Elektronische Gesundheitskarte und Telematikinfrastruktur

Feature: Anbindung Digitaler Gesundheitsanwendungen an die elektronische Patientenakte

Version:	1.0.0 CC
Revision:	352132
Stand:	30.03.2021
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

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
- medizinische 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 7 SGB V-E bis zum 1. 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 betroffenen 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 auf seinem mobilen Endgerät 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): "Daten, die der Versicherte seiner Krankenkasse für die Nutzung in zusätzlichen von der Krankenkasse angebotenen Anwendungen nach § 345 Abs. 1 Satz 1 SGB V zur Verfügung stellen kann".

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 strukturiert oder auch als ein von der KBV spezifiziertes sogenanntes Medizinisches Informationsobjekt (MIO) als FHIR-Ressource (DiGA-MIO) definiert worden sein. Für jede DiGA 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 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 maximalen 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 Kabinettentwurfs 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 Gesundheitsanwendungen 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>`

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 Berechtigungsverwaltung

4.1.1 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	CRUD	CRUD	R	CRUD	R	R	R	CRUD	R	-	RDM	-
1a2	hospital	CRUD	CRUD	R	CRUD	R	R	R	CRUD	R	-	RDM	-
1a3	laboratory	CRUD	CRUD	R	CRUD	R	R	R	CRUD	R	-	RDM	--
1a4	physiotherapy	CRUD	CRUD	R	CRUD	R	R	CRUD	CRUD	R	-	RDM	-
1a5	psychotherapy	CRUD	CRUD	R	CRUD	R	R	R	CRUD	R	-	RDM	-
1a6	dermatology	CRUD	CRUD	R	CRUD	R	R	R	CRUD	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	CRU D	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 DiGA an der professionOID der DiGAs und als eine bestimmte DiGA anhand der Telematik-ID identifiziert wird, für diese DiGA den folgenden Ordner für den Versicherten anlegen:

- DiGA-Ordner der Kategorie 9 gemäß A_20190-01 in gemSpec_DM_ePA (Belegung `Folder.codeList`) unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in gemSpec_DM_ePA#A_14760-01 (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.

[<=]

A_21514 - Komponente ePA-Dokumentenverwaltung - Prüfung der FolderUniqueID
Die Komponente ePA-Dokumentenverwaltung MUSS nach dem erstmaligen Einstellen eines Dokumentes in die Akte des Versicherten (`Operation I_Document_Management::CrossGatewayDocumentProvide()`) durch eine bestimmte DiGA, sicherstellen, dass im nachfolgenden Request die beim erstmaligen Einstellen der DiGA durch die mittels Telematik-ID identifizierte DiGA verwendete FolderUniqueID verwendet wird. Dabei MUSS auf die Identität des authentifizierten Nutzers (Telematik-ID des übergebenen Zertifikats der Client-Authentisierung) geprüft werden. Falls die Komponente ePA-Dokumentenverwaltung feststellt, dass die durch die Telematik-ID identifizierte DiGA in einem anderen Submissionset eine andere FolderUniqueID als die aktuell benutzte FolderUniqueID verwendet hatte, MUSS sie den Request mit einem `XDSRepositoryMetadataError` quittieren.
[<=]

Weitere Änderungen in gemSpec_Dokumentenverwaltung:

- Einfügen einer neuen statischen PermissionPolicy in das Kapitel 9.5, analog zu 9.5.8, aber mit "diga" statt "epa", aus dem Codesystem "1.2.276.0.76.5.512".
- Einfügen in das Kapitel 9.3 einer Zeile für "diga" in die Auflistung der mittelgranularen Berechtigungen, analog zur Zeile für ega.
- Einfügen in das PolicySet zur Blacklist/whitelist: "Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "`diga`" erteilt werden soll, und dann den Wert "`urn:gematik:policy-id:permissions-access-group-hcp:categories:diga`" besitzen."

4.1.2 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.

405 **Tabelle 2: Tab_DM_Dokumentenkategorien**

Nr	Dokumentenkategorie	technischer Identifier	Metadatenvorgaben
1a1	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_20190-01 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

[<=]

Kapitel 5.2.2

Aufnahme in die extensionale Aufzählung enthaltener Codes:

Code=diga, CodeSystem=1.2.276.0.76.5.512, Anzeigename=Digitale Gesundheitsanwendung (diga), Beschreibung= Die Kategorie kann für Dokumente vergeben werden, die aus einer digitalen Gesundheitsanwendung importiert worden sind.

4.1.3 gemSpec_FM_ePA

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_16212-03 (neu: A_16212-04), 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.

4.1.4 gemSpec_Zugangsgateway_Vers

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

- Der LDAP-Proxy DARF NICHT Fachdaten an das anfragende ePA-Modul Frontend des Versicherten (ePA-Modul FdV) zurückgegeben, es sei denn, die Daten sind zur Ermittlung von DiGA-Einträgen erforderlich.
- 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.

4.1.5 gemSpec_VZD

Tab_VZD_Mapping_Eintragstyp_und_ProfessionOID, Hinzufügen der Reihe:

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

4.1.6 gemSpec_ePA_FdV

4.1.6.1 Neues Kapitel nach 6.2.7.6: Berechtigungen für DiGA am FdV 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 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 organizationName (Name des DiGA-Herstellers) und commonName (Name der DiGA) erfolgen.

Das Verschlüsselungszertifikat im Ergebnis der Abfrage beinhaltet die Telematik-ID (siehe [gemSpec_PKI#Tab_SMCB_TID_GKVSV) 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_XXX umsetzen.

Tabelle 3: TAB_FdV_XXX – Berechtigung an Kostenträger 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. Ein Verschlüsselungszertifikat, die Telemantik-ID des DiGA-Herstellers und der Name der DiGA sind bekannt. Der Nutzer hat die Vergabe der Berechtigung bestätigt.
Nachbedingung	Die DiGA ist zum Zugriff auf das Aktenkonto berechtigt. Das notwendige Schlüsselmaterial ist in der Autorisierung hinterlegt. Ein Policy Document für die DiGA ist in der Dokumentenverwaltung hinterlegt.
Standardablauf	Aktivitäten im Standardablauf 1. AuthorizationKey für DiGA erstellen 2. Schlüsselmaterial im ePA-Aktensystem speichern 3. Policy Document für DiGA erstellen 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.**[<=]**

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: Name des DiGA-Herstellers und Name der DiGA

anzeigen.
[<=]

4.1.6.2 Neues Kapitel nach 6.2.7.9.4: Berechtigung für DiGA löschen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter einer 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 übergreifenden 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_166 umsetzen.

Tabelle 4: TAB_FdV_166 – 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. Der Nutzer hat eine DiGA zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt. 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 1. Policy Document in Dokumentenverwaltung löschen 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.**[<=]**

4.1.6.3 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.

4.1.6.4 Kapitel 6.2.3.7 Vergebene Berechtigung bestimmen

Berechtigung für Vertreter: Versicherten-ID, Name des Vertreters

Berechtigung für KTR: Telematik-ID, Name des KTR

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

Berechtigung für DiGA: Telematik-ID

4.1.6.5 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.

4.1.6.6 Kapitel 6.2.3.8 AuthorizationKey

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

4.1.6.7 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 heute + 100 Jahre 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 Anbieter wechseln	Versicherter	Verschlüsseln	[gemSpec_SGD_ePA#2.4 Initiale Schlüsselableitung für den Kontoinhaber]
Berechtigung für LEI vergeben Berechtigung für DiGA vergeben Vertretung einrichten Berechtigung für Kostenträger	Versicherter	Verschlüsseln	[gemSpec_SGD_ePA#2.6 Schlüsselableitung für einen Berechtigungsempfänger]

vergeben Berechtigung für LEI ändern			
Berechtigung für LEI vergeben Berechtigung für DiGA vergeben Berechtigung für Kostenträger vergeben Berechtigung für LEI ändern	Vertreter	Verschlüsseln	[gemSpec_SGD_ePA#2.8 Schlüsselableitung für einen Berechtigungsempfänger durch einen Vertreter]
Login	Versicherter Vertreter	Entschlüsseln	Für das Entschlüsseln müssen keine Anwendungsfälle für SGD unterschieden werden. Es wird das Element AssociatedData des ermittelten AuthorizationKey für den Aufruf der Operation KeyDerivation beim SGD wie folgt verwenden: `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 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.

4.2.1 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 "Provide and Register Document Set-b" [ITI-41] erfolgen.
[<=]

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.

4.2.2 gemSpec_DM_ePA

A_14760-07 (neu: A_14760-08), Tabelle Nutzungsvorgaben für Metadatenattribute XDS.b:

Umbenennung Spalte "PS" in "PS/DiGA", Änderung folgender Nutzungsvorgaben:

- author: Die DiGA MUSS mindestens das Subattribut authorPerson und 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 jede DiGA pro Versicherten bei jedem Aufruf immer gleich sein.

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) - 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 authorInstitution für DIGAs
Die DiGA sowie die ePA-Produkttypen, welche IHE ITI XDS-Metadaten verarbeiten, MÜSSEN 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

[<=]

4.2.3 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

4.3 Nutzung von DiGA-Daten beim Leistungserbringer

4.3.1 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.

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 SOLL DiGA-Daten, deren Formatvorgabe interoperabel gestaltet sind, bei vorliegender Berechtigung aus dem ePA-Aktensystem des Versicherten auslesen und anzeigen können.**[<=]**

4.4 Umschlüsselung

4.4.1 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. Die Akte befindet sich im Zustand "ACTIVATED".
Nachbedingung	1. Neuer Aktenschlüssel ist erzeugt 2. Neuer Kontextschlüssel ist erzeugt. 3. Für jeden Berechtigten sind neue SGD1 und SGD2 Schlüssel erzeugt 4. Für alle Berechtigten sind der neue Akten- und der neue Kontextschlüssel mit den neuen SGD Schlüsseln geschützt in der Autorisierungskomponente hinterlegt. 5. Alle Dokumentenschlüssel in der Dokumentenverwaltungskomponente sind mit dem neuen Aktenschlüssel umgeschlüsselt. 6. Die Akte befindet sich im Zustand "ACTIVATED". 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 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. 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. 2. Das FdV generiert einen neuen Akten- und einen neuen Kontextschlüssel wie in gemSpecFdv#6.2.5.1. beschrieben. 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. 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()`.
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.
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.
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. 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. 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. 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. 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.

[<=]

4.5 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.

4.6 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.

4.7 Test

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

5 Beispiele und Referenzimplementierungen

Diesem Feature sind keine Beispiele oder Referenzimplementierungen beigefügt.

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 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. Der Code "diga" für das Code-System "1.2.276.0.76.5.512" solltein das offizielle IHE-D XDS ValueSet registriert werden.
4. 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?
5. Das "DiGA-MIO", d.h. die Festlegung der strukturierten Daten einer Digitalen Gesundheitsanwendung, ist noch nicht entwickelt worden.
6. Änderungen an der Architektur der TI, die in der Ausbaustufe ePA 3 enthalten sein werden, sind aktuell noch nicht abschließend spezifiziert.