

## **Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Feature: E-Rechnung**

Version:	1.0.0_RC
Revision:	935074
Stand:	20.06.2024
Status:	zur Freigabe empfohlen
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemF_E-Rechnung

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

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

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0_CC	15.04.2024		initiale Erstellung	gematik
1.0.0_RC	20.06.2024		überarbeiteter Stand nach Kommentierung	gematik

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Feature-Dokuments.....</b>	<b>7</b>
1.1 Zielsetzung.....	7
1.2 Zielgruppe.....	8
1.3 Abgrenzung.....	9
1.4 Einbindung in die TI 2.0.....	9
1.5 Umfang des MVP.....	10
1.6 Methodik.....	11
1.7 Nutzergruppen und verwendete Begriffe.....	12
1.7.1 Rollen und Nutzergruppen.....	12
1.7.2 Verwendete Begriffe.....	13
<b>2 Epics und User Stories.....</b>	<b>16</b>
2.1 Übermittlung von Rechnungen durch Rechnungsersteller.....	16
2.2 Empfang und Verwaltung von Rechnungen durch Rechnungsempfänger	17
2.3 Einreichung von Rechnungen.....	19
2.3.1 Rechnungseinreicher.....	19
2.3.2 Kostenträger.....	19
2.4 Einrichtung und Verwaltung von Nutzerkonten.....	20
2.4.1 Versicherte.....	20
2.4.2 Institutionen.....	21
2.5 Nutzerprotokolle für Versicherte.....	21
<b>3 Einordnung in die Telematikinfrastruktur.....</b>	<b>22</b>
<b>4 Fachliches Konzept.....</b>	<b>25</b>
4.1 Einreichung per Post.....	25
4.2 Einreichung über das Frontend.....	26
4.3 Angereichertes PDF.....	28
4.4 Workflow und Bearbeitungsstatus.....	29
4.4.1 Workflow einer Rechnung.....	29
4.4.1.1 Automatische Verschiebung und Löschung von Rechnungen.....	32
4.4.1.2 Stornierung und Korrektur von Rechnungen.....	33
4.4.2 Markierungen.....	33
4.4.2.1 Einreichung per Frontend.....	34
4.4.2.2 Einreichung per Post.....	35
4.4.2.3 Einreichung per "Teilen".....	35
4.4.2.4 Abgerufen durch Kostenträger.....	35
4.4.2.5 Gelesen.....	35
4.4.2.6 Beahlt.....	35
4.4.2.7 Archiviert.....	36
4.4.2.8 Persönlich.....	36

4.4.3 Aktive Benachrichtigungen.....	36
<b>4.5 Nutzung der elektronischen Patientenakte (ePA).....</b>	<b>37</b>
<b>4.6 Berechtigungen.....</b>	<b>37</b>
4.6.1 Rollenbasierte Berechtigungen.....	38
4.6.2 Nutzerbasierte Berechtigungen.....	38
4.6.3 Regelbasierte Berechtigungen.....	38
4.6.3.1 Allgemeines.....	39
4.6.3.2 Berechtigungsregeln im E-Rechnung Fachdienst.....	39
<b>4.7 Protokollierung für den Nutzer.....</b>	<b>41</b>
<b>4.8 Informationsmodell.....</b>	<b>41</b>
4.8.1 Dokument (Obertyp).....	42
4.8.1.1 Rechnung.....	42
4.8.1.2 Ergänzendes Dokument.....	48
4.8.2 Rechnungs-Workflow.....	49
4.8.3 Markierung.....	49
4.8.4 Nutzer.....	49
4.8.4.1 Institutionen.....	49
4.8.4.2 Versicherte.....	50
4.8.5 Berechtigungen.....	50
4.8.6 Protokolleintrag.....	50
<b>5 Technisches Konzept.....</b>	<b>51</b>
<b>5.1 Zerlegung des Fachdienstes.....</b>	<b>51</b>
<b>5.2 Zugang zum Fachdienst in der TI.....</b>	<b>52</b>
<b>5.3 Gestaltung der Architektur gemäß Zero Trust Ansatz.....</b>	<b>52</b>
5.3.1 Schutz der Fachdienst-Ressource.....	52
5.3.2 Registrierung der Clients.....	53
5.3.3 Attestation der Client-Eigenschaften.....	53
5.3.4 Zugriffsentscheidung.....	53
5.3.5 Durchsetzung der Zugriffsentscheidung.....	53
5.3.6 Bereitstellung einer maschinell interpretierbaren Policy durch die gematik.....	53
<b>5.4 Funktionaler Aufbau und Schnittstellen.....</b>	<b>54</b>
5.4.1 Anwendungsdienst.....	55
5.4.2 Schnittstelle Autorisierung.....	56
5.4.2.1 Verwendete Identitätsattribute.....	57
5.4.2.2 Verwendete Geräteattribute.....	58
5.4.2.3 Bereitgestellte Claims und Scopes.....	59
5.4.2.3.1 Claims.....	59
5.4.2.3.2 Scopes.....	59
5.4.3 Client-Registrierungs-Schnittstelle.....	60
5.4.4 Schnittstelle für Versicherte.....	61
5.4.5 Schnittstelle für die Benachrichtigung.....	61
<b>5.5 Datenschutz und Informationssicherheit.....</b>	<b>61</b>
5.5.1 Schutzbedarf.....	61
5.5.2 Maßnahmen.....	62
5.5.3 Vertrauenswürdige Ausführungsumgebung.....	63
5.5.4 Prüfnutzeridentitäten.....	64
5.5.5 Datenschutzaspekte.....	65
5.5.6 Fristen für die Löschung und Aufbewahrung von Daten im Fachdienst.....	65
5.5.6.1 Inaktivität und automatische Löschung.....	65
5.5.6.2 Löschfristen für Nutzerkonten.....	66

5.5.6.3 Fristen für die Löschung und Aufbewahrung von Rechnungen und Dokumenten.....	66
5.5.7 Authentizität und Integrität von Rechnungen und Dokumenten.....	68
5.5.8 Schutz personenbezogener Daten in Token.....	68
5.5.9 Nutzerprotokolle.....	69
5.5.10 Grenzen der Sicherheitsleistung.....	70
<b>5.6 Betrieb.....</b>	<b>71</b>
5.6.1 Schnittstellen und Anwendungsfälle.....	71
5.6.2 Leistungsanforderungen.....	71
5.6.2.1 Mengengerüst.....	71
5.6.2.2 Produktspezifische Rahmenbedingungen.....	73
5.6.2.3 Anbieterspezifische Rahmenbedingungen.....	74
5.6.3 Monitoring.....	75
5.6.3.1 Erfassung und Lieferung von Betriebsdaten.....	75
5.6.4 Supportkonzept.....	75
5.6.4.1 1st Level Support.....	76
5.6.4.2 2nd Level Support.....	77
5.6.4.3 3rd Level Support.....	77
5.6.4.4 Mitwirkung und Support TI-ITSM.....	78
<b>6 Anwendungsfälle.....</b>	<b>79</b>
6.1 Anmerkungen zur Beschreibung der Anwendungsfälle.....	79
6.2 Übermittlung von Rechnungen.....	80
6.2.1 Konstellationen bei der Ermittlung des Rechnungsempfängers.....	80
6.2.2 Plausibilisierung.....	81
6.2.3 Ermittlung des Rechnungsempfängers.....	81
6.2.4 Validierung und Versand von Rechnungen und Dokumenten.....	82
6.3 Empfang von Rechnungen.....	91
6.3.1 Abruf von Rechnungen und Dokumenten.....	91
6.3.2 Berechtigung zum Rechnungsversand.....	96
6.3.3 Benachrichtigung empfangen.....	98
6.4 Verwaltung von empfangenen Rechnungen.....	99
6.5 Einreichung von Rechnungen.....	102
6.5.1 Anwendungsfälle des Rechnungseinreichers.....	102
6.5.2 Anwendungsfälle des Kostenträgers.....	103
6.6 Einrichtung und Registrierung von Nutzerkonten.....	105
6.6.1 Versicherte.....	105
6.6.2 Institutionen.....	111
6.7 Nutzerprotokolle.....	113
<b>7 Dokumentenhaushalt.....</b>	<b>116</b>
7.1 Neue Dokumente.....	116
7.2 Übersicht betroffener Dokumente.....	116
7.3 Übersicht Produkt- und Anbietertypen.....	116
<b>8 Anhang A - TI-Zugänge und Authentifizierungslösungen für die Nutzergruppen.....</b>	<b>117</b>
<b>9 Anhang B - Verzeichnisse.....</b>	<b>119</b>

<b>9.1 Abkürzungen.....</b>	<b>119</b>
<b>9.2 Abbildungsverzeichnis.....</b>	<b>120</b>
<b>9.3 Tabellenverzeichnis.....</b>	<b>120</b>
<b>9.4 Referenzierte Dokumente.....</b>	<b>122</b>
9.4.1 Dokumente der gematik.....	122
9.4.2 Weitere Referenzen.....	122

---

## 1 Einordnung des Feature-Dokuments

---

Dieses Feature-Dokument beschreibt das Feature der Anwendung E-Rechnung (eRg) als neue Anwendung der Telematikinfrastruktur (TI) für die Abrechnung medizinischer oder sonstiger Leistungen, die nicht dem Sachleistungsprinzip unterliegen. Der Fokus liegt zunächst auf der Beschreibung der fachlichen Anforderungen über *Epics* und *User Stories* sowie der Ableitung von Anforderungen im *fachlichen Konzept* als *Workflows*, *Berechtigungen* und einem *Informationsmodell*. Im darauf folgenden *technischen Konzept* werden die logischen Komponenten des Fachdienstes und Rahmenbedingungen für die technische Umsetzung seitens *Datenschutz und Informationssicherheit*, *Betrieb* und *Test* beschrieben. Die konkreten Umsetzungsanforderungen finden sich in Form von *Anwendungsfällen* (Use Cases) im darauf folgenden Kapitel.

Das vorliegende Feature-Dokument ist Teil der Gesamtspezifikation des Fachdienstes E-Rechnung (eRg FD) (siehe auch Kapitel 7- Dokumentenhaushalt). Beschrieben wird der eRg FD als Backend-Applikation. Die aufgeführten User Stories und Use Cases inkludieren die Sicht der Nutzer auf den Fachdienst und benötigten Schnittstellen für eine Frontend-Integration. Das Frontend des Versicherten für die E-Rechnung (eRg FdV) an sich ist allerdings nicht Teil der aktuellen Gesamtspezifikation. Die Umsetzung der eRg FdV-Funktionalitäten und Zulassung in neuen UIs oder deren Integration in vorhandene Produkte obliegt den Kostenträgern oder weiteren Anbietern von Versicherten-Frontends. Eine entsprechende eRg FdV-Spezifikation wird zu diesem Zwecke zukünftig zur Verfügung gestellt.

### 1.1 Zielsetzung

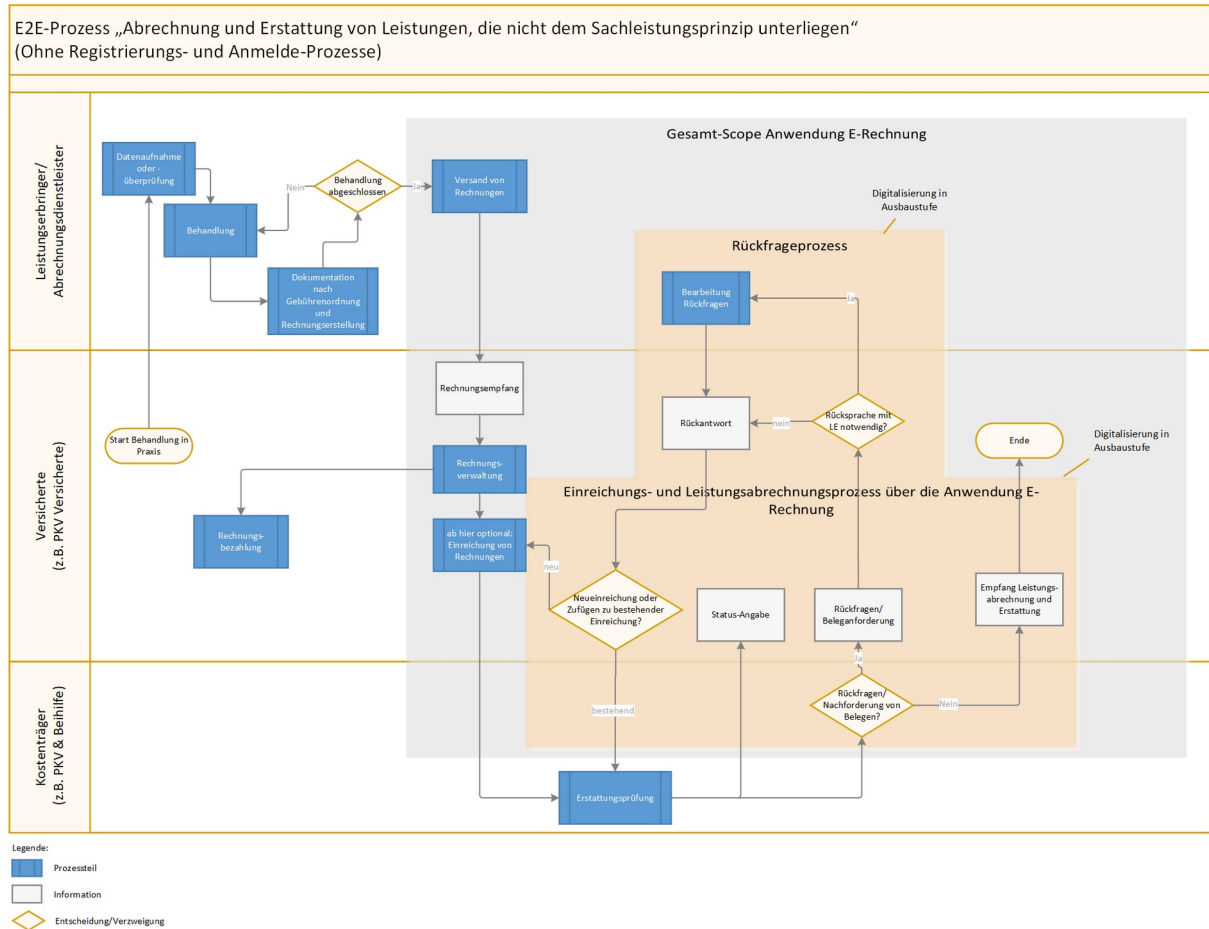
Die derzeitigen Abrechnungsprozesse bei Kostenträgern (KTR) wie z.B. privaten Krankenversicherungen (PKV) und Beihilfestellen basieren aktuell vielfach auf papiergebundenen Rechnungen, Einreichungen und Abrechnungen. Der Versicherte erhält seine Rechnungen vom Arzt oder einem Abrechnungsdienstleister (ADL) in Papierform. Er entscheidet, welche Rechnungen er bei seinem KTR einreichen möchte, wozu eine Rechnung oftmals noch per Post eingesendet werden muss. Zwar haben einige KTR bereits digitale Einreichungslösungen und manche ADL digitale Zustellmöglichkeiten. Eine standardisierte branchen-übergreifende und Ende-zu-Ende digitalisierte Lösung existiert allerdings nicht.

Eine solche durchgängig auf digitalen Daten basierende Lösung für den Abrechnungsprozess von Gesundheitsleistungen, die nicht dem Sachleistungsprinzip unterliegen, soll durch den neu zu erstellenden eRg FD geschaffen werden. Standard-Formate und -Schnittstellen sollen allen am Prozess beteiligten Institutionen sowie den Versicherten über nutzerfreundliche Oberflächen zur Verfügung gestellt werden. Ziel ist es, eine Lösung für die digitale Abrechnung zu schaffen, die Medienbrüche sowie Postversand vermeidet und für den Versicherten komfortabel in der Nutzung ist.

Der Fachdienst zur Unterstützung des Prozesses soll in mehreren Stufen entwickelt werden. Die Planung sieht folgende Stufen vor (siehe auch Abschnitt 1.5- Umfang des MVP):

- E-Rechnung 1.0: Minimum Viable Product (MVP), erste Stufe
- E-Rechnung 2.0 und weitere: Ausbaustufen auf Basis des MVP

Das folgende Prozessbild zeigt die Prozessbestandteile des eRg FD und dessen Scope auf. Elemente, die Ausbaustufen betreffen, sind entsprechend farblich (Digitalisierung in Ausbaustufe) markiert.



**Abbildung 1: E2E-Prozess "Abrechnung und Erstattung von Leistungen, die nicht dem Sachleistungsprinzip unterliegen"**

Dieses Feature-Dokument zielt auf die Beschreibung des eRg FD 1.0 (MVP) ab, siehe auch Abschnitt 1.5- Umfang des MVP.

## 1.2 Zielgruppe

Das Feature-Dokument richtet sich an den Hersteller und Anbieter des Produkttyps "E-Rechnung-Fachdienst". Darüber hinaus wendet es sich an die Hersteller

- von Primärsystemen aufseiten der Leistungserbringer (LE) und ADL,
- von Frontends der Versicherten sowie
- aufseiten der KTR eingesetzten IT-Systeme.



## 1.3 Abgrenzung

Der eRg FD wird nicht die Prozessteile Rechnungsdocumentation beim LE und Rechnungsbezahlung durch den Versicherten unterstützen. Darüber hinaus sind auch Leistungen von ADL (wie Forderungsübernahme, Durchführung von Mahnverfahren usw.) nicht Gegenstand der eRg.

Der eRg FD wird Schnittstellen zu den Systemen der LE und KTR sowie zum eRg FdV bereitstellen, aber nicht die Prozesse der Schnittstellennutzer spezifizieren. Zur Orientierung für Best-Practice-Nutzungen werden Click Dummys bzw. Prototypen der Frontends und Implementierungsleitfäden zur Verfügung gestellt.

## 1.4 Einbindung in die TI 2.0

Bei der Einführung der eRg als eine neue Anwendung der TI sollen die aktuellen Prinzipien aus dem Technologieportfolio der gematik verwendet werden. Dazu gehört insbesondere ein schrittweiser Ausbau der Anwendung in Richtung TI 2.0 Architektur.

### **Föderiertes Identitätsmanagement**

Die Authentisierung der Versicherten wird über die GesundheitsID realisiert. Die KTR stellen ihren Versicherten mittels sektoraler Identity Provider (IdP) elektronische Identitäten bereit. Durch App2App-Flow, Web2App-Flow und 2-Geräte-Flow können perspektivisch unterschiedlichste Nutzungsszenarien abgedeckt werden: die Nutzung eines Smartphones mit vollintegrierter 1-App Lösung oder mittels separaten Apps für private Voll- und Zusatzversicherte, als auch die Nutzung eines PCs (ggf. auch Smartphone) für Browser-basierte Versichertenportale.

Die Authentisierung der LE wird in der ersten Version der eRg über den vorhandenen IDP-Dienst der TI realisiert. Damit erfolgt die Authentisierung der LE/Leistungserbringerinstitutionen (LEI) weiterhin Smartcard-basiert analog zu E-Rezept und elektronischer Patientenakte (ePA).

Der eRg FD wird als Relying-Party in die IDP- und Dienste-Föderation aufgenommen.

### **Universelle Erreichbarkeit der Dienste**

Der eRg FD ist sowohl über das Internet als auch über das geschlossene Netz der TI erreichbar. Die Kommunikation mit dem eRg FD erfolgt, unabhängig vom Zugangsweg, über eine standardisierte Schnittstelle (REST API).

Der Zugriff über das Internet ist in der ersten Version nur für Versicherte möglich. Leistungserbringer und andere Institutionen (z.B. Abrechnungsstellen) können den Fachdienst zunächst nur über das geschlossene Netz der TI erreichen.

### **Moderne Sicherheitsarchitektur**

Die eRg verwendet die ersten Bausteine der Sicherheitsarchitektur der TI 2.0. Dazu gehört insbesondere die Verwendung von konkreten Leistungen und Komponenten zur Umsetzung von Zero-Trust Prinzipien, wie bspw. role based access nach dem least privilege Prinzip, eine Client-Registrierung und -Attestierung, eine sichere Client-Kommunikation mittels mutual authentication TLS (mTLS) und kurzfristig an die jeweils aktuelle Sicherheitslage anpassbare Sicherheitsrichtlinien für den Fachdienstzugriff. Weiterhin kommen die bereits in der TI etablierten Protokolle wie OAuth2.0 und OpenID Connect für die Authentisierung und Autorisierung zur Anwendung.

**Verteilte Dienste**

Beim eRg FD handelt es sich zunächst um einen einzelnen Dienst, der in der TI-Föderation registriert ist. Durch die Verwendung von standardisierten Schnittstellen und Protokollen kann die Nutzung des eRg FD in Kombination mit anderen Diensten mittels eines integrierten Frontends ("Versicherten-App") genutzt werden, welches z.B. durch Kombination von eRg FdV und ePA FdV die Abrechnung und die Dokumentation von Leistungen im E-Rechnung Fachdienst bzw. in der ePA zu vereinfachen.

**Interoperabilität und strukturierte Daten**

Die fachlichen Schnittstellen der E-Rechnung und ihre Informationsobjekte basieren auf HL7 FHIR. Dadurch reiht sich die E-Rechnung in die Reihe der FHIR-basierten Anwendungen der TI ein. Die Verwendung von FHIR und insbesondere standardisierter Profile ermöglicht die Interoperabilität mit anderen Anwendungen der TI und darüber hinaus.

Zu Gewährleistung einer hohen Datenqualität validiert der eRg FD zentral die übertragenen strukturierten Daten gegen das jeweils geltende FHIR-Profil, wodurch eine Klartextdatenverarbeitung im Fachdienst notwendig ist. Die Verarbeitung der personenbezogenen medizinischen Daten der E-Rechnung durch den Fachdienst setzt jedoch voraus, dass der eRg FD in einer vertrauenswürdigen Ausführungsumgebung (VAU) betrieben wird. Aufgrund der sicherheitstechnisch herausgehobenen Stellung des Service für die Client-Registrierung, gilt für diesen dieselbe Anforderung.

**Automatisierte Verarbeitung von Zugriffsrichtlinien (Policies)**

Im Rahmen der Zero Trust Sicherheitsarchitektur der TI 2.0 wird die automatisierte Verarbeitung der TI-Policy, die sowohl übergreifende als auch fachdienstspezifische Zugriffsregeln umfasst, durch die Zero-Trust Komponenten als Teil der betrieblichen Infrastruktur des eRg FD umgesetzt. Dies ermöglicht die Bereitstellung von Regeln für den eRg FD aus einem integrierten Policy Management der gematik heraus. Der eRg FD wendet diese Regeln automatisch an. In der ersten Version der eRg wird das Policy Management zunächst fachdienstspezifisch aufgebaut.

Da Zero Trust per se kein Standard oder Produkt ist, sondern vielmehr ein Architekturprinzip, ist es geplant, einzelne Bausteine der Zero Trust Architektur iterativ nacheinander einzuführen.

**1.5 Umfang des MVP**

Der eRg FD soll stufenweise umgesetzt werden. Das MVP unterstützt folgende Funktionalitäten :

- Es werden die folgenden Prozesssteile unterstützt:
  - Rechnungsübermittlung durch einen Rechnungsersteller über den Fachdienst an den Versicherten
  - Verwaltung der Rechnungen durch den Versicherten
  - Einreichung durch den Versicherten per Frontend an den Kostenträger, z.B. per "Teilen"
  - Abruf von digitalen Daten zu per Post eingereichten Rechnungen durch den KTR aus dem Fachdienst
- Es werden Rechnungen für medizinische oder sonstige Leistungen von Ärzten, Zahnärzten und Apothekern unterstützt, die nicht dem Sachleistungsprinzip unterliegen.

- Es werden die Gebührenordnungen GOÄ und GOZ unterstützt.
- Es wird die Nutzung des Fachdiensts für Versicherte 16+ unterstützt. Die Altersschwelle "16+" im Rahmen dieses Feature-Dokuments orientiert sich primär an der datenschutzrechtlichen Einwilligungsfähigkeit eines minderjährigen Versicherten gemäß Art. 8 DSGVO.
- Berechtigungen für LEI zur Rechnungsübermittlung im Fachdienst werden pauschal angelegt, Versicherte können Berechtigungen widersprechen.
- Es erfolgt eine technische Validierung der Rechnungen auf Basis festgelegter Pflichtangaben mit dem Ziel einer erfolgreichen Rechnungszustellung.

Das vorliegende Feature-Dokument beschreibt nur die Anforderungen an das MVP. Use Cases, die für weitere Ausbaustufen des eRg FD angedacht sind, werden in einem Backlog gesammelt.

## 1.6 Methodik

Das Dokument beschreibt Anforderungen an den eRg FD auf verschiedenen Abstraktionsebenen als Epics, User Stories und Use Cases.

*Epics* orientieren sich an Teilprozessen und gliedern sich wie folgt (siehe [2- Epics und User Stories](#)):

- Übermittlung von Rechnungen durch Rechnungsersteller
- Empfang und Verwaltung von Rechnungen durch Rechnungsempfänger
- Einreichung von Rechnungen
- Einrichtung und Verwaltung von Nutzerkonten
- Nutzerprotokolle für Versicherte

Pro Epic sind *User Stories* verfasst, die Software-Anforderungen aus Sicht verschiedener Prozessteilnehmer in Alltagssprache formulieren. Daraus leiten sich im technischen Konzept *Use Cases* ab, die *funktionale und technische Anforderungen* enthalten. Use Cases sind wie folgt als Anwendungsfallobjekte (AF) dargestellt:

**AF\_<ID> - <Titel des Use Case>**

### Tabelle

[<=]

Für jeden Use Case sind die folgenden Einzelemente beschrieben:

- **ID:** ein eindeutiger Identifier. Bei einem Use Case besteht der Identifier aus der Zeichenfolge 'AF\_' gefolgt von einer Zahl.
- **Titel des Use Cases:** ein Titel, welcher zusammenfassend den Inhalt beschreibt.
- **Tabelle:** eine Beschreibung des Inhalts in tabellarischer Form mit Vor- und Nachbedingungen, Ablauf und möglichen Alternativen.

Ein Use Case umfasst dabei immer sämtliche zwischen ID und Textmarke [<=] angeführten Inhalte.

## 1.7 Nutzergruppen und verwendete Begriffe

### 1.7.1 Rollen und Nutzergruppen

Im Folgenden sind die Rollen und zugehörigen Nutzergruppen der Anwendung E-Rechnung beschrieben:

- **Rechnungsersteller** - unter diesem Begriff werden folgende Institutionen (siehe auch 4.8.4.1- Institutionen) zusammengefasst :
  - Leistungserbringer-Institution (LEI) - das sind Institutionen mit Leistungserbringern, die selber Rechnungen erstellen.
  - Abrechnungsdienstleister (ADL) - darunter werden hier alle Dienstleister verstanden, die im Auftrag von LEI Rechnungen über erbrachte Leistungen erstellen und den Versicherten zukommen lassen - auch bekannt als "privatärztliche Verrechnungsstellen" oder "Factoring-Unternehmen". Darüber hinausgehende Leistungen von ADL wie Forderungsübernahme, Durchführung von Mahnverfahren usw. sind nicht Gegenstand der Anwendung E-Rechnung (siehe 1.3- Abgrenzung).
- **Forderungsinhaber** - Institution (z.B. LEI oder ADL) oder Person (z.B. Leistungserbringer), die für die Zahlung einer ausgestellten Rechnung die Forderung innehat.  
Der Forderungsinhaber kann gleich dem Rechnungsersteller sein. Abweichend vom Rechnungsersteller ist er beispielsweise dann, wenn bei der Übernahme der Rechnungserstellung durch ADL die Forderung bei der LEI verbleibt.
- **Behandelnder Leistungserbringer** - Institution oder Person, die in der Rechnung aufgeführte Behandlungsleistungen erbracht hat. Die in einer Rechnung zusammengefassten Leistungen können auch durch mehrere Leistungserbringer erbracht worden sein.
- **Rechnungsempfänger** - der Versicherte, der in der Rechnung als Rechnungsempfänger benannt wird und zu dessen Nutzerkonto die Rechnung zugesendet werden soll. Dies ist meist der zahlungspflichtige Versicherte, an den die Forderung gerichtet wird. Im weiteren Sinne kann allerdings jeder Nutzer, der am Fachdienst registriert werden kann, die Rolle des Rechnungsempfängers einnehmen. Rechnungsempfänger können sein:
  - PKV-Vollversicherte
  - PKV-Zusatzversicherte
  - GKV-Versicherte
  - Beihilfeberechtigte

**Im MVP wird auf die PKV-Voll- und Zusatzversicherten sowie Beihilfeberechtigte fokussiert.**

Die Anwendung ermöglicht rein technisch die Einreichung von Rechnungen bei einer PKV durch Versicherte, die über eine Gesundheits-ID verfügen. Somit können auch Zusatzversicherte, d.h. Versicherte, die bei einer anderen PKV oder einer GKV vollversichert sind, Rechnungen einreichen.

Ein Rechnungsempfänger ist zudem mindestens 16 Jahre alt und mindestens eingeschränkt geschäftsfähig. Die "eingeschränkte Geschäftsfähigkeit" bezieht sich auf Minderjährige, aber wenigstens 16 Jahre alte Versicherte, die zwar nicht als Versicherungsnehmer agieren können, aber schon eigenverantwortlich

entscheiden dürfen, ob sie Rechnungen mit sensiblen, sie betreffenden medizinischen Angaben selbst empfangen möchten.

- **Behandelte Person/Behandelter** - eine Person, die eine Behandlung in Anspruch nimmt, für die eine Rechnung erstellt wird. Diese wird als behandelte Person in der Rechnung genannt und kann gleich dem Rechnungsempfänger sein.
- **Abweichender Rechnungsempfänger** - der Rechnungsempfänger entspricht nicht dem Behandelten. Dies kann z.B. der Fall sein, wenn ein Rechnungsersteller die Rechnung für eine behandelte Person, die minderjährig ist, an den Erziehungsberechtigten zustellt.
- **Rechnungseinreicher** - eine Person, die bei einem KTR Rechnungen zur Bearbeitung (z.B. Kostenerstattungsprüfung) einreicht. Diese kann der Rechnungsempfänger selbst oder eine andere Person sein, mit der die Rechnung durch den Rechnungsempfänger geteilt wurde.
- **Kostenträger** - Institution, bei der für die Kostenerstattungsprüfung Rechnungen eingereicht werden können (siehe auch 4.8.4.1- Institutionen ). Dies sind z.B.:
  - Private Krankenversicherungen (PKV)
  - Beihilfestellen
  - Gesetzliche Krankenversicherungen (GKV)

### 1.7.2 Verwendete Begriffe

#### Anwendung E-Rechnung

Der Begriff "Anwendung E-Rechnung" wird folgend immer dann verwendet, wenn die neue Anwendung der TI allgemein bzw. in ihrer Gesamtheit beschrieben wird - in verkürzter Form auch "eRg". Sobald es die konkretisierende Darstellung technischer Komponenten betrifft, wird dies mit der Verwendung des jeweiligen Begriffs verdeutlicht, insbesondere:

- "E-Rechnung Fachdienst" - in verkürzter Form auch "eRg FD".
- "E-Rechnung Frontend des Versicherten" - in verkürzter Form auch "eRg FdV".

#### Client-System

Dieser Terminus umfasst die folgenden Begriffe:

- KTR-System - damit ist das Client-System des KTR gemeint.
- Primärsystem - damit ist das Client-System der LEI oder des ADL gemeint, sofern nicht explizit anders angegeben.
- Frontend des Versicherten - das Client-System, welches der Versicherte nutzt.

#### App

Mit dem Begriff "App" sind insbesondere mobile Apps als Umsetzung des eRg FdV gemeint, auf die sich dieses Dokument zunächst beschränkt. In zukünftigen Ausbaustufen können aber auch Desktop-Anwendungen oder browserbasierte Anwendungen für die Umsetzung des eRg FdV verwendet werden.

#### E-Rechnung

Eine "E-Rechnung" ist eine vom Rechnungsersteller unter Verwendung der Anwendung eRg in den Fachdienst eingestellte Rechnung für den Versicherten.

#### Dokumente

Der Begriff "Dokument" wird im Gegensatz zu Rechnungen im Folgenden vereinfachend als Bezeichner für Dokumente im Sinne der sonstigen, eine Rechnung lediglich ergänzenden Dokumente verwendet (siehe die Definition im Informationsmodell 4.8.1.2-Ergänzendes Dokument).

### PDF

Die Nennung PDF als Dateiformat bezeichnet im vorliegenden Feature-Dokument stets die spezifische Ausprägung PDF/A. PDF-Eingabe- und Ausgabedateien müssen stets in diesem PDF/A-Format vorliegen, selbst wenn keine strukturierten Daten eingebettet sind.

### Gravierende und nicht gravierende Fehler (in Rechnungsdaten)

Unter "gravierenden Fehlern" in Rechnungsdaten werden im Folgenden solche Fehler verstanden, die eine zuverlässige Zustellung oder Verarbeitung von E-Rechnungen im Fachdienst verhindern würden. Darunter fallen z.B. fehlende wichtige Pflichtangaben wie die Krankenversicherungsnummer (KVNR) des Rechnungsempfängers oder das Rechnungsdatum. Dies wird in der Spezifikation im Einzelnen weiter festgelegt (siehe 4.8.1.1-Rechnung).

Unter "nicht gravierenden Fehlern" in Rechnungsdaten werden solche Fehler verstanden, die eine zuverlässige Zustellung und Verarbeitung von E-Rechnungen nicht verhindern. Eine Rechnung mit "nicht gravierenden Fehlern" würde vom Fachdienst nicht abgelehnt, sondern es werden Warnungen an den Rechnungsersteller zurückgegeben, um auf die Fehler hinzuweisen. Die Prüfung von Rechnungen auf das Vorliegen "nicht gravierender" Fehler ist im MVP des eRg FD nicht vorgesehen.

### Hybrider Postversand/Postweg

Die Anwendung E-Rechnung ermöglicht auch die digitale Übertragung von Daten zu Rechnungen oder Dokumenten, die als Ausdrucke per Post versendet werden. Dieser Anwendungsfall, der digitale Übertragung und papiergebundenen Postversand betrifft, wird im Folgenden "hybrider Postversand" oder "hybrider Postweg" genannt. Der hybride Postversand findet in erster Linie dann Anwendung, wenn der Versicherte zwar seine Einwilligung zur digitalen Verarbeitung gegeben hat, aber dennoch den Postweg für den Rechnungsempfang bevorzugt.

### Postversand als Ersatzverfahren

Dies ist zu unterscheiden vom Postversand als Ersatzverfahren, d.h. dem Versand von papiergebundenen Rechnungen oder Dokumenten in dem Fall, dass die Anwendung E-Rechnung

- nicht genutzt werden kann aus technischen Gründen (insbesondere Nichtverfügbarkeit) oder
- nicht genutzt werden darf (insbesondere bei Widerspruch des Versicherten gegen die Nutzung der Anwendung).

---

## 2 Epics und User Stories

---

### 2.1 Übermittlung von Rechnungen durch Rechnungsersteller

#### Grundlegendes

Als Leistungserbringer (LE), der Rechnungen von einem Abrechnungsdienstleister (ADL) erstellen lässt, möchte ich dessen Dienstleistungen weiterhin und in möglichst unveränderter Weise nutzen können.

Als Rechnungsersteller möchte ich eine Rechnung auf rein digitalem Weg übermitteln können, um Fehler (z.B. durch falsche Empfängeranschrift bei der Postzustellung) zu vermeiden, sowie Zeit, Druck- und Versandkosten zu sparen.

Als Rechnungsersteller möchte ich, dass die Übermittlung digitaler Rechnungen möglichst einfach in den vorhandenen Prozessen und Primärsystemen umgesetzt und integriert wird, damit keine zusätzlichen Aufwände daraus resultieren.

Als Rechnungsersteller möchte ich bei erfolgreicher Übermittlung einer digitalen Rechnung eine Bestätigung mit Zeitpunkt erhalten, um einen Nachweis über die erfolgreiche Übermittlung an den Fachdienst zu haben.

Als Rechnungsersteller möchte ich bei nicht vorliegender Zustimmung des Rechnungsempfängers zur digitalen Rechnungsübermittlung auf diesen Umstand hingewiesen werden, damit ich den Postversand als Ersatzverfahren nutzen kann.

Als Rechnungsersteller möchte ich - ergänzend zur digitalen Rechnungsübermittlung - Rechnungen ausdrucken können, um bei Bedarf dem Rechnungsempfänger eine Kopie in Papierform zukommen lassen zu können, ohne dass dadurch die Verarbeitung digitaler Rechnungsdaten ausgeschlossen wird.

Als Rechnungsersteller möchte ich bei der digitalen Rechnungsübermittlung dem Rechnungsempfänger stets auch ein PDF der Rechnung zukommen lassen, damit dieser ein Rechnungsdokument mit dem von mir vorgegebenen Aussehen erhält.

Als Rechnungsersteller möchte ich mehrere Rechnungen gleichzeitig im Fachdienst einstellen, um diese gesammelt an verschiedene Rechnungsempfänger übermitteln zu können.

Als Rechnungsersteller möchte ich bei der digitalen Rechnungsübermittlung dem Rechnungsempfänger bei Bedarf auch ein oder mehrere ergänzende Dokumente (z.B. Belege) zukommen lassen können, damit dem Rechnungsempfänger ergänzende Belege zu einer Rechnung zur Verfügung gestellt werden können.

Als Rechnungsersteller möchte ich Rechnungen als Korrekturrechnung für eine zuvor übermittelte Rechnung kennzeichnen können, um diesen Umstand für Rechnungsempfänger und Kostenträger (KTR) transparent zu machen.

Als Rechnungsersteller möchte ich bei der digitalen Rechnungsübermittlung dem Rechnungsempfänger auch ein oder mehrere ergänzende persönliche Dokumente (z.B. Informationsschreiben) zukommen lassen können, um auf Dokumente aufmerksam zu machen, die üblicherweise nur für den Rechnungsempfänger bestimmt sind und nicht zur Einreichung beim Kostenträger geeignet sind.

#### Wahl des Rechnungsempfängers



Als Rechnungsersteller möchte ich selbst auswählen können, ob ich digitale Rechnungen an den Patienten selbst oder einen abweichenden Rechnungsempfänger übermittle, um denjenigen auswählen zu können, der gemäß Behandlungsvertrag und Situation des Patienten der richtige Rechnungsempfänger ist.

Als Rechnungsersteller möchte ich bei der digitalen Rechnungsübermittlung den Rechnungsempfänger eindeutig und sicher identifizieren können, damit keine schützenswerten Rechnungsdaten an einen falschen Empfänger gelangen.

Als Rechnungsersteller möchte ich Daten des Rechnungsempfängers von der Anwendung beziehen und mit den mir vorliegenden Daten abgleichen können, um eine fehlerhafte Zustellung der Rechnung zu vermeiden.

### **Prüfung und Umgang mit Fehlern**

Als Rechnungsersteller möchte ich, dass vor der digitalen Rechnungsübermittlung eine einfache Prüfung der Rechnungsdaten auf das Vorliegen aller Informationen für die erfolgreiche Zustellung an den Versicherten erfolgt und gefundene Fehler ggf. verständlich angezeigt werden, damit erkannte Fehler (gravierende Fehler) von mir behoben werden können.

Als Rechnungsersteller möchte ich, dass Rechnungen mit gravierenden Fehlern in den Rechnungsdaten erkannt und zurückgewiesen werden, damit ich andernfalls davon ausgehen darf, dass übermittelte Rechnungen auch zugestellt und verarbeitet werden können.

Als Rechnungsersteller möchte ich, dass gravierende Fehler in Rechnungsdaten so dokumentiert werden, dass diese analysiert, deren Ursachen (etwa Fehler in der verwendeten Software) behoben und somit zukünftig vermieden werden können.

## **2.2 Empfang und Verwaltung von Rechnungen durch Rechnungsempfänger**

### **Grundlegendes**

Als Versicherter möchte ich Rechnungen und ggf. ergänzende Dokumente meiner behandelnden LE digital empfangen können, um diese digital verwalten und bei Bedarf einfacher bei meinen KTR auf digitalem Wege einreichen zu können.

Als Rechnungsempfänger möchte ich Rechnungen und ggf. ergänzende Dokumente stets auch als PDF-Dokumente empfangen, um eine für mich gewohnte Darstellung zu erhalten und um diese bei Bedarf auch ausdrucken zu können - z.B. zwecks Archivierung oder Postversand.

Als Rechnungsempfänger möchte ich digitale Rechnungen und ggf. ergänzende Dokumente stets auch als PDF-Dokumente empfangen, um diese auch in meinem persönlichen Dokumentenbestand digital ablegen (z.B. in der ePA) oder auch digital "teilen" zu können.

Als Versicherter möchte ich, dass die in der Anwendung gespeicherten und über das Frontend des Versicherten (eRg FdV) abgerufenen Daten nicht direkt meinem KTR zur Kenntnis gelangen, sondern der KTR erst durch eine von mir aktiv initiierte Weitergabe von Daten Zugriff darauf bekommt, zum Beispiel durch das "Teilen" mit einer App des Kostenträgers.



### Nutzererlebnis

Als Rechnungsempfänger möchte ich Rechnungen meiner LE auch mit einer mobilen App empfangen können, um ortsunabhängig und mit meinem mobilen Endgerät (z.B. Smartphone) Rechnungen einsehen zu können.

Als Rechnungsempfänger möchte ich mit einer einzigen App auf alle meine digitalen Rechnungen und Statusinformationen zugreifen können, um einen besseren Überblick zu haben und einen mühsamen Wechsel zwischen verschiedenen Apps vermeiden zu können.

Als Rechnungsempfänger möchte ich stets den Zugriff auf meine digitalen Rechnungen behalten - unabhängig von der gerade verwendeten App -, damit ich problemlos auf die App eines anderen Anbieters wechseln kann.

Als Rechnungsempfänger möchte ich stets den Zugriff auf meine digitalen Rechnungen behalten - unabhängig von meiner gerade gewählten Krankenversicherung -, damit ich problemlos die Krankenversicherung wechseln kann.

Als Rechnungsempfänger möchte ich beim Eintreffen einer neuen digitalen Rechnung durch eine begleitende Mitteilung benachrichtigt werden, um zeitnah über zu begleichende oder einzureichende Rechnungen informiert zu bleiben.

Als Rechnungsempfänger möchte ich ungelesene und gelesene Rechnungen in einer Übersicht einsehen und unterscheiden können, um den Überblick über meine Rechnungen zu bewahren.

Als Rechnungsempfänger möchte ich einzelne Rechnungen zur Detailansicht auswählen können, um deren Inhalt vollständig sehen zu können.

Als Rechnungsempfänger möchte ich sehen und unterscheiden können, ob eine Rechnung offen und unerledigt ist oder ob eine Rechnung von mir bereits bearbeitet - z.B. eingereicht oder bezahlt - wurde.

Als Rechnungsempfänger möchte ich Korrekturrechnungen erkennen können und eine Information erhalten, auf welche ursprünglich erhaltene Rechnung sich die Korrektur bezieht, um ggf. notwendige Bearbeitungsschritte durchführen zu können.

Als Rechnungsempfänger möchte ich erkennen können, ob ein die Rechnung ergänzendes Dokument vom Rechnungsersteller für mich als persönlich gekennzeichnet ist, um darauf hingewiesen zu werden, dass dieses Dokument ggf. nicht mit der Rechnung an den Kostenträger eingereicht werden muss.

Als Rechnungsempfänger möchte ich die für eine Bezahlung erforderlichen Daten aus den Rechnungsdaten entnehmen können, um diese einfach in einem Bezahlvorgang außerhalb des eRg FdV nutzen zu können.

Als Rechnungsempfänger möchte ich sehen und unterscheiden können, ob eine von mir empfangene Rechnung für mich als behandelte Person oder eine andere Person erstellt wurde.

Als Rechnungsempfänger möchte ich eine Rechnung aus meiner Rechnungsübersicht zum Löschen vormerken (Papierkorb) oder endgültig aus dem Fachdienst löschen können.

Als Rechnungsempfänger möchte ich über eine anstehende automatische Löschung einer Rechnung rechtzeitig vorab informiert werden, damit ich die Möglichkeit habe, das Dokument herunterzuladen und zu archivieren, falls es noch von mir benötigt wird.

### Berechtigungen

Als Versicherter möchte ich per App eine Berechtigung zum digitalen Rechnungsversand für einzelne LE jederzeit einsehen, widerrufen und wieder erteilen können.

## **2.3 Einreichung von Rechnungen**

### **2.3.1 Rechnungseinreicher**

#### **Grundlegendes**

Als Rechnungseinreicher möchte ich per App empfangene Rechnungen einzeln oder gebündelt zu einem von mir wählbaren Zeitpunkt bei meinem KTR einreichen können, um die Erstattung meiner Kosten bei einem KTR beantragen zu können.

Als Rechnungseinreicher möchte ich eine Rechnung oder ein Dokument gleichzeitig oder auch hintereinander bei unterschiedlichen KTR einreichen können, um flexibel eine Erstattung meiner Kosten bei unterschiedlichen KTR beantragen zu können - z.B. bei einer PKV und der Beihilfe.

Als Rechnungseinreicher möchte ich bei der Einreichung von Rechnungen auch Dokumente mit einreichen können, die ich als ergänzende Dokumente zu einer Rechnung erhalten habe, um meinem KTR alle für die Leistungsabrechnung benötigten Informationen zur Verfügung stellen zu können.

Als Rechnungseinreicher möchte ich per App empfangene Rechnungen und ggf. ergänzende Dokumente als PDF herunterladen und ausdrucken können, um diese auch per Post bei einem KTR einreichen zu können, sofern eine digitale Einreichung nicht möglich ist oder ich aus persönlichen Gründen eine postalische Einreichung bevorzuge.

#### **Nutzererlebnis**

Als Rechnungseinreicher möchte ich erkennen können, ob und wann ich bei welchem KTR meine Rechnungen und Dokumente eingereicht habe.

### **2.3.2 Kostenträger**

Als KTR möchte ich eingereichte Rechnungen als strukturierte Daten empfangen und direkt einer digitalen, idealerweise automatischen Verarbeitung zuführen können, um Aufwände für Scan, OCR, Korrektur oder Klassifizierung beim Input Management vermeiden zu können.

Als KTR möchte ich bei postalisch eingereichten Rechnungen die zugehörigen digitalen Daten durch Einlesen der aufgedruckten Rechnungstoken im Fachdienst identifizieren, abrufen und einer digitalen, idealerweise automatischen Verarbeitung zuführen können, um Aufwände für Scan, OCR, Korrektur oder Klassifizierung beim Input Management vermeiden zu können.

Als KTR möchte ich Informationen (v.a. Metadaten) zu eingereichten ergänzenden Dokumenten als strukturierte Daten empfangen können, um die Klassifizierung und die Wahl des geeigneten Verarbeitungsprozesses zu erleichtern.

Als KTR möchte ich bei postalisch eingereichten ergänzenden Dokumenten die ggf. zugehörigen digitalen Daten (v.a. Metadaten) durch Einlesen der aufgedruckten Dokumenttoken im Fachdienst identifizieren können, um die Klassifizierung und die Wahl des geeigneten Verarbeitungsprozesses zu erleichtern.

Als KTR möchte ich die Authentizität und Integrität einer eingereichten Rechnung (Daten und PDF) jederzeit prüfen können, um Fälschungen und Manipulationen sicher erkennen zu können.

Als KTR möchte ich neben strukturierten Daten bei eingereichten Rechnungen jeweils ein zugehöriges PDF erhalten, um einen Ausdruck oder eine gut lesbare Darstellung für die manuelle Bearbeitung zu ermöglichen.

Als KTR möchte ich erkennen können, ob eine eingereichte Rechnung die Korrekturrechnung zu einer anderen Rechnung darstellt, um diese in der automatischen oder manuellen Sachbearbeitung berücksichtigen zu können.

## 2.4 Einrichtung und Verwaltung von Nutzerkonten

Im Folgenden werden User Stories zum Themenbereich Einrichtung und Verwaltung von Nutzerkonten aufgeführt, einschließlich der ggf. erforderlichen administrativen Eingriffe im Hinblick auf Datenschutz und Informationssicherheit.

### 2.4.1 Versicherte

Als Versicherter möchte ich mein Nutzerkonto jederzeit einfach selbst einrichten können, um die Nutzung der E-Rechnung aufwandsarm und schnell initiieren zu können.

Als Versicherter möchte ich, dass mein Nutzerkonto so abgesichert ist, dass nur ich als sicher authentifizierter und autorisierter Nutzer auf dieses zugreifen kann.

Als Versicherter möchte ich bei der Einrichtung oder Neueinrichtung eines eRg FdV (z.B. Wechsel der App) mein bereits bestehendes Nutzerkonto verwenden können, um weiterhin auf meine bereits vorhandenen Daten zugreifen zu können.

Als Versicherter möchte ich mit verschiedenen eRg FdV auf mein Nutzerkonto zugreifen können, um nicht an ein bestimmtes eRg FdV gebunden zu sein.

Als Versicherter möchte ich mich jederzeit mit dem eRg FdV vom E-Rechnung Fachdienst (eRg FD) abmelden können, um meine Nutzer-Sitzung gezielt beenden zu können.

Als Versicherter möchte ich mein Nutzerkonto mit allen mich betreffenden Daten (inklusive Berechtigungen) jederzeit selbst löschen können, um mein Recht auf informationelle Selbstbestimmung ausüben zu können.

Als Versicherter möchte ich mein Nutzerkonto jederzeit sperren oder auch löschen lassen können, um bei Verdacht auf Kompromittierung meines Nutzerkontos einen unautorisierten Zugriff auf meine Daten unterbinden zu können.

### 2.4.2 Institutionen

*Hinweis: Die folgenden User Stories betreffen Rechnungsersteller und/oder KTR. Wenn beide Nutzergruppen betroffen sind, wird zusammenfassend "Institution" verwendet.*

Als Institution möchte ich mein Nutzerkonto jederzeit selbst einrichten können, um möglichst einfach die eRg in Benutzung nehmen zu können.

Als Institution möchte ich mich unter Verwendung meiner digitalen ID für Institutionen mittels des zugehörigen Identity Providers am eRg FD anmelden können, um meine vorhandene digitale Identität für die Anmeldung nutzen zu können.

Als Institution möchte ich mich jederzeit vom eRg FD abmelden können, um meine Nutzer-Sitzung gezielt beenden zu können.

Als Institution möchte ich mein Nutzerkonto jederzeit sperren oder auch löschen lassen können, um bei Verdacht auf Kompromittierung meines Nutzerkontos einen unautorisierten Zugriff auf Daten unterbinden zu können oder um die Nutzung der E-Rechnung aus anderen Gründen beenden zu können.

## 2.5 Nutzerprotokolle für Versicherte

Im Folgenden werden User Stories zu Nutzerprotokollen aufgeführt, die die nötige Transparenz bzgl. der Verwendung von Daten für die Versicherten sicherstellen sollen.

Als Versicherter möchte ich, dass Zugriffe auf meine Daten im eRg FD in Form eines Nutzerprotokolls so erfasst werden, dass ich jederzeit einsehen und nachvollziehen kann, wer auf meine Daten wann und zu welchem Zweck zugegriffen hat.

Als Versicherter möchte ich die Möglichkeit haben, eine Kopie meines Nutzerprotokolls aus dem eRg FD herunterladen zu können, um dieses unabhängig von meinem Nutzerkonto aufbewahren und einsehen zu können.

*Hinweis: Dies zielt insbesondere auch auf das Sichern des Protokolls vor der Löschung eines Nutzerkontos ab.*

---

### 3 Einordnung in die Telematikinfrastruktur

---

Entsprechend der Beteiligung der Nutzergruppen der E-Rechnung sind die jeweils genutzten IT-Systeme in die Gesamtlösung zu integrieren (siehe auch Abbildung unten, "Einordnung der Anwendung E-Rechnung in die TI"). Dies sind:

- Die Primärsysteme (PS) der Leistungserbringer (LE) und der Abrechnungsdienstleister (ADL)

Da ADL im Kontext der Rechnungserstellung als Dienstleister für Leistungserbringer-Institutionen (LEI) tätig sein können, können E-Rechnungen nicht nur direkt aus den PS der LEI, sondern auch aus denen der ADL heraus erzeugt werden. Daher werden diese im Folgenden meist gleichbehandelt und als *Primärsysteme der Rechnungsersteller* bezeichnet, sofern nicht explizit unterschieden wird. Bei einer Rechnungserstellung durch ADL werden die abzurechnenden Leistungen und sonstigen Angaben über Schnittstellen zwischen der LEI und dem ADL übertragen. Die genannten PS dienen der Erzeugung und der Übermittlung von E-Rechnungen an den Fachdienst.

- Das Frontend des Versicherten der E-Rechnung (eRg FdV)

Der Versicherte kann mit dem eRg FdV neue E-Rechnungen und Dokumente von der LEI/dem ADL empfangen, einsehen und bei seinen Kostenträgern (KTR) einreichen. Außerdem kann er den Bearbeitungsstatus seiner E-Rechnungen und Dokumente festhalten und verwalten sowie E-Rechnungen und Dokumente in seine persönliche Ablage oder sein ePA-Aktenkonto übertragen, siehe auch nächster Punkt zum ePA FdV. Nicht mehr benötigte E-Rechnungen und Dokumente kann der Versicherte manuell löschen oder automatisch nach einer Frist löschen lassen.

Der Zugriff auf die Anwendung ist erst nach Authentisierung mittels GesundheitsID möglich. Dazu wird ggf. eine separate Authentisierungs-App benötigt, falls die Authentisierung nicht per eRg FdV erfolgt (im Bild nicht dargestellt).

*Hinweis: eine prototypische Beispielimplementierung des eRg FdV soll FdV-Herstellern bereitgestellt werden.*

- Das Frontend des Versicherten für die elektronische Patientenakte (ePA FdV)

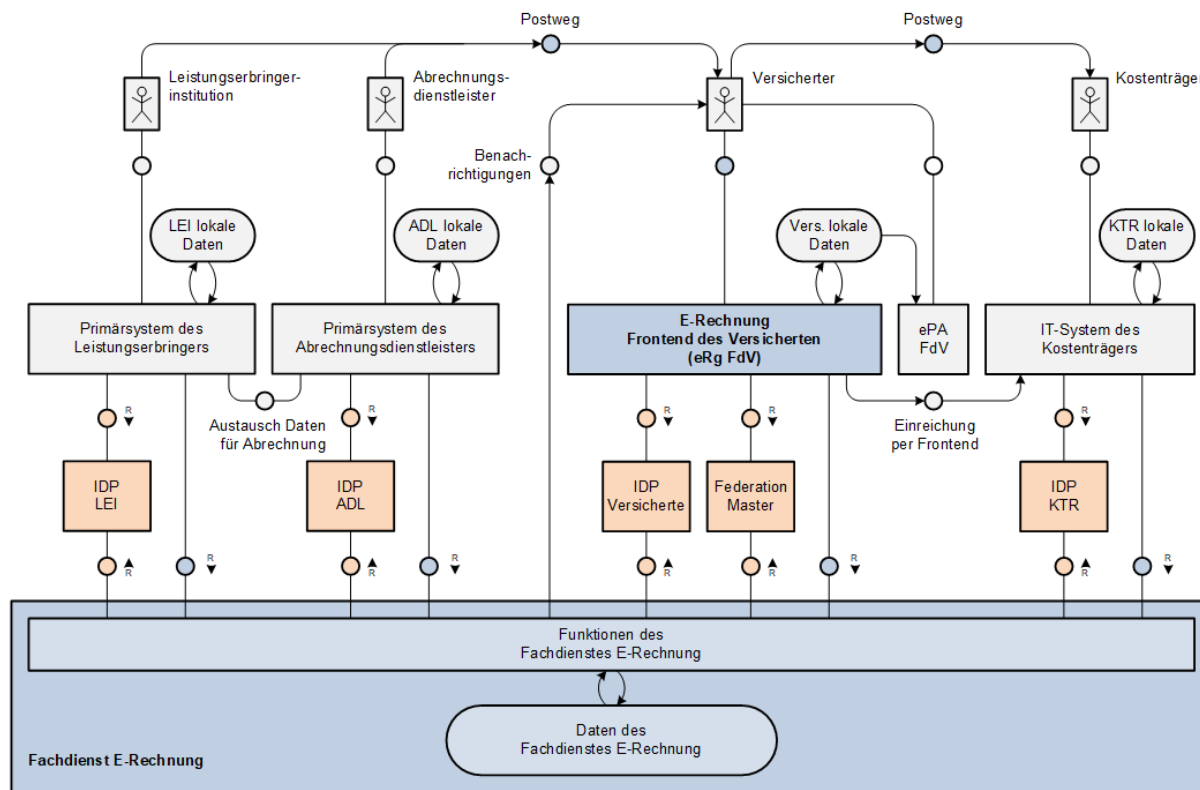
Die längerfristige Aufbewahrung von E-Rechnungen über die eingangs beschriebenen Epics hinaus ist nicht Gegenstand der Anwendung E-Rechnung (eRg). Daher soll dem Versicherten zukünftig eine komfortable Möglichkeit geboten werden, E-Rechnungen in seine ePA zu übertragen. Vorerst soll diese Übertragung durch Übergabe (z.B. mittels "Teilen"-Funktion) von E-Rechnungen (PDF) an das ePA FdV und daran anschließendes Einstellen der E-Rechnungen in das ePA-Aktensystem (nicht dargestellt) per ePA FdV ermöglicht werden.

- Die IT-Systeme der KTR (KTR-Systeme)

Die KTR-Systeme nehmen eingereichte Rechnungen und Dokumente vom Versicherten entgegen zwecks Bearbeitung und Leistungsabrechnung. Dies können digital über das Frontend eingereichte Rechnungen und Dokumente sein, aber auch per Post eingereichte - und mit einem Barcode versehene - Ausdrucke von E-Rechnungen und Dokumenten. Beim Postweg bietet der Fachdienst dem KTR die Möglichkeit, durch Auslesen eines Barcodes die zugehörige E-Rechnung oder das zugehörige Dokument aus dem Fachdienst abzurufen. Neben diesem "hybriden" Postversand kann der Postversand auch unabhängig von der eRg als

Ersatzverfahren genutzt werden. Die folgenden Betrachtungen beschränken sich auf den hybriden Postweg, der Gegenstand der Anwendung ist.

Die Rückmeldung des Bearbeitungsstatus' und die Bereitstellung der Leistungsabrechnung durch die KTR erfolgen in der ersten Ausbaustufe nicht über die eRg.



**Abbildung 2: Einordnung der Anwendung E-Rechnung in die TI**

Folgende Dienste setzen Funktionen der Anwendung in der TI um:

- E-Rechnung Fachdienst ( eRg FD)

Der eRg FD wird als neuer offener Fachdienst der TI eingeführt. Es soll diesen Dienst nur in einer einzigen logischen Instanz geben, sodass ein indirekter Datenaustausch zwischen den oben erwähnten Primär- bzw. KTR-Systemen und dem eRg FdV darüber in einfacher Weise erfolgen kann. Die indirekte Kopplung vermeidet Punkt-zu-Punkt-Verbindungen und reduziert somit die Komplexität. Gleichzeitig hält dies die technische Ausgestaltung der angebundenen Systeme offen.

Es ist insbesondere nicht ausgeschlossen, dass verfügbare oder künftige Produkte die Funktionen verschiedener angeschlossener Systeme in sich vereinen. So könnte z.B. das eRg FdV als Kundenportal (Web-Anwendung) umgesetzt werden, welches integraler Bestandteil eines KTR-Systems ist, solange die Bereitstellung der Daten über den Fachdienst weiterhin gewährleistet bleibt. Auch könnte das eRg FdV zusammen mit dem ePA FdV realisiert werden, um dem Versicherten

einen umfassenden Funktionsumfang in einer einzigen "Versicherten-App" zu bieten, usw.

Der Fachdienst hält die Daten zu E-Rechnungen nur solange vor, wie diese für die Zustellung, Einreichung oder Kostenerstattung benötigt werden (siehe auch 5.5.6- Fristen für die Löschung und Aufbewahrung von Daten im Fachdienst). Eine Aufbewahrung darüber hinaus, insbesondere Archivierung, ist im Sinne der Zweckgebundenheit nicht vorgesehen.

Der Zugriff auf Dienste der TI soll bei den Institutionen vorerst nur über das zentrale Netz der TI erfolgen. Die eRg soll ohne Fachmodul im Konnektor auskommen, deshalb wird der Fachdienst in der Zone der offenen Fachdienste betrieben. Für das eRg FdV muss der Fachdienst über das Internet erreichbar sein. Zur Absicherung dieses Zugangs siehe 5.3- Gestaltung der Architektur gemäß Zero Trust Ansatz.

- Identity Provider (IDP) und Federation Master

Sämtliche, auf die eRg zugreifende Nutzer werden mittels der jeweiligen (ggf. sektoralen) IDP authentifiziert:

- IDP für Versicherte

Hier finden die sektoralen IDP der privaten und gesetzlichen Krankenversicherungen Anwendung. Zur Auswahl des für den Versicherten zu verwendenden IDP wird der Federation Master als Dienst genutzt, der eine Liste der verfügbaren sektoralen IDP bereitstellt.

- IDP für LEI, Organisationen des Gesundheitswesens (hier die ADL) und KTR

Perspektivisch sollen die sektoralen IDP der jeweiligen Nutzergruppe eingesetzt werden. Solange diese noch nicht bereitgestellt sind, wird stattdessen auf den zentralen IDP der TI zurückgegriffen, bei dem die Authentisierung mittels SMC-B oder HSM-B erfolgt.

Der Zugriff der verschiedenen Nutzer mittels der von ihnen verwendeten Client-Systeme ist geeignet abzusichern. Der Zugriff der Versicherten soll - mit Hinblick auf die TI 2.0 - über das Internet nach dem Zero-Trust-Prinzip ermöglicht werden. Dazu wird eine Prüfung der Integrität des Nutzerendgerätes (Device Attestation) sowie der Bindung an den Nutzer durchgeführt, deren Ergebnis bei der Autorisierung des Nutzers mit ausgewertet wird. Auf diese Weise kann z.B. der Zugriff mittels eines von einer Sicherheitslücke betroffenen Endgerätes unterbunden werden.

E-Rechnungen sollen durch die PS bzw. KTR-Systeme validiert werden bzgl. der Vollständigkeit und Korrektheit. Der Fachdienst prüft übergebene E-Rechnungen ebenfalls, allerdings ist dies im Minimum Viable Product (MVP) auf die Absicherung gegen gravierende Fehler beschränkt.

## 4 Fachliches Konzept

Das Minimum Viable Product (MVP) der Anwendung E-Rechnung (eRg) zielt auf die Unterstützung zweier wichtiger Wege zur Einreichung von Rechnungen und Dokumenten vom Versicherten an den Kostenträger.

### 4.1 Einreichung per Post

Der Postweg kann alternativ zur E-Rechnung genutzt werden, d.h. in Situationen, in denen der Fachdienst nicht genutzt werden kann - aufgrund betrieblicher Nichtverfügbarkeit als Ersatzverfahren oder weil der Versicherte der digitalen Verarbeitung von Rechnungen widersprochen hat oder weil der Rechnungsersteller den Rechnungsversand per E-Rechnung nicht anbieten möchte.

Die Anwendung E-Rechnung soll jedoch einen "hybriden" Postversand ermöglichen, d.h. parallel zum Versand einer ausgedruckten E-Rechnung oder Dokument werden die zugehörigen digitalen Daten über den Fachdienst bereitgestellt. Bei der Verarbeitung des Posteingangs soll der Kostenträger die Möglichkeit haben, durch Einlesen eines auf der Rechnung bzw. dem Dokument aufgedruckten Barcodes einen Code (Token) zu erhalten, über den der Abruf der zugehörigen Daten aus dem Fachdienst ermöglicht wird. Die Anwendung sieht daher die Ergänzung von Rechnungen oder Dokumenten im PDF-Format um einen solchen Barcode vor. Im Folgenden wird im Zusammenhang mit dem Postweg nur dieser hybride Postversand betrachtet, sofern nichts anderes gesagt wird, siehe auch folgende Darstellung.

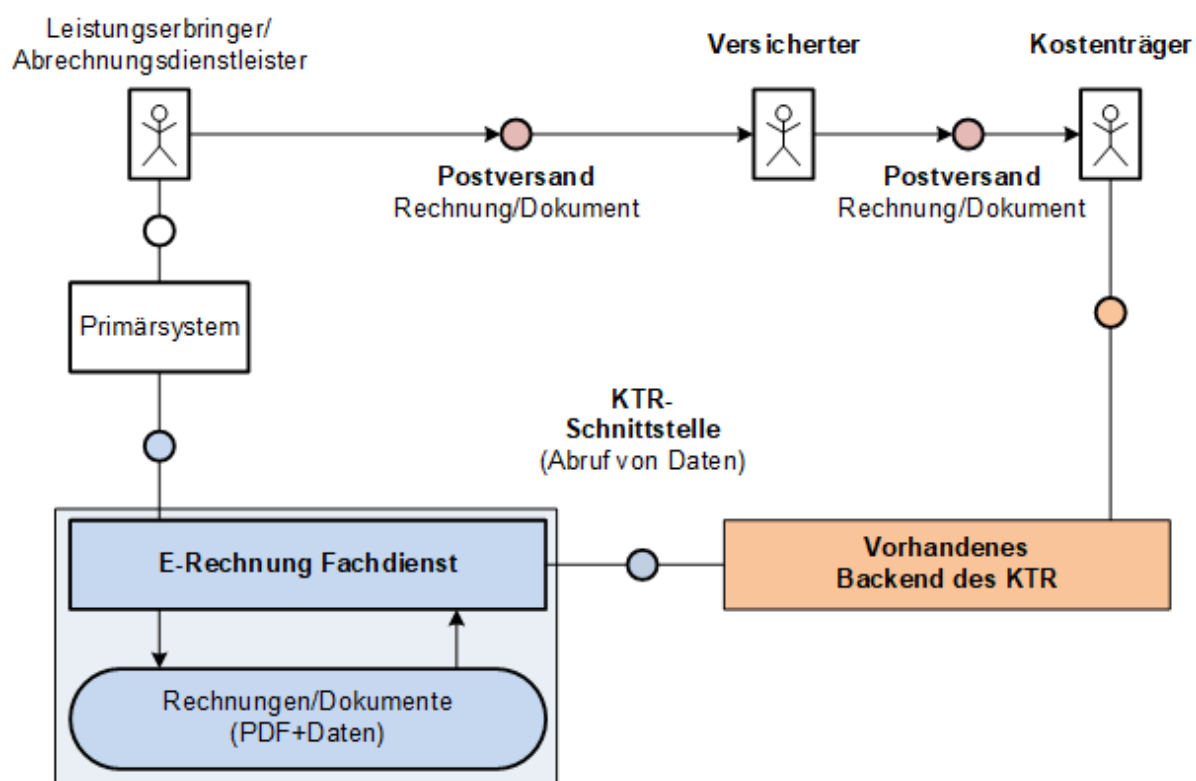


Abbildung 3: Hybrider Postversand



## 4.2 Einreichung über das Frontend

Ziel der Anwendung E-Rechnung ist primär der Versand und die Einreichung von E-Rechnungen und Dokumenten - einschließlich strukturierter Daten - auf rein digitalem Weg. Der Versand von E-Rechnungen und Dokumenten durch die Leistungserbringer-Institutionen (LEI) oder den Abrechnungsdienstleister (ADL) erfolgt dabei über den Fachdienst, d.h. der Versicherte kann die Daten nur über den Fachdienst mittels seines Frontend des Versicherten (eRg FdV) empfangen.

Für die Einreichung von E-Rechnungen und Dokumenten ist im MVP keine Einreichung über den Fachdienst vorgesehen. Stattdessen wird die "Einreichung per Frontend" umgesetzt, bei der der Versicherte per eRg FdV abgerufene E-Rechnungen oder Dokumente über meistens beim Kostenträger schon vorhandene digitale Einreichungswege einreicht. Dabei erfolgt die Datenübertragung an den Kostenträger außerhalb der eRg. (Dies schließt jedoch den oben beschriebenen Postweg nicht aus, bei dem der Kostenträger Daten vom Fachdienst bezieht.) Betrachtete Varianten der Einreichung per Frontend sind:

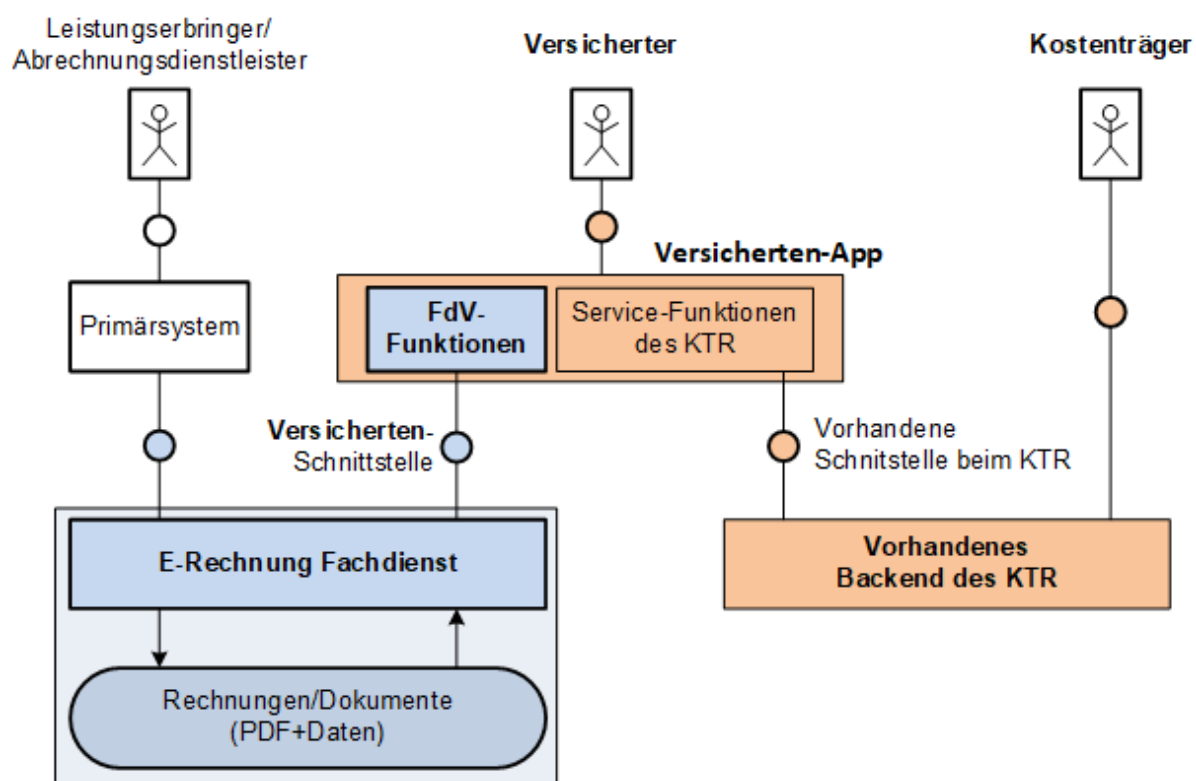
- Einreichung mittels integrierter "Versicherten-App"

Bei dieser Variante wird das eRg FdV durch eine App umgesetzt, die neben den Funktionen des eRg FdV auch weitere Service-Funktionen anbietet, die dem Versicherten eine Datenübergabe über eine bereits vorhandene Schnittstelle an das KTR-System ermöglichen.

Eine solche integrierte "Versicherten-App" verfügt also über

1. eine Anbindung an den E-Rechnung Fachdienst (eRg FD) für den Empfang von E-Rechnungen und Dokumenten und
2. eine kostenträgerspezifische Anbindung außerhalb der TI an das KTR-System zur Einreichung von E-Rechnungen und Dokumenten.

Siehe auch folgende Darstellung:



**Abbildung 4: Einreichen per eRg FdV als Teil einer integrierten Versicherten-App**

- Einreichung per "Teilen"

Hier gilt die Annahme, dass es neben einer App, die das eRg FdV umsetzt, eine separate App (kurz "Service-App") gibt, die über eine kostenträgerspezifische Anbindung außerhalb der TI an das KTR-System verfügt, worüber die Einreichung beim Kostenträger erfolgt.

Eine solche "Service-App" verfügt also über *keine* Anbindung an den E-Rechnung Fachdienst (eRg FD), aber eine kostenträgerspezifische Anbindung außerhalb der TI an das KTR-System zur Einreichung von E-Rechnungen und Dokumenten.

Bei der Einreichung per Teilen wird die auf mobilen Endgeräten vorhandene "Teilen-Funktion" zur Übergabe von Daten von einer App an eine andere App genutzt - hier konkret die Übergabe von empfangenen E-Rechnungen und Dokumenten durch den Versicherten vom eRg FdV an die "Service-App" - siehe auch folgende Darstellung.

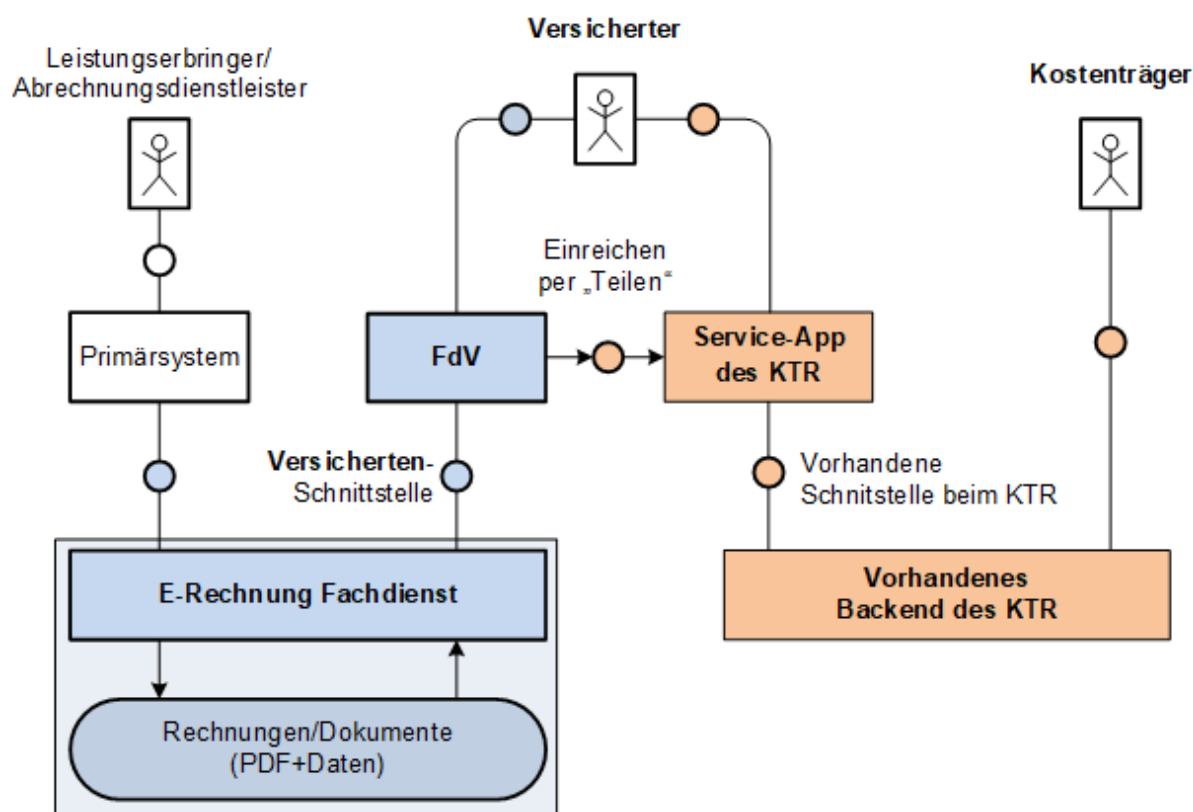


Abbildung 5: Einreichen per "Teilen"

Bei der Einreichung über das Frontend sind zwei Ausprägungen bzgl. der Weitergabe der Daten möglich:

- Weitergabe eines PDF mit strukturierten Daten  
Dabei wird die E-Rechnung (bzw. das Dokument) in Form einer PDF-Datei weitergegeben, in die die strukturierten Daten eingebettet sind - siehe auch 4.3. Damit stehen dem Kostenträger die Daten zur Verfügung, ohne dass dieser sich an den Fachdienst anbinden muss.
- Weitergabe eines Tokens  
Hier wird ggf. die Anbindung des KTR an den Fachdienst genutzt, d.h. die Schnittstelle, über die der KTR (auch) im Fall des Postversands Tokens (eingescannte Barcodes) für den Zugriff auf die Daten nutzt. Beim Einreichen per Frontend wird dazu auch die Weitergabe eines Tokens anstelle der entsprechenden E-Rechnung oder des entsprechenden Dokuments über das Frontend ermöglicht. Die so erhaltenen Token kann der Kostenträger in gleicher Weise wie beim Postversand nutzen, um die zugehörigen Daten aus dem Fachdienst abzurufen.

### 4.3 Angereichertes PDF

Ein Dokument kann somit unter Verwendung des PDF ausgedruckt und z.B. per Postversand - oder auch in digitaler Form (Einreichung über das Frontend) - eingereicht werden. Auch in diesem Fall soll jedoch eine Verwendung der strukturierten Daten möglich sein, um ein aufwändiges Einscannen und anschließendes Auswerten des Dokuments zu vermeiden.

Daher soll der Fachdienst eine Visualisierung des Dokuments im PDF-Format bereitstellen können, bei dem

- das Token als optisch lesbarer Code (Barcode) aufgebracht ist und
- zusätzlich die strukturierten Daten eingebettet sind.

Auf diese Weise kann bei Vorliegen eines Papierausdrucks durch Einscannen des Codes das Dokument-Token gewonnen und damit der Abruf der zugehörigen Daten im Fachdienst ermöglicht werden. Im Falle einer digitalen Weitergabe des PDFs können die strukturierten Daten direkt aus dem PDF entnommen werden.

Ein solches, um den Barcode und die strukturierten Daten erweitertes PDF wird im Folgenden auch *angereichertes PDF* genannt. Das ursprüngliche, in den Fachdienst übergebene PDF wird dagegen auch als *Original-PDF* bezeichnet. Das angereicherte PDF wird vom Fachdienst nach Bedarf erzeugt und bereitgestellt. Der Fachdienst versieht das angereicherte PDF außerdem mit einer fortgeschrittenen Signatur, damit dessen Authentizität und Integrität jederzeit überprüft werden kann (siehe 5.5.7- Authentizität und Integrität von Rechnungen und Dokumenten).

## 4.4 Workflow und Bearbeitungsstatus

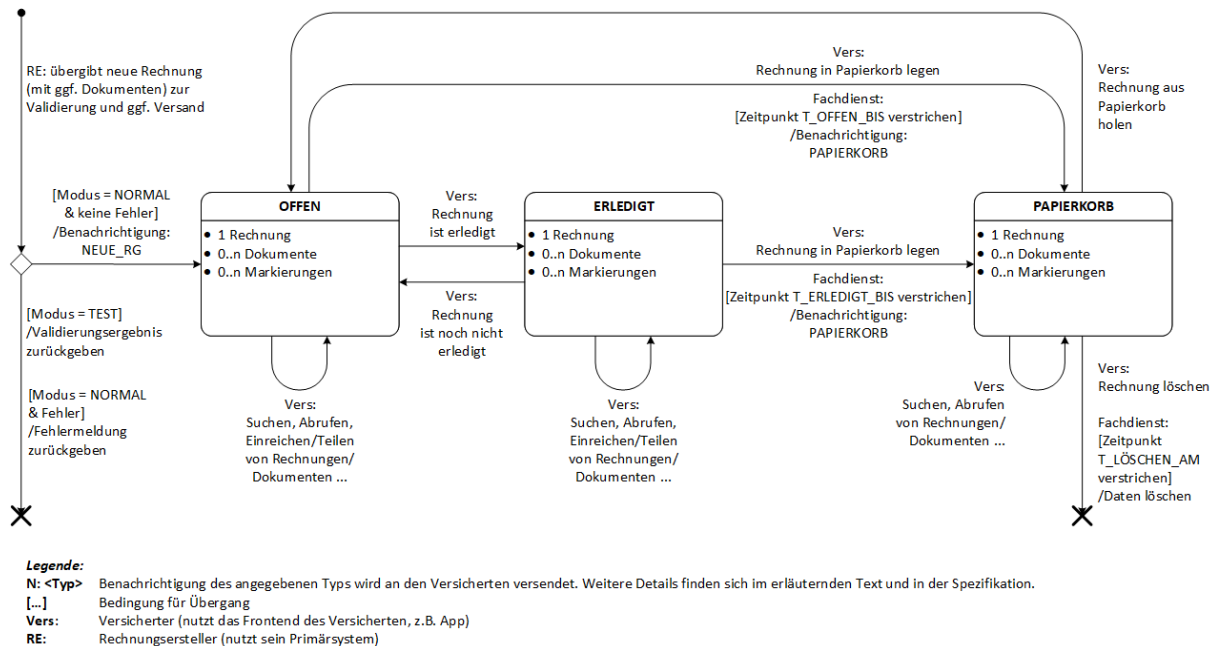
Die eRg soll den Datenaustausch zwischen den angeschlossenen Systemen in koordinierter Weise ermöglichen. Dazu speichert der eRg FD neben den eigentlichen E-Rechnungen und ergänzenden Dokumenten auch den Bearbeitungsstatus einer Rechnung - vom Versenden einer E-Rechnung durch den Rechnungsersteller, über die Bearbeitung der Rechnung durch den Versicherten und ggf. bis zur Übergabe an den KTR.

Der Bearbeitungsstatus wird auf zwei Ebenen erfasst:

1. auf Ebene einer E-Rechnung - welchen Status hat die Rechnung insgesamt? Hier wird ein einfacher Workflow pro Rechnung unterstützt.
2. auf Ebene einzelner Bearbeitungsschritte zu Rechnungen und Dokumenten - insbesondere, ob und wann eine Rechnung oder ein Dokument eingereicht wurde, und bei welchem KTR. Der Bezug zu einem KTR ist dabei möglichst herzustellen, da es mehrere - auch parallele - Einreichungen pro Rechnung bzw. Dokument bei verschiedenen KTR geben kann. Um diese Informationen festzuhalten, werden ergänzend zum Workflow-Status sogenannte "Markierungen" verwendet.

### 4.4.1 Workflow einer Rechnung

Das folgende Bild zeigt die verschiedenen Status und Status-Übergänge, die eine E-Rechnung durchlaufen kann. Die fett beschrifteten Knoten stehen für jeweils einen bestimmten Zustand. Unter jedem Zustandsbezeichner (z.B. "OFFEN") sind die wesentlichen Daten aufgelistet, die zu einer E-Rechnung in diesem Zustand vorliegen. Dies sind zum einen die eigentlichen Rechnungen und Dokumente - diese werden im Prozess nicht mehr verändert. Zum anderen sind es die Markierungen, die jeweils ergänzende Informationen zum Bearbeitungsstand erfassen.



**Abbildung 6: Workflow einer Rechnung**

## Start des Workflows

Ein Rechnungsersteller kann einen Rechnungs-Workflow initiieren, indem er eine E-Rechnung - bestehend aus strukturierten Daten und dem Original-PDF - zusammen mit ergänzenden Dokumenten im Primärsystem (PS) erstellt und an den eRg FD übergibt. Die Art der Bearbeitung durch den eRg FD kann dabei durch den Parameter "Modus" gesteuert werden, den das aufrufende PS mit übergeben kann:

- Modus = TEST

Der eRg FD validiert die übergebenen Daten. Der eRg FD gibt das Ergebnis der Validierung zurück, d.h. ggf. die gefundenen Fehler. Der Modus dient nur der Validierung und führt daher nicht zu einem Workflow.

- Modus = NORMAL (dies ist der Default)

Der eRg FD validiert die übergebenen Daten. Falls dies keine gravierenden Fehler ergibt, werden alle übergebenen Daten gespeichert und der Rechnungs-Workflow angelegt. Andernfalls gibt der eRg FD die erkannten Fehler zurück. Ein Rechnungs-Workflow wird dann nicht angelegt.

Soll ein Workflow angelegt werden, dann gilt Folgendes:

- Das Primärsystem kann bei der Übergabe mittels Parameter steuern, ob zu einer Rechnung bzw. einem Dokument ein angereichertes PDF (siehe 4.3) vom Fachdienst erzeugt und bereitgestellt werden soll.
- Der eRg FD speichert die übergebene Rechnung sowie zugehörige Dokumente und verknüpft diese mit dem Workflow.
- Zusätzlich erzeugt und speichert er pro Rechnung bzw. Dokument ein Token, über das die Rechnung bzw. das Dokument fortan identifiziert werden kann. Jedes Token muss auf einem eindeutigen, nicht erratbaren Zufallswert aufbauen.
- Der eRg FD gibt im Erfolgsfall diese Token zurück und - falls gewünscht - das jeweilige angereicherte PDF. Dieses kann z.B. genutzt werden, falls ein Ausdruck der Rechnung mit Barcode für den Versicherten benötigt wird.

- Der Fachdienst erzeugt für jede E-Rechnung und jedes ergänzende Dokument jeweils eine Signatur der strukturierten Daten und des PDF (siehe 5.5.7- Authentizität und Integrität von Rechnungen und Dokumenten) und speichert diese.
- Der eRg FD löst eine Benachrichtigung (NEUE\_RG - Vorliegen einer neuen E-Rechnung) an den Versicherten aus, sodass dieser über das Vorliegen einer neuen E-Rechnung informiert wird.
- Der Workflow beginnt im Status "OFFEN".

### Status einer Rechnung

Eine E-Rechnung (inkl. der zugehörigen Dokumente) kann sich im Workflow-Status "OFFEN", "ERLEDIGT" oder "PAPIERKORB" befinden. Diese Status und die Wechsel zwischen ihnen werden im Folgenden beschrieben. Da Dokumente hier stets als Ergänzungen zu einer Rechnung gelten, bezieht sich der Status einer E-Rechnung stets auch auf die zugehörigen Dokumente, für die daher kein eigener Status vorgesehen ist.

- **Status "OFFEN"**

Sobald eine E-Rechnung im Zustand "OFFEN" im eRg FD vorliegt, kann diese über das eRg FdV abgerufen werden. Der Versicherte kann die E-Rechnung und die zugehörigen Dokumente einsehen, sie in seine persönliche Ablage übernehmen ("Download", "Teilen") oder auch umgehend oder zu einem späteren Zeitpunkt bei einem Kostenträger einreichen. Der Status "OFFEN" soll allgemein im eRg FdV dem Versicherten bei der Auswahl derjenigen E-Rechnungen helfen, bei denen noch Aktionen auszuführen sind.

Der Status "OFFEN" kann auch durch folgende Nutzerinteraktionen im eRg FdV erreicht werden:

- Der Versicherte "verschiebt" eine bereits auf "ERLEDIGT" stehende E-Rechnung (siehe auch Status "ERLEDIGT" weiter unten) nach "OFFEN", da sie aus bestimmten Gründen für ihn *noch nicht erledigt ist* und in diesem Sinne von ihm als offen betrachtet wird - dies kann z.B. der Fall sein, wenn eine bereits eingereichte Rechnung erneut eingereicht werden soll (etwa bei einem anderen KTR) oder weil der Versicherte diese erst als erledigt betrachtet, wenn er diese bezahlt hat.
- Der Versicherte verschiebt eine E-Rechnung aus dem Papierkorb in den Status "OFFEN", da er diese noch benötigt und sie daher noch nicht gelöscht werden darf. Die Frist für die automatische Löschung wird verlängert (siehe 5.5.6.3- Fristen für die Löschung und Aufbewahrung von Rechnungen und Dokumenten). (siehe auch Status "PAPIERKORB" weiter unten)

*Hinweis: Die Markierung "eingereicht" bleibt erhalten, falls eine Rechnung in den Status OFFEN verschoben wird. Es könnte daher ggf. ein Hinweis an den Versicherten gegeben werden, wenn eine erneute Einreichung erkannt wird. Dieses wäre in der Umsetzungsfreiheit des FdV-Herstellers.*

- **Status "ERLEDIGT"**

Sobald aus Sicht des Versicherten bei einer Rechnung aktuell nichts zu tun ist, kann diese in den Zustand "ERLEDIGT" verschoben werden. Da der Versicherte auch selbst entscheiden kann, dass eine offene E-Rechnung "für ihn erledigt ist", soll er über das eRg FdV die Möglichkeit erhalten, eine E-Rechnung vom Status "OFFEN" direkt auf "ERLEDIGT" zu setzen. Ein typisches Anwendungsszenario dafür sind E-Rechnungen, die der Versicherte gar nicht einreichen möchte.

In der Abbildung ist auch der Fall vorgesehen, dass der Versicherte sich bei einer bereits erledigten E-Rechnung entscheidet, die Einordnung als "ERLEDIGT" zurückzunehmen. Dies ist mit dem entsprechenden Zustandsübergang von "ERLEDIGT" zu "OFFEN" erfasst. Dies bildet u.a. das Anwendungsszenario ab, dass der Versicherte die Absicht hat, eine bereits bei einem KTR eingereichte und bearbeitete E-Rechnung bei einem weiteren KTR einzureichen.

- **Status "PAPIERKORB" (zu löschen)**

Der Versicherte soll im eRg FdV die Möglichkeit bekommen, E-Rechnungen im Status "OFFEN" oder "ERLEDIGT" in den Papierkorb zu verschieben (Status "PAPIERKORB"). In diesem Zustand kann die E-Rechnung von ihm manuell unwiederbringlich gelöscht werden.

#### **4.4.1.1 Automatische Verschiebung und Löschung von Rechnungen**

Daten im E-Rechnung Fachdienst sollen dort nicht zeitlich unbegrenzt gespeichert werden. Daher werden E-Rechnungen aus den Zuständen "OFFEN" und "ERLEDIGT" durch den Fachdienst automatisiert in den Status "PAPIERKORB" überführt, wenn die jeweils festgelegte Frist für die Aufbewahrung in einem dieser Zustände (T\_OFFEN\_BIS bzw. T\_ERLEDIGT\_BIS) verstrichen ist. Der Versicherte soll dann durch eine Benachrichtigung über die Verschiebung in den Papierkorb und die bevorstehende Löschung der Daten (PAPIERKORB) informiert werden, sodass er in jedem Fall die Möglichkeit hat, eine E-Rechnung vor der endgültigen Löschung auszudrucken, oder sie in seiner persönlichen Datenablage oder seiner elektronischen Patientenakte (ePA) zu speichern.

Der Versicherte erhält auf diese Weise außerdem die Möglichkeit, eine E-Rechnung aus dem Status "PAPIERKORB" wieder auf "OFFEN" zu setzen, wenn er diese vor einer endgültigen Löschung bewahren möchte. In diesem Fall wird die Frist für die Aufbewahrung im Zustand "OFFEN" neu gesetzt. Eine E-Rechnung im Status "PAPIERKORB" wird unwiederbringlich gelöscht, sobald die festgelegte Löschfrist (T\_LÖSCHEN\_AM) überschritten ist. Die längste Aufbewahrungsdauer sind 10 Jahre. Zu den verschiedenen erwähnten Fristen siehe auch Abschnitt 5.5.6.3.

Es muss ausgeschlossen werden, dass eine Löschung erfolgt, ohne dass der Versicherte ausreichend Gelegenheit hatte, die E-Rechnung in eine von ihm gewählte Ablage oder seine elektronische Patientenakte zu übernehmen.

Nach Löschung einer E-Rechnung aus dem Fachdienst muss eine erneute Vergabe des verwendeten Rechnungs-Tokens für eine andere E-Rechnung ausgeschlossen werden.

#### **4.4.1.2 Stornierung und Korrektur von Rechnungen**

Das Stornieren einer in den Fachdienst eingestellten, zugestellten oder ggf. bereits eingereichten E-Rechnung wird nicht aktiv durch eine Operation des Fachdienstes unterstützt. In den meisten Fällen der Stornierung sendet der Rechnungsersteller eine Korrekturrechnung an den Versicherten, die Bezug auf die somit stornierte Rechnung nimmt. Dieser Use Case wird insofern vom Fachdienst abgebildet, dass in den strukturierten Rechnungsdaten angegeben werden kann, ob es sich um eine Korrekturrechnung handelt und auf welche Rechnung sich die Korrektur bezieht (siehe 4.8.1.1- Rechnung).

#### **4.4.2 Markierungen**

Unabhängig vom Status einer E-Rechnung soll es dem Nutzer auch ermöglicht werden, bestimmte "Markierungen" an E-Rechnungen vorzunehmen. Beispielsweise könnte ein Versicherter bestimmte E-Rechnungen als "bezahlt" markieren, wenn er den Rechnungsbetrag beglichen hat. Der Bezahlprozess an sich ist nicht Teil des eRg FD,



aber ein Vermerk, dass dieser durchgeführt wurde, kann festgehalten werden. Darüber hinaus soll das eRg FdV die Möglichkeit bieten, E-Rechnungen oder Dokumente als ungelesen oder gelesen zu markieren - etwa, um noch nicht gelesene Rechnungen optisch hervorzuheben.

Markierungen können einerseits durch das eRg FdV erzeugt, bearbeitet und gelöscht werden. Dies kann nach Bedarf automatisch oder manuell durch den Nutzer erfolgen. Neben dem Rechnungsempfänger (Versicherter) kann jedoch auch der Rechnungsersteller Markierungen bei der Erstellung von Rechnungen vorgeben (siehe unten, Markierung "Persönlich"). In diesem Fall erfolgt das Setzen der Markierung bei der Übergabe der entsprechenden Dokumente durch das PS. Des Weiteren kann der Fachdienst bei bestimmten Vorgängen Markierungen setzen, etwa die Markierung "Abgerufen durch Kostenträger", wenn der Kostenträger E-Rechnungen oder Dokumente über die KTR-Schnittstelle abgerufen hat.

Die vorgesehenen Typen und Inhalte der Markierungen werden hier zunächst abschließend aufgeführt. Diese sollen jedoch zukünftig flexibel erweiterbar sein. Die folgende Tabelle zeigt eine Übersicht der vorgesehenen Typen von Markierungen. Im Folgenden werden diese kurz beschrieben.

**Tabelle 1: Typen von Markierungen**

<b>Typ der Markierung</b>	<b>Mehrfach-Markierung ?</b>	<b>Verwendung (wann und durch wen)</b>	<b>Verknüpfungen</b>	<b>ergänzende Informationen</b>
Eingereicht (per Frontend)	ja, eine pro Kostenträger	Bei Einreichung durch Versicherten	- Versicherter, der einreicht - optional: Kostenträger, bei dem eingereicht wird	- Zeitpunkt - optional: Details
Eingereicht (per Post)	ja, eine pro Kostenträger	Bei Postversand durch Versicherten	- Versicherter, der einreicht - optional: Kostenträger, bei dem eingereicht wird	- Zeitpunkt - optional: Details
Geteilt	ja, eine pro Kostenträger	Bei Teilen durch den Versicherten	- Versicherter, der Dokument/Rechnung teilt - optional: Kostenträger, mit dem geteilt wird	- Zeitpunkt - optional: Details
Abgerufen durch Kostenträger	ja, eine pro Kostenträger	Bei Abruf eines Dokuments/einer Rechnung durch den Kostenträger, durch den Fachdienst	- Versicherter, - Kostenträger, der abgerufen hat	- Zeitpunkt
Gelesen	nein	Beim Einsehen von Rechnungen oder	- Versicherter	- gelesen ja/nein



		Dokumenten durch den Versicherten im eRg FdV		
Bezahlt	nein	Bei Zahlung durch den Versicherten	- Versicherter	- Zeitpunkt - optional: Details
Archiviert	nein	Bei Archivierung durch den Versicherten	- Versicherter	- Art der Archivierung: ePA oder persönliche Ablage - optional: Details
Persönlich	nein	Durch den Rechnungsersteller bei Versenden von Dokumenten, die ausschließlich nur persönlich an den Versicherten gerichtet sind.	- Versicherter	- optional: Details

#### 4.4.2.1 Einreichung per Frontend

Sobald ein Versicherter eine oder mehrere E-Rechnungen auswählt, um diese mittels eRg FdV bei einem KTR einzureichen, wird jede ausgewählte und an den KTR weitergegebene E-Rechnung bzw. jedes Dokument mit einer Markierung versehen, welche die E-Rechnung bzw. das Dokument als "Eingereicht (per Frontend)" kennzeichnet. Eine solche Markierung sollte erst dann ergänzt werden, wenn durch die Umsetzung im eRg FdV auch die erfolgreiche Weitergabe der Daten an den ausgewählten KTR sichergestellt ist. Der Zeitpunkt der Einreichung und der KTR werden dabei festgehalten.

#### 4.4.2.2 Einreichung per Post

Sollte eine Einreichung auf digitalem Weg nicht möglich sein oder der Versicherte aus anderen Gründen eine Einreichung auf dem Postweg vornehmen wollen, dann kann er die entsprechenden Rechnungen und Dokumente über das eRg FdV vom Fachdienst als angereichertes PDF abrufen und ausdrucken. Die Markierung "Eingereicht (per Post)" kann verwendet werden, um die eingereichten Rechnungen und Dokumente zu kennzeichnen und den Zeitpunkt festzuhalten. Der Versicherte hat außerdem die Möglichkeit, den adressierten KTR zuzuordnen und bei Bedarf weitere Details als Freitext festzuhalten.

#### 4.4.2.3 Einreichung per "Teilen"

Auf mobilen Endgeräten kann die Einreichung beim Kostenträger auch dadurch erfolgen, dass mittels eRg FdV die einzureichenden Rechnungen und Dokumente als angereichertes PDF geladen und per ausschließlich geräteinterner "Teilen-Funktion" auf digitalem Weg an den KTR geschickt werden, beispielsweise durch Weitergabe an eine "Service-App" des Kostenträgers.

Da bei diesem Verfahren die tatsächliche Weitergabe der Daten im eRg FdV nicht sichergestellt werden kann, sollten solche Dokumente und Rechnungen nur als "Geteilt" markiert werden, wobei wieder der Zeitpunkt festzuhalten ist. Eine Zuordnung des KTR und weitere Details können optional ergänzt werden.

Die Markierung "Geteilt" kann zudem allgemein genutzt werden, um die Weitergabe an andere Empfänger (z.B. Finanzamt, Steuerberater ...) zu vermerken.

#### **4.4.2.4 Abgerufen durch Kostenträger**

Sobald ein KTR Daten zu einem Dokument oder einer Rechnung abrufen, wird diese(s) mit einer Markierung "Abgerufen durch Kostenträger" versehen, dabei werden der KTR und der Zeitpunkt festgehalten. Die Markierung ermöglicht den Nachvollzug des Abrufs und damit auch eine bessere Kontrolle darüber, ob Daten aus dem Fachdienst gelöscht werden können.

#### **4.4.2.5 Gelesen**

Mit der Markierung "Gelesen" (ja oder nein) können Rechnungen und Dokumente als gelesen oder ungelesen gekennzeichnet werden.

#### **4.4.2.6 Beahlt**

Mit der Markierung "Beahlt" können Rechnungen und Dokumente als bezahlt gekennzeichnet werden, wobei der Zeitpunkt festgehalten wird und ggf. weitere Details als Freitext erfasst werden können ("Bar bezahlt in der Arztpraxis", "per PayPal" ...).

#### **4.4.2.7 Archiviert**

Die Markierung "Archiviert" kann verwendet werden, um festzuhalten, welche Rechnungen und Dokumente bereits per eRg FdV in die ePA des Versicherten übertragen wurden. Falls der Versicherte alternativ eine eigene persönliche Ablage verwendet, kann dies ebenfalls vermerkt werden, und es können ggf. zusätzliche Details als Freitext erfasst werden ("Auf PC gespeichert", "Abgeheftet" ...).

#### **4.4.2.8 Persönlich**

Falls ein Rechnungsersteller beim Rechnungsversand ein Dokument anhängt, welches nur für den Rechnungsempfänger persönlich gedacht ist, kann diese Markierung verwendet werden. Die Markierung ermöglicht es, solche Dokumente gesondert zu behandeln - beispielsweise können diese im eRg FdV besonders optisch hervorgehoben werden und beim Versuch der Weitergabe durch Teilen oder Einreichen könnte der Nutzer gewarnt werden.

### **4.4.3 Aktive Benachrichtigungen**

Der Versicherte muss über bestimmte Vorgänge aktiv informiert werden. Dazu versendet der Fachdienst (Anwendungsdienst) eine entsprechende Benachrichtigung an den Nutzer. Dabei wird der gleiche technische Benachrichtigungsweg verwendet, der bei der Registrierung eines Nutzer-Endgerätes (Client Registrierung) auch zur Übermittlung eines Bestätigungs-Code verwendet und damit auch validiert wurde, siehe auch [5.4.5](#).

Der Fachdienst darf Benachrichtigungen für einen Versicherten nur auslösen, wenn er vom eRg FdV des Versicherten eine zuvor eingeholte informierte Einwilligung in das Verfahren übermittelt bekommen hat. Beim Einholen dieser Einwilligung müssen

- die Datenübermittlung und die übertragenden Metainformationen dargestellt werden,

- die Nutzer ggf. auf typische Risiken der eingesetzten Technologie hingewiesen werden (z.B. erschwerte Durchsetzung von Betroffenenrechten, fehlende Kontrolle der Weiterverarbeitung und Übermittlung der Daten, fehlende Datenschutzaufsicht oder Zugriffe durch staatliche Stellen, sofern Daten in ein Drittland übertragen werden).

Der Fachdienst muss sich die Einwilligung merken und wieder löschen, wenn der Versicherte seine Einwilligung zurückgezogen hat.

Für eine Benachrichtigung dürfen nur folgende Informationen verwendet werden:

- Typ der Benachrichtigung (siehe Tabelle unten), d.h. aus dem Text der Nachricht und dem Betreff darf nur allgemein die Art des Vorgangs hervorgehen.
- Empfänger der Benachrichtigung (Identifikation des Versicherten) zwecks Zustellung an diesen

Die abschließenden Festlegungen zur technischen Umsetzung der Benachrichtigungen sind in [gemF\_Zero-Trust] beschrieben.

Der Fachdienst darf beim Versenden von Benachrichtigungen keine weiteren Daten - insbesondere Gesundheitsdaten oder weitere personenbezogene Daten - übermitteln. Den eigentlichen Gegenstand der Mitteilung an den Versicherten - etwa die Inhalte einer E-Rechnung oder eines Dokuments - kann der Versicherte nur über das eRg FdV nach erfolgter Authentifizierung und Autorisierung einsehen.

**Tabelle 2: Typen von Benachrichtigungen**

Typ der Nachricht	Erläuterung (Bedeutung der Benachrichtigung aus Sicht des Versicherten)
NEUE_RG	Es liegen eine neue E-Rechnung und ggf. zugehörige Dokumente vor.
PAPIERKORB	Eine E-Rechnung und ggf. zugehörige Dokumente wurden vom Fachdienst in den Papierkorb verschoben, da diese zu lange unbearbeitet im Zustand OFFEN oder ERLEDIGT im Fachdienst lagen. Es wird eine automatische Löschung nach Ablauf einer Frist erfolgen, wenn der Nutzer nichts dagegen unternimmt. (Siehe auch <a href="#">5.5.6.3</a> zu Fristen und automatischer Löschung)
KONTO_LÖSCHUNG	Für ein Nutzerkonto steht die Löschung bevor, da der Nutzer zu lange inaktiv war. Es wird eine automatische Löschung nach Ablauf einer Frist erfolgen, wenn der Nutzer nichts dagegen unternimmt. (Siehe auch <a href="#">5.5.6.2</a> zu Fristen und automatischer Löschung)

## 4.5 Nutzung der elektronischen Patientenakte (ePA)

Im Sinne der Datensparsamkeit und Zweckgebundenheit erfolgt keine langfristige Speicherung von E-Rechnungen und ergänzenden Dokumenten über den Kontext der oben beschriebenen Workflows hinaus. Stattdessen soll dem Versicherten eine einfache Möglichkeit geboten werden, diese Dokumente in seine ePA zu übertragen. Dies soll zunächst durch Übergabe der Dokumente vom eRg FdV an das ePA FdV erfolgen (z.B. durch "Teilen"-Funktion), mit dem dann der Versicherte die Dokumente in seiner ePA ablegen kann.

Dem Versicherten steht es weiterhin frei, sich gegen eine Nutzung der ePA zu entscheiden. Für diesen Fall muss die eRg eine Möglichkeit anbieten, die Dokumente in die persönliche Ablage des Versicherten außerhalb der ePA zu überführen. Dies kann in digitaler Form durch Herunterladen der PDF-Dateien oder auch in Form eines papiergebundenen Ausdrucks erfolgen.

## **4.6 Berechtigungen**

Der Zugriff der unterschiedlichen Client-Systeme auf den eRg FD darf nur nach Autorisierung erfolgen, basierend auf

1. der Erfüllung grundlegender Sicherheitsanforderungen - z.B. wird ein geeignetes, d.h. hinreichend sicheres und dem Nutzer zugeordnetes Endgerät verwendet?
2. den Identitäten der Nutzer, bereitgestellt durch den entsprechenden Identity Provider (IDP), sowie
3. den im eRg FD durch die Nutzer verwalteten Berechtigungsregeln - etwa Berechtigungen als abweichender Rechnungsempfänger, Berechtigungen aufgrund eines Betreuungsverhältnisses usw.

Im Folgenden werden nur die Berechtigungen betrachtet, die sich aus Identitäten der Nutzer und Berechtigungsregeln ergeben. Der erste Punkt wird später betrachtet, siehe auch [5.3.3](#).

Der Autorisierungsdienst des eRg FD muss für jeden Zugriff sicherstellen, dass die Berechtigung für die durchzuführende Operation und die betroffenen Daten für den Nutzer gegeben ist.

### **4.6.1 Rollenbasierte Berechtigungen**

Die verschiedenen Nutzer sind auf unterschiedliche Weise an dem Gesamtprozess des eRg FD beteiligt. Um Zugriffe, die nicht prozesskonform sind, auszuschließen, verfügen die Nutzer über beschränkte Berechtigungen. Diese Berechtigungen ergeben sich bereits aus ihrer Rolle gemäß Object Identifier (OID, siehe [gemSpec\_OID]). Je nach Nutzerrolle stehen nur bestimmte Typen von Operationen zur Verfügung, siehe folgende Beispiele:

- Nur Rechnungsersteller (LEI, ADL) dürfen E-Rechnungen versenden.
- Nur Versicherte dürfen E-Rechnungen einreichen oder löschen.

### **4.6.2 Nutzerbasierte Berechtigungen**

Zusätzlich zu den rollenbasierten Berechtigungen gelten Berechtigungen für den einzelnen Nutzer, identifiziert durch die Telematik-ID der Institution (LEI, ADL, KTR) oder die Krankenversichertennummer (Versicherte), siehe auch Abschnitt [5.4.2.1](#). Ein Zugriff ist auf bestimmte, der Identität des Nutzers (seinem "Nutzerkonto") zugeordnete Daten beschränkt. So kann beispielsweise ein bestimmter Rechnungsersteller nur E-Rechnungen übermitteln, in denen er als Rechnungsersteller zugeordnet ist. Ein bestimmter Versicherter kann nur E-Rechnungen abrufen, bei denen er als Rechnungsempfänger zugeordnet ist, usw.

### 4.6.3 Regelbasierte Berechtigungen

Als weiterer Typ von Berechtigung wird hier die regelbasierte Berechtigung betrachtet. Solche Berechtigungen können durch einen Nutzer erstellt und verwaltet werden. Dabei wird einem bestimmten Nutzer das Recht eingeräumt, auf Daten eines bestimmten anderen Nutzers zuzugreifen - oder allgemein: Funktionen auszuführen, von denen der andere Nutzer betroffen ist. Ein Beispiel stellt die Berechtigung eines Rechnungserstellers dar, E-Rechnungen an einen bestimmten Versicherten schicken zu dürfen. Diese - im Folgenden Rechnungsversandberechtigung genannte - Berechtigung kann durch den Versicherten für einen bestimmten Rechnungsersteller vergeben oder zurückgezogen werden.

#### 4.6.3.1 Allgemeines

Eine solche Berechtigung kann durch einen Nutzer selbst über das eRg FdV (allgemein: Client-System) als Regel im Fachdienst angelegt und bearbeitet werden. Der eRg FD sieht ein Berechtigungskonzept vor, das in der ersten Ausbaustufe zunächst die oben erwähnte Rechnungsversandberechtigung unterstützt. In zukünftigen Ausbaustufen sind weitere Berechtigungstypen vorgesehen, wie die Vergabe von Zugriffsrechten von einem Versicherten an einen anderen Versicherten - etwa beim "Familienmanagement" oder bei Vertreterregelungen. Das Berechtigungskonzept sieht eine Erweiterbarkeit um solche weiteren Berechtigungstypen vor.

Bei der Anlage einer regelbasierten Berechtigung kann es sein, dass der betroffene Nutzer selbst der *Initiator* ist, also "ein Recht erteilt oder anbietet". Der berechtigte Nutzer kann dann die Berechtigung annehmen oder ablehnen. Es ist aber auch denkbar, dass der berechtigte Nutzer selbst die Berechtigung initiiert, also eine Berechtigung anfragt. In diesem Fall kann dann der betroffene Nutzer diese Berechtigung gewähren oder verwehren.

Es gelten daher folgende konkrete Festlegungen und *Rollenbezeichner* bei regelbasierten Berechtigungen:

- Es gibt genau einen *Berechtigten* - der Nutzer, dem durch die Regel eine Berechtigung zugewiesen wird.
- Es gibt genau einen *Betroffenen* - der Nutzer, der von der Ausübung der Berechtigung betroffen ist.
- Es gibt genau einen *Initiator* - der Nutzer, der die Anlage einer Berechtigung initiiert (hat).
- Es gibt genau einen *Bestätiger* - dieser Nutzer kann eine vom Initiator angelegte Berechtigung bestätigen oder ablehnen.

Weitere allgemeine Festlegungen:

- Ein Bestätiger kann eine anstehende oder bereits von ihm vorgenommene Bestätigung verweigern bzw. zurücknehmen, also
  - eine ihm angebotene Berechtigung ablehnen (Bestätigender ist gleichzeitig Berechtigter) - bzw.
  - eine ihn betreffende Berechtigung (Bestätigender ist gleichzeitig Betroffener) verwehren.
- Eine durch einen Nutzer verweigte Bestätigung kann nur von dem gleichen Nutzer wieder zurückgenommen werden, d.h. nur er kann die Berechtigungsregel "reaktivieren".

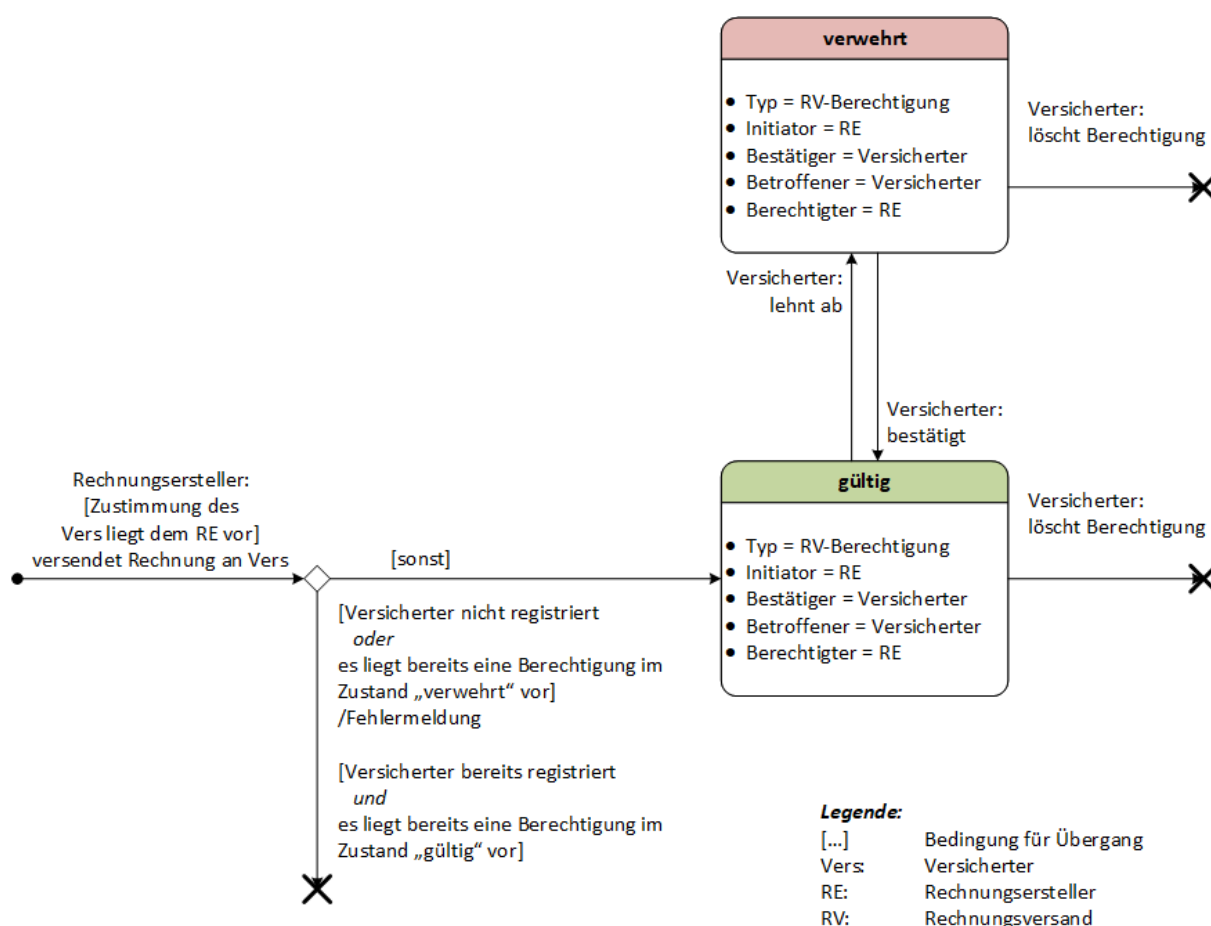
#### 4.6.3.2 Berechtigungsregeln im E-Rechnung Fachdienst

Im MVP sind für die Anwendung E-Rechnung nur Berechtigungen vom Typ *Rechnungsversandberechtigung* vorgesehen. Eine Rechnungsversandberechtigung bestimmt, ob ein bestimmter Rechnungsersteller E-Rechnungen oder Dokumente an einen bestimmten Versicherten als Rechnungsempfänger schicken darf oder nicht.

Für die weiteren Betrachtungen gelten diese Annahmen:

- Mit der Einrichtung seines Nutzerkontos stimmt der Versicherte grundsätzlich der Verarbeitung seiner Daten im Kontext der E-Rechnung zu.
- Ergänzend dazu holt der Rechnungsersteller vor dem Versand einer ersten E-Rechnung an einen Versicherten dessen Einwilligung zum Versand von E-Rechnungen ein.
- Der Versicherte soll zusätzlich die technische Möglichkeit erhalten, über das eRg FdV einen bestimmten Rechnungsersteller "sperrern" oder (wieder) "entsperren" zu können.

Ausgehend von diesen Annahmen gilt für eine Rechnungsversandberechtigung das unten dargestellte Status-Diagramm.



**Abbildung 7: Status-Diagramm Rechnungsversandberechtigung**

Die individuelle Regel wird automatisch durch den Fachdienst angelegt, wenn

1. der Versicherte ein Nutzerkonto eingerichtet hat mit Zustimmung zum Erhalt von E-Rechnungen und

2. der Rechnungsersteller erstmalig eine E-Rechnung an den Versicherten schickt.

Auf diese Weise kann der Versicherte in seiner Rechteverwaltung fortan den Rechnungsersteller als derzeit berechtigt sehen. Bei Bedarf kann er diese Berechtigung individuell für den Rechnungsersteller ablehnen, danach wieder bestätigen, usw. Der Versicherte kann den Eintrag auch löschen, womit der Ausgangszustand wiederhergestellt ist.

### 4.7 Protokollierung für den Nutzer

Um dem Versicherten eine Transparenz bezüglich der Zugriffe auf seine Daten zu gewährleisten, müssen die Zugriffe durch die verschiedenen Nutzer im Nutzerprotokoll vermerkt werden. Dazu wird erfasst, welcher Nutzer wann und zu welchem Zweck (ausgeführte Operation) auf welche Daten zugegriffen hat. Siehe dazu auch die Darstellungen zum Protokolleintrag in Kapitel [4.8.6- Protokolleintrag](#) und [5.5.9- Nutzerprotokolle](#).

### 4.8 Informationsmodell

Der eRg FD muss die im Bild unten dargestellten Informationen in geeigneter Form speichern und Operationen auf diese Daten über seine Schnittstellen bereitstellen.

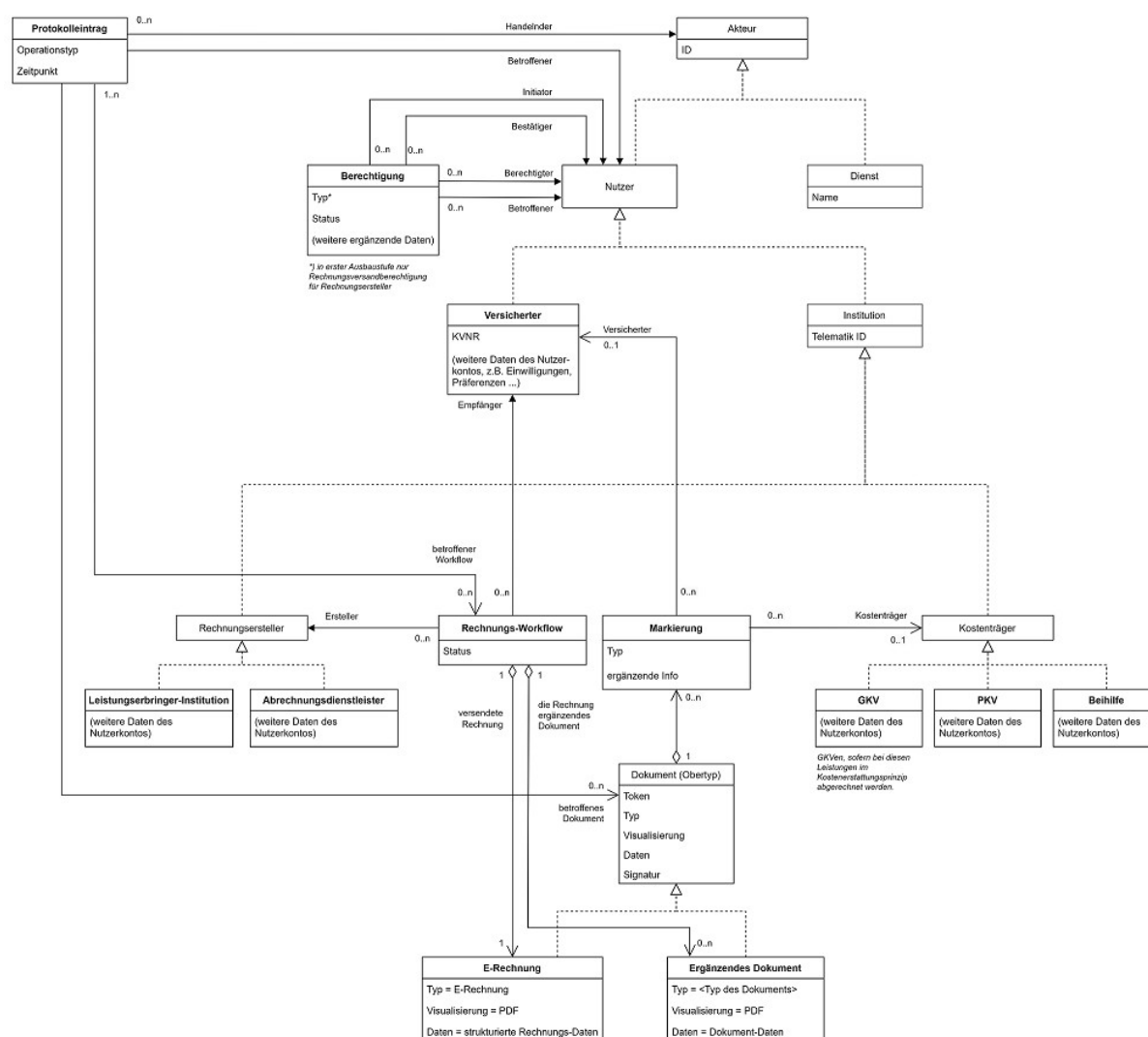


Abbildung 8: Informationsmodell der Anwendung E-Rechnung

Im Folgenden wird das Informationsmodell im Überblick vorgestellt. Die detaillierte und abschließende Festlegung der Datentypen, zulässigen Werte usw. findet man in der Spezifikation als FHIR Ressourcen und Operationen, siehe [gemSpec\_eRg\_FD] .

#### 4.8.1 Dokument (Obertyp)

Der eRg FD unterstützt den Austausch verschiedener Typen von Dokumenten, d.h. E-Rechnungen und ergänzende Dokumente. Diese bestehen jeweils aus:

- **Dokument-Token:**  
Jedes im Fachdienst abgelegte Dokument (E-Rechnung, ergänzendes Dokument) erhält dort einen vom Fachdienst erzeugten, eindeutigen, nicht erratbaren Zufallswert als Identifikator - im Folgenden kurz Dokument-Token - oder im Fall von Rechnungen - auch Rechnung-Token genannt. Das Dokument-Token enthält keine personenbezogenen oder medizinischen Daten. Über das Dokument-Token können jedoch zu einem Dokument sowohl die Visualisierung als auch die strukturierten Daten beim Fachdienst abgerufen werden, sofern der Nutzer dazu berechtigt ist.



- **Visualisierung des Dokuments:**  
Die Visualisierung soll ermöglichen, dass E-Rechnungen oder ergänzende Dokumente im originalen Aussehen (vom Ersteller gewünschtes Aussehen) ausgedruckt, verschickt und auf einem Frontend angezeigt werden können. Das Format der Visualisierung ist vom Dokumententyp abhängig, wobei im MVP nur PDF vorgesehen ist.
- **Strukturierte Daten:**  
Die strukturierten Daten dienen der automatisierten Verarbeitung. Struktur, Inhalt und Umfang sind dabei vom Dokumententyp abhängig.
- **Signatur:**  
Bei der Speicherung eines neuen Dokuments im Fachdienst erzeugt der Fachdienst eine fortgeschrittene digitale Signatur für das Dokument, d.h. über Visualisierung und strukturierte Daten.

#### 4.8.1.1 Rechnung

Eine E-Rechnung wird vom eRg FD als Dokument mit dem besonderen Typ "E-Rechnung" abgebildet. Dieses umfasst das *Original-PDF* und den zugehörigen strukturierten Rechnungsdatensatz, wie vom PS des Rechnungserstellers an den Fachdienst übergeben. (Auf Basis dieser Daten wird vom Fachdienst bei Bedarf das für die Ausgabe relevante *angereicherte PDF* bereitgestellt.) Zusätzlich erhält die E-Rechnung stets eine Signatur, erstellt durch den Fachdienst. Diese umfasst das Original-PDF und die strukturierten Daten. Details zum Signaturverfahren werden in [gemSpec\_eRg\_FD] beschrieben.

Die grundlegenden Datenfelder für die Teilmenge der strukturierten Rechnungsdaten und notwendige Pflichtangaben im MVP sind in der folgenden Tabelle dargestellt. Diese bezieht sich auf die in 1.5- Umfang des MVP genannten Funktionalitäten des MVP. Die technischen Details werden in der FHIR Spezifikation festgelegt, siehe [gemSpec\_eRg\_FD].

Neben den aufgelisteten inhaltlichen Daten, werden als technische Daten die Telematik-ID des Rechnungserstellers und das vom FD vergebene Rechnungstoken ergänzt.

Das Fehlen einer Pflichtangabe wird im MVP als gravierender Fehler gemeldet und führt zu einer Ablehnung der Rechnung durch den Fachdienst. Weitere Validierungen hinsichtlich gravierender oder nicht gravierender Fehler können in einer Ausbaustufe hinzukommen (siehe auch 1.7.2- Verwendete Begriffe).

Tabelle 3: Grundlegende Datenfelder einer E-Rechnung im MVP

Bezeichner	Datenfelder	GOÄ relevante Datenfelder im Bezug auf die Gebührenord- nung, Pflichtangab- en (MUSS) siehe letzte Spalte	GOZ relevante Datenfelder im Bezug auf die Gebührenord- nung, Pflichtangab- en (MUSS) siehe letzte Spalte	Pflichtangabe n (MUSS) führen bei Fehlen zu einer Ablehnung der Rechnung bei der Erstellung im Fachdienst Ziel: zuverlässige Zustellung und Verarbeitbar- keit der Rechnung
Typ des Dokuments	Auswahl aus	x	x	

	Verzeichnis nach [KDL CodeSystem], hier: AM0101 - Abrechnungsdokumente			
Abrechnungsart	Auswahl aus Liste: <ul style="list-style-type: none"> <li>Standard (Default)</li> <li>Abrechnung nach §13 Abs. 2 SGB</li> </ul>	x	x	
Behandlungsart	Auswahl aus Liste (nur ambulante Behandlung Teil des MVPs): <ul style="list-style-type: none"> <li>ambulante Behandlung (Default)</li> </ul>	x	x	
Fachrichtung	Auswahl aus Verzeichnis nach [IHE Profile]	x	x	
Rolle: Behandelnder Leistungserbringer (Mehrfachnennung möglich)	Person: <ul style="list-style-type: none"> <li>Anrede, Titel, Vorname, Nachname</li> <li>Straße, Hausnummer</li> <li>PLZ, Ort</li> </ul> ODER Institution: <ul style="list-style-type: none"> <li>IK-Nummer</li> <li>Institutionsname</li> <li>Straße, Hausnummer</li> <li>PLZ, Ort</li> </ul> UND Fachrichtung: Auswahl aus Verzeichnis (z.B. Zahnarzt) ODER nach [IHE Profile]	x	x	MUSS
Rolle: Forderungsinhaber	Person: <ul style="list-style-type: none"> <li>Anrede, Titel, Vorname,</li> </ul>	x	x	MUSS

	Nachname <ul style="list-style-type: none"> <li>• Straße, Hausnummer</li> <li>• PLZ, Ort</li> </ul> ODER Institution: <ul style="list-style-type: none"> <li>• IK-Nummer</li> <li>• Institutionsname</li> <li>• Straße, Hausnummer</li> <li>• PLZ, Ort</li> </ul>			
Rolle: Sonstige	Person: <ul style="list-style-type: none"> <li>• Anrede, Titel, Vorname, Nachname</li> <li>• Straße, Hausnummer</li> <li>• PLZ, Ort</li> </ul> ODER Institution: <ul style="list-style-type: none"> <li>• IK-Nummer</li> <li>• Institutionsname</li> <li>• Straße, Hausnummer</li> <li>• PLZ, Ort</li> </ul>	x	x	
Rechnungsempfänger	KVNR	x	x	MUSS
	Vorname	x	x	
	Nachname	x	x	
	Straße, Hausnummer	x	x	
	PLZ, Ort	x	x	
	Geburtsdatum	x	x	MUSS
Rechnungsdatum	Datum	x	x	MUSS
Rechnungs-Nr. (bei LEI)	Freitext/Numerisch	x	x	MUSS
Info Korrekturrechnung	ja/nein (nein als Default)	x	x	

	Rechnungs-Nr. der stornierten Rechnung beim LE, auf die sich die Korrektur bezieht	x	x	
	Rechnungstoken der stornierten Rechnung, auf die sich die Korrektur bezieht	x	x	
Behandelte Person	KVNR	x	x	
	Vorname	x	x	MUSS
	Nachname	x	x	MUSS
	Geburtsdatum	x	x	MUSS
Gesamtsumme der E-Rechnung	Betrag in EURO	x	x	MUSS
Behandlungszeitraum	Startdatum	x	x	
	Enddatum	x	x	
Diagnose (Mehrfachangabe möglich)	Code nach ICD-10	x		
	Text zum ICD-10 Code	x		
	Freitext	x		
Rechnungsposition (Mehrfachangabe möglich) <ul style="list-style-type: none"> <li>• nach GOÄ/GOZ</li> <li>• auch analoge Rechnungsposition</li> <li>• Entschädigung nach §8,9 GOÄ/GOZ (Wegegeld oder Reiseentschädigung)</li> <li>• Auslagen nach §10 GOÄ/§9 GOZ (Material- und Sachkosten)</li> </ul>	Datum	x	x	
	Gebührenordnung (GOZ oder GOÄ)	x	x	
	Nummer (Nr) z.B. Ziffer oder Paragraph aus Gebührenordnung Zusatz "a"/"A"/"analog" oder "Honorar/HV" als Prä-/Postfix zur Gebührennummer	x	x	
	Leistungsbezeichnung aus	x	x	

	Gebührenordnung			
	Zusatztext/ Beschreibung des erbrachten Leistungsinhalts (z.B. bei analoger Rechnungsposition, Auslagen/Sachkosten)	x	x	
	Begründung (z.B. bei Überschreitung der Regelsätze (hier nur wenn nicht auf Rechnungsebene angegeben)	x	x	
	Mindestdauer oder Dauer	x		
	Zahn/Region		x	
	Organ	x		
	Wegegeld <ul style="list-style-type: none"> <li>Entfernung (bis zu 2 km, mehr als 2 bis 5 km, mehr als 5 bis 10 km, mehr als 10 bis 25 km)</li> <li>Tageszeit (Tag, Nacht)</li> </ul> ODER Reisekosten (Stunden, Weg in km, Kosten Übernachtung) UND Betrag in EURO	x	x	
	Wirkstoffname	x		
	Konkret verbrauchte Menge	x		
	Zeitangabe (Vor/Nachmittag oder konkrete Uhrzeit)	x		

	Gebühr Einzelsatz	x	x	
	Anzahl	x	x	
	Steigerungssatz (Dezimalzahl)	x	x	
	Betrag in EURO	x	x	
Minderungen nach §6 GOÄ/§7 GOZ	Dezimalzahl/Prozent	x	x	
Begründung für Überschreitung der Regelsätze	Freitext	x	x	
Zahlungsziel	Datum oder Fristangabe	x	x	
Zahlungsdaten (Mehrfachangabe möglich)	Kontoinhaber	x	x	
	IBAN	x	x	
	BIC	x	x	
	Name der Bank	x	x	
	Verwendungszweck (z.B. Rechnungs-Nr.)	x	x	

#### 4.8.1.2 Ergänzendes Dokument

Ergänzende Dokumente sind solche, die der Rechnungsersteller einer E-Rechnung ergänzend beigefügt hat. Ein solches Dokument enthält als strukturierte Daten nur grundlegende Metadaten wie den Titel und Typ des Dokuments, Erstellungsdatum sowie die Visualisierung als PDF. Als Typ kommen nur die Typen gemäß der Dokumentenklassifikation (siehe [gemSpec\_eRg\_FD] zur Festlegung der Dokumententypen) in Frage.

Einige Dokumente sind je nach Rechnungsinhalt verpflichtend notwendig für die Erstattung beim KTR. Eine diesbezügliche Prüfung über die Vollständigkeit der Dokumente für die Erstattungsprüfung ist Gegenstand einer zukünftigen Ausbaustufe.

Die grundlegenden Datenfelder für die Teilmenge der strukturierten Daten und notwendige Pflichtangaben im MVP sind in der folgenden Tabelle dargestellt. Diese bezieht sich auf die in 1.5- Umfang des MVP genannten Funktionalitäten des MVP. Die technischen Details werden in der FHIR Spezifikation festgelegt, siehe [gemSpec\_eRg\_FD].

Neben den aufgelisteten inhaltlichen Daten, werden als technische Daten die Telematik-ID des Rechnungserstellers und das vom FD vergebene Dokument-Token ergänzt. Zusätzlich erhält das Dokument stets eine Signatur, erstellt durch den

Fachdienst. Diese umfasst das PDF und die strukturierten Daten. Details zum Signaturverfahren werden in [gemSpec\_eRg\_FD] beschrieben.

Das Fehlen einer Pflichtangabe führt im MVP zu einer Ablehnung der Rechnung im Fachdienst und wird als gravierender Fehler gemeldet. Weitere Validierungen hinsichtlich gravierender oder nicht gravierender Fehler können in einer Ausbaustufe hinzukommen (siehe auch 1.7.2- Verwendete Begriffe).

Tabelle 4: Grundlegende Datenfelder eines die Rechnung ergänzenden Dokuments im MVP

Bezeichner	Datenfelder	GOÄ relevante Datenfelder im Bezug auf die Gebührenordnu ng, Pflichtangaben (MUSS) siehe letzte Spalte	GOZ relevante Datenfelder im Bezug auf die Gebührenordnu ng, Pflichtangaben (MUSS) siehe letzte Spalte	Pflichtangaben (MUSS) führen bei Fehlen zu einer Ablehnung des Dokuments bei der Einstellung in den Fachdienst
Titel des Dokuments	Textfeld	x	x	MUSS
Erstellungsdatum	Datum	x	x	MUSS
Rechnungs-Nr. (bei LEI), zu der das Dokument einen Anhang darstellt	Freitext/Numerisch	x	x	
Typ des Dokuments	Auswahl aus Verzeichnis nach [KDL CodeSystem]	x	x	

## 4.8.2 Rechnungs-Workflow

Jeder E-Rechnung, die in den Fachdienst eingestellt wird, wird genau ein Rechnungs-Workflow zugeordnet - und pro Rechnungs-Workflow gibt es nur eine E-Rechnung (siehe 4.8.1.1- Rechnung). Rechnungs-Workflows zeichnen sich dadurch aus, dass sie den Bearbeitungsstatus aus Sicht des Versicherten speichern. Der Fachdienst setzt diesen Status ausgehend von der aktuell durch ein Client-System aufgerufenen Operation.

Neben der E-Rechnung werden ggf. auch die ergänzenden Dokumente (siehe 4.8.1.2) mit dem Rechnungs-Workflow verknüpft, sodass nachvollzogen werden kann, welche Dokumente zusammen mit einer E-Rechnung durch den Rechnungsersteller bereitgestellt wurden.

## 4.8.3 Markierung

Jedes Dokument (E-Rechnung oder ergänzendes Dokument) kann mit beliebig vielen Markierungen versehen werden, damit der Versicherte eine Möglichkeit hat, Bearbeitungsschritte festzuhalten oder nachzuvollziehen - oder um einfach bestimmte zusätzlichen Merkmale zuordnen zu können. Es sind unterschiedlichste Typen von

Markierungen denkbar, wobei im MVP nur die in [4.4.2](#) beschriebenen vorgesehen sind. In zukünftigen Ausbaustufen können aber auch weitere Typen von Markierungen hinzu kommen.

Markierungen können mit einem Versicherten oder einem KTR verknüpft sein und können mit ergänzenden Informationen versehen werden, in Abhängigkeit vom Typ der Markierung.

### 4.8.4 Nutzer

#### 4.8.4.1 Institutionen

PKVen, GKVn, Beihilfestellen, LEI und ADL werden im eRg FD als Nutzer verwaltet und sind über die Telematik ID Ihrer Institutionsidentität eindeutig identifizierbar.

Eine LEI (z.B. Arztpraxis) oder ein ADL kann als Ersteller einer E-Rechnung auftreten. Daher wird diese beim entsprechenden Rechnungs-Workflow referenziert.

Weitere als Nutzer zu berücksichtigende Institutionen sind die Kostenträger (PKV, GKV oder Beihilfe). Diese können z.B. bei einer Einreichung von Rechnungen und Dokumenten über die entsprechende Markierung als "Empfänger" der Einreichung verknüpft werden.

Bei den einzelnen Institutionen sind ferner weitere Daten im Nutzerkonto verfügbar, gemäß der Registrierung im eRg FD (siehe auch [6.6.2](#) ).

#### 4.8.4.2 Versicherte

Versicherte werden als Nutzer des eRg FD verwaltet und sind über ihre Krankenversicherungsnummer (KVNR) eindeutig identifizierbar. Dem Nutzerkonto sind weitere Daten zugeordnet, etwa z.B. Einstellungen des Nutzers für eRg FdV, Einwilligungen, usw. (siehe auch [6.6.1](#) ).

Dem Nutzerkonto sind alle Daten zugeordnet, auf die der Versicherte zugreifen darf. Wird z.B. eine E-Rechnung erstellt, so muss der Versicherte (genau einer), dem die E-Rechnung zugestellt werden soll, im Rechnungs-Workflow als Empfänger referenziert werden.

### 4.8.5 Berechtigungen

Regelbasierte Berechtigungen werden als Berechtigungsobjekte im Fachdienst gespeichert, siehe Kapitel [4.6- Berechtigungen](#). Entsprechend dem dort beschriebenen Konzept verweist eine Berechtigung daher stets auf Nutzer in bestimmten Rollen (Berechtigter, Betroffener, Initiator, Bestätiger). Weitere Angaben zu Berechtigungen sind insbesondere der Typ der Berechtigung. Im MVP sind zunächst nur Berechtigungen von Typ Rechnungsversandberechtigung vorgesehen.

### 4.8.6 Protokolleintrag

Das Nutzerprotokoll, welches dem Versicherten einen Nachvollzug der Zugriffe auf seine Daten ermöglichen soll, besteht aus einer Folge von Protokolleinträgen. Jeder Eintrag enthält

- eine Angabe zum Typ des Zugriffs,
- den Zeitpunkt des Zugriffs,
- Angaben zum Akteur (Nutzer oder eRg FD), der den Zugriff durchgeführt hat, und
- ggf. Angaben zu dem betroffenen Dokument oder Workflow.

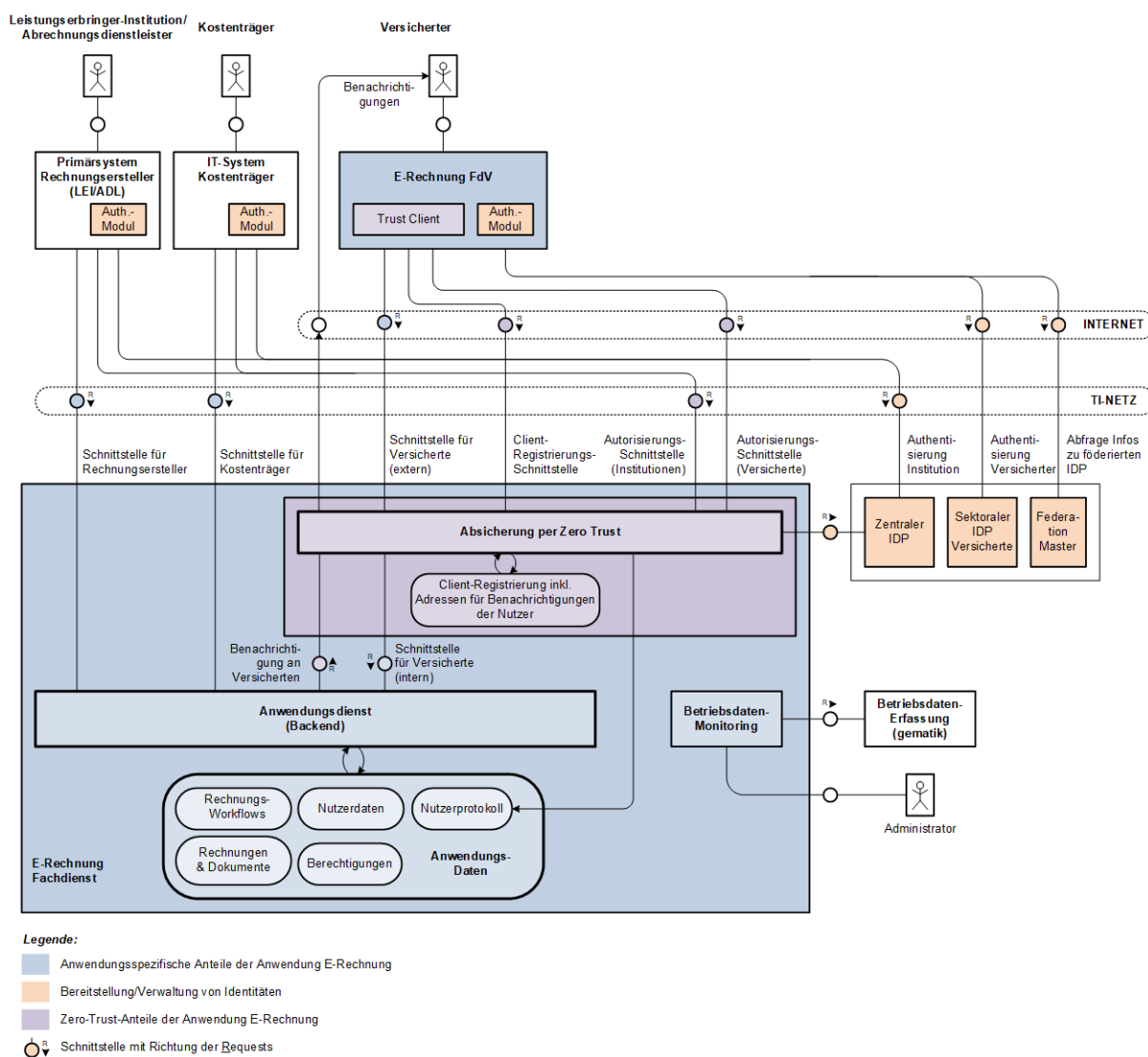


Weitere Informationen zu den Protokolleinträgen für Versicherte finden sich in 5.5.9-Nutzerprotokolle.

## 5 Technisches Konzept

### 5.1 Zerlegung des Fachdienstes

Das folgende Bild zeigt die funktionale Aufteilung des Fachdienstes sowie die Schnittstellen zu den Client-Systemen und weiteren benötigten Diensten.



**Abbildung 9: Funktionaler Aufbau der Anwendung E-Rechnung**

In den folgenden Kapiteln werden die verschiedenen Zugangslösungen zur TI sowie die Komponenten der dargestellten Architektur erläutert.

## 5.2 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)

Diese müssen über einen sicheren Zugang zur Telematikinfrastruktur (TI) verfügen - d.h. der Zugriff muss gemäß TI 1.0 über eine Anbindung an das zentrale Netz mittels zugelassener dezentraler Komponenten erfolgen:

- 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. Der E-Rechnung Fachdienst (eRg FD) ist somit ein offener Fachdienst gemäß der Systematik der TI 1.0.

Eine Zusammenstellung der verschiedenen möglichen TI-Zugangslösungen findet sich in Anhang A.

### Versicherte

Der Zugriff erfolgt über das Internet, hier erfolgt eine Absicherung nach Zero Trust Ansatz, siehe nächster Abschnitt und [gemF\_Zero-Trust].

## 5.3 Gestaltung der Architektur gemäß Zero Trust Ansatz

Die Internet-Schnittstellen der eRg für die Versicherten werden nach Prinzipien einer Zero Trust Architektur abgesichert. In der Darstellung des Fachdienstes sind die zur Umsetzung der Zero Trust Architektur benötigten Anteile farblich abgegrenzt. Eine detaillierte Beschreibung dazu findet sich in [gemF\_Zero-Trust]. Im Folgenden werden daher nur die wesentlichen Merkmale kurz vorgestellt.

### 5.3.1 Schutz der Fachdienst-Ressource

Der Zugriff auf die Ressourcen des eRg FD werden im Wesentlichen durch folgende Sicherheitsleistungen geschützt:

- erlaubte Zugriffe nur von bekannten, zugelassenen und auf einen Nutzer registrierten Clients
- Zugriffe nur auf Basis authentifizierter Nutzer und gemäß des erforderlichen Level of Assurance
- Zugriffe nur mit den rollenspezifischen Rechten in Abhängigkeit der angefragten Ressource
- Regelmäßige Prüfung erlaubter und valider Zugriffe auf Basis der Client-Zertifikate und Access-Token
- Ausstellen von Client-Zertifikaten, Access- und Client-Token nur für Clients, die den aktuell geltenden Sicherheitsrichtlinien (Policies) genügen und dies mittels Testat nachweisen

### 5.3.2 Registrierung der Clients

Der Begriff Client umfasst ein (zugelassenes) Frontend des Versicherten (eRg FdV) auf einem dedizierten Endgerät (Client-Gerät), mit dem der Versicherte auf die Internet-Schnittstellen des eRg FD zugreift. Clients müssen durch ihre Nutzer an der Client-Registry registriert werden. Durch die Registrierung wird auf dem Client-Gerät eine Hardware-gebundene kryptografische Identität (Client-Zertifikat) erzeugt, die Serverseitig an die Identität des Endanwenders und dessen Benachrichtigungs-Adresse gebunden wird. Die Adresse wird im Rahmen der Client-Registrierung validiert. Es wird damit ein kryptographischer Vertrauensraum für die eRg geschaffen, in dem nur bekannte, richtlinienkonforme und einem Versicherten zugeordnete Clients nach erfolgreicher Authentifizierung von Versicherten auf den eRg FD zugreifen können und dürfen.

### 5.3.3 Attestation der Client-Eigenschaften

Für die Clients, die im Minimum Viable Product (MVP) der Lösung als mobile Apps entwickelt werden, wird eine Attestation auf Basis geltender Richtlinien durchgeführt. Zum Schutz der Nutzerdaten wird so sichergestellt, dass nur Geräte und eRg FdVs genutzt werden, die bestimmten Sicherheitsanforderungen entsprechen und im Falle der eRg FdVs zugelassen sind. Falls die Eigenschaften nicht attestiert werden können oder die attestierten Eigenschaften nicht den Mindestanforderungen entsprechen, wird der Zugriff auf die eRg verweigert.

### 5.3.4 Zugriffsentscheidung

Die Zugriffsentscheidung erfolgt im Kern auf Basis eines authentifizierten Nutzers, seiner Rolle, seines verwendeten, registrierten und attestierten Clients sowie der dediziert angeforderten Ressource (bzw. des angeforderten Scopes). Des Weiteren können zusätzliche Kontextinformationen, die bspw. über das TI-IT Service Management (TI-ITSM) bereitgestellt werden, in die Zugriffsentscheidung einfließen. Die Zugriffsentscheidung wird bei Ablehnung mittels Fehlermeldung oder bei einer Gewährung mittels ausgestellttem Access-Token manifestiert und transportiert.

### 5.3.5 Durchsetzung der Zugriffsentscheidung

Die Versicherten-Schnittstelle für den eigentlichen Zugriff auf Ressourcen des eRg FD ist durch eine Komponente geschützt, die die Zugriffsentscheidung durchsetzt und Zugriff nur gewährt, wenn der Aufrufkontext mit den attestierten Zugriffsinformationen und Befugnissen innerhalb des Access-Tokens konsistent sind und der Access-Token gültig ist (Signatur, Gültigkeitszeitraum).

### 5.3.6 Bereitstellung einer maschinell interpretierbaren Policy durch die gematik

Für die eRg wird die Policy durch die gematik in einem maschinenlesbaren Format bereitgestellt. Hierfür werden mit dem *Open Policy Agent* (siehe [Open Policy Agent]) kompatible Policy Bundles verwendet. Die Policy Bundles werden durch die gematik erstellt sowie signiert und somit über einen integritätsschützenden Wege dem eRg FD bereitgestellt. Die eRg muss regelmäßig prüfen, ob aktualisierte Policy Bundles vorliegen.

Die im eRg FD genutzte Policy enthält

1. allgemeine, von der Anwendung unabhängige Sicherheitsrichtlinien, etwa grundlegend benötigte Geräte-Eigenschaften als Voraussetzung für die Nutzung in der TI.
2. anwendungsspezifische Richtlinien. Diese beschreiben insbesondere die rollenabhängigen Berechtigungsregeln, etwa, dass nur bestimmte Typen von Leistungserbringer-Institutionen (LEI) Rechnungen im Fachdienst erstellen dürfen.

## 5.4 Funktionaler Aufbau und Schnittstellen

Im Folgenden werden die unterschiedlichen Funktionen des eRg FD sowie seine Schnittstellen zu Client-Systemen und genutzten Diensten beschrieben. Außerdem wird kurz auf Module eingegangen, die im Client-System umzusetzen sind.

Im Wesentlichen sind innerhalb des Fachdienstes zu unterscheiden:

- Anteile zur Absicherung des Zugriffs gemäß Zero Trust Ansatz
  - Forward Proxy  
Dieser sichert den Zugriff auf die eigentliche - interne - eRg-Schnittstelle für Versicherte ab.
  - Client Registrierung  
Diese ermöglicht die Prüfung und Registrierung vom Versicherten genutzten Endgeräts und der darauf befindlichen Software, siehe auch [5.3](#).
  - Authorization Server und Policy  
Der Authorization Server prüft, ob der Zugriff eines Clients gemäß Policy zulässig ist. Dabei werden neben den allgemeinen Sicherheitsrichtlinien auch die anwendungsspezifischen Richtlinien ausgeführt, siehe auch [5.3.6](#).
- Fachliche Funktionen der Anwendung
  - Anwendungsdienst  
Dieser umfasst die eigentlichen fachlichen Funktionen der Anwendung im Fachdienst. Diese werden für Client-Systeme über funktionale Schnittstellen bereitgestellt, siehe auch [5.4.1](#).
  - Daten der eRg (Im Bild: "Anwendungsdaten")  
Dazu zählen die im Fachdienst gespeicherten E-Rechnungen und Dokumente, deren Bearbeitungsstatus (Workflow) und die Daten zu Nutzern (Nutzerkonto, Nutzerprotokoll). Außerdem werden hier die anwendungsspezifischen, regelbasierten Berechtigungen gespeichert. Diese werden nachgelagert und ergänzend zu den Bedingungen, die der Authorization Server prüft, ausgewertet.

Bei den Client-Systemen sind - neben den eigentlichen Anwendungsfunktionen - folgende Module zu unterscheiden:

- Trust Client  
Bestandteil der Zero Trust Architektur. Der Trust Client setzt auf dem Endgerät u.a. Funktionen im Zusammenhang mit der Client Attestation, Client Registrierung und dem sicheren Verbindungsaufbau zum Fachdienst um. Näheres dazu ist [gemF\_Zero-Trust] zu entnehmen.
- Authentisierungsmodul  
Dieses setzt Client-seitig Funktionen um, die bei der Authentifizierung des Nutzers und der Freigabe von Identitätsattributen durch den Identity Provider (IdP) benötigt werden. Näheres dazu ist [gemF\_Zero-Trust] zu entnehmen.

### Hinweis

Im Rahmen dieses Dokuments werden die Komponenten zur Umsetzung des Zero Trust Ansatzes nur so weit erläutert, wie es für das Verständnis der Gesamtlösung erforderlich ist. Eine *abschließende und verbindliche Beschreibung* dieser Anteile findet sich in [gemF\_Zero-Trust].

### 5.4.1 Anwendungsdienst

Der Anwendungsdienst umfasst die eigentlichen Funktionen der Anwendung, siehe folgende Tabelle.

**Tabelle 5: Funktionale Schnittstellen und Operationstypen des Fachdienstes E-Rechnung**

<b>Funktionale Schnittstellen nach Nutzergruppe</b>	<b>Verfügbare Operationstypen</b>
<b>Schnittstelle für Rechnungsersteller</b>	Daten des Rechnungsempfängers lesen
	E-Rechnungen mit Dokumenten anlegen, lesen
	<b>Token und angereichertes PDF abrufen zu E-Rechnung/Dokument</b>
	<b>Nutzerkonto des Rechnungserstellers anlegen, bearbeiten, löschen</b>
<b>Schnittstelle für Versicherte</b>	E-Rechnungen und Dokumente lesen, bearbeiten <sup>1</sup> , löschen, suchen
	Token und angereichertes PDF abrufen zu E-Rechnung/Dokument
	<b>Nutzerkonto des Versicherten anlegen, bearbeiten, löschen</b>
	<b>Einträge des Nutzerprotokolls lesen, löschen<sup>2</sup>, suchen</b>
	<b>Berechtigungen als Versicherter lesen, bearbeiten</b>
<b>Schnittstelle für Kostenträger</b>	E-Rechnungen und Dokumente lesen, bearbeiten <sup>1</sup>
	<b>Nutzerkonto des Kostenträgers anlegen, bearbeiten, löschen</b>

#### **Hinweise:**

<sup>1</sup> Das "Bearbeiten" von Dokumenten und E-Rechnungen, die eine LEI oder ein Abrechnungsdienstleister (ADL) erstellt hat, beschränkt sich für den Versicherten oder Kostenträger (KTR) 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.

<sup>2</sup> Das Löschen von Protokolleinträgen bezieht sich auf das gesamte Protokoll. Das Löschen einzelner Einträge ist nicht vorgesehen.

Eine detaillierte Festlegung der technischen Schnittstellen findet man in der Spezifikation zum Fachdienst, siehe [gemSpec\_eRg\_FD].

## 5.4.2 Schnittstelle Autorisierung

Der Zugriff auf den Anwendungsdienst, also die eigentlichen Funktionen des eRg FD, werden mittels des Authorization Servers abgesichert:

- die Funktionen des Anwendungsdienstes werden als ReSTful API (siehe [ReSTful API]) bereitgestellt
- der Zugriff darauf wird durch ein Access-Token gemäß OAuth2 (siehe [OAuth2]) autorisiert wird, welches der Authorization Server ausstellt.

Ein Zugriff auf die verschiedenen Funktionen des Anwendungsdienstes kann somit nur erfolgen, wenn der Client beim Aufruf einer Operation ein gültiges und zur Operation passendes Access-Token (Bearer Token) präsentieren kann, welches zuvor vom Authorization Server ausgestellt wurde, siehe nächster Abschnitt.

Der Authorization Server benötigt zur Vergabe eines Access-Tokens Identitätsattribute des Nutzers. Diese bezieht er vom jeweiligen IdP, siehe auch [gemSpec\_IDP\_FD]. Darüber hinaus erfolgt die Gewährung des Zugriffs durch den Autorisierungsdienst bei den verschiedenen Nutzergruppen und deren Client-Systemen auf unterschiedliche Weise:

### Institutionen

Hier verwendet der Authorization Server das seitens des *zentralen IDP* bereitgestellte ID-Token, unter Verwendung der SMC-B (oder HSM-B) als Authentisierungsmittel (Nutzung als "Smartcard IDP", siehe [gemSpec\_IDP\_Dienst]).

- Es erfolgt eine Prüfung gemäß den *Sicherheitsrichtlinien (Policy)* der gematik.

### Versicherte

Hier wird eine Autorisierung nach den Prinzipien von Zero Trust umgesetzt, siehe auch 5.3.

- Für den Bezug der *Identitätsattribute* des Nutzers verwendet der Authorization Server das seitens des *sektoralen IDP* bereitgestellte ID-Token (siehe [gemSpec\_IDP\_Sek]). Für die Anmeldung mit GesundheitsID wird ggf. eine separate Authentisierungs-App benötigt, falls die Authentisierung nicht per Authentisierungsmodul im eRg FdV erfolgt (im Bild nicht dargestellt).
- Zusätzlich erfordert die Autorisierung die Auswertung von Geräteigenschaften, die über die Client Attestation bzw. Client Registrierung bereitgestellt werden, siehe auch 5.4.2.2.
- Es erfolgt eine Prüfung gemäß den *Sicherheitsrichtlinien (Policy)* der gematik.

Bei beiden Nutzergruppen ruft der Authorization Server den anwendungsspezifischen Autorisierungsdienst auf. Dieser prüft ggf. ergänzende, anwendungsspezifische Bedingungen, sofern diese nicht über den Authorization Server und die Sicherheitsrichtlinien abgedeckt sind.

### 5.4.2.1 Verwendete Identitätsattribute

Der Authorization Server bezieht für die Versicherten und die Institutionen die für den Use Case ggf. benötigten Identitätsattribute in Form von Claims, aus dem vom jeweiligen IdP bereitgestellten ID-Token, siehe folgende Tabelle. Der Authorization Server gibt diese

Angaben als Claims im Access-Token weiter, soweit diese benötigt werden und die Ausstellung eines Access-Tokens zulässig ist.

**Tabelle 6: Verwendete IDP Claims**

<b>Identitätsattribut</b>	<b>Verwendeter Claim aus ID Token (zentraler IDP / Institutionen)</b>	<b>Verwendeter Claim aus ID Token (sektoraler IDP / Versicherte)</b>	<b>Bereitgestellter Claim im Access Token (Authorization Server)</b>
<b>ID-Nummer</b>	idNummer = <Telematik-ID>	urn:telematik:claims:id = <KVNR> (genauer: der unveränderliche Anteil der Krankenversicherungsnummer)	urn:telematik:claims:id (bei Versicherten und Institutionen)
<b>professionOID (genaue Nutzergruppe)</b>	professionOID = <OID> (OID der zulässigen Institutionen)	urn:telematik:claims:profession = <1.2.276.0.76.4.49> (OID für Versicherte)	urn:telematik:claims:profession (bei Versicherten und Institutionen)
<b>Geburtsdatum</b>	(nicht verfügbar)	birthdate = <Geburtsdatum>	birthdate (bei Versicherten)
<b>Vorname</b>	givenName = <Vorname> (Vorname des verantwortlichen Inhabers der SMC-B bzw. HSM-B)	urn:telematik:claims:given_name = <Vorname>	urn:telematik:claims:given_name (bei Versicherten und Institutionen)
<b>Nachname</b>	surname = <Nachname> (Nachname des verantwortlichen Inhabers der SMC-B bzw. HSM-B)	(nicht verfügbar)	surname (bei Institutionen, sonst leer)
<b>Vollständiger Name ("Displayname")</b>	display_name = <Displayname>	urn:telematik:claims:display_name = <Displayname>	urn:telematik:claims:display_name (bei Versicherten und Institutionen)
<b>Institutionsname</b>	commonName	(nicht verfügbar)	commonName



ame	e		(bei Institutionen, sonst leer)
-----	---	--	---------------------------------

#### 5.4.2.2 Verwendete Geräteattribute

Der Authorization Server bezieht die benötigten Geräteattribute des Endgeräts des Nutzers (Versicherter) über die Client Attestation/Client Registrierung. Er wertet diese Angaben zusammen mit den Identitätsattributen aus dem ID-Token und weiteren Signalen aus und entscheidet, ob für den angefragten Scope ein Access-Token ausgestellt werden kann.

Aus Sicht des Anwendungsdienstes sind diese Eigenschaften des Clients (d.h. das Endgerät und die darauf befindliche Plattform- und eRg FdV-Software) zu prüfen und sicherzustellen:

- Der Zugriff auf den Anwendungsdienst muss mit einem zugelassenen eRg FdV-Software-Produkt erfolgen.
- Das verwendete Gerät muss auf den aktuellen Nutzer registriert sein.

Die Geräteattribute werden von den Plattformen der Endgeräte geliefert. Ihre Erhebung erfolgt im Trust Client des Endgeräts mittels plattformspezifischer Attestierungs- und Erhebungsmechanismen. Näheres dazu und zu weiteren verwendeten Geräteattributen sind [gemF\_Zero-Trust] zu entnehmen.

#### 5.4.2.3 Bereitgestellte Claims und Scopes

Der Authorization Server stellt dem Client-System die angeforderten Zugriffsberechtigungen in Form von Claims und Scopes in einem Access-Token bereit.

##### 5.4.2.3.1 Claims

Als Claims werden ggf. die vom IdP bezogenen Claims weitergegeben, um dem Fachdienst sicher bestätigte Identitätsattribute zur Verfügung zu stellen, damit dieser die Daten des aktuellen Nutzers sicher abgrenzen kann.

- Die Krankenversicherungsnummer (KVNR) bzw. Telematik-ID  
Das entscheidende Merkmal um das richtige Nutzerkonto auszuwählen.
- Namenangaben  
Diese werden benötigt, damit einem Nutzer ein anderer Nutzer, mit dem er Daten austauscht, auf nutzerfreundliche Art und Weise angezeigt werden kann.
- Das Geburtsdatum des Versicherten  
Dieses wird ggf. verwendet, um neben der KVNR über ein zusätzliches Merkmal zur Plausibilisierung/Identifikation zu verfügen.

Welche Claims wann im Einzelnen benötigt werden, ist den Anwendungsfallbeschreibungen und den Spezifikationen der Operationen zu entnehmen, siehe [gemSpec\_eRg\_FD].

##### 5.4.2.3.2 Scopes

Die Scopes bilden dagegen die ggf. bestätigten Berechtigungen ab, die zum Zugriff auf bestimmte Funktionen erforderlich sind. Die folgende Tabelle stellt diese im Überblick dar. Die dort aufgeführten Berechtigungen sind zunächst rollenbasiert. Bei der Ausübung der Rechte im Fachdienst erfolgt eine Beschränkung auf die dem Nutzer verfügbaren/zugänglichen Daten anhand der Claims - eine Berechtigung zum Verwalten

eines Kontos betrifft z.B. nur das Konto desjenigen Nutzers, welcher anhand der KVNR oder Telematik-ID identifiziert wird.

**Tabelle 7: Scopes und Zugriffsberechtigungen**

<b>Zu berechtigender Nutzer</b>	<b>Zugriffsberechtigung (für welche Operationstypen gilt der Scope?)</b>	<b>Scope<sup>1</sup></b>
<b>Rechnungsersteller</b>	Daten des Rechnungsempfängers suchen und lesen	insurantAccount.rs
	E-Rechnungen mit Dokumenten anlegen, lesen	invoiceDoc.cr
	<b>Token und angereichertes PDF abrufen zu E-Rechnung/Dokument</b>	
	<b>Nutzerkonto des Rechnungserstellers anlegen, lesen, bearbeiten, löschen</b>	practitionerAccount.crud
<b>Versicherter</b>	E-Rechnungen und Dokumente lesen, bearbeiten <sup>2</sup> , löschen, suchen	invoiceDoc.ruds
	Token und angereichertes PDF abrufen zu E-Rechnung/Dokument	
	<b>Nutzerkonto des Versicherten anlegen, lesen, bearbeiten, löschen</b>	insurantAccount.crud
	<b>Einträge des Nutzerprotokolls lesen und suchen</b>	auditEvent.rs
	<b>Berechtigungen als Versicherter lesen, bearbeiten, löschen</b>	permissionInsurant.rud
<b>Kostenträger</b>	E-Rechnungen und Dokumente lesen, bearbeiten <sup>2</sup>	invoiceDoc.ru
	<b>Nutzerkonto des Kostenträgers anlegen, lesen, bearbeiten, löschen</b>	insuranceAccount.crud

**Hinweise:**

<sup>1</sup> Der Aufbau der oben aufgeführten Scopes orientiert sich an den Empfehlungen gemäß SMART on FHIR (siehe [SMART on FHIR]).

- <Ressource/Datenobjekt>.c = Ressource/Datenobjekt erzeugen (create)

- `<Ressource/Datenobjekt>.r` = Ressource/Datenobjekt lesen (read)
- `<Ressource/Datenobjekt>.u` = Ressource/Datenobjekt bearbeiten (update)
- `<Ressource/Datenobjekt>.d` = Ressource/Datenobjekt löschen (deleate)
- `<Ressource/Datenobjekt>.s` = Ressource/Datenobjekt suchen (search)

<sup>2</sup> Das "Bearbeiten" von Dokumenten und E-Rechnungen beschränkt sich für den Versicherten oder Kostenträger (KTR) 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.

### 5.4.3 Client-Registrierungs-Schnittstelle

Diese Schnittstelle dient zur Registrierung und Attestierung des Clients der Versicherten.

Die erstmalige Client Registrierung erfolgt auf Basis der GesundheitsID des Versicherten. In diesem Zuge muss der Nutzer auch eine Adresse zur Benachrichtigung registrieren, die einen zusätzlichen und von der GesundheitsID unabhängigen Sicherheitsfaktor für die Verwaltung der Versicherten-Clients darstellt. Im Falle einer erfolgreichen respektive Richtlinien-konformen Registrierung des Versicherten-Clients erhält dieser ein von der Client-Registry signiertes X.509 Zertifikat zur Ermöglichung der beidseitig authentisierten TLS-Kommunikation (mTLS) mit dem eRg FD.

Die Client-Attestierung erfolgt unter Nutzung der Services der einschlägigen Anbieter mobiler Plattformen (Apple, Google) sowie einer weiteren und darauf aufbauenden Prüfung und Attestierung weiterer Client-Eigenschaften wie bspw. den Zulassungsstatus des verwendeten eRg FdV. Der Autorisierungsdienst übergibt an einen Client nur dann Access-Token, wenn dieser als Richtlinien-konform attestiert wurde.

Eine detaillierte Beschreibung befindet sich in [gemF\_Zero-Trust].

### 5.4.4 Schnittstelle für Versicherte

Die externe Schnittstelle sichert den Zugriff der Versicherten auf die Ressourcen des eRg FD ab. Ankommende Requests eines eRg FdV werden geprüft und erst dann an den Anwendungsdienst (Backend) weitergeleitet - oder abgelehnt. Dabei erfolgt insbesondere eine Entschlüsselung und Prüfung des Access-Tokens. Die für die Anwendung benötigten Inhalte des Access-Tokens werden aus dem Token extrahiert und im Header an die interne Schnittstelle des Anwendungsdienstes (Backend) zusammen mit dem Request Body weitergegeben.

Eine detaillierte Beschreibung befindet sich in [gemF\_Zero-Trust].

### 5.4.5 Schnittstelle für die Benachrichtigung

Im Rahmen der Client Registrierung ist die Verwendung von Benachrichtigungen zwecks Bestätigung der Registrierung (Bestätigungs-Code) vorgesehen. Damit wird eine Verknüpfung einer validierten Benachrichtigungs-Adresse mit einem Nutzer (Versicherter) hergestellt, siehe auch [gemF\_Zero-Trust]. Der E-Rechnung Fachdienst (Anwendungsdienst) nutzt ebenfalls diesen Weg, um den Versicherten über bestimmte Vorgänge zu informieren (siehe 4.4.3- Aktive Benachrichtigungen). Zu diesem Zweck wird eine fachdienstinterne Schnittstelle zur Client Registrierung genutzt, über die der Typ der Nachricht und der Empfänger vorgegeben werden können.

## 5.5 Datenschutz und Informationssicherheit

In der Anwendung E-Rechnung (eRg) werden personenbezogene medizinische Daten verarbeitet, die gemäß ihrem Schutzbedarf durch eine Ende-zu-Ende-Sicherheit durchgängig von der Kollektion bis zur Nutzung geschützt werden müssen.

### 5.5.1 Schutzbedarf

Maßgeblich für den Schutzbedarf der Anwendung ist das Informationsobjekt „E-Rechnung“, das u. a. Angaben zum behandelnden Leistungserbringer (LE), zur behandelten Person und den abgerechneten Leistungen sowie den Rechnungs-Token enthält. Diese Informationen sind als personenbezogene medizinische Daten klassifiziert und besitzen damit einen sehr hohen Schutzbedarf in Hinsicht auf die Vertraulichkeit. Der Schutzbedarf für die Integrität der Daten wird mit hoch bewertet, da diese personenbezogenen medizinischen Daten nicht als Grundlage für eine Behandlung dienen, bei einer Verfälschung also keine Gefahr für Leib und Leben besteht. An die Authentizität des Informationsobjekts E-Rechnung werden – wie im papiergebunden Verfahren – keine besonderen Anforderungen gestellt.

Da die Anwendungsfälle der Anwendung E-Rechnung im Versorgungskontext der Versicherten nicht kritisch sind, wird der Schutzbedarf hinsichtlich der Verfügbarkeit pauschal mit "mittel" festgestellt.

Da in den Anwendungsfällen der eRg personenbezogene Daten besonderer Kategorien (medizinische Daten) verarbeitet werden, wird der Schutzbedarf hinsichtlich der Gewährleistungsziele des Grundrechtseingriffs (Datenminimierung, Nichtverketzung, Transparenz, Intervenierbarkeit) pauschal mit „hoch“ festgestellt.

### 5.5.2 Maßnahmen

Der Schutzbedarf der verarbeiteten Daten und die vollständige Integration der Anwendung in die TI haben zur Folge, dass für den Hersteller des Frontend des Versicherten (eRg FdV) und des E-Rechnung Fachdienstes (eRg FD), die Produkte selbst und den Anbieter/Betreiber des Fachdienstes grundsätzlich alle übergreifenden Datenschutz- und Sicherheitsanforderungen der Telematikinfrastruktur (TI) gelten. Insbesondere betrifft dies die Anforderungen an den sicheren Softwareentwicklungsprozess und die Integration des Betriebs des eRg FD in das Security Monitoring und andere für die TI sicherheitsrelevante Prozesse der gematik. Die Erfüllung dieser Anforderungen wird über Sicherheitsgutachten und Prozessprüfungen nachgewiesen. Der Nachweis der Datenschutzkonformität und Sicherheit der Produkte wird über Produktgutachten erbracht.

In der Umsetzung werden alle personenbezogenen medizinischen Daten transportverschlüsselt übertragen (data in motion), verschlüsselt gespeichert (data at rest) und derart geschützt verarbeitet (data in use), dass der Betreiber des eRg FD keinen Zugriff darauf erhalten kann (Verarbeitung in einer vertrauenswürdigen Ausführungsumgebung (VAU)).

Die Authentizität und Integrität der E-Rechnung wird im Fachdienst durch die Authentifizierung des Rechnungserstellers bzw. durch den Schutz der Daten vor unbefugtem Zugriff mittels VAU sichergestellt. Zusätzlich wird bei der Speicherung im Fachdienst eine Signatur durch den Fachdienst erzeugt, sodass Authentizität und Integrität auch nach Übertragung der E-Rechnung aus dem Fachdienst in ein Client-System geprüft werden kann. Beim Abruf von E-Rechnungen von Kostenträgern (KTR) werden Informationen mitgeliefert, die kenntlich machen, von welchem Nutzer die Rechnung eingestellt wurde.

Vom Hersteller und Betreiber des eRg FD wird verlangt, dass alle technischen Kommunikationsstrecken zwischen dem eRg FD und den E-Rechnung-Clients sowie die Kommunikation zwischen den Komponenten des eRg FD verschlüsselt sind.

Von außen dürfen nur berechtigte Nutzer auf den eRg FD zugreifen und innerhalb des Betreibers dürfen nur berechtigte Administratoren Zugriff auf rein administrative Funktionen erhalten. Dabei ist auszuschließen, dass das Personal des Betreibers Zugriff auf die im eRg FD verarbeiteten personenbezogenen medizinischen Daten erhält.

Die Authentisierung der Nutzer erfolgt über die (sektoralen) Identity Provider (IdP) der TI. Die Use Cases der eRg dürfen nur von dafür berechtigten Personen bzw. Rolleninhabern ausgeführt werden. Die Umsetzung der Zugriffssteuerung erfolgt durch den Autorisierungsdienst des Fachdienst eRg. Ein Versicherter kann außerdem einem KTR den Zugriff auf eine E-Rechnung im eRg FD ermöglichen durch das Übersenden des Rechnungs-Token. Dies kann bspw. durch Übersenden einer gedruckten Rechnung erfolgen, auf die der Rechnungs-Token aufgedruckt ist - oder das Token kann auch digital übermittelt werden. Mittels dieses Token kann ein authentifizierter KTR auf eine E-Rechnung im eRg FD zugreifen.

Nutzer können ihr Konto jederzeit selbst löschen. Konten für Versicherte werden nach einer angemessenen Zeit (Festlegung in 5.5.6- Fristen für die Löschung und Aufbewahrung von Daten im Fachdienst) der Inaktivität automatisch im eRg FD gelöscht. Dies ist erforderlich, da sich im Prinzip auch Versicherte ein Konto anlegen können, die nicht (mehr) privat versichert sind oder Versicherte sich ein Konto anlegen, ohne die Absicht, die Funktionen der Anwendung zu nutzen. Falls ein Nutzer keinen Zugriff mehr auf sein Konto hat, kann er sein Konto löschen lassen. Durch das Löschen eines Kontos werden auch alle damit verknüpften Dokumente sowie das Zugriffsprotokoll unwiederbringlich im eRg FD gelöscht. Erfolgt die Aktivierung des Löschbefehls mittels des eRg FdV, muss dieses durch eine geeignete Nutzerinteraktion sicherstellen, dass ein versehentliches Löschen durch den Nutzer praktisch nicht auftreten kann.

Die Entwicklung der Software der Komponenten und des Dienstes der eRg muss mittels eines sicheren Softwareentwicklungsprozesses stattfinden. Den Nachweis hierüber erbringt der Hersteller einer Komponente bzw. Dienstes über ein Sicherheitsgutachten, das eine Voraussetzung für die Zulassung dieser Komponente bzw. dieses Dienstes ist.

Die Autorisierung zum Betrieb einer neuen Version der Software für den eRg FD muss im Mehr-Augen-Prinzip und unter Beteiligung der gematik erfolgen. Das hierfür zu etablierende Verfahren muss die Beteiligung der gematik technisch erzwingen, wobei die Aktivitäten der gematik dafür aus der Ferne (remote via VPN) und asynchron (zeitlich versetzt) zu den Aktivitäten des Betreibers ablaufen können sollten. Das Verfahren und die zugrundeliegenden Informationen müssen für die gematik aussagekräftig sein. Details dazu werden in den Spezifikationen geregelt.

Insbesondere zur Sicherstellung der Verfügbarkeit des eRg FD muss der Betreiber Maßnahmen zur Erkennung von Anomalien und Reaktionen darauf auf Netzwerkebene implementieren (Schutz vor DDoS-Attacken).

Sobald die Komponenten der Zero Trust Architektur der TI 2.0 zur Verfügung stehen, müssen diese im Produkt und dessen Betrieb eingesetzt werden. Im ersten Schritt dahin stellt der eRg FD sicher, dass nur eRg FdV mit definierten (Sicherheits-) Eigenschaften zugreifen können.

Die Umsetzung der FdV-Funktionalitäten und die Zulassung in neuen UIs oder deren Integration in vorhandene Produkte obliegt den Kostenträgern oder weiteren Anbietern von Versicherten-Frontends. Eine entsprechende FdV-Spezifikation wird zu diesem Zwecke zukünftig zur Verfügung gestellt.

### 5.5.3 Vertrauenswürdige Ausführungsumgebung

Der eRg FD verarbeitet personenbezogene medizinische Daten einer großen Zahl von Versicherten im Klartext. Diese Daten müssen bei der Verarbeitung vor unberechtigten Zugriffen zuverlässig geschützt werden. Abzuwehren sind damit auch Angreifer aus dem betrieblichen Umfeld des eRg FD, d. h. Angreifer aus dem Kreis der an Entwicklung und Bereitstellung der Software sowie an Bereitstellung und Betrieb der Hardware des Dienstes beteiligten Personen. Die Abwehr muss auf wirksamen technischen Mitteln aufbauen, umfasst jedoch auch eine sichere Ausgestaltung der für Entwicklung und Betrieb erforderlichen organisatorischen Strukturen und Prozesse.

Mit der elektronischen Patientenakte (ePA), dem E-Rezept sowie mit den Sektoralen IDPs für die Versicherten existieren bereits zugelassene Lösungen mit vergleichbarem Schutzbedarf sowie das Konzept der VAU, das eine Anforderungslage mit dem erforderlichen Schutzniveau schafft. In den existierenden Lösungen sind für die VAU jeweils eigene Anforderungen gestellt worden. Diese sind Teil der jeweiligen Produktspezifikation.

Die Anforderungen an die VAU des eRg FD werden gleichfalls in der Spezifikation gestellt. Gegebenenfalls erfolgt eine Auslagerung dieser Anforderungen in eine übergreifende Spezifikation [gemSpec\_DS\_VAU], falls die entsprechende anwendungsübergreifende Abstimmung dazu bis zum Abschluss der Spezifikationen für die eRg abgeschlossen ist. Eine solche Auslagerung wird keine signifikanten Änderungen der Anforderungslage aus Sicht des Anbieters mit sich bringen.

Für die konkrete Ausgestaltung der VAU des eRg FD werden im Rahmen der Leistungsbeschreibung im Vergabeverfahren für den Fachdienst weitere Vorgaben (ggf. als Soll-Anforderungen) gemacht, die der Weiterentwicklung der VAU zu einem Sicherheitskonzept für den Betrieb von Anwendungen in einer nach den Prinzipien der Cloud betriebenen Infrastruktur dienen. Hiermit soll eine Brücke geschaffen werden, um den eRg FD in einem folgenden Schritt auf der Grundlage einer Produkttypspezifikation für Healthcare Confidential Computing (HCC) weiterbetreiben zu können.

*Offener Punkt: Die Zulassungsgrundlagen für HCC-Anbieter sind noch nicht finalisiert und werden über eine separate Beauftragung erarbeitet und festgelegt.*

Um für die Umsetzung des eRg FD in einer mit anderen Diensten geteilten Rechenzentrumsumgebung keine unüberwindlichen Barrieren zu errichten, werden - dem bereits im Kontext der sektoralen IDPs erprobten Vorgehen entsprechend - in der Spezifikation keine Anforderungen zu einer dienstspezifischen physischen Trennungen der Systeme mittels Käfig oder speziellen Schutzschranken gestellt, wenn die Rechenzentrumsumgebung für den Betrieb des eRg FD mittels gängiger technischer u. organisatorischer Maßnahmen (TOM) einen angemessenen Schutz vor physischen Angriffen aus dem Betriebsumfeld bietet.

### 5.5.4 Prüfnutzeridentitäten

Die gematik hat den Bedarf, die sichere Inbetriebnahme neuer Anwendungen und Dienste in der Produktivumgebung zu begleiten und gemeldete Störungen aus der Produktivumgebung zu analysieren, ohne den Datenschutz in der TI zu gefährden (vgl. § 331 Absatz 5 SGB V). Dazu werden Prüfnutzeridentitäten in einer speziellen Verifikationsumgebung (VU), die Bestandteil der Produktivumgebung ist, für die Ausführung von Use Cases verwendet. In der eRg müssen diese Prüfnutzeridentitäten als solche erkennbar sein. Es muss ausgeschlossen sein, dass mittels Prüfnutzeridentitäten auf Daten von real existierenden Nutzern der Anwendung zugegriffen werden kann und



das real existierende Nutzer auf die Daten von Prüfnutzeridentitäten zugreifen können. Insbesondere dürfen Prüfnutzeridentitäten nicht als Vertreter von real existierenden Nutzern bzw. real existierende Nutzer als Vertreter von Prüfnutzeridentitäten eingerichtet werden können.

### 5.5.5 Datenschutzaspekte

Die eRg muss eine Nichtverkettbarkeit gewährleisten. Es gilt demnach ein grundsätzliches Verbot der Profilbildung für die gesamte Anwendung – insbesondere jedoch für den eRg FD, der dies technisch umsetzen muss. Davon unberührt kann die gematik nach §331 Abs. 2 SGB V Daten festlegen, die Anbieter von Komponenten und Diensten der gematik offenzulegen haben, sofern diese erforderlich sind, um den gesetzlichen Auftrag der gematik zur Überwachung des Betriebs zur Gewährleistung der Sicherheit, Verfügbarkeit und Nutzbarkeit der TI zu erfüllen. Nur die hierfür erforderlichen personenbezogenen Daten dürfen vom Betreiber als Ausnahme vom Profilbildungsverbot erhoben werden. Die konkreten Daten werden in der Spezifikation für den eRg FD festgelegt (siehe [gemSpec\_eRg\_FD]). Zur Verhinderung einer zweckfremden Verkettung personenbezogener Daten müssen die Daten beim Transport und der Speicherung verschlüsselt werden.

In den Verarbeitungsvorgängen der eRg dürfen nur Daten verarbeitet werden, die für die Durchführung des jeweiligen Verarbeitungsvorgangs erforderlich sind (Datenminimierung).

Zum Zweck der Transparenz muss es den Versicherten ermöglicht werden, die Verarbeitung ihrer personenbezogenen Daten zu überwachen. Dazu werden alle Zugriffe auf Dokumente eines Versicherten im eRg FD protokolliert. Dieses Protokoll ist für die Versicherten über das eRg FdV einsehbar. Für das eRg FdV muss eine Datenschutzerklärung existieren, die u. a. über Verantwortlichkeiten der Datenverarbeitung, die Art und den Zweck der verarbeiteten Daten sowie die Betroffenenrechte aufklärt.

Die eRg ist eine freiwillige Anwendung. Insofern kann ein Versicherter in die Nutzung der Anwendung einwilligen bzw. die Einwilligung widerrufen (Intervenierbarkeit). Das Erteilen der Einwilligung in den Zugriff auf die Daten des Nutzers für LE (Ärzte, Zahnärzte), deren Verrechnungsstellen und KTR erfolgt im eRg FdV über eine eindeutige bestätigende Handlung und wird im Fachdienst gespeichert. Der eRg FD darf Daten nur von Nutzern verarbeiten, die in die Anwendung eingewilligt haben und muss die Daten von Nutzern löschen, die ihre Einwilligung widerrufen haben.

### 5.5.6 Fristen für die Löschung und Aufbewahrung von Daten im Fachdienst

#### 5.5.6.1 Inaktivität und automatische Löschung

Neben einer durch den Nutzer ausgelösten Löschung von seinem Nutzerkonto oder ihm zugeordneten E-Rechnungen und Dokumenten, soll nach bestimmten Fristen auch eine automatische Löschung der Elemente durch den Fachdienst erfolgen, wobei die automatische Löschung nur Nutzerkonten von Versicherten (Rechnungsempfängern) betrifft. Dies beruht auf folgenden Grundüberlegungen:

- Der Fachdienst setzt keine Aufbewahrungs- oder Löschfristen um, die in der Verantwortung der LEI, ADL oder KTR liegen.
- Der Rechnungsempfänger erhält nur eine zweckgebundene Möglichkeit, seine Daten im Fachdienst zu speichern - nämlich primär um sie bei KTR einreichen zu können.

- Die Aufbewahrung im Fachdienst soll zweckbezogen und zeitlich beschränkt sein. Insbesondere dient der Fachdienst nicht der Archivierung. Dazu ist die ePA zu nutzen, oder eine eigene persönliche Ablage außerhalb der eRg.

Eine Löschung darf erst nach einer längeren Inaktivität erfolgen. Eine solche liegt vor, wenn

- das Nutzerkonto vom Versicherten längere Zeit nicht mehr aktiv, d.h. mit Login benutzt wurde  
und
- keine E-Rechnungen und Dokumente mehr darüber weitergegeben werden.

Bei der ersten Bedingung ist der Zeitpunkt des letzten erfolgreichen Logins entscheidend.

Die zweite Bedingung wird als erfüllt angesehen, wenn keine E-Rechnungen und Dokumente mehr im Nutzerkonto vorliegen. Dies tritt genau dann ein, wenn ggf. noch vorhandene E-Rechnungen und Dokumente durch automatische oder manuelle Löschung entfernt wurden und seit dem auch keine neuen mehr durch einen Rechnungsersteller dort eingebracht wurden.

Die Löschung des Nutzerkontos darf stets erst erfolgen, nachdem vorher eine Benachrichtigung über die anstehende Löschung an den Nutzer gesendet wurde und dieser hinreichend Zeit zur Reaktion hatte.

### 5.5.6.2 Löschfristen für Nutzerkonten

**Tabelle 8: Löschfristen für Nutzerkonten**

Benennung im Dokument	Aktion	Frist
T_KONTO_HINWEIS	Information des Nutzers über bevorstehende Löschung und Möglichkeit der Reaktivierung	zum nächsten Monatsende [T_KONTO_LÖSCHEN - 3 Monate]
T_KONTO_LÖSCHEN	Nutzerkonto sowie alle verknüpften Daten (inkl. Nutzerprotokolle) werden endgültig gelöscht.	zum nächsten Jahresende 1 Jahr nach letzter Aktivität und Nutzerkonto wurde nicht reaktiviert

### 5.5.6.3 Fristen für die Löschung und Aufbewahrung von Rechnungen und Dokumenten

Da E-Rechnungen und ergänzende Dokumente nicht beliebig lange, sondern nur zweckgebunden aufbewahrt werden dürfen, erfolgt bei Inaktivität des Versicherten eine automatische Vormerkung zur Löschung ("Verschiebung in den Papierkorb") und schließlich Löschung der E-Rechnung und ergänzender Dokumente. Dies erfolgt in Abhängigkeit des aktuellen Status der E-Rechnung zu einem Zeitpunkt nach Verstreichen einer Frist, siehe unten stehende Tabelle.

Der Zeitpunkt für die Verschiebung bzw. Löschung soll dabei auf das jeweils nächste Jahres- oder Monatsende "aufgerundet" werden, um eine effiziente Verarbeitung in Jahres- oder Monatsscheiben zu ermöglichen.

**Tabelle 9: Zeitpunkte zur Löschung und Aufbewahrung von Rechnungen und Dokumenten gemäß Fristen**

Benennung im	Aktion <sup>1</sup>	Zeitpunkt der Durchführung
--------------	---------------------	----------------------------



Dokument		gemäß Frist <sup>2</sup>
T_OFFEN_BIS	<p>E-Rechnung inkl. strukturierter Daten und verknüpfter Dokumente wird in den Papierkorb verschoben, deren Frist für die Aufbewahrung im Zustand OFFEN abgelaufen ist.</p> <p>Der Nutzer erhält eine Benachrichtigung.</p>	<p>zum nächsten Jahresende, frühestens 3 Jahre nach Wechsel in den Status OFFEN (z.B. bei Neuerstellung einer Rechnung oder Verschiebung durch den Nutzer aus einem anderen Status heraus)</p> <p>Beispiel: Rechnungsübermittlung an den eRg FD am 02.07.2024, Verschiebung in den Papierkorb am 01.01.2028</p> <p>Hinweis: der Zeitpunkt ist angelehnt an die gesetzliche Verjährungsfrist von Arztrechnungen nach §195 BGB und §199 BGB.</p>
T_ERLEDIGT_BIS	<p>E-Rechnung inkl. strukturierter Daten und verknüpfter Dokumente wird in den Papierkorb verschoben, deren Frist für die Aufbewahrung im Zustand ERLEDIGT abgelaufen ist.</p> <p>Der Nutzer erhält eine Benachrichtigung.</p>	<p>zum Monatsende, frühestens nach einem Jahr nach Wechsel in den Status ERLEDIGT</p> <p>Beispiel: Verschiebung einer Rechnung in den Status ERLEDIGT durch den Versicherten am 06.08.2025, Verschiebung in den Papierkorb am 01.09.2026</p>
T_LÖSCHEN_AM	<p>E-Rechnung inkl. strukturierten Daten und verknüpften Dokumenten wird endgültig aus dem Papierkorb gelöscht.</p>	<p>zum Monatsende frühestens 3 Monate nach Wechsel in den Status PAPIERKORB</p> <p>Beispiele:</p> <ol style="list-style-type: none"> <li>1. Verschiebung einer Rechnung in den Status PAPIERKORB am 01.09.2026, Löschung aus dem Fachdienst am 01.01.2027</li> <li>2. Verschiebung einer Rechnung in den Status PAPIERKORB am 20.09.2026, Löschung aus dem Fachdienst am 01.01.2027</li> </ol>

<sup>1</sup> siehe auch [4.4.1- Workflow einer Rechnung](#)

<sup>2</sup> abweichend zu den Festlegungen muss gewährleistet werden, dass eine Rechnung und die ergänzenden Dokumente nach maximal 10 Jahren nach Erstellungsdatum automatisch endgültig aus dem Fachdienst gelöscht werden.

### 5.5.7 Authentizität und Integrität von Rechnungen und Dokumenten

E-Rechnungen und Dokumente können vom Rechnungsersteller nur in den Fachdienst eingestellt werden, wenn dessen Identität sicher über den IdP authentifiziert wurde (Institutionsidentität). Die Übertragung zwischen Client-Systemen und dem Fachdienst sowie die Speicherung im Fachdienst erfolgen stets verschlüsselt. Eine Verarbeitung erfolgt im Fachdienst nur geschützt, in einer VAU (siehe auch [5.5.3- Vertrauenswürdige Ausführungsumgebung](#)).

Um die jederzeitige Überprüfbarkeit der Authentizität und Integrität von E-Rechnungen oder Dokumenten zu gewährleisten - insbesondere auch *außerhalb* des Fachdienstes, *nach* der Übertragung in Client-Systeme der KTR -, *müssen* E-Rechnungen (strukturierte Daten und PDF) vom Fachdienst mit einer Dokumenten-Signatur (Signaturidentität des Fachdienstes, aus dem Vertrauensraum der Komponenten-PKI der TI) versehen werden. Dokumente, die der Rechnungsersteller zu einer E-Rechnung hinzufügt, *müssen* ebenfalls mit dieser Signatur versehen werden.

Abrufende Client-Systeme *können* die Signaturen prüfen, falls die Sicherheits-Policies der Institution dies erfordern.

Die technischen Eigenschaften von Signaturen sind in der Übergreifende Spezifikation [gemSpec\_Krypt] festgelegt.

### 5.5.8 Schutz personenbezogener Daten in Token

Identitätsattribute des Nutzers werden vom Fachdienst (Authorization Server) über den jeweiligen IdP bezogen (siehe auch [gemSpec\_IDP\_FD]). Die hier genutzten Identity-Token werden zum Schutz der personenbezogenen Daten über sichere "Backend"-Verbindungen zwischen IdP und Fachdienst (Authorization Server) übertragen.

Das Gleiche gilt für die Übertragung von personenbezogenen Daten zwischen Gerätemanagement und Fachdienst (Authorization Server).

Die Übertragung von Access-Token und den ggf. darin enthaltenen personenbezogenen Daten vom Autorisierungsdienst - über das eRg FdV - zum Anwendungsdienst erfolgt verschlüsselt. Eine Verarbeitung der Access-Token erfolgt geschützt im Fachdienst, in einer VAU (siehe auch [5.5.3- Vertrauenswürdige Ausführungsumgebung](#)).

Für weitere Informationen zum Token-Handling siehe [gemF\_Zero-Trust].

### 5.5.9 Nutzerprotokolle

Für den Nachvollzug von Zugriffen auf Dokumente und Daten von Versicherten sollen vom eRg FD Protokolle geschrieben und z.B. für die Einsicht durch den Versicherten über das eRg FdV zur Verfügung gestellt werden.

Diese sollen mindestens enthalten:

**Tabelle 10: Zugriffstypen auf Dokumente und Daten für Nutzerprotokolle**

Typ des Zugriffs	Zeitpunkt des Zugriffs	Akteur des Zugriffs [Darstellung]	Betroffene Daten [Darstellung]
E-Rechnung von Rechnungsersteller übermittelt	Datum und Uhrzeit der Übermittlung	Rechnungsersteller [Anzeigenname der Institution]	E-Rechnung [Rechnungs-Nr. vom Rechnungsersteller]

Weitergabe ("Einreichen per Frontend") von Rechnungen und Dokumenten über die Versicherten-Schnittstelle	Datum und Uhrzeit des Zugriffs	Rechnungseinreicher [Anzeigenname des Versicherten]	Alle weitergegebenen E-Rechnungen [Rechnungs-Nr. vom Rechnungsersteller]
Automatisches Verschieben einer E-Rechnung mit zugehörigen Dokumenten in den Papierkorb aufgrund Löschfrist (siehe 5.5.6.3)	Datum und Uhrzeit des Verschiebens	Fachdienst ["Automatisch durch Anwendung"]	E-Rechnung [Rechnungs-Nr. vom Rechnungsersteller]
Automatisches Löschen einer E-Rechnung mit zugehörigen Dokumenten aus dem Papierkorb aufgrund Löschfrist (siehe 5.5.6.3)	Datum und Uhrzeit des Löschens	Fachdienst ["Automatisch durch Anwendung"]	E-Rechnung [Rechnungs-Nr. vom Rechnungsersteller]
Automatisches Setzen einer Markierung bei einer Rechnung/einem Dokument	Datum und Uhrzeit des Zugriffs	Fachdienst ["Automatisch durch Anwendung"]	E-Rechnung [Rechnungs-Nr. vom Rechnungsersteller] und/oder betroffene Dokumente [Titel und Typ]
Setzen einer Markierung bei einer Rechnung/einem Dokument durch einen Versicherten	Datum und Uhrzeit des Zugriffs	Versicherter [Anzeigenname des Versicherten]	E-Rechnung [Rechnungs-Nr. vom Rechnungsersteller] und/oder betroffene Dokumente [Titel und Typ]
Neue individuelle Berechtigung zum Rechnungsversand eines Rechnungsersteller angelegt	Datum und Uhrzeit des Anlegens	Rechnungsersteller [Anzeigenname der Institution]	Typ der Berechtigung ["Berechtigung zum Rechnungsversand"]
Bestätigung/Widerruf einer Berechtigungsregel zu	Datum und Uhrzeit der Bestätigung/des	Rechnungsempfänger [Anzeigenname des	Typ der Berechtigung ["Berechtigung zum

m Rechnungsversand durch den Rechnungsempfänger	Widerrufs	Versicherten]	Rechnungsversand"]
Abfrage Berechtigung zum Rechnungsversand durch den Rechnungsersteller	Datum und Uhrzeit der Abfrage	Rechnungsersteller [Anzeigename der Institution]	Typ der Berechtigung ["Berechtigung zum Rechnungsversand"]
Einrichtung Nutzerkonto und Einwilligung	Datum und Uhrzeit der Einrichtung und Einwilligung	Versicherter [Anzeigename des Versicherten]	Nutzerkonto ["Nutzerkonto"]

### 5.5.10 Grenzen der Sicherheitsleistung

Im Bedrohungsmodell zur eRg werden Missbrauchsszenarien berücksichtigt, die die Verfügbarkeit der Use Cases, die Vertraulichkeit und Integrität der verarbeiteten Daten bedrohen.

Missbrauchsszenarien auf der Anwendungsebene, die von berechtigten Nutzern der Anwendung ausgehen, werden nicht abgewehrt. Dies erfolgt - nach wie vor - in den Systemen der KTR.

So liegen unterstützende Funktionen zur Entdeckung von Abrechnungsbetrug außerhalb der Grenzen der Sicherheitsleistung der eRg.

Der eRg FD validiert die eingehenden strukturierten Daten und lässt nur ausgewählte Dokumententypen zu (im MVP nur PDF/A). Dadurch wird die Wahrscheinlichkeit, dass Daten bzw. Dokumente mit Schadsoftware eingestellt werden, stark reduziert. Es kann jedoch nicht gänzlich ausgeschlossen werden, dass diese Schadcode enthalten, der von manchen Leseprogrammen aktiviert würde. Deshalb sollten Clients, die Daten bzw. Dokumente vom eRg FD abrufen mit einer Virenschutz-Software ausgestattet sein.

Dies betrifft auch Sicherheitsleistungen, die von der eRg benötigt werden und von der TI-Plattform bereitgestellt werden. Hierzu gehören:

- die Identifikation von TI-Teilnehmern durch die (sektoralen) IdP sowie
- die Authentisierung mittels SMC-B und Konnektor.

## 5.6 Betrieb

In diesem Kapitel werden betriebliche Anforderungen gestellt und begründet oder auf Kapitel mit speziellen Ausprägungen für den eRg FD in normativen Querschnittsdokumenten verwiesen.

### 5.6.1 Schnittstellen und Anwendungsfälle

Die durch den eRg FD zur Verfügung gestellten Schnittstellen und Anwendungsfälle werden im Kapitel [gemKPT\_Betr#E-Rechnung-Fachdienst (PDT74)] dokumentiert werden, welche gemeinsam mit der Spezifikation [gemSpec\_eRg\_FD] veröffentlicht werden.

## 5.6.2 Leistungsanforderungen

Die vom eRg FD zu leistenden Vorgaben werden übersichtlich im Kapitel "gemSpec\_Perf#Performancevorgaben E-Rechnung-Fachdienst" dargestellt, welche gemeinsam mit der Spezifikation [gemSpec\_eRg\_FD] veröffentlicht werden.

### 5.6.2.1 Mengengerüst

Die derzeitigen Informationen zum Mengengerüst des eRg FD werden anhand folgender Tabelle übersichtlich aufgeschlüsselt:

**Tabelle 11: Mengengerüst Versichertenstruktur Deutschland**

Mengengröße	Wert
Gesetzlich Krankenversicherte der Bundesrepublik Deutschland 2023 <sup>(1)</sup>	73.800.000
Privat Krankenversicherte der Bundesrepublik Deutschland 2022 <sup>(2)</sup>	8.704.500
Privat Zusatzversicherte der Bundesrepublik Deutschland 2022 <sup>(3)</sup>	28.500.000

1. Basis der ermittelten Zahlen ist die Anzahl der GKV-Versicherten im Jahr 2023. (Quelle: [Gesundheitsberichterstattung] des Bundesministeriums für Gesundheit)
2. Basis der ermittelten Zahlen ist die Anzahl der PKV-Vollversicherten im Jahr 2022. (Quelle: VDEK - Versichertendaten "PKV - Versichertenstruktur" unter [VDEK])
3. Basis der ermittelten Zahlen ist die Anzahl von Privat Zusatzversicherten im Jahr 2021 (Quelle: Mitteilung des Wissenschaftlichen Instituts der PKV und Expertenrat)

Auf Basis der aktuellen Versichertenstruktur ist es möglich, die folgenden Mengengrößen der Rechnungserstellung und Abrechnung in den Kontext des eRg FD zu setzen. Auf Grundlage der eingeholten Quellinformationen des Wissenschaftlichen Instituts der PKV und des Expertenrates, wurden die zuletzt 2018 erhobenen Zahlen in den darauf folgenden Jahren nicht signifikant überschritten und sind auch in den folgenden "Corona"-Jahren und darüber hinaus tragbar.

**Tabelle 12: Mengengerüst Eingereichte Rechnungen 2018**

Mengengröße in Anzahl der eingereichten Rechnungen im Jahr 2018	Wert
Ambulante Versorgung Vollversicherung	53.200.000
Ambulante Versorgung Zusatzversicherung	1.000.000
Wahlärztliche Versorgung Vollversicherung	3.500.000
Wahlärztliche Versorgung Zusatzversicherung	2.600.000
Krankenhausfälle Vollversicherung	1.500.000
Zahn-Vollversicherung	10.100.000

Zahn-Zusatzversicherung	4.400.000
<b>Gesamt</b>	76.300.000
davon Rechnungen der Vollversicherung	68.300.000
davon Rechnungen der Zusatzversicherung	8.000.000

Mit Zuhilfenahme der beiden Tabellen zu den vorliegenden Mengengrößen ist eine nähere Abschätzung der kommenden Aufrufzahlen am eRg FD möglich. Sollten sich die gegebenen Annahmen als tragfähig erweisen, kann mit den vorliegenden Werten bereits eine Grundlast berechnet werden, die auf den Vollausbau der eRg in den hier abgebildeten, sichtbaren Grenzen der ambulanten und wahlärztlichen Versorgung sowie Krankenhaus- und Zahn-Versorgung, abgeleitet werden.

Es muss deshalb für eine E-Rechnung immer der Ende-zu-Ende Anwendungsfall bedacht werden und die zugrundeliegenden Aufrufe der Endpunkte entsprechend des Workflows von Start bis Ende mitberücksichtigt werden. Die Berechnung des Rechnungsvolumens pro Jahr auf den einzelnen Werktag folgt nachfolgend:

#### Annahmen:

1. Die Last wird linear über 12 Monate gleichverteilt (konservative Streckung, da üblicherweise stärkere und schwächere Monate zu beobachten sind).
2. Es werden 4 Wochen im Monat angenommen (konservative Stauchung).
3. Es werden 5 Arbeitstage in der Woche angenommen (konservative Stauchung).
4. Es werden 8 Arbeitsstunden am Tag angenommen (konservative Stauchung).

**Lineare Monatsverteilung:**  $76.300.000 / 12 = 6.358.333$  E-Rechnungen pro Monat

**Lineare Wochenverteilung:**  $6.358.333 / 4 = 1.589.583$  E-Rechnungen pro Woche

**Lineare Tagesverteilung:** 317.917 E-Rechnungen pro Tag

**Lineare Stundenverteilung:** 39.739 E-Rechnungen pro Stunde

**Lineare Sekundenverteilung:** 11 E-Rechnungen pro Sekunde

In dieser linearen Verteilung ist die Grundlast gleichmäßig auf den angenommenen Zeitraum verteilt. Die Angaben zur tatsächlichen Lastverteilung schwanken stark. KTR berichten, dass in den Zeiträumen vor Weihnachten und vor dem Sommer, zusammen 80% der Einreichungen erfolgen. Nach Angaben des Wissenschaftlichen Instituts der PKV machen Einreichungen im November und Dezember rund die Hälfte des linearen Rechnungsvolumens aus, mit dem Januar als Gegenpol mit der anderen Hälfte. Diese stark divergierenden Lastverhältnisse sind bei der Betrachtung des Gesamtworkflows zu berücksichtigen. Ebenfalls wichtig ist es herauszustellen, dass die Nutzungszeiten von Versicherten und LE gänzlich unterschiedlich sind - was auch eine Limitation des linearen Nutzungsverhaltens darstellt. Hier sind die LE im Rahmen ihrer Öffnungs- und Geschäftszeiten weitaus besser modellierbar, als ein in seinen individuellen Lebensumständen befindlicher Versicherter. Das führt am Ende zu dem Schluss, dass dieses Mengengerüst anschaulich darlegt, welche Grundlast auf dem System bei voller Ausbaustufe zu erwarten ist, und dass diese Last zu einem beliebigen Zeitpunkt ebenfalls um ein Vielfaches höher ausfallen kann, als linear modelliert.

In der Spezifikation des Fachdienstes werden die für den Start des eRg FD geltenden Last- und Performance-Anforderungen, bezogen auf die konkreten Endpunkte und Workflowschritte, spezifiziert. Dabei werden neben ausreichender Dienstperformanz auch die Lastkapazitäten des Dienstes im Hochlauf und die Nutzerakzeptanz im Feld berücksichtigt (siehe [gemSpec\_eRg\_FD]).

Sobald also die konkreten Endpunkte und Workflowschritte spezifiziert sind, werden Last- und Performancewerte spezifiziert, welche die aufgezeigten Annahmen und angesprochenen Unzulänglichkeiten mit einem Performancemodell unterlegt. Dadurch soll sichergestellt werden, dass neben ausreichender Dienstperformanz auch die Lastkapazitäten des Dienstes und damit auch die Nutzerakzeptanz im Feld erfüllt werden.

### 5.6.2.2 Produktspezifische Rahmenbedingungen

Folgende Anforderungen an die Leistungsfähigkeit des eRg FD sollen definiert werden:

1. Durchschnittliche Bearbeitungszeiten bei Aufruf eines Endpunktes
2. Maximale Bearbeitungszeiten bei Aufruf eines Endpunktes
3. Spitzenlasten zu Aufrufzahlen eines Endpunktes
4. Verfügbarkeit des Fachdienstes
5. nähere Vorgaben zur Durchführung von Wartungsfenstern

Die folgend beschriebene Anforderungslage wird entsprechend der zugeordneten Festlegungen in [gemSpec\_Perf] hinterlegt.

#### Performancevorgaben für Endpunkte

Die Angaben zu den Punkten 1-3 werden gemeinsam mit den konkreten Endpunkten des eRg FD im Spezifikationsdokument festgelegt. Dabei liegt der Fokus auf der Schaffung einer Spezifikationsgrundlage, welche für den Start der eRg tragfähig ist und durch die Entwicklung und Nutzung des Fachdienstes validiert und ggf. angepasst werden kann (siehe [gemSpec\_eRg\_FD]).

#### Verfügbarkeit

Da im Rahmen der Dienstauführung keine kritische Prozesslandschaft greift, sondern erst mittelbar eine Versorgungsrelevanz gegeben ist, wird keine Hochverfügbarkeit gefordert. Es wird daher ein abgestuftes Verfügbarkeitskonzept mit gängigen Erwartungswerten aufgeplant.

Die Festlegung zur Verfügbarkeit soll sich generell zur **Hauptzeit** mit 99,80% und zur **Nebenzeit** mit 99,00% richten.

Die Definition der Servicezeiten des eRg FD soll folgende Regelung enthalten:

- **Hauptzeit** ist Montag bis Freitag von 6 bis 22 Uhr.
- Bundeseinheitliche Feiertage und alle übrigen Stunden der Woche sind **Nebenzeit**.

#### Wartungsfenster

Wartungsfenster sollen generell in der Nebenzeit durchgeführt werden. Mit Genehmigung der gematik sind davon abweichend auch Wartungsfenster, z.B. zur akuten Fehlerbehebung, in der Hauptzeit möglich. Die Zeiten einer genehmigten Wartung sind nicht dem Anbieter im Rahmen seiner Verfügbarkeitsberechnung zur Last zu legen.

### 5.6.2.3 Anbieterspezifische Rahmenbedingungen

Folgende Rahmenbedingungen zu den Pflichten des Anbieters eRg FD sollen definiert werden:

1. Mitwirkung zu Haupt- und Nebenzeiten im **TI-ITSM**, gem. [TIP1-A\_7265-03] gem. [gemKPT\_Betr]
2. Mitgeltende Pflichten aus der Mitwirkung am TI-ITSM zur Nutzung der angebotenen ITSM-Prozesse



3. Automatisierte Lieferung von Betriebsdaten an die gematik, siehe Kapitel 5.6.3.1-Erfassung und Lieferung von Betriebsdaten

### 5.6.3 Monitoring

Das Monitoring ist als Teil des Event-Managements gemäß [ITIL] anzusehen. Es umfasst die kontinuierliche Aufnahme und Überwachung von Ereignissen und stellt die Informationsgrundlage zu den verfügbaren IT-Services her. Der eRg FD erzeugt zu jeder Zeit Informationen, welche genutzt werden sollen, um den Zustand des Systems zu analysieren und dessen Qualität zu bewerten.

Für ein lückenloses Monitoring eines TI-Dienstes ist es notwendig, dass hinreichend viele Informationen zur Qualität und Verfügbarkeit (Telemetrie) des Dienstes zeitnah der gematik vorliegen. Es wird erwartet, dass moderne IT-Services sowohl laufend Daten über den eigenen Zustand, als auch über ankommende und abgehende Transaktionen loggen und diese Daten zur Informationsgewinnung zuerst vom Anbieter gemonitort werden. Für die übergreifenden TI-Betriebstätigkeiten ist es für die gematik unerlässlich, dass die Implementation einer modernen Betriebsdatenlieferung erfolgt und dass ein spezifizierter Teil dieser Daten in kurzen Intervallen automatisiert an die gematik gesendet werden.

Die Einordnung der Betriebsdatenerfassung in die Dienstarchitektur findet sich in der Abbildung "Funktionaler Aufbau der Anwendung E-Rechnung" unter Kapitel 5.1-Zerlegung des Fachdienstes wieder.

#### 5.6.3.1 Erfassung und Lieferung von Betriebsdaten

Durch die Lieferung von Betriebsdaten wird es der gematik u.a. ermöglicht, Aussagen über die Nutzung, die Nutzerakzeptanz, das erwartete Anfrageaufkommen und weitere Qualitätsinformationen zu ermitteln, um bestehende Spezifikation zu verbessern oder Fehler schnell zu erkennen und zur Beseitigung dieser maßgeblich beizutragen. Auf der Grundlage dieser Daten sollen ausdrücklich keine Profile über die Nutzung des Dienstes von einzelnen LE erstellt werden. Vielmehr werden diese Daten genutzt, um mittels Data Science weitere Erkenntnisse für den zukünftigen TI-Betrieb zu ermitteln und vorhandene Annahmen - wie beispielsweise das Mengengerüst, die Bearbeitungszeiten und die Spitzenlasten - fortlaufend zu validieren und gegebenenfalls nachzubessern. Darüber hinaus hat die Erfahrung im E-Rezept Kontext gezeigt, dass eine eindeutige Identifikation der nutzenden Primärsysteme (PS) mittels Vorgaben zum Dienstaufwurf mit einer Client-ID und entsprechendem User Agent auch auf Implementationsschwierigkeiten der PS-Hersteller hindeuten kann. Durch die eindeutige Zuordnung kann so bei entsprechendem Fehlverhalten effektiv die Nutzung des Dienstes überwacht und durch hilfreiche Unterstützung das zugrundeliegende Problem zügig behoben werden. So wird es der gematik ermöglicht, proaktive Verbesserungen für alle beteiligten Nutzergruppen bereitzustellen, bevor eine tatsächlich negative Betroffenheit des Dienstes durch ein unerkanntes und weitreichendes Fehlverhalten eintritt.

Die durch den eRg FD zu erfüllenden Anforderungen hinsichtlich der Erfassung und Lieferung von Betriebsdaten an die gematik, werden im entsprechenden Kapitel zur E-Rechnung in der [gemSpec\_Perf] dargestellt.

### 5.6.4 Supportkonzept

Der Anbieter des eRg FD wird im Rahmen seiner Tätigkeit und Zulassung mit festgelegten Mitteln Unterstützungsleistungen für einen definierten Nutzerkreis anbieten. Diese Unterstützungsleistungen dienen dazu, die Nutzung des eRg FD verständlich zu kommunizieren - das bedeutet grundlegend die angebotenen Endpunkte fachlich korrekt



und übersichtlich zu dokumentieren und Unterstützungsangebote zur Implementierung des eRg FD, sowie Kontaktwege zur Fehlerbehebung zur Verfügung zu stellen.

Das Supportkonzept schließt hier den Produkttyp eRg FdV entsprechend mit ein, da dieser untrennbar von den Workflowprozessen zum direkten Versicherten ist. Da jedoch nicht abschließend geklärt ist, ob der Hersteller des eRg FdV gleichzeitig auch Anbieter des eRg FdV sein wird, ist der Kontext hier als zur Anbieterrolle zugeordnet zu betrachten.

Dabei müssen die Kontexte "eRg FD - Leistungserbringer" und "eRg FdV - Versicherter" getrennt voneinander betrachtet werden, um ein vollständiges Bild des Supportkonzeptes zu erhalten. Denn weder der Versicherte, noch der LE greifen über ein und dasselbe Implementierungssystem auf den eRg FD zu.

Da die Nutzung des eRg FD hauptsächlich über angeschlossene PS und das mobiles eRg FdV erfolgt, sind hauptsächlich diese beiden Implementationsverantwortlichen für die direkte Kommunikation mit dem Anbieter eRg FD vorgesehen.

#### **5.6.4.1 1st Level Support**

Der 1st Level Support, auch First Level Support, nach [ITIL], befindet sich auf der untersten Ebene und steht in direktem Kontakt mit den tatsächlichen Endnutzern des Systems. Der 1st Level Support sorgt bei eingehenden Meldungen für schnellstmögliche Behebung im Falle von Störungen.

Der Anbieter eRg FD muss keinen direkten 1st Level Support für Versicherte oder LE erbringen.

##### **Kontext "eRg FD - Leistungserbringer"**

In diesem Kontext benutzt der LE sein PS, um die Funktionalität des eRg FD zu nutzen. Sollten dabei Probleme auftreten, soll der LE Kontakt zum Hersteller des PS aufnehmen, um eine Lösungsfindung anzustoßen. Je nach eingegangenen Vertragsbeziehungen, können hier noch weitere Dienstleister zwischen dem LE und dem Hersteller des PS liegen, an die sich der LE zur Fehlerbehebung wenden kann. Es ist von Vorteil, wenn das PS bereits mit einem umfangreichen FAQ für den LE ausgestattet ist und die auftretenden Meldungen für den LE klar und deutlich die Ursache des Fehlers zum Ausdruck bringen.

Sollte sich der kommunizierte Incident auf die Verfügbarkeit oder produktive Funktionalität des eRg FD beziehen, so ist vom Hersteller des PS - sofern dieser sich für eine Mitwirkung im Rahmen des TI-ITSM entscheiden - ein Ticket im TI-ITSM gegen den Anbieter eRg FD zu eröffnen.

##### **Kontext "eRg FdV - Versicherter"**

In diesem Kontext benutzt der Versicherte das eRg FdV seiner Krankenversicherung, um die Funktionalität des eRg FD zu nutzen. Sollten dabei Probleme auftreten, soll der Versicherte Kontakt zum Hersteller des eRg FdVs oder ggf. mit der anbietenden Krankenversicherung aufnehmen, um eine Lösungsfindung anzustoßen. Welcher Weg dabei der Beste ist, muss für den aufgetretenen Fehler spezifisch betrachtet werden. Nicht immer ist ein Fehler im Workflow-Schritt ein fachlicher, sondern kann sich auch als Bug herausstellen. Hier kann es ggf. notwendig sein, dass die Krankenversicherung und der Hersteller des eRg FdVs eng im 1st Level Support zusammenarbeiten. Es ist von Vorteil, wenn das eRg FdV bereits mit einem umfangreichen FAQ für den Versicherten ausgestattet ist und die auftretenden Meldungen für den Versicherten klar und deutlich die Ursache des Fehlers zum Ausdruck bringen.

Neben Störungen, werden hier ebenfalls Anfragen der Versicherten gegenüber fachlichen oder organisatorischen Rückfragen zu vorhandenen Workflows ihrer eingestellten und/oder zu Abrechnung vorgelegten E-Rechnungen behandelt.

Sollte sich der kommunizierte Incident auf die Verfügbarkeit oder die produktive Funktionalität des eRg FD beziehen, so ist hier vom Hersteller des eRg FdV - sofern dieser sich für eine Mitwirkung im Rahmen des TI-ITSM entscheiden - ein Ticket im TI-ITSM gegen den Anbieter eRg FD zu eröffnen.

#### **5.6.4.2 2nd Level Support**

Der 2nd Level Support, auch Second Level Support, nach [ITIL], befindet sich auf der mittleren Ebene im Stufenkonzept und wird dann aktiviert, wenn die Störung, der Fehler oder das Problem nicht zeitnah vom 1st Level Support gelöst werden konnte. Der 2nd Level Support ist im Rahmen der fachlichen Auseinandersetzung höher spezialisiert und mit breitem Fachwissen ausgestattet.

Der Anbieter eRg FD muss hier Unterstützungsleistungen für den 2nd Level Support für Hersteller von PS, dem Hersteller des eRg FdV und KTR im Rahmen Ihrer Supportwege bereitstellen.

In diesem Kontext existiert bereits ein Vorgang beim Hersteller des PS oder dem Hersteller des eRg FdV und dieser kann weiterführende Informationen und Unterstützungsleistungen vom Anbieter eRg FD auf einem geeigneten Kommunikationskanal (z.B. zugänglichem Ticketsystem) anfordern.

Sollte sich der kommunizierte Incident auf die Verfügbarkeit oder produktive Funktionalität des eRg FD beziehen, so ist hier vom Hersteller des PS oder dem Hersteller des eRg FdV - sofern diese sich für eine Mitwirkung im Rahmen des TI-ITSM entscheiden - ein Ticket im TI-ITSM gegen den Anbieter eRg FD zu eröffnen.

#### **5.6.4.3 3rd Level Support**

Der 3rd Level Support, auch Third Level Support, nach [ITIL], befindet sich am Ende des Stufenkonzepts und wird dann eingeschaltet, wenn die Störung im 2nd Level Support nicht gelöst werden konnte. Der 3rd Level Support soll dazu befähigt sein, mit Spezial- und Expertenwissen auf eine Lösung des Problems hinzuwirken.

In diesem Kontext existiert bereits ein Vorgang beim Hersteller des PS oder dem Hersteller des eRg FdV und es ist nicht möglich, das Problem mit der angebotenen Unterstützung im Rahmen des 2nd Level Supports zu lösen. Es wird zusätzlich Spezial- und Expertenwissen vom Anbieter eRg FD und ggf. der gematik benötigt, um dieses Problem zu lösen.

Der Anbieter eRg FD stellt hier für das im TI-ITSM vorgeschriebene Incident und Problem Management entsprechendes Spezialwissen bereit, welches im Rahmen der ITSM-Prozesse für Aufgaben des 3rd Level Supports zur Verfügung steht. Dazu gehört u.a. die Teilnahme an TI-ITSM Taskforces zur Problemlösung von schwerwiegenden produktiv auftretenden Einschränkungen, welche verbindlich zu einer Problemlösung führen soll.

#### **5.6.4.4 Mitwirkung und Support TI-ITSM**

Parallel zum Stufenkonzept der Supportleistungen muss der Anbieter eRg FD ggf. auch Supportleistungen im Rahmen des TI-ITSM als TI-Teilnehmer erbringen oder von anderen TI-Teilnehmern erwarten. Dies folgt aus den gegebenen Abhängigkeiten zu anderen TI-Diensten und deren, sowie der eigenen Kritikalität bei Ausfall, Wartung oder sonstigen Einschränkungen der Diensterbringung.

---

## 6 Anwendungsfälle

---

### 6.1 Anmerkungen zur Beschreibung der Anwendungsfälle

Im Folgenden werden die Anwendungsfälle für die E-Rechnung in tabellarischer Form beschrieben.

Über Vorbedingungen wird die Ausgangssituation beschrieben, in der der Anwendungsfall durchführbar ist, etwa benötigte Berechtigungen, das Vorliegen bestimmter Daten im Fachdienst oder der Ausgangs-Zustand des eRg FdV.

Der Ablauf erläutert die Aktionen, die der Nutzer durchführt und welche Aktivitäten bei eRg FdV und/oder Fachdienst daraus resultieren. Dabei wird *nicht* auf die Details der Nutzerschnittstelle des eRg FdV eingegangen, da deren konkrete Ausgestaltung offen gehalten werden soll.

Die Nachbedingungen beschreiben das gewünschte Ergebnis des Anwendungsfalls, etwa entstandene Daten, Ziel-Zustand des eRg FdV oder verschickte Benachrichtigungen.

Bestimmte Formulierungen werden wiederkehrend verwendet und sollen daher vorab kurz erläutert werden:

**Tabelle 13: Formulierungen in Anwendungsfallbeschreibungen**

Formulierung	Erläuterung / technische Bedeutung
Der Nutzer verfügt über ein Konto	Ein Nutzerkonto beim Fachdienst existiert für den Nutzer. Dieses enthält die Daten, die bei der Einrichtung des Nutzerkontos aus dem ID-Token entnommen und über das Access-Token weitergegeben wurden.
Der Nutzer wurde autorisiert	<p>Sofern nichts anderes beschrieben ist:</p> <ul style="list-style-type: none"><li>Für Versicherte:<ul style="list-style-type: none"><li>Die Identität des Nutzers wurde durch den sektoralen IDP authentifiziert, der ein entsprechendes ID-Token ausstellt.</li><li>Das vom Nutzer verwendete Gerät und die von ihm verwendete Software wurden von der Client Registrierung als registrierter Client erkannt.</li><li>Die für den Anwendungsfall benötigten Zugriffsrechte des Nutzers wurden vom Autorisierungsdienst gemäß den Sicherheitsrichtlinien geprüft und gewährt, basierend auf Identitätsattributen und den Eigenschaften des Clients.</li></ul></li><li>Für Nutzer einer Institution:<ul style="list-style-type: none"><li>Die Institutions-Identität des Nutzers wurde durch den zentralen IDP authentifiziert, der</li></ul></li></ul>

	<p>ein entsprechendes ID-Token ausstellt.</p> <ul style="list-style-type: none"> <li>• Die für den Anwendungsfall benötigten Zugriffsrechte des Nutzers wurden vom Autorisierungsdienst gemäß den Sicherheitsrichtlinien geprüft und gewährt, basierend auf den Daten aus dem ID-Token.</li> <li>• Für alle Nutzer: Grundlegende Sicherheitsrichtlinien wurden geprüft und als erfüllt bewertet, soweit dies für die Autorisierung erforderlich ist.</li> </ul> <p>Dem Client wird vom Autorisierungsdienst ein entsprechendes Access-Token bereitgestellt, welches</p> <ul style="list-style-type: none"> <li>• die den <i>gewährten Berechtigungen</i> entsprechenden Scopes (siehe <a href="#">5.4.2.3.2</a>) enthält und</li> <li>• die <i>benötigten Identitäts-Attribute</i> des authentifizierten Nutzers in Form von Claims (siehe <a href="#">5.4.2.3.1</a>) enthält.</li> </ul>
--	---

## 6.2 Übermittlung von Rechnungen

### 6.2.1 Konstellationen bei der Ermittlung des Rechnungsempfängers

Im Zusammenhang des Rechnungsversands sind aus Sicht des Rechnungserstellers folgende Konstellationen zu unterscheiden:

#### **Behandelter ist Rechnungsempfänger**

Der Rechnungsersteller verfügt über die Daten des Behandelten - der gleichzeitig Rechnungsempfänger ist -, insbesondere dessen Krankenversichertennummer (KVNR) und Geburtsdatum.

#### **Abweichender Rechnungsempfänger**

Der Rechnungsersteller kennt zu einem Behandelten die Daten des abweichenden Rechnungsempfängers, insbesondere dessen KVNR und Geburtsdatum.

In beiden Fällen muss für den Rechnungsempfänger im Fachdienst ein Nutzerkonto vorhanden sein und für den Rechnungsersteller muss der Rechnungsversand an den vorgesehenen Rechnungsempfänger erlaubt sein (d.h. der Rechnungsempfänger muss dem digitalen Rechnungsversand zugestimmt haben und es darf kein Widerruf der Berechtigung zum Rechnungsversand für diesen Rechnungsersteller seitens des Rechnungsempfängers vorliegen (Berechtigung im Zustand "verwehrt").

Im Fall des abweichenden Rechnungsempfängers wird *kein* Nutzerkonto für den *Behandelten* benötigt, da für die Zustellung der Rechnung das Nutzerkonto des Rechnungsempfängers genügt.

## 6.2.2 Plausibilisierung

Bei Abfrage der Daten des Rechnungsempfängers sind die Angabe und der Abgleich des Geburtsdatums alleine zwecks Plausibilisierung vorgesehen, d.h. nur wenn der Rechnungsersteller den Versicherten per KVNR und Geburtsdatum identifizieren kann, kann er weitere Daten (konkret: Namensangaben) des Versicherten aus dem Fachdienst erfragen.

## 6.2.3 Ermittlung des Rechnungsempfängers

### AF\_10132 - Abfrage des Rechnungsempfängers und dessen Einwilligung zum Rechnungsversand

**Tabelle 14 : Use Case Abfrage des Rechnungsempfängers und dessen Einwilligung zum Rechnungsversand**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Abfrage der Daten eines Rechnungsempfängers aus dessen Nutzerregistrierung durch den Rechnungsersteller, zwecks Plausibilisierung/Vergleich mit den Daten beim Rechnungsersteller. Gleichzeitig dient dies zur Abfrage der Rechnungsversandberechtigung des Rechnungserstellers für den vorgesehenen Rechnungsempfänger.
Vorbedingungen	<ul style="list-style-type: none"> <li>• Der Rechnungsersteller (Nutzer) verfügt über ein Konto und ist autorisiert.</li> <li>• Der Rechnungsersteller verfügt über die zur Identifikation eines Rechnungsempfängers benötigten Daten, insbesondere dessen KVNR und Geburtsdatum.</li> <li>• Der Rechnungsempfänger verfügt über ein Konto.</li> <li>• Der Rechnungsempfänger hat dem Rechnungsversand durch diesen Rechnungsersteller nicht widersprochen.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Rechnungsersteller übergibt mittels Primärsystem (PS) die Daten des Rechnungsempfängers an den Fachdienst. Er übergibt dazu <ul style="list-style-type: none"> <li>• die KVNR und das Geburtsdatum des Rechnungsempfängers und</li> <li>• die eigene Telematik-ID.</li> </ul> </li> <li>• Der Fachdienst sucht das zur KVNR und dem Geburtsdatum passende Nutzerkonto.</li> <li>• Der Fachdienst prüft, ob der gefundene Rechnungsempfänger dem Rechnungsversand durch diesen Rechnungsersteller widersprochen hat.</li> <li>• Falls nein, gibt der Fachdienst die Daten des gefundenen Nutzerkontos zurück.</li> </ul>
Nachbedingungen	<ul style="list-style-type: none"> <li>• Das PS des Rechnungserstellers hat vom Fachdienst die Daten des Rechnungsempfängers aus dessen Nutzerkonto erhalten. (Dies bedeutet gleichzeitig, dass der Rechnungsempfänger</li> </ul>

	<p>dem Rechnungsversand durch den Rechnungsersteller nicht widersprochen hat.)</p> <p>Anmerkung: Der Rechnungsersteller kann diese Daten bei Bedarf mit seinem PS abgleichen und als Rechnungsempfänger-Daten verwenden.</p>
Alternativen	<p>Falls</p> <ul style="list-style-type: none"> <li>• anhand der übergebenen Daten des Rechnungsempfängers kein Nutzerkonto im Fachdienst gefunden werden kann, <i>oder</i></li> <li>• der Rechnungsempfänger dem Rechnungsversand durch diesen Rechnungsersteller widersprochen hat,</li> </ul> <p>dann erhält das PS des Rechnungserstellers die Information, dass der Versand einer Rechnung für den Versicherten nicht möglich ist.</p> <p>Anmerkung: Das PS sollte in diesem Fall die Nutzung eines Ersatzverfahrens anbieten, etwa den Postversand eines Ausdrucks der Rechnung und der ggf. weiteren Dokumente.</p>

[&lt;=]

## 6.2.4 Validierung und Versand von Rechnungen und Dokumenten

### AF\_10136 - Rechnung mit Dokumenten validieren und versenden

**Tabelle 15: Use Case Rechnung mit Dokumenten validieren und versenden**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Übergabe einer Rechnung mit ggf. zugehörigen Dokumenten an den Fachdienst durch den Rechnungsersteller, zwecks Validierung und ggf. Übermittlung an den Rechnungsempfänger.
Vorbedingungen	<ul style="list-style-type: none"> <li>• Der Rechnungsersteller hat ein Nutzerkonto im Fachdienst und ist autorisiert.</li> <li>• Der Rechnungsersteller verfügt über die zur Identifikation des Rechnungsempfängers (Versicherter) benötigten Daten, insbesondere dessen KVN und Geburtsdatum.</li> <li>• Der Rechnungsersteller hat in seinem PS einen Datensatz erzeugt, bestehend aus <ul style="list-style-type: none"> <li>• einer Rechnung - bestehend aus strukturierten Daten und einem PDF - und</li> <li>• ggf. weiteren Dokumenten - jeweils bestehend aus strukturierten Daten und einem PDF.</li> </ul> </li> <li>• Der Rechnungsempfänger hat ein Nutzerkonto im Fachdienst.</li> <li>• Der Rechnungsempfänger hat dem Rechnungsversand durch</li> </ul>

	diesen Rechnungsersteller nicht widersprochen.
Ablauf	<ul style="list-style-type: none"> <li>• Der Rechnungsersteller übergibt mittels PS dem Fachdienst: <ul style="list-style-type: none"> <li>• die zu validierenden Daten aus seinem PS: <ul style="list-style-type: none"> <li>• Rechnung</li> <li>• ggf. ergänzende Dokumente</li> <li>• Daten des Rechnungsempfängers</li> </ul> </li> <li>• die eigene Telematik-ID</li> <li>• den gewünschten Modus für die Validierung (siehe 4.4.1) - TEST oder NORMAL</li> <li>• das gewünschte Format der zurückzugebenden Daten - nur Token oder auch angereichertes PDF</li> </ul> </li> <li>• Der Fachdienst validiert die übergebenen Daten auf Nichtvorliegen von gravierenden Fehlern: <ul style="list-style-type: none"> <li>• Grundlegende Korrektheit der Rechnungsdaten (zu den Pflichtfeldern, siehe 4.8.1.1- Rechnung)</li> <li>• Korrektheit ggf. der Metadaten/Typangaben der Dokumente</li> <li>• Korrektheit des Formats des jeweiligen PDF</li> </ul> </li> <li>• Der Fachdienst speichert die übergebenen Daten, abhängig vom angegebenen Modus: <ul style="list-style-type: none"> <li>• TEST: nur Validierung, d.h. es werden <i>keine</i> Daten gespeichert</li> <li>• NORMAL: Speicherung nur, wenn <i>keine gravierenden</i> Fehler vorliegen</li> </ul> </li> <li>• Falls der Fachdienst die Daten speichert, werden außerdem folgende Schritte durchgeführt: <ul style="list-style-type: none"> <li>• Es wird ein neuer Rechnungs-Workflow angelegt im Zustand "OFFEN".</li> <li>• Dieser wird <ul style="list-style-type: none"> <li>• dem Nutzerkonto des Rechnungserstellers gemäß Telematik-ID als Ersteller und</li> <li>• dem Nutzerkonto des Rechnungsempfängers gemäß KVN-R als Empfänger zugeordnet.</li> </ul> </li> <li>• Der Rechnung und jedem ggf. zugehörigen Dokument wird vom Fachdienst jeweils <ul style="list-style-type: none"> <li>• ein Rechnungs- bzw. Dokument-Token zugeordnet sowie</li> <li>• eine Signatur erzeugt und gespeichert.</li> </ul> </li> </ul> </li> <li>• Der Fachdienst gibt das Ergebnis an das PS zurück, bestehend aus: <ul style="list-style-type: none"> <li>• Ergebnis der Validierung (inkl. ggf. Fehlern)</li> <li>• falls Daten gespeichert wurden:</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Referenz auf den angelegten Workflow,</li> <li>• das Rechnungs-Token und</li> <li>• ggf. die Dokument-Token</li> <li>• ggf. im FD erzeugtes angereichertes PDF, sofern dies angefordert wurde</li> </ul> <ul style="list-style-type: none"> <li>• Falls Daten gespeichert wurden, erzeugt der Fachdienst eine Benachrichtigung (NEUE_RG) an den Rechnungsempfänger.</li> </ul> <p>Hinweis: Bei Bedarf kann der Rechnungsersteller ein zu versendendes Dokument als "Persönlich" (nur für den Versicherten) markieren.</p>
Nachbedingungen	<p>Im Modus NORMAL, Erfolgsfall:</p> <ul style="list-style-type: none"> <li>• Der Fachdienst hat einen neuen Rechnungs-Workflow angelegt.</li> <li>• Das PS des Rechnungserstellers verfügt über das angereicherte PDF (falls angefordert), das Rechnungs-Token und ggf. Dokument-Token.</li> <li>• Dem Rechnungs-Workflow ist der Rechnungsempfänger zugeordnet.</li> <li>• Dem Rechnungs-Workflow ist der Rechnungsersteller zugeordnet.</li> <li>• Der Rechnungs-Workflow befindet sich im Status OFFEN.</li> <li>• Die Rechnung und die ggf. ergänzenden Dokumente sind als "ungelesen" markiert.</li> <li>• Der Versicherte wurde benachrichtigt (Typ der Benachrichtigung "NEUE_RG").</li> </ul> <p>Im Modus TEST, Erfolgsfall:</p> <ul style="list-style-type: none"> <li>• Das PS des Rechnungserstellers erhält den Status OK zurück.</li> </ul> <p>Im Fehlerfall (Modus TEST oder NORMAL), d.h. bei gravierenden Fehlern:</p> <ul style="list-style-type: none"> <li>• Das PS des Rechnungserstellers erhält die Fehlermeldung, dass der Versand der Rechnung nicht möglich ist, und eine verständliche Fehlermeldung, die den spezifischen Grund angibt.</li> </ul>



Alternativen	<p>Falls</p> <ul style="list-style-type: none"> <li>anhand der übergebenen Daten des Rechnungsempfängers kein Nutzerkonto im Fachdienst gefunden werden kann, <i>oder</i></li> <li>der Rechnungsempfänger dem Rechnungsversand durch diesen Rechnungsersteller widersprochen hat,</li> </ul> <p>dann erhält das PS des Rechnungserstellers die Information, dass der Versand einer Rechnung für den Rechnungsempfänger nicht möglich ist.</p> <p>Anmerkung: Das PS sollte in diesem Fall die Nutzung eines Ersatzverfahrens anbieten, etwa den Postversand eines Ausdrucks der Rechnung und der ggf. weiteren Dokumente.</p>
--------------	--

[&lt;=]

**AF\_10264 - Rechnung mit Dokumenten validieren und versenden (Bulk)****Tabelle 16: Use Case Rechnung mit Dokumenten validieren und versenden (Bulk)**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Übergabe einer Menge von Datensätzen, bestehend jeweils aus Rechnung mit ggf. zugehörigen Dokumenten, an den Fachdienst durch den Rechnungsersteller, zwecks Validierung und ggf. Übermittlung an die jeweiligen Rechnungsempfänger. Dieser Anwendungsfall entspricht AF_10136, jedoch erweitert für die Verarbeitung größerer Datenmengen, typischerweise relevant bei Abrechnungsdienstleistungen.
Vorbedingungen	<ul style="list-style-type: none"> <li>Der Rechnungsersteller hat ein Nutzerkonto im Fachdienst und ist autorisiert.</li> <li>Der Rechnungsersteller möchte eine größere Menge von Datensätzen versenden, jeweils bestehend aus Rechnungen und ergänzenden Dokumenten für einen Rechnungsempfänger.</li> <li>Pro Datensatz gilt: <ul style="list-style-type: none"> <li>Der Rechnungsersteller verfügt über die zur Identifikation des Versicherten benötigten Daten, insbesondere dessen KVNR und Geburtsdatum.</li> <li>Der Rechnungsersteller hat in seinem PS einen Datensatz erzeugt, bestehend aus <ul style="list-style-type: none"> <li>einer Rechnung - bestehend aus strukturierten Daten und einem PDF - und</li> <li>ggf. weiteren Dokumenten - jeweils bestehend aus strukturierten Daten und einem PDF.</li> </ul> </li> <li>Der Rechnungsempfänger hat ein Nutzerkonto im Fachdienst.</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Der Rechnungsempfänger hat dem Rechnungsversand durch diesen Rechnungsersteller nicht widersprochen.</li> </ul>
Ablauf	<p>Der Rechnungsersteller übergibt mittels PS dem Fachdienst die zu versendenden Datensätze. Dies umfasst:</p> <ul style="list-style-type: none"> <li>• für alle Datensätze übergreifend:             <ul style="list-style-type: none"> <li>• die eigene Telematik-ID</li> <li>• den gewünschten Modus für die Validierung (siehe 4.4.1) - TEST oder NORMAL</li> <li>• das gewünschte Format der zurückzugebenden Daten - nur Token oder auch angereichertes PDF</li> </ul> </li> <li>• pro Datensatz:             <ul style="list-style-type: none"> <li>• die zu validierenden Daten aus seinem PS                 <ul style="list-style-type: none"> <li>• Rechnung</li> <li>• ggf. ergänzende Dokumente</li> <li>• Daten des Rechnungsempfängers</li> </ul> </li> </ul> </li> </ul> <p>Der Fachdienst verarbeitet die Datensätze, d.h. pro Datensatz:</p> <ul style="list-style-type: none"> <li>• Er validiert die Daten auf Nichtvorliegen von gravierenden Fehlern:             <ul style="list-style-type: none"> <li>• Grundlegende Korrektheit der Rechnungsdaten (vgl. 4.8.1.1)</li> <li>• Korrektheit ggf. der Metadaten/Typangaben der Dokumente</li> <li>• Korrektheit des Formats des jeweiligen PDF</li> </ul> </li> <li>• Der Fachdienst speichert die übergebenen Daten, abhängig vom angegebenen Modus:             <ul style="list-style-type: none"> <li>• TEST: nur Validierung, d.h. es werden <i>keine</i> Daten gespeichert</li> <li>• NORMAL: Speicherung nur, wenn <i>keine gravierenden</i> Fehler vorliegen</li> </ul> </li> <li>• Falls der Fachdienst die Daten speichert, werden außerdem folgende Schritte durchgeführt:             <ul style="list-style-type: none"> <li>• Es wird ein neuer Rechnungs-Workflow angelegt im Zustand "OFFEN".</li> <li>• Dieser wird                 <ul style="list-style-type: none"> <li>• dem Nutzerkonto des Rechnungserstellers gemäß Telematik-ID als Ersteller und</li> <li>• dem Nutzerkonto des Rechnungsempfängers gemäß KVN-R als Empfänger zugeordnet.</li> </ul> </li> <li>• Der Rechnung und jedem ggf. zugehörigen Dokument wird vom Fachdienst jeweils                 <ul style="list-style-type: none"> <li>• ein Rechnungs- bzw. Dokument-Token zugeordnet sowie</li> <li>• eine Signatur erzeugt und gespeichert.</li> </ul> </li> <li>• Der Fachdienst erzeugt eine Benachrichtigung (NEUE_RG) an</li> </ul> </li></ul>

	<p>den Rechnungsempfänger.</p> <p>Der Fachdienst gibt das Ergebnis an das PS zurück, d.h. pro Datensatz einen Antwort-Datensatz, bestehend aus:</p> <ul style="list-style-type: none"> <li>• Ergebnis der Validierung (inkl. ggf. Fehlern)</li> <li>• falls Daten gespeichert wurden: <ul style="list-style-type: none"> <li>• Referenz auf den angelegten Workflow,</li> <li>• das Rechnungs-Token und</li> <li>• ggf. die Dokument-Token</li> <li>• ggf. im FD erzeugtes angereichertes PDF, sofern dies angefordert wurde</li> </ul> </li> </ul> <p>Hinweis: Bei Bedarf kann der Rechnungsersteller ein zu versendendes Dokument als "Persönlich" (nur für den Versicherten) markieren.</p>
Nachbedingungen	<p>Pro erfolgreich versendetem Datensatz (Modus NORMAL):</p> <ul style="list-style-type: none"> <li>• Der Fachdienst hat einen neuen Rechnungs-Workflow angelegt.</li> <li>• Das PS des Rechnungserstellers verfügt über das angereicherte PDF (falls angefordert), das Rechnungs-Token und ggf. Dokument-Token.</li> <li>• Dem Rechnungs-Workflow ist der Rechnungsempfänger zugeordnet.</li> <li>• Dem Rechnungs-Workflow ist der Rechnungsersteller zugeordnet.</li> <li>• Der Rechnungs-Workflow befindet sich im Status OFFEN.</li> <li>• Die Rechnung und die ggf. ergänzenden Dokumente sind als "ungelesen" markiert.</li> <li>• Der Versicherte wurde benachrichtigt (Typ der Benachrichtigung "NEUE_RG").</li> </ul> <p>Für jeden sonstigen Datensatz, d.h. ein Datensatz, der nur validiert (also im Modus TEST) oder aufgrund von gravierenden Fehlern abgelehnt wurde, wird das Validierungsergebnis oder eine Fehlermeldung zurückgegeben. Falls bei einem Datensatz</p> <ul style="list-style-type: none"> <li>• anhand der übergebenen Daten des Rechnungsempfängers kein Nutzerkonto im Fachdienst gefunden werden kann, <i>oder</i></li> <li>• der Rechnungsempfänger dem Rechnungsversand durch diesen Rechnungsersteller widersprochen hat,</li> </ul> <p>dann erhält das PS des Rechnungserstellers die Information, dass der Versand einer Rechnung für den Rechnungsempfänger nicht möglich ist.</p>
Alternativen	-

[&lt;=]

**AF\_10271 - Abfrage von angereicherten PDF per Token (Rechnungsersteller)****Tabelle 17: Use Case Abfrage von angereicherten PDF per Token (Rechnungsersteller)**

Attribute	Bemerkung
Beschreibung	Dieser Anwendungsfall beschreibt den Abruf eines angereicherten PDF aus dem Fachdienst seitens des Rechnungserstellers mittels eines Tokens, welches er zuvor bei der Übergabe einer Rechnung bzw. eines Dokuments vom Fachdienst erhalten hat.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Rechnungsersteller hat ein Nutzerkonto.</li> <li>• Der Rechnungsersteller ist autorisiert.</li> <li>• Der Rechnungsersteller verfügt über ein Token, welches er zuvor bei der Übergabe einer Rechnung bzw. eines Dokuments vom Fachdienst erhalten hat.</li> <li>• Im Fachdienst liegen die dem Token entsprechenden Daten vor (Rechnung oder Dokument).</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Rechnungsersteller ruft das angereicherte PDF zu einer Rechnung bzw. einem Dokument aus dem Fachdienst ab. Er übergibt dazu das Token.</li> <li>• Der Fachdienst prüft, ob es zu dem Token eine Rechnung bzw. ein Dokument gibt.</li> <li>• Falls ja, wird das angereicherte PDF zurückgegeben.</li> </ul>
Nachbedingung	Im Erfolgsfall: <ul style="list-style-type: none"> <li>• Der Rechnungsersteller hat das angereicherte PDF erhalten.</li> </ul>
Alternativen	<ul style="list-style-type: none"> <li>• Im Fehlerfall wird eine Fehlermeldung zurückgegeben.</li> <li>• Der Anwendungsfall kann alternativ auch für eine Menge ("Bulk") von Token durchgeführt werden. In diesem Fall <ul style="list-style-type: none"> <li>• werden mehrere Token übergeben und</li> <li>• pro Token entweder das angereicherte PDF - oder im Fall eines Fehlers - eine Fehlermeldung zurückgegeben.</li> </ul> </li> </ul>

[&lt;=]

**6.3 Empfang von Rechnungen****6.3.1 Abruf von Rechnungen und Dokumenten****AF\_10138 - Abruf von Rechnungen (Rechnungsempfänger)****Tabelle 18: Use Case Abruf von Rechnungen (Rechnungsempfänger)**

Attribute	Bemerkung
-----------	-----------

Beschreibung	Der Anwendungsfall beschreibt den Abruf einer Liste von Rechnungen und zugehörigen Dokumenten durch den Rechnungsempfänger mittels Suchabfrage aus dem eRg FdV.
Vorbedingungen	<ul style="list-style-type: none"> <li>• Der Rechnungsempfänger (Nutzer) ist autorisiert und hat ein Nutzerkonto.</li> <li>• Im Fachdienst sind Rechnungs-Workflows vorhanden, die ihm als Empfänger zugeordnet sind.</li> </ul>
Ablauf	<p>Der Rechnungsempfänger ruft mittels eRg FdV im Fachdienst Rechnungen ab und übergibt dazu:</p> <ul style="list-style-type: none"> <li>• Suchparameter (Filter): <ul style="list-style-type: none"> <li>• Status (einer oder mehrere) des Rechnungs-Workflows</li> <li>• Behandelte Person (in den Rechnungen genannte behandelte Person nach Vorname, Name)</li> <li>• Behandelnder Leistungserbringer</li> <li>• optional: Markierung(en)</li> </ul> </li> <li>• Sortierkriterium - genau eines der folgenden: <ul style="list-style-type: none"> <li>• Rechnungsdatum (ist Default, wenn kein anderes ausgewählt)</li> <li>• Zahlungszieldatum (optional)</li> <li>• Gesamtbetrag</li> </ul> </li> <li>• Im eRg FdV gewählte/definierte Parameter für das Paging<sup>1</sup>: <ul style="list-style-type: none"> <li>• Paging Size (Maximalanzahl der zurückzugebenden Rechnungs-Workflows)</li> <li>• Auswahl der ersten/nächsten/vorherigen anzuzeigenden Treffermenge (Page) zur Suche, entsprechend Sortierkriterium</li> </ul> </li> <li>• Der Fachdienst liefert die Treffermenge zurück.</li> </ul>
Nachbedingungen	<p>Das eRg FdV hat eine Liste der Rechnungs-Workflows erhalten:</p> <ul style="list-style-type: none"> <li>• gefiltert entsprechend Suchparameter</li> <li>• sortiert gemäß Sortierkriterium</li> <li>• Ausschnitt der Treffermenge gemäß Paging Parametern</li> </ul> <p>Zu jedem Rechnungs-Workflow gibt es:</p> <ul style="list-style-type: none"> <li>• eine <u>Zusammenfassung</u> zwecks Anzeige in einer Übersicht mit den wichtigsten Daten: <ul style="list-style-type: none"> <li>• Status des Workflows</li> <li>• Markierung(en)</li> <li>• Name des behandelnden Leistungserbringers (LE)</li> <li>• Datum der Rechnung</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Information, ob Korrekturrechnung</li> <li>• Gesamtbetrag</li> <li>• Anzahl der ergänzenden Dokumente (falls vorhanden)</li> <li>• Referenz (Rechnungs-Token) auf das angereicherte PDF</li> <li>• <u>Detailinformationen</u> zwecks Anzeige in einer Detailansicht: <ul style="list-style-type: none"> <li>• Name des behandelnden LE</li> <li>• Datum der Rechnung</li> <li>• Information, ob Korrekturrechnung</li> <li>• Diagnose(n)</li> <li>• Liste der Rechnungspositionen (alle Informationen, siehe 4.8.1.1- Rechnung)</li> <li>• Gesamtbetrag</li> <li>• Informationen zur Zahlung der Rechnung: <ul style="list-style-type: none"> <li>• Zahlungszieldatum</li> <li>• Bankverbindung</li> </ul> </li> <li>• Referenz (Rechnungs-Token) auf das angereicherte PDF</li> <li>• Liste der ergänzenden Dokumente (falls vorhanden), jeweils mit: <ul style="list-style-type: none"> <li>• grundlegende Angaben wie Titel und Typ des Dokuments (wenn vorhanden)</li> <li>• Markierung(en)</li> <li>• Referenz (Dokument-Token) auf das angereicherte PDF</li> </ul> </li> </ul> </li> </ul> <p>Der Rechnungsempfänger kann</p> <ul style="list-style-type: none"> <li>• die Liste der Rechnungen in einer Übersicht im eRg FdV ansehen,</li> <li>• einzelne Einträge in der Detailansicht öffnen und</li> <li>• zu den Rechnungen und Dokumenten das angereicherte PDF abrufen</li> </ul>
Alternativen	-

【<=】

<sup>1</sup>Anmerkung: Die Auswahl der abzurufenden Treffermenge aus der Gesamtmenge der Treffer und das Durchlaufen der Treffermenge können z.B. durch Verwendung der FHIR Search API erfolgen. Näheres wird in der Spezifikation [gemSpec\_eRg\_FD] festgelegt.

#### **AF\_10262 - Abfrage von Daten zu Rechnungen und Dokumenten per Token (Rechnungsempfänger)**

**Tabelle 19: Use Case Abfrage von Daten zu Rechnungen und Dokumenten per Token (Rechnungsempfänger)**

Attribute	Bemerkung
Beschreibung	Dieser Anwendungsfall beschreibt den Abruf des angereicherten PDF

	und optional von strukturierten Daten und/oder Original-PDF aus dem Fachdienst seitens des Rechnungsempfängers (Versicherter) mittels eines Tokens, welches er zuvor durch Abfrage per eRg FdV erlangt hat (siehe auch AF_10138).
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Rechnungsempfänger hat ein Nutzerkonto.</li> <li>• Der Rechnungsempfänger ist autorisiert.</li> <li>• Der Rechnungsempfänger hat mittels Abfrage per eRg FdV ein Token erlangt.</li> <li>• Im Fachdienst liegen die dem Token entsprechenden Daten vor (Rechnung oder Dokument).</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Rechnungsempfänger ruft das angereicherte PDF und optional strukturierte Daten und/oder Original-PDF zu einer Rechnung oder einem Dokument aus dem Fachdienst ab. Er übergibt dazu: <ul style="list-style-type: none"> <li>• ein Token (zu Dokument oder Rechnung)</li> <li>• eine Angabe, ob strukturierte Daten und/oder Original-PDF und/oder die Signatur zusätzlich angefordert werden</li> </ul> </li> <li>• Der Fachdienst prüft, ob es zu dem Token ein Dokument bzw. eine Rechnung gibt.</li> <li>• Falls ja, wird das angereicherte PDF zurückgegeben.</li> <li>• Falls angegeben, werden zusätzlich strukturierte Daten und/oder Original-PDF und/oder die Signatur zurückgegeben.</li> </ul>
Nachbedingung	<p>Im Erfolgsfall:</p> <ul style="list-style-type: none"> <li>• Der Rechnungsempfänger hat das angereicherte PDF und ggf. strukturierte Daten und/oder Original-PDF erhalten.</li> <li>• Die Rechnung/das Dokument wurde im FD markiert als "gelesen".</li> </ul>
Alternativen	Im Fehlerfall wird eine Fehlermeldung zurückgegeben.

[&lt;=]

### 6.3.2 Berechtigung zum Rechnungsversand

#### AF\_10140 - Automatische Anlage der individuellen Berechtigung zum Rechnungsversand

Der im Anwendungsfall beschriebene Vorgang dient dazu, individuelle Berechtigungen seitens des Rechnungsempfängers für einzelne Rechnungsersteller festzuhalten und individuelle Widerrufe zu ermöglichen. Durch die Versendung der ersten Rechnung an den Rechnungsempfänger initiiert der Rechnungsersteller die Anlage einer für ihn geltenden individuellen Berechtigungsregel - basierend auf der generellen Zustimmung des Rechnungsempfängers. Diese Zustimmung hat der Rechnungsempfänger mit der Einrichtung seines Nutzerkontos bereits erteilt, sodass hier keine explizite Bestätigung durch ihn erforderlich ist, siehe 6.6.1-1- Einrichten eines Kontos für Versicherte. Die automatisch angelegten Berechtigungsregeln ermöglichen jedoch, dass der Rechnungsempfänger im eRg FdV sehen kann, welche Rechnungsersteller die Berechtigung zum Rechnungsversand an ihn konkret genutzt haben. Außerdem bietet

sich dem Rechnungsempfänger so die Möglichkeit, die Berechtigung für einzelne Rechnungsersteller über das eRg FdV individuell zu widerrufen, wieder zu bestätigen, usw.

**Tabelle 20: Use Case Automatische Anlage der individuellen Berechtigung zum Rechnungsversand**

Attribute	Bemerkung
Beschreibung	Der im Anwendungsfall beschriebene Vorgang dient dazu, ausgehend vom Versand von Rechnungen, die individuelle Berechtigung zum Rechnungsversand für einzelne Rechnungsersteller für den Versicherten sichtbar zu machen und deren Widerruf zu ermöglichen.
Vorbedingungen	<ul style="list-style-type: none"> <li>• Der Rechnungsersteller (Nutzer) hat im Rahmen des Behandlungsvertrags die Einwilligung des Rechnungsempfängers zum Versand digitaler Rechnungen erhalten.</li> <li>• Der Rechnungsempfänger (Versicherter) hat ein Nutzerkonto im Fachdienst. (Somit hat er generell zugestimmt, dass digitale Rechnungen an ihn geschickt werden dürfen.)</li> <li>• Der Rechnungsersteller hat bislang noch keine Rechnung an den Rechnungsempfänger geschickt. Es liegt dementsprechend noch keine Berechtigungsregel vor, die die individuelle Berechtigung dieses Rechnungserstellers zum Rechnungsversand erfasst.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Rechnungsersteller sendet eine Rechnung über den Fachdienst an den Rechnungsempfänger (siehe Anwendungsfälle dazu in 6.2.4).</li> <li>• Dadurch wird die Anlage einer Berechtigungsregel im Fachdienst ausgelöst.</li> </ul>
Nachbedingungen	<ul style="list-style-type: none"> <li>• Eine Berechtigungsregel wurde vom Fachdienst angelegt mit diesen Angaben: <ul style="list-style-type: none"> <li>• Typ: "Rechnungsversand"</li> <li>• Initiator: der Rechnungsersteller</li> <li>• Bestätiger: der Rechnungsempfänger</li> <li>• Berechtigter: der Rechnungsersteller</li> <li>• Betroffener: der Rechnungsempfänger</li> <li>• Zustand: "gültig"</li> </ul> </li> <li>• Der Rechnungsempfänger kann den Rechnungsersteller und die für ihn geltende individuelle Berechtigung in der Berechtigungsverwaltung sehen und die Berechtigung bei Bedarf bearbeiten (widerrufen, bestätigen).</li> </ul>
Alternativen	-

[<=]

## AF\_10265 - Bearbeitung von Berechtigungen



Tabelle 21: Use Case Bearbeitung von Berechtigungen

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Bearbeitung der Berechtigungen durch einen Rechnungsempfänger in seinem Nutzerkonto.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Nutzer (Versicherter) ist autorisiert.</li> <li>• Der Nutzer hat ein Nutzerkonto.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Nutzer ruft im eRg FdV die Funktion zur Bearbeitung der Berechtigungen zu seinem Nutzerkonto auf.</li> <li>• Das eRg FdV ruft vom Fachdienst die aktuell hinterlegten Berechtigungen ab und stellt diese dar.</li> <li>• Der Nutzer passt diese ggf. nach seinen Bedürfnissen an, d.h. ggf. vorhandene Berechtigungen können <ul style="list-style-type: none"> <li>• widerrufen/wieder entzogen werden,</li> <li>• (wieder) erteilt werden,</li> <li>• gelöscht werden.</li> </ul> </li> <li>• Das eRg FdV überträgt die Einstellungen an den Fachdienst.</li> <li>• Der Fachdienst speichert die aktualisierten Einstellungen.</li> </ul> <p>Hinweise:</p> <ul style="list-style-type: none"> <li>• Im MVP ist dieser Anwendungsfall auf die Rechnungsversandberechtigungen beschränkt, d.h. der Nutzer ist Rechnungsempfänger.</li> <li>• Näheres zu Berechtigungen siehe <a href="#">4.6.3.2</a>.</li> </ul>
Nachbedingung	Die aktualisierten Berechtigungen sind gespeichert im Fachdienst und ab sofort wirksam.
Alternativen	-

[&lt;=]

### 6.3.3 Benachrichtigung empfangen

#### AF\_10186 - Benachrichtigung empfangen

Tabelle 22: Use Case Benachrichtigung empfangen

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt den Empfang von Benachrichtigungen durch den Empfänger (Versicherter).
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Fachdienst hat eine Benachrichtigung mit einem angegebenem Typ (siehe <a href="#">4.4.3</a>) an den Empfänger (Versicherter) geschickt.</li> </ul>

	<ul style="list-style-type: none"> <li>Der Empfänger hat den Empfang von Benachrichtigungen dieses Typs nicht blockiert.</li> <li>Der Empfänger hat ein Nutzerkonto und hat Zugriff auf sein registriertes Endgerät mit eRg FdV.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>Die Benachrichtigung wird vom Fachdienst auf das Endgerät des Empfängers weitergeleitet.</li> <li>Der Empfänger nimmt die Benachrichtigung zur Kenntnis und öffnet das eRg FdV, wo er erforderlichenfalls zunächst seine Identität authentifizieren lassen muss.</li> <li>Der Versicherte sieht nach erfolgter Autorisierung im eRg FdV im entsprechenden Bereich der Nutzeroberfläche eine für ihn verständliche Anzeige, welcher Typ von Benachrichtigung eingetroffen ist.</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>Die Benachrichtigung ist im eRg FdV im entsprechenden Bereich der Nutzeroberfläche für den Empfänger sichtbar.</li> </ul>
Alternativen	-

[&lt;=]

## 6.4 Verwaltung von empfangenen Rechnungen

### AF\_10245 - Manuelles Ändern des Bearbeitungsstatus' von Rechnungen

Tabelle 23: Use Case Manuelles Ändern des Bearbeitungsstatus' von Rechnungen

Attribute	Bemerkung
Beschreibung	Eine E-Rechnung (inkl. der zugehörigen Dokumente) kann sich im Workflow-Status "OFFEN", "ERLEDIGT" oder "PAPIERKORB" befinden. Da Dokumente hier stets ergänzend zu einer Rechnung sind, bezieht sich der Status einer E-Rechnung stets auch auf die zugehörigen Dokumente (siehe <a href="#">4.4.1- Workflow einer Rechnung</a> ). Eine Änderung soll manuell über das eRg FdV ermöglicht werden, um Rechnungen nach ihren Bearbeitungszuständen verwalten zu können.
Vorbedingung	<ul style="list-style-type: none"> <li>Der Rechnungsempfänger hat ein Nutzerkonto.</li> <li>Der Rechnungsempfänger ist autorisiert.</li> <li>Der Rechnungsempfänger hat Zugriff auf mindestens eine Rechnung (einen Rechnungs-Workflow inklusive referenzierter Rechnungen und Dokumente).</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>Der Rechnungsempfänger wählt im eRg FdV eine Rechnung (einen Rechnungs-Workflow) aus.</li> <li>Der Rechnungsempfänger ändert über das eRg FdV den Status der ausgewählten Rechnung</li> </ul>

	<ul style="list-style-type: none"> <li>• von "OFFEN" auf "ERLEDIGT" oder "PAPIERKORB",</li> <li>• von "ERLEDIGT" auf "OFFEN" oder "PAPIERKORB",</li> <li>• von "PAPIERKORB" auf "OFFEN".</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>• Der zugehörige Rechnungs-Workflow befindet sich in dem vom Rechnungsempfänger gewählten Status.</li> <li>• Bei einem Übergang von "PAPIERKORB" oder "ERLEDIGT" auf "OFFEN" wurde die Frist T_OFFEN_BIS für das Löschdatum neu gesetzt (siehe 5.5.6.3).</li> <li>• Bei einem Übergang von "OFFEN" auf "ERLEDIGT" wurde die Frist T_ERLEDIGT_BIS für das Löschdatum neu gesetzt (siehe 5.5.6.3).</li> </ul>
Alternative	<p>Der Anwendungsfall soll auch für die gleichzeitige Änderung mehrerer Rechnungs-Workflows umgesetzt werden, wobei hier Unterschiede bei den erlaubten Statusübergängen je nach Ausgangsstatus der Rechnungen beachtet werden müssen.</p> <p>Neben einer Statusänderung soll der Nutzer alternativ die Möglichkeit erhalten, eine Rechnung aus dem Status PAPIERKORB manuell endgültig aus dem Fachdienst zu löschen.</p>

[&lt;=]

**AF\_10160 - Manuelles Markieren von Rechnungen und Dokumenten****Tabelle 24: Use Case Manuelles Markieren von Rechnungen und Dokumenten**

Attribute	Bemerkung
Beschreibung	Unabhängig vom Status einer E-Rechnung soll es dem Nutzer auch ermöglicht werden, "Markierungen" an E-Rechnungen vorzunehmen, um bestimmte Bearbeitungsschritte zu vermerken (siehe 4.4.2-Markierungen). Diese beziehen sich - anders als die Workflow-Status - jeweils auf eine einzelne Rechnung oder ein einzelnes ergänzendes Dokument.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Rechnungsempfänger hat ein Nutzerkonto.</li> <li>• Der Rechnungsempfänger ist autorisiert.</li> <li>• Der Rechnungsempfänger hat Zugriff auf mindestens eine Rechnung mit ggf. ergänzenden Dokumenten (einen Rechnungs-Workflow).</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Rechnungsempfänger wählt im eRg FdV wenigstens eine Rechnung oder ein ergänzendes Dokument aus.</li> <li>• Der Rechnungsempfänger nutzt eine im eRg FdV vorhandene Funktionalität, die genutzt werden kann, um einen der folgenden Bearbeitungsschritte - jeweils mit Zeitpunkt - manuell zu dokumentieren: <ul style="list-style-type: none"> <li>• Markieren (einer Rechnung) als "bezahlt" mit Zeitpunkt</li> <li>• Markieren (einer Rechnung/eines Dokuments) als "gelesen" oder "ungelesen"</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Markieren (einer Rechnung/eines Dokuments) als "archiviert"</li> <li>• Markieren (einer Rechnung/eines Dokuments) als "geteilt"</li> <li>• Markieren (einer Rechnung/eines Dokuments) als "eingereicht per Post"</li> <li>• Der Rechnungsempfänger gibt ggf. ergänzende Informationen zur Markierung ein.</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>• Im Fachdienst wurde die ausgewählte Rechnung/das ausgewählte Dokument mit der entsprechenden Markierung versehen.</li> <li>• Die Markierung ist mit den entsprechenden Nutzern verknüpft.</li> <li>• Ggf. wurden optionale ergänzende Informationen der Markierung hinzugefügt.</li> </ul>
Alternativen	Der Anwendungsfall soll auch für die gleichzeitige Änderung mehrerer Rechnungen und Dokumente umgesetzt werden.

[&lt;=]

**AF\_10261 - Automatisches Markieren als "gelesen"****Tabelle 25: Use Case Automatisches Markieren als "gelesen"**

Attribute	Bemerkung
Beschreibung	Sobald ein Rechnungsempfänger sich eine zuvor ungelesene Rechnung oder ein zuvor ungelesenes Dokument ansieht, soll diese oder dieses automatisch als gelesen markiert werden.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Rechnungsempfänger hat ein Nutzerkonto.</li> <li>• Der Rechnungsempfänger ist autorisiert.</li> <li>• Der Rechnungsempfänger hat Zugriff auf mindestens eine Rechnung mit ggf. ergänzenden Dokumenten (einen Rechnungs-Workflow).</li> <li>• Die Rechnung ist als "ungelesen" markiert.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Rechnungsempfänger nutzt eine Funktion im eRg FdV, um die Rechnung zu lesen (z.B. Öffnen der Detailansicht der strukturierten Rechnungsdaten oder des PDF).</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>• Die Rechnung ist als "gelesen" markiert.</li> </ul>
Alternativen	-

[&lt;=]

**AF\_10246 - Automatisches Verschieben von Rechnungen in den Papierkorb****Tabelle 26: Use Case Automatisches Verschieben von Rechnungen in den Papierkorb**

Attribute	Bemerkung
-----------	-----------

Beschreibung	Daten im eRg FD sollen dort nicht zeitlich unbegrenzt gespeichert werden. Daher werden E-Rechnungen und ggf. ergänzende Dokumente aus den Zuständen "OFFEN" und "ERLEDIGT" durch den Fachdienst automatisiert in den Status "PAPIERKORB" überführt, wenn die jeweils festgelegte Frist für die Aufbewahrung in einem dieser Zustände (T_OFFEN_BIS bzw. T_ERLEDIGT_BIS) verstrichen ist (siehe <u>4.4.1.1- Automatische Verschiebung und Löschung von Rechnungen</u> ).
Vorbedingung	<ul style="list-style-type: none"> <li>Es liegt ein Rechnungs-Workflow im Status "OFFEN" vor und der Zeitpunkt T_OFFEN_BIS ist verstrichen. <i>oder</i></li> <li>Es liegt ein Rechnungs-Workflow im Status "ERLEDIGT" vor und der Zeitpunkt T_ERLEDIGT_BIS ist verstrichen.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>Automatisierte Funktionalität des Fachdienstes (z.B. zum Monatsende)</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>Der Rechnungs-Workflow (E-Rechnung und ggf. ergänzende Dokumente) befindet sich im Zustand "PAPIERKORB".</li> <li>Der Versicherte wurde benachrichtigt (Typ der Benachrichtigung "PAPIERKORB").</li> </ul>
Alternativen	-

[&lt;=]

**AF\_10247 - Automatisches endgültiges Löschen von Rechnungen****Tabelle 27: Use Case Automatisches endgültiges Löschen von Rechnungen**

Attribute	Bemerkung
Beschreibung	Eine E-Rechnung mit ggf. ergänzenden Dokumenten im Status "PAPIERKORB" wird unwiederbringlich gelöscht, sobald die festgelegte Löschfrist (T_LÖSCHEN_AM) überschritten ist (siehe <u>4.4.1.1- Automatische Verschiebung und Löschung von Rechnungen</u> ).
Vorbedingung	<ul style="list-style-type: none"> <li>Es liegt ein Rechnungs-Workflow im Status "PAPIERKORB" vor und der Zeitpunkt T_LÖSCHEN_AM ist erreicht.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>Automatisierte Funktionalität des Fachdienstes (z.B. zum Monatsende)</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>Der Rechnungs-Workflow (E-Rechnung inklusive Daten und ggf. ergänzenden Dokumenten) ist unwiderruflich aus dem Fachdienst entfernt.</li> </ul>
Alternativen	-

[&lt;=]

## 6.5 Einreichung von Rechnungen

### 6.5.1 Anwendungsfälle des Rechnungseinreichers

Die verschiedenen Möglichkeiten des Versicherten, eine E-Rechnung und/oder ergänzende Dokumente bei seinem KTR einzureichen, sind in Abschnitt 4- Fachliches Konzept erläutert. In allen Varianten erfolgt die Einreichung nicht über den eRg FD und führt beim Einreichen "per Teilen" auch zu keiner automatischen Zustandsänderung von Rechnungen und Dokumenten. Im folgenden ist deshalb nur der Use Case des Einreichens per Frontend beschrieben, da alleinig dieser eine Änderung im Fachdienst nach sich zieht.

#### AF\_10260 - Einreichung per Frontend

**Tabelle 28: Use Case Einreichung per Frontend**

Attribute	Bemerkung
Beschreibung	Der Rechnungseinreicher reicht eine Rechnung über schon vorhandene digitale Einreichewege über die Service-App seines Kostenträgers ein.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Rechnungseinreicher hat ein Nutzerkonto.</li> <li>• Der Rechnungseinreicher ist autorisiert.</li> <li>• Der Rechnungseinreicher hat Zugriff auf mindestens eine Rechnung mit ggf. ergänzenden Dokumenten - das heißt, er ist auch Rechnungsempfänger.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Rechnungseinreicher wählt im eRg FdV eine Rechnung oder ein Dokument aus, welches er bei seinem KTR (Herausgeber des eRg FdV) einreichen möchte.</li> <li>• Der Rechnungseinreicher nutzt im eRg FdV eine (außerhalb des FD eRg) existierende Funktionalität für die Einreichung von Dokumenten: <ul style="list-style-type: none"> <li>• per Weitergabe eines PDF mit strukturierten Daten <i>oder</i></li> <li>• per Weitergabe eines Token</li> </ul> </li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>• Die vom Rechnungseinreicher gewählte Rechnung oder das gewählte Dokument wurde <ul style="list-style-type: none"> <li>• als angereichertes PDF (siehe <u>6.3.1-2- Abfrage von Daten zu Rechnungen und Dokumenten per Token (Rechnungsempfänger)</u>) <i>oder</i></li> <li>• als Rechnungs-/Dokument-Token aus dem Fachdienst geladen und an das Backend des KTR weitergegeben.</li> </ul> </li> <li>• Die Rechnung/das Dokument wurde als "eingereicht (per Frontend)" markiert, mit dem Datum versehen und mit dem KTR verknüpft.</li> </ul>

Alternativen	Der Anwendungsfall soll auch für die gleichzeitige Weitergabe mehrerer Rechnungen und Dokumente umgesetzt werden.
--------------	---

[&lt;=]

## 6.5.2 Anwendungsfälle des Kostenträgers

### AF\_10180 - Abfrage von Daten zu Rechnungen und Dokumenten per Token (Kostenträger)

**Tabelle 29: Use Case Abfrage von Daten zu Rechnungen und Dokumenten per Token (Kostenträger)**

Attribute	Bemerkung
Beschreibung	<p>Dieser Anwendungsfall beschreibt den Abruf von Daten aus dem Fachdienst seitens des Kostenträger (KTR) mittels Token zu eingereichten Rechnungen und/oder Dokumenten, d.h.</p> <ul style="list-style-type: none"> <li>mit Token aus den Barcodes postalisch eingereichter Rechnungen/Dokumente (siehe <u>4.1- Einreichung per Post</u>) oder</li> <li>per Frontend geteilten Rechnungs-/Dokumententoken (siehe <u>4.2- Einreichung über das Frontend</u>).</li> </ul>
Vorbedingung	<ul style="list-style-type: none"> <li>Der KTR (Nutzer) hat ein Nutzerkonto.</li> <li>Der KTR ist autorisiert.</li> <li>Der KTR hat vom Versicherten eine oder mehrere Rechnungen und ggf. ergänzende Dokumente <ul style="list-style-type: none"> <li>per Post erhalten und die Token durch Scannen der Barcodes ausgelesen oder</li> <li>digital als Token erhalten.</li> </ul> </li> <li>Der Versicherte hat ein Nutzerkonto.</li> <li>Dort liegen die dem KTR zugeschickten Rechnungen und Dokumente in digitaler Form vor.</li> </ul>
Ablauf	<p>Der KTR nimmt eine Eingangsverarbeitung der eingegangenen Dokumente vor. Bei Rechnungen und Dokumenten mit Rechnungs-/Dokument-Token:</p> <ul style="list-style-type: none"> <li>Auslesen der Token</li> <li>Übergabe der Token an den Fachdienst, dabei Übergabe einer Information zu gewünschten Rückgabeformaten (strukturierte Daten, Original-PDF, angereichertes PDF, Signatur)</li> <li>Der Fachdienst prüft, ob es zu jedem Token ein Dokument bzw. eine Rechnung gibt.</li> <li>Falls ja, werden die Daten in der angeforderten Formatauswahl zurückgegeben.</li> </ul>

Nachbedingung	<p>Im Erfolgsfall:</p> <ul style="list-style-type: none"> <li>• Der KTR hat je nach Formatauswahl die gewünschten Ausgabedaten erhalten.</li> <li>• Die Rechnungen/Dokumente wurden im FD markiert als "Vom Kostenträger abgerufen" unter Angabe von KTR und Zeitpunkt.</li> </ul> <p>Hinweis: Ziel ist es, den Vorgang der postalischen Einreichung im Fachdienst "digital abzubilden", sodass</p> <ul style="list-style-type: none"> <li>• im Fachdienst erfasst ist, dass die Daten durch diesen KTR bereits abgerufen wurden und für diesen nicht länger relevant sind.</li> <li>• Nutzer, die ein eRg FdV verwenden, sehen können, dass die postalische Einreichung "angekommen ist", d.h. für den Einreicher ist die Einreichung wie eine auf anderem Weg erfolgte Einreichung sichtbar.</li> </ul>
Alternativen	Im Fehlerfall werden eine Fehlermeldung zurückgegeben und die nicht "einlösbaren" Token aufgeführt.

[&lt;=]

## 6.6 Einrichtung und Registrierung von Nutzerkonten

### 6.6.1 Versicherte

Im Folgenden werden Anwendungsfälle zu Registrierung und Nutzerkonten beschrieben, jedoch nur in dem Umfang, wie es für den Anwendungsdienst relevant ist. Eine Anmeldung oder Abmeldung bei der Anwendung mittels GesundheitsID erfolgt über den Autorisierungsdienst unter Verwendung des für den Nutzer zuständigen Identity Providers (IdP). Die diesbezüglichen Vorgaben und Anwendungsfälle finden sich in [gemF\_Zero-Trust].

#### AF\_10187 - Einrichten eines Kontos für Versicherte

**Tabelle 30: Use Case Einrichten eines Kontos für Versicherte**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Einrichtung eines Nutzerkontos für einen Versicherten durch den Versicherten selbst. Voraussetzung ist die Anmeldung mittels GesundheitsID unter Verwendung des für den Nutzer zuständigen IdP.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Versicherte (Nutzer) hat die Installation des Frontends des Versicherten (eRg FdV) und die Einrichtung seines Nutzerkontos begonnen.</li> <li>• Der Nutzer ist autorisiert und verfügt noch nicht über ein Nutzerkonto im Anwendungsdienst.</li> </ul>
Ablauf	<p>Der Nutzer</p> <ul style="list-style-type: none"> <li>• stimmt der Verwendung der benötigten und angefragten</li> </ul>



	<p>Identitätsattribute durch die Anwendung E-Rechnung (KVNR, Namensangaben, Geburtsdatum) zu.</p> <ul style="list-style-type: none"> <li>• stimmt den Nutzungsbedingungen des eRg FdV und des eRg FD zu.</li> <li>• stimmt der Übermittlung digitaler Rechnungen und ergänzender Dokumente über ihn betreffende medizinische Leistungen durch seine LE oder deren ADL mittels der Anwendung E-Rechnung (eRg) zu.</li> <li>• stimmt zu, dass die Zuordnung digitaler Rechnungen in den Eingang seines Nutzerkontos von ihm als verbindliche Zustellung anerkannt wird.</li> <li>• stimmt dem Empfang eingereichter digitaler Rechnungen und Dokumente durch seine KTR mittels der eRg zu.</li> <li>• nimmt die Einstellungen zu Benachrichtigungen vor, d.h. welche Typen von Nachrichten an ihn gesendet werden sollen.</li> </ul> <p>Nach erfolgreichem Durchlaufen dieser Schritte legt der Fachdienst ein Nutzerkonto für den Nutzer an und speichert dort:</p> <ul style="list-style-type: none"> <li>• Identitätsdaten (KVNR, Geburtsdatum, Namensangaben)</li> <li>• Einwilligungen</li> <li>• Einstellungen</li> </ul>
Nachbedingung	Der Nutzer hat ein gültiges Nutzerkonto und kann nun alle für Versicherte verfügbaren Funktionen der Anwendung nutzen.
Alternativen	<p>Ein Nutzerkonto kann nicht erfolgreich eingerichtet und aktiviert werden, wenn</p> <ul style="list-style-type: none"> <li>• bereits ein Nutzerkonto für den Nutzer existiert oder</li> <li>• der Nutzer der Verwendung der für die Anwendung erforderlichen Identitätsattribute widerspricht <i>oder</i></li> <li>• der Nutzer eine sonstige, aus technischen, rechtlichen oder sonstigen Gründen zwingend erforderliche Zustimmung verweigert.</li> </ul>

[&lt;=]

**AF\_10263 - Bearbeitung von Einstellungen des Nutzerkontos****Tabelle 31: Use Case Bearbeitung von Einstellungen des Nutzerkontos**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Anpassung von Nutzer-Einstellungen im Nutzerkonto eines Versicherten.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Nutzer (Versicherter) ist autorisiert.</li> <li>• Der Nutzer hat ein Nutzerkonto.</li> </ul>

Ablauf	<ul style="list-style-type: none"> <li>• Der Nutzer ruft im eRg FdV die Funktion zur Bearbeitung der Einstellungen zu seinem Nutzerkonto auf.</li> <li>• Das eRg FdV ruft vom Fachdienst die aktuell hinterlegten Einstellungen ab und stellt diese dar.</li> <li>• Der Nutzer passt diese ggf. nach seinen Bedürfnissen an: im MVP können die Einstellungen zu Benachrichtigungen geändert werden, d.h. welche Typen von Nachrichten an ihn gesendet werden.</li> <li>• Das eRg FdV überträgt die Einstellungen an den Fachdienst.</li> <li>• Der Fachdienst speichert die aktualisierten Einstellungen.</li> </ul>
Nachbedingung	Die aktualisierten Einstellungen sind gespeichert im Fachdienst und ab sofort wirksam.
Alternativen	-

[&lt;=]

### AF\_10267 - Bearbeitung von Identitätsdaten des Nutzerkontos (Namensänderung)

**Tabelle 32: Use Case Bearbeitung von Identitätsdaten des Nutzerkontos (Namensänderung)**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Übernahme eines geänderten Namens in das Nutzerkonto eines Versicherten.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Nutzer (Versicherter) ist autorisiert.</li> <li>• Der Nutzer hat ein Nutzerkonto.</li> <li>• Die Namensangaben gemäß GesundheitsID des Nutzers sind aus der aktuell gültigen Nutzeranmeldung entnehmbar.</li> </ul> <p>Hinweis: Die Namensangaben zum Nutzer können über Claims aus dem Access-Token bezogen werden. Bei Bedarf muss der Anwendungsdienst diese Claims anfordern.</p>
Ablauf	<ul style="list-style-type: none"> <li>• Der Nutzer ruft im eRg FdV die Funktion zur Bearbeitung der Identitätsdaten zu seinem Nutzerkonto auf.</li> <li>• Das eRg FdV ruft vom Fachdienst die aktuell hinterlegten Einstellungen ab und stellt diese dar.</li> <li>• Das eRg FdV zeigt die aktuell gemäß GesundheitsID gültigen Namensangaben und bietet dem Nutzer an, diese in sein Nutzerkonto zu übernehmen.</li> <li>• Der Nutzer bestätigt dies.</li> <li>• Der Fachdienst speichert die aktualisierten Angaben.</li> </ul>
Nachbedingung	Die aktualisierten Angaben sind gespeichert im Fachdienst und ab sofort wirksam.

Alternativen	<p>Falls der Nutzer die Übernahme der Daten nicht bestätigt, bleiben die zuletzt gespeicherten Angaben gültig.</p> <p>Hinweis: Dies kann in der Folge dazu führen, dass Rechnungsersteller über abweichende Namensangaben zu dem Versicherten verfügen. Der Nutzer sollte darauf hingewiesen werden.</p>
--------------	--

[&lt;=]

**AF\_10191 - Löschen seines Nutzerkontos durch den Versicherten****Tabelle 33: Use Case Löschen seines Nutzerkontos durch den Versicherten**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Löschung eines Nutzerkontos für einen Versicherten durch den Versicherten selbst. Voraussetzung ist die Anmeldung mittels GesundheitsID unter Verwendung des für den Nutzer zuständigen Identity Providers.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Nutzer (Versicherter) ist autorisiert.</li> <li>• Der Nutzer hat ein Nutzerkonto.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Nutzer wählt die Funktion zum Löschen des Nutzerkontos im eRg FdV aus.</li> <li>• Das Nutzerkonto mit allen damit verknüpften Daten wird gelöscht.</li> <li>• Die Nutzer-Sitzung am Fachdienst wird beendet.</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>• Das Nutzerkonto ist gelöscht.</li> <li>• Die Nutzer-Sitzung ist beendet.</li> </ul>
Alternativen	-

[&lt;=]

**AF\_10268 - Nutzerkonto eines Versicherten löschen lassen (Support)****Tabelle 34: Use Case Nutzerkonto eines Versicherten löschen lassen (Support)**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Löschung eines Nutzerkontos für einen Versicherten durch den Support auf Veranlassung des Nutzers.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Nutzer hat ein Nutzerkonto.</li> <li>• Der Nutzer wünscht die Löschung seines Nutzerkontos.</li> <li>• Der Nutzer kann oder möchte dies nicht selbst vornehmen.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Nutzer richtet seinen Wunsch nach Löschung seines</li> </ul>

	<p>Nutzerkontos an den Support.</p> <ul style="list-style-type: none"> <li>• Ein Verantwortlicher im Support überprüft die Nutzeridentität.</li> <li>• Nach Sicherstellung der Identität des Nutzers wird das Nutzerkonto mit allen damit verknüpften Daten durch den Verantwortlichen gelöscht.</li> <li>• Die Nutzer-Sitzung am Fachdienst wird ggf. beendet.</li> </ul> <p>Hinweis: Die sichere Überprüfung der Nutzeridentität durch den Support muss gewährleistet sein. Die konkrete Ausgestaltung erfolgt im Rahmen der Spezifikation und dem Support-Konzept (siehe [gemSpec_eRg_FD]).</p>
Nachbedingung	<ul style="list-style-type: none"> <li>• Das Nutzerkonto ist gelöscht.</li> <li>• Die Nutzer-Sitzung ist ggf. beendet.</li> </ul>
Alternativen	-

[&lt;=]

### Löschung bei Inaktivität

Die folgenden Anwendungsfälle betreffen die automatische Löschung von Nutzerkonten, wenn diese längere Zeit nicht mehr genutzt wurden, siehe [5.5.6.1- Inaktivität und automatische Löschung](#). Zu den Fristen zur Steuerung des Benachrichtigungs- bzw. Lösungszeitpunktes siehe [5.5.6.2- Löschfristen für Nutzerkonten](#).

### AF\_10270 - Hinweis auf anstehende Konto-Löschung bei Inaktivität

**Tabelle 35: Use Case Hinweis auf anstehende Konto-Löschung bei Inaktivität**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt, wie ein Versicherter auf die anstehende automatische Löschung seines Nutzerkontos bei Inaktivität hingewiesen wird.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Nutzer hat ein Nutzerkonto.</li> <li>• Der Nutzer war längere Zeit inaktiv, sodass seit der letzten Anmeldung die Frist bis zum Hinweis auf automatische Löschung verstrichen ist (T_KONTO_HINWEIS, siehe <a href="#">5.5.6.2- Löschfristen für Nutzerkonten</a>).</li> <li>• Es liegen keine E-Rechnungen und Dokumente mehr für diesen Nutzer vor.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Fachdienst stellt fest, dass seit der letzten Anmeldung die Frist bis zum Hinweis auf automatische Löschung des Kontos verstrichen ist und dort keine E-Rechnungen und Dokumente mehr vorliegen.</li> <li>• Der Fachdienst sendet eine Benachrichtigung an den Nutzer (Nachricht: KONTO_LÖSCHUNG).</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>• Die Benachrichtigung wurde verschickt.</li> </ul>

Alternativen	-
--------------	---

[&lt;=]

**AF\_10269 - Nutzerkonto eines Versicherten löschen bei Inaktivität****Tabelle 36: Use Case Nutzerkonto eines Versicherten löschen bei Inaktivität**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die automatische Löschung eines Nutzerkontos für einen Versicherten im Falle von langer Inaktivität, nach vorherigem Hinweis.
Vorbedingung	<ul style="list-style-type: none"> <li>Der Nutzer hat ein Nutzerkonto.</li> <li>Der Nutzer war längere Zeit inaktiv, sodass seit der letzten Anmeldung die Frist bis zur automatischen Löschung verstrichen ist (T_KONTO_LÖSCHEN, siehe 5.5.6.2- Löschfristen für Nutzerkonten).</li> <li>Es liegen keine E-Rechnungen und Dokumente mehr für diesen Nutzer vor.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>Der Fachdienst stellt fest, dass seit der letzten Anmeldung die Frist bis zur automatischen Löschung des Kontos verstrichen ist und dort keine E-Rechnungen und Dokumente mehr vorliegen.</li> <li>Der Fachdienst löscht das Nutzerkonto und alle damit verknüpften Daten.</li> </ul>
Nachbedingung	<ul style="list-style-type: none"> <li>Das Nutzerkonto ist gelöscht.</li> </ul>
Alternativen	-

[&lt;=]

**6.6.2 Institutionen**

Im Folgenden werden Anwendungsfälle zu Registrierung und Nutzerkonten beschrieben, jedoch nur in dem Umfang, wie es für den Anwendungsdienst relevant ist. Eine Anmeldung oder Abmeldung bei der Anwendung mittels SMC-B/HSM-B erfolgt über den Autorisierungsdienst unter Verwendung des für den Nutzer zuständigen Identity Providers. Die diesbezüglichen Vorgaben und Anwendungsfälle finden sich in [gemF\_Zero-Trust].

Die Einrichtung eines Nutzerkontos ist erforderlich für:

- Rechnungsersteller.
- KTR, die die KTR-Schnittstelle nutzen wollen (bspw. zum Abruf von Daten zu Rechnungs-/Dokument-Token).

**AF\_10266 - Einrichten eines Kontos einer Institution**

**Tabelle 37: Use Case Einrichten eines Kontos einer Institution**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Einrichtung eines Nutzerkontos für eine Institution durch die Institution selbst. Voraussetzung ist die Anmeldung mittels SMC-B/HSM-B unter Verwendung des für den Nutzer zuständigen Identity Providers.
Vorbedingung	<ul style="list-style-type: none"> <li>Die Institution verfügt über den erforderlichen TI-Zugang.</li> <li>Die Institution ist autorisiert.</li> <li>Die Institution verfügt noch nicht über ein Nutzerkonto im Anwendungsdienst.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>Die Institution ruft im Primärsystem (PS) bzw. KTR-System die Funktion zum Einrichten eines Nutzerkontos auf.</li> <li>Die Institution stimmt der Verwendung ihrer Identitätsattribute in dem für die Anwendung E-Rechnung zu nutzenden Umfang zu: <ul style="list-style-type: none"> <li>die Telematik-ID</li> <li>der Anzeigename der Institution</li> </ul> </li> <li>Die Institution stimmt den Nutzungsbedingungen zu.</li> <li>Das PS bzw. KTR-System übergibt Telematik-ID und Anzeigenamen an den Fachdienst.</li> <li>Das Nutzerkonto wird im Fachdienst angelegt.</li> </ul>
Nachbedingung	Die Institution verfügt über ein Nutzerkonto des entsprechenden Typs (Rechnungsersteller oder KTR) und kann die für diesen Institutionstyp vorgesehenen Funktionen nutzen.
Alternativen	<p>Ein Nutzerkonto kann nicht erfolgreich eingerichtet und aktiviert werden, wenn</p> <ul style="list-style-type: none"> <li>bereits ein Nutzerkonto für die Institution existiert oder</li> <li>die Institution der Verwendung der für die Anwendung erforderlichen Identitätsattribute widerspricht oder</li> <li>die Institution eine sonstige, aus technischen, rechtlichen oder sonstigen Gründen zwingend erforderliche Zustimmung verweigert.</li> </ul>

[&lt;=]

**AF\_10193 - Löschen ihres Nutzerkontos durch die Institution****Tabelle 38: Use Case Löschen ihres Nutzerkontos durch die Institution**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Löschung eines Nutzerkontos für eine Institution durch die Institution selbst. Voraussetzung ist die Anmeldung mittels SMC-B/HSM-B unter Verwendung des für den Nutzer zuständigen Identity Providers.

Vorbedingung	<ul style="list-style-type: none"> <li>Die Institution hat ein Nutzerkonto im E-Rechnung Fachdienst.</li> <li>Die Institution ist autorisiert.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>Die Institution wählt die Funktion zum Löschen des Nutzerkontos im Primärsystem bzw. KTR-System aus.</li> <li>Das Nutzerkonto mit allen damit verknüpften Daten wird gelöscht.</li> <li>Die Nutzer-Sitzung am Fachdienst wird beendet.</li> </ul> <p>Hinweis: Es ist mit technisch-organisatorischen Maßnahmen sicherzustellen, dass ein versehentliches Löschen des Nutzerkontos möglichst ausgeschlossen ist. Dies kann z.B. durch einen zusätzlichen Bestätigungsschritt erfolgen.</p>
Nachbedingung	<ul style="list-style-type: none"> <li>Das Nutzerkonto ist gelöscht.</li> <li>Die Nutzer-Sitzung ist beendet.</li> </ul>
Alternativen	-

[&lt;=]

## 6.7 Nutzerprotokolle

Nutzerprotokolle werden im E-Rechnung Fachdienst (eRg FD) ausschließlich für Versicherte geführt. Sofern für Leistungserbringer (LE) und Kostenträger (KTR) die Erforderlichkeit besteht, müssen die Systeme dieser Nutzer die Aktivitäten für die Anwendung E-Rechnung (eRg) protokollieren.

Die Protokolle für Versicherte enthalten insbesondere alle Zugriffe auf die Dokumente und Statuswechsel für Vorgänge, sowie fehlgeschlagene Login-Versuche. Die einzelnen Protokolleinträge enthalten grundsätzlich die Informationen darüber, wer wann was getan hat (Akteure). Einzelheiten hierzu werden in der Spezifikation festgelegt (siehe [gemSpec\_eRg\_FD]).

Versicherte können ihr Protokoll mittels eRg FdV (gefiltert) vom eRg FD abrufen und anschließend im eRg FdV sortieren und daraus exportieren.

### AF\_10203 - Nutzerprotokoll einsehen

**Tabelle 39: Use Case Nutzerprotokoll einsehen**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt die Einsichtnahme eines Versicherten in sein Nutzerprotokoll.
Vorbedingung	<ul style="list-style-type: none"> <li>Der Versicherte hat ein Nutzerkonto im Fachdienst.</li> <li>Der Versicherte ist autorisiert.</li> </ul>

Ablauf	<ul style="list-style-type: none"> <li>• Der Versicherte ruft den Funktionsbereich für die Anzeige seines Nutzerprotokolls auf.</li> <li>• Das eRg FdV bietet dem Versicherten die Möglichkeit, Suchparameter auszuwählen, nach denen die Protokolleinträge gefiltert werden sollen: <ul style="list-style-type: none"> <li>• Akteure - Auswahl aus: <ul style="list-style-type: none"> <li>• Rechnungsersteller</li> <li>• Kostenträger</li> <li>• Versicherte</li> <li>• Dienste</li> </ul> </li> <li>• Zeitraum</li> </ul> </li> <li>• Das eRg FdV bietet dem Versicherten die Möglichkeit, ein Sortierkriterium auszuwählen, nach denen die Protokolleinträge sortiert werden sollen:</li> <li>• Akteure (siehe oben)</li> <li>• Zeit</li> </ul> <p>Der Versicherte wählt Suchparameter und Sortierkriterium aus und ruft mittels eRg FdV das Nutzerprotokoll vom Fachdienst ab. Das eRg FdV übergibt dazu:</p> <ul style="list-style-type: none"> <li>• KVNR des Versicherten</li> <li>• Suchparameter</li> <li>• Sortierkriterium</li> <li>• Im eRg FdV gewählte/definierte Parameter für das Paging<sup>1</sup>: <ul style="list-style-type: none"> <li>• Paging Size (Maximalanzahl der zurückzugebenden Protokolleinträge)</li> <li>• Auswahl der ersten/nächsten/vorherigen anzuzeigenden Treffermenge (Page) zur Suche, entsprechend Sortierkriterium</li> </ul> </li> <li>• Der Fachdienst liefert die Treffermenge zurück.</li> </ul>
Nachbedingung	<p>Das eRg FdV hat eine Liste der Protokolleinträge (entsprechend den AuditEvents) erhalten:</p> <ul style="list-style-type: none"> <li>• gefiltert entsprechend Suchparameter</li> <li>• sortiert gemäß Sortierkriterium</li> <li>• Ausschnitt der Treffermenge gemäß Paging Parametern</li> <li>• Zu jedem Protokolleintrag gibt es eine Zusammenfassung mit den wichtigsten Daten: <ul style="list-style-type: none"> <li>• Name der durchgeführten Aktivität (gemäß Operationstyp)</li> <li>• Name des Akteurs</li> <li>• ggf. Detailangaben zu betroffenen Gegenständen (Dokument, Rechnung, Berechtigung)</li> </ul> </li> </ul>



	Der Versicherte kann die Liste im eRg FdV ansehen.
Alternativen	-

【<=】

<sup>1</sup>Anmerkung: Die Auswahl der abzurufenden Treffermenge aus der Gesamtmenge der Treffer und das Durchlaufen der Treffermenge können z.B. durch Verwendung der FHIR Search API erfolgen. Näheres wird in der Spezifikation [gemSpec\_eRg\_FD] festgelegt.

## AF\_10194 - Nutzerprotokoll exportieren

**Tabelle 40: Use Case Nutzerprotokoll exportieren**

Attribute	Bemerkung
Beschreibung	Der Anwendungsfall beschreibt, wie der Versicherte sein Nutzerprotokoll zwecks Aufbewahrung außerhalb des Fachdienstes aus dem Fachdienst exportieren kann. Dies dient insbesondere dazu, das Nutzerprotokoll bewahren zu können, bevor es im Rahmen einer Löschung des Nutzerkontos ebenfalls gelöscht wird.
Vorbedingung	<ul style="list-style-type: none"> <li>• Der Versicherte hat ein Nutzerkonto im Fachdienst.</li> <li>• Der Versicherte ist autorisiert.</li> </ul>
Ablauf	<ul style="list-style-type: none"> <li>• Der Versicherte ruft die Funktion zum Exportieren (Download) des Nutzerprotokolls auf.</li> <li>• Das eRg FdV fragt beim Fachdienst das Nutzerprotokoll ab mit der KVNR des Versicherten.</li> <li>• Der Fachdienst liefert das Protokoll an das eRg FdV.</li> </ul>
Nachbedingung	Der Versicherte kann das Protokoll mit seinem eRg FdV exportieren ("Speichern als ..." o.ä.).
Alternativen	-

【<=】

---

## 7 Dokumentenhaushalt

---

Dieses Dokument hat die nachfolgenden Auswirkungen auf den Dokumenten- und Anforderungshaushalt der Telematikinfrastruktur.

### 7.1 Neue Dokumente

Das vorliegende Dokument referenziert die folgenden Dokumente, die sich zum aktuellen Zeitpunkt in der Erstellung befinden.

**Tabelle 41: Neue Dokumente der gematik**

[Quelle]	Herausgeber: Titel
[gemSpec_DS_VAU]	gematik: Spezifikation zur vertrauenswürdigen Ausführungsumgebung
[gemSpec_eRg_FD]	gematik: Spezifikation E-Rechnung Fachdienst

### 7.2 Übersicht betroffener Dokumente

Aus dieser Spezifikation ergeben sich zunächst keine direkten Änderungsbedarfe an anderen Dokumenten.

### 7.3 Übersicht Produkt- und Anbietertypen

Die hier aufgelisteten Anforderungen richten sich an die Produkt- und Anbietertypen des E-Rechnung Fachdienstes und werden zu einem späteren Zeitpunkt zusammen mit Anforderungen aus anderen Dokumenten wie gemSpec\_eRg\_FD Eingang in diese finden.

## 8 Anhang A - TI-Zugänge und Authentifizierungslösungen für die Nutzergruppen

Tabelle 42: TI-Zugänge und Authentifizierungslösungen für die Nutzergruppen

Nutzergruppe	Empfehlung	Anbindung TI	Routing	Authentifizierung	Anmerkungen
LEI	falls schon vorhanden	Einbox-Konnektor	zentrales Netz der TI	zentraler IDP / SMC-B	Bei LEI, die bereits an die TI angebunden sind (also solche die z.B. auch GKV-Patienten haben), sind dann bereits Einbox-Konnektoren vorhanden.
LEI	empfohlen	TI Gateway (HSK)	zentrales Netz der TI	zentraler IDP / SMC-B oder SM-B (HSM-B, erst später verfügbar <sup>1</sup> )	betrifft vor allem neu anzubindende LEI betreffen, die noch keinen Einbox-Konnektor haben.
ADL	falls schon vorhanden	Einbox-Konnektor	zentrales Netz der TI	zentraler IDP / SMC-B ORG	Abrechnungsdienstleister (aka privatärztliche Verrechnungsstellen) können SMC-B Org bereits beziehen und nutzen. Falls schon Einbox-Konnektoren verfügbar, können diese genutzt werden.
ADL	empfohlen	TI Gateway (HSK)	zentrales Netz der TI	zentraler IDP / SMC-B oder SM-B (HSM-B, erst später verfügbar <sup>1</sup> )	Abrechnungsdienstleister (aka privatärztliche Verrechnungsstellen) können eine SMC-B ORG bereits beziehen und nutzen.
KTR (PKV)	falls schon vorhanden	Basis-Consumer	zentrales Netz der TI	zentraler IDP / SM-B KTR (HSM)	Falls wegen anderer TI-Anwendungen bereits eine Anbindung per Basis-Consumer vorhanden ist.
KTR (PKV)	falls schon vorhanden	Einbox-Konnektor	zentrales Netz der TI	zentraler IDP / SMC-B KTR	Falls wegen anderer TI-Anwendungen bereits eine Anbindung per Konnektor vorhanden

	n				ist.
KTR (PKV)	empfohlen	TI Gateway (HSK)	zentrales Netz der TI	zentraler IDP / SMC-B KTR oder SM-B KTR (HSM, erst später verfügbar <sup>1</sup> )	
KTR (Beihilfe)	empfohlen	TI Gateway (HSK)	zentrales Netz der TI	zentraler IDP / SMC-B KTR oder SM-B KTR (HSM, erst später verfügbar <sup>1</sup> )	Der Basis-Consumer als technische Option hat keine praktische Relevanz, da die Beihilfestellen i.d.R. erst an die TI angeschlossen werden und somit das TI Gateway als aktuellere Lösung nutzen werden.
Versicherte (GKV)	einzige Option	Internet	Internet	föderierter IDP / GesundheitsID.	
Versicherte (PKV)	einzige Option	Internet	Internet	föderierter IDP / GesundheitsID.	

<sup>1</sup> Hinweis: Die Verfügbarkeit von HSM-basierten SM-B-Identitäten wird beim TI Gateway erst später gegeben sein. Für Q1/25 ist die normative Veröffentlichung der diesbezüglichen Spezifikationen vorgesehen, mit einer flächendeckenden Verfügbarkeit ist erst im Laufe des Jahres 2025 zu rechnen.

---

## 9 Anhang B - Verzeichnisse

---

### 9.1 Abkürzungen

**Tabelle 43: Im Dokument verwendete Abkürzungen**

Kürzel	Erläuterung
ADL	Abrechnungsdienstleister
BDE	Betriebsdatenerfassung
ePA	elektronische Patientenakte
eRg	E-Rechnung
FD	Fachdienst
FdV	Frontend des Versicherten
FHIR	Fast Healthcare Interoperability Resources
GesundheitsID	Digitale Identität
GMS	Geräte Management Service
GOÄ	Gebührenordnung für Ärzte
GOZ	Gebührenordnung für Zahnärzte
HSK	High Speed Konnektor
IdP	Identity Provider
KTR	Kostenträger
KVNR	Krankenversichertensumme
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
MVP	Minimum Viable Product
PKV	Private Krankenversicherung

TEE	Trusted Execution Environment
TI	Telematikinfrastruktur
TI-ITSM	IT-Service-Management der TI
TOM	Technische u. organisatorische Maßnahmen
VZD	Verzeichnisdienst

## 9.2 Abbildungsverzeichnis

Abbildung 1: E2E-Prozess "Abrechnung und Erstattung von Leistungen, die nicht dem Sachleistungsprinzip unterliegen".....	8
Abbildung 2: Einordnung der Anwendung E-Rechnung in die TI.....	23
Abbildung 3: Hybrider Postversand.....	26
Abbildung 4: Einreichen per eRg FdV als Teil einer integrierten Versicherten-App.....	27
Abbildung 5: Einreichen per "Teilen".....	28
Abbildung 6: Workflow einer Rechnung.....	30
Abbildung 7: Status-Diagramm Rechnungsversandberechtigung.....	40
Abbildung 8: Informationsmodell der Anwendung E-Rechnung.....	41
Abbildung 9: Funktionaler Aufbau der Anwendung E-Rechnung.....	51

## 9.3 Tabellenverzeichnis

Tabelle 1: Typen von Markierungen.....	33
Tabelle 2: Typen von Benachrichtigungen.....	37
Tabelle 3: Grundlegende Datenfelder einer E-Rechnung im MVP.....	43
Tabelle 4: Grundlegende Datenfelder eines die Rechnung ergänzenden Dokuments im MVP.....	48
Tabelle 5: Funktionale Schnittstellen und Operationstypen des Fachdienstes E-Rechnung.....	55
Tabelle 6: Verwendete IDP Claims.....	57
Tabelle 7: Scopes und Zugriffsberechtigungen.....	59
Tabelle 8: Löschfristen für Nutzerkonten.....	66
Tabelle 9: Zeitpunkte zur Löschung und Aufbewahrung von Rechnungen und Dokumenten gemäß Fristen.....	67
Tabelle 10: Zugriffstypen auf Dokumente und Daten für Nutzerprotokolle.....	69
Tabelle 11: Mengengerüst Versichertenstruktur Deutschland.....	71

Tabelle 12: Mengengerüst Eingereichte Rechnungen 2018.....	72
Tabelle 13: Formulierungen in Anwendungsfallbeschreibungen.....	79
Tabelle 14 : Use Case Abfrage des Rechnungsempfängers und dessen Einwilligung zum Rechnungsversand.....	81
Tabelle 15: Use Case Rechnung mit Dokumenten validieren und versenden.....	82
Tabelle 16: Use Case Rechnung mit Dokumenten validieren und versenden (Bulk).....	87
Tabelle 17: Use Case Abfrage von angereicherten PDF per Token (Rechnungsersteller).....	90
Tabelle 18: Use Case Abruf von Rechnungen (Rechnungsempfänger).....	91
Tabelle 19: Use Case Abfrage von Daten zu Rechnungen und Dokumenten per Token (Rechnungsempfänger).....	95
Tabelle 20: Use Case Automatische Anlage der individuellen Berechtigung zum Rechnungsversand.....	96
Tabelle 21: Use Case Bearbeitung von Berechtigungen.....	97
Tabelle 22: Use Case Benachrichtigung empfangen.....	98
Tabelle 23: Use Case Manuelles Ändern des Bearbeitungsstatus' von Rechnungen.....	99
Tabelle 24: Use Case Manuelles Markieren von Rechnungen und Dokumenten.....	100
Tabelle 25: Use Case Automatisches Markieren als "gelesen".....	101
Tabelle 26: Use Case Automatisches Verschieben von Rechnungen in den Papierkorb.....	101
Tabelle 27: Use Case Automatisches endgültiges Löschen von Rechnungen.....	102
Tabelle 28: Use Case Einreichung per Frontend.....	102
Tabelle 29: Use Case Abfrage von Daten zu Rechnungen und Dokumenten per Token (Kostenträger).....	103
Tabelle 30: Use Case Einrichten eines Kontos für Versicherte.....	105
Tabelle 31: Use Case Bearbeitung von Einstellungen des Nutzerkontos.....	106
Tabelle 32: Use Case Bearbeitung von Identitätsdaten des Nutzerkontos (Namensänderung).....	107
Tabelle 33: Use Case Löschen seines Nutzerkontos durch den Versicherten.....	108
Tabelle 34: Use Case Nutzerkonto eines Versicherten löschen lassen (Support).....	109
Tabelle 35: Use Case Hinweis auf anstehende Konto-Löschung bei Inaktivität.....	109
Tabelle 36: Use Case Nutzerkonto eines Versicherten löschen bei Inaktivität.....	110
Tabelle 37: Use Case Einrichten eines Kontos einer Institution.....	111
Tabelle 38: Use Case Löschen ihres Nutzerkontos durch die Institution.....	112
Tabelle 39: Use Case Nutzerprotokoll einsehen.....	113
Tabelle 40: Use Case Nutzerprotokoll exportieren.....	115
Tabelle 41: Neue Dokumente der gematik.....	116
Tabelle 42: TI-Zugänge und Authentifizierungslösungen für die Nutzergruppen.....	117
Tabelle 43: Im Dokument verwendete Abkürzungen.....	119
Tabelle 44: Referenzierte Dokumente der gematik.....	122
Tabelle 45: Weitere Referenzen.....	122

## 9.4 Referenzierte Dokumente

### 9.4.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

**Tabelle 44: Referenzierte Dokumente der gematik**

[Quelle]	Herausgeber: Titel
[gemF_Zero-Trust]	gematik: Feature Zero Trust
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb
[gemRL_Betr_TI]	gematik: Betrieb der TI
[gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider-Dienst
[gemSpec_IDP_FD]	gematik: Spezifikation Identity Provider - Nutzungsspezifikation für Fachdienste
[gemSpec_IDP_Sek]	gematik: Spezifikation Sektoraler Identity Provider
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_OM]	gematik: Operations und Maintenance
[gemSpec_Perf]	gematik: Performance und Mengengerüst TI-Plattform

### 9.4.2 Weitere Referenzen

**Tabelle 45: Weitere Referenzen**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Android Platform Security Model]	<a href="https://dl.acm.org/doi/pdf/10.1145/3448609">https://dl.acm.org/doi/pdf/10.1145/3448609</a> (Abruf 10/23)
[Android Zero Trust]	<a href="https://developers.google.com/android/work/zero-trust-signals">https://developers.google.com/android/work/zero-trust-signals</a>



signals]	(Abruf 10/23)
[App Attest]	<a href="https://developer.apple.com/documentation/devicecheck/establishing_your_app_s_integrity">https://developer.apple.com/documentation/devicecheck/establishing_your_app_s_integrity</a> (Abruf 10/23)
[Apple Platform Security Guide]	<a href="https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf">https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf</a> (Abruf 10/23)
[Attestierungsschlüssel]	<a href="https://android-developers.googleblog.com/2022/03/upgrading-android-attestation-remote.html">https://android-developers.googleblog.com/2022/03/upgrading-android-attestation-remote.html</a> (Abruf 10/23)
[Gesundheitsbericht erstattung]	<a href="https://www.bundesgesundheitsministerium.de/gesetzlich-versicherte.html">https://www.bundesgesundheitsministerium.de/gesetzlich-versicherte.html</a> (Abruf 10/23)
[IHE Profile]	<a href="https://simplifier.net/packages/de.ihe-d.terminology/3.0.0/files/2374176">https://simplifier.net/packages/de.ihe-d.terminology/3.0.0/files/2374176</a>
[ITIL]	AXELOS: ITIL Foundation, ITIL 4 edition. TSO (The Stationery Office)
[KBV Schlüsseltabellen]	<a href="https://applications.kbv.de/S_BAR2_ARZTNRFACHGRUPPE_V1.03.xhtml">https://applications.kbv.de/S_BAR2_ARZTNRFACHGRUPPE_V1.03.xhtml</a> (Abruf 10/23)
[KDL CodeSystem]	<a href="https://simplifier.net/guide/KDL-Implementierungsleitfaden-2024/Hauptseite/CodeSystem-2024.page.md?version=current">https://simplifier.net/guide/KDL-Implementierungsleitfaden-2024/Hauptseite/CodeSystem-2024.page.md?version=current</a>
[Key & ID Attestation]	<a href="https://developer.android.com/reference/android/security/keystore/KeyProperties#PURPOSE_ATTEST_KEY">https://developer.android.com/reference/android/security/keystore/KeyProperties#PURPOSE_ATTEST_KEY</a> (Abruf 10/23)
[OAuth2]	<a href="https://datatracker.ietf.org/doc/html/rfc6749">https://datatracker.ietf.org/doc/html/rfc6749</a> (Abruf 10/23)
[Open Policy Agent]	<a href="https://www.openpolicyagent.org/">https://www.openpolicyagent.org/</a> (Abruf 10/23)
[Play Integrity API]	<a href="https://developer.android.com/google/play/integrity/verdicts">https://developer.android.com/google/play/integrity/verdicts</a> (Abruf 10/23)
[ReSTful API]	<a href="https://ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation_2up.pdf">https://ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation_2up.pdf</a> (Abruf 10/23)
[SMART on FHIR]	<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 10/23)
[VDEK]	<a href="https://www.vdek.com/presse/daten/b_versicherte.html">https://www.vdek.com/presse/daten/b_versicherte.html</a> (Abruf 10/23)
[VerifiedBoot]	<a href="https://source.android.com/docs/security/features/verifiedboot?hl=de">https://source.android.com/docs/security/features/verifiedboot?hl=de</a> (Abruf 10/23)