**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Feature: Anbindung Digitaler Gesundheitsanwendungen an die elektronische Patientenakte

| | |
|---|---|
| Version: | 1.1.0 CC 2 |
| Revision: | 446893 |
| Stand: | 18.03.2022 |
| Status: | zur Abstimmung freigegeben |
| Klassifizierung: | öffentlich_Entwurf |

Referenzierung: gemF_ePA_DiGA_Anbindung

# Dokumentinformationen

*Beim vorliegenden Dokument handelt es sich um einen Entwurf in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik versendet diesen Entwurf mit dem Ziel, dass sich Interessierte vorab einen Überblick zur möglichen Weiterentwicklung der Anwendung elektronische Patientenakte verschaffen können.*

*Die gematik übernimmt keine Gewähr für Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfs. Die gematik behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt oder teilweise Abstand zu nehmen.*

### Änderungen zur Vorversion

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

### Dokumentenhistorie

| Version | Stand | Kap./ Seite | Grund der Änderung, besondere Hinweise | Bearbeitung |
|---|---|---|---|---|
| 0.1.0 | 25.02.21 | | initiale Erstellung | gematik |
| 1.0.0 CC | 30.03.21 | | zur Abstimmung freigegeben | gematik |
| 1.0.0 CC 2 | 09.06.21 | | Einarbeitung Kommentierung | gematik |
| 1.0.0 | 09.07.21 | | freigegeben | gematik |
| 1.1.0 CC | 14.03.22 | | weitere Abstimmungen durchgeführt | gematik |
| 1.1.0 CC 2 | 18.03.22 | | weitere Abstimmungen durchgeführt | gematik |

# Inhaltsverzeichnis

# 1 Motivation des Features

Die im DVPMG enthaltenden Regelungen nach § 351 Abs. 2 SGB V-E verpflichten Krankenkassen ab dem 01.01.2023, die Daten der Versicherten aus digitalen Gesundheitsanwendungen (DiGA) unter Einwilligung der Versicherten vom DiGA-Hersteller über den Anbieter der elektronischen Patientenakte (ePA) in die ePA nach § 341 Abs. 2 Nr. 9 SGB V zu übermitteln und dort zu speichern. Die Kenntnisnahme der Daten durch den Anbieter der ePA und der Zugriff auf die Daten ist gemäß § 344 Abs. 2 Satz 2 SGB V nicht zulässig.

Eine DiGA ist ein CE-gekennzeichnetes Medizinprodukt, das folgende Eigenschaften vorweisen muss:

- Medizinprodukt niedriger Risikoklasse (I oder IIa nach MDR)
- Hauptfunktion beruht auf digitalen Technologien
- medizinischer Zweck wird wesentlich durch digitale Hauptfunktion sichergestellt
- unterstützt die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen
- Nutzung durch den Patienten oder gemeinsam durch Leistungserbringer und Patienten

Wenn eine DiGA den zuvor genannten Anforderungen aus § 33a SGB V entspricht, wird diese vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zugelassen und im Verzeichnis für DiGA nach § 139e SGB V gelistet. Der Patient bekommt die DiGA durch den behandelnden Arzt oder Psychotherapeuten verordnet oder durch eine Krankenkasse insofern die entsprechende Indikation für die jeweilige DiGA ärztlich bescheinigt wurde.

Da die Übermittlung der Daten über die Telematikinfrastruktur erfolgt, müssen auch die DiGA-Hersteller an die Telematikinfrastruktur angeschlossen werden. Dazu ist in § 351 Abs. 3 SGB V-E geregelt, dass DiGA-Hersteller neben einer entsprechenden Infrastruktur (bestehend aus Kartenterminal, Konnektor und VPN-Kartendienst) eine Komponente zur Authentifizierung (SMC-B) benötigen. Diese soll durch die gematik GmbH ausgegeben werden. Die hierfür erforderliche Bestätigung, dass es sich um einen berechtigten Hersteller i.S.d. Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (DiGAV) handelt, erfolgt durch das BfArM.

Es ist die Aufgabe der gematik gemäß § 354 Abs. 2 Nummer 6 SGB V-E bis zum 01. Januar 2022 die Festlegungen dafür zu treffen, dass Daten der Versicherten aus digitalen Gesundheitsanwendungen nach § 33a vom Hersteller der Anwendungen über den Anbieter der elektronischen Patientenakte über eine Schnittstelle, die den Anforderungen des Zwölften Kapitels genügt, in die elektronische Patientenakte übermittelt und dort verarbeitet werden können.

## 1.1 Zielsetzung

Dieses Dokument legt die Umsetzung der Anbindung einer DiGA an die Telematikinfrastruktur und die Möglichkeit zur Übermittlung von Informationen aus einer DiGA in eine elektronische Patientenakte fest.

## 1.2 Zielgruppe

Das Dokument richtet sich an DiGA-Hersteller, sowie Hersteller die von den Änderungen der ePA-Komponenten betroffen sind.

Das Dokument bildet alle Schritte des Entwicklungsprozesses in verschiedenen Kapiteln ab. Daher unterscheidet sich die intendierte Zielgruppe zwischen den einzelnen Kapiteln.

Das Kapitel 2 betrachtet die fachliche Ebene. Es dient der fachlichen Abstimmung mit Stakeholdern und fachlichen Verbänden.

Kapitel 3 beschreibt das Umsetzungskonzept. Es schafft ein übergreifendes Verständnis der angestrebten Lösung und bildet das Bindeglied zwischen der fachlichen Ebene in Kapitel 2 und der Spezifikationsebene im Kapitel 4 und 5.

Kapitel 4 und 5 beschreiben die konkrete Lösung und deren Auswirkung auf Produkttypen. Es ist daher hauptsächlich für die Abstimmung mit Herstellern, Anbietern und deren Auftraggebern relevant.

## 1.3 Abgrenzungen

Das Dokument beschreibt nur die DiGA-spezifischen Aspekte der ePA-Anpassung sowie der SMC-B-Herausgabe für DiGA-Hersteller. Weitere Aspekte, wie etwa Festlegungen zu Signaturzertifikaten einer DiGA-SMC-B werden hier nicht getroffen.

## 1.4 Methodik

### 1.4.1 User Story

User Stories werden durch eine eindeutige ID gekennzeichnet und werden im Dokument wie folgt dargestellt:
**<USt-ID> - <Zusammenfassung der User Story>**
Text / Beschreibung
[<=]

Dabei umfasst die User Story sämtliche zwischen USt-ID und der Textmarke [<=] angeführten Inhalte.

### 1.4.2 Anforderungen

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

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

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

Text / Beschreibung
[<=]

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

In Kapitel 4 werden neue oder geänderte Anforderungen und Begleittexte zumeist direkt aufgeführt (und nur in seltenen Fällen beschrieben statt aufgeführt).

Dabei werden in geänderten Afos und Begleittexten Änderungen gelb markiert.

Bei AFOs und Textänderungen, die sehr umfangreiche Tabellen betreffen, werden die Änderungen nur beschrieben, nicht schon umgesetzt, um die Lesbarkeit des Dokumentes nicht zu gefährden.

# 2 Epic und User Stories

Der Versicherte nutzt die durch seinen Leistungserbringer verschriebene DiGA und möchte die darin dokumentierten persönlichen Daten in seine ePA übermitteln lassen, um diese einem zugriffsberechtigten Leistungserbringer über das ePA-Aktensystem bereitzustellen. Dazu stellt ein DiGA-Hersteller auf Wunsch des Versicherten und mit dessen ausdrücklicher Berechtigung, strukturierte Daten aus seiner DiGA in die ePA des Versicherten ein.

## 2.1 User Stories

**USt-1 - Anbindung des DiGA-Herstellers an die TI**
Der DiGA-Hersteller möchte jeweils eine Anbindung an die Telematikinfrastruktur für seine DiGA-Instanzen, um Daten aus einer DiGA auf expliziten Wunsch in die ePA des Versicherten zu übermitteln. [<=]

**USt-2 - Datenübermittlung aus einer DiGA in eine ePA**
Der Versicherte möchte Daten, die über seine DiGA gesammelt wurden, in seine ePA übermitteln lassen, um diese Daten dort zu persistieren und im Behandlungskontext mit seinen Leistungserbringern zu nutzen. [<=]

**USt-3 - Einsehen der DiGA-Daten im ePA FdV durch den Versicherten**
Der Versicherte möchte die von einer DiGA in die ePA eingestellten Daten in einem ePA-FdV einsehen, um nachzuvollziehen was ein berechtigter Leistungserbringer einsieht. [<=]

**USt-4 - Erstellung einer LE-Berechtigung für DiGA im ePA-FdV**
Der Versicherte möchte die in seiner ePA befindlichen DiGA-Daten für seinen Leistungserbringer über das ePA-FdV freigeben, um ihm die DiGA-Daten zugänglich zu machen. [<=]

**USt-5 - Erstellung einer LE-Berechtigung für DiGA ad-hoc in der Leistungserbringerumgebung**
Der Versicherte möchte die in seiner ePA befindlichen DiGA-Daten für seinen Leistungserbringer während eines Praxisbesuches vor Ort mittels mittelgranularer Ad-hoc-Berechtigung freigeben, um ihm die DiGA-Daten zugänglich zu machen. [<=]

**USt-6 - Einsehen der DiGA-Daten durch einen Leistungserbringer**
Der berechtigte Leistungserbringer möchte DiGA-Daten aus der ePA des Versicherten einsehen, um diese als Sekundärdokumentation im Rahmen einer Behandlung nutzen zu können. [<=]

**USt-7 - Widerruf einer DiGA-Berechtigung am ePA-FdV**
Der Versicherte möchte eine bestehende Berechtigung zur Datenübermittlung aus einer DiGA in die ePA widerrufen, um Daten nicht mehr automatisch oder nur noch manuell aus einer DiGA in die ePA zu übermitteln. [<=]

**USt-8 - Löschung von DiGA-Daten in einer ePA**
Der Versicherte möchte die in seiner ePA gespeicherten DiGA-Daten über das ePA-FdV löschen, um diese Daten zu entfernen. [<=]

# 3 Technisches Konzept

Der DiGA-Hersteller wird mithilfe einer für ihn ausgestellten SMC-B über einen Konnektor an die TI und die ePA angebunden. Die Daten werden in der ePA als Daten des Versicherten aus digitalen Gesundheitsanwendungen (Kategorie 9) behandelt (vgl. § 341 Abs. 2 Nr. 9 SGB V-E): "9. Daten des Versicherten aus digitalen Gesundheitsanwendungen des Versicherten nach § 33a".

## 3.1 Rahmenbedingungen

Alle Hersteller von denen durch das BfArM zugelassenen und zugleich zertifizierten DiGA können eine SMC-B bei der gematik GmbH beantragen. Ein DiGA-Hersteller kann berechtigt werden, für eine zugelassene DiGA, Daten einzustellen. Die Daten selbst können unstrukturiert oder auch als ein von der KBV spezifiziertes sogenanntes Medizinisches Informationsobjekt (MIO) als FHIR-Ressource (DiGA-MIO) definiert worden sein. Für Daten digitaler Gesundheitsanwendungen der Versicherten nach § 33a SGB V definiert die KBV „erstmals bis zum 30.06.2022 die notwendigen Festlegungen für die semantische und syntaktische Interoperabilität" (§ 355 Abs. 2a SGB V-E).

Jeder Hersteller kann für unterschiedliche DiGAs jeweils spezifische DiGA-Daten einstellen. Ein ePA-FdV interagiert mit der DiGA niemals direkt, sodass es keinen Rückkanal vom ePA-FdV zur DiGA gibt.

Die Integration offener standardisierter Schnittstellen von Hilfsmitteln und Implantaten sowie Implementierung der Schnittstellen zum Datenexport aus den DiGAs gemäß §§ 139e, 374a SGB V werden nicht im Rahmen der DiGA-Anbindung von der gematik GmbH festgelegt.

Versicherten ohne ePA-FdV fehlt die Möglichkeit, eine DiGA für einen Aktenzugriff zu berechtigen, und ihnen fehlt die Möglichkeit, DiGA-Daten in der ePA einzusehen. Beide dazugehörigen Use Cases können durch einen Vertreter des Versicherten ohne ePA-FdV ausgeführt werden.

## 3.2 Beschreibung des technischen Konzepts

Es werden ausschließlich bereits in ePA 2.0 vorhandene Komponenten und Prozesse verwendet, vgl. aber Kap. 3.2.2.

Der DiGA-Hersteller ist ein Client, der seine DiGA wie ein Primärsystem mittels Konnektor und SMC-B an die TI anbindet. Die Anforderungslage für Primärsysteme gilt, wenn nicht ausdrücklich anders geregelt auch für DiGA-Clients.

Die Kategorienfreigabe erfolgt aufgrund von § 341 Abs. 2 Nr. 9 SGB V. Zusätzlich dazu ist am ePA-FdV noch eine Vergabe von feingranularen Zugriffsrechten möglich.

Die SMC-B der DiGA des Herstellers beinhaltet im AUT-Zertifikat eine für ihn konzipierte professionOID ("oid_diga"). Die Zugriffsrechte des DiGA-Nutzers auf die ePA werden anhand dieser professionOID eingeschränkt.

### 3.2.1 DiGA-Daten innerhalb der ePA

Die Nutzungsszenarien der DiGA-Daten folgen grob den Nutzungsszenarien der ePA, d.h.

- es gibt eine Datenquelle, die ausschließlich schreibende Zugriffsrechte erhalten kann und
- die Daten werden als Daten der Kategorie 9 verwendet und vom Versicherten verwaltet (§ 341 Abs. 2: „9. Daten des Versicherten aus digitalen Gesundheitsanwendungen des Versicherten nach § 33a,").

Die Zugriffskontrolle auf DiGA-Daten erfolgt entweder mittelgranular als Freigabe auf alle Daten der Kategorie 9 oder aber feingranular, falls dies am ePA-FdV so durch den Versicherten festgelegt wird. Die DiGA-Daten selbst müssen in einem interoperablem Dokumentenformat aus [gemSpec_DM_ePA] vorliegen. Sobald ein DiGA-MIO definiert ist, kann es dynamisch in die ePA integriert werden (bspw. wäre ein Sammlungstyp "DiGA" vorstellbar, von dem es mehrere Instanzen in der Akte geben kann).

Neben der Möglichkeit, dass DiGA strukturierte Daten nutzen, besteht die Möglichkeit der Nutzung unstrukturierter Formate wie PDF.

### 3.2.2 SMC-B Herausgabe für DiGAs

Die gematik GmbH gibt SMC-Bs für DiGAs heraus.

Offener Punkt: Der Typ einer SMC-B für DiGAs ist aktuell vor dem Hintergrund des Kabinettentwurf zum PDSG nicht abschließend festgelegt. Als eine geeignete Ausprägung einer SMC-B kann die SMC-B ORG angesehen werden.

Ein DiGA-Hersteller stellt für jede seiner DiGA einen eigenen Antrag für eine separate SMC-B ORG. Die attributbestätigende Stelle ist das BfArM.

Aus Sicht der ePA wird für die SMC-B für DiGA das Feld `professionOID` im Zertifikatsprofil C.HCI.AUT gesondert festgelegt. Weitere Eigenschaften der SMC-B für DiGA-Hersteller werden nicht über das vorliegende Dokument gesteuert, wie etwa die Signaturzertifikate dieser SMC-B oder der komplette Satz an Zertifikatsprofilelementen.

Anforderungen an die gematik GmbH (z.B. für eine SMC-B ORG geregelt über [gemRL_SMC-B_ORG_AP] und [gemRL_SMC-B_ORG_BP]):

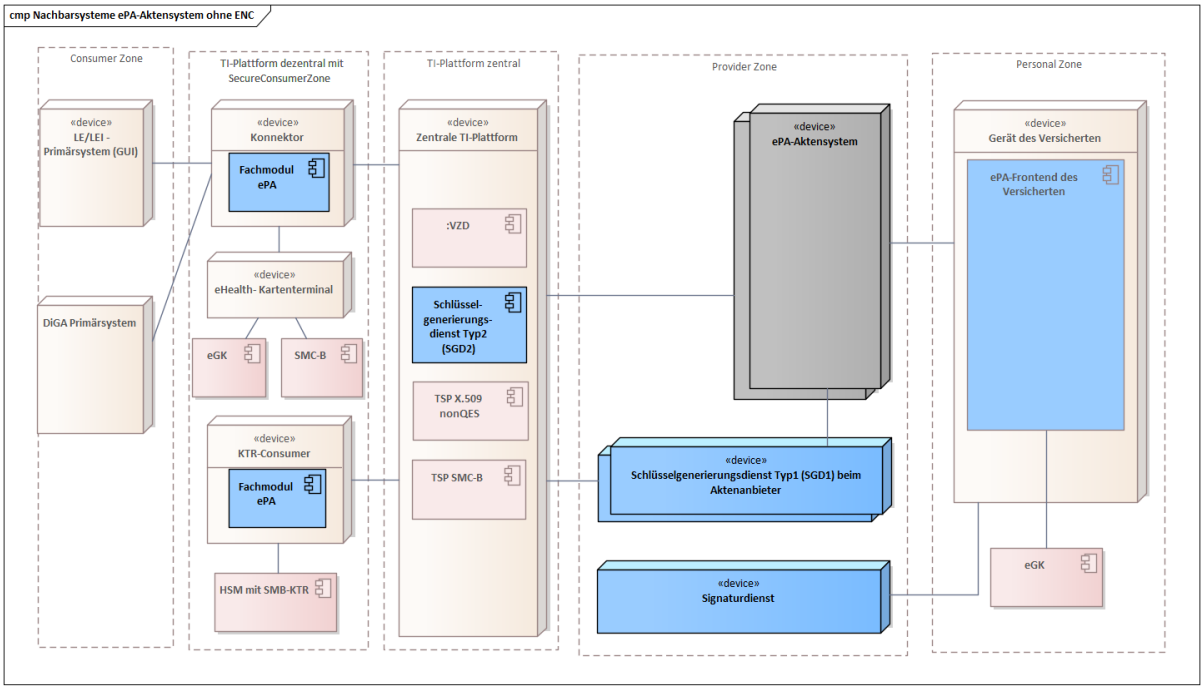
- Der Herausgeber der DiGA-SMC-B MUSS sicherstellen, dass der Antragsteller mit seiner digitalen Gesundheitsanwendung beim BfArM zugelassen und gelistet ist. Die DiGA, für die er den Antrag stellt, wird in die Felder `professionItem`/ `commonName` eingetragen.
- Der Herausgeber der DiGA-SMC-B MUSS sicherstellen, dass der Antragsteller als Hersteller der digitalen Gesundheitsanwendung an geeigneter Stelle erklärt, dass er nur Daten der vom BfArM zugelassenen Gesundheitsanwendung in die ePA einstellen wird.
- Der Herausgeber der DiGA-SMC-B MUSS einen Eintrag im Verzeichnisdienst der TI für die DiGA des Antragstellers erstellen.
  (`entryType= 9 DiGA`), `Admission` / `professionOID=<oid_diga>` gemäß [gemSpec_OID#GS-A_4443] und entsprechend
  `professionItem` / `commonName<Name der DiGA>`, `organizationName<Name des DiGA-Herstellers>`
  und `domainId<PZN der DiGA>`

Im Resultat ist **jede DiGA über eine individuelle Telematik-ID identifizierbar**. Damit der entryType der DiGA "9" ist, wird entsprechend [gemSpec_OID] angepasst, denn der Bezeichner: Eintragstyp wird vom Verzeichnisdienst der TI anhand der im Zertifikat enthaltenen OID (Extension Admission, Attribut ProfessionOID) und der Spalte Eintragstyp
in Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID automatisch eingetragen (siehe auch [gemSpec_OID# Tab_PKI_402 und Tab_PKI_403]).

# 4 Spezifikation

## 4.1 gemSpec_Aktensystem

Abbildung 2 aktualisieren:




## 4.2 Berechtigungsverwaltung

## 4.2.1 gemSpec_Dokumentenverwaltung

**A_19303-04 - Komponente ePA-Dokumentenverwaltung – Zugriffsunterbindungsregeln**
Die Komponente ePA-Dokumentenverwaltung MUSS alle in der Tabelle Tab_Dokv_030 - Zugriffsunterbindungsregeln aufgeführten Zugriffsunterbindungsregeln durchsetzen. Die Komponente ePA-Dokumentenverwaltung MUSS beim Aufruf einer der Operationen der Schnittstelle I_Document_Management die übergebene `AuthenticationAssertion` dahingehend prüfen, ob die `ProfessionOID` der ZertifikatsExtension `Admission` gemäß [gemSpec_PKI#Anhang A] im Signaturzertifikat C.HCI.OSIG (`/saml2:Assertion/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate`) für die Operation, ausgeführt auf eine bestimmte Dokumentenkategorie, zugriffsberechtigt ist. Das Ausführen von Operationen auf Dokumentenkategorien, die nicht explizit erlaubt sind, muss verhindert werden ("Access Deny").

**Tabelle 1: Tab_Dokv_030 - Zugriffsunterbindungsregeln**

| **Dokumentenkategorie gemäß § 341 PDSG Absatz 2** | | **Zugriffsrecht** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Nr. | Technischer Identifier | Arzt | ZArzt | Apo | Psych | Pflege | Heba | Phys | GD | AM | KTR | Ver | DIGA |
| 1a1 | practitioner | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1a2 | hospital | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1a3 | laboratory | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | -- |
| 1a4 | physiotherapy | CR UD | CR UD | R | CR UD | R | R | CR UD | CR UD | R | - | RDM | - |
| 1a5 | psychotherapy | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1a6 | dermatology | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1a7 | gynaecology_urology | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1a8 | dentistry_oms | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1a9 | other_medical | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1a10 | other_non_medical | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1b | emp | CR UD | CR UD | CR UD | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1c | nfd | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 1d | eab | CR UD | CR UD | R | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 2 | dentalrecord | CR UD | CR UD | - | CR UD | R | - | - | CR UD | R | - | RDM | - |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | childsrecord | CR UD | CR UD | R | CR UD | R | CR UD | R | CR UD | R | - | RDM | - |
| 4 | mothersrecord | CR UD | CR UD | R | CR UD | R | CR UD | R | CR UD | R | - | RDM | - |
| 5 | vaccination | CR UD | CR UD | CR UD | CR UD | R | R | - | CR UD | CR UD | - | RDM | - |
| 6 | patientdoc | RD | RD | R | RD | R | R | R | RD | R | - | CRU DM | - |
| 7 | ega | RD | RD | R | RD | R | R | R | RD | R | - | CRU DM | - |
| 8 | receipt | RD | RD | RD | RD | R | R | R | RD | R | C U | RDM | - |
| 9 | diga | R | R | R | R | R | R | R | R | R | - | RDM | CU |
| 10 | care | CR UD | CR UD | R | CR UD | CR UD | R | R | CR UD | R | - | RDM | - |
| 11 | prescription | CR UD | CR UD | CR UD | CR UD | R | R | R | CR UD | R | - | RDM | - |
| 12 | eau | CR UD | CR UD | - | CR UD | - | - | - | CR UD | R | - | RDM | - |
| 13 | other | CR UD | CR UD | - | CR UD | - | - | - | CR UD | R | - | RDM | - |

Legende der Zugriffsrecht CRUD, Zuordnung zur Operation:

- C (create)=I_Document_Management::CrossGatewayDocumentProvide, I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b, I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b;
- R (read)=I_Document_Management::CrossGatewayQuery, I_Document_Management::CrossGatewayRetrieve, I_Document_Management_Insurant::CrossGatewayQuery, I_Document_Management_Insurant::CrossGatewayRetrieve;
- U (update)=Document Replacement (über `urn:ihe:iti:2007:AssociationType:RPLC`) via Operationen I_Document_Management::CrossGatewayDocumentProvide, I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b, I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b;
- D (delete)=I_Document_Management::RemoveMetadata, I_Document_Management::RemoveDocuments, I_Document_Management_Insurant::RemoveMetadata;

- M (metadata update)=I_Document_Management_Insurant::RestrictedUpdateDocumentSet;
- "-" = keine Zugriffsrechte;

Legende der Institutionen, Zuordnung zur `ProfessionOID`:

- Arzt=oid_praxis_arzt, oid_krankenhaus, oid_institution-vorsorge-reha, oid_sanitaetsdienst-bundeswehr;
- ZArzt=oid_zahnarztpraxis;
- Apo=oid_öffentliche_apotheke;
- Psych=oid_praxis_psychotherapeut;
- Pflege=oid_institution-pflege;
- Heba=oid_institution-geburtshilfe;
- Phys=oid_praxis-physiotherapeut;
- GD=oid_institution-oegd;
- AM=oid_institution-arbeitsmedizin;
- KTR=oid_epa_ktr;
- DIGA=oid_diga

Legende Zugriffsberechtigte, Zuordnung über KVNR:

- Ver=Versicherter/Vertreter;

**[<=]**

**A_21512 - Komponente ePA-Dokumentenverwaltung – dynamisches Anlegen von DIGA-Ordnern**

Die Komponente ePA-Dokumentenverwaltung MUSS beim erstmaligen Einstellen eines Dokumentes in die Akte des Versicherten (`Operation I_Document_Management::CrossGatewayDocumentProvide()`) durch eine bestimmte DiGA, die als solche über die professionOID gekennzeichnet ist, den folgenden Ordner für den Versicherten anlegen:

- DiGA-Ordner der Kategorie 9 gemäß gemSpec_DM_ePA#A_20190 (Belegung `Folder.code`) unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in gemSpec_DM_ePA#14760 (Belegung der restlichen Metadatenfelder). Der Request muss eine FolderUniqueID enthalten, die für jede DiGA mit ihrer Telematik-ID in einer eins-zu-eins-Relation stehen muss.

**[<=]**

Neue AFO: Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass auf DiGA-Daten nur eine kategorienbasierte Freigabe erfolgen kann.

**A_22619 - Komponente ePA-Dokumentenverwaltung - Prüfung der Folder-Zuordnung**

Die Komponente ePA-Dokumentenverwaltung MUSS beim Einstellen eines DiGA-Dokumentes in die Akte des Versicherten (Operation I_Document_Management::CrossGatewayDocumentProvide()) sicherstellen, dass die im Request enhaltene Identität des authentifizierten Nutzers (TelematikID) identisch ist zu submissionSet.author.authorInstitution, welches dem Folder bereits zugeordnet ist. Andernfalls MUSS die Komponente ePA-Dokumentenverwaltung den Request mit einem XDSRepositoryMetadataError ablehnen.**[<=]**

**Todo:**

- Erweitern des policy-Dokuments \epa\src\policies\hci-policy-definition.xml um Kategorie diga
- Erstellen eines policy-Dokuments für Digas, analog zu GIT\epa\src\policies\insurance-policy-definition.xml

### 4.2.1.1 neues Kapitel 5.4.2.5 Berechtigung für eine DiGA

**A_22705 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Document zur Berechtigung einer DiGA**
Die Komponente ePA-Dokumentenverwaltung MUSS ein vom ePA-Frontend des Versicherten übermitteltes Policy Document gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in der Policy Definition in [gemSpec_ePA_Policy_DiGA] prüfen.**[**<=**]**

## 4.2.2 gemSpec_DM_ePA

**A_19388-03 - Nutzungsvorgaben für die Verwendung von Dokumentenkategorien**
Das Primärsystem, das ePA-Frontend des Versicherten, die Dokumentenverwaltung sowie das Fachmodul ePA KTR-Consumer MÜSSEN im Kontext der Berechtigungserteilung und der autorisierten Nutzung von ePA-Dokumenten die nachstehenden Nutzungsvorgaben für Dokumentenkategorien berücksichtigen.

**Tabelle 2: Tab_DM_Dokumentenkategorien**

| Nr | Dokumentenkategorie | technischer Identifier | Metadatenvorgaben |
|---|---|---|---|
| 1a 1 | Hausarzt/ Hausärztin | practitioner | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `practitioner` gemäß A_20190-01 enthält. |
| 1a2 | Krankenhaus | hospital | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `hospital` gemäß A_20190-01 enthält. |
| 1a3 | Labor und Humangenetik | laboratory | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `laboratory` gemäß A_20190-01 enthält. |
| 1a4 | Physiotherapeut | physiotherapy | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `physiotherapy` gemäß A_20190-01 enthält. |

| | | | |
|---|---|---|---|
| 1a5 | Psychotherapeut | psychotherapy | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `psychotherapy` gemäß A_20190-01 enthält. |
| 1a6 | Dermatologie | dermatology | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `dermatology` gemäß A_20190-01 enthält. |
| 1a7 | Urologie/Gynäkologie | gynaecology_urology | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `gynaecology_urology` gemäß A_20190-01 enthält. |
| 1a8 | Zahnheilkunde und Mund-Kiefer-Gesichtschirurgie | dentistry_oms | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `dentistry_oms` gemäß A_20190-01 enthält. |
| 1a9 | Weitere Fachärzte/ Fachärztinnen | other_medical | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `other_medical` gemäß A_20190-01 enthält. |
| 1a10 | Weitere nicht-ärztliche Berufe | other_non_medical | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code `other_non_medical` gemäß A_20190-01 enthält. |
| 1b | Medikationsplan | emp | DocumentEntry.formatCode="urn:gematik:ig: Medikationsplan:r3.1" |
| 1c | Notfalldaten | nfd | DocumentEntry.formatCode="urn:gematik:ig: Notfalldatensatz:r3.1" oder DocumentEntry.formatCode="urn:gematik:ig: DatensatzPersoenliche Erklaerungen:r3.1" |
| 1d | eArztbrief | eab | DocumentEntry.formatCode="urn:gematik:ig: Arztbrief:r3.1" |
| 2 | Zahnbonusheft | dentalrecord | DocumentEntry.formatCode="urn:gematik:ig: Zahnbonusheft:r4.0" |
| 3 | Kinderuntersuchungsheft | childsrecord | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code gemäß A_20577-01 enthält. |

| | | | |
|---|---|---|---|
| 4 | Mutterpass | mothersrecord | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code gemäß A_20577-01 enthält. |
| 5 | Impfpass | vaccination | DocumentEntry.formatCode="urn:gematik:ig:Impfausweis:r4.0" |
| 6 | Vom Versicherten eingestellte Daten | patientdoc | submissionset.authorRole = "102" |
| 7 | eGA -Daten | ega | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code eGA gemäß A_20190-01 enthält. |
| 8 | Quittungen (auch receipt genannt) | receipt | DocumentEntry.healthcareFacilityTypeCode="VER" und DocumentEntry.typeCode="ABRE" |
| 9 | Digitale Gesundheitsanwendung | diga | Dokument muss in einem Ordner sein, bei dem Folder.codeList den Code diga gemäß A_20190* enthält. |
| 10 | Pflegedokumente | care | DocumentEntry.practiceSettingCode = "PFL" |
| 11 | Rezept | prescription | DocumentEntry.formatCode="urn:gematik:ig:VerordnungsdatensatzMedikation:r4.0" |
| 12 | Arbeitsunfähigkeitsbescheinigung | eau | DocumentEntry.formatCode="urn:gematik:ig:Arbeitsunfähigkeitsbescheinigung:r4.0" |
| 13 | Sonstige von der LEI bereitgestellte (nicht medizinische) Dokumente | other | ( (XDSDocumentEntry.practiceSettingCode stammt aus dem Code-System "1.3.6.1.4.1.19376.3.276.1.5.4" (Ärztliche Fachrichtungen) UND typeCode = SCHR oder PATI oder ABRE |

Legende:

- Kategorie Nr. 1a*=Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, zu Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen;

- Kategorie Nr. 7, "eGA-Daten"=Daten der Versicherten aus einer von den Krankenkassen nach § 68 finanzierten elektronischen Akte der Versicherten;
- Kategorie Nr. 8, Quittungen (Patientenquittung)=bei den Krankenkassen gespeicherte Daten über die in Anspruch genommenen Leistungen der Versicherten;
- Kategorie Nr. 11, Rezept (elektronische Verordnungen)=Daten elektronischer Verordnungen/Verordnungsdatensatz nach § 360 Abs. 1

**[<=]**

**Todo:**

**in GIT\epa\src\vocabulary\value_sets\vs-specialty-oth.xml:**

Aufnahme in die extensionale Aufzählung enthaltener Codes:

- Code=diga,
- CodeSystem=1.2.276.0.76.5.512,
- Anzeigename="DiGA Toolkit",
- Beschreibung= "Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass) sowie Daten, die sich aus der Versorgung der Versicherten mit Hebammenhilfe ergeben."

### 4.2.3 gemSpec_FM_ePA

Für ePA 2.5 wird für den Konnektor der Produkttyp PTV5.5 eingeführt.

Beim LE kann nur eine mittelgranulare Kategorienfreigabe erfolgen, keine feingranulare Freigabe und keine Freigabe für Daten einzelner DiGA. Mittelgranular wird die Kategorie "diga" im Falle der Freigabe in der AuthorizationConfiguration.DocumentCategoryList vom Primärsystem übergeben.

A_16212-07 (neu: A_16212-08), Tab_FM_ePA_042 - Mapping von DocumentCategoryEnum auf Anzeigetext am Kartenterminal: Aufnahme der Kategorie "diga" (DocumentCategoryEnum) = "Digitale•Gesundheitsanwendung" (Anzeigetext am Kartenterminal) in die Liste der Kategorien.

Ein PTV5.5 Konnektor muss nicht den Migrationspfad zu ePA 1 abdecken. Deshalb entfällt das Interface PHRService1.x und PHRManagementService 1.x entfällt in PTV5.5

Folgende Anforderungen werden durch eine Suffix-Afo angepasst:

- A_13828 -> A_13828-01
- A_15142 -> A_15142-01

Folgende Anforderungen entfallen:

- A_20090
- A_16212-03

Todo in GIT - Erweiterung von DocumentCategoryEnum um Wert "diga":

- api-telematik\conn\phrs\PHRManagementService_V2_5_0.xsdm

- api-telematik\conn\phrs\PHRManagementService_V2_5_0.wsdl

**A_22702 - FM ePA: PHRManagementService Version 2.5.0**
Das Fachmodul ePA MUSS für Primärsysteme den Webservice PHRManagementService Version 2.5.0 gemäß Tabelle Tab_FM_ePA_061 anbieten.

**Tabelle 3: Tab_FM_ePA_061 Beschreibung des Webservices PHRManagementService**

| | | |
|---|---|---|
| Name | PHRManagementService | |
| **Version** | 2.5.0 | |
| **Namensraum** | http://ws.gematik.de/conn/phrs/PHRManagementService/WSDL/v2.5 | |
| **Abkürzung Namensraum** | phr_management | |
| **Operationen** | **Name** | **Beschreibung** |
| | ActivateAccount | Aktivierung eines Aktenkontos |
| | RequestFacilityAuthorization | Berechtigungsvergabe für eine LEI (kategoriebasierte Berechtigungserteilung) |
| | GetHomeCommunityID | Identifizierung eines ePA-Aktensystems |
| | GetAuthorizationList | Abruf aller Berechtigungen einer LEI |
| | GetAuthorizationState | Abruf aller Berechtigungen für ein Aktenkonto |
| **WSDL** | **PHRManagementService_V2_5_0.wsdl** | |

Der Dienst wird vom Fachmodul ePA im Dienstverzeichnis des Konnektors registriert und damit für Primärsysteme auffindbar gemacht (siehe Kapitel 6.8 Verwendung des Dienstverzeichnisdienstes).**[<=]**

**A_22703 - FM ePA: RequestFacilityAuthorization Version 2.5 - Anzeige am Kartenterminal - Anzeigetext**
Im Rahmen der Abfrage der PIN.CH zur Erteilung der Berechtigung MUSS die Operation RequestFacilityAuthorization Version 2.5 unmittelbar vor der PIN-Abfrage die Anzeigetexte in der vorgegebenen Reihenfolge gemäß Tab_FM_ePA_060 am Kartenterminal darstellen.

**Tabelle 4: Tab_FM_ePA_060: Operation RequestFacilityAuthorization Version 2.5 - Ausgabetexte am Kartenterminal**

| Ausgabe am Kartenterminal | Quelle | Verfügbare Länge für Parameter | Rubrik |
|---|---|---|---|
| Es•folgen•4•Anzeigen.<br>•***0x0B***<br>Bitte•mit•OK•bestätigen | - | - | Dialogstart |
| 1:Berechtigung•für•***0x0B***<br><OrganizationName> | Parameter OrganizationName* | 27 | Basisanzeige |
| 2:auf•Akte•von•***0x0B***<br><Vorname>•<Nachname> | Parameter InsurantName*<br>Wenn die Länge <Vorname> + Länge <Nachname> größer ist als 30 Zeichen, dann wird der Vorname nach 9 Zeichen abgeschnitten und mit '.' beendet. | 30 | |
| 3:mit•Ende•der•Berechtigung:•***0x0B***<br><ExpirationDate> | Parameter ExpirationDate als tt.mm.jjjj | 10 | |
| 4:<AuthorizationConfidentiality>•Zugriff | Parameter AuthorizationConfiguration.AuthorizationConfidentiality<br>Anzeige: erweiterter, wenn Wert "extended"<br>Anzeige: einfacher, wenn Wert "normal"<br>(Anzeige der Vertraulichkeitsstufe:<br>einfach bedeutet Zugriff auf Dokumente mit Vertraulichkeitsstufe "normal"<br>erweitert bedeutet Zugriff auf Dokumente mit Vertraulichkeitsstufe "normal" und "vertraulich") | nicht relevant | |

| | | | |
|---|---|---|---|
| Details•zu•<number>•***0x0B***Kategorien?•***0x0B***Ja=1,•Nein=2 | <number> entspricht der Anzahl der in AuthorizationConfiguration.DocumentCategoryList übergebenen Dokumentenkategorien als Dezimalzahl.<br>Das Kartenterminal erwartet die Eingabe folgender Zeichen:<br>"1" : Dialog wird mit Details zu Dokumentenkategorien fortgesetzt.<br>oder<br>"2": Dialog wird ohne Details zu Dokumentenkategorien fortgesetzt. | 2 | Detailabfrage |
| Zugriff•auf•folgende•***0x0B***•Kategorien•erlaubt: | - | - | Kategorieanzeige |
| Bitte•mit•OK•bestätigen | - | - | |
| *Es folgt eine Auflistung der Dokumentenkategorien aus Parameter* DocumentCategoryList. *Zur Anzeige wird ein Mapping der übertragenen Enumerated Werte gemäß Tab_FM_ePA_042 durchgeführt.*<br>*Bei der Auflistung der Dokumentenkategorien muss das Display des angeschlossenen Kartenterminals für z.B. 5 Zeilen zur Anzeige zur Verfügung stehen, dann ist jede Zeile für die Anzeige zu nutzen.*<br>*Ziel ist, dass der Versicherte ein Minimum an erforderlichen Bestätigungen durch Drücken der Taste "OK" durchführen muss.* | Parameter AuthorizationConfiguration.DocumentCategoryList (Anzeige der Dokumentkategorien) | max. 48 Zeichen pro Zeile (weniger bei panning) | |

Hinweise:
1. Die Inhalte der mit '*' markierten Parameter werden auf die maximal mögliche Anzahl der verbleibenden Zeichen für den Eingabetext gekürzt. Nicht genutzte Zeichen werden

nicht zur Anzeige gebracht.
2. Leerzeichen werden als "•" dargestellt
3. 0x0B und 0x0F (Sollbruchstellen bzw. Trennung zwischen Nachricht und PIN-Prompt) sind Trennzeichen gemäß [SICCT#5.6.1]
4. Die Zeilenumbrüche in der Spalte "Ausgabe am Kartenterminal" sind editorisch bedingt.

**Tabelle 5 : Tab_FM_ePA_042 - Mapping von DocumentCategoryEnum auf Anzeigetext am Kartenterminal**

| DocumentCategoryEnum | Anzeigetext am Kartenterminal |
|---|---|
| practitioner | Dokumente•von•**0x0B**Hausärzt:innen |
| hospital | Dokumente•aus•**0x0B**Krankenhaus |
| laboratory | Dokumente•aus•**0x0B**Labor,Humangenetik |
| physiotherapy | Dokumente•aus•**0x0B**Physiotherapie |
| psychotherapy | Dokumente•aus•**0x0B**Psychotherapie |
| dermatology | Dokumente•aus•**0x0B**Dermatologie |
| gynaecology_urology | Dokumente•aus•**0x0B**Urologie,Gynäkologie |
| dentistry_oms | Dokumente•aus•**0x0B**Zahnheilkunde,MKG |
| other_medical | Dokumente•von•**0x0B**weiteren•**0x0B**Fachärzt:innen |
| other_non_medical | Dokumente•aus•**0x0B**weiteren•**0x0B**nicht-ärztl.•**0x0B**Berufen |
| emp | Medikationsplan |
| nfd | Notfalldaten |
| eab | Arztbriefe |
| dentalrecord | Zahnbonusheft |
| childsrecord | U-Hefte |
| mothersrecord | Dokumente•von•**0x0B**Schwangerschaft,Geburt |
| vaccination | Impfdokumentation |
| patientdoc | Von•mir•**0x0B**eingestellte•**0x0B**Daten |
| ega | eGA-Daten |

| | |
|---|---|
| receipt | Quittungen |
| care | Pflegedokumente |
| diga | Digitale•Gesundheitsanwendung |
| prescription | Verordnungen |
| eau | Arbeitsunfähigkeit |
| other | Sonstige•Dokumente |

**[<=]**

## 4.2.4 gemSpec_Zugangsgateway_Vers

Änderung in A_17748-01 (neu: A_17748-02):

...

- Es MUSS sichergestellt sein, dass ausschließlich Einträge des Verzeichnisdienstes mit Eintragstyp nach [gemSpec_VZD#Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID] == 3 oder 6 oder 9 zurückgegeben werden.

**A_17748-02 - Zugangsgateway des Versicherten, Schnittstelle I_Proxy_Directory_Query, Beschränkung auf ePA relevante Informationen**
Der LDAP-Proxy der Komponente Zugangsgateway des Versicherten MUSS sicherstellen, dass ein anfragendes ePA-Modul Frontend des Versicherten (ePA-Modul FdV) ausschließlich die Informationen des Verzeichnisdienstes erhält, welche für die Erfüllung der Aufgaben benötigt werden. Folgende Vorgaben MÜSSEN eingehalten werden:

- Der LDAP-Proxy DARF NICHT Fachdaten an das anfragende ePA-Modul Frontend des Versicherten (ePA-Modul FdV) zurückgegeben.
- Es MUSS sichergestellt sein, dass ausschließlich Einträge des Verzeichnisdienstes mit Eintragstyp nach [gemSpec_VZD#Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID] == 3 oder 6 oder 9 zurückgegeben werden.

**[<=]**

## 4.2.5 gemSpec_VZD

Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID, Hinzufügen der Reihe:

Eintragstyp=9, Eintragstyp Bedeutung=Digitale Gesundheitsanwendung, ProfessionOID (ProfessionItem)=beantragte OID

## 4.2.6 gemSpec_OID

GS-A_4445-03 referenziert Tab_PKI_405-02 OID-Festlegung Zertifikatstyp in X.509-Zertifikaten.

Tab_PKI_405-02 OID-Festlegung Zertifikatstyp in X.509-Zertifikaten wird erweitert um oid_diga.

## 4.2.7 gemSpec_ePA_FdV

Daten digitaler Gesundheitsanwendungen auslesen

**A_21703 - ePA-Frontend des Versicherten: Daten digitaler Gesundheitsanwendungen auslesen**
~~Das ePA-Frontend des Versicherten MUSS DiGA-Daten bei vorliegender Berechtigung aus dem ePA-Aktensystem des Versicherten auslesen und anzeigen können.~~ **[<=]**

### 4.2.7.1 In Kapitel 5.3.1 Policy Document

...

Für jeden Versicherten, Vertreter, jede berechtigte Leistungserbringerinstitution (LEI), den berechtigten Kostenträger (KTR), die berechtigte DiGA und den Aktenkontoinhaber wird je ein Policy Document im Aktenkonto verwaltet.

Bei der Neuvergabe einer Berechtigung für Vertreter, LEI, DiGA oder KTR erstellt das ePA-Frontend des Versicherten ein neues Policy Document und lädt es in das Aktenkonto hoch.

...

### 4.2.7.2 in Kapitel 6.1.5 Zertifikatsprüfung

Das ePA-Frontend des Versicherten  verwendet bei den in TAB_FdV_110 dargestellten Aktivitäten Zertifikate.

**Tabelle 6: TAB_FdV_110 – Zertifikatsnutzung**

| Aktivität | Zertifikat der TI | Zertifikatstyp | Rollen-OID | Nutzung |
|---|---|---|---|---|
| Einlesen der eGK | ja | C.CH.AUT | oid_egk_aut | passiv |
| TLS-Verbindungsaufbau zum Zugangsgateway des Versicherten | nein | TLS Internet Zertifikat | n/a | aktiv |

| | | | | |
|---|---|---|---|---|
| Authentisierung | ja | C.CH.AUT<br>C.CH.AUT_ALT | oid_egk_aut<br>oid_egk_aut_alt | passiv |
| Aufbau sicherer Kanal zur VAU | ja | C.FD.AUT | oid_epa_vau | aktiv |
| Berechtigung von LEI, DiGA oder KTR erteilen Berechtigung von LEI ändern | ja | C.HCI.ENC | oid_smc_b_enc | aktiv |
| Verbindungsaufbau SGD | ja | C.SGD-HSM.AUT | oid_sgd1_hsm<br>oid_sgd2_hsm | aktiv |

### 4.2.7.3 in Kapitel 6.2.3.4 Dokumentenset aus Dokumentenverwaltung herunterladen

**A_15317-02 - ePA-Frontend des Versicherten: Dokumentenset aus Dokumentenverwaltung herunterladen**

Das ePA-Frontend des Versicherten MUSS die Aktivität "Dokumentenset aus Dokumentenverwaltung herunterladen" gemäß TAB_FdV_112 umsetzen.

**Tabelle 7: TAB_FdV_112 – Dokumentenset aus Dokumentenverwaltung herunterladen**

| | |
|---|---|
| `I_Document_Management_Insurant::RetrieveDocumentSet`<br>Request erstellen | Eingangsparameter:<br>• `RetrieveDocumentSet_Message` gemäß IHE XDS-Transaktion [ITI-43]<br>• `AuthenticationAssertion` aus Session-Daten |
| `I_Document_Management_Insurant::RetrieveDocumentSet`<br>Response verarbeiten | Rückgabedaten:<br>• RetrieveDocumentSetResponse_Message gemäß IHE XDS-Transaktion [ITI-43]<br>RetrieveDocumentSetResponse_Message beinhaltet ein oder mehrere Dokumente. Jedes medizinisches Dokument ist mit einem individuellen Dokumentenschlüssel verschlüsselt. Der Dokumentenschlüssel ist mit dem Aktenschlüssel verschlüsselt. |

| | |
|---|---|
| für jedes medizinische Dokument aus RetrieveDocumentSetResponse_Message:<br>Plattformbaustein PL_TUC_SYMM_DECIPHER nutzen<br><br>Hinweis: Der Begriff "medizinische Dokumente" umfasst alle Dokumente, welche durch LEI, KTR, DiGA oder Versicherte in das ePA-Aktensystem eingestellt wurden. Davon abgegrenzt werden die technischen Dokumente (Policy Documents). Sie werden unverschlüsselt übertragen. | Für Vorgaben zum Entschlüsseln eines Dokumentes aus dem ePA-Aktensystem siehe [gemSpec_DM_ePA#2.4.2 Entschlüsselung].<br><br>Dokumentenschlüssel mit PL_TUC_SYMM_DECIPHER entschlüsseln<br>Eingangsdaten:<br>• verschlüsselter Dokumentenschlüssel aus EncryptedData\EncryptedKey\CipherData<br>• Aktenschlüssel (`RecordKey`) aus Session-Daten<br>• Der optionale Parameter AD wird nicht verwendet.<br>Rückgabedaten:<br>• entschlüsselter Dokumentenschlüssel<br><br>Dokument mit PL_TUC_SYMM_DECIPHER entschlüsseln<br>Eingangsdaten:<br>• verschlüsseltes Dokument aus EncryptedData\CipherData<br>• entschlüsselter Dokumentenschlüssel<br>• Der optionale Parameter AD wird nicht verwendet.<br>Rückgabedaten:<br>• entschlüsseltes Dokument |

**[<=]**

### 4.2.7.4 Kapitel 6.2.7.1.1 kategorienbasierte Berechtigung

Bei der kategorienbasierten Berechtigung wird der Zugriff auf die vorhandenen Dokumente der elektronischen Patientenakte in Dokumentenkategorien organisiert. Diese sind in der Spezifikation gemSpec_DM_ePA aufgeführt. Die Zuordnung eines einzelnen Dokumentes zu einer einzelnen Dokumentenart legt (mit Ausnahme der Dokumentenarten **Dokumente des Versicherten,** der **Kostenträgerdokumente** und **Dokumente einer DiGA**) die ePA-Dokumentenverwaltung fest. Alle Dokumente, die der Versicherte selbst einstellt, sind immer der Kategorie **Dokumente des Versicherten** zugeordnet. Eine DiGA kann ausschließlich DiGA-Dokumente einstellen. Ein Kostenträger kann ausschließlich Kostenträgerdokumente einstellen.

Der Versicherte kann über das ePA-Frontend des Versicherten einer einzelnen Leistungserbringerinstitution den Zugriff auf einzelne **Dokumentenkategorien** erteilen oder entziehen.

### 4.2.7.5 Kapitel 6.2.7.1.2 dokumentenspezifische Berechtigung

**A_22685 - ePA_Frontend des Versicherten: Abbilden eines entzogenen Zugriffs für DiGAs in dem Policy Document**

~~Das ePA-Frontend des Versicherten MUSS einen Blacklist-Eintrag mit dem Folder.entryUUID (eines Folders mit zugehörigem Code "diga" in Folder.codeList) in der Blacklist-Policy des Policy Document der LEI erstellen, wenn der Nutzer dieser LEI den Zugriff auf ein konkretes DiGA-Dokument oder eine konkrete DiGA entziehen möchte.~~ **[<=]**

### 4.2.7.6 Neues Kapitel nach 6.2.7.4 Vergebene Berechtigungen anzeigen

**A_15403-05 - ePA-Frontend des Versicherten: Ergebnisliste Berechtigungen Felder**

Das ePA-Frontend des Versicherten MUSS im Ergebnis der Suche nach Berechtigungen mindestens

- Name der Leistungserbringerinstitution, des Kostenträgers bzw. des Vertreters im Klartext,
- für LEI: Zugriffsrecht gemäß grobgranularer Berechtigung (normal vs. erweitert)
- für LEI: Berechtigte Kategorien gemäß mittelgranularer Berechtigung
- für LEI: Explizit erlaubte oder geblockte Dokumente gemäß feingranularer Berechtigung
- für LEI: eingestellte und verbleibende Berechtigungsdauer
- für Vertreter: Anzeige der E-Mail-Adresse der berechtigten Vertreter (Nur für den Fall, dass der Aufrufende der Versicherte ist. Bei Aufruf durch Vertreter erfolgt die Ausgabe der E-Mail-Adresse der Vertreter nicht.)
- für DiGA: PZN der DiGA, Name des DiGA-Herstellers und Name der DiGA

anzeigen.
**[<=]**

### 4.2.7.7 Neues Kapitel nach 6.2.7.6: Berechtigungen für DiGA vergeben

Mit diesem Anwendungsfall richtet ein Versicherter oder ein berechtigter Vertreter Zugriffsberechtigungen auf das Aktenkonto für jede einzelne DiGA ein. Die Zugriffrechte einer DiGA sind auf das Einstellen und Aktualisieren von Dokumenten beschränkt.

**A_21491 - ePA-Frontend des Versicherten: DiGA im Verzeichnisdienst der TI finden**

Das ePA-Frontend des Versicherten MUSS es dem Nutzer mittels der Aktivität "Suchanfrage Verzeichnisdienst der TI" ermöglichen, eine DiGA im Verzeichnisdienst zu suchen und für die Vergabe von Berechtigungen auszuwählen.**[<=]**

Hinweis:

Für die Suche ist mindestens das Kriterium (`entryType`= 9 DiGA) (ePA DiGA-Zugriffsautorisierung, siehe [gemSpec_VZD#5]), zu verwenden. Das Ergebnis kann eine Liste von Apps unterschiedlicher Hersteller sein, aus welcher der Versicherte diejenige DiGA auswählt, die er berechtigen möchte. Eine genauere Eingrenzung der Suchergebnisse kann am FdV über domainId (PZN), organizationName (Name des DiGA-Herstellers) und commonName (Name der DiGA) erfolgen.

Das Verschlüsselungszertifikat im Ergebnis der Abfrage beinhaltet die Telematik-ID des zu berechtigenden DiGA-Herstellers und den Namen der DiGA.

**A_21492 - ePA-Frontend des Versicherten: Bestätigung der Berechtigung für eine DiGA**
Das ePA-Frontend des Versicherten MUSS, bevor es eine Berechtigung an eine DiGA vergibt, eine Bestätigung vom Nutzer einholen. Hierbei ist der Name der zu berechtigenden DiGA kenntlich zu machen.**[<=]**

Hinweis: Der Name der DiGA entspricht dem displayName aus [gemSpec_VZD#Tabelle 29].

**A_21493 - ePA-Frontend des Versicherten: Berechtigung für eine DiGA für ein Aktensystemkonto vergeben**
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.1 - Berechtigung durch einen Versicherten vergeben" aus [gemSysL_ePA] für die DiGA, für die eine Berechtigung vergeben werden soll, gemäß TAB_FdV_181 umsetzen.

**Tabelle 8: TAB_FdV_181 – Berechtigung an DiGA für Aktenkonto vergeben**

| | |
|---|---|
| Name | Berechtigung an DiGA für Aktenkonto vergeben |
| Auslöser | Aufruf des Anwendungsfalls in der GUI |
| Akteur | Versicherter oder berechtigter Vertreter |
| Vorbedingung | Es besteht eine Aktensession mit gültigen Session-Daten.<br>Ein Verschlüsselungszertifikat, die Telemantik-ID des DiGA-Herstellers und der Name der DiGA sind bekannt.<br>Der Nutzer hat die Vergabe der Berechtigung bestätigt. |
| Nachbedingung | Die DiGA ist zum Zugriff auf das Aktenkonto berechtigt.<br>Das notwendige Schlüsselmaterial ist in der Autorisierung hinterlegt.<br>Ein Policy Document für die DiGA ist in der Dokumentenverwaltung hinterlegt. |
| Standardablauf | Aktivitäten im Standardablauf<br>1. AuthorizationKey für DiGA erstellen<br>2. Schlüsselmaterial im ePA-Aktensystem speichern<br>3. Policy Document für DiGA erstellen<br>4. Policy Document in Dokumentenverwaltung laden |

**[<=]**

**A_21494 - ePA-Frontend des Versicherten: Berechtigung DiGA vergeben - AuthorizationKey erstellen**
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an DiGA für Aktenkonto vergeben" einen AuthorizationKey mit `AuthorizationType` = DOCUMENT_AUTHORIZATION für die zu berechtigende DiGA erstellen.**[<=]**

**A_21495 - ePA-Frontend des Versicherten: Berechtigung DiGA vergeben - Schlüsselmaterial im ePA-Aktensystem speichern**

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an DiGA für Aktenkonto vergeben" für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey` = erstellter AuthorizationKey ausführen. Der optionale Parameter `NotificationInfoRepresentative` wird nicht belegt.**[<=]**

**A_21496 - ePA-Frontend des Versicherten: Berechtigung DiGA vergeben - Policy Document erstellen**
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an DiGA für Aktenkonto vergeben" ein Policy Document für die zu berechtigende DiGA erstellen.**[<=]**

**A_21497 - ePA-Frontend des Versicherten: Berechtigung DiGA vergeben - Policy Document hochladen**
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an DiGA für Aktenkonto vergeben" zum Hochladen des Policy Documents in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für Policy Documents ausführen.**[<=]**

## 4.2.7.8 Neues Kapitel nach 6.2.7.6.4: Berechtigung für DiGA löschen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter der DiGA die Berechtigung auf die elektronische Patientenakte entziehen.

**A_21499 - ePA-Frontend des Versicherten: DiGA zum Entzug der Berechtigung markieren**
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, berechtigte DiGAs für den Entzug der Berechtigung auszuwählen.**[<=]**

Hinweis:
Die zum Zugriff auf das Aktenkonto berechtigten DIGA werden mit der übergreifende Aktivität "Vergebene Berechtigungen bestimmen" ermittelt.

**A_21500 - ePA-Frontend des Versicherten: Berechtigung für DiGA löschen**
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" aus [gemSysL_ePA] für die DiGA, deren Berechtigung entzogen werden soll, gemäß TAB_FdV_190 umsetzen.

**Tabelle 9: TAB_FdV_190 – Berechtigung für DiGA löschen**

| | |
|---|---|
| Name | Berechtigung für DiGA löschen |
| Auslöser | Aufruf der Aktion zum Löschen der Berechtigung in der GUI |
| Akteur | Versicherter oder berechtigter Vertreter |
| Vorbedingung | Es besteht eine Aktensession mit gültigen Session-Daten.<br>Der Nutzer hat eine DiGA zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt.<br>Das Policy Document und Informationen zum AuthorizationKey der DiGA stehen zur Verfügung. |

| | |
|---|---|
| Nachbedingung | Die DiGA ist nicht mehr für den Zugriff auf das Aktenkonto autorisiert. |
| Standardablauf | Aktivitäten im Standardablauf<br>1. Policy Document in Dokumentenverwaltung löschen<br>2. Schlüsselmaterial in ePA-Aktensystem löschen |

**[<=]**

**A_21501 - ePA-Frontend des Versicherten: Berechtigung für DiGA löschen - Policy Document in Dokumentenverwaltung löschen**
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für DiGA löschen" für das Löschen des Policy Document in der Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung löschen" mit einer RemoveMetadata_Message für den über die XDS-Metadaten ermittelten Dokument Identifier des Policy Documents der DiGA ausführen.**[<=]**

Hinweis:
Die Telematik-ID der DiGA kann aus dem Policy Document bestimmt werden.

**A_21502 - ePA-Frontend des Versicherten: Berechtigung für DiGA löschen - Schlüsselmaterial in ePA-Aktensystem löschen**
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für DiGA löschen" für das Löschen des Schlüsselmaterials die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem löschen" mit dem Eingangsparameter`ActorID` = Telematik-ID der DiGA ausführen.**[<=]**

## 4.2.7.9 Kapitel 6.2.3.6 Suche nach Dokumenten in Dokumentenverwaltung

**Hinweistext nach der AFO A_15321:**

Als Ergebnis liegen, falls Berechtigungen erteilt wurden, ein oder mehrere AuthorizationKeys sowie Policy Documents für berechtigte LEI, KTR,DiGA und für Vertreter vor.

## 4.2.7.10 Kapitel 6.2.3.7 Vergebene Berechtigung bestimmen

...

Das Ergebnis der Suchanfrage query:AdhocQueryResponse_Message liefert, falls Berechtigungen erteilt wurden, die XDS-Metadaten von einem oder mehreren Policy Documents (je ein Policy Document pro LEI, KTR, DiGA bzw. Vertreter). Die XDS-Metadaten beinhalten die eindeutigen Kennungen (`DocumentEntry.uniqueId`) der Policy Documents. Mittels dieser werden die Policy Documents im nächsten Schritt aus der Dokumentenverwaltung heruntergeladen.

...

Als Ergebnis liegen, falls Berechtigungen erteilt wurden, ein oder mehrere AuthorizationKeys sowie Policy Documents für berechtigte LEI, KTR, DiGA und für Vertreter vor.

...

**Berechtigung für Vertreter:** Versicherten-ID, Name des Vertreters

**Berechtigung für KTR:** Telematik-ID, Name des KTR

**Berechtigung für DiGA:** Telematik-ID, Name der DiGA

Die Policy Documents lassen sich auf Basis der Versicherten-ID des Vertreters bzw. der Telematik-ID der LEI, DiGA oder KTR den AuthorizationKeys zuordnen.

### 4.2.7.11 Kapitel 6.2.7 Berechtigungsverwaltung

Dieses Kapitel beschreibt Anwendungsfälle zur Vergabe und Administration von Berechtigungen zum Zugriff auf das Aktenkonto.

Im ePA-FdV können nur Berechtigungen an LEI,KTR und DiGA vergeben werden, die im Verzeichnisdienst (VZD) der TI registriert sind.

Die zulässigen Berechtigungsvergaben für die verschiedenen Leistungserbringerinstitutionen, DiGA, Kostenträger und Vertreter werden vom Aktensystem durchgesetzt. Das ePA-FdV kann die grundsätzlich gesetzlich möglichen Berechtigungsvergaben nicht erweitern, sondern nur weiter einschränken.

### 4.2.7.12 Kapitel 6.2.3.8 AuthorizationKey

Der AuthorizationKey enthält Parameter zur Berechtigung sowie die für den Berechtigten verschlüsselten Akten- und Kontextschlüssel.

### 4.2.7.13 Kapitel 6.2.3.8.1 Struktur AuthorizationKeyType

Die Struktur AuthorizationKeyType ist in [AuthorizationService.xsd] beschrieben.

Das Attribut `validTo` beinhaltet die Gültigkeit des AuthorizationKey, d.h. den Zeitpunkt bis zu dem die Berechtigung erteilt wird. Für eine Berechtigung ohne zeitliche Begrenzung wird ein technisches Datum 31.12.9999 verwendet.

Das Attribut `actorID` beinhaltet die ID des Berechtigenden, d.h. die Versicherten-ID für Aktenkontoinhaber und Vertreter bzw. die Telematik-ID für LEIs, DiGA und KTR.

Das Element `DisplayName` beinhaltet den Klartextnamen des Berechtigten oder den Namen der DiGA.

Das Element `AuthorizationType` beinhaltet den Berechtigungstyp. Siehe auch [gemSpec_Autorisierung#6.3 Berechtigungstypen der Autorisierung].

Das Element `phrs:AuthorizationKey/phrs:EncryptedKeyContainer` enthält das Chiffrat mit dem verschlüsselten Akten- und Kontextschlüssel sowie AssociatedData.

Die Datenstruktur für EncryptedKeyContainer und die Klartextpräsentation für Akten- und Kontextschlüssel ist in [gemSpec_SGD_ePA#8 Interoperables Austauschformat] beschrieben.

Änderungen in der Tabelle nach der Anforderung A_17842-01:

Im Schritt 7 des Basisablaufs erfolgt der Aufruf für `KeyDerivation` abhängig vom Anwendungsfall:

| Anwendungsfall im FdV | Akteur | Zweck | Anwendungsfall für SGD |
|---|---|---|---|
| Aktenkonto aktivieren<br>Anbieter wechseln | Versicherter | Verschlüsseln | [gemSpec_SGD_ePA#2.4 Initiale Schlüsselableitung für den Kontoinhaber] |
| Berechtigung für LEI vergeben<br>Berechtigung für DiGA vergeben<br>Vertretung einrichten<br>Berechtigung für Kostenträger vergeben<br>Berechtigung für LEI ändern | Versicherter | Verschlüsseln | [gemSpec_SGD_ePA#2.6 Schlüsselableitung für einen Berechtigungsempfänger] |
| Berechtigung für LEI vergeben<br>Berechtigung für DiGA vergeben<br>Berechtigung für Kostenträger vergeben<br>Berechtigung für LEI ändern | Vertreter | Verschlüsseln | [gemSpec_SGD_ePA#2.8 Schlüsselableitung für einen Berechtigungsempfänger durch einen Vertreter] |
| Login | Versicherter<br>Vertreter | Entschlüsseln | Für das Entschlüsseln müssen keine Anwendungsfälle für SGD unterschieden werden.<br>Es wird das Element AssociatedData des ermittelten AuthorizationKey für den Aufruf der Operation KeyDerivation beim SGD wie folgt verwenden:<br>`KeyDerivation <Teilstring aus AssociatedData für den` |

| | | | |
|---|---|---|---|
| | | | entsprechenden SGD> |

Änderungen im Hinweistext nach der Anforderung A_15336-01

Der Name einer Institution oder einer DiGA wird aus dem Basisdatensatz Attribut `displayName` bestimmt. Die Telematik-ID einer Institution oder einer DiGA wird aus einem Verschlüsselungszertifikat des Datensatzes bestimmt (siehe [gemSpec_PKI]).

### 4.2.7.14 zu Kapitel 6.2.3.8.3 AuthorizationKey erstellen

Für den Aktenkontoinhaber, Vertreter, DiGA und KTR wird die Berechtigung ohne zeitliche Begrenzung vergeben. Für LEI ist das Enddatum entsprechend der vom Nutzer gewählten Berechtigungsdauer zu setzen. Der für `DisplayName` zu verwendende Name einer LEI, DiGA oder eines KTR und die Telematik-ID werden aus dem Eintrag der zu berechtigenden Institution im VZD bestimmt (siehe [gemSpec_ePA_FdV#6.2.3.15]).

...

Es werden bei der Autorisierung verschiedene Berechtigungstypen unterschieden. Siehe [gemSpec_Autorisierung#6.3 Berechtigungstypen der Autorisierung]. Für Aktenkontoinhaber, Vertreter, LEIs, DiGA und KTR wird immer ein Berechtigung mit Zugriff auf die Dokumente vergeben.

...

### 4.2.7.15 Neues Kapitel nach 6.2.3.14: DiGA im Verzeichnisdienst der TI finden

Informationen zu DiGAs sind im Verzeichnisdienst (VZD) der TI-Plattform hinterlegt. Der Nutzer der FdV kann (bspw. für die Vergabe von Berechtigungen an eine DiGA) mit verschiedenen Kriterien nach DiGAs im VZD suchen und Informationen abrufen. Das Informationsmodell des Verzeichnisdienstes ist in [gemSpec_VZD#5] beschrieben.

**A_22668 - ePA-Frontend des Versicherten: Search Operation mittels LDAP-Directory Basisdatensatz Attribut**
Das ePA-Frontend des Versicherten MUSS es dem Versicherten ermöglichen, DiGAs über Suchkriterien gemäß TAB_FdV_190 zu suchen.

**Tabelle 10: TAB_FdV_190 – Suchkriterien LDAP Search für DiGA**

| Suchkriterium | Beschreibung für die Suche nach konkreter DiGA | LDAP-Directory Basisdatensatz Attribut |
|---|---|---|
| Anzeigename | Name der DiGA | displayName |
| Institutionsname | Name des DiGA-Herstellers | organization |

| | | |
|---|---|---|
| DiGA allgemein | DiGA allgemein | professionOID = oid_diga |
| TelematikID | Eindeutiger technischer Identifier der DiGA | telematikID |
| PZN | Pharmazentralnummer | domainID |

**[<=]**

Die Suche nach einer konkreten DiGA erfolgt primär über die PZN oder Anzeigename/Hersteller.

### 4.2.7.16 zu Kapitel 7

Berechtigungen:

| Datenfeld | Herkunft | Beschreibung |
|---|---|---|
| Name des Berechtigten | DisplayName aus AuthorizationKey | |
| Kategorie | Policy Document | LEI, DiGA , KTR oder Vertreter |
| ID | AuthorizationKey / Policy Document | für LEI, DiGA oder KTR: Telematik-ID<br>für Vertreter: Versicherten-ID |
| Berechtigung gültig bis | Policy Document | LEI , DiGA, KTR, Vertreter |
| Berechtigung für LEI | PolicyDocument mit "`urn:gematik:policy:2.0:<record-id>:lei:<telematik-id>`" | LEI |
| Berechtigung für KTR | Policy Document mit "`urn:gematik:policy:2.0:<record-id>:ktr:<telematik-id>`" | KTR |
| Berechtigung für Vertreter | Policy Document mit "`urn:gematik:policy:2.0:<record-id>:rep:<kvnr>`" | Vertreter |

| | | |
|---|---|---|
| Berechtigung für DiGA | Policy Document<br>mit "urn:gematik:policy:2.0:<record-id>:diga:<telematik-id>" | DiGA |

## 4.2.8 gemSpec_Autorisierung

Tabelle xx: Anwendungsfälle der Schlüsselverwaltung nach Umgebung

-> Tabelle um Assoziation für DiGA erweitern

**A_17839-04 - Komponente Autorisierung - Prüfung der Empfänger-Rolle**
Die Komponente Autorisierung MUSS beim Aufruf einer der Operation

- I_Authorization::getAuthorizationKey

den übergebenen Parameter `AuthenticationAssertion` dahingehend prüfen, ob mindestens eine `ProfessionOID` der ZertifikatsExtension `Admission` gemäß [gemSpec_PKI#Tab_PKI_226] im Signaturzertifikat C.HCI.OSIG `/saml2:Assertion/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate` in der Liste der zulässigen Autorisierungsempfänger-Rollen gemäß [gemSpec_OID#Tab_PKI_403]

- oid_praxis_arzt
- oid_zahnarztpraxis
- oid_praxis_psychotherapeut
- oid_krankenhaus
- oid_oeffentliche_apotheke
- oid_epa_ktr
- oid_institution-pflege
- oid_institution-geburtshilfe
- oid_praxis-physiotherapeut
- oid_institution-oegd
- oid_institution-arbeitsmedizin
- oid_institution-vorsorge-reha
- oid_sanitaetsdienst-bundeswehr
- oid_diga

enthalten ist und sofern nicht, die Operation mit dem Fehler AUTHORIZATION_ERROR abbrechen.**[<=]**

**A_14188-05 - Komponente Autorisierung - Umfang Verwaltungsprotokoll**
Die Komponente Autorisierung MUSS dem Versicherten oder berechtigten Vertreter die Einträge des Verwaltungsprotokolls gemäß der Festlegung in [gemSpec_DM_ePA#A_14471-*] übergeben:

**Tabelle 11: Parameter des Verwaltungsprotokolls**

| Protokoll-parameter | Parameterwerte gemäß aufgerufener Operation |
|---|---|
| UserID | Wert des AttributeStatements der übergebenen übergebenen AuthenticationAssertion in `SAML:Assertion/SAML:AttributeStatement`<br><br>**Variante a: Akteur des Aufrufs ist Versicherter bzw. Vertreter**<br>(unveränderbare Anteil der KVNR des aufrufenden Versicherten bzw. Vertreters)<br>*X*Path-Ausdruck zur "Subject-ID" der im Operationsaufruf übergebenen Authentication Assertion:<br>`//*[local-name()='Assertion' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion'][@Name= 'urn:gematik:subject:subject-id']/*[local-name()='AttributeValue']/*[local-name()='InstanceIdentifier']/data(@extension)`<br><br>*Hinweis: Bei Aufrufen der Fälle PHR-451 sowie PHR-470 (via Webseite) kann der Wert für die UserID nicht aus der AuthenticationAssertion bezogen werden, sondern es MUSS die actorID aus dem AuthorizationKey des Betroffenen (Versicherter oder Vertreter) entnommen werden.*<br><br>**Variante b: Akteur des Aufrufs ist LEI, DiGA oder Kostenträger**<br>(Telematik-ID der aufrufenden LEI, DiGA oder Kostenträgers)<br>XPath-Ausdruck zur "Organization-ID" der im Operationsaufruf übergebenen Authentication Assertion:<br>`//*[local-name()='Assertion' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion'][@Name= 'urn:gematik : subject:organization-id']/*[local-name()='AttributeValue']/*[local-name()='InstanceIdentifier']/data(@extension)` |
| UserName | XPath-Ausdruck zur Behauptung "name" (beinhaltet commonName aus dem X.509-Zertifikat), der im Operationsaufruf übergebenen Authentication Assertion:<br>`//*[local-name()='Assertion' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion'][@Name='http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name']/*[local-name()='AttributeValue']`<br><br>*Hinweis: Bei Aufrufen der Fälle PHR-451 sowie PHR-470 (via Webseite) kann der Wert für den UserName nicht aus der AuthenticationAssertion bezogen werden sondern es MUSS der DisplayName aus dem AuthorizationKey des Betroffenen (Versicherter oder Vertreter) entnommen werden.* |

| | |
|---|---|
| Object ID | `ActorID` des im Operationsaufruf gelesenen, gespeicherten oder geänderten AuthorizationKey<br>*Hinweis: Bei Aufruf von Operationen ohne Bezug zu einem AuthorizationKey wird der Wert im Protokolleintrag nicht belegt (z.B. getAuditEvents).* |
| Object Name | `DisplayName` des AuthorizationKeys<br>*Hinweis: Bei Aufruf von Operationen ohne DisplayName wird der Wert im Protokolleintrag nicht belegt.* |
| Device ID | `DeviceID`-Parameter `DeviceIdType::Displayname` des Operationsaufrufs<br>*Hinweis: Bei Aufruf der Operationen der Schnittstelle I_Authorization_Management gibt es den Parameter nicht, DeviceID wird im Protokolleintrag demzufolge nicht belegt.* |
| Object Detail | Falls die Operation mit einem Fehler ASSERTION_INVALID aufgrund einer ungültigen übergebenen Authentication Assertion abbricht, MUSS ParticipantObjectDetail mit folgenden Wertepaaren (`type/value`) belegt werden: |

| **type** | **value** |
|---|---|
| `ErrorInformation` | `"fehlgeschlagene Authentifizierung des Zugreifenden"` |

**[<=]**

## 4.3 Dokumentenverwaltung

Der DiGA-Hersteller agiert gegenüber seinem Konnektor und der ePA wie ein Primärsystem, d.h. ein Konnektor-Client mit im Vergleich zum PS eingeschränkten Möglichkeiten.

### 4.3.1 gemSpec_Dokumentenverwaltung

**A_21505 - Komponente ePA-Dokumentenverwaltung – Zugriffsrechte DiGA-Hersteller**
Die Komponente ePA-Dokumentenverwaltung MUSS alle IHE-ITI-Transaktionen von DiGA-Herstellern ablehnen, die nicht als Einstellen von Dokumenten in `I_Document_Management::CrossGatewayDocumentProvide` gemäß "Cross-Gateway Document Provide" [ITI-80] erfolgen.
**[<=]**

## 4.3.2 gemSpec_DM_ePA

A_14760-07 (neu: A_14760-15), Tabelle Nutzungsvorgaben für Metadatenattribute XDS.b:

Änderung folgender Nutzungsvorgaben:

- author: Die DiGA MUSS das Subattribut authorInstitution inhaltlich belegen.
- authorRole: Die DiGA MUSS authorRole mit dem Wert "102" (Patient) belegen.
- healthcareFacilityTypeCode: Die DiGA MUSS healthcareFacilityTypeCode mit dem Wert "PAT" belegen.
- practiceSettingCode: Die DiGA MUSS practiceSettingCode mit dem Wert "PAT" belegen.
- SubmissionSet.FolderUniqueID MUSS für ~~jedee~~ine bestimmte DiGA pro Versicherten bei jedem Aufruf immer gleich sein.

**A_14760-15 - Nutzungsvorgaben für die Verwendung von XDS-Metadaten**
Das Primärsystem, das ePA-Frontend des Versicherten sowie das Fachmodul ePA KTR-Consumer als XDS-Akteur "Document Source" MÜSSEN zur Registrierung von Dokumenten in der ePA-Dokumentenverwaltung die nachstehenden Nutzungsvorgaben für Metadaten berücksichtigen. Diese Systeme sowie die Komponente ePA-Dokumentenverwaltung MÜSSEN diese Metadaten verarbeiten können und ergänzen diese Metadaten ggf. während des Registriervorgangs. Metadaten können über die Operationen

- `I_Document_Management::CrossGatewayDocumentProvide`,
- `I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b` sowie
- `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b`

registriert oder über die Operation `I_Document_Management_Insurant::RestrictedUpdateDocumentSet` (ausschließlich DocumentEntry.confidentialityCode) geändert werden.

Die Produkttypen ePA-Fachmodul sowie ePA-Frontend des Versicherten sind von den nachstehenden Nutzungsvorgaben ausgenommen, sofern ein Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] erzeugt und registriert werden soll. Hierzu ist die gesonderte Anforderung A_14961-* zu beachten.

**Tabelle 12: Nutzungsvorgaben für Metadatenattribute XDS.b**

| Metadatenattribut XDS.b | Mult. PS | Mult. KTR | Mult. DV | Mult. FV | Kurzbeschreibung | Nutzungsvorgabe | FV Edit |
|---|---|---|---|---|---|---|---|
| **Metadaten für DocumentEntry** | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| author | | [1..n] | [1..1] | [0..0] | [0..n] | Person oder System, welche(s) das Dokument erstellt hat | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.1] genügen.<br><br>Das Primärsystem oder das ePA-Fachmodul KTR-Consumer MUSS mindestens das Subattribut authorPerson oder authorInstitution inhaltlich belegen. | |
| | authorPerson | [0..1] | [0..1] | [0..0] | [0..1] | Name des Autors | Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 2.1.4.3.1 genügen.<br>Die DiGA MUSS author inhaltlich belegen. | X |
| | authorInstitution | [0..n] | [0..n] | [0..0] | [0..n] | Institution, die dem Autor zugeordnet ist | Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 2.1.4.3.2 (A_21209) genügen.<br>Die DiGA MUSS authorInstitution inhaltlich belegen. | X |
| | authorRole | [0..n] | [0..n] | [0..0] | [0..n] | Rolle des Autors | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.authorRole entsprechen.<br>Die DiGA MUSS authorRole mit dem Wert "102" (Patient) belegen. | X |
| | authorSpecialty | [0..n] | [0..0] | [0..0] | [0..n] | Fachliche Spezialisierung des Autors | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.authorSpecialty oder aus der Tabelle in der Anforderung A_15744-* entsprechen. | X |
| | authorTelecommunication | [0..n] | [0..0] | [0..0] | [0..n] | Telekommunikationsdaten des Autors | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen. | X |
| availabilityStatus | | [0..0] | [0..0] | [1..1] | [0..0] | Status des Dokuments ("Approved" oder "Deprecated") | Der Wert MUSS initial "`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" entsprechen. | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| classCode | [1..1] | [1..1] | [0..0] | [1..1] | Grobe Klassifizierung des Dokuments | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.classCode entsprechen.<br><br>Sofern das Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 2.1.4.4 genügen.<br><br>Der ePA-Fachmodul KTR-Consumer MUSS ausschließlich den Code "ADM" (Administratives Dokument) aus dem in [IHE-ITI-VS] definierten Value Set für DocumentEntry.classCode verwenden. | X |
| comments | [0..1] | [0..1] | [0..0] | [0..1] | Ergänzende Hinweise in Freitext | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.4] genügen. | X |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| confidentialityCode | [1..n] | [1..1] | [0..0] | [1..n] | Vertraulichkeitskennzeichnung des Dokuments | Gemäß den Beschreibungen zur Zugriffskontrolle in [gemSpec_Dokumentenverwaltung#5.1.1.5, 5.3] sind die folgenden Codes unter der OID "1.2.276.0.76.5.491" mit dem Code System Name "ePA-Vertraulichkeit" definiert.<br>Es MUSS für die gewünschte Vertraulichkeitsstufe des Dokumentes einer der Codes<br>• Code = "N", Display Name = "normal",<br>• Code = "R", Display Name = "vertraulich" oder<br>• Code = "V", Display Name = "streng vertraulich"<br>aus dem Code System 2.16.840.1.113883.5.25 (siehe auch [IHE-ITI-VS]) gesetzt werden.<br><br>Nur noch von ePA1-Clientsystemen während der Migration von ePA1 zu ePA2 zu verwenden sind:<br>• Code = "LEI", Display Name = "Dokument einer Leistungserbringerinstitution"<br>• Code = "KTR", Display Name = "Dokument eines Kostenträgers"<br>• Code = "PAT", Display Name = "Dokument eines Versicherten"<br>• Code = "LEÄ", Display Name="Leistungserbringeräquivalentes Dokument eines Versicherten oder Kostenträgers"<br>Während der Migration von ePA1 zu ePA2 werden die vorgenannten ConfidentialityCodes gemäß [gemSpec_Dokumentenverwaltung#5.4.3] auf Dokumentenkategorien von ePA2 abgebildet. | X |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | Die weitere Angabe von Codes des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.confidentialityCode ist möglich. | |
| creationTime | [1..1] | [1..1] | [0..0] | [1..1] | Erstellungszeitpunkt des Dokuments | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.6] genügen und DARF NICHT in der Zukunft liegen. Bei der Prüfung ist eine Toleranz von 5 Minuten zulässig. | X |
| entryUUID | [1..1] | [1..1] | [0..1] | [1..1] | Intern verwendete, aktenweit eindeutige Kennung des Dokuments | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.7] genügen.<br><br>Die ePA-Dokumentenverwaltung MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen. | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| eventCodeList | [0..n] | [0..0] | [0..0] | [0..n] | Ereignisse, die zur Erstellung des Dokuments geführt haben. | Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 2.1.4.3.5 genügen. | X |
| formatCode | [1..1] | [1..1] | [0..0] | [1..1] | Global eindeutiger Code für das Dokumentenformat.<br><br>Zusammen mit dem DocumentEntry.typeCode eines Dokuments soll es einem potentiellen zugreifenden System erlauben, im Vorfeld festzustellen, ob das Dokument verarbeitet werden kann. | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.formatCode oder aus der Tabelle in der Anforderung A_14761-* entsprechen. Der Wert KANN "`urn:ihe:iti:xds:2017:mimeTypeSufficient`" (siehe [IHE-ITI-TF-3#4.2.3.2.9]) entsprechen, um anzuzeigen, dass über den MIME-Type hinaus keine genaueren Angaben zum Dokumentenformat gemacht werden können oder der MIME-Type ausreichend ist.<br><br>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 2.1.4.4 genügen. | |
| hash | [0..0] | [0..0] | [0..0] | [0..0] | Kryptographische Prüfsumme des Dokuments | | |
| healthcareFacilityTypeCode | [1..1] | [1..1] | [0..0] | [1..1] | Art der Einrichtung, in der das dokumentierte Ereignis stattgefunden hat. | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.healthcareFacilityTypeCode entsprechen.<br><br>Das ePA-Fachmodul KTR-Consumer MUSS ausschließlich den Code "`VER`" (Versicherungsträger) aus dem in [IHE-ITI-VS] definierten Value Set für DocumentEntry.healthcareFacilityTypeCode verwenden.<br>Die DiGA MUSS healthcareFacilityTypeCode mit dem Wert "`PAT`" belegen. | X |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| homeCommunityId | [1..1] | [1..1] | [1..1] | [0..1] | Bei unterschiedlichen Aktensystemen ("Cross-Community") Kommunikation wird hier die Kennung des adressierten Aktensystems hinterlegt. | Der Wert MUSS der Kennung des Aktenanbieters entsprechen und den Vorgaben aus Abschnitt 2.1.4.3.4 genügen.<br><br>Die ePA-Dokumentenverwaltung MUSS die Home Community ID setzen, falls diese nicht durch das ePA-Frontend des Versicherten gesetzt wurde. | |
| languageCode | [1..1] | [1..1] | [0..0] | [1..1] | Sprache, in der das Dokument abgefasst ist. | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.languageCode entsprechen. Es MÜSSEN mindestens die in der Tabelle Tab_DM_LanguageCodes angegebenen Codes unterstützt werden, alle weiteren Codes KÖNNEN unterstützt werden. | X |
| legalAuthenticator | [0..1] | [0..0] | [0..0] | [0..1] | Rechtlich Verantwortlicher für das Dokument | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.14] genügen.<br><br>Das Attribut DARF NICHT gesetzt werden, falls es sich um ein automatisch erstelltes und nicht durch eine natürliche Person freigegebenes Dokument handelt. | |
| limitedMetadata | [0..0] | [0..0] | [0..0] | [0..0] | Markierungsattribut, dass das Metadatenelement DocumentEntry nicht den vollständigen Satz an Metadaten enthält. | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| mimeType | [1..1] | [1..1] | [0..0] | [1..1] | MIME-Type des Dokuments | Ein Wert aus der folgenden Liste MUSS als MIME-Type verwendet werden:<br>`application/pdf`<br>`image/jpeg`<br>`image/png`<br>`image/tiff`<br>`text/plain`<br>`text/rtf`<br>`application/xml`<br>`application/hl7-v3`<br>`application/pkcs7-mime`<br>`application/fhir+xml`<br><br>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 2.1.4.4 genügen. | |
| objectType | [1..1] | [1..1] | [0..0] | [1..1] | Typ des Dokuments | Der Wert MUSS immer "`urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1`" betragen. Dieser Wert steht für stabile Dokumente im IHE ITI XDS.b-Profil [IHE-ITI-TF3#4.2.5.2]. | |
| patientId | [1..1] | [1..1] | [0..0] | [1..1] | Systemweit eindeutige Kennung des Patienten | Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 2.1.4.3.3 genügen.<br>Außerdem MUSS der Wert der Identität des Akteninhabers entsprechen und MUSS von der ePA-Dokumentenverwaltung dahingehend bei Registrierung der Metadaten geprüft werden. | |
| practiceSettingCode | [1..1] | [0..0] | [0..0] | [1..1] | Art der Fachrichtung der erstellenden Einrichtung, in der das dokumentiere Ereignis stattgefunden hat. | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.practiceSettingCode oder aus der Tabelle in der Anforderung A_16944-* entsprechen.<br>Die DiGA MUSS practiceSettingCode mit dem Wert "`PAT`" belegen. | X |
| referenceIdList | [0..n] | [0..0] | [0..0] | [0..n] | Liste von IDs, mit denen das Dokument | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.28] genügen. | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | assoziiert wird. | | |
| repositoryUniqueId | [0..1] | [0..1] | [1..1] | [0..1] | Kennung des Document Repository, in welches das Dokument eingestellt wird/wurde. | Wenn ein Wert vorhanden ist, MUSS er identisch mit dem Wert für DocumentEntry.homeCommunityId sein, da ein Anbieter ePA-Aktensystem immer nur über ein logisches Repository verfügt.<br><br>Hinweis: Sie wird über einen Slot kodiert und enthält nicht das Präfix "urn:oid:", wie bei dem Attribut für die Home Community ID. | |
| serviceStartTime | [0..1] | [0..1] | [0..0] | [0..1] | Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis begonnen wurde. | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.19] genügen. | X |
| serviceStopTime | [0..1] | [0..1] | [0..0] | [0..1] | Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis beendet wurde. | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.20] genügen. | X |
| size | [0..0] | [0..0] | [1..1] | [0..0] | Größe des Dokuments in Bytes | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.21] genügen.<br><br>Die ePA-Dokumentenverwaltung MUSS die Größe des Dokuments berechnen und in den Metadaten während des Registriervorgangs setzen (vgl. [IHE-ITI-TF2b#3.41.4.1.3]). | |
| sourcePatientId | [0..1] | [0..0] | [0..0] | [0..0] | Kennung des Patienten im Quellsystem | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.22] genügen. | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| sourcePatientInfo | [0..n] | [0..0] | [0..0] | [0..0] | Demographische Daten zum Patienten im Quellsystem | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.23] genügen. | |
| title | [0..1] | [0..1] | [0..0] | [0..1] | Titel des Dokuments | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.24] genügen. | X |
| typeCode | [1..1] | [1..1] | [0..0] | [1..1] | Art des Dokuments | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.typeCode entsprechen.<br><br>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Inhalts- und Formatvorgaben aus Abschnitt 2.1.4.4 genügen.<br><br>Der ePA-Fachmodul KTR-Consumer MUSS ausschließlich den Code "ABRE" (Abrechnungsdokumente) aus dem in [IHE-ITI-VS] definierten Value Set für DocumentEntry.classCode verwenden. | X |
| uniqueId | [1..1] | [1..1] | [0..0] | [1..1] | Eindeutige, aktenweite Kennung des Dokuments | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.26] genügen. | |
| URI | [1..1] | [1..1] | [0..0] | [1..1] | URI für das Dokument | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.27] genügen . | |
| **Metadaten für SubmissionSet** | | | | | | | |
| author | [1..n] | [1..1] | [0..0] | [1..1] | Person oder System, welche(s) das Submission Set erstellt hat. | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.1] genügen. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | authorPerson | [1..1] | [0..1] | [0..0] | [1..1] | Name der einstellenden Person oder des einstellenden Systems | Der Wert MUSS den Formatvorgaben aus Abschnitt 2.1.4.3.1 genügen.<br><br>Das ePA-Frontend des Versicherten MUSS mindestens Vorname, Nachname und Titel aus dem Authentisierungszertifikat des Nutzers hinterlegen.<br><br>Im Gegenzug MUSS die ePA-Dokumentenverwaltung dieses Metadatenattribut auf Gleichheit zu den Behauptungen aus der angegeben XUA Authentication Assertion prüfen. Eine Gleichheit liegt vor, wenn der Vorname sowie der Nachname aus der XCN-Struktur des Autors nach den Vorgaben von A_14762-* mit den entsprechenden Werten aus der Behauptung in `saml2:Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims /givenname"` und `Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims /surname"` der XUA Authentication Assertion übereinstimmt und die KVNR aus der XCN-Struktur des Autors mit dem entsprechenden Wert aus der Behauptung in `saml2:Attribute Name="urn:gematik:subject:subject-id"` der XUA Authentication Assertion übereinstimmt. | |
| | authorInstitution | [1..1] | [1..1] | [0..0] | [0..0] | Institution, welcher die einstellende Person oder das einstellende System zugeordnet ist. | Der Wert MUSS den Formatvorgaben aus Abschnitt 2.1.4.3.2 (A_21209) genügen.<br><br>Das Primärsystem MUSS die Identität der am Aktensystem angemeldeten Leistungserbringerinstitution als authorInstitution hinterlegen. Im Gegenzug MUSS die ePA-Dokumentenverwaltung dieses Metadatenattribut auf Gleichheit der SAML Behauptung aus der angegeben XUA Authentication Assertion prüfen. Eine Gleichheit | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | liegt vor, wenn die Telematik-ID aus der XON-Struktur der Institution des Autors nach den Vorgaben von A_14763-* mit dem entsprechenden Wert aus der Behauptung in `saml2:Attribute Name="urn:gematik:subject:organization-id"` der XUA Authentication Assertion übereinstimmt. | |
| | authorRole | [1..n] | [1..n] | [0..0] | [1..1] | Rolle der einstellenden Person oder des einstellenden Systems | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.authorRole entsprechen.<br><br>Das ePA-Fachmodul KTR-Consumer MUSS den Code "`105`" (Kostenträgervertreter) aus dem in [IHE-ITI-VS] definierten Value Set für DocumentEntry.authorRole verwenden.<br><br>Das ePA-Frontend des Versicherten und die ePA-AdV-App MUSS den Code "`102`" (der Patient selbst) aus dem in [IHE-ITI-VS] definierten Value Set für DocumentEntry.authorRole verwenden. Die ePA-Dokumentenverwaltung MUSS dieses Metadatenattribut auf Gleichheit gegenüber der SAML Behauptung aus der angegeben XUA Authentication Assertion prüfen. Eine Gleichheit liegt vor, wenn die KVNR aus der Behauptung in`saml2:Attribute Name="urn:gematik:subject:subject-id"` der XUA Authentication Assertion den Akteninhaber oder einen Vertreter darstellt. | |
| | authorSpecialty | [0..n] | [0..0] | [0..0] | [0..n] | Fachliche Spezialisierung der einstellenden Person oder des | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für DocumentEntry.authorSpecialty oder aus der Tabelle in der | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | einstellenden Systems | Anforderung A_15744-* entsprechen. | |
| | authorTelecommunication | [0..n] | [0..0] | [0..0] | [0..n] | Telekommunikationsdaten der einstellenden Person oder des einstellenden Systems | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen. | |
| availabilityStatus | | [0..0] | [0..0] | [1..1] | [0..0] | Status des Submission Sets ("Approved") | Der Wert MUSS "`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" entsprechen. | |
| comments | | [0..1] | [0..1] | [0..0] | [0..1] | Ergänzende Hinweise zum Submission Set in Freitext | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.3] genügen. | X |
| contentTypeCode | | [0..1] | [0..1] | [0..0] | [0..1] | Klinische Aktivität, die zum Einstellen des Submission Set geführt hat. | Der Wert MUSS einem Code des in [IHE-ITI-VS] definierten Value Sets für SubmissionSet.contentTypeCode entsprechen. | |
| entryUUID | | [1..1] | [1..1] | [0..1] | [1..1] | Intern verwendete, aktenweit eindeutige Kennung des Submission Sets | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.5] genügen.<br><br>Die ePA-Dokumentenverwaltung MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen. | |
| homeCommunityId | | [1..1] | [1..1] | [1..1] | [0..1] | Zur Cross-Community-Kommunikation die Kennung des adressierten Aktensystems | Der Wert MUSS identisch mit dem Wert für DocumentEntry.homeCommunityId sein. | |
| intendedRecipient | | [0..n] | [0..0] | [0..0] | [0..n] | Vorgesehener Adressat des | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.7] genügen. | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | Submission Set | | |
| limitedMetadata | [0..0] | [0..0] | [0..0] | [0..0] | Markierung, welche anzeigt, dass das Submission Set nicht den durch das IHE ITI TF vorgegebenen Satz an Metadaten enthält. | | |
| patientId | [1..1] | [1..1] | [0..0] | [1..1] | Patienten-ID, zu der das Submission Set gehört | Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 2.1.4.3.3 genügen und inhaltlich identisch zur DocumentEntry.patientId sein. | |
| sourceId | [0..0] | [0..0] | [0..0] | [0..0] | Weltweit eindeutige, unveränderliche Kennung des einstellenden Systems | | |
| submissionTime | [1..1] | [1..1] | [0..0] | [1..1] | Zeit, zu der das Submission Set zusammengestellt wurde. | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.10] genügen.<br>Die ePA-Dokumentenverwaltung MUSS prüfen, ob der Wert der aktuellen Systemzeit entspricht. Sollte diese von der lokalen Zeit über mehr als eine Minute abweichen, MUSS der Wert mit der aktuellen Systemzeit ersetzt werden. Diese Systemzeit MUSS dabei synchron zur Systemzeit des Produkttyps Zeitdienst gemäß [gemSpec_Net#5] sein. | |
| title | [0..1] | [0..1] | [0..0] | [0..1] | Titel des Submission Sets | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.11] genügen. | X |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| uniqueId | [1..1] | [1..1] | [0..0] | [1..1] | Eindeutige Kennung des Submission Sets | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.12] genügen. | |
| **Metadaten für dynamische Folder** | | | | | | | |
| availabilityStatus | [1..1] | n/a | [0..0] | n/a | Status des Ordners ("Approved") | Der Wert MUSS "`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" entsprechen. | |
| codeList | [1..1] | n/a | [0..0] | n/a | Liste von Codes, die mit dem Ordner assoziiert werden. | Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] genügen.<br><br>Bei Folder.codeList=mothersrecord and childsrecord MUSS das Primärsystem diese Codes angeben. | |
| comments | [0..1] | n/a | [0..0] | n/a | Freitextkommentar für diesen Ordner. | Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen. | |
| entryUUID | [1..1] | n/a | [1..1] | n/a | Intern verwendete, aktenweit eindeutige Kennung des Ordners | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen.<br><br>Die Komponente ePA-Dokumentenverwaltung MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen. | |
| homeCommunityId | Der Wert MUSS analog zu DocumentEntry.homeCommunityId belegt werden. | | | | | | |
| lastUpdateTime | [0..0] | n/a | [1..1] | n/a | Zeitstempel, an dem der Ordner das letzte mal geändert wurde | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.6] genügen.<br><br>Die Komponente ePA-Dokumentenverwaltung MUSS den Wert automatisch gemäß [IHE-ITI-TF2b#3.42.4.1.3.6] aktuell halten. | |
| limitedMetadata | Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden. | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| patientId | [1..1] | n/a | [0..0] | n/a | Patienten ID, zu der der Ordner gehört. | Der Wert MUSS analog zu DocumentEntry.patientId belegt werden. | |
| title | [0..1] | n/a | [0..0] | n/a | Titel des Ordners | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.8] genügen. | |
| uniqueId | [1..1] | n/a | [0..0] | n/a | Eindeutige, aktenweite Kennung des Ordners | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.9] genügen. | |
| **Metadaten für statische Folder** | | | | | | | |
| availabilityStatus | n/a | n/a | [1..1] | n/a | Status des Ordners ("Approved") | Der Wert MUSS "`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" entsprechen. | |
| codeList | n/a | n/a | [1..1] | n/a | Liste von Codes, die mit dem Ordner assoziiert werden. | Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] genügen.<br><br>Die Komponente ePA-Dokumentenverwaltung MUSS codeList gemäß A_19388-* setzen. | |
| comments | n/a | n/a | [0..1] | n/a | Freitextkommentar für diesen Ordner. | Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen. | |
| entryUUID | n/a | n/a | [1..1] | n/a | Intern verwendete, aktenweit eindeutige Kennung des Ordners | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen.<br><br>Die Komponente ePA-Dokumentenverwaltung MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen. | |
| homeCommunityId | Der Wert MUSS analog zu DocumentEntry.homeCommunityId belegt werden. | | | | | | |
| lastUpdateTime | n/a | n/a | [1..1] | n/a | Zeitstempel, an dem der Ordner das letzte mal geändert wurde | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.6] genügen.<br><br>Die Komponente ePA-Dokumentenverwaltung MUSS den Wert automatisch | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | gemäß [IHE-ITI-TF2b#3.42.4.1.3.6] aktuell halten. | |
| limitedMetadata | Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden. | | | | | | |
| patientId | n/a | n/a | [1..1] | n/a | Patienten ID, zu der der Ordner gehört. | Der Wert MUSS analog zu DocumentEntry.patientId belegt werden. | |
| title | n/a | n/a | [0..1] | n/a | Titel des Ordners | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.8] genügen. | |
| uniqueId | n/a | n/a | [1..1] | n/a | Eindeutige, aktenweite Kennung des Ordners | Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.9] genügen. | |

**Tabelle 13: Tab_DM_LanguageCodes - Mindestanforderung an zu unterstützende Language Codes**

| Language / Country Code Kombination | Language / Country Code Kombination |
|---|---|
| `bg-BG` (bulgarisch, Bulgarien) | `it-IT` (italienisch, Italien)<br>`it-CH` (italienisch, Schweiz) |
| `cs-CZ` (tschechisch, Tschechien) | `lt-LT` (litauisch, Litauen) |
| `da-DK` (dänisch, Dänemark) | `lb-LU` (luxemburgisch, Luxemburg) |
| `de-AT` (deutsch, Österreich)<br>`de-DE` (deutsch, Deutschland)<br>`de-CH` (deutsch,Schweiz)<br>`de-LI` (deutsch, Liechtenstein)<br>`de-LU` (deutsch, Luxemburg) | `lv-LV` (lettisch, Lettland) |
| `el-GR` (griechisch, Griechenland) | `mt-MT` (maltesisch, Malta) |
| `en-GB` (englisch, Vereinigtes Königreich) | `nl-NL` (niederländisch, Niederlande)<br>`nl-BE` (niederländisch, Belgien) |
| `es-ES` (spanisch, Spanien) | `no-NO` (norwegisch, Norwegen) |
| `et-EE` (estnisch, Estland) | `pl-PL` (polnisch, Polen) |
| `fi-FI` (finnisch, Finnland) | `pt-PT` (portugiesisch, Portugal) |

| | |
|---|---|
| `fr-FR` (französisch, Frankreich)<br>`fr-CH` (französisch, Schweiz)<br>`fr-LU` (französisch, Luxemburg)<br>`fr-BE` (französisch, Belgien) | `rm-CH` (rätoromanisch, Schweiz) |
| `ga-IE` (irisch, Irland) | `ro-RO` (rumänisch, Rumänien) |
| `hr-HR` (kroatisch, Kroatien) | `sk-SK` (slowakisch, Slowakei) |
| `hu-HU` (ungarisch, Ungarn) | `sl-SI` (slowenisch, Slowenien) |
| `is-IS` (isländisch, Island) | `sv-SE` (schwedisch, Schweden) |

Weitere Sprach- und Länder-Codes (gemäß [IHE-ITI-VS]) sind erlaubt. Diese können beliebig für DocumentEntry.languageCode kombiniert werden.
**[<=]**

Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner gesammelt. Der Ordner wird über seine FolderUniqueID identifiziert.

Beim Speichern von Dokumenten muss die Dokumentenverwaltung ermitteln können, welchem DiGA-Ordner ein Dokument zuzuordnen ist. Die DiGA muss beim Einstellen ihrer Dokumente über die FolderUniqueID den eigenen DiGA-Ordner adressieren.

Durch Einstellen eines aktualisierten DiGA unter einer ihm bekannten DocumentUniqueID realisiert die DiGA ein Update eines bestehenden Dokuments.

Anpassung der Anforderung, siehe Kapitel 4.2.1

**A_14762-02 - Nutzungsvorgabe für authorPerson als Teil von DocumentEntry.author und SubmissionSet.author**
Das Primärsystem sowie die ePA-Produkttypen, welche IHE ITI XDS-Metadaten verarbeiten, MÜSSEN die folgenden Nutzungsvorgaben für das Metadatenattribut authorPerson unterhalb von DocumentEntry.author und SubmissionSet.author berücksichtigen. Der Wert dieses Attributs MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.1.4.2] genügen und ist inhaltlich nach den folgenden Vorschriften zusammenzufügen bzw. zu belegen.

**Leistungserbringer als Autor**

1. Lebenslange Identifikationsnummer eines Arztes (Lebenslange Arztnummer - LANR 9 Stellen) oder im Falle eines Zahnarztes die Zentrale Zahnarztnummer- sofern bekannt
2. "^"
3. Nachname
4. "^"
5. Vorname

6. "^"
7. Weiterer Vorname
8. "^"
9. Namenszusatz
10. "^"
11. Titel
12. "^^^&" - sofern LANR angegeben, ansonsten "^^^"
13. "1.2.276.0.76.4.16" - sofern LANR angegeben
14. "&ISO" - sofern LANR angegeben

Beispiele:
`165746304^Weber^Thilo^^^Dr.^^^&1.2.276.0.76.4.16&ISO`
`^Weber^Thilo^^^Dr.^^^`

**Versicherter als Autor**

1. Der unveränderbare Teil der KVNR (10 Stellen)
2. "^"
3. Nachname
4. "^"
5. Vorname
6. "^"
7. Weiterer Vorname
8. "^"
9. Namenszusatz
10. "^"
11. Titel
12. "^^^&"
13. "1.2.276.0.76.4.8"
14. "&ISO"

Beispiel: `G995030566^Gundlach^Monika^^^^^^&1.2.276.0.76.4.8&ISO`

**Software-Komponente bzw. Gerät als Autor**
Beim (automatisierten) Einstellen von Dokumenten MUSS der max. 256-Zeichen lange Name der Software-Komponente bzw. des Geräts als Nachname und ggf. als Vorname(n) eingetragen werden.
Beispiel: `^PHR-Gerät-XY^PHR-Software-XY`
Im Falle einer DiGA MUSS das Feld Autor folgendermaßen aufgebaut sein:

1. Telematik-ID der DiGA
2. "^"
3. Name der Software

4. "^"
5. PZN (Pharmazentralnummer), unter der die DiGA beim Bfarm registriert ist
6. "^"
7. optionale Ergänzung der Bezeichnung der SW
8. "^"
9. optionale Ergänzung der Bezeichnung der SW
10. "^"
11. optionale Ergänzung der Bezeichnung der SW
12. "^^^&"
13. <OID für DiGAs, wie in professionOID>
14. "&ISO"

Für alle drei Arten von Autoren (Versicherter, LE, Gerät) MUSS jeweils Vorname und Nachname angegeben sein.**[<=]**

**A_21511 - Nutzungsvorgabe SubmissionSet.authorInstitution für DIGAs**
Das DiGA-PS sowie die ePA-Produkttypen, welche IHE ITI XDS-Metadaten verarbeiten, MÜSSEN für DiGAs die folgenden Nutzungsvorgaben für das Metadatenattribut DocumentEntry.authorInstitution sowie SubmissionSet.authorInstitution berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.1.4.1] genügen und ist inhaltlich nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen.

1. Name des Anbieters der DiGA
2. "`^^^^^&`"
3. "`1.2.276.0.76.4.188`" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "`&ISO^^^^`"
5. Hersteller - Institutionskennzeichnung im DiGA-Verzeichnis des BFARM

**[<=]**

## 4.3.3 gemSpec_ePA_FdV Kapitel 6.2.8.2 Dokumente suchen

Der Hinweistext nach der A_15469 ist wie folgt anzupassen:

Folgende Suchanfragen sollen mindestens möglich sein (ggf. mit zusätzlichem Nachfiltern auf dem ePA-FdV):

- Suche nach allen medizinischen Dokumenten im Aktenkonto
- Suche nach Ersteller bzw. Einsteller (`$XDSSubmissionSetAuthorPerson`, `$XDSDocumentEntryAuthorPerson`, `$XDSDocumentEntryAuthorInstitution` siehe [gemSpec_Dokumentenverwaltung#A_18070] und A_17854)
- Suche nach in einem Zeitraum erstellten bzw. eingestellten Dokumenten (`$XDSDocumentEntryCeationTimeFrom/To` / `$XDSSubmissionSetSubmissionTimeFrom/To`)

- Suche nach Dokumententitel (siehe [gemSpec_Dokumentenverwaltung#A_17185] und A_17854)
- Suche nach durch LEI bereitgestellte Dokumente
- Suche nach durch DiGA bereitgestellte Dokumente
- Suche nach Dokumenten mit Kennzeichnung "Versicherteninformation"(siehe [gemSpec_DM_ePA#A_14986])
- Suche nach durch Krankenkassen bereitgestellte Informationen

## 4.4 Nutzung von DiGA-Daten beim Leistungserbringer

### 4.4.1 Neues Kapitel gemILF_PS_ePA nach 6.3.4 Daten digitaler Gesundheitsanwendungen

Daten digitaler Gesundheitsanwendungen (DiGA) liegen in interoperablen Formaten vor, die den Festlegungen in [gemSpec_DM_ePA] und falls vorhanden, Vorgaben der KBV folgen.

Nur DiGA können berechtigt werden, DiGA-Daten in für jeden Versicherten eindeutige Folder einzustellen. Andere Rechte auf Daten der Kategorie 9 bzw. DiGA können ihnen nicht eingeräumt werden.

Die DiGA hat zwei IHE-konforme Optionen zur Bereitstellung von Daten in die ePA: Einstellen neuer Dokumente oder Replacement bestehender Dokumente.

**A_21522 - DiGA-PS: Persistierung der FolderUniqueID der DiGA**
Das DiGA-PS bzw. der DiGA-Client, der`DocumentRepository_ProvideAndRegisterDocumentSet-b` nutzt, MUSS im SubmissionSet eine`FolderUniqueID` verwenden. Das DiGA-PS MUSS die beim initialen Einstellen in die Akte eines Versicherten verwendete`FolderUniqueID` persistieren und in allen nachfolgenden Requests für denjenigen Versicherten verwenden. Requests des DIGA-PS, bei denen in nachfolgenden Requests für einen Versicherten abweichende `FolderUniqueIDs` verwendet werden, führen in diesen Fällen zu einem`IHEMetadataError`. **[<=]**

Der Leistungserbringer kann berechtigt werden, DiGA-Daten, d.h. Daten der Kategorie 9 bzw. "diga" zu lesen. Andere Rechte auf Daten der Kategorie 9 bzw. "diga" können ihnen nicht eingeräumt werden

**A_21503 - PS: Daten digitaler Gesundheitsanwendungen auslesen**
Das Primärsystem MUSS DiGA-Daten, deren Formatvorgabe als Medizinisches Informationsobjekt gemäß [gemSpec_DM_ePA] definiert sind, bei vorliegender Berechtigung aus dem ePA-Aktensystem des Versicherten auslesen und anzeigen können.**[<=]**

## 4.5 Umschlüsselung

### 4.5.1 gemSpec_ePA_FdV Kapitel 6.2.6 Umschlüsselung

**A_20479-02 - ePA-Frontend des Versicherten: Umschlüsselung durchführen**
Das Frontend des Versicherten muss den Anwendungsfall "Umschlüsselung" für den Versicherten umsetzen.

| | |
|---|---|
| Name | Umschlüsselung |
| Auslöser | Aufruf des Anwendungsfalls in der GUI |
| Akteur | Versicherter |
| Vorbedingung | Es besteht eine Aktensession mit gültigen Session-Daten.<br>Die Akte befindet sich im Zustand "ACTIVATED". |
| Nachbedingung | 1. Neuer Aktenschlüssel ist erzeugt<br>2. Neuer Kontextschlüssel ist erzeugt.<br>3. Für jeden Berechtigten sind neue SGD1 und SGD2 Schlüssel erzeugt<br>4. Für alle Berechtigten sind der neue Akten- und der neue Kontextschlüssel mit den neuen SGD Schlüsseln geschützt in der Autorisierungskomponente hinterlegt.<br>5. Alle Dokumentenschlüssel in der Dokumentenverwaltungskomponente sind mit dem neuen Aktenschlüssel umgeschlüsselt.<br>6. Die Akte befindet sich im Zustand "ACTIVATED".<br>7. Der Versicherte kann innerhalb von 4 Wochen die Umschlüsselung rückgängig machen. Dazu werden von der Dokumentenverwaltungskomponente und von der Autorisierungskomponente der alte Aktenschlüssel, der alte Kontext-Schlüssel und die alten chiffrierten Dokumentenschlüssel aufbewahrt und nach Ablauf der Frist, wenn die Umschlüsselung nicht rückgängig gemacht wurde, datenschutzkonform gelöscht. |
| Standardablauf | Aktivitäten im Standardablauf<br>1. Der Versicherte startet die Umschlüsselung mit dem Aufruf der Funktion `StartKeyChange()` (gemSpec_Autorisierung#6.2.4.13) an der Komponente Autorisierung. Als Rückgabewert liefert die Autorisierung die rollbackTime. Die Autorisierungkomponente setzt den Status der Akte auf den Zustand KEY_CHANGE. Wenn innerhalb der rollbackTime (z.B.24 h) die Umschlüsselung nicht abgeschlossen ist, werden sowohl die Autorisierung als auch das Aktensystem den Zustand einnehmen, den sie vor der |

| | |
|---|---|
| | Umschlüsselung hatten. Sollte die Autorisierungskomponente auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab.<br>Das FdV muss dem Versicherten einen Hinweistext anzeigen, dass nach der Umschlüsselung die alten Kontext- und Aktenschlüssel sowie die alten verschlüsselten Dokumentenschlüssel vier Wochen aufbewahrt werden. Weiterhin muss explizit darauf hingewiesen werden, dass es sehr empfehlenswert ist, sich nach der erfolgreichen Umschlüsselung erneut anzumelden und Dokumente aus der ePA herunterzuladen und zu betrachten, um sich so von dem Erfolg der Umschlüsselung zu überzeugen. Der Hinweistext muss Informationen enthalten, wie man sich über einen anderen Weg als über das FdV an den Hersteller der Akte wenden kann. Dem Versicherten muss über diesen Weg die Möglichkeit geboten werden, die Umschlüsselung innerhalb von 4 Wochen rückgängig zu machen, wenn sie nicht erfolgreich verlaufen war. Weiterhin kann der Versicherte, wenn die Umschlüsselung erfolgreich war, die Aufbewahrung der alten Schlüssel und dem Schlüsselchiffrat verkürzen und sofort löschen lassen. Dies kann geboten sein, wenn der Grund für die Umschlüsselung eine Kompromittierung der alten Schlüssel war.<br>2. Das FdV generiert einen neuen Akten- und einen neuen Kontextschlüssel wie in gemSpecFdv#6.2.5.1. beschrieben.<br>3. Das FdV ruft die Funktion `StartKeyChange(newKS,rollbackTime)` an der Dokumentenverwaltung (gemSpec_Dokumentenverwaltung#5.3.2.1) auf. Die Dokumentenverwaltung führt einen Logout aller angemeldeten anderen Instanzen (z.B. LEI oder Kassen) durch. Dieser Aufruf liefert als Rückgabewert eine Struktur mit KVNRs und / oder Telematik-IDs berechtigter LEIs, Kassen, DiGAs oder Vertretern zurück. Sollte die Dokumentenverwaltung auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das ePA-FdV die Umschlüsselung nach A_20507 ab.<br>4. Das FdV ruft für den Versicherten, jede berechtigte LEI, für jede berechtigte Kasse, jede berechtigte DiGA und für jeden Vertreter die Funktion `KeyGeneration()` am SGD1 und am SGD2 (gemSpec_SGD_ePA#6.6) auf. Hierbei ist die Ableitungsregel für eine Erstableitung von Schlüsseln für den berechtigten Nutzer durch den Kontoinhaber zu verwenden. Als Rückgabewert vom SGD1 und vom SGD2 erhält das FdV jeweils einen neu generierten Schlüssel. Sollten die Schlüsselgenerierungsdienste auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab. Eine Ausnahme bildet der Fehlerfall, dass eine LEI oder eine DiGA nicht mehr im VZD gefunden wird. In diesem Fall ist der Nutzer des FdV darüber zu benachrichtigen, dass die |

Berechtigungen für diese LEIoder diese DiGA nicht mehr gültig sind, da die LEI oder die DiGA nicht mehr im VZD verzeichnet ist. Anschließend wird die Umschlüsselung fortgesetzt.

5. Das FdV verschlüsselt für den Versicherten, für jede berechtigte LEI, jede berechtigte Kasse, jede berechtigte DiGA und jeden berechtigten Vertreter den neuen Aktenschlüssel mit den von den SGD1 und SGD2 generierten nutzerindividuellen Schlüsseln.
6. Das FdV verschlüsselt für den Versicherten, für jede berechtigte LEI, jede berechtigte Kasse, jede berechtigte DiGA und jeden berechtigten Vertreter den neuen Kontextschlüssel mit den von den SGD1 und SGD2 generierten nutzerindividuellen Schlüsseln.
7. Das FdV übermittelt mit dem Aufruf der Methode `PutForReplacement(SetOfEncryptedKeys)` die in (5 und 6) verschlüsselten Schlüssel an die Komponente Autorisierung, wo sie als neue Schlüssel gekennzeichnet, zunächst gespeichert werden. Nach erfolgreichem Abschluss der Umschlüsselung ersetzt die Autorisierungskomponente die alten Schlüssel durch die neuen. Sollte die Autorisierungskomponente auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab.
8. Das FdV ruft mit der Methode `GetAllDocumentKeys()` der Komponente Dokumentenverwaltung alle verschlüsselten Dokumentenschlüssel (Rückgabewert `DocumentKeyList`) vom Aktensystem ab. Dokumente werden dabei nicht übertragen. Sollte die Komponente Dokumentenverwaltung auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab.
9. Das FdV entschlüsselt die verschlüsselten Dokumentenschlüssel mit dem alten Aktenschlüssel.
10. Das FdV verschlüsselt die entschlüsselten Dokumentenschlüssel mit dem neuen Aktenschlüssel.
11. Das FdV wählt aus den empfangenen DokumentenIDs einige aus und lädt zu diesen die verschlüsselten Dokumente aus der Dokumentenverwaltung, entschlüsselt sie und bildet über die einzelnen Dokumente mittels einer Hashfunktion eindeutige Hashwerte. Diese werden zusammen mit den Dokumenten-IDs gespeichert und benötigt, um später prüfen zu können, ob die Umschlüsselung erfolgreich war.
12. Das FdV übermittelt mit dem Aufruf der Methode `PutAllDocumentKeys()` die mit dem neuen Aktenschlüssel verschlüsselten Dokumentenschlüssel an die Komponente Dokumentenverwaltung. Sollte die Dokumentenverwaltung auf diesen Aufruf nicht innerhalb des Funktions-Timeouts oder mit einem Fehler antworten, dann bricht das FdV die Umschlüsselung nach A_20507 ab.

| | |
|---|---|
| | 13. Das FdV schließt die VAU in der Dokumentenverwaltung über `closeContext()`.<br>14. Um den Erfolg der Umschlüsselung zu überprüfen, holt sich das FdV von der Autorisierungskomponente den neuen Kontext-Schlüssel und öffnet dann damit die VAU in der Komponente Dokumentenverwaltung. Anschließend lädt es mit den in Schritt 11 gespeicherten Dokumenten-IDs die verschlüsselten Dokumente aus der Dokumentenverwaltung.<br>15. Das FdV entschlüsselt die in Schritt 14 heruntergeladenen Dokumente und bildet mit der in Schritt 11 verwendeten Hashfunktion erneut den Hashwert über jedes der entschlüsselten Dokumente.<br>16. Anschließend vergleicht das FdV die in Schritt 11 und Schritt 15 für jedes Dokument erzeugten Hashwerte, wenn sie identisch sind, dann ist die Umschlüsselung erfolgreich durchgeführt worden.<br>17. Wenn in Schritt 16 die erfolgreiche Umschlüsselung festgestellt worden ist, dann ruft das FdV an der Komponente Dokumentenverwaltung die Methode `finishKeyChange(true)` auf. Diese ersetzt die alten Schlüssel durch die neuen und sichert die alten Schlüssel für einen Zeitraum von 4 Wochen, bzw. sichert diese für eventuell vorhandene Backups verschlüsselter Dokumente im Rahmen eines Backup-Konzepts. Anschließend setzt die Dokumentenverwaltung den Status der Akte wieder auf ACTIVATED. Damit ist für die Dokumentenverwaltung die Umschlüsselung abgeschlossen.<br>18. Wenn Schritt 17 erfolgreich durchgeführt wurde, dann ruft das FdV an der Autorisierungskomponente die Methode `finishKeyChange(true)` auf. Diese sichert für einen Zeitraum von vier Wochen die alten Schlüssel, bzw. sichert sie für eventuell vorhandene Backups verschlüsselter Dokumente im Rahmen eines Backup-Konzepts. Anschließend setzt die Autorisierungskomponente den Status der Akte wieder auf ACTIVATED. Damit ist für die Autorisierungskomponente die Umschlüsselung abgeschlossen.<br>19. Wenn in Schritt 16 die Umschlüsselung als fehlgeschlagen erkannt wurde (weil die verglichenen Hashwerte nicht gleich waren), dann ruft das FdV an der Komponente Dokumentenverwaltung die Methode `finishKeyChange(FALSE)` auf. Diese ruft die Rollback()- Methode auf, welche die alten gespeicherten Schlüssel wieder aktiviert und die neuen Schlüssel löscht.<br>20. Wenn der Schritt 19 durchgeführt wurde, dann ruft das FdV an der Autorisierungskomponente die Methode finishKeyChange(FALSE) auf. Diese ruft die Rollback()- Methode auf, welche die alten gespeicherten Schlüssel wieder aktiviert die neuen löscht. Anschließend setzt die |

| | |
|---|---|
| | Autorisierungskomponente den Status der Akte wieder auf ACTIVATED. Damit ist die Umschlüsselung abgeschlossen. |

**[<=]**

## 4.6 Anbieter wechseln

## 4.6.1 gemSpec_ePA_FdV - zu Kapitel 6.2.5.2 Anbieter wechseln

**A_22669 - ePA-Frontend des Versicherten: Anbieter wechseln - Berechtigung DiGA erteilen**
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln", wenn die Berechtigungen in das Aktenkonto des neuen Anbieters übernommen werden sollen, für jede aus dem Aktenkonto des alten Anbieters ermittelte Berechtigung einer DiGA einen AuthorizationKey erstellen und das Schlüsselmaterial in das ePA-Aktensystem des neuen Anbieters laden.**[<=]**

Das Hochladen des Schlüsselmaterials in das ePA-Aktensystem erfolgt mit der übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem EingangsparameterAuthorizationKey = erstellter AuthorizationKey. Der optionale Parameter NotificationInfoRepresentative wird für LEI, DiGA und KTR nicht belegt.

## 4.7 Protokollierung

## 4.7.1 gemSpec_ePA_FdV#A_15489-05:

-> PHR-230 und PHR-510 für DiGA erweitern

**A_15489-06 - ePA-Frontend des Versicherten: Standard-Anzeige für Protokolldaten**
Das ePA-Frontend des Versicherten MUSS eine Standard-Anzeige für die Protokolldaten umsetzen, in der die Protokolleinträge für folgende Zugriffe übersichtlich dargestellt werden:

- PHR-220 (Login Versicherter/Vertreter (Abruf der Berechtigung)
- PHR-230 (Login aus der ärztlichen Umgebung, einer DiGA oder eines Kostenträgers)
- PHR-451 (Änderung E-Mail-Adresse)
- PHR-470 (Geräteverwaltung)
- PHR-510 (Hinzufügen eines Dokuments aus der ärztlichen Umgebung oder einer DiGA)
- PHR-520 (Suchanfrage aus der ärztlichen Umgebung)

- PHR-530 (Löschen eines Dokuments aus der ärztlichen Umgebung)
- PHR-540 (Abruf eines Dokuments aus der ärztlichen Umgebung)
- PHR-560 (Löschen von Dokumenten oder Ordnern aus der ärztlichen Umgebung)
- PHR-610 (Hinzufügen eines Dokuments aus der privaten Umgebung)
- PHR-620 (Suchanfrage aus der privaten Umgebung)
- PHR-630 (Löschen eines Dokuments aus der privaten Umgebung)
- PHR-640 (Abruf eines Dokuments aus der privaten Umgebung)
- PHR-680 (Löschen von Dokumenten, Ordnern aus der privaten Umgebung)
- PHT-690 (Änderungen der Vertraulichkeitsstufe von Dokumenten aus der privaten Umgebung)
- PHR-710 (Hinzufügen eines Dokuments aus der Kostenträger-Umgebung)
- PHR-810 (Start eines Umschlüsselungsvorgangs)
- PHR-870 (Erfolgreicher Abschluss des Umschlüsselungsvorgangs durch den Versicherten)
- PHR-860 (Abbruch des Umschlüsselungsvorgangs)

**[<=]**

## 4.7.2 gemSpec_DM_ePA#A_14505-04

-> PHR-230 und PHR-510 für DiGA erweitern

**A_14505-06 - Event Codes für Protokollereignisse**
ePA-Produkttypen und Komponenten, die Ereignisse in einem Protokoll hinzufügen, MÜSSEN im Protokolleintrag für die jeweils aufgerufene Operation die Event Codes und den Display Name gemäß der folgenden Tabelle verwenden:

**Tabelle 14: Event Codes für Protokollereignisse**

| Operation | EventID.code | EventID.displayName |
|---|---|---|
| `I_Authentication_Insurant::loginCreateToken` | PHR-110 | Login des Versicherten (Authentisierung) |
| `I_Authentication_Insurant::logoutToken` | PHR-112 | Logout des Versicherten |
| `I_Authentication_Insurant::getAuditEvents` | PHR-120 | Abruf des Zugriffsprotokolls (Teil 1/3) aus der privaten Umgebung |

| | | |
|---|---|---|
| `I_Authentication_Insurant::getSignedAuditEvents` | PHR-121 | Abruf des signierten Zugriffsprotokolls (Teil 1/3) aus der privaten Umgebung |
| `I_Authorization_Insurant::getAuthorizationKey` | PHR-220 | Login des Versicherten/Vertreter (Abruf der Berechtigung) |
| `I_Authorization::getAuthorizationKey` | PHR-230 | Login aus der ärztlichen Umgebung, einer DiGA oder eines Kostenträgers |
| `I_Authorization_Management::putAuthorizationKey` | PHR-310 | Erteilung der Berechtigung aus der ärztlichen Umgebung |
| `I_Authorization_Management_Insurant::putAuthorizationKey` | PHR-410 | Erteilung der Berechtigung aus der privaten Umgebung |
| `I_Authorization_Management_Insurant::deleteAuthorizationKey` | PHR-420 | Löschen der Berechtigung aus der privaten Umgebung |
| Interner Prozess Löschen veralteter Berechtigungen | PHR-421 | Automatisches Löschen veralteter Berechtigungen durch das Aktensystem |
| `I_Authorization_Management_Insurant::replaceAuthorizationKey` | PHR-430 | Aktualisierung der Berechtigung aus der privaten Umgebung |
| `I_Authorization_Management_Insurant::getAuditEvents` | PHR-440 | Abruf des Zugriffsprotokolls (Teil 2/3) aus der privaten Umgebung |

| | | |
|---|---|---|
| I_Authorization_Management_Insurant::getSignedAuditEvents | PHR-441 | Abruf des signierten Zugriffsprotokolls (Teil 2/3) aus der privaten Umgebung |
| I_Authorization_Management_Insurant::putNotificationInfo | PHR-450 | Aktualisierung der Benachrichtigungsadresse aus der privaten Umgebung |
| Interner Prozess Support E-Mailadresse | PHR-451 | Änderung E-Mailadresse |
| I_Authorization_Management_Insurant::getNotificationInfo | PHR-452 | Abfrage der Benachrichtigungsadresse aus der privaten Umgebung |
| I_Authorization_Management_Insurant::getAuthorizationList | PHR-460 | Abruf der Liste der berechtigten Kontonutzer |
| Interner Prozess Geräteverwaltung | PHR-470 | Geräteverwaltung |
| I_Authorization_Management_Insurant::startKeyChange | PHR-480 | Initialer Schritt zum Start eines Umschlüsselungsvorgangs |
| I_Authorization_Management_Insurant::finishKeyChange | PHR-482 | Initialer Schritt zum Abschluss des Umschlüsselungsvorgangs |
| I_Document_Management::CrossGatewayDocumentProvide | PHR-510 | Hinzufügen eines Dokuments aus der ärztlichen Umgebung oder einer DiGA |
| I_Document_Management::CrossGatewayQuery | PHR-520 | Suchanfrage aus der ärztlichen Umgebung |
| I_Document_Management::RemoveDocuments | PHR-530 | Löschen eines Dokuments aus der ärztlichen |

| | | |
|---|---|---|
| | | Umgebung.<br><br>Hinweis (nicht protokolliert): in ePA2.0 entfallen |
| I_Document_Management::CrossGatewayRetrieve | PHR-540 | Abruf eines Dokuments aus der ärztlichen Umgebung |
| I_Document_Management::RestrictedUpdateDocumentSet | PHR-550 | Markierung eines Dokuments als leistungserbringeräquivalent aus der ärztlichen Umgebung<br><br>Hinweis (nicht protokolliert): in ePA2.0 entfallen |
| I_Document_Management::RemoveMetadata | PHR-560 | Löschen von Dokumenten oder Ordnern aus der ärztlichen Umgebung |
| I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b | PHR-610 | Hinzufügen eines Dokuments aus der privaten Umgebung |
| I_Document_Management_Insurant::RegistryStoredQuery | PHR-620 | Suchanfrage aus der privaten Umgebung |
| I_Document_Management_Insurant::RemoveDocuments | PHR-630 | Löschen eines Dokuments aus der privaten Umgebung.<br><br>Hinweis (nicht protokolliert): in ePA2.0 entfallen |

| | | |
|---|---|---|
| I_Document_Management_Insurant::RetrieveDocumentSet | PHR-640 | Abruf eines Dokuments aus der privaten Umgebung |
| I_Account_Management_Insurant::SuspendAccount | PHR-650 | Starten des Aktenkontowechsels zu einem neuen Anbieter aus der privaten Umgebung |
| I_Account_Management_Insurant::ResumeAccount | PHR-660 | Abschluss des Aktenkontowechsels zu einem neuen Anbieter aus der privaten Umgebung |
| I_Account_Management_Insurant::GetAuditEvents | PHR-670 | Abruf des Zugriffsprotokolls (Teil 3/3) aus der privaten Umgebung |
| I_Account_Management_Insurant::GetSignedAuditEvents | PHR-671 | Abruf des signierten Zugriffsprotokolls (Teil 3/3) aus der privaten Umgebung |
| I_Document_Management_Insurant::RemoveMetadata | PHR-680 | Löschen von Dokumenten, Ordnern aus der privaten Umgebung |
| I_Document_Management_Insurant::RestrictedUpdateDocumentSet | PHR-690 | Änderungen der Vertraulichkeitsstufe von Dokumenten aus der privaten Umgebung |
| I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b | PHR-710 | Hinzufügen eines Dokuments aus der Kostenträger-Umgebung |
| I_Key_Management_Insurant::StartKeyChange | PHR-810 | Start eines Umschlüsselungsvorgangs |

| | | |
|---|---|---|
| `I_Key_Management_Insurant::FinishKeyChange` | PHR-840 | Aufforderung zum Abschluss des Umschlüsselungsvorgangs durch den Versicherten |
| Interner Prozess: Rollback während des Umschlüsselungsvorgangs in Komponente Authorisierung | PHR-850 | Initialer Schritt zum Abbruch des Umschlüsselungsvorgangs (Wiederherstellung des alten Schlüsselmaterials) |
| Interner Prozess: Rollback während des Umschlüsselungsvorgangs in Komponente Dokumentenverwaltung | PHR-860 | Abbruch des Umschlüsselungsvorgangs (Wiederherstellung des alten Schlüsselmaterials) |
| Interner Prozess: Erfolgreicher Abschluss der Umschlüsselung in der Komponente Dokumentenverwaltung | PHR-870 | Erfolgreicher Abschluss des Umschlüssungsvorgangs durch den Versicherten |

**[<=]**

## 4.8 Sicherheit

Der Herausgeber der DiGA-SMC-B MUSS sicherstellen, dass der Antragsteller als Hersteller der digitalen Gesundheitsanwendung an geeigneter Stelle erklärt, dass er nur Daten der vom BfArM zugelassenen Gesundheitsanwendung in die ePA einstellen wird.

## 4.9 Betrieb

Es werden keine gesonderten Anforderungen an den Betrieb einer DiGA als ePA-Client erhoben. Die DiGA wird aus betrieblicher Sicht wie ein Leistungserbringer behandelt.

## 4.10 Test

Es werden keine gesonderten Anforderungen an den Test der UseCases der DiGA erhoben.

# 5 Änderungen an Produkt- und Anbietertypsteckbriefen

# 6 Anhang A – Verzeichnisse

## 6.1 Abkürzungen

| Kürzel | Erläuterung |
|---|---|
| BfArM | Bundesinstitut für Arzneimittel und Medizinprodukte |
| DiGA | Digitale Gesundheitsanwendung |
| DiGAV | Digitale-Gesundheitsanwendungen-Verordnung |
| DVPMG | Gesetz zur digitalen Modernisierung von Versorgung und Pflege |
| ePA-FdV | ePA-Frontend des Versicherten |
| FHIR | Fast Healthcare Interoperability Resources |
| KBV | Kassenärztliche Bundesvereinigung |
| MDR | Medical Device Regulation |
| MIO | Medizinisches Informationsobjekt |
| OID | Object-Identifier (dient zur eineindeutigen Referenzierung zu Objekten |
| SMC-B ORG | Secure Module Card vom Type B für Organisationen |
| PS | Primärsystem |

## 6.2 Referenzierte Dokumente

### 6.2.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der

aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

| [Quelle] | Herausgeber: Titel |
|---|---|
| [gemGlossar] | gematik: Glossar der Telematikinfrastruktur |
| [gemRL_SMC-B_ORG_AP] | gematik: Richtlinie für die Herausgabe der SMC-B ORG |
| [gemRL_SMC-B_ORG_BP] | Berechtigungsgrundlagen zur Beantragung und zum Erhalt der SMC-B ORG |
| [gemSpec_DM_ePA] | gematik: Datenmodell ePA |
| [gemSpec_Dokumentenverwaltung] | gematik: Dokumentenverwaltung ePA |
| [gemSpec_FdV_ePA] | gematik: Spezifikation ePA-Frontend des Versicherten |
| [gemSpec_OID] | gematik: Spezifikation Festlegung von OIDs |
| [gemSpec_PKI] | gematik: Übergreifende Spezifikation PKI |
| [gemSpec_SGD_ePA] | gematik: Spezifikation Schlüsselgenerierungsdienst ePA |

### 6.2.2 Weitere Dokumente

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
|---|---|
| | |
| | |

# 7 Anhang B – Anmerkungen aus der Industrie

# 8 Anhang C – Offene Punkte, Fragen

1. Offener Punkt: Der Typ einer SMC-B für DiGAs ist aktuell vor dem Hintergrund des Kabinettentwurf zum PDSG nicht abschließend festgelegt. Als eine geeignete Ausprägung einer SMC-B kann die SMC-B ORG angesehen werden.
2. Gibt es keine speziellen Einschränkungen für Zugriffsrechte bei gesonderten Berufsgruppen?
3. Soll beim Berechtigen einer DiGA durch den Versicherten festlegbar sein, welche Berechtigungsstufe die Dokumente der DiGA haben dürfen? Ist die DiGA-Nutzung beim Leistungserbringer praktikabel, wenn zugelassen wird, dass der Versicherte DiGA-Daten als vertraulich kennzeichnet? Soll eine Berechtigungsstufe (z.B. normal) vorgeschrieben werden?
4. Das "DiGA-MIO", d.h. die Festlegung der strukturierten Daten einer Digitalen Gesundheitsanwendung, ist noch nicht entwickelt worden.
5. Änderungen an der Architektur der TI, die in der Ausbaustufe ePA 3 enthalten sein werden, sind aktuell noch nicht abschließend spezifiziert.