreichen und Validieren von Rechnungen als Bulk-Operation einen Claim mit der Telematik-ID des Nutzers und den Scope `invoiceDoc.c` enthalten und andernfalls diese abweisen.[<=]

#### **5.4.1.4 Abfrage von Daten zu Rechnungen und Dokumenten per Token**

##### **A\_25854-01 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Abfrage von Daten zu Rechnungen und Dokumenten per Token - Abfrage**

Der E-Rechnung Fachdienst MUSS die Abfrage von angereicherten PDFs per Token mittels HTTP-POST-Methode als FHIR-Operation `$retrieve` mit der Definition <https://gematik.de/fhir/erg/OperationDefinition/Retrieve> auf dem Endpunkt `/DocumentReference/` unterstützen, wie unter [IG eRg RE-PS#R3] beschrieben.[<=]

##### **A\_25882-01 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Abfrage von Daten zu Rechnungen und Dokumenten per Token - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-POST-Anfragen auf dem Endpunkt `/DocumentReference/` mit der Operation `$retrieve` mit Status-Codes antworten, wie unter [IG eRg RE-PS#R3] beschrieben.[<=]

##### **A\_26031 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Abfrage von Daten zu Rechnungen und Dokumenten per Token - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Abfrage von angereicherten PDFs per Token einen Claim mit der Telematik-ID des Nutzers und den Scope `invoiceDoc.r` enthalten und andernfalls diese abweisen.[<=]

#### **5.4.1.5 Abfrage von angereicherten PDFs per Token (Bulk)**

##### **A\_25855 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Abfrage von angereicherten PDFs per Token (Bulk) - Abfrage**

Der E-Rechnung Fachdienst MUSS die Abfrage von angereicherten PDFs per Token als Bulk-Operation mittels HTTP-POST-Methode auf dem Endpunkt `/` unterstützen, wie unter [IG eRg RE-PS#R4] beschrieben.[<=]

##### **A\_25883 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Abfrage von angereicherten PDFs per Token (Bulk) - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-POST-Anfragen auf dem Endpunkt `/` zur Abfrage von angereicherten PDFs als Bulk-Operation mit Status-Codes antworten, wie unter [IG eRg RE-PS#R4] beschrieben.[<=]

##### **A\_26032 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - RE-PS als Akteur - Abfrage von angereicherten PDFs per Token (Bulk) - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Abfrage von angereicherten PDFs per Token als Bulk-Operation einen Claim mit der Telematik-ID des Nutzers und den Scope `invoiceDoc.r` enthalten und andernfalls diese abweisen.[<=]

#### **5.4.2 FdV als Akteur**

Nachfolgend beschrieben sind Anforderungen für Anwendungsfälle, in denen das Frontend des Versicherten (FdV) der Akteur ist.

#### 5.4.2.1 Abrufen/Suchen von Rechnungen

##### **A\_25857 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Abrufen/Suchen von Rechnungen - Abfrage**

Der E-Rechnung Fachdienst MUSS den Abruf und die Suche von Rechnungen mittels HTTP-GET-Methode auf dem Endpunkt /DocumentReference mit den Suchparametern unterstützen, wie unter [IG eRg FdV#R5] beschrieben. [≤]

##### **A\_25884 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Abrufen/Suchen von Rechnungen - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-GET-Anfragen auf dem Endpunkt /DocumentReference mit den Suchparametern mit Status-Codes antworten, wie unter [IG eRg FdV#R5] beschrieben. [≤]

##### **A\_26033 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Abrufen/Suchen von Rechnungen - Claims und Scopes (Abfrage)**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zum Abruf von Rechnungen einen Claim mit der KVN-R des Nutzers und den Scope invoiceDoc.r enthalten und andernfalls diese abweisen. [≤]

##### **A\_26034 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Abrufen/Suchen von Rechnungen - Claims und Scopes (Suche)**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Suche von Rechnungen einen Claim mit der KVN-R des Nutzers und den Scope invoiceDoc.s enthalten und andernfalls diese abweisen. [≤]

#### 5.4.2.2 Abfrage von Daten zu Rechnungen und Dokumenten per Token

##### **A\_25885-01 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Abfrage von Daten zu Rechnungen und Dokumenten per Token - Abfrage**

Der E-Rechnung Fachdienst MUSS die Abfrage von angereicherten PDFs per Token mittels HTTP-POST-Methode als FHIR-Operation \$retrieve mit der Definition <https://gematik.de/fhir/erg/OperationDefinition/Retrieve> auf dem Endpunkt /DocumentReference/ unterstützen, wie unter [IG eRg FdV#R6] beschrieben. [≤]

##### **A\_25886-01 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Abfrage von Daten zu Rechnungen und Dokumenten per Token - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-POST-Anfragen auf dem Endpunkt /DocumentReference/ mit der Operation \$retrieve mit Status-Codes antworten, wie unter [IG eRg FdV#R6] beschrieben. [≤]

##### **A\_26035 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Abfrage von Daten zu Rechnungen und Dokumenten per Token - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Abfrage von angereicherten PDFs per Token einen Claim mit der KVN-R des Nutzers und den Scope invoiceDoc.r enthalten und andernfalls diese abweisen. [≤]

#### 5.4.2.3 Statuswechsel

##### **A\_25858 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Statuswechsel - Abfrage**

Der E-Rechnung Fachdienst MUSS die Änderung des Status mittels HTTP-POST-Methode als FHIR-Operation \$change-status mit der Definition <https://gematik.de/fhir/erg/OperationDefinition/ChangeStatus> mit dem Parameter tag und den Werten erledigt, offen und papierkorb auf dem Endpunkt /DocumentReference/<id>/ unterstützen, wie unter [IG eRg FdV#R7] beschrieben. [≤]



**A\_25887 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Statuswechsel - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-POST-Anfragen auf dem Endpunkt /DocumentReference/<id>/ mit der FHIR-Operation \$change-status und mit dem Parameter tag mit Status-Codes antworten, wie unter [IG eRg FdV#R7] beschrieben. [≤]

**A\_26036 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Statuswechsel - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Änderung des Status einen Claim mit der KVN-R des Nutzers und den Scope invoiceDoc.u enthalten und andernfalls diese abweisen. [≤]

**5.4.2.4 Markieren von Rechnungen und Dokumenten****A\_25888 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Markieren von Rechnungen und Dokumenten - Abfrage**

Der E-Rechnung Fachdienst MUSS das Markieren von Rechnungen und Dokumenten mittels HTTP-POST-Methode als FHIR-Operation \$process-flag mit der Definition <https://gematik.de/fhir/erg/OperationDefinition/ProcessFlag> auf dem Endpunkt /DocumentReference/<id>/ unterstützen, wie unter [IG eRg FdV#R8] beschrieben. [≤]

**A\_25889 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Markieren von Rechnungen und Dokumenten - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-POST-Anfragen auf dem Endpunkt /DocumentReference/<id>/ mit der FHIR-Operation \$process-flag mit Status-Codes antworten, wie unter [IG eRg FdV#R8] beschrieben. [≤]

**A\_26039 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Markieren von Rechnungen und Dokumenten - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zum Markieren von Rechnungen und Dokumenten einen Claim mit der KVN-R des Nutzers und den Scope invoiceDoc.u enthalten und andernfalls diese abweisen. [≤]

**5.4.2.5 Löschen eines Rechnungsvorgangs****A\_25859 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Löschen eines Rechnungsvorgangs - Abfrage**

Der E-Rechnung Fachdienst MUSS das Löschen eines Rechnungsvorgangs mittels HTTP-POST-Methode als FHIR-Operation \$erase mit der Definition <https://gematik.de/fhir/erg/OperationDefinition/Erase> auf dem Endpunkt /DocumentReference/<id>/ unterstützen, wie unter [IG eRg FdV#R9] beschrieben. [≤]

**A\_25890 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Löschen eines Rechnungsvorgangs - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-POST-Anfragen auf dem Endpunkt /DocumentReference/<id>/ mit der FHIR-Operation \$erase mit Status-Codes antworten, wie unter [IG eRg FdV#R9] beschrieben. [≤]

**A\_26040 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Löschen eines Rechnungsvorgangs - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zum Löschen eines Rechnungsvorgangs einen Claim mit der KVN-R des Nutzers und den Scope invoiceDoc.d enthalten und andernfalls diese abweisen. [≤]

**5.4.2.6 Nutzerprotokoll einsehen****A\_25891 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Nutzerprotokoll einsehen - Abfrage**

Der E-Rechnung Fachdienst MUSS die Abfrage des Nutzerprotokolls mittels HTTP-GET-Methode auf dem Endpunkt /AuditEvent unterstützen, wie unter [IG eRg FdV#R10] beschrieben. [≤]

**A\_25892 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Nutzerprotokoll einsehen - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-GET-Anfragen auf dem Endpunkt /AuditEvent antworten, wie unter [IG eRg FdV#R10] beschrieben. [≤]

**A\_26041 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - FdV als Akteur - Nutzerprotokoll einsehen - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Abfrage des Nutzerprotokolls einen Claim mit der KVN-R des Nutzers und den Scope auditEvent.r.s enthalten und andernfalls diese ablehnen. [≤]

### 5.4.3 KTR als Akteur

Nachfolgend beschrieben sind Anforderungen für Anwendungsfälle, in denen Kostenträger (KTR) Akteure sind.

#### 5.4.3.1 Abfrage von Daten zu Rechnungen und Dokumenten per Token

**A\_25893-01 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - KTR als Akteur - Abfrage von Daten zu Rechnungen und Dokumenten per Token - Abfrage**

Der E-Rechnung Fachdienst MUSS die Abfrage von angereicherten PDFs per Token mittels HTTP-POST-Methode als FHIR-Operation \$retrieve mit der Definition <https://gematik.de/fhir/erg/OperationDefinition/Retrieve> auf dem Endpunkt /DocumentReference/ unterstützen, wie unter [IG eRg PSK#R11] beschrieben. [≤]

**A\_25894-01 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - KTR als Akteur - Abfrage von Daten zu Rechnungen und Dokumenten per Token - Status-Codes**

Der E-Rechnung Fachdienst MUSS auf HTTP-POST-Anfragen auf dem Endpunkt /DocumentReference/ mit der Operation \$retrieve mit Status-Codes antworten, wie unter [IG eRg PSK#R11] beschrieben. [≤]

**A\_26042 - E-Rechnung Fachdienst - FHIR-Endpunkte und -Operations - KTR als Akteur - Abfrage von Daten zu Rechnungen und Dokumenten per Token - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Abfrage von angereicherten PDFs per Token einen Claim mit der Telematik-ID des Nutzers und den Scope invoiceDoc.r enthalten und andernfalls diese ablehnen. [≤]

### 5.5 Weitere REST-Endpunkte

Der E-Rechnung Fachdienst muss neben den FHIR-Endpunkten und -Operationen weitere REST-Endpunkte anbieten. Diese betreffen Anfragen, die nicht durch FHIR abbildbar sind, wie beispielsweise das Berechtigungsmanagement.

**A\_25967 - E-Rechnung Fachdienst - Weitere REST-Endpunkte - Berechtigungen**

Der E-Rechnung Fachdienst MUSS die Schnittstelle für das Abfragen, Bearbeiten und Löschen von Berechtigungen als HTTP-REST-Anfragen unterstützen, wie unter [API eRg] beschrieben. [≤]



**A\_26043 - E-Rechnung Fachdienst - Weitere REST-Endpunkte - Berechtigungen Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zum Abfragen, Bearbeiten und Löschen von Berechtigungen einen Claim mit der Telematik-ID bzw. KVNR des Nutzers und zum Abfragen, Bearbeiten oder Löschen respektive den entsprechenden Scope `permission.r`, `permission.u` oder `permission.d` enthalten und andernfalls diese abweisen. [≤]

**5.6 Nutzerregistrierung****5.6.1 Institutionen**

Institutionen wie Rechnungsersteller und Kostenträger (KTR) sollen sich am E-Rechnung Fachdienst registrieren können. Diese Registrierung ermöglicht Institutionen den Zugriff auf eben diesen. Die Registrierung von KTR erlaubt außerdem Versicherten, bei Markierungen auf KTR zu verweisen. Sind KTR nicht am Fachdienst registriert, so kann bei einer Markierung der Verweis nur über einen Freitext erfolgen.

**A\_27554 - E-Rechnung Fachdienst - Nutzerregistrierung - Institutionen - REST-Endpunkt**

Der E-Rechnung Fachdienst MUSS die Registrierung von Institutionen mittels eines REST-Endpunkts unterstützen. [≤]

**A\_27555 - E-Rechnung Fachdienst - Nutzerregistrierung - Institutionen - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Registrierung von Institutionen Claims mit dem Anzeigenamen der Institution, die Telematik-ID des Nutzers und den Scope `practitionerAccount.c` (bei Rechnungserstellern) bzw. `insuranceAccount.c` (bei Kostenträgern) enthalten und andernfalls diese abweisen. Die übermittelten Informationen müssen gespeichert werden. [≤]

**A\_27556 - E-Rechnung Fachdienst - Nutzerregistrierung - Institutionen - Registrierungsdaten**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass die bei der Registrierung von Institutionen übermittelten Claims des Anzeigenamens und der Telematik-ID im erstellten Nutzeraccount gespeichert werden. [≤]

**5.6.2 Versicherte****A\_27557 - E-Rechnung Fachdienst - Nutzerregistrierung - Versicherte - REST-Endpunkt**

Der E-Rechnung Fachdienst MUSS die Registrierung von Versicherten mittels eines REST-Endpunkts unterstützen. [≤]

**A\_27558 - E-Rechnung Fachdienst - Nutzerregistrierung - Versicherte - Claims und Scopes**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass Anfragen zur Versichertenregistrierung Claims mit dem Anzeigenamen des Versicherten, die KVNR und das Geburtsdatum des Nutzers und den Scope `insurantAccount.c` enthalten und andernfalls diese abweisen. Die übermittelten Informationen müssen gespeichert werden. [≤]

**A\_27559 - E-Rechnung Fachdienst - Nutzerregistrierung - Versicherte - Registrierungsdaten**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass die bei der Versichertenregistrierung übermittelten Claims mit dem Anzeigenamen des Versicherten, die KVN-R und das Geburtsdatum im erstellten Nutzeraccount gespeichert werden.【<=】

## 5.7 Benachrichtigungen

### A\_26102 - E-Rechnung Fachdienst - Benachrichtigungen

Der E-Rechnung Fachdienst MUSS aktive Benachrichtigungen gemäß [gemF\_E-Rechnung#4.4.3] per Mail an die Versicherten senden. Als Empfänger-Adressen MÜSSEN dabei ausschließlich die Mail-Adressen genutzt werden, die bei der Registrierung von Endgeräten der Versicherten (siehe Client-Registrierung in [gemSpec\_ZETA]) validiert wurden und den Versicherten zugeordnet sind.【<=】

## 5.8 Interne Fehlercodes

### A\_27547 - E-Rechnung Fachdienst - interne Fehlercodes

Der E-Rechnung Fachdienst MUSS folgende interne Fehlercodes verwenden:

**Tabelle 2 : Tab\_eRg\_interne\_Fehlercodes**

BDE-Code	Errorcode Referenz	Beschreibung	Fehler-adressat
79030	MISSING_OR_INVALID_HEADER	The required header <header> is missing or invalid.	Clientsystem
79031	UNSUPPORTED_MEDIATYPE	The clientsystem asked for an unsupported media type <media type>.	Clientsystem
79032	UNSUPPORTED_ENCODING	The clientsystem asked for an unsupported encoding scheme <encoding scheme>.	Clientsystem
79040	INVALID_HTTP_OPERATION	ERROR	Clientsystem
79041	INVALID_ENDPOINT	ERROR	Clientsystem
79100	SERVICE_INTERNAL_SERVER_ERROR	Unexpected internal server error.	Clientsystem
79112	OCSP_NOTREACHABLE	Certificate validation services can not be reached	HTTP-Proxy
79113	OCSP_TIMEOUT	Certificate validation	HTTP-Proxy

		services timed out	
79205	MISSING_HEADER_CLIENTDATA	Header ZTA-Client-Data fehlt.	HTTP-Proxy
79206	MISSING_HEADER_USERINFO	Header ZTA-User-Info fehlt.	HTTP-Proxy
79400	ERROR_HEADER_CLIENTDATA	Client-Data Daten können nicht verarbeitet werden.	HTTP-Proxy
79401	ERROR_HEADER_USERINFO	User-Info Daten können nicht verarbeitet werden.	HTTP-Proxy
79403	ZETA_DPOP_VALIDATION_ERROR	Signature verification of the DPoP-JWT failed	Clientsystem
79404	ZETA_INVALID_ACCESSTOKEN	Signature verification of the presented access token failed	Clientsystem
79405	ZETA_EXPIRED_ACCESSTOKEN	Access token has expired	Clientsystem

【<=】

---

## 6 Informationsmodell

---

### 6.1 FHIR-Ressourcen

Der E-Rechnung Fachdienst muss FHIR-Ressourcen akzeptieren, verarbeiten und produzieren können, die dem Anwendungsfall entsprechen. Diese sind im vorhergehenden Kapitel beschrieben und deren Spezifikation befindet sich unter [Simplifier eRg].

### 6.2 Zugriffsprotokoll

#### A\_25829 - E-Rechnung Fachdienst - Zugriffsprotokoll - Allgemeine Protokollinformationen

Der E-Rechnung Fachdienst MUSS bei jedem Zugriff, der Informationen liest, erstellt, verändert oder löscht, als Protokolleintrag eine AuditEvent FHIR-Instanz mit folgenden Informationen erstellen:

- **AuditEvent**
  - **subtype**: zutreffender Wert aus <http://hl7.org/fhir/ValueSet/audit-event-sub-type>
    - <https://gematik.de/fhir/erg/CodeSystem/erg-operationen-cs>
  - **action**: zutreffender Wert aus <http://hl7.org/fhir/ValueSet/audit-event-action>
    - "C" = erstellt
    - "R" = gelesen
    - "U" = aktualisiert
    - "D" = gelöscht
  - **recorded**: Zeitpunkt des Ereignisses
  - **entity**: Liste an betroffenen Ressourcen
    - **what**: Referenz auf die betroffene Ressource
    - **name**: Name der Ressource
    - **description**: Beschreibung der Ressource

[<=]

#### A\_25836 - E-Rechnung Fachdienst - Zugriffsprotokoll - Protokolleintrag REST-Schnittstelle

Der E-Rechnung Fachdienst MUSS bei jedem Zugriff über die REST-Schnittstelle zusätzlich zu den allgemeinen Informationen in dem AuditEvent folgende Informationen protokollieren:

- **AuditEvent**
  - **type**: fester Wert
    - "rest" ( <http://terminology.hl7.org/CodeSystem/audit-event-type> )
  - **agent**:

- **name:** Anzeigenname der initierenden Entität
- **type:** fester Wert
  - "humanuser" ( <http://terminology.hl7.org/CodeSystem/extra-security-role-type>)
- **who:**
  - Identifier und Displayname von Versicherten, ADL, LEI oder KTR (Information aus Auth-Token)
- **requestor:** fester Wert
  - "false" (wird nicht vom Initiator selbst erstellt)

[&lt;=]

### **A\_25837 - E-Rechnung Fachdienst - Zugriffsprotokoll - Protokolleintrag automatische Verarbeitung**

Der E-Rechnung Fachdienst MUSS bei jeder automatischen Verarbeitung durch den E-Rechnung Fachdienst zusätzlich zu den allgemeinen Informationen in dem AuditEvent folgende Informationen protokollieren:

- **AuditEvent**
  - **type:** fester Wert
    - "110100" ("Application Activity", <http://dicom.nema.org/resources/ontology/DCM>)
  - **agent:**
    - **name:** fester Wert
      - "E-Rechnung-Fachdienst"
    - **type:** fester Wert
      - "dataprocessor" ( <http://terminology.hl7.org/CodeSystem/extra-security-role-type>)
    - **who:**
      - display
    - **requestor:** fester Wert
      - "true" (wird vom Initiator selbst erstellt)

[&lt;=]

## **6.3 Rechnungs- oder Dokumenten-Token**

### **6.3.1 Zufallswert**

#### **A\_26050 - E-Rechnung Fachdienst - Rechnung/Dokument-Token - Zufallswert**

Der E-Rechnung Fachdienst MUSS als Rechnungs- oder Dokument-Token einen Zufallswert generieren, der hexadezimal codiert genau 64 Zeichen lang ist, wobei die Vorgaben zu Zufallszahlen gemäß [gemSpec\_Krypt] zu beachten sind. [<=]

Dieses soll die Erratbarkeit gen Null senken. Ein Beispiel für einen Token wäre 777bea0e13cc9c42ceec14aec3ddee2263325dc2c6c699db115f58fe423607ea.

## 6.3.2 Darstellung als Barcode

### **A\_25724 - E-Rechnung Fachdienst - Rechnung/Dokument-Token - Barcode-Format**

Der E-Rechnung Fachdienst MUSS den Barcode für das Rechnungs- oder Dokumenten-Token als einen möglichst kompakten DataMatrix-Code gemäß [DataMatrix] in einem Format generieren, welches:

- den eigentlichen Token und
- einen eindeutigen Typ-Identifikator enthält, der der Anwendung E-Rechnung zuzuordnen ist.

[<=]

*Hinweis: Die genaue Ausgestaltung des Formats obliegt dem Hersteller des Fachdienstes.*

### **A\_25725 - E-Rechnung Fachdienst - Rechnung/Dokument-Token - Barcode-Inhalt**

Der E-Rechnung Fachdienst MUSS den Barcode aus dem zum Dokument gehörigen E-Rechnung- oder Dokumenten-Token generieren und darf keine anderen Informationen enthalten. [<=]

## 6.4 Angereichertes PDF

### **A\_25740 - E-Rechnung Fachdienst - Angereichertes PDF - Strukturierte Daten**

Der E-Rechnung Fachdienst MUSS die strukturierten Daten im FHIR-XML- oder FHIR-JSON-Format als Attachment in das angereicherte PDF integrieren. [<=]

### **A\_25726 - E-Rechnung Fachdienst - Angereichertes PDF - Größe Barcode**

Der E-Rechnung Fachdienst MUSS den Barcode in einer Größe und mit einem äußeren Abstand in das Dokument integrieren, so dass sich dieser vom ausgedruckten Dokument mit gängigen Methoden und gängiger Hardware einlesen lässt. [<=]

### **A\_25727 - E-Rechnung Fachdienst - Angereichertes PDF - Positionierung Barcode Default**

Der E-Rechnung Fachdienst MUSS den Barcode so platzieren, dass bei gängigen Layouts des PDF und ohne explizite Vorgabe (Default) der Position keine Elemente des Dokuments (Original-PDF) durch diesen verdeckt werden. [<=]

### **A\_27461 - E-Rechnung Fachdienst - Angereichertes PDF - Positionierung Barcode für Kuvertierung**

Der E-Rechnung Fachdienst MUSS den Barcode so platzieren, dass er bei gängigen Verfahren der Kuvertierung für den Postversand im Format DIN A4 nicht von Knickfalten betroffen wäre. [<=]

### **A\_27462 - E-Rechnung Fachdienst - Angereichertes PDF - Positionierung Barcode nach Vorgabe**

Der E-Rechnung Fachdienst MUSS es ermöglichen, die Platzierung des Barcodes durch Angabe einer Position und Orientierung zu variieren, um ggf. Probleme mit:

- Knickfalten,
- verdeckten Inhalten oder
- Sichtbarkeit in einem Sichtfenster (DIN A4 Umschlag)

beheben zu können.

[<=]

### **A\_25728 - E-Rechnung Fachdienst - Angereichertes PDF - Positionierung Barcode Wiederholbarkeit**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass die Positionierung des Barcodes sowohl bei dem optionalen, initialen Bereitstellen als auch bei späteren, wiederholten Abrufen identisch ist.【<=】

*Hinweis: Die konkrete Ausgestaltung des Positionierungsverfahrens obliegt dem Hersteller des Fachdienstes.*

### 6.5 Signatur

#### **A\_26051 - E-Rechnung Fachdienst - Signatur - Allgemeine Anforderungen**

Der Hersteller des E-Rechnung Fachdienst MUSS für die Signatur alle Anforderungen laut [gemSpec\_Krypt#3.7, 3.8] erfüllen.【<=】

#### **A\_26052 - E-Rechnung Fachdienst - Signatur - Erstellung**

Der E-Rechnung Fachdienst MUSS bei Empfang von Rechnungen und strukturierten Daten die Signatur über der Konkatenation aller Base64-kodierten Inhalte der Rechnung in der Reihenfolge Rechnungsdokument und strukturierte Daten bilden und diese anschließend speichern.【<=】

#### **A\_26061 - E-Rechnung Fachdienst - Signatur - Erneuerung**

Der E-Rechnung Fachdienst MUSS sicherstellen, dass alle Signaturen vor Ablauf der Gültigkeit erneuert werden.【<=】

Dieses kann beispielsweise für alle Signaturen gleichzeitig durchgeführt werden, wenn das Zertifikat erneuert wird.

---

## 7 Verteilungssicht

---

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



---

## 8 Anhang A - Verzeichnisse

---

### 8.1 Abkürzungen

**Tabelle 3: Im Dokument verwendete Abkürzungen**

Kürzel	Erläuterung
ADL	Abrechnungsdienstleister
CA	Certification Authority
CC	Common Criteria
FdV	Frontend des Versicherten
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
ITSEC	Information Technology Security Evaluation Criteria
KTR	Kostenträger
KVNR	Krankenversichertennummer
LEI	Leistungserbringerinstitution
PoPP	Proof of Patient Presence
RE	Rechnungsersteller
RE-PS	Rechnungsersteller Primärsystem
VAU	Vertrauenswürdigen Ausführungsumgebung

### 8.2 Glossar

**Tabelle 4: Glossar der explizit im Dokument verwendeten Begriffe**

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.
--	-------------------------------------

### 8.3 Abbildungsverzeichnis

Abbildung 1 Funktionaler Aufbau der Anwendung E-Rechnung.....	7
---	---

### 8.4 Tabellenverzeichnis

Tabelle 1 Erlaubte Nutzergruppen und Rollen.....	9
Tabelle 2 : Tab_eRg_interne_Fehlercodes.....	35
Tabelle 3: Im Dokument verwendete Abkürzungen.....	42
Tabelle 4: Glossar der explizit im Dokument verwendeten Begriffe.....	42
Tabelle 5: Referenzierte Dokumente der gematik.....	43
Tabelle 6: Weitere Referenzen.....	44

### 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.

**Tabelle 5: Referenzierte Dokumente der gematik**

[Quelle]	Herausgeber: Titel
[gemSpec_DS_Hersteller]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller
[gemF_E-Rechnung]	gematik: Feature Spezifikation/Konzept der Anwendung E-Rechnung
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Übergreifende Spezifikation: Festlegung von OIDs
[gemSpec_ZETA]	gematik: Spezifikation Zero Trust Access (ZETA)

## 8.5.2 Weitere Referenzen

**Tabelle 6: Weitere Referenzen**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[API eRg]	E-Rechnung API <a href="https://github.com/gematik/api-erg">https://github.com/gematik/api-erg</a> (Abruf 02/25)
[DataMatrix]	ISO/IEC 16022:2024: Information technology - Automatic identification and data capture techniques - Data Matrix bar code symbology specification
[IG eRg FdV]	Implementierungsleitfaden eRechnung - Szenarien - FdV als Akteur <a href="https://simplifier.net/guide/eRechnung-Implementierungsleitfaden/Starseite/Szenarien/eRg-FdV-als-Akteur?version=current">https://simplifier.net/guide/eRechnung-Implementierungsleitfaden/Starseite/Szenarien/eRg-FdV-als-Akteur?version=current</a> (Abruf 02/25)
[IG eRg RE-PS]	Implementierungsleitfaden eRechnung - Szenarien - RE-PS als Akteur <a href="https://simplifier.net/guide/eRechnung-Implementierungsleitfaden/Starseite/Szenarien/RE-PS-als-Akteur?version=current">https://simplifier.net/guide/eRechnung-Implementierungsleitfaden/Starseite/Szenarien/RE-PS-als-Akteur?version=current</a> (Abruf 02/25)
[IG eRg PSK]	Implementierungsleitfaden eRechnung - Szenarien - PSK als Akteur <a href="https://simplifier.net/guide/erechnung-implementierungsleitfaden/Starseite/Szenarien/ITSys-KTR-als-Akteur?version=current">https://simplifier.net/guide/erechnung-implementierungsleitfaden/Starseite/Szenarien/ITSys-KTR-als-Akteur?version=current</a> (Abruf 02/25)
[ISO 19005]	ISO 19005 - PDF Association (Abschnitt "PDF/A = ISO 19005") <a href="https://pdfa.org/pdf-standards/">https://pdfa.org/pdf-standards/</a> (Abruf 02/25)
[Simplifier eRg]	Simplifier Projekt E-Rechnung <a href="https://simplifier.net/e-rechnung">https://simplifier.net/e-rechnung</a> (Abruf 02/25)
[SMART on FHIR]	SMART on FHIR - Scopes <a href="https://build.fhir.org/ig/HL7/smart-app-launch/scopes-and-launch-context.html">https://build.fhir.org/ig/HL7/smart-app-launch/scopes-and-launch-context.html</a> (Abruf 02/25)