Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation ePA-Frontend des Versicherten

Version:	3.0.0 CC
Revision:	1755849
Stand:	15.10.2026
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_ePA_FdV

Dokumenteninformation

Gender-Hinweis
Aus Gründen der besseren Lesbarkeit wird in diesem Dokument überwiegend die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.50.0	06.04.2022		**ePA-Stufe 2.5:**gemF_ePA_DiGA_Anbindung, gemF_ePA_FDZ_Anbindung und gemF_ePA_Gesundheitsportal	gematik
1.50.1	23.05.2022		Einarbeitung Kommentierung	gematik
1.51.0	25.07.2022		Änderungsliste ePA_Maintenance_22.2, redaktionell: diskriminierungsfreie Sprache (Black-/Whitelist in Deny-/Allowlist)	gematik
1.51.1	17.08.2022		Anpassung zur Einarbeitung Änderungsliste ePA_Maintenance_22.2 nach weiteren Abstimmungen	gematik
1.52.0	12.04.2023		Einarbeitung ePA_Maintenance_23.1	gematik
2.0.0	30.01.2024		Einarbeitung ePA für alle	gematik
2.1.0	28.03.2024		ePA für alle - Release 3.0.1	gematik
2.2.0	12.07.2024		ePA für alle - Release 3.0.2	gematik
2.3.0	14.08.2024		ePA für alle - Release 3.1.0	gematik
2.3.1	16.08.202		red. Anpassungen	gematik

	4			
2.4.0	28.02.2025		ePA für alle - Release 3.0.5	gematik
2.5.0	27.05.2025		ePA für alle - Release 3.1.2	gematik
2.5.1	12.09.2025		ePA für alle - Release 3.1.3 (inkl.Release 3.1.2-1)	gematik
2.6.0	15.12.2025		ePA für alle - Release 3.1.3-1	gematik
2.7.0	20.03.2026		ePA für alle - Release 3.1.3-2	gematik
2.8.0	14.07.2026		ePA für alle - ePA_3_1_3-4	gematik
3.0.0 CC	15.10.2026		ePA 27	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes 7
1.1 Zielsetzung 7
1.2 Zielgruppe 7
1.3 Geltungsbereich 7
1.4 Abgrenzungen 7
1.5 Methodik 8
2 Systemüberblick 9
3 Systemkontext 10
3.1 Akteure und Rollen 10
3.2 Nachbarsysteme 11
3.2.1 Identität des Nutzers 12
4 Zerlegung des Produkttyps 13
5 Übergreifende Festlegungen 14
5.1 Datenschutz und Sicherheit 15
5.1.1 Anforderungen bei CC-Zertifizierung 24
5.2 Verwendete Standards 25
5.3 Integrating the XDS of Healthcare Enterprise IHE 25
5.4 Benutzeroberfläche 26
5.4.1 Visuelle Darstellung 26
5.4.2 Benutzerführung 26
5.4.2.1 Technische Normen und Verordnungen zur Beachtung 27
5.4.3 Anzeige von Dokumenten 30
5.4.4 Drucken und Speichern von Verwaltungs- und Inhaltsdaten 31
5.4.5 Sammlungen 31
5.4.5.1 Weiterentwicklung bzw. Ablösung von Sammlungen 32
5.4.6 Nutzungsvorgaben für IHE ITI XDS-Metadaten 33
5.4.6.1 Metadaten für einzustellende Dokumente 33
5.4.7 Konfiguration des ePA-Frontend des Versicherten 34
5.5 Bereitstellung für UX-Messdaten 37
6 Funktionsmerkmale 39
6.1 Allgemein 39
6.1.1 Kommunikation mit dem ePA-Aktensystem 39
6.1.2 Sicherer Kanal zur Aktenkontoverwaltung 40
6.1.3 Authentisierung 41
6.1.4 Geräteregistrierung 42
6.1.5 Zertifikatsprüfung 43
6.1.6 Dokumente 44
6.1.7 ePA-FdV für Desktop-Plattformen 44

6.1.8 Anbindung an das Nationale Gesundheitsportal....45
6.1.9 Anbindung VZD-FHIR-Directory....45
6.1.10 Dokumente für den statischen Ordner "technical"....46
6.2 Implementation ePA-Anwendungsfälle im FdV....46
6.2.1 Übergreifende Festlegungen....46
6.2.2 Fehlerbehandlung....46
6.2.3 Aktivitäten....47
6.2.3.1 Authentisieren des Nutzers....47
6.2.3.2 Leistungserbringerinstitution im Verzeichnisdienst der TI finden....48
6.2.3.3 DiGA im Verzeichnisdienst der TI finden....50
6.2.3.4 Land (EU-Zugriff) im Verzeichnisdienst der TI finden....50
6.2.4 Nutzerzugang ePA....51
6.2.4.1 Login User....51
6.2.4.2 Logout User....53
6.2.5 Aktenkontoverwaltung....53
6.2.5.1 Widersprüche für Funktionen der ePA verwalten....53
6.2.5.2 Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke....55
6.2.5.3 Widerspruch gegen die Nutzung der ePA durch eine spezifische LEI....56
6.2.5.4 Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI....57
6.2.6 Befugnisverwaltung....57
6.2.6.1 Befugnisverwaltung für LEI....59
6.2.6.2 Befugnisverwaltung für DiGA....59
6.2.6.3 Vertretung verwalten....60
6.2.6.4 Vergebene Befugnisse anzeigen....62
6.2.6.5 Eingerichtete Vertretungen anzeigen....62
6.2.6.6 Befugnisverwaltung EU-Zugriff....62
6.2.7 Verbergen und Sichtbarmachen von Dokumenten....65
6.2.7.1 Kategorienbasiertes Verbergen von Dokumenten....66
6.2.7.2 Dokumentenspezifisches Verbergen von Dokumenten....67
6.2.8 Medical Services....68
6.2.8.1 Document Services....68
6.2.8.1.1 Dokumente einstellen....69
6.2.8.1.2 Dokumente suchen....70
6.2.8.1.3 Dokument herunterladen....71
6.2.8.1.4 Dokumente im Aktenkonto löschen....72
6.2.8.1.5 Metadaten von Dokumenten ändern....73
6.2.8.2 Medication Service....73
6.2.8.3 MHD Service....74
6.2.8.4 Patient Service....74
6.2.9 Protokollverwaltung....74
6.2.10 Geräteverwaltung....74
6.2.11 Verwaltung von E-Mail-Adressen....75
6.2.12 Push Notification....76
6.2.12.1 FdV-Instanz registrieren....76
6.2.12.2 Channel für FdV-Instanz konfigurieren....76
6.2.12.3 Push Notification Historie....77
6.3 Testtreiber-Modul für ePA-Frontend des Versicherten....77
7 Verteilungssicht....78

8 Anhang A – Verzeichnisse 79
8.1 Abkürzungen 79
8.2 Glossar 80
8.3 Abbildungsverzeichnis 80
8.4 Tabellenverzeichnis 81
8.5 Referenzierte Dokumente 81
8.5.1 Dokumente der gematik 81
8.5.2 Weitere Dokumente 84

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps ePA-Frontend des Versicherten.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller von Produkten des Frontend des Versicherten sowie an Hersteller und Anbieter von weiteren Produkttypen der Fachanwendung ePA.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. gemPTV_ATV_Festlegungen, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

Im Dokument wird spezifiziert, wie Schnittstellen benutzt werden, um fachliche Anwendungsfälle umzusetzen. Die Schnittstellen selbst werden in der Spezifikation desjenigen Produkttypen beschrieben, der die Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang 9.5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten. Diese sind in dem Produkttypsteckbrief des Produkttyps ePA-Frontend des Versicherten verzeichnet.

1.5 Methodik

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.

Sie werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

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

Die Spezifikation der durch den Produkttyp genutzten Interfaces erfolgt in der Spezifikation des Produkttypen, welcher das Interface anbietet. Eine Übersicht befindet sich in Kapitel "3.2- Nachbarsysteme".

2 Systemüberblick

Das ePA-Frontend des Versicherten (FdV) ist eine Anwendung, welche die für die Nutzung der ePA notwendigen Funktionalitäten bündelt und dezentrale Fachlogik der Fachanwendung ePA ausführt. Das FdV ermöglicht es Versicherten, ePA-Anwendungsfälle auszuführen.

Ausführungsumgebung des FdV ist ein Gerät des Versicherten (GdV), bspw. ein stationäres Gerät oder ein mobiles Endgerät. Es steht unter alleiniger Kontrolle des Versicherten. Dem Versicherten obliegt es, durch geeignete Maßnahmen die Sicherheit der Daten zu stärken.

Das FdV kann zusätzliche Funktionalitäten anbieten, die nicht der Fachanwendung ePA zugeordnet werden und somit nicht der Regelungshoheit der gematik unterliegen.

3 Systemkontext

Das Grobkonzept der "ePA für alle", siehe [gemKPT_ePAfuerAlle], beschreibt wesentliche Kernmechanismen, Basisfunktionalitäten sowie technische Konzepte zu den Diensten des ePA-Aktensystems und den beteiligten Client-Systemen der Fachanwendung ePA.

3.1 Akteure und Rollen

Im Systemkontext des FdV interagieren verschiedene Akteure (aktive Komponenten) in unterschiedlichen Rollen mit dem FdV.

Tabelle 1: Akteure und Rollen

Akteur	Rolle	Beschreibung
Nutzerdes FdV	Versicherter (als Aktenkontoinhaber) oder Vertreter eines Versicherten	Primärer Anwender, Ausführen von fachlichen Anwendungsfällen mit Zugriff auf ein ePA-Aktensystem
Ausführungsumgebung	Gerät des Versicherten	Betriebs-/Ablaufumgebung des FdV
Anbieter ePA-Aktensystem	Organisatorisch, kein Akteur in der Ausführung von ePA-Anwendungsfällen	Der Anbieter stellt Informationen bereit, um sich via FdV am ePA-Aktensystem anzumelden.
Hersteller ePA-Frontend des Versicherten	Organisatorisch, kein Akteur in der Ausführung von ePA-Anwendungsfällen	Der Hersteller FdV stellt im Handbuch Informationen bereit bezüglich • Anforderungen an die Ausführungsumgebung • Möglichkeiten zur Anbindung der GesundheitsID Der Hersteller FdV erfüllt sicherheitstechnische Anforderungen zum Herstellungsprozess.

3.2 Nachbarsysteme

Die vom FdV direkt erreichbaren Produkttypen der TI sind

- ePA-Aktensystem,
- Signaturdienst
- Verzeichnisdienst FHIR-Directory

Der Signaturdienst bietet die Schnittstelle `I_Remote_Sign_Operations` für Signaturen an. Siehe [gemSpec_SigD].
In der folgenden Tabelle sind die Schnittstellen des ePA-Aktensystems gelistet, welche durch das ePA-Frontend des Versicherten genutzt werden.

Tabelle 2: Schnittstellen des ePA-Aktensystems

Schnittstelle	Operationen
I_Authorization_Service	Operationen siehe [I_Authorization_Service]
I_Consent_Decision_Management	Operationen siehe [I_Consent_Decision_Management]
I_Constraint_Management_Insurant	Operationen siehe [I_Constraint_Management_Insurant]
I_Device_Management_Insurant	Operationen siehe [I_Device_Management_Insurant]
I_Document_Management_Insurant	Operationen siehe [XDSDocumentService]
I_Email_Management	Operationen siehe [I_Email_Management]
I_Entitlement_Management	Operationen siehe [I_Entitlement_Management]
I_Entitlement_Management_EU	Operationen siehe [I_Entitlement_Management_EU]
I_Push_Notification_Management	Operationen siehe [I_Push_Notification_Management]
ePA Audit Event Service	Operationen siehe [gemIG_ePA_Basic]
ePA Medication Service	Operationen siehe gemäß [gemIG_ePA_Medication]
ePA Patient Service	Operationen siehe [gemIG_ePA_Basic]
ePA MHD Service	Operationen siehe [gemIG_ePA_MHD]

3.2.1 Identität des Nutzers

Ein Nutzer des FdV in seiner Rolle als Versicherter oder Vertreter verwendet die GesundheitsID für die Authentisierung gegenüber dem ePA-Aktensystem. Mit dieser digitalen Identität meldet sich der Versicherte an den Diensten der ePA sowie weiteren Diensten der TI an.

Das ePA-Aktensystem etabliert hierzu einen Authorization Server welcher als OpenID Relying-Party (Client) Mitglied der TI-Föderation ist.

Nach initialem Login-Request des FdV (unter Signalisierung des zu verwendenden Identity Provider (IDP) authentisiert sich der Authorization Server gegenüber dem für den Versicherten zuständigen sektoralen IDP. Anschließend leitet er einen Authentication Request über das ePA Frontend an die Authenticator-Modul Komponente des IDP innerhalb des FdV.

Das Authenticator-Modul realisiert die Authentisierung des Versicherten mittels eGK, online Ausweisfunktion oder weiteren zulässigen Verfahren des IDP. Anschließend wird über das FdV der sogenannte Authorization_Code an den Authorization Server des Aktensystems gesendet.

Dieser authentisiert sich nun erneut gegenüber dem sektoralen IDP und tauscht den Authorization_Code gegen ein verschlüsseltes ID_TOKEN mit den personenbezogenen Daten des Versicherten ein.

Diese Daten können anschließend der etablierten VAU/User Session zugeordnet werden und signalisieren dem Aktensystem die Identität des Nutzers.

4 Zerlegung des Produkttyps

Im Folgenden wird die Zerlegung des Produkttyps ePA-Frontend des Versicherten dargestellt, welche für die Übersicht der funktionalen Leistungsmerkmale in der vorliegenden Spezifikation nötig ist.

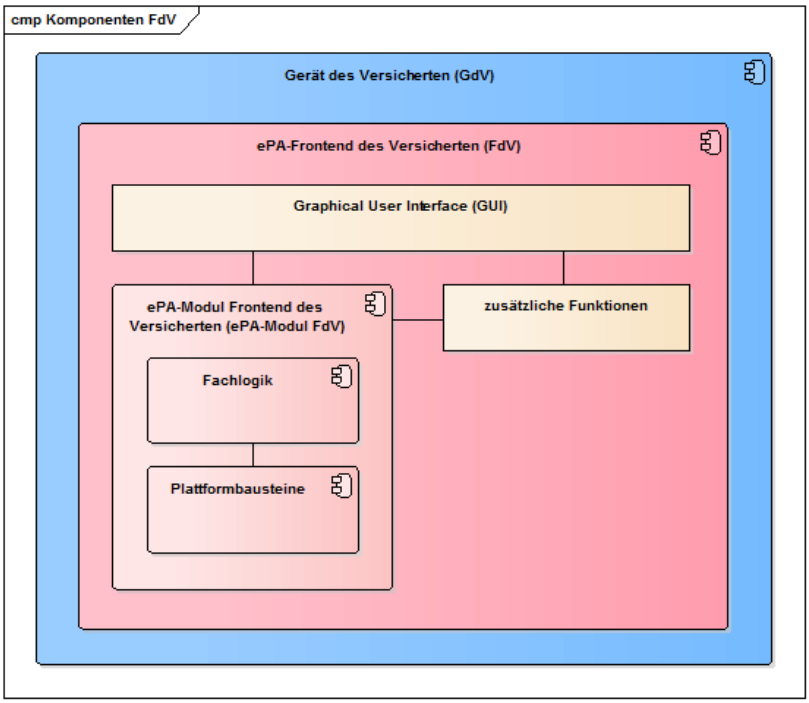


Abbildung 1: Komponenten ePA-Frontend des Versicherten

Tabelle 3: Komponenten des FdV

Komponente	Verantwortung und Funktionalität	Spezifiziert in
Fachlogik	Die Komponente steuert die Anwendungsfälle entsprechend den fachanwendungsspezifischen Festlegungen.	Kap. 6.2

Das für die Nutzung des ePA-Frontend des Versicherten notwendige GUI ist Teil des FdV und wird nicht normativ durch die Spezifikation des FdV vorgegeben.

Das FdV kann zusätzliche Funktionen beinhalten, hierzu zählen Module/Funktionen (z.B. Authenticator-Modul, weitere fachliche Anwendungen der gematik) und bspw. kassenspezifische Funktionen, welche Schnittstellen zu kassenspezifischen Diensten außerhalb der TI nutzen.

Das ePA-Frontend des Versicherten besitzt eine produktspezifische anwendungsinterne Schnittstelle, welche durch das GUI oder die zusätzlichen Funktionalitäten der integrierenden Anwendung genutzt werden kann, um ePA-Anwendungsfälle auszuführen.

5 Übergreifende Festlegungen

Das ehemalige ePA-Modul FdV wurde als eigenständiges Objekt der Produktzulassung vollständig abgelöst vom ePA-Frontend des Versicherten (also der Gesamt-App). Das sollte durch die Verfahrensbeschreibung und den Aufbau sowie die Bezeichnung der Produkttypsteckbriefe eindeutig und normativ dargestellt sein. Das heißt, prinzipiell richten sich alle Anforderungen des Produkttypsteckbriefs an die gesamte ePA-App bzw. an deren Entwicklungsprozess. Der Nachweis zur Erfüllung der Anforderungen erfolgt dabei im Einzelnen folgendermaßen:

- Die Menge der Anforderungen zur funktionalen Eignung, deren Erfüllung im Produkttest bzw. Produktübergreifenden Test nachzuweisen ist, entspricht weitgehend der, die ursprünglich dem ehemaligen ePA-Modul zugeordnet war. Es handelt sich um die Vorgaben an die Funktionalität für den Zugriff auf die ePA (die Komponenten der TI).
- Die Menge der Anforderungen zur funktionalen Eignung, deren Erfüllung durch Herstellererklärung zu belegen ist, umfasst nunmehr auch Anforderungen, die bisher nur mittelbar durch das Verfahren der Bestätigung der Entwicklungsprozesse an die gesamte App gestellt wurden. Dabei handelt es sich beispielsweise um elementare Anforderungen an die Nutzerinteraktion (Anzeige etc.).
- Die Anforderungen der sicherheitstechnischen Eignung, deren Erfüllung im Produktgutachten bzw. in der CC-Evaluierung nachzuweisen ist, richten sich an die gesamte App – der Betrachtungsgegenstand der Prüfung ist die gesamte App einschließlich der von der gematik nicht spezifizierten Funktionalität.
- Die Herstellererklärung zur sicherheitstechnischen Eignung bezieht sich auf die Erfüllung von Anforderungen an die gesamte App.
- Die Anforderungen zur Sicherheitsbegutachtung entsprechen denen, die nach dem bisherigen Verfahren in der Bestätigung der sicheren Entwicklungsprozesse des Herstellers nachgewiesen wurden.

Die Gesamtmenge der Anforderungen, die sich aus der Zusammenführung der Produktzulassung und der Bestätigung der Entwicklungsprozesse des Herstellers ergibt, ist im Wesentlichen unverändert geblieben.

Leistungserbringerinstitutionen

Der Begriff Leistungserbringerinstitutionen (LEI) umfasst in diesem Dokument alle Nutzergruppender TI, welche durch eine TelematikID eindeutig adressiert werden und eine professionOID gemäß A_24463* (außer oid_diga) besitzen.

Digitale Gesundheitsanwendung

Eine Digitale Gesundheitsanwendung (DiGA) wird durch eine TelematikID eindeutig adressiert und ist mit der professionOID mit dem Wert oid_diga gekennzeichnet.

Land (EU-Zugriff)

Land (EU-Zugriff) bezeichnet ein Land, welches zu den beteiligten EU-Mitgliedsstaaten gehört, die die Bereitstellung der Gesundheitsdaten (z.B. ePA-ePS - ePA European Patient Summary) für autorisierte Leistungserbringer im EU-Ausland (LE-EU) unterstützen.

5.1 Datenschutz und Sicherheit

In diesem Kapitel werden übergreifende Anforderungen beschrieben, die sich aus den Themenfeldern Datenschutz und Sicherheit ergeben.

Für das ePA-FdV ist die Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten“ des BSI [BSI PVePAeRp] einzuhalten.“

A_24960-01 -ePA-Frontend des Versicherten: Konvertieren von PDF in PDF/A
Das ePA-Frontend des Versicherten MUSS Dokumente im PDF-Format, die in das Aktenkonto eingestellt werden sollen, automatisch in ein erlaubtes PDF/A-Format konvertieren bzw. durch das Aktensystem konvertieren lassen und ausschließlich das Dokument im PDF/A-Format in das Aktenkonto übermitteln.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Die im ePA-Aktensystem erlaubten Formate sind durch A_25233 definiert.

A_25457 -ePA-Frontend des Versicherten: Konvertieren von PDF im Aktensystem
Das ePA-Frontend des Versicherten KANN für die Konvertierung von Dokumenten im PDF-Format in das PDF/A-Format die Operation `convertPDF` gemäß [I_Tool_Convert_PDF_Insurant] verwenden.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25693 -ePA-Frontend des Versicherten: Anzeige von konvertierten PDF-Dokumenten
Das ePA-Frontend des Versicherten MUSS das Ergebnis eines konvertierten PDF-Dokuments vor dem Einstellen in das Aktenkonto dem Nutzer anzeigen.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Hinweis: Die Anzeige eines konvertierten PDF-Dokuments für den Nutzer ist erforderlich, da sich durch die Konvertierung Unterschiede im Layout ergeben können.

Zur Verbesserung der UX im ePA FdV ist die Umsetzung von A_25693 eine akzeptable Lösung, wenn dem Versicherten eine Möglichkeit zur Konfiguration am FdV angeboten wird. Der Versicherte kann somit nach ausreichender Belehrung worin die Risiken der Konvertierung liegen auf die zukünftige Anzeige des Ergebnisses der PDF/A-Konvertierung verzichten.
Eine andere Möglichkeit der Umsetzung von A_25693 ist beispielsweise eine Übersichtsseite, über die im nächsten Schritt einzustellenden bereits konvertierten Dokumente, mit den notwendigen Informationen/Risiken für den Versicherten und der Möglichkeit diese konvertierten Dokumente vor dem Upload einzusehen.

A_16973-01 -ePA-Frontend des Versicherten: lokale Ausführung
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass alle ePA-fachanwendungsspezifischen Anteile lokal auf dem Gerät des Versicherten ausgeführt werden.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Der auszuführende Code für die ePA-Funktionen des ePA-FdV muss lokal vorliegen und ausgeführt werden, so dass insbesondere alle ePA-Daten (medizinische Daten, sicherheitskritische Daten wie Schlüssel) ausschließlich lokal verarbeitet werden. Zudem erschwert es Administratoren von Servern, auf denen der Code liegen könnte, den Code zu manipulieren.

Dies bedeutet insbesondere, dass eine Auslagerung von ePA-Funktionen auf Webserver nicht erlaubt ist. Dies verhindert jedoch nicht, das ePA-FdV mithilfe von Webtechnologien umzusetzen, um eine Plattformunabhängigkeit zu erreichen. Mithilfe des Frameworks *Electron* können beispielsweise in HTML, CSS und JavaScript entwickelte Anwendungen lokal unabhängig vom verwendeten Betriebssystem (Windows, MacOS, Linux) ausgeführt werden. *Electron* bietet auch die Möglichkeit der Nutzung von *WebAssembly*.

A_15251-01 -ePA-Frontend des Versicherten: Anforderungen an Ausführungsumgebung
Der Hersteller des ePA-Frontend des Versicherten MUSS den Nutzer über die Annahmen und Anforderungen seines Produktes an das Gerät, auf dem das ePA-FdV läuft, sowie über den Bezug des Produkts aus vertrauenswürdigen App Stores informieren.
[Frontend_Vers_ePA,Sich.techn. Eignung: Herstellererklärung,<=**]**

Die Annahmen und Anforderungen sollen insbesondere Hinweise enthalten, mit welchen Maßnahmen der Nutzer seine Ausführungsumgebung sicher gestalten kann.

A_21235 -ePA-Frontend des Versicherten: Versicherten über Konsequenzen der Datenfreigabe informieren
Der Hersteller des ePA-Frontend des Versicherten MUSS den Nutzer darüber informieren, dass das Erteilen einer Zugriffsberechtigung auf Daten für Leistungserbringer mit einem Speichern dieser Daten in der Umgebung des Leistungserbringers verbunden sein kann.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_17723 -ePA-Frontend des Versicherten: Über mögliche Schadsoftware informieren
Der Hersteller des ePA-Frontend des Versicherten MUSS den Nutzer darüber informieren, dass Dokumente Schadsoftware enthalten können und welche Maßnahmen der Nutzer zum Selbstschutz vornehmen kann.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Herstellererklärung,<=**]**

A_15252-02 -ePA-Frontend des Versicherten: Schlüsselmaterial nicht persistent speichern
Das ePA-Frontend des Versicherten DARF alle verwendeten symmetrischen und privaten asymmetrischen Schlüssel NICHT persistent speichern, sofern es sich nicht um Authentisierungsmerkmale handelt.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Die Anforderung für die Bedingungen für die persistente Speicherung von Authentisierungsmerkmalen legt das Authenticator-Modul fest.

A_15253-01 -ePA-Frontend des Versicherten: Schutz Session-Daten
Das ePA-Frontend des Versicherten DARF Session-Daten NICHT an Dritte, außer im Rahmen der in den Anwendungsfällen spezifizierten Kommunikation, weitergeben.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten,<=**]**

A_15254-01 -ePA-Frontend des Versicherten: Session-Daten nicht persistent speichern
Das ePA-Frontend des Versicherten DARF Session-Daten NICHT persistent speichern.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_20746 -ePA-Frontend des Versicherten: Authentifizierung des Nutzers am ePA-FdV
Das ePA Frontend des Versicherten MUSS den Nutzer beim Starten des ePA Frontends des Versicherten am ePA Frontend des Versicherten authentisieren.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Für die Authentifizierung des Nutzers am ePA-FdV können die Authentifizierungsfunktionen des Betriebssystems des Endgerätes (z.B. Logscreen-Credentials, Biometrie) genutzt werden. Bei der Authentifizierung der oberen Anforderung ist nicht die Anmeldung an Backendsystemen (z.B. ePA-Aktensystem) gemeint, sondern die Authentifizierung am ePA-Frontend des Versicherten.

A_15255-01 -ePA-Frontend des Versicherten: Schutzmaßnahmen gegen die OWASP-Mobile-Top-10-Risiken

Das ePA-Frontend des Versicherten MUSS Maßnahmen zum Schutz vor den in der aktuellen Version genannten OWASP-Top-10-Mobile-Risiken [OWASPMobileTop10] umsetzen.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Dies betrifft bspw. die folgenden Aspekte:

- Schutz von Reverse Engineering
- Verwendung von Plattform Sicherheit Best Practice
- Secure Data Storage
- Schutz gegen code tampering
- Extraneous functionality

Für mobile Anwendungen sind OWASP Top Ten Mobile Controls [OWASP TTMC] und OWASP MASVS – L2 + R [OWASP MASVS] zu beachten. Anforderung A_15255-01 ist sowohl für Lösungen auf mobilen als auch Desktop-Plattformen umzusetzen.

A_17660 -ePA-Frontend des Versicherten: Schutzmaßnahmen gegen Schadsoftware aus Dokumenten
Das ePA-Frontend des Versicherten MUSS, wenn es Dokumentinhalte direkt anzeigt, Maßnahmen zum Schutz vor Schadsoftware in den Dokumenten umsetzen. **[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Folgende Maßnahmen sind sinnvoll:

- Prüfen, ob Dokumenten-Format und Inhalt mit dem angegebenen Dokumententyp in den Metadaten übereinstimmt
- Prüfen, ob Dokumenten-Format und Inhalt zu den erlaubten ePA-Dokumentenformaten passt
- Vor der Anzeige eines Dokumentes sind Sonder- und Meta-Zeichen im Dokument für die jeweilige Anzeigesoftware mit der richtigen Escape-Syntax zu entschärfen.
- Die Anzeigesoftware ist in einer Art Sandbox zu betreiben.

A_15256-02 -ePA-Frontend des Versicherten: Verbot von Werbe-Tracking
Das ePA-Frontend des Versicherten DARF ein Werbe-Tracking NICHT verwenden. **[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Im Folgenden wird unter Tracking Usability-Tracking sowie Crash-Reporting verstanden.

A_18767 -Tracking-Funktionen – Keine Weitergabe von Sicherheitsmerkmalen
Das ePA-Frontend des Versicherten MUSS sicherstellen, falls es Tracking-Funktionen implementiert, dass in den übermittelten Tracking-Informationen keine Sicherheitsmerkmale enthalten sind.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Sicherheitsmerkmale sind die Gerätekennung (DeviceID) und Session-Daten wie z. B. geheime oder private Schlüssel, Authentifizierungs- oder Autorisierungsbestätigungen.

A_18768 -Tracking-Funktionen – Verarbeitung und Auswertung der Tracking-Daten
Der Hersteller des ePA-Frontend des Versicherten MUSS die Verarbeitung und Auswertung der gesammelten Tracking-Daten des ePA-Frontends des Versicherten selbst durchführen und nicht von einem Drittanbieter durchführen lassen. **[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_18769 -Tracking-Funktionen – Keine direkt identifizierenden personenbezogenen Daten

Das ePA-Frontend des Versicherten MUSS sicherstellen, falls es Tracking-Funktionen nutzt, dass die Tracking-Daten keine Daten enthalten, die natürliche Personen direkt identifizieren.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Personenbezogene Daten mit direktem Personenbezug sind bspw. Namen von natürlichen Personen, Geräteidentifikatoren, Nutzerkennungen oder ein „Fingerabdruck“ auf Basis von Geräteeigenschaften und Einstellungen.

A_25267 -ePA-Frontend des Versicherten: Verbot der Profilbildung
Falls der Hersteller des ePA-Frontend des Versicherten Tracking Informationen verarbeitet, DARF er diese Informationen NICHT für eine Profilbildung verwenden.
[Frontend_Vers_ePA,Sich.techn. Eignung: Herstellererklärung,<=**]**

Tracking Anforderungen für Trackingdaten ohne Einwilligung

A_18770 -Tracking-Funktionen – Ohne Einwilligung des Nutzers
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen ohne Einwilligung des Versicherten nutzt, sicherstellen, dass die Tracking-Daten

- sich nur auf eine Nutzersession (von der ersten Interaktion des Nutzers mit dem FdV bis zum Schließen des FdVs bzw. bis zum Inaktivitätstimeout) beziehen und nicht mit anderen Sessions des Nutzers verknüpft werden,
- weder personenbezogene noch pseudonymisierte personenbezogene Daten enthalten,
- keine nutzerbezogenen IDs oder gerätespezifischen IDs der Nutzergeräte enthalten,
- keinen Rückschluss auf Versicherte, deren Vertreter, Leistungserbringer oder Kostenträger ermöglichen, insbesondere Rückschlüsse anhand des Nutzerverhaltens über die Zeit oder über Nutzersessions hinweg,
- nicht durch die Verknüpfung mit personenbezogenen Daten aus anderen Quellen de-anonymisiert werden können.

[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Andere Quellen sind z.B. Webtracker, Tracker von anderen Apps oder Trackingmerkmale des Betriebssystems (z.B. Hardware IDs, Network IDs oder Advertising IDs).

A_19061 -Tracking-Funktionen – Nutzer Informieren
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen ohne Einwilligung des Versicherten nutzt, den Nutzer über das Tracking im ePA-FdV in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache informieren, bevor die Trackingdaten erhoben werden.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Diese Anforderung ist nicht durch einen alleinigen Verweis auf die AGB oder Nutzungsbedingungen des FdVs erfüllbar. Verständliche Form bedeutet eine kurze nicht juristische Erklärung zum Zweck des Trackings. Leicht zugängliche Form bedeutet direkt im FdV.

A_18771 -Tracking-Funktionen – Generierung von Nutzersession basierte Trackingmerkmale
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen ohne Einwilligung des Versicherten nutzt, beim Start einer Nutzersession die Nutzersession-ID zufällig neu generieren.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Anforderungen zur Einwilligung zum Session-übergreifenden Tracking

A_18772 -Tracking-Funktionen - Opt-in
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass diese

Tracking-Funktionen bei der Installation des FdV standardmäßig deaktiviert sind und nur nach expliziter Einwilligung durch den Versicherten als Nutzer des FdV aktiviert werden (Opt-in).**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_18773 -Tracking-Funktionen – Kopplungsverbot
Das ePA-Frontend des Versicherten DARF, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpft, die Nutzung des FdVs NICHT an die Aktivierung dieser Trackingfunktion koppeln.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Das FdV muss voll-funktional ohne aktiviertes Tracking nutzbar sein.

A_18774-01 -Tracking-Funktionen - Einwilligungsinformation des Nutzers
Das ePA-Frontend des Versicherten MUSS den Versicherten vor der Einwilligung in die Aktivierung von Tracking-Funktionen in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache folgende Einwilligungsinformationen anzeigen:

- welche Daten durch die Tracking-Funktionen erhoben werden,
- zu welchen Zwecken die Daten erhoben werden,
- welche Informationen durch die Auswertung der erhobenen Daten gewonnen werden und ob Rückschlüsse auf den Gesundheitszustand des Nutzers möglich wären,
- wer die Empfänger der Daten sind,
- wie lange die Daten gespeichert werden,
- wie die Tracking-Funktionen deaktiviert werden können.

[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Diese Anforderung ist nicht durch einen alleinigen Verweis auf die AGB oder Nutzungsbedingungen des FdVs erfüllbar. Verständliche Form bedeutet eine kurze nicht juristische Erklärung zum Zweck des Trackings. Leicht zugängliche Form bedeutet direkt im FdV.

A_18775 -Tracking-Funktionen – Aktivierung erst nach Lesebestätigung der Einwilligungsinformationen
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, sicherstellen, dass die Einwilligung des Nutzers in die Aktivierung der Tracking-Funktionen erst erfolgt, wenn der Nutzer bestätigt, die angezeigten Einwilligungsinformationen gelesen zu haben.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_18776 -Tracking-Funktionen – Deaktivierung ist jederzeit möglich
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass aktivierte Tracking-Funktionen jederzeit durch den Nutzer des FdVs deaktiviert werden können.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_18777-01 -Tracking-Funktionen – Neue Generierung der Pseudonyme ist jederzeit möglich
Das ePA-Frontend des Versicherten SOLL, falls es Tracking-Funktionen implementiert, technisch sicherstellen, dass eine neue Generierung der pseudonymen Identifier jederzeit durch den Nutzer des FdVs veranlasst werden kann.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_18778 -Tracking-Funktionen – Verbot von mehrmaligen Einwilligungsabfragen
Das ePA-Frontend des Versicherten MUSS, falls es Tracking-Funktionen implementiert, die Tracking-Daten mehrerer Nutzersessions verknüpfen, technisch sicherstellen, dass der Benutzer der App maximal einmal eine Abfrage zur Einwilligung des Trackings angezeigt bekommt.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Wenn der Benutzer seine Einwilligung zum Tracking nicht erteilt, darf das FdV den Nutzer nicht solange nach seiner Einwilligung fragen, bis der Nutzer diese erteilt.

Das ePA-Frontend des Versicherten bietet nur Funktionalitäten an, welche sich aus den Anwendungsfällen der Fachanwendung ePA und weiteren Fachanwendungen der TI (z.B. E-Rezept, TI-Messenger) ergeben.

Zusätzliche Funktionalitäten können durch das FdV angeboten werden. Folgende Anforderungen gelten für die Abgrenzung der zusätzlichen Funktionalitäten zu denen der Fachanwendungen der TI.

A_16438 -ePA-Frontend des Versicherten: Unterscheidbarkeit zusätzlicher Funktionalitäten
Das ePA-Frontend des Versicherten MUSS sicherstellen, falls es zusätzliche Funktionalitäten enthält, dass der Nutzer diese zusätzlichen Funktionalitäten von den Funktionalitäten für die ePA unterscheiden kann.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Herstellererklärung,<=**]**

Die Information, welche Funktionalitäten zusätzlich zu den Funktionen für die ePA enthalten und damit nicht Gegenstand der Zulassung durch die gematik sind, kann im Handbuch oder den Informationen zur Zustimmung gemäß A_16439 beschrieben werden.

A_18401 -ePA-Frontend des Versicherten: Verarbeiten von ePA-Daten in zusätzlichen Funktionalitäten - Zustimmung
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass der Nutzer dem Verarbeiten der ePA-Daten in zusätzlichen Funktionalitäten des ePA-Frontends des Versicherten bezüglich Umfang, Art und Dauer der Verarbeitung vor dem Zugriff der Zusatzfunktionen auf die ePA-Daten zustimmen muss.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_18402 -ePA-Frontend des Versicherten: Verarbeiten von ePA-Daten in zusätzlichen Funktionalitäten - Opt-In
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass die Zustimmung zur Verarbeitung der ePA-Daten in zusätzlichen Funktionalitäten des ePA-Frontends des Versicherten optional (Opt-In) und jederzeit widerrufbar ist.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_16439 -ePA-Frontend des Versicherten: Weiterleiten von Daten - Zustimmung
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass Daten, die aus der ePA ins FdV geladen werden, nur mit Zustimmung des Versicherten unter Nutzung von expliziten Opt-in-Lösungen weitergeleitet werden können, wobei sich das Opt-In nur genau auf die Weiterleitung beziehen und nicht mit anderen Zustimmungen kombiniert werden darf.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Die in A_16439 geforderte Zustimmung kann einmalig durch den Versicherten erteilt werden und bis auf Widerruf des Versicherten für alle Datenweiterleitungen, die von dem Versicherten veranlasst werden, gelten. Das FdV kann dabei die Möglichkeit einer expliziten Opt-in-Lösung mit Widerrufsrecht oder ein anlassbezogenes Zustimmungsverfahren oder eine Wahlmöglichkeit beider Verfahren vorsehen.

A_20721 -Weiterleiten von Daten an Krankenkassen erst nach Einwilligung
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass Daten, die aus der ePA ins FdV geladen werden, nur an von Krankenkassen angebotene Anwendungen weitergeleitet werden, falls der Versicherte zuvor gegenüber der Krankenkasse in die Verarbeitung dieser Daten eingewilligt hat.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Die A_20721 setzt die Forderung des § 345 Abs. 1 SGB V um. Die Einwilligung gegenüber der Krankenkasse kann elektronisch erfolgen. Dies betrifft insbesondere auch die Übermittlung des Nachweises, mit dem die Krankenkasse die Einwilligung des Versicherten in die Verarbeitung der Daten nachweisen kann (vgl. Art. 7 Abs. 1 DSGVO).

A_16440 -ePA-Frontend des Versicherten: Weiterleiten von Daten - Information
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass der Versicherte vor der Zustimmung zur Nutzung von aus der ePA ins FdV geladenen Daten durch Anwendungen oder Apps im oder außerhalb des Frontends in verständlicher Weise darüber informiert wird, welche Daten, wann und an wen weitergeleitet werden und zu welchem Zwecke die Anwendungen die Daten verarbeiten.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_16441 -ePA-Frontend des Versicherten: Weiterleiten von Daten - Nachvollziehbarkeit
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass der Versicherte eine Weiterleitung der Daten im Nachhinein nachvollziehen kann (z.B. durch Protokollierung). **[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_19110 -ePA-Frontend des Versicherten: – Unterbindung bei einer erheblichen Störung
Der Hersteller des ePA-Frontend des Versicherten MUSS bei Bekanntwerden einer erheblichen Störung (gemäß §291b Abs.6 S.3 SGB V) in einer Version des ePA-Frontend des Versicherten die Nutzung dieser Version unverzüglich unterbinden.
[Frontend_Vers_ePA,Sich.techn. Eignung: Herstellererklärung,<=**]**

A_21342 -ePA-FdV für Desktop-Plattformen: Anzeige eines Hinweistextes zum Betrieb auf Hardware, die nicht unter der Kontrolle des Versicherten steht
Das ePA-FdV MUSS den Versicherten in einem Hinweistext auf die Gefahren hinweisen, die bei einem Betrieb des ePA-FdV auf Hardware, die nicht unter der Kontrolle des Versicherten steht, gegeben sind.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Hinweis: Im Gegensatz zu Betriebssystem für Smartphones und Tablets wie etwa Android und iOS sind Betriebssysteme für stationäre Geräte wie etwa PCs durchaus im öffentlichen Raum verfügbar. So läuft etwa auf den meisten Geräten in Internet-Cafes Windows. Würde hier das ePA-FdV ausgeführt werden und der Versicherte sich Dokumente aus seiner Akte herunterladen, dann müsste der Versicherte dafür sorgen, dass keine Daten von ihm auf der Hardware verbleiben, wenn er den Zugriff auf die Hardware beendet. Es wird empfohlen, die Nutzung des ePA-FdV auf öffentlich zugänglicher Hardware zu unterlassen.

Hinweis: Die einmalige Anzeige des Hinweises mit Bestätigung pro Versicherten ist ausreichend. Es muss dabei sichergestellt sein, dass jedem Nutzer (Mehrbenutzerbetrieb) dieser Hinweis zur Bestätigung angezeigt wird. Dieses könnte etwa durch Anzeige vor der Authentisierung gegenüber dem ePA-FdV erfolgen.

A_21343-01 -ePA-Frontend des Versicherten: Ausführen von begutachtetem Code
Der Hersteller des ePA-FdV MUSS technisch sicherstellen, dass im ePA-FdV nur Code ausgeführt wird, welcher im Scope des Produktgutachtens liegt oder Code-Änderungen nach Vorgaben der gematik durch den Hersteller des ePA-FdV als nicht zulassungsrelevant bewertet wurden.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Das Verbot des dynamischen Nachladens von ungeprüftem Code soll insbesondere sicherstellen, dass zum Zeitpunkt der Prüfung des ePA-FdV durch den Produktgutachter der gesamte Anwendungscode vorliegt und dieser nicht später durch ungeprüften Code ersetzt bzw. ergänzt werden kann. Die Anforderung verhindert zum Beispiel nicht, das Kartendaten eines externen Kartendienstes oder Bilder aus externen Quellen ins ePA-FdV geladen werden können. Es ist aber z.B. nicht möglich, ausführbaren Code wie z.B. Java Script nachzuladen.

Im Zulassungsverfahren für das ePA-FdV ist festgelegt, wann Änderungen durch die gematik als zulassungsrelevant betrachtet werden. Zulassungsrelevante Änderungen sind

z.B. Änderungen von Sicherheitsfunktionen oder deren Implementierung (z.B. Wechsel der TLS-Implementierung). Nicht-zulassungsrelevante Änderungen sind z.B. Sicherheitsupdates für von anderen Herstellern bezogenen Software-Komponenten der Plattform (z.B. Bibliotheken), die aus einer vertrauenswürdigen Quelle bezogen werden.

A_21344-01 -ePA-Frontend des Versicherten: Code von Drittanbietern aus vertrauenswürdigen Quellen
Der Hersteller des ePA-FdV MUSS die Software-Komponenten des ePA-FdV, die nicht vom Hersteller des ePA-FdV selbst entwickelt oder zur Entwicklung beauftragt werden (z.B. TLS-Bibliotheken), aus bekannten und vertrauenswürdigen Quellen beziehen. **[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_21355 -ePA-Frontend des Versicherten: Zugriff auf den Geräteidentifikator durch Zusatzfunktionen
Das ePA-FdV DARF Zusatzfunktionen des FdV (d.h. kassenspezifische Dienste) NICHT auf den Geräteidentifikator zugreifen lassen.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_21356 -ePA-Frontend des Versicherten: Speicherung des Geräteidentifikators
Das ePA-FdV MUSS sicherstellen, dass die Speicherung des Geräteidentifikators ausschließlich verschlüsselt erfolgt.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_21357 -ePA-Frontend des Versicherten: Zugriff auf den Geräteidentifikator
Das ePA-FdV MUSS sicherstellen, dass auf den verschlüsselten gespeicherten Geräteidentifikator ausschließlich nach erfolgreicher Authentifizierung des Versicherten beim Start des ePA-FdV zugegriffen werden kann.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Nach A_20746 muss sich der Nutzer beim Starten des ePA-FdV am ePA-FdV authentisieren.

A_21350 -ePA-FdV für Desktop-Plattformen: Informieren des Versicherten über sichere Bezugsquellen für die Verteilung des FdV
Der Hersteller des ePA-FdV MUSS Versicherte über die vertrauenswürdigen Quellen informieren, von denen Versicherte das ePA-FdV beziehen können und wie sie die Vertrauenswürdigkeit der Quelle erkennen können.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Hinweis: Krankenkassen (als Anbieter eines ePA-Aktensystems) können zur Umsetzung dieser Anforderung z.B. den Versicherten hierzu entsprechendes Informationsmaterial zur Verfügung stellen, wo die Download-Punkte aufgelistet sind.

A_21351 -ePA-FdV für Desktop-Plattformen: Sicherstellung der Authentifizierung der Bezugsquelle bei Erstbezug
Der Hersteller des ePA-FdV MUSS sicherstellen, dass der Versicherte bei Erstbezug eines ePA-FdV die Authentizität der vertrauenswürdigen Bezugsquelle verifizieren kann. **[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Beim Erstbezug des ePA-FdV kann die Prüfung der Authentizität der Quelle noch nicht durch das ePA-FdV selbst erfolgen. Dies kann z.B. über eine TLS-Server-Authentifizierung der Bezugsquelle erreicht werden. Bei ePA-FdVs in den Stores der mobilen Plattformen kann der Versicherte die Vertrauenswürdigkeit daran erkennen, dass er den offiziellen Store nutzt. Auch unter Windows und Mac OS und Linux/Debian gibt es einen offiziellen Store.

A_21352 -ePA-FdV für Desktop-Plattformen: Technische Authentifizierung der Update-Bezugsquellen für die sichere Verteilung der ePA-FdV-Anwendung
Das ePA-FdV MUSS sicherstellen, dass Updates nur von bekannten und vertrauenswürdigen Quellen bezogen werden, nach dem die Authentizität der Quelle

technisch erfolgreich verifiziert wurde.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung, Sich.techn. Eignung: Produktgutachten,<=**]**

A_21475 -Zugriff auf das Nationale Gesundheitsportal nur nach Zustimmung des Versicherten (Opt-in)
Das ePA-FdV MUSS sicherstellen, dass Zugriffe mit dem ePA-FdV auf das Nationale Gesundheitsportal erst erfolgen können, nachdem der Versicherte dem zugestimmt hat, und nicht mehr erfolgen können, nachdem der Versicherte eine zuvor gegebene Zustimmung zurückgenommen hat.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_21476 -Informationen zum Datenschutz bei Nutzung des Nationalen Gesundheitsportals
Das ePA-FdV MUSS den Versicherten vor Nutzung des Nationalen Gesundheitsportals mindestens informieren über

- den Zweck, Umfang und Art der Verarbeitung der Daten des Versicherten im Nationalen Gesundheitsportal,
- die Maßnahmen im Nationalen Gesundheitsportal zur Verhinderung einer Profilbildung,
- den nach DSGVO Verantwortlichen des Nationalen Gesundheitsportals und
- die zuständige datenschutzrechtliche Aufsichtsbehörde für das Nationale Gesundheitsportal.

[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_21477 -Sichere Verbindung zum Nationalen Gesundheitsportal
Das ePA-FdV MUSS sicherstellen, dass auf das Nationale Gesundheitsportal ausschließlich zugegriffen wird, nachdem die Authentizität des Nationalen Gesundheitsportals vom ePA-FdV erfolgreich geprüft wurde und eine vertrauliche und integritätsgeschützte Verbindung zwischen ePA-FdV und Nationalem Gesundheitsportal aufgebaut wurde.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_21700 -Verbot der Übermittelung persönlicher Daten an das Nationale Gesundheitsportal
Das ePA-FdV MUSS sicherstellen, dass bei Zugriffen auf das Nationale Gesundheitsportal keine personenbezogenen Daten oder Einstellungen an das Nationale Gesundheitsportal übermittelt oder dem Nationalen Gesundheitsportal Zugriffe auf diese Daten gewährt werden, außer sie sind für die technische Verbindung vom ePA-FdV zum Nationalen Gesundheitsportal zwingend notwendig.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_27569 -Erzeugung einer Instance-ID durch eine ePA-FdV Instanz bei separater Authenticator-APP (befristet)
Das ePA-FdV MUSS, wenn eine Nutzerauthentifizierung über SSO erfolgen soll, eine Instance-ID erzeugen und diese beim Aufruf der URI-PAR an das Authenticator-Modul als Parameter `sso_instance_id` übergeben. Die Instance-ID MUSS ein UUID V4 [RFC9562.html#name-uuid-version-4] generierter Wert und unique für den Anwendungskontext sein. Die Instance-ID MUSS nach Beendigung der App (Beenden des Anwendungskontextes durch Nutzer oder Betriebssystem) ungültig sein.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis 1: Der Anwendungskontext ist die Laufzeit des ePA-FdV vom Start bis zum Beenden auf dem Gerät des Nutzers.
Hinweis 2: Die Anforderung gilt für die zeitlich befristete Übergangslösung. Diese wird von einer ePA-FdV unabhängigen SSO-Lösung nach Abnahme durch das BSI abgelöst.

Das Snippet Management ermöglicht es technische Artefakte zur Optimierung eines ePA FdV im Kontext eines Users im ePA-Aktensystem zu speichern. Da diese Inhalte nicht

innerhalb der Akte gespeichert werden dürfen dort keine medizinischen Daten dort hinterlegt werden.

A_28577 -ePA-Frontend des Versicherten - keine medizinischen Daten im Device Management
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass die Operation putSnippet [I_Device_Management_Insurant] keine medizinischen Daten im Device Management hinterlegt.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_30476 -ePA-Frontend des Versicherten - Verwaltung von Einwilligungen für Zusatzfunktionen
Falls das ePA-Frontend des Versicherten die Nutzung einer backendseitigen Zusatzfunktion unterstützt, MUSS das ePA-Frontend des Versicherten die Verwaltung der Einwilligung der backendseitigen Zusatzfunktion ermöglichen.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

5.1.1 Anforderungen bei CC-Zertifizierung

A_19143 -ePA-Frontend des Versicherten: Mitwirkungspflicht bei der CC-Zertifizierung
Falls der Hersteller des ePA-Frontend des Versicherten entscheidet, eine CC-Zertifizierung statt eines Produktgutachtens durchzuführen, MUSS der Hersteller des ePA-Frontend des Versicherten bei der Einreichung eines CC-Zertifizierungsantrags sein Security Target Dokument der gematik zur Verfügung stellen.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Herstellererklärung,<=**]**

A_19144 -ePA-Frontend des Versicherten: Dokumentationspflicht bei der CC-Zertifizierung
Falls der Hersteller des ePA-Frontend des Versicherten entscheidet, eine CC-Zertifizierung statt eines Produktgutachtens durchzuführen, MUSS der Hersteller des ePA-Frontend des Versicherten

- die zusätzlichen Funktionen des ePA-Frontend des Versicherten,
- die in den zusätzlichen Funktionen verarbeiteten Daten,
- die Schnittstellen zwischen dem ePA-Frontend des Versicherten und den ggf. genutzten Backend-Diensten der zusätzlichen Funktionen inklusive ihrer Sicherheitsmaßnahmen und
- die Sicherheitsannahmen an das ePA-Frontend des Versicherten und die Ausführungsumgebung

im Security Target beschreiben.
[Frontend_Vers_ePA,Sich.techn. Eignung: Herstellererklärung,<=**]**

5.2 Verwendete Standards

Für die Nutzung der Schnittstellen werden u.a. die folgenden Standards verwendet.

A_15268-01 -ePA-Frontend des Versicherten: Konformität zu WS-I Basic Profil 2.0
Das ePA-Frontend des Versicherten MUSS SOAP-Nachrichten gemäß den Vorgaben aus WS-I Basic Profile V2.0 [WSIBP] unterstützen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

5.3 Integrating the XDS of Healthcare Enterprise IHE

Die dokumentenbezogenen Schnittstellen des ePA-Aktensystems und die Verarbeitungslogik des ePA-Frontends des Versicherten basieren auf Transaktionen des IHE ITI Technical Frameworks (IHE ITI TF). Die IHE ITI-Implementierungsstrategie ist in [gemSpec_Aktensystem_ePAfuerAlle#XDS Document Service] beschrieben.

Das ePA-Frontend des Versicherten nutzt die folgenden Integrationsprofile des IHE ITI TF:

- Cross-Enterprise Document Sharing (XDS.b) Profile
- Remove Metadata and Documents (RMD) Profile

Die folgende Tabelle bietet einen Überblick über die durch das ePA-Frontend des Versicherten umzusetzenden IHE ITI-Akteure und assoziierte Transaktionen.

Tabelle 4: IHE Akteure und Transaktionen

Aktion	Profile	IHE-Akteur	Transaktion	Referenz
Suchanfrage auf Metadaten	XDS.b	Document Consumer	Registry Stored Query [ITI-18]	[IHE-ITI-TF2]#3.18
Herunterladen von Dokumenten	XDS.b	Document Consumer	Retrieve Document Set [ITI-43]	[IHE-ITI-TF2]#3.43
Löschen von Dokumenten	RMD	Document Administrator	Remove Metadata [ITI-62]	[IHE-ITI-RMD]#3.62

XDS-Option "Folder Management" - Verwendung von Ordnern

Ordner können durch die Option "Folder Management" (XDS.b Document Source) verwendet werden. Die Zuordnung von Dokumenten zu Ordnern im Aktensystem erfolgt durch die Metadaten des Dokuments. Dynamische Ordner werden durch Primärsysteme (Mutterpass) oder Aktensystem (DiGA) erstellt und vom FdV ggf. ausgewertet. Durch die Assoziation eines Dokumentes zu einem dieser Ordner wird das Dokument dem Ordner der entsprechenden Datenkategorie bzw. Sammlung zugeordnet.

Die XDS-Option "Folder Management" ist nur für den geschilderten Verwendungszweck zugelassen; ein selbständiges Anlegen oder Bearbeiten von Ordnern und ihrer Metadaten ist durch das FdV nicht möglich.Das Entfernen von Dokumenten aus einem Ordner durch Löschen der entsprechenden Assoziation ist nicht vorgesehen, da dies die direkte Zuordnung gemäß einer Zugriffsunterbindungsregel verletzten könnte.

Weitere Festlegungen

Weitere übergreifenden Einschränkungen von IHE ITI-Transaktionen sowie Festlegungen spezieller Umsetzungsvorgaben bzgl. einzelner Transaktionen sind in [gemSpec_Aktensystem_ePAfuerAlle#XDS Document Service]beschrieben.

Wenn im Rahmen der IHE Schnittstellen-Beschreibung der Begriff "Patient" verwendet wird, ist im Rahmen der vorliegenden Spezifikation darunter der Aktenkontoinhaber zu verstehen.

Im ePA-Frontend des Versicherten werden fachliche Dokumente (Versichertendokumente) und technische Dokumente unterschieden.

5.4 Benutzeroberfläche

Die Benutzeroberfläche, welche durch den Versicherten genutzt wird, um ePA-Anwendungsfälle auszuführen, ist Teil des FdV.

Die folgenden Ausführungen zu Anforderungen an die visuelle Darstellung und Benutzerführung sind informativ und nicht normativ.

5.4.1 Visuelle Darstellung

Für die visuelle Darstellung der Inhalte ist eine grafische Benutzeroberfläche erforderlich, welche die Daten des Versicherten strukturiert und übersichtlich darstellt.

Das FdV soll eine einheitlich gestaltete Oberfläche zur Benutzerführung besitzen, um die Übersichtlichkeit in allen Anwendungsfällen für den Nutzer zu gewährleisten. Es soll Menüfunktionen, Texte und andere Anzeigen eindeutig, verständlich und widerspruchsfrei benennen bzw. darstellen.

Das FdV soll es dem Nutzer ermöglichen, zu jeder Zeit zu erkennen, in welchem ePA-Anwendungsfall sich die Applikation gerade befindet.

5.4.2 Benutzerführung

Die Bedienung des FdV soll für den Nutzer intuitiv gestaltet werden. Das FdV soll dem Nutzer alle anzeigbaren Texte mindestens in der Sprache Deutsch bereitstellen.

DIN Normen und Verordnungen zur Beachtung:

Eine hohe Akzeptanz der Benutzerfreundlichkeit oder Usability wird durch eine einfache, selbsterklärende Bedienung der Oberfläche erreicht, die sich an gängigen Mustern des App-Designs orientiert.

Hierfür ist es auch erforderlich, die Erwartungshaltung der Zielgruppe zu kennen und zu berücksichtigen (z.B. auch Menschen mit körperlichen oder geistigen Einschränkungen).

Die Akzeptanz des Frontends für den Versicherten hängt in großem Maße von folgenden Faktoren ab:

- Anwendbarkeit auf verschiedenen Bildschirmgrößen und Auflösungen
- Intuitive und unkomplizierte Handhabung
- Anwendbarkeit auch im Offline-Modus
- Zielgruppenorientierung
- Leichte und verständliche Bereitstellung von Informationen
- Einhaltung ergonomischer Aspekte (z.B. kurze Touchwege)
- Konsistente Gestaltung der Links, Buttons, etc.

5.4.2.1 Technische Normen und Verordnungen zur Beachtung

Die Entwicklung einer barrierearmen Anwendung unterliegt einem sich fortlaufend weiterentwickelnden Prozess. Die Umsetzung aller Anforderungen kann nicht mit der Ersteinführung der Anwendung sichergestellt werden.

Zusätzlich zu den in diesem Kapitel aufgeführten Anforderungen zur Benutzerführung sollen auch die in der ISO 9241 aufgeführten Qualitätsrichtlinien zur Sicherstellung der Ergonomie interaktiver Systeme und Anforderungen aus der Verordnung zur Schaffung

barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung – BITV 2.0) beachtet werden.

DIN EN ISO 9241 – Teile mit Bezug zur Software-Ergonomie

Insbesondere sollen die nachfolgend aufgeführten Teile der ISO 9241 berücksichtigt werden:

- Teil 8: Anforderungen an Farbdarstellungen
- Teil 9: Anforderungen an Eingabegeräte – außer Tastaturen
- Teil 110: Grundsätze der Dialoggestaltung (ersetzt den bisherigen Teil 10)
- Teil 11: Anforderungen an die Gebrauchstauglichkeit – Leitsätze
- Teil 12: Informationsdarstellung
- Teil 13: Benutzerführung
- Teil 14: Dialogführung mittels Menüs
- Teil 15: Dialogführung mittels Kommandosprachen
- Teil 16: Dialogführung mittels direkter Manipulation
- Teil 17: Dialogführung mittels Bildschirmformularen
- Teil 171: Leitlinien für die Zugänglichkeit von Software BITV 2.0

Für die Entwicklung eines barrierefreien Frontend des Versicherten ist insbesondere die Verordnung zur barrierefreien Gestaltung von Informationstechnik zu beachten.

BITV 2.0 - Barrierefreie Informationstechnik-Verordnung

Hinweis: Die Versionsnummern der aufgeführten Normen und Richtlinien spiegeln den Stand zum Zeitpunkt der Erstellung dieses Dokumentes wider.

Die seit 2018 bestehende umfassende Forderung nach Umsetzung von Barrierefreiheit in der Informationstechnik erwächst aus der EU Richtlinie 2016/2102 zur „Barrierefreiheit von Webseiten und mobiler Anwendungen öffentlicher Stellen“. Diese Richtlinie musste im Jahr 2018 in Bundes- und Landesrecht übertragen werden. – Diese Gesetze verweisen jeweils auf die Barrierefreie Informationstechnik-Verordnung mit Ausgabe vom 21. Mai 2019 (BITV 2.0).

Zur Erfüllung der BITV 2.0 § 3 Abs. 2 ist die durch die Veröffentlichung im europäischen Amtsblatt harmonisierte EN 301549 „Barrierefreiheitsanforderungen für IKT-Produkte und -Dienstleistungen“ (V 2.1.2 von 2018-08) anzuwenden. Diese liegt in der Fassung von 2020-02 als DIN EN 301549 als deutsche Übersetzung vor. Die DIN EN 301549 ist eine Beschaffungsnorm. Die darin aufgeführten und für den Anwendungsfall des FdV des E-Rezepts anzuwendenden Erfolgskriterien sind in Kapitel 9 (Web mit 50 Erfolgskriterien), Kapitel 10 (Dokumente mit 46 Erfolgskriterien) und Kapitel 11 (Nicht webbasierte Software mit 44 Erfolgskriterien) aufgeführt. Sie entsprechen den Erfolgskriterien von Level AA der 2.1. WCAG 2.1 (Web Content Accessibility Guidelines).

Der sachliche Geltungsbereich der BITV 2.0 umfasst folgende relevanten Anwendungsbereiche für diese Spezifikation:

- Webseiten,
- nicht webbasierte Software mit mobilen Anwendungen.

Folgende Gestaltungsmerkmale der Anwendungen stellen die Barrierefreiheit sicher:

- wahrnehmbar,
- bedienbar,
- verständlich und

- robust.

In den genannten Normen und Standards werden nebeneinander die Belange von in der Handmotorik eingeschränkter, blinder, sehbehinderter, gehörloser, schwerhöriger, geistig und lernbehinderter Menschen berücksichtigt.

Nach BITV 2.0 müssen Dokumente, die über dem FdV angezeigt werden, die gleichen Anforderungen an die Barrierefreiheit erfüllen, wie sie an die Anwendung gestellt werden. Sämtliche bereitgestellten Dokumente müssen als barrierefreie Formate angeboten werden, die mit dem Screenreader lesbar und navigierbar sind. Hierbei müssen die behinderungsspezifischen Standardsoftwares zur Herstellung von Zugänglichkeit berücksichtigt werden.

Allgemeine Anforderungen an die Benutzerfreundlichkeit

A_20092 -ePA-Frontend des Versicherten: Intuitive Bedienung
Die Bedienung des ePA-Frontend des Versicherten SOLL für den Nutzer intuitiv gestaltet werden.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_20094 -ePA Frontend des Versicherten: Bereitstellung Sprachen
Das ePA-Frontend des Versicherten SOLL dem Nutzer alle anzeigbaren Texte in der Sprache Deutsch bereitstellen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Zusätzliche Sprachen können unterstützt werden.

A_20095-02 -ePA-Frontend des Versicherten: Abbruch Anwendungsfälle
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Anwendungsfälle auch vor dem Ende der Verarbeitung jederzeit abzubrechen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_20096 -ePA-Frontend des Versicherten: Arten der Verwaltung
Das ePA-Frontend des Versicherten SOLL dem Nutzer anzeigen, welche Arten von Dokumentenzugriffen und Verwaltungsfunktionen ausgeführt werden können. **[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_20097 -ePA-Frontend des Versicherten: Bezeichnung der Anwendungsfälle
Das ePA-Frontend des Versicherten MUSS für die Inhalte und Anwendungsfälle eindeutige und verständliche Bezeichnungen verwenden.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Bezeichnungen sollen nach Möglichkeit vollständig ausgeschrieben sein, Abkürzungen sind zu vermeiden.

A_20098 -ePA-Frontend des Versicherten: Navigierbarkeit bereitgestellter Inhalte
Das ePA-Frontend des Versicherten SOLL sicherstellen, dass bereitgestellte Inhalte maschinenlesbar und navigierbar sind, um dem Nutzer eine barrierefreie Bedienung zu ermöglichen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_20099-01 -ePA-Frontend des Versicherten: Nutzung Gerätefunktionalitäten
Zur Umsetzung der Barrierefreiheit SOLL das ePA-Frontend des Versicherten gerätespezifische Funktionalitäten (z.B. Lagebestimmung, Kamerafunktion, Multi-Touch-Gesten) nutzen und unterstützen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_20100 -ePA-Frontend des Versicherten: Nutzung Schnittstellen Bedienungsmöglichkeiten des Betriebssystems
Das ePA-Frontend des Versicherten SOLL die Schnittstellen für die Unterstützung der barrierefreien Bedienungsmöglichkeit, welche vom Betriebssystem zur Verfügung gestellt werden, nutzen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_20101 -ePA-Frontend des Versicherten: Nutzung Bedienhilfen des Betriebssystems
Das ePA-Frontend des Versicherten SOLL die Bedienhilfen der verwendeten Betriebssysteme zur barrierefreien Nutzung verwenden.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_20102 -ePA-Frontend des Versicherten: Kontrastverhältnis
Das ePA-Frontend des Versicherten SOLL für das GUI ein Kontrastverhältnis verwenden, welches unter verschiedenen Bedingungen eine optimale Ablesbarkeit gewährleistet. **[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_20103 -ePA-Frontend des Versicherten: Hinweise
Das ePA-Frontend des Versicherten SOLL dem Nutzer Hinweise anzeigen, die den Zweck sowie den inhaltlichen Ablauf eines Anwendungsfalls betreffen, um dem Nutzer die Bedienung zu vereinfachen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Ist ein Anwendungsfall durchgeführt worden, muss das FdV das Ergebnis für den Nutzer klar verständlich anzeigen, z. B. "Die Vertretung wurde erfolgreich eingerichtet.".

Ist ein Anwendungsfall durch den Nutzer abgebrochen worden oder technisch nicht durchführbar, muss der Nutzer ebenfalls einen für ihn verständlichen Hinweis erhalten. In jedem Fall muss das Ergebnis für den Nutzer klar erkennbar sein.

Für die Anzeige in Fehlerfällen siehe Kapitel "6.2.2- Fehlerbehandlung".

Zur Sicherstellung, dass keine Daten versehentlich gelöscht werden, soll der Nutzer nach der Auswahl der Löschen-Funktion für Dokumente darauf hingewiesen werden, dass es sich hierbei um eine unwiderrufliche Aktion handelt.

5.4.3 Anzeige von Dokumenten

Der Nutzer kann nach Dokumenten in der ePA suchen und diese herunterladen oder sich anzeigen lassen.

A_18257 -ePA-Frontend des Versicherten: Dokumentengrösse an Aussenschnittstellen
Das ePA-Frontend des Versicherten MUSS für alle Außenschnittstellen, welche für Dokumente in ePA-Anwendungsfälle genutzt werden, Dokumente mit einer Größe von mindestens 25 MB unterstützen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_17226 -ePA-Frontend des Versicherten: Anzeige Metadaten von Dokumenten
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die zu einem Dokument zugehörigen Metadaten mit fachlichen Informationen einzusehen. **[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Technische Metadaten zu einem Dokument müssen nicht angezeigt werden.

A_15284 -ePA-Frontend des Versicherten: Anzeige von Dokumenten
Das ePA-Frontend des Versicherten SOLL Standardprogramme zur Anzeige von aus der ePA heruntergeladenen Dokumenten verwenden.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Für die Anzeige der Dokumente werden die auf dem Gerät des Versicherten (GdV) verfügbaren Standardprogramme verwendet. Unter einem Standardprogramm wird das im GdV mit einem Dokumenttypen verknüpfte Programm verstanden (z.B. Dateityp PDF mittels eines auf dem GdV verfügbaren PDFReader). Das FdV braucht keine Funktionalität zur Anzeige von Dokumenten in beliebigem Format bereitstellen.

Ist kein Programm zur Anzeige des Dokumentenformates auf dem GdV verfügbar, dann kann der Nutzer das Dokument nur lokal speichern.

A_15285 -ePA-Frontend des Versicherten: Anzeige strukturierter Dokumente
Das ePA-Frontend des Versicherten MUSS für strukturierte Dokumente eine für den Nutzer lesbare Darstellung mit dem vollständigen Inhalt des Dokumentes generieren und dem Nutzer anzeigen können.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Für Informationen zu strukturierten Dokumenten siehe[A_14761-*].

Wenn ein Arztbrief Dokument mit xml- und pdf-Anteil vorliegt, muss nur das PDF angezeigt werden.

Der Nutzer kann Dokumente in die ePA einstellen. Dafür müssen diese im FdV ausgewählt werden.

A_22974 -ePA-Frontend des Versicherten: Keine Anzeige von Dokumenten des Ordners "technical"
Das ePA-Frontend des Versicherten DARF einem Nutzer die Dokumente und Metadaten der Dokumente des Ordners "technical" NICHT zur Anzeige anbieten oder anzeigen. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

5.4.4 Drucken und Speichern von Verwaltungs- und Inhaltsdaten

In der ePA für alle wird grundsätzlich unterschieden zwischen Daten, die für den Versicherten inhaltlich relevant sind, und Daten, die der Verwaltung dieser Inhaltsdaten dienen.
Inhaltsdaten sind beispielsweise medizinische Dokumente, wie Arztbrief, Daten des Medikationsprozesses oder des Kostenträgers. Verwaltungsdaten sind beispielsweise Informationen zu Widersprüchen oder zur Zugriffssteuerung (Verbergen und Sichtbar machen), aber auch eine Liste der aktuell hinterlegten Befugnisse oder ein Ergebnis der Suche nach Dokumenten.

A_24426 -ePA-Frontend des Versicherten: Drucken und Speichern von Verwaltungs- und Inhaltsdaten
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Verwaltungs- und Inhaltsdaten auszudrucken oder lokal zu speichern.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

5.4.5 Sammlungen

Strukturierte Dokumente sind Dokumente, die Inhalte nach einem festgelegten Format dokumentieren. Diese werden durch Implementation Guides für strukturierte Dokumente [gemSpec_IG_ePA] eindeutig identifiziert. Eine besondere Form von strukturierten Dokumenten sind Sammlungen.
Als Sammlung gemäß [gemSpec_Aktensystem_ePAfuerAlle#Sammlungstypen] wird eine Zusammenstellung von strukturierten Dokumenten verstanden, die in ihrer Gesamtheit betrachtet, verborgen oder anderweitig besonders behandelt werden müssen. Das betrifft alle Sammlungen vom Typ "uniform" und "mixed". Zum Beispiel werden einzelne Einträge im Impfpass als separate Dokumente in der ePA abgelegt. Als Sammlung "Impfpass" unterliegen sie jedoch bestimmten Verarbeitungsregeln. Beispiele für andere Sammlungen sind der Mutterpass oder das Kinderuntersuchungsheft.

A_19897-01 -ePA-Frontend des Versicherten: Anzeige von Sammlungsinstanzen vom Typ "mixed" und "uniform"
Das ePA-Frontend des Versicherten MUSS für eine für den Nutzer lesbare Darstellung mit dem vollständigen Inhalt aller zur Sammlungsinstanz gehörenden Dokumente generieren und dem Nutzer anzeigen können.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Das Löschen einer Sammlungsinstanz umfasst das Löschen aller zur Instanz gehörenden Dokumente.

A_19961-02 -ePA-Frontend des Versicherten: Löschen einer Sammlungsinstanz
Das ePA-Frontend des Versicherten MUSS einen Nutzer beim Löschen einer Sammlungsinstanz, dem gesamtheitlichen Löschen bei Instanzen des Typs "mixed" und "uniform", unterstützen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Für das Verbergen der Sichtbarkeit auf eine Sammlung vom Typ "uniform" und "mixed" muss das ePA-Frontend des Versicherten die Sammlung in ihrer Gesamtheit unterstützen.

A_24458 -ePA-Frontend des Versicherten: Verbergen einer Sammlung vom Typ "mixed" oder "uniform"
Das ePA-Frontend des Versicherten MUSS einen Nutzer unterstützen, eine Sammlung vom Typ "`mixed`" oder "`uniform`" zu verbergen bzw. sichtbar zu machen.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Hat eine Sammlung vom Typ "`uniform`" die "`folderCardinality.max`"=1 gemäß [gemSpec_IG_ePA], dann gibt es nur eine Instanz dieser Sammlung, welche gleichbedeutend mit dem statischen Ordner, also der Datenkategorie ist. Ein Impfpass wird demzufolge verborgen, indem die Datenkategorie mit dem technischen Identifier"`vaccination`" verborgen wird.

Hat eine Sammlung vom Typ "`uniform`" die "`folderCardinality.max`">1 gemäß [gemSpec_IG_ePA], dann kann es mehrere Instanzen dieser Sammlung geben. Jede Instanz wird durch einen dynamischen Ordner abgebildet, welcher sich innerhalb der Datenkategorie befindet. Ein Mutterpass wird demzufolge verborgen, indem der dynamische Ordner des Mutterpasses verborgen wird. Wird die Datenkategorie "`pregnancy_childbirth`" verborgen, dann werden alle in dieser Kategorie enthaltenen Mutterpässe verborgen.

5.4.5.1 Weiterentwicklung bzw. Ablösung von Sammlungen

Im ePA Release "ePA 27" wird die Pflege des Zahnbonushefts durch die Dokumentenverwaltung des MHD Service weitergeführt, d.h. Dokumente der Sammlung Zahnbonusheft können via MHD Service verwaltet und durch eine LEI in das Aktenkonto eingestellt werden.

Die Sammlungen Mutterpass, Kinderuntersuchungsheft, Impfpass können über den XDS Document Service weiterhin gelesen werden, auch das Löschen ist weiterhin möglich. In späteren ePA Releases werden diese Sammlungen nicht mehr unterstützt. Damit keine Informationen für den Versicherten verloren gehen, besteht die Möglichkeit, diese Sammlungen im ePA-FdV als PDF/A zu speichern.

A_30250 -ePA-Frontend des Versicherten - Sammlungen als PDF/A-Dokumente bereitstellen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen für die folgenden im Aktenkonto hinterlegten Sammlungen (deprecated) die jeweiligen Inhalte in ein oder mehrere PDF/A-Dokumente zu überführen und zum Speichern bzw. Drucken bereitzustellen:

- Mutterpass
- Kinderuntersuchungsheft
- Impfpass

[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_30252 -ePA-Frontend des Versicherten - Hinweis zum Sichern von Sammlungen

Das ePA-Frontend des Versicherten MUSS den Nutzer darauf hinweisen, dass Sammlungen (deprecated) in späteren ePA Releases nicht mehr zu Verfügung stehen und dem Nutzer die Sammlungen als PDF/A-Export zur Verfügung stehen.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Der Hinweis für den Nutzer wird nur für den Fall angezeigt, dass Sammlungen (deprecated) vorhanden sind.

5.4.6 Nutzungsvorgaben für IHE ITI XDS-Metadaten

5.4.6.1 Metadaten für einzustellende Dokumente

Für Dokumente, welche durch den Nutzer in die ePA eingestellt werden, sind Metadaten anzugeben, auf deren Basis Dokumente nachfolgend gesucht und heruntergeladen werden können.

Die XDS-Metadaten und ihre Nutzungsvorgaben sind in [gemSpec_Aktensystem_ePAfuerAlle#Nutzungsvorgaben für IHE ITI XDS-Metadaten] beschrieben.
Es kann auf die Anzeige einzelner nutzbarer Metadatenattribute verzichtet werden, um eine übersichtliche Darstellung beim Einstellen der Dokumente zu erreichen.

Das FdV soll für die Eingabe von Metadaten required-Attribute als Pflichtfelder kennzeichnen. Dabei soll unterschieden werden zwischen einer einfachen Ansicht für das Einstellen von Dokumenten des Versicherten und einer erweiterten Ansicht für das Einstellen von LE-Dokumenten durch den Versicherten.

Defaultmäßig wird der Nutzer als Submission Set author (Einstellender) gesetzt. Die Werte für den author werden mindestens mit den Informationen `givenname`, `surname` und `title` vorbelegt.

Entsprechend den Nutzungsvorgaben für die Verwendung von XDS-Metadaten sind für einzelne Attribute Value Sets zu verwenden. Für eine bessere Bedienbarkeit bei der Eingabe der Metadaten werden die in der GUI auswählbaren Werte defaultmäßig auf einen Teil des Value Sets eingeschränkt. Über die Konfiguration des FdV hat der Nutzer die Möglichkeit, die anzuzeigenden Werte zu ändern, d.h. nicht angezeigte Werte aus dem Value Set hinzuzunehmen oder angezeigte Werte zu verbergen.

Das FdV soll dem Nutzer in der GUI für Attribute von Metadaten, welche entsprechend einem Value Set belegt werden, eine konfigurierbare Auswahl anbieten. Wenn das Attribut optional ist, dann muss die Auswahl einen leeren Eintrag beinhalten.

Dokumente, die vom Versicherten am FdV eingestellt werden, werden vom Aktensystem entsprechend der verwendeten Metadaten in die Datenkategorien "`patientdoc`" oder "`child`" eingeordnet (submissionset.authorRole = 102). Zusätzliche Metadaten können Dokumente als medizinisch relevante Dokumente auszeichnen, etwa als Arztbrief, ohne dass sie deswegen in Ordner einsortiert werden, die für Datenkategorien der Leistungserbringer stehen.

Das Frontend kann den Nutzer auch durch eine sinnvolle Vorauswahl bei der Klassifizierung und Typisierung unterstützen, insbesondere falls Versicherte Dokumente in ihre Akte einstellen wollen, die ursprünglich von anderen Leistungserbringern erstellt wurden, etwa Arztbriefe, die der Versicherte in Kopie erhalten hat.

A_15291 -ePA-Frontend des Versicherten: Schlüsselwerte aus Value Sets decodieren
Das ePA-Frontend des Versicherten MUSS Schlüsselwerte aus Value Sets decodieren und in einem für den Nutzer verständlichen Text anzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Ggf. kann dazu bei unbekannten Codes der Anzeigename eines Codes (sofern mit übertragen bzw. verfügbar) angezeigt werden.

5.4.7 Konfiguration des ePA-Frontend des Versicherten

Im Folgenden sind Konfigurationsparameter beschrieben, deren Werte für die Nutzung der Schnittstellen benötigt werden. Darüber hinaus kann der Hersteller des ePA-Frontend des Versicherten zusätzliche Konfigurationsparameter definieren.

A_15292-06 -ePA-Frontend des Versicherten: Parameter speichern und laden
Das ePA-Frontend des Versicherten MUSS die folgenden Parameter persistent speichern und bei der Initialisierung laden.

Tabelle 5: Parameter FdV

Parameter	Beschreibung	Wertebereich (Default Wert)
Aktenkontoinhaber: Akten-ID	Akten-ID (KVNR) des Aktenkontos für den Versicherten	unveränderliche Teil der KVNR; 10 Stellen
Aktenkontoinhaber: FQDN Anbieter ePA-Aktensystem	FQDN für den Zugriff auf das ePA-Aktensystem des zugehörigen Anbieters für den Versicherten	wird durch den Hersteller des FdV fest vorgegeben
Nutzer: Geräteinformation	u. a. Geräteidentifikator und Gerätestatus Der Geräteidentifikator besteht aus deviceIdentifier und deviceToken. Diese werden vom Device Management bei der Geräteregistrierung erzeugt, durch das ePA-FdV übernommen und sind nicht durch den Nutzer konfigurierbar. Der Gerätestatus bezeichnet den Status der	Rückgabewerte bei Geräteregistrierung der Operation `I_Device_Management_Insurant::registerDevice` gemäß [I_Device_Management_Insurant]

	Geräteregistrierung.	
Aktenkontoinhaber: Letzte Anmeldung zum Aktenkonto	Zeitpunkt des letzten erfolgreichen Logins des Nutzers in das Aktenkonto von dem Gerät; dient der Auswahl der Benachrichtigungen. Der Parameter wird durch das ePA-FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.	Timestamp
für jede Vertretung: Name des Versicherten	Name des zu vertretenden Versicherten Der Datensatz Vertretung (Versicherten Name, Akten-ID, ...) muss für mehrere Vertretungen konfigurierbar sein.	
für jede Vertretung: FQDN Anbieter ePA-Aktensystem	FQDN für den Zugriff auf das ePA-Aktensystem des zugehörigen Anbieters für den zu vertretenden Versicherten	Wert als Ergebnis von A_24588*
für jede Vertretung: Versicherten-ID des zu Vertretenden	unveränderlicher Teil der KVNR des zu Vertretenden	alphanummerisch, 10-stellig
für jede Vertretung: letzte Anmeldung zum Aktenkonto	Zeitpunkt des letzten erfolgreichen Logins des Nutzers in das	Timestamp

	Aktenkonto von dem Gerät. Dient der Auswahl der Benachrichtigungen. Der Parameter wird durch das ePA-FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.	
Benachrichtigungen aktivieren	Benachrichtigung über neue, geänderte oder gelöschte ePA-Dokumente	ja/nein Default: ja
Benachrichtigungszeitraum		Optionen: • seit der letzten Anmeldung • seit einem konkreten Datum • in einem durch den Versicherten einstellbaren, beliebig zurückliegenden Zeitraum (x Wochen, x Monate) bis zum aktuellen Datum • Default: seit der letzten Anmeldung
Gerätenamen	Bezeichnung des GdV durch den Nutzer, um es im Freischaltprozess und während der Geräteverwaltung leichter wiedererkennen zu können.	string, 64 Zeichen
URL des Signaturdienstes	URL des Signaturdienstes des Kostenträgers	URL

[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Entsprechend dem für die Akten-ID spezifizierten Format, besitzt die Akten-ID einen variablen und einen konstanten Anteil. Der variable Anteil entspricht der Versicherten-ID, welche bspw. auf der eGK des Versicherten aufgedruckt ist. Das Erfassen der Akten-ID kann auf die Versicherten-ID beschränkt werden und automatisch um die konstanten Anteile ergänzt werden.

A_15293 -ePA-Frontend des Versicherten: Konfigurationsparameter verwalten
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, die nicht automatisch bestimmbaren Parameter aus A_15292* zu verwalten (anzeigen, ändern, löschen). **[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_24588 -ePA-Frontend des Versicherten: Lokalisierung eines Aktenkontos
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, die Lokalisierungsinformation für ein gewünschtes Aktenkonto (Vertreterszenario) durch Abruf der herstellerspezifischen Schnittstelle gemäß A_24801* am ePA-Aktensystem zu ermitteln.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Die Operation zur Ermittlung der Liste aller Kostenträger und der FQDN, unter der deren ePA-Aktensystem im Internet erreichbar ist, wird nicht normativ vorgegeben, sondern ist herstellerspezifisch.

Hinweis: Während eines Wechsels eines Kostenträgers zu einem anderen Aktensystem wird es für diesen Kostenträger zwei Einträge in der Liste geben. In diesem Fall muss das ePA-FdV probieren auf die konkrete Akte zuzugreifen um zu erkennen, auf welchem Aktensystem die Akte zu finden ist. Es muss darauf geachtet werden, dass dem Nutzer nicht mehrere Einträge für einen Kostenträger angezeigt werden.

A_23209 -Konfiguration SSO durch den Nutzer
Das ePA-FdV MUSS sicherstellen, dass der Nutzer konfigurieren kann, für welche Fachdienste er seine Zustimmung für ein SSO erteilt, diese Konfiguration persistent speichern und bei der Initialisierung laden.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_25047 -ePA-Frontend des Versicherten: Default-Einstellung kein SSO
Das ePA-FdV MUSS sicherstellen, dass in der Default-Einstellung kein SSO konfiguriert ist und somit für jeden Fachdienst eine explizite Authentisierung des Nutzers erforderlich ist. **[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_25048 -ePA-Frontend des Versicherten: Information des Nutzers über SSO
Das ePA-FdV MUSS den Nutzer im ePA-FdV mindestens vor der ersten Nutzung eines SSO über die Sicherheitskonsequenzen bei der Nutzung eines SSO informieren. **[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

5.5 Bereitstellung für UX-Messdaten

Zur Verbesserung der User Experience werden Messdaten erfasst und an das Aktensystem übertragen. Dabei werden folgende Anwendungsfälle betrachtet:

A_24669-01 -ePA-Frontend des Versicherten: UX-Messdaten erfassen
Das ePA-Frontend des Versicherten MUSS bei Durchführung der Anwendungsfälle aus Tab_UX_KPI_Messung_ePA die in der Spalte "Beschreibung" beschriebene Messung durchführen und das Ergebnis in Millisekunden speichern.

Tabelle 6: Tab_UX_KPI_Messung_ePA

UX-Anwendungsfälle	Beschreibung
UX_Login_V	Es wird der Zeitraum gemessen, den ein Nutzer nach der Auswahl einer ePA warten muss, bis die angeforderte Akte geöffnet ist. Dabei beginnt die Messung mit der letzten Versicherteninteraktion (z. B. Antippen eines Feldes "ePA mit KVNR A12345680") bevor die Akte geöffnet wird und endet mit der Anzeige von Inhalten der Akte (z. B. der Information über Aktivitäten seit dem letzten Login, Dokumentenübersicht,

	allgemeine Informationen zur Akte wie Anzahl Befugnisse, Anzahl Dokumente).
UX_Doc_Upload_V	Es wird der Zeitraum gemessen, den ein Nutzer nach dem Befehl zum Hochladen eines Dokumentes warten muss, bis dieses Dokument in der ePA sichtbar ist oder die Information über den Erfolg/Misserfolg der Operation angezeigt wird.
UX_Doc_Download_V	Es wird der Zeitraum gemessen, den ein Nutzer nach dem Befehl zum Herunterladen eines Dokumentes warten muss, bis dieses Dokument vollständig heruntergeladen wurde.
UX_LEI_search	Es wird der Zeitraum gemessen, den ein Nutzer nach der Eingabe von Suchparametern warten muss, bis die ersten Suchergebnisse angezeigt werden.
UX_MHD_Search_V	Es wird der Zeitraum zwischen "Absenden der MHD Find Document References - Nachricht" bis zur "Anzeige der Ergebnisse" gemessen.
UX_MHD_Download_V	Es wird der Zeitraum zwischen "Absenden der MHD Retrieve Document - Nachricht" bis zur "Information des Nutzers über den erfolgreichen Download" / "Anzeige des Dokumentes" gemessen.

Es sind ausschließlich Anwendungsfälle von Nutzern zu berücksichtigen, bei denen sie das zu ihrem FdV zugehörige Aktensystem nutzen. Vertreter-Szenarios, in denen ein Nutzer über sein FdV mit einem anderen Aktensystem kommuniziert, sind nicht zu berücksichtigen.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_24670 -ePA-Frontend des Versicherten: UX-Messdaten übertragen
Das ePA-Frontend des Versicherten MUSS unmittelbar nach erfolgreicher Durchführung der UX-Anwendungsfälle das Messergebnis im Hintergrund an das gleiche Aktensystem übermitteln und den gespeicherten Wert löschen, sofern die Übermittlung erfolgreich war.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Hinweis: Die Schnittstelle zur Übermittlung der Messwerte zwischen FdV und Aktensystem ist nicht normiert, da die Entwicklung von FdVs und Aktensystem je Kasse abgestimmt erfolgt.
"*Im Hintergrund*" *bedeutet, dass die Übermittlung einerseits automatisch (ohne Nutzerinteraktion) geschieht und andererseits für den Nutzer auch keine* "*Wartezeit*" *entsteht.*

6 Funktionsmerkmale

6.1 Allgemein

6.1.1 Kommunikation mit dem ePA-Aktensystem

Das ePA-Frontend des Versicherten nutzt TLS-Verbindungen für die Kommunikation zum ePA-Aktensystem. Es verbindet sich mit der Komponente Access Gateway des ePA-Aktensystems. Das ePA-Frontend des Versicherten führt eine Authentisierung des Servers durch, wobei sich das Access Gateway mittels eines öffentlich prüfbaren Zertifikats authentisiert. Für die TLS-Verbindung gelten die Vorgaben aus [gemSpec_Krypt].

Im Falle einer Vertretung wird dem Vertreter durch das ePA-Aktensystem der Name des Anbieters für den Zugriff auf das ePA-Aktensystem mitgeteilt, damit der Vertreter beim Login den relevanten Anbieter aus der Anbieterliste auswählen kann.

Falls für den FQDN mehrere IP-Adressen hinterlegt sind, wählt das ePA-Frontend des Versicherten zufällig eine der IP-Adressen als Endpunkt für den Verbindungsaufbau aus. Die Komponente Access Gateway weist bei Vollauslastung der Systemressourcen im ePA-Aktensystem die Verbindunganfrage ab. In diesem Fall kann das ePA-Frontend des Versicherten zufällig eine der weiteren IP-Adressen für einen neuen Verbindungsaufbau auswählen.

A_15297-01 -ePA-Frontend des Versicherten: Kommunikation über TLS-Verbindung
Das ePA-Frontend des Versicherten MUSS mit dem Access Gateway ausschließlich über TLS kommunizieren.**[**Frontend_Vers_ePA,funkt. Eignung: Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA,<=**]**

A_15298-01 -ePA-Frontend des Versicherten: Unzulässige TLS-Verbindungen ablehnen
Das ePA-Frontend des Versicherten MUSS bei jedem Verbindungsaufbau das Access Gateway anhand seines TLS-Zertifikats authentifizieren und MUSS die Verbindungen ablehnen, falls die Authentifizierung fehlschlägt.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Das Access Gateway authentisiert sich mit einem extended-validation-X.509-Zertifikat. Für Kriterien zur Prüfung des Zertifikates siehe "6.1.5- Zertifikatsprüfung".

Es gelten die Bedingungen für das TLS-Handshake gemäß [gemSpec_PKI#GS-A_4662].

A_15300-02 -ePA-Frontend des Versicherten: TLS-Verbindungsaufbau nach Notwendigkeit
Das ePA-Frontend des Versicherten MUSS eine TLS-Verbindung zum Access Gateway aufbauen, wenn die ausgeführte Operation eine Kommunikation zum ePA-Aktensystem oder den zentralen Diensten der TI beinhaltet und keine TLS-Verbindung zum Access Gateway für die User Session besteht.**[**Frontend_Vers_ePA,funkt. Eignung: Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA,<=**]**

A_15301-02 -ePA-Frontend des Versicherten: TLS-Verbindung beenden
Das ePA-Frontend des Versicherten MUSS die für eine User Session aufgebaute TLS-Verbindung zum Access Gateway schließen, wenn die User Session beendet wird. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_15303-01 -ePA-Frontend des Versicherten: SOAP-Responses valide

Das ePA-Frontend des Versicherten MUSS bei allen SOAP-Responses eine Schemaprüfung durchführen und mit einer qualifizierten Fehlermeldung abbrechen, wenn die Nachricht nicht valide ist.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_24678 -ePA-Frontend des Versicherten: Useragent
Das ePA-Frontend des Versicherten MUSS das HTTP Header Element mit dem Namen "x-useragent" bei jedem Request sowohl im HTTP-Header der VAU-Nachricht, als auch im HTTP-Header der Nachricht an den Service gemäß A_22470* senden.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_27704 -ePA-Frontend des Versicherten: Requestkennung
Das ePA-Frontend des Versicherten KANN für einen Request eine Requestkennung als UUID erzeugen und die Requestkennung im HTTP Header Element mit dem Namen "X-Request-ID" sowohl im HTTP-Header der VAU-Nachricht, als auch im HTTP-Header der Nachricht an den Service senden.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.1.2 Sicherer Kanal zur Aktenkontoverwaltung

Das ePA-Frontend des Versicherten kommuniziert als ePA-Client mit der Aktenkontoverwaltung in einer Vertrauenswürdigen Ausführungsumgebung (VAU). Diese stellt sicher, dass sensible Klartext-Daten wie z. B die medizinischen Daten des Versicherten sicher vor Angriffen verarbeitet werden können. Die Daten werden ausschließlich in einem VAU-Kanal zwischen ePA-Frontend des Versicherten und ePA-Aktensystem übertragen.

Das ePA-Frontend des Versicherten initiiert den Aufbau eines VAU-Kanals zum Aktensystem. Dabei authentisiert sich die VAU mit ihrem Zertifikat als authentische VAU des Aktensystems.

A_24557 -Frontend des Versicherten: Kommunikation mit der Vertrauenswürdigen Ausführungsumgebung (VAU)
Das Frontend des Versicherten MUSS als ePA-Client für die Kommunikation mit der Vertrauenswürdigen Ausführungsumgebung (VAU) die Vorgaben aus [gemSpec_Krypt#6 und #3.14] umsetzen.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Für Informationen zum Kommunikationsprotokoll zwischen dem ePA-Frontend des Versicherten und einer VAU siehe [gemSpec_Krypt#3.15 ePA-spezifische Vorgaben] und [gemSpec_Krypt#8 VAU-Protokoll für ePA füralle].

Anschließend wird für den Nutzer, repräsentiert durch die GesundheitsID, mit Hilfe des sektoralen IDPs eine User Session angelegt. Diese User Session ermöglicht den Zugriff auf alle Aktenkonten des Aktensystems, sofern der Nutzer für diese befugt ist. Durch eine Anfrage an eine bestimmte Akte wird diese in der User Session als Health Record Context geladen und der Nutzer kann mit der Akte arbeiten.

Eine User Session in einem ePA-Frontend des Versicherten bezeichnet die Sitzung eines Nutzers, in der dieser fachliche Anwendungsfälle im Aktenkonto eines Versicherten ausführt. Hierbei kann es sich um das Aktenkonto des Nutzers selber (Nutzer ist Aktenkontoinhaber=Versicherter) oder um das Aktenkonto eines zu vertretenden Versicherten handeln, wenn dieser eine entsprechende Vertretung für den Nutzer eingerichtet hat. Die im Rahmen der User Session ausgehandelten Daten werden als Session-Daten bezeichnet.

Ein Aktenkonto wird eindeutig durch eine Akten-ID (unveränderbare Teil der KVNR; 10 Stellen) referenziert.

Eine User Session im ePA-Frontend des Versicherten beginnt mit dem Login und endet mit dem Logout des Nutzers oder einem impliziten Logout. Das Logout erfolgt auf Wunsch des Nutzers, mittels eines Time-outs oder nach einem Fehler beim Login.

A_15294-02 -ePA-Frontend des Versicherten: Login nach Notwendigkeit
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "Login User" vor der Ausführung einer fachlichen Operation, welche eine Kommunikation mit dem ePA-Aktensystem beinhaltet, starten, wenn keine gültigen Session-Daten vorhanden sind. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_15295-02 -ePA-Frontend des Versicherten: Beenden der User Session
Das ePA-Frontend des Versicherten MUSS zum Beenden der User Session den Anwendungsfall "Logout User" ausführen.**[**Frontend_Vers_ePA,funkt. Eignung: Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA,<=**]**

A_15296-02 -ePA-Frontend des Versicherten: Abmeldung des Nutzers nach Inaktivität
Das ePA-Frontend des Versicherten MUSS den Nutzer nach spätestens 20 Minuten Inaktivität (Zeitspanne nach der letzten Nutzer-Aktivität) automatisch abmelden und die User Session beenden.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Das FdV kann dem Nutzer vor der Abmeldung wegen Inaktivität einen Hinweis einblenden, der es dem Nutzer ermöglicht, die User Session fortzuführen.

Zu einer User Session im FdV gehören Session-Daten, welche für die Dauer der User Session vorzuhalten sind. Die Session-Daten beinhalten die ausgehandelten VAU-Schlüssel gemäß [gemSpec_Krypt#VAU-Protokoll für ePA-für-alle].

Die Session-Daten ergeben sich aus dem Anwendungsfall "Login User".

Nach dem Ende der User Session (Anwendungsfall "Logout User") werden die Session-Daten verworfen.

A_15304-02 -ePA-Frontend des Versicherten: Umsetzung sicherer Kanal zur Aktenkontoverwaltung
Das ePA-Frontend des Versicherten MUSS die im Rahmen des sicheren Verbindungsaufbaus zur Aktenkontoverwaltung ausgehandelten Sitzungsschlüssel verwenden, um den HTTP Body aller über den sicheren Kanal zu sendenden Requests an die Aktenkontoverwaltung zu verschlüsseln und alle über den sicheren Kanal gesendeten Responses von der Aktenkontoverwaltung zu entschlüsseln.**[**Frontend_Vers_ePA,funkt. Eignung: Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA,<=**]**

6.1.3 Authentisierung

Zur Authentisierung des Nutzers wird ein Request an den Authorization Service im ePA-Aktensystem gesendet. Es folgt folgender Ablauf:

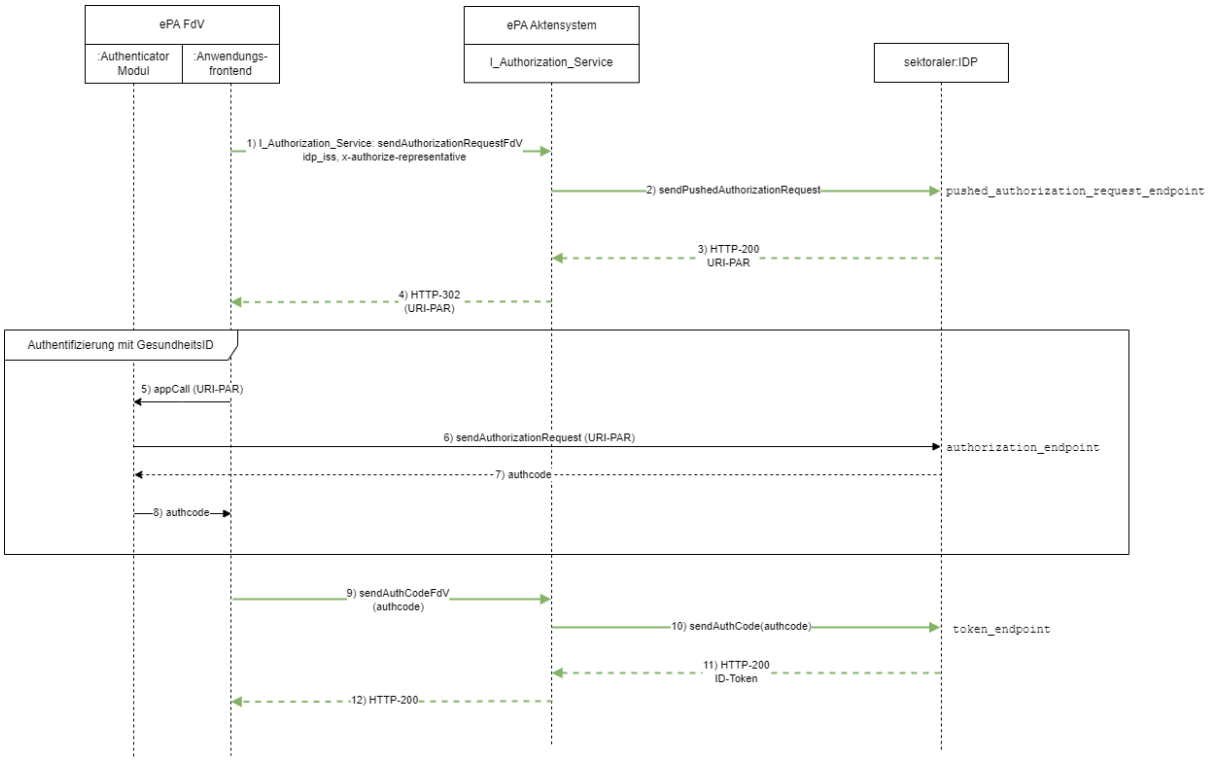


Abbildung 2: Authentisieren des Nutzers

Das ePA FdV agiert generell analog zu anderen Anwendungsfrontends, welche gegenüber dem Authorization Server ihres Fachdienstes die Anmeldung des Nutzers über einen sektoralen Identity Provider der Föderation unterstützen. Dazu werden die generellen Anforderungen aus [gemSpec_IDP_Frontend#Kapitel9 Nutzung sektoraler Identity Provider] konkretisiert bzw. sind für die Anwendung der elektronischen Patentenakte nicht relevant.

Das Authenticator-Modul übernimmt die Authentisierung des Nutzers gegenüber dem für den Versicherten zuständigen sektoralen IDP.

A_24829 -ePA-Frontend des Versicherten: Kenntnis über issuer ID des zugehörigen sektoralen IDP
Das ePA-Frontend des Versicherten MUSS die Adresse des für die Authentisierung seiner Nutzer verantwortlichen sektoralen IDP kennen und bei Autorisierungsanfragen gegenüber allen Aktensystemen verwenden. Dabei handelt es sich um die Identität (iss URL) des IDP innerhalb der Open-ID Connect Föderation der Telematikinfrastruktur.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Bevor im ePA-Aktensystem eine User Session für diesen Nutzer etabliert wird, erfolgt die Prüfung, ob das vom Nutzer verwendete Gerät registriert ist. Wenn nicht, dann wird die Geräteregistrierung gestartet.

6.1.4 Geräteregistrierung

Um einen möglichen Missbrauch und Identitätsdiebstahl erkennen zu können, wird eine Berechtigungsprüfung für das Gerät des Nutzers umgesetzt. Hierzu wird bei erstmaliger Nutzung des Gerätes eine Geräteregistrierung am Home-AS aufgerufen. Als Home-AS wird das ePA-Aktensystem desjenigen Betreibers bezeichnet, der vom Kostenträger des Versicherten beauftragt wurde. Als Ergebnis wird an das ePA-FdV die DeviceID mit deviceIdentifier als Gerätekennung und das deviceToken als Sicherheitsmerkmal zurückgegeben. Diese DeviceID wird für den Nutzer im ePA-FdV persistent gespeichert.

Ist für den Nutzer eine Geräteregistrierung für das verwendete Gerät bereits erfolgt kann diese für folgende Logins erneut genutzt werden. Der Zugriff auf ein Aktenkonto ist nur mit einem registrierten Gerät möglich.

Die DeviceID einer neuen Geräteregistrierung muss vor der Verwendung durch den Nutzer in der Geräteverwaltung des Aktensystems einmalig bestätigt werden. Dafür erhält der Nutzer über einen separaten Benachrichtigungskanal (E-Mail) den Geräteregistrierungscode (Confirmation Code) für dieses Gerät.

Falls der Nutzer als Vertreter auf ein anderes als sein Home-AS zugreifen möchte muss das ePA-FdV eine Bestätigung der Geräteregistrierung (deviceAttestation) am Home-AS abfragen und diese beim Login an einem anderen als dem Home-AS als Nachweis der Geräteregistrierung in der Operation sendAuthCodeFdV mitgeben.

A_15305-03 -ePA-Frontend des Versicherten: Geräteinformationen speichern
Falls eine Geräteregistrierung beim Login des Nutzers erfolgt, MUSS das ePA-Frontend des Versicherten die Geräteinformationen persistent und sicher speichern.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_24924 -ePA-Frontend des Versicherten: Geräteinformationen anzeigen
Falls eine Geräteregistrierung beim Login des Nutzers erfolgt, MUSS das ePA-Frontend des Versicherten den Nutzer darüber informieren, dass der Nutzer die Geräteregistrierung bestätigen muss und ein Zugang zum ePA-Aktensystem erst nach erfolgter Verifikation durch den Nutzer möglich ist.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_26073-01 -ePA-Frontend des Versicherten: email-Adresse für Geräteregistrierungscode anzeigen
Das ePA-Frontend des Versicherten MUSS dem Nutzer die email-Adresse, an welche der Geräteregistrierungscode versendet wurde, anzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.1.5 Zertifikatsprüfung

Es gelten die Vorgaben für die Prüfung von Zertifikaten gemäßA_24624* und A_24958* aus [gemSpec_Krypt].

A_15872-01 -ePA-Frontend des Versicherten: verpflichtende Zertifikatsprüfung
Das ePA-Frontend des Versicherten MUSS alle Zertifikate, die es aktiv verwendet (bspw. TLS-Verbindungsaufbau) auf Integrität und Authentizität prüfen. Falls die Prüfung kein positives Ergebnis ("gültig") liefert, so MUSS es die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen.
Das ePA-Frontend des Versicherten MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Folgende Vorgaben gelten für die Prüfung von Internet-Zertifikaten.

A_15887-03 -ePA-Frontend des Versicherten: Prüfung Internet-Zertifikate
Das ePA-Frontend des Versicherten MUSS für die Prüfung des internetseitigen Zertifikats des Zugangsgateways des Versicherten das Zertifikat auf ein CA-Zertifikat einer CA, die die "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (https://cabforum.org/baseline-requirements-documents/) erfüllt, kryptographisch (Signaturprüfung) zurückführen können. Ansonsten MUSS es das Zertifikat als "ungültig" bewerten.
Es MUSS die zeitliche Gültigkeit des Zertifikats prüfen. Falls diese Prüfung negativ ausfällt, muss es das Zertifikat als "ungültig" bewerten.
Bei der Prüfung auf eine gültige CA SOLL die Prüfung auf ausgewählte Zertifikate aus der Liste https://wiki.mozilla.org/CA/Included_Certificates -> "Included Root CA

Certificates" beschränkt werden (bez. Auswahl vgl. Hinweis 2 zu A_15887-*).
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis 1: Der erste Teil von A_15887- ist gleichbedeutend damit, dass das CA-Zertifikat im Zertifikats-Truststore eines aktuellen Webbrowsers ist.*

Hinweis 2: gemäß Absprache mit den ePA-Industriekonsortien soll bei der Prüfung nach A_15887- die Menge der zulässigen CA:*

1. *initial auf die CA-Zertifikate von GlobalSign, DigiCert, Sectigo/Entrust und D-Trust aus der Liste von https://wiki.mozilla.org/CA/Included_Certificates -> "Included CA Certificates" beschränkt werden.*
2. *weiterhin muss die Liste die CA-Zertifikate von ISRG (Let's encrypt) enthalten (fachlicher Hintergrund: das Gesundheitsportal https://gesund.bund.de/ verwendet diesen TSP).*
3. *und zukünftig auf eine Menge von CA-Zertifikaten beschränkt werden, die in Abhängigkeit zu [gemSpec_Aktensystem_ePAfueralle#A_22409] steht und bei Änderung von der gematik an die ePA-FdV-Hersteller gesendet wird.*

6.1.6 Dokumente

Das ePA-Aktensystem unterstützt die einzelne Dokumente bis zu einer Größe von 25 MB.

A_15283-01 -ePA-Frontend des Versicherten: Dokumentgrößen von 25 MB
Das ePA-Frontend des Versicherten MUSS für alle Außenschnittstellen, in denen ein Dokument verarbeitet wird, Dokumente mit einer Größe von mindestens 25 MB unterstützen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_21301 -ePA-FdV für Desktop-Plattformen: Kein Ausführen von aktiven Inhalten bei der Anzeige
Das ePA-FdV DARF bei der Anzeige von Dokumenten aktive Elemente NICHT ausführen.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Aktive Elemente sind alle code-ausführenden Anteile eines Dokuments, also etwa Makros oder Skripte. Diese dürfen im Kontext des FdV nicht ausgeführt werden, etwa indem auch bei zugelieferten Bibliotheken diese Funktionalität deaktiviert wird. Die Verwendung explizit externer Applikationen wird dabei nicht betrachtet, da hier aus Sicht des ePA-FdV der Vorgang mit dem Herunterladen des Dokuments als abgeschlossen angesehen wird.

6.1.7 ePA-FdV für Desktop-Plattformen

Wird das FdV nicht auf einem mobilen Gerät betrieben, muss die Verwendung des FdV durch mehrere Versicherte für den Zugriff auf die individuellen ePA möglich sein.

A_21358 -ePA-FdV für Desktop-Plattformen: Mehrbenutzerfähigkeit des Desktop-Clients
Das ePA-FdV MUSS die Ausführung der Aktensteuerung über verschiedene, lokale Benutzerkonten des Betriebssystems oder alternativ eine FdV-interne Benutzer-Kontensteuerung ermöglichen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_27448 -ePA-FdV für Desktop-Plattformen - Integration eines Authenticator Moduls für Desktop-Plattformen
Das ePA-Frontend des Versicherten für Desktop Plattformen MUSS ein Authenticator Modul für Desktop-Plattformen gemäß [gemSpec_IDP_Sek#5.4] integrieren.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_27449 -ePA-FdV für Desktop-Plattformen - Authentisierung mit eGK und PIN
Das ePA-Frontend des Versicherten für Desktop Plattformen MUSS mindestens die Authentisierung am IdPmittels eGK und PIN für stationäre Endgeräte gemäß [I_Authorization_Service] unterstützen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Hinweis: Zur Signalisierung der Anmeldung an der ePA mit eGK und PIN wird der Parameter x-authorize-egk verwendet.

6.1.8 Anbindung an das Nationale Gesundheitsportal

Durch die Kopplung der ePA mit dem Nationalen Gesundheitsportal ([NGP]) soll dem Versicherten über das ePA-FdV, unabhängig von Gesundheitskompetenzniveau, eine Hilfestellung angeboten werden, durch die sich der Versicherte einen Zugang zu einfach verständlichen und von Experten bereitgestellten Gesundheitsinformationen verschaffen kann.

Der Versicherte hat über das ePA-FdV zwei Möglichkeiten auf die Inhalte des Nationalen Gesundheitsportal zu zugreifen. Einerseits kann der Versicherte über eine selektive schlagwortbasierte Suche aus dem ePA-FdV heraus auf die Inhalte des Nationalen Gesundheitsportal zugreifen. In dem Fall, dass im ePA-Aktensystem bereits strukturierte Daten vorliegen (eingestellt durch den Versicherten und/oder befugte Leistungserbringerinstitutionen bzw. Dritte), kann der Versicherte über das ePA-FdV gezielt auf im Nationalen Gesundheitsportal liegende Informationen zu Symptomen, Diagnosen oder medizinische Fachbegriffe zugreifen.

A_21473 -Zugriff auf das Nationale Gesundheitsportal aus dem ePA-FdV
Das ePA-FdV MUSS es dem Versicherten ermöglichen, auf Informationen des Nationalen Gesundheitsportals barrierefrei zuzugreifen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_21474 -Verknüpfen von Daten aus der ePA mit Informationen des Nationalen Gesundheitsportals
Das ePA-FdV MUSS es dem Versicherten ermöglichen, Informationen des Nationalen Gesundheitsportals mit Daten, die in der elektronischen Patientenakte des Versicherten gespeichert sind, zu verknüpfen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.1.9 Anbindung VZD-FHIR-Directory

Zur Authentisierung am VZD-FHIR-Directory nutzt das ePA-FdV ein search-access_token, welches das ePA-FdV am ePA-Aktensystem anfragt.

A_25177 -ePA-Frontend des Versicherten: Authentisierung am FHIR VZD
Das ePA-Frontend des Versicherten MUSS einmalig für die Suche des Versicherten nach Einträgen imVZD-FHIR-Directory den Anwendungsfall "AF_10219* - Versicherter sucht Einträge im FHIR-Directory" gemäß [gemSpec_VZD_FHIR_Directory] als Client unterstützen und dabei für die Client Anfrage von search-access_token die Operation getFHIRVZDtoken gemäß [I_Authorization_Service] verwenden.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.1.10 Dokumente für den statischen Ordner "technical"

Ein ePA-FdV kann technische Dokumente (Dokumente, die nicht Dokumente des Versicherten sind) bei Bedarf im Ordner "technical" ablegen, beispielsweise für eine Synchronisation von Zuständen zwischen verschiedenen ePA-FdVs des Versicherten.

A_23145 -ePA-Frontend des Versicherten: formatCode für Dokumente des Ordners "technical"
Das ePA-Frontend des Versicherten MUSS für herstellerspezifische Dokumente, die im Ordner "technical" abgelegt werden, einen formatCode mit der codeSystem OID "2.25.154081344090540725127779452347992051720" und einem code der Form "urn:<Hersteller>:ig:<Bezeichner>:<Version>" verwenden.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Hinweis: Der Teil <Hersteller> in code muss dabei so gewählt werden, dass eine Verwechselung mit einem anderen Hersteller ausgeschlossen ist.

Ein ePA-Frontend des Versicherten soll alle Dokumente des Ordners "technical" ignorieren, wenn diese nicht für den Verarbeitungskontext des ePA-FdV notwendig oder unbekannt sind.

Der Ordner "technical" im ePA-Aktensystem hat einen unveränderlichen Wert von Folder.entryUUID, siehe A_24491.

6.2 Implementation ePA-Anwendungsfälle im FdV

In diesem Kapitel wird die Umsetzung der Anwendungsfälle für ePA für alle im FdV beschrieben.

6.2.1 Übergreifende Festlegungen

Voraussetzung für die Nutzung des FdV ist das Vorhandensein eines Aktenkontos:

- Der Versicherte verfügt über ein Aktenkonto oder ist als Vertreter für ein Aktenkonto befugt worden.
- Die Akten-ID (KVNR) des Aktenkontos, welche sich mittels der Versicherten-ID des Aktenkontoinhabers bestimmen lässt, ist im ePA-Frontend des Versicherten bekannt.
- Der FQDN für den Zugriff auf das ePA-Aktensystem ist im ePA-Frontend des Versicherten bekannt.

6.2.2 Fehlerbehandlung

Tritt ein Fehler bei der Verarbeitung von Operationsaufrufen des ePA-Aktensystems auf, dann antwortet das ePA-Aktensystem mit einer Fehlermeldung. Das Format und die verwendeten Fehlercodes sind in den Spezifikationen der Schnittstellen der jeweiligen Produkttypen beschrieben. Weiterhin können Fehler in der lokalen Verarbeitung auftreten.

A_15307-01 -ePA-Frontend des Versicherten: Abbruch bei Fehler im Anwendungsfall
Das ePA-Frontend des Versicherten MUSS, wenn bei der Abarbeitung der Aktivitäten eines Anwendungsfalls ein Fehler auftritt und keine Fehlerbehandlung beschrieben ist, den Anwendungsfall abbrechen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Das FdV muss dem Nutzer nach einem Abbruch eine verständliche Fehlermeldung anzeigen.

A_24402 -ePA-Frontend des Versicherten: verständliche Fehlermeldung
Falls das ePA-Frontend des Versicherten wegen eines Fehlers einen Anwendungsfall abbricht, dann MUSS der Nutzer mit einer verständlichen Fehlermeldung über den Fehler informiert werden.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Wenn die Möglichkeit besteht, dass der Nutzer das fehlerverursachende Problem selbst beheben kann, kann das FdV den Nutzer auf die Lösung hinweisen.

A_15308 -ePA-Frontend des Versicherten: Anzeige von Handlungsmöglichkeiten im Fehlerfall
Das ePA-Frontend des Versicherten SOLL dem Nutzer im Fehlerfall einen Hinweis geben, wenn es für den Nutzer Handlungsmöglichkeiten dazu gibt.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.2.3 Aktivitäten

Dieser Abschnitt beschreibt Aktivitäten, welche durch verschiedene Anwendungsfälle genutzt werden.

6.2.3.1 Authentisieren des Nutzers

Auslösung der Benutzerauthentifizierung

A_24830 -ePA-Frontend des Versicherten: Senden von Authorization Request gegenüber Aktensystemen
Das ePA-Frontend des Versicherten MUSS, um die Nutzerauthentifizierung zu starten, die Operation `sendAuthorizationRequestFdV`nutzen gemäß [I_Authorization_Service]. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Der Authorization Server kontaktiert nach dem Authorization Request des FdV auf einem direkten Kanal den sektoralen IDP mittels eines sogenannten Pushed Authorization Request, authentisiert sich diesem gegenüber und überträgt die für die Authentisierung des Nutzers gewünschten Parameter. Anschließend antwortet er dem FdV mit einem Satz an Parametern, welche an das Authenticator-Modul des sektoralen IDP übermittelt werden. Diese Response enthält Client-ID (des Aktensystems) und request_uri (Identifikation des Request beim zugehörigen IDP).

Das Authenticator-Modul kann entweder in das FdV integriert sein oder in einer separaten Authenticator-App implementiert sein.

Aufruf des Authenticator-Moduls

Das ePA-Frontend gibt die Antwort der sendAuthorizationRequestFdV Operation an das Authenticator-Modul weiter.

Ist das Authenticator-Modul in das ePA-Fontend integriert, so kann gemäß A_24756 [gemSpec_IDP_Frontend] ein Single-Sign-On (SSO) für den Zugriff auf die im ePA-Frontend integrierten TI-Fachdienste (z.B. E-Rezept) erfolgen. In diesem Fall erfolgt der Aufruf des Authenticator-Moduls über FdV interne Schnittstellen.

Ist das Authenticator-Modul in einer separaten Authenticator-App implementiert, so erfolgt der Aufruf als App-App-Kommunikation über Plattformmechanismen (deeplink, universal-link).

Das Authenticator-Modul realisiert die Authentisierung des Versicherten mittels eGK, online Ausweisfunktion oder weiteren zulässigen Verfahren des IDP.

Anwendungsinterner Aufruf durch Authenticator-Modul

Nach Abschluss der Nutzerauthentisierung durch den sektoralen IDP liefert dieser einen sogenannten Authorization_Code (Auth_Code) an das Authenticator-Modul des sektoralen IDP. Dieses leitet den Auth_Code zum FdV.

Ist das Authenticator-Modul in das FdV integriert, so erfolgt die Weiterleitung des Auth_Code über anwendungsinterne Schnittstellen.

Ist das Authenticator-Modul in einer separaten Authenticator-App implementiert, so erfolgt die Weiterleitung des Auth_Code als App-App-Kommunikation über Plattformmechanismen (deeplink, universal-link).

Anschließend wird über das FdV der Auth_Code an den Authorization Server des Aktensystems weitergeleitet.

A_24831 -ePA-Frontend des Versicherten: Weiterleitung des Auth_Code vom Authenticator-Modul zum Authorization Server
Das ePA-Frontend des Versicherten MUSS den Auth_Code vom Authenticator-Modul annehmen und an den Authorization-Server unter Verwendung der Operation sendAuthCodeFdV gemäß [I_Authorization_Service] weiterleiten.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Der Authorization Server des Aktensystems authentisiert sich nun erneut gegenüber dem sektoralen IDP und tauscht den Auth_Code gegen ein ID_TOKEN mit den personenbezogenen Daten des Versicherten ein.

Diese Daten werden anschließend der etablierten VAU Sitzung im ePA-Aktensystem zugeordnet und signalisieren damit dem Aktensystem die Identität des Nutzers.

Mit der *sendAuthCodeFdV*-Response erhält das FdV die Zugriffserlaubnis auf das Aktensystem. Die User-Session ist etabliert und fachliche Operationen sind möglich.

6.2.3.2 Leistungserbringerinstitution im Verzeichnisdienst der TI finden

Informationen zu Leistungserbringerinstitutionen sind im Verzeichnisdienst FHIR-Directory (VZD-FHIR-Directory) der TI-Plattform hinterlegt. Der Nutzer des FdV kann (bspw. für die Erstellung einer Befugnis für eine LEI) mit verschiedenen Kriterien nach Leistungserbringerinstitutionen im VZD-FHIR-Directory suchen und Informationen abrufen. Das Informationsmodell des Verzeichnisdienstes ist in [gemSpec_VZD_FHIR_Directory#4.1.1 Datenmodell] beschrieben.

Die Suche nach LEIs erfolgt primär über den Namen oder Institutionsnamen, aber auch über zusätzliche Informationen wie Adressen, Fachgebiet oder Institutionstyp.

A_24387-01 -ePA-Frontend des Versicherten: LEI - Search Operation am VZD-FHIR-Directory
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Leistungserbringerinstitutionen über die folgenden Suchkriterien im VZD-FHIR-Directory gemäß [gemSpec_VZD_FHIR_Directory#5.5] zu suchen.

Tabelle 7: FHIR Suche LEI

Suchkriterium	Beschreibung der Suche nach Leistungserbringerinstitutionen	FHIR-Ressource	FHIR-Element
Anzeigename	Name der Organisation/Einrichtung des Gesundheitswesens	[Organization in gematik Directory]	name
Institutionsname	Name der Organisation/Einrichtung des Gesundheitswesens		alias
Strasse,	Straße, Hausnummer	[Location in	address.line

Hausnummer		gematik Directory]	
Postleitzahl	Postleitzahl		address.postalCode
Ort	Ort		address.city
Bundesland	Bundesland		address.state
Institution/ Berufsgruppe	Institution	[Organization in gematik Directory]	type
TelematikID	Eindeutige ID der Institution in der TI	[Organization in gematik Directory]	identifier.system = "https://gematik.de/fhir/sid/telematik-id" identifier.value = telematikID
Fachgebiet	Fachabteilung	[HealthcareService in gematik Directory]	type

[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Da nur Leistungserbringerinstitutionen und keine einzelnen Leistungserbringer für den Zugriff auf ein Aktenkonto befugt werden können, müssen die durch den Nutzer eingegebenen Suchparameter ggf. für die Abfrage am VZD-FHIR-Directory so ergänzt werden, dass nur Informationen zu Leistungserbringerinstitutionen abgefragt werden.

A_25134 -ePA-Frontend des Versicherten: LEI - Volltextsuche am VZD-FHIR-Directory
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, LEIs über die Volltextsuche im VZD-FHIR-Directory gemäß https://github.com/gematik/api-vzd/blob/main/docs/FHIR_VZD_HOWTO_Search.adoc#full-text-searchzu suchen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.3.3 DiGA im Verzeichnisdienst der TI finden

Informationen zu DiGAs sind im Verzeichnisdienst FHIR-Directory (VZD-FHIR-Directory) der TI-Plattform hinterlegt.

Der Nutzer des FdV kann (bspw. für die Erstellung einer Befugnis für eine DiGA) mit verschiedenen Kriterien nach DiGAs im VZD-FHIR-Directory suchen und Informationen abrufen. Das Informationsmodell des Verzeichnisdienstes ist in [gemSpec_VZD_FHIR_Directory#4.1.1 Datenmodell] beschrieben.

Die Suche nach DiGAs erfolgt primär über den Namen der DiGA.

A_25131 -ePA-Frontend des Versicherten: DiGA - Search Operation am VZD-FHIR-Directory
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, DiGAs über die folgenden Suchkriterien im VZD-FHIR-Directory gemäß [gemSpec_VZD_FHIR_Directory#5.5] zu suchen.

Tabelle 8: FHIR Suche DiGA

Suchkriterium	Beschreibung der Suche nach DiGAs	FHIR-Ressource	FHIR-Element
Anzeigename	Name der DiGA	[Organization in gematik Directory]	name
Institution/ Berufsgruppe	Institution		type
TelematikID	Eindeutige ID der Institution in der TI		identifier.system = "https://gematik.de/fhir/sid/telematik-id" identifier.value = telematikID

[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_25133 -ePA-Frontend des Versicherten: DiGA - Volltextsuche am VZD-FHIR-Directory
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, DiGAs über die Volltextsuche im VZD-FHIR-Directory gemäß https://github.com/gematik/api-vzd/blob/main/docs/FHIR_VZD_HOWTO_Search.adoc#full-text-searchzu suchen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.3.4 Land (EU-Zugriff) im Verzeichnisdienst der TI finden

Informationen zu Ländern (EU-Zugriff) sind im Verzeichnisdienst FHIR-Directory (VZD-FHIR-Directory) der TI-Plattform hinterlegt.

Der Versicherte kann über das ePA-FdV (bspw. für die Erstellung einer Befugnis EU-Zugriff) mit verschiedenen Kriterien nach dem entsprechenden Land im VZD-FHIR-Directory suchen und Informationen abrufen. Das Informationsmodell des Verzeichnisdienstes ist in [gemSpec_VZD_FHIR_Directory#4.1.1 Datenmodell] beschrieben.

Die Suche nach dem Land erfolgt primär über den Namen des Landes.

A_25828-01 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Search Operation am VZD-FHIR-Directory
Das ePA-Frontend des Versicherten MUSS die Suche des Versicherten nach einem Land (EU-Zugriff) im VZD-FHIR-Directory gemäß [gemSpec_VZD_FHIR_Directory#5.5] auf professionOID = oid_ncpeh und specialty =60591-5 einschränken.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Hinweis: professionOID ist Elementtype:profession der FHIR-Ressource [Organization in gematik Directory] und specialty ist Element der FHIR-Ressource [HealthcareService in gematik Directory].

6.2.4 Nutzerzugang ePA

6.2.4.1 Login User

Mit diesem Anwendungsfall wird eine sichere Verbindung in das ePA-Aktensystem für den Nutzer gestartet.

Für die Anmeldung des Nutzers wird die GesundheitsID verwendet. Das ePA-Frontend des Versicherten unterstützt den Vertreter bei der Auswahl des Aktensystems.

A_24746 -ePA-Frontend des Versicherten: Login User - Auswahl Aktensystem für Vertreter
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login User" einen Vertreter dabei unterstützen, das Aktensystem unter Verwendung der vom Aktensystem bereitgestellten Operation gemäß A_24801* auszuwählen.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_15340-02 -ePA-Frontend des Versicherten: Login - Session-Daten für Nutzer prüfen
Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "Login User" ohne Fehler abbrechen, wenn bereits gültige Session-Daten zu dem Nutzer vorliegen.
[Frontend_Vers_ePA,funkt. Eignung: Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA,<=**]**

A_15343-02 -ePA-Frontend des Versicherten: Login - Authentisieren des Nutzers
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login User" die übergreifende Aktivität "Authentisieren des Nutzers" ausführen.
[Frontend_Vers_ePA,funkt. Eignung: Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA,<=**]**

A_25227 -ePA-Frontend des Versicherten: Login - registriertes Gerät
Falls das verwendete Gerät des Nutzers bereits registriert ist, MUSS das ePA-Frontend des Versicherten im Anwendungsfall "Login User" diese Registrierungsdaten bei der Kommunikation mit dem Authorization Service verwenden gemäß [I_Authorization_Service].**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Da die Registrierung eines Gerätes immer im Home-AS erfolgt werden 2 Fälle beim Login und bereits erfolgter Registrierung unterschieden:

1. Login in Home-AS
Die Registrierungsdaten sind mit der DeviceID im ePA-FdV persistiert. Es wird die DeviceID beim Login übergeben.

2. Login in anderem ePA-Aktensystem, nicht Home-AS (Vertreter)

Das ePA FdV ruft am Device Management Service des Home-AS die Operation `getDeviceAttestation` auf. Diese Operation liefert ein vom Home-AS signiertes Token `deviceAttestation`, welches die Geräteregistrierung bestätigt. Das Token`deviceAttestation` wird beim Login übergeben. Dadurch entfällt eine erneute Registrierung an einem weiteren ePA-Aktensystem.

A_26149 -ePA-Frontend des Versicherten: Login - Device Attestation
Falls ein Login an einem NICHT Home-As erfolgt MUSS das ePA-Frontend des Versicherten sich bestätigen lassen, dass das verwendete Gerät des Nutzers bereits im Home-AS registriert ist. Dies erfolgt durch Aufruf der Operation `getDeviceAttestation` gemäß [I_Authorization_Service].**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25293 -ePA-Frontend des Versicherten: Login - neues Gerät registrieren
Falls das verwendete Gerät des Nutzers noch nicht registriert ist, MUSS das ePA-Frontend des Versicherten im Anwendungsfall "Login User" die Geräteregistrierung unter

Verwendung der Operation`registerDevice` gemäß [I_Device_Management_Insurant] aufrufen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Benachrichtigungen

Die Anzeige von Benachrichtigungen im Anwendungsfall "Login User" ist optional gemäß den Konfigurationsdaten.

A_15350 -ePA-Frontend des Versicherten: Login - Benachrichtigungen anzeigen optional
Das ePA-Frontend des Versicherten MUSS, wenn die Konfiguration Benachrichtigungen aktivieren = nein gesetzt ist, die Aktivitäten zum Anzeigen von Benachrichtigungen ignorieren.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_15352-04 -ePA-Frontend des Versicherten: Login - Protokolldaten abfragen
Das ePA-Frontend des Versicherten MUSS in einer User Session beim erstmaligen Zugriff auf ein Aktenkonto, wenn die Konfiguration Benachrichtigungen aktivieren = ja gesetzt ist, die Protokolldaten des ePA-Aktensystems abfragen und das Ergebnis gemäß der Konfiguration Benachrichtigungszeitraum filtern. Falls gemäß A_15354-* noch kein Wert "Zugriff auf das Aktenkonto" vorliegt, ist es ausreichend, wenn die Protokolldaten für den Zeitraum der letzten 30 Tage abgefragt werden. Der Versicherte MUSS dann über eine Einschränkung der Protokolldaten informiert werden.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_15353-01 -ePA-Frontend des Versicherten: Login - Benachrichtigungen-Anzeige
Das ePA-Frontend des Versicherten MUSS eine Anzeige für Benachrichtigungen umsetzen, in der die Protokolleinträge für folgende Zugriffe übersichtlich dargestellt werden:

- Dokumente einstellen aus der LEI-Umgebung
- Dokumente löschen aus der LEI-Umgebung
- Dokumente einstellen aus der privaten Umgebung
- Dokumente löschen aus der privaten Umgebung

[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_15354-02 -ePA-Frontend des Versicherten: Konfiguration letzte Anmeldung
Das ePA-Frontend des Versicherten MUSS in einer User Session beim erstmaligen Zugriff auf ein Aktenkonto den Wert "Zugriff auf das Aktenkonto" für das Aktenkonto in den Konfigurationsdaten aktualisieren.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.2.4.2 Logout User

Dieser Anwendungsfall beendet eine User Session und verwirft die für den sicheren Kanal zur Aktenkontoverwaltung ausgehandelten VAU-Schlüssel.

A_24759 -ePA-Frontend des Versicherten: Logout User
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Logout User" die OperationlogoutFdV gemäß [I_Authorization_Service] aufrufen.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_15358-02 -ePA-Frontend des Versicherten: Logout - Session-Daten löschen
Das ePA-Frontend des Versicherten MUSS zum Abschluss des Anwendungsfall "Logout User" alle Session-Daten aus dem lokalen Speicher löschen.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis: Zu den Session-Daten gehören z. B. die geheimen Schlüssel für ein SSO oder für den VAU-Kanal.

6.2.5 Aktenkontoverwaltung

Der Widerspruch bzw. die Rücknahme des Widerspruchs in die grundsätzliche Nutzung der ePA und die Übertragung von Abrechnungsdokumenten in die ePA durch den Kostenträger werden durch den Kostenträger verwaltet und werden nicht über das hier dargestellte Widerspruchsmanagement der ePA verwaltet.

Der Versicherte hat jederzeit das Recht, seine ePA endgültig zu schließen.

A_21128 -Hinweis im FdV zur selbstständigen Sicherung der Protokolle bei Schließen der Akte
Falls das ePA-FdV dem Nutzer eine Funktion zum Schließen seiner Akte anbietet, MUSS das ePA-FdV beim Schließen einer Akte über das ePA-FdV den Versicherten darauf hinweisen, seine Protokolldaten aus der Akte für eine weitere Verwendung selbstständig zu exportieren, da diese nach Schließen der Akte im Aktensystem nur noch eingeschränkt und nicht mehr vollständig für datenschutzrechtliche Auskünfte zur Verfügung stehen. Der Versicherte MUSS auf die Möglichkeit des signierten Exports der Protokolle hingewiesen werden.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_21129-03 -Revisionssicherer Export der Protokolle
Das ePA-FdV MUSS dem Nutzer eine Funktion zum Export signierter Protokolldaten aus der Akte unter Nutzung der "Render API: PDF Audit" des FHIR Implementation Guide für den Audit Event Service [gemIG_ePA_Basic] bereitstellen.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA,<=**]**

6.2.5.1 Widersprüche für Funktionen der ePA verwalten

Das Consent Management des ePA-Aktensystems verwaltet den Zustand der erteilten oder nicht erteilten Widersprüche des Versicherten oder eines Vertreters gegen oder für die Nutzung widerspruchsfähiger Funktionen der ePA.

Die Liste der widerspruchsfähigen Funktionen ist in A_23874* [gemSpec_Aktensystem_ePAfueralle] definiert.

Über das Frontend des Versicherten kann der aktuelle Zustand der Widersprüche eingesehen oder geändert werden. Der initiale Zustand nach Aktivierung eines Aktenkontos ist "kein Widerspruch erteilt" für alle Funktionen.

Eine Änderung eines Zustands führt dazu, dass die betroffene Funktion entweder nicht mehr durch Akteure der ePA ausgeführt wird ("Widerspruch erteilt") oder aber ausgeführt wird ("kein Widerspruch erteilt"). Ein Zustand kann dabei jederzeit durch einen Versicherten oder einen Vertreter geändert werden.

Ein erteilter Widerspruch kann, abhängig von der betroffenen Funktion, dazu führen, dass beispielsweise bereits hinterlegte Dokumente gelöscht bzw. keine Dokumente mit Bezug zu dieser Funktion neu in das Aktenkonto eingestellt werden.

Für eine fundierte Entscheidung des Versicherten oder eines Vertreters für oder gegen die Nutzung einer widerspruchsfähigen Funktion der ePA ist die Bereitstellung geeigneter Informationen erforderlich. Diese Information muss durch den Versicherten oder einen Vertreter auch nach der Änderung eines Widerspruchs einsehbar sein.

A_24056-01 -ePA-FdV: Information des Nutzers über Möglichkeit des Widerspruchs in Funktionen der ePA
Das ePA-Frontend des Versicherten MUSS einen Versicherten bei der ersten Nutzung eines ePA FdV über die widerspruchsfähigen Funktionen der ePA und seine Möglichkeit einer Änderung dieser umfassend informieren.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis zu A_24056-:*
Um zu vermeiden, dass dem Versicherten die Informationen bei Gerätewechseln und

Neuinstallationen eines ePA-FdV immer wieder erneut angezeigt werden, kann im Backend-System der Krankenkasse nachgehalten werden, dass der Versicherte die Informationen bereits einmal erhalten hat und die Information nicht nochmals am ePA-FdV angezeigt werden muss.

A_23870 -ePA-FdV: Information des Nutzers über die Auswirkungen bei Änderungen von Widersprüchen
Das ePA-Frontend des Versicherten MUSS einen Nutzer über die Auswirkungen eines Widerspruchs gegen die Nutzung einzelner widerspruchsfähiger Funktionen der ePA und die Auswirkungen bei Rücknahme des Widerspruchs umfassend informieren, so dass auch ein nicht technisch vorgebildeter Nutzer eine fundierte Entscheidung über die Teilnahme oder Nicht-Teilnahme an einer Funktion treffen kann.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Die geforderten Informationen des Nutzers betrifft auch die Widersprüche zu Sekundärnutzungszwecken, siehe 6.2.5.2- Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke .

Einige Funktionen haben weitergehende Auswirkungen, die vor einem Widerspruch gegen die Nutzung der Funktionen berücksichtigt werden müssen (siehe dazu die Kapitel "Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die Dokumente des Aktenkontos" [gemSpec_Aktensystem_ePAfueralle]).

Der Nutzer hat die Möglichkeit, die Daten vor Erteilung eines Widerspruchs aus seiner Akte lokal zu speichern (siehe 6.2.8.1.3- Dokument herunterladen).

Die Anzeige der widerspruchsfähigen Funktionen und deren aktueller Zustand (Widerspruch erklärt/nicht erklärt) erfolgt durch das ePA FdV. Ein Nutzer des ePA FdV kann die aktuelle Einstellung bei Bedarf ändern, also Widersprüche erklären oder zurücknehmen.
Dabei ist die umfassende Information eines Nutzers vor einer Änderungsausführung gemäß A_23870-* zu beachten.

Bei der Verwaltung der Widersprüche zu Sekundärnutzungszwecken ist zu beachten, dass dieses Feature nur für gesetzlich Versicherte (GKV) besteht. Die Oberfläche des ePA-FdV sollte daher entsprechende Funktionen der Verwaltung an Aktenkonten außerhalb der GKV nicht anbieten, da das Aktensystem entsprechende Operationen mit einem Fehler abbrechen würde. Die Zuordnung des Kostenträgers kann der Konfigurationsliste der Endpunkte der verschiedenen Kostenträger gemäß A_24801* am ePA-Aktensystem entnommen werden, die bei der Einrichtung einer Vertretung genutzt wird.

A_26311 -ePA-Frontend des Versicherten: Anzeige Widersprüche zu Sekundärnutzungszwecken bei Rücknahme Widerspruch gegen die Sekundärdatennutzung durch das FDZ
Falls ein Widerspruch gegen die Sekundärdatennutzung durch das FDZ zurückgenommen wird MUSS das ePA-Frontend des Versicherten dem Versicherten die im Aktensystem hinterlegten Widersprüche zu Sekundärnutzungszwecken anzeigen.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_23875 -ePA-Frontend des Versicherten: Anzeige der Widersprüche
Das ePA-Frontend des Versicherten MUSS dem Nutzer alle im Aktensystem hinterlegten Widersprüche unter Verwendung der Operation `getConsentDecisions` gemäß [I_Consent_Decision_Management] anzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_23880-01 -ePA-Frontend des Versicherten: Anwendungsfall "Widerspruch für Funktionen der ePA ändern"
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Widerspruche für Funktionen der ePA gemäß A_23874 unter Verwendung der Operation

updateConsentDecision gemäß [I_Consent_Decision_Management] zu erteilen bzw. zurückzunehmen .**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25234-01 -ePA-Frontend des Versicherten: Anzeige der Widersprüche - Information für Nutzer
Das ePA-Frontend des Versicherten MUSS den Nutzer darüber informieren, dass ein erteilter Widerspruch "Teilnahme am digital gestützten Medikationsprozess" dazu führt, dass ausschließlich der E-Rezept-Fachdienst und der Versicherte/Vertreter auf eML-Daten zugreifen darf.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.5.2 Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke

Wenn kein Widerspruch gegen die Sekundärdatennutzung durch das FDZ für das Aktenkonto erteilt wurde kann der Versicherte (bzw. ein Vertreter) die Verwendung seiner Daten auf die in § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszwecke einschränken.

Über das Frontend des Versicherten kann die Liste der Sekundärnutzungszwecke und deren Zustand hinsichtlich Widerspruch eingesehen oder geändert werden. Der initiale Zustand nach Aktivierung eines Aktenkontos ist für jeden Sekundärnutzungszweck "kein Widerspruch erteilt".

Eine Änderung der Liste der Sekundärnutzungszwecke durch den Versicherten oder einen Vertreter führt dazu, dass diese Information an das Forschungsdatenzentrum Gesundheit übermittelt wird. Die Widersprüche des Versicherten in die Sekundärnutzungszwecke ist dort bindend für die Verarbeitung der übermitteltenpseudonymisierten medizinischen Daten.

A_26283 -ePA-Frontend des Versicherten: Anzeige der Sekundärnutzungszwecke
Falls kein Widerspruch gegen die Sekundärdatennutzung erteilt wurde MUSS das ePA-Frontend des Versicherten dem Nutzer die Widersprüche zu den einzelnen Sekundärnutzungszwecken unter Verwendung der Operation getDataUsagePurposes gemäß [I_Consent_Decision_Management] anzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_26439 -ePA-Frontend des Versicherten: Art der Anzeige der Sekundärnutzungszwecke
Das ePA-Frontend des Versicherten MUSS dem Nutzer die Widersprüche zu den einzelnen Sekundärnutzungszweckenimmer im exakten Wortlaut des Gesetzes sowie in einer für Laien verständlichen Beschreibung anzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Weiterführende Informationen zu Sekundärnutzungszwecken und laienverständliche Darstellungen können unter [Nutzungszwecke des FDZ] gefunden werden.

A_26284 -ePA-Frontend des Versicherten: Anwendungsfall "Widersprüche in Sekundärnutzungszwecke ändern"
Falls kein Widerspruch gegen die Sekundärdatennutzung erteilt wurde MUSS das ePA-Frontend des Versicherten dem Nutzer ermöglichen, die Widersprüche zu den einzelnen Sekundärnutzungszwecken unter Verwendung der Operation updateDataUsagePurposes gemäß [I_Consent_Decision_Management] zu erteilen bzw. zurückzunehmen. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.5.3 Widerspruch gegen die Nutzung der ePA durch eine spezifische LEI

Der Widerspruch gegen die Nutzung der ePA durch eine spezifische LEI erfolgt über die Ombudsstelle des zuständigen Kostenträgers oder das ePA-Frontend des Versicherten.

Dabei wird im Entitlement Management vermerkt, dass für die spezifische LEI keine Befugnisse registriert werden können. Falls bereits eine Befugnis für diese spezifische LEI existiert, so wird diese Befugnis gelöscht.

A_25136 -ePA-Frontend des Versicherten: LEI - Widerspruchs gegen die Nutzung der ePA durch eine spezifische LEI - Suche in Verzeichnisdienst
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine LEI im VZD-FHIR-Directory zu suchen und für die Erteilung eines Widerspruchs gegen die Nutzung der ePA durch eine spezifische LEI auszuwählen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_24410 -ePA-Frontend des Versicherten: Erteilung eines Widerspruchs gegen die Nutzung der ePA durch eine spezifische LEI
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, einen Widerspruch gegen die Nutzung der ePA durch eine spezifische LEI zu erteilen unter Verwendung der Operation setBlockedUserPolicyAssignment gemäß [I_Entitlement_Management]. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_24460 -ePA-Frontend des Versicherten: Löschen eines Widerspruchs gegen die Nutzung der ePA durch eine spezifische LEI
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, einen Widerspruch gegen die Nutzung der ePA durch eine spezifische LEI zurückzunehmen unter Verwendung der Operation deleteBlockedUserPolicyAssignment gemäß [I_Entitlement_Management].**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_24411 -ePA-Frontend des Versicherten: Anzeigen von Widersprüchen gegen die Nutzung der ePA durch spezifische LEIs
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Liste der erteilten Widersprüche gegen die Nutzung der ePA durch spezifische LEIs unter Verwendung der Operation getBlockedUserPolicyAssignmentgemäß [I_Entitlement_Management] anzuzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.5.4 Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI

Ein Versicherter bzw. Vertreter hat die Möglichkeit der Nutzung des Medication Service durch eine oder mehrere spezifische LEI zu widersprechen. Dieser Widerspruch führt dazu, dass die LEI, für die ein Widerspruch gegen die Nutzung des Medication Service erfolgt ist, die Operationen des Medication Service nicht nutzen kann und auch keinen Zugriff auf die Dokumente der Kategorie "`emp`" der Dokumentenverwaltung erhält.

Die Verwaltung dieser Widersprüche durch das ePA FdV erfolgt im Consent Management. Ein Nutzer kann einen Widerspruch wieder zurücknehmen.

A_26425 -ePA-Frontend des Versicherten: Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI - Suche in Verzeichnisdienst
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine LEI im VZD-FHIR-Directory zu suchen und für die Erteilung eines Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI auszuwählen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_26426 -ePA-Frontend des Versicherten: Erteilung eines Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, einen Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI zu erteilen unter Verwendung der Operation`setUserSpecificMedicationDeny` gemäß [I_Consent_Decision_Management].**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_26427 -ePA-Frontend des Versicherten: Löschen eines Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, einen Widerspruch gegen des Medication Service durch eine spezifische LEI zurückzunehmen unter Verwendung der Operation `deleteUserSpecificMedicationDeny` gemäß [I_Consent_Decision_Management].**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_26428 -ePA-Frontend des Versicherten: Anzeigen von Widersprüchen gegen die Nutzung des Medication Service durch spezifische LEIs
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Liste der erteilten Widersprüche gegen die Nutzung des Medication Service durch spezifische LEIs unter Verwendung der Operation `getUserSpecificMedicationDenyList` gemäß [I_Consent_Decision_Management] anzuzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.6 Befugnisverwaltung

Dieses Kapitel beschreibt Anwendungsfälle zur Vergabe und Administration von Befugnissen (Entitlements) zum Zugriff auf das Aktenkonto. Im ePA-Aktensystem wird die Verwaltung der Befugnisse im Entitlement Management realisiert.
Mit einer Befugnis befähigt der Versicherte einen Nutzer oder eine DiGAzur Verarbeitung seiner Daten. Es können nur Befugnisse für die in A_23941* aufgeführten Nutzer bzw. Nutzergruppen erteilt werden.

Ein Versicherter ist immer zum Zugriff auf sein Aktenkonto befugt.
Ein Vertreter ist nur befugt, wenn dies explizit durch den Versicherten für sein Aktenkonto vergeben wurde.
Eine LEI ist nur befugt, wenn:

- dies explizit durch den Versicherten oder Vertreter für das Aktenkonto des Versicherten vergeben wurde, oder
- eine Behandlungssituation in der LEI vorlag und somit automatisch eine Befugnis für die Telematik-ID dieser LEI des zugehörigen Aktenkontos erstellt wurde.

Eine DiGA ist nur befugt, wenn:

- dies explizit durch den Versicherten oder Vertreter für sein Aktenkonto vergeben wurde

Die Prüfung des Zugriffs durch den Nutzer auf die Daten bzw. Dokumente des Aktenkontos erfolgt durch das ePA-Aktensystem.

Im ePA-Frontend des Versicherten können nur Befugnisse an LEI oder DiGA vergeben werden, die im VZD-FHIR-Directory der TI registriert sind.

Eine Besonderheit bildet der Zugriff aufGesundheitsdaten im grenzüberschreitenden Austausch zwischen den Mitgliedsstaaten der Europäischen Union (EU-Zugriff), siehe Kapitel6.2.6.6- Befugnisverwaltung EU-Zugriff .

A_23968 -ePA-Frontend des Versicherten: Befugnisverwaltung am Aktensystem - Nutzung Schnittstelle
Das ePA-Frontend des Versicherten MUSS beim Erstellen, Anzeigen, Ändern und Löschen von Befugnissen am ePA-Aktensystem die Operationen getEntitlement, getEntitlements, setEntitlement, deleteEntitlements der Schnittstelle`I_Entitlement_Management` gemäß [I_Entitlement_Management] verwenden.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_24399-01 -ePA-Frontend des Versicherten: Befugnis signieren

Das ePA-Frontend des Versicherten MUSS beim Erstellen und Ändern einer Befugnis diese Befugnis mit der Datenstruktur`EntitlementRequestType` für Vertreter und`EntitlementRequestType` für alle anderen Befugnisse gemäß [I_Entitlement_Management] erstellen und diese durchAufruf der Schnittstelle`I_Remote_Sign_Operations::sign_Data` unter Verwendung von`privacy_mode=true` am Signaturdienst mit der Identität des Nutzers gemäß [gemSpec_SigD] signieren.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Vor dem Signieren der Befugnis wird das Zertifikat des Nutzers vom SigD unter Verwendung der Operation `I_Remote_Get_Certificate::get_Certificate` für die Erstellung des JWT abgerufen. Es wird der Hashwert des jwt vom ePA-Frontend des Versicherten gebildet und signiert.

A_26280 -ePA-Frontend des Versicherten: Keine Übermittlung von Informationen des Befugten an den Signaturdienst
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass beim Aufruf der Schnittstellen des Signaturdienstes zum Zwecke des Signierens einer Befugnis keine Informationen über den zu befugenden Nutzer an den Signaturdienst übermittelt werden. **[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis zu A_26280: Um dies zu ermöglichen, bietet der Signaturdienst die Möglichkeit des privacy mode, so dass nur der zu signierende Hashwert der Befugnis an den Signaturdienst übermittelt werden muss.

A_27734 -ePA-Frontend des Versicherten: Verzeichnisdienst-Resultate enthalten keine KVNR
Das ePA-Frontend des Versicherten DARF eine über den VZD-FHIR-Directory bezogene Nutzer-ID NICHT für die Vergabe von Befugnissen nutzen, falls diese die Struktur einer KVNR besitzt.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

6.2.6.1 Befugnisverwaltung für LEI

In diesem Kapitel werden die folgenden Anwendungsfälle umgesetzt:

- "Befugnis für eine LEI erstellen"
- "Befugnis für eine LEI ändern"
- "Befugnis für eine LEI löschen"

A_23960 -ePA-Frontend des Versicherten: LEI - Befugnis verwalten
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine Befugnis für eine LEI zu erstellen, zu ändern bzw. zu löschen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_23965 -ePA-Frontend des Versicherten: LEI - Suche in Verzeichnisdienst
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine oder mehrere LEI im VZD-FHIR-Directory zu suchen und für die Vergabe der Befugnisse auszuwählen. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Für die Umsetzung der Suche siehe Aktivität 6.2.3.2- Leistungserbringerinstitution im Verzeichnisdienst der TI finden.

A_24549 -ePA-Frontend des Versicherten: LEI - Berücksichtigung der Legal Policy bei Erstellen einer Befugnis
Das ePA-Frontend des Versicherten MUSS beim Erstellen einer Befugnis die Legal Policy beachten. Daraus folgt, dass dem Nutzer nur Leistungserbringerinstitutionen zur Auswahl angezeigt werden, die den erlaubten Berufsgruppen gemäß der Legal Policy entsprechen. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_20109-05 -ePA-Frontend des Versicherten: LEI - Konfiguration der Befugnisdauer
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die zeitliche Begrenzung für eine Leistungserbringerinstitution für die erteilte Befugnis zu konfigurieren. Folgende Optionen MUSS das ePA-Frontend anbieten:

- flexibles Enddatum
- unbefristet
- 90 Tage [default] (heutiges Datum + 89 Kalendertage)
  bzw. 3 Tage [default] (heutiges Datum + 2 Kalendertage) bei Nutzergruppen gemäß § 342 Abs. 2 Nr. 1 lit. l SGB V.(siehe A_23941-*)

[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25482 -ePA-Frontend des Versicherten: LEI - Endzeitpunkt der Befugnisdauer
Das ePA-Frontend des Versicherten MUSS zu dem vom Nutzer gewählten Endedatum den Endezeitpunkt auf das Ende des Tages der aktuellen Zeitzone in Deutschland, d.h. MEZ (UTC+1) bzw. MESZ (UTC+2) setzen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Hinweis: Befugniserstellungszeitpunkt ist 2024-04-12T10:05:30+01:00. Der daraus resultierende Befugniszeitpunkt ist 2024-04-12T23:59:59+01:00

6.2.6.2 Befugnisverwaltung für DiGA

Eine Befugnis für eine DiGA gilt unbegrenzt, d.h. die Befugnis gilt solange bis der Nutzer diese Befugnis löscht.

In diesem Kapitel werden die folgenden Anwendungsfälle umgesetzt:

- "Befugnis für eine DiGA erstellen"
- "Befugnis für eine DiGA löschen"

A_25129 -ePA-Frontend des Versicherten: DiGA - Befugnis verwalten
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine Befugnis für eine DiGA zu erstellen bzw. zu löschen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25130 -ePA-Frontend des Versicherten: DiGA - Suche in Verzeichnisdienst
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine DiGA im VZD-FHIR-Directory zu suchen und für die Vergabe der Befugnis auszuwählen.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Für die Umsetzung der Suche siehe Aktivität 6.2.3.3- DiGA im Verzeichnisdienst der TI finden.

6.2.6.3 Vertretung verwalten

Ein Versicherter (Aktenkontoinhaber) kann eine Befugnis für einen Vertreter einrichten oder auch entziehen. Ein Vertreter muss über eine GesundheitsID verfügen. Es können maximal 5 Vertreter gleichzeitig befugt sein.

Der Anwendungsfall "Vertretung einrichten" steht einem befugten Vertreter nicht zur Verfügung. Vor der Berechtigung müssen der Name, die Versicherten-ID sowie die E-Mail-Adresse des Vertreters für die Geräteautorisierung erfasst werden.

A_15389 -ePA-Frontend des Versicherten: Daten des Vertreters
Das ePA-Frontend des Versicherten MUSS es dem Nutzer im Anwendungsfall "Vertretung einrichten" ermöglichen, den Namen, die Versicherten-ID und eine

Benachrichtigungsadresse (E-Mail) für die Geräteautorisierung des Vertreters zu erfassen. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Die Befugnisdauer für Vertreter kann nicht zeitlich oder inhaltlich begrenzt werden. Wenn ein Vertreter befugt ist, auf die Dokumente zuzugreifen, dann kann der Vertreter dauerhaft auf alle Dokumente im Aktenkonto zugreifen, bis ihm die Befugnis generell wieder entzogen wird.

A_23971 -ePA-Frontend des Versicherten: Vertreter verwalten
Das ePA-Frontend des Versicherten MUSS es dem Versicherten ermöglichen, eine Befugnis für einen Vertreter zu erstellen oder zu löschen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25245 -ePA-Frontend des Versicherten: eigene Befugnis als Vertreter löschen
Das ePA-Frontend des Versicherten MUSS es dem Vertreter ermöglichen, die eigene Befugnis als Vertreter zu löschen.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_15400-02 -ePA-Frontend des Versicherten: PDF mit Information für Vertretung
Das ePA-Frontend des Versicherten MUSS dem Versicherten die Möglichkeit geben, ein druckbares Format (z. B. PDF) mit den Informationen für die Vertretung zu erzeugen. Das Dokument MUSS alle Informationen enthalten die zum Einrichten der Vertretung auf dem Gerät des Vertreters erforderlich sind.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Anwendungsfall "Vertretung am fremden FdV verwalten" als Sonderfall

Für den Fall, dass der zu Vertretende kein eigenes ePA FdV nutzt, aber eine Vertretung einrichten oder löschen möchte, ist die Umsetzung des Anwendungsfalls "Vertretung am fremden FdV verwalten" wie folgt möglich.

A_23555-02 -ePA-Frontend des Versicherten: Vertretung am fremden FdV verwalten - Ablauf
Das ePA-Frontend des Versicherten KANN den Anwendungsfall "Vertretung am fremden FdV verwalten" umsetzen

Tabelle 9: Vertretung am fremden FdV verwalten

Name	Vertretung am fremden FdV verwalten
Auslöser	Aufruf des Anwendungsfalls in der GUI
Akteur	Nutzer (in der Rolle zukünftiger Vertreter; wird im weiteren Verlauf Vertreter genannt)
Vorbedingung	Der Nutzer hat sein ePA-FdV gestartet. Der zu Vertretende ist anwesend, um sich mit seiner eGK anzumelden.
Nachbedingung	Die Befugnis für den Vertreter ist im Aktenkonto des zu Vertretenden hinterlegt bzw. wurde gelöscht.
Standardablauf	Aktivitäten im Standardablauf 1. Der Vertreter startet an seinem FdV den Anwendungsfall (ohne dass der zu Vertretende zu diesem Zeitpunkt am Aktensystem eingeloggt ist).

	2. Das FdV initiiert die Anmeldung des zu Vertretenden am Aktensystem. Hierzu muss der zu Vertretende seine eGK nutzen. 3. Das FdV fordert dazu auf, einen Vertreter einzurichten bzw. zu löschen. Bei der Vertretereinrichtung wird die KVNR des Vertreters, dessen Name und dessen E-Mail-Adresse benötigt. 4. Für Vertreterbefugnis erstellen: Befugnis für den Vertreter am FdV erstellen, unter Verwendung des SigD mit der Identität des zu Vertretenden signieren und im Aktenkonto hinzufügen. 5. Für Vertreterbefugnis löschen: Befugnis für den Vertreter im Aktenkonto löschen.

[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Hinweis:
Im Anwendungsfall "Vertretung am fremden FdV verwalten" ist die Authentisierung des zu Vertretenden ausschließlich mittels eGK und PIN möglich.

A_24405-01 -ePA-Frontend des Versicherten: Vertretung am fremden FdV verwalten - Authentisierung
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung am fremden FdV verwalten" die Authentisierung des zu Vertretenden am IdPmittels eGK und PIN ohne Prüfung Gerätebindung verlangen gemäß [I_Authorization_Service].
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Die Anmeldung des zu Vertretenden in diesem Szenario erfolgt ohne Geräteregistrierung.

6.2.6.4 Vergebene Befugnisse anzeigen

Mit diesem Anwendungsfall kann ein Nutzer eine Liste der für das Aktenkonto vergebenen Befugnisse anzeigen lassen. Diese Liste beinhaltet die befugten Leistungserbringerinstitutionen, DiGAs und Vertreter sowie die Details zu Berechtigungen (für LEI: Berechtigungsdauer).

A_23963 -ePA-Frontend des Versicherten: Befugnisse anzeigen
Das ePA-Frontend des Versicherten MUSS dem Nutzer alle im Aktensystem hinterlegten Befugnisse einschließlich Gültigkeitszeitraum anzeigen und dem Nutzer nach Nutzergruppen (LEI, DiGA, Vertreter) geordnet anzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_23972-01 -ePA-Frontend des Versicherten: Ergebnisliste Befugnisse Felder
Das ePA-Frontend des Versicherten MUSS im Ergebnis der Suche nach Befugnissen mindestens

- für LEI: Name der Leistungserbringerinstitution, Ende der Befugnis(nicht im Kontext des Anwendungsfalls "Anbieter wechseln")
- für DiGA: Name der DiGA
- für Vertreter: Name des Vertreters

anzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Das Ergebnis der Suche soll für den Nutzer sortierbar und filterbar dargestellt werden.

Das ePA-FdV ermöglicht es dem Nutzer, über Einträge in der Ergebnisliste Befugnisse zu bearbeiten oder zu löschen.

6.2.6.5 Eingerichtete Vertretungen anzeigen

Mit diesem Anwendungsfall kann ein Nutzer eine Liste der Versicherten anzeigen lassen, für die im ePA-Frontend des Versicherten die Wahrnehmung der Vertretung durch ihn konfiguriert ist ("*ich bin Vertreter für*"). Es wird dabei nicht geprüft, ob im Aktenkonto des zu Vertretenden auch tatsächlich eine Befugnis für den Nutzer vorliegt.

A_15406 -ePA-Frontend des Versicherten: Liste "ich bin Vertreter für" anzeigen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine Liste mit den im ePA-Frontend des Versicherten für ihn konfigurierten Vertretungen anderer Versicherter anzuzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.2.6.6 Befugnisverwaltung EU-Zugriff

Auf Gesundheitsdaten kann auch im grenzüberschreitenden Austausch zwischen den Mitgliedsstaaten der Europäischen Union zugegriffen werden. Voraussetzung hierfür ist eine durch den Versicherten erstellte Befugnis für das entsprechende Land. Der Versicherte wählt hierzu im FHIR-VZD das Land aus. Für die ermittelte Telematik-ID dieses Landes wird eine Befugnis erstellt und mit der Identität des Versicherten signiert. Die Befugnis EU-Zugriff ist 1 Stunde gültig und kann verlängert werden. Die Verlängerung einer Befugnis EU-Zugriff wird technisch als Erstellen einer neuen Befugnis umgesetzt, welche eine noch existierende Befugnis ersetzt. Es gibt zu einem Zeitpunkt maximal eine Befugnis EU-Zugriff.

Das ePA-FdV erzeugt zusätzlich zur Befugnis einen 6-stelligen Zugriffscode. Der Zugriffscode wird zur Befugnis im Entitlement Management hinterlegt und dient als Geheimnis, welches der Versicherte dem LE im EU-Ausland übergibt und erteilt diesem dadurch die Erlaubnis zum Zugriff auf die Daten.

In diesem Kapitel werden die folgenden Anwendungsfälle umgesetzt:

- "Befugnis für einenEU-Zugriff erstellen"
- "Befugnis für einenEU-Zugriff verlängern"
- "Befugnis für einenEU-Zugriff löschen"
- "Befugnis für einenEU-Zugriff anzeigen"

A_26108 -ePA-Frontend des Versicherten (EU): EU Zugriff - Erstellung Befugnis am Aktensystem - Nutzung Schnittstelle
Das ePA-Frontend des Versicherten MUSS beim Erstellen einer Befugnissen für EU-Zugriff am ePA-Aktensystem die Operation setEntitlementEU der Schnittstelle`I_Entitlement_Management_EU` gemäß [I_Entitlement_Management_EU] verwenden.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_26122 -ePA-Frontend des Versicherten (EU): EU Zugriff - Abruf Zugriffscode für EU Zugriff am Aktensystem - Nutzung Schnittstelle
Das ePA-Frontend des Versicherten MUSS beim Abruf des für die Befugnis hinterlegten Zugriffscode am ePA-Aktensystem die Operation getAccessCode der Schnittstelle`I_Entitlement_Management_EU` gemäß [I_Entitlement_Management_EU] verwenden.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Löschen und Lesen einer Befugnis für EU-Zugriff unterscheidet sich nicht von den anderen Befugnissen, d.h. diese werden mit den Operationen von [I_Entitlement_Management] umgesetzt.

Die Operation getEntitlements liefert alle im Aktensystem hinterlegten Entitlements einschließlich eines evt. hinterlegten Entitlements für EU-Zugriff.

A_25825 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Befugnis verwalten

Das ePA-Frontend des Versicherten MUSS es dem Versicherten ermöglichen, eine Befugnis EU-Zugriff zu erstellen, zu verlängern, zu löschen bzw. anzuzeigen. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25826 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Suche in Verzeichnisdienst
Das ePA-Frontend des Versicherten MUSS es dem Versicherten ermöglichen, ein Land für eine Befugnis EU-Zugriff im VZD-FHIR-Directory zu suchen. Länder für EU-Zugriff besitzen die Rolle = `oid_ncpeh`. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Für die Umsetzung der Suche siehe 6.2.3.4- Land (EU-Zugriff) im Verzeichnisdienst der TI finden .

A_25839 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Zugriffscode erstellen
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Befugnis für einen EU-Zugriff erstellen" einen Zugriffscode (AccessCode) als Zufallswert erstellen (vgl. A_26301) und diesen Zugriffcode gemeinsam mit der Befugnis EU-Zugriff im Entitlement Management hinterlegen. Für jede Befugnis EU-Zugriff MUSS ein neuer AccessCode erzeugt werden.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA,<=**]**

Die zufällige Erzeugung des Zugriffscodes wird in [gemSpec_Krypt#Zugriffscode-Erzeugung] detaillierter betrachtet.

A_25841 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Anzeige Zugriffscode
Das ePA-Frontend des Versicherten MUSS, den bei einer Befugnis EU-Zugriff erzeugten Zugriffscode dem Versicherten anzeigen und auf Wunsch wiederholt anzeigen. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_27453 -Unterscheidbarkeit der Zeichen bei Zugriffscode
Das ePA-Frontend des Versicherten MUSS bei der Anzeige des Zugriffscodes die Lesbarkeit der Zeichen des Zugriffscodes sicherstellen. **[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Hinweis zu A_27453:
Mit Lesbarkeit ist das Erkennen und Unterscheiden einzelner Buchstaben und Ziffern gemeint, d.h. die Unterscheidbarkeit von beispielsweise 0 (Null) und O (Großbuchstabe O), sowie I (Großbuchstabe i) und l (Kleinbuchstabe L) und 1 (Ziffer Eins).

A_25842 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Information für Versicherten allgemein
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Befugnis für EU-Zugriff erstellen" vor Erteilung der Befugnis den Versicherten über seine Rechte in Bezug auf den Schutz seiner persönlichen und Gesundheitsdaten und der Verarbeitung seiner Daten innerhalb der grenzüberschreitenden Dienste (Aufklärungstext zur Einwilligung in den Datenaustausch) informieren.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis:
Eine Befugnis EU-Zugriff ist eine Stunde gültig. Das Gültigkeitsendedatum validTo wird bei Erstellung der Befugnis durch das Aktensystem gesetzt, d.h. der Wert im JWT der Befugnis wird vom Aktensystem nicht ausgewertet.

Eine nicht abgelaufene Befugnis EU-Zugriff kann um eine Stunde auch wiederholt verlängert werden. Hierzu erzeugt das ePA-FdV einen neuen Zugriffscode und erstellt eine neue Befugnis EU-Zugriff mit diesem Zugriffscode.

A_25843 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Befugnis verlängern
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Befugnis für EU-Zugriff verlängern" für die aktuell gültige Befugnis EU-Zugriff erneut eine Befugnis EU-Zugriff für

dieses Land erzeugen, d.h. einen Zugriffscode (AccessCode) als Zufallswert erstellen und diesen Zugriffcode gemeinsam mit der Befugnis EU-Zugriff im Entitlement Management hinterlegen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25866 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Befugnis anzeigen
Das ePA-Frontend des Versicherten MUSS dem Versicherten die im Aktensystem hinterlegte Befugnis EU-Zugriff anzeigen und dabei die folgenden Inhalte anzeigen:

- Name des Landes
- Gültigkeitsende
- Zugriffscode
- KVNR des Versicherte

[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Damit kann der Versicherte dem LE-EU die Informationen auf seinem Endgerät zeigen und so die Nutzung der Zugriffsdaten verständlich machen.

A_25868 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Anzeige vor Ablauf
Fallsdie Restdauer der Befugnis EU-Zugriff < 10 Minuten MUSS das ePA-Frontend des Versicherten denZeitwert für den Versicherten deutlich hervorgehoben anzeigen. (z.B. farblich)**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Die Anzeige vor Ablauf der Befugnis EU-Zugriff kann z.B. farblich hervorgehoben werden.

A_25871 -ePA-Frontend des Versicherten (EU): EU-Zugriff - Anzeige bei Ablauf
Fallsdie Befugnis EU-Zugriff zeitlich abgelaufen ist MUSS das ePA-Frontend des Versicherten eine Informationfür den Versicherten über den Ablauf der Befugnis EU-Zugriff anzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Hinweis: Es reicht aus, dass die Information über den Ablauf der Befugnis EU-Zugriff nur angezeigt wird, während der Nutzer auf dem Gerät aktiv ist.

Der zeitliche Ablauf der Befugnis EU-Zugriff wird nicht durch das ePA-Aktensystem signalisiert.

6.2.7 Verbergen und Sichtbarmachen von Dokumenten

Dokumente sind für eine befugte LEI prinzipiell sichtbar. Allerdings besteht die Möglichkeit die Sichtbarkeit bei Zugriffen von Leistungserbringerinstitutionen einzuschränken. Es gibt folgende Möglichkeiten zum Verbergen von Dokumenten:

1. **Kategorienbasiertes Verbergen von Dokumenten ggü. allen Leistungserbringerinstitutionen:**
   Der Nutzer wählt im ePA-Frontend des Versicherten die zu verbergenden Datenkategorien aus. Das ePA-Frontend des Versicherten übermittelt diese Datenkategorien über eine spezifische Schnittstelle an den Constraint Management Service, welcher sie in die General Deny Policy aufnimmt.
   Alle Dokumente dieser Datenkategorie sind für alle Leistungserbringerinstitutionen zum Zugriff **nicht sichtbar**.
2. **Dokumentenspezifisches Verbergen von Dokumenten ggü. allen Leistungserbringerinstitution**
   Der Nutzer wählt im ePA-Frontend des Versicherten die zu verbergenden Dokumente aus. Das ePA-Frontend des Versicherten übermittelt diese Dokumenten-IDs über eine spezifische Schnittstelle an den Constraint Management Service, welcher sie in die General Deny Policy aufnimmt.
   Alle verborgenen Dokumente sind für alle Leistungserbringerinstitutionen zum Zugriff **nicht sichtbar**.

Die Datenkategorien sind in der Legal Policy (A_19303) aufgeführt.

Das **Sichtbar machen von bisher verborgenen Dokumenten oder einer bisher verborgenen Datenkategorie** erfolgt in gleicher Art und Weise. Der Nutzer wählt im ePA-Frontend des Versicherten die verborgenen Dokumente oder Datenkategorien aus, welche er sichtbar machen möchte. Das ePA-Frontend des Versicherten übermittelt diese Auswahl an den Constraint Management Service, welcher sie in der General Deny Policy aktualisiert.

Verbergen und Sichtbarmachen von MIOs

Eine Besonderheit stellt das Verbergen von MIOs dar. Ein MIO aus Nutzersicht entspricht einem Dokument in seiner Gesamtheit, auch wenn ein MIO technisch aus einzelnen Dokumenten bestehen kann.
Einzelne Dokumente eines MIOs dürfen nicht verborgen werden, damit die Aussage des MIOs in seiner Gesamtheit nicht verfälscht wird.
Das Verbergen eines konkreten MIOs erfolgt entweder über das Verbergen der Datenkategorie (MIOs die durch einen statischen Ordner repräsentiert werden, z. B. Impfpass, Zahnbonusheft, Kinderuntersuchungsheft) oder über das Verbergen eines dynamischen Ordners (Mutterpass).

Für das Sichtbarmachen eines MIOs gilt alles in gleicher Weise.

Verbergen und Sichtbarmachen von DiGAs

Es gibt verschiedene Möglichkeien zum Verbergen und Sichtbarmachen von DiGAs.
Alle DiGAs können verborgen bzw. sichtbar gemacht werden durch Verbergen bzw. Sichtbarmachen der Kategorie "diga".
Eine konkrete DiGA kann verborgen bzw. sichtbar gemacht werden durch Verbergen bzw. Sichtbarmachen des dynamischen Ordners dieser DiGA.
Ausgewählte Dokumente einer DiGA können verborgen bzw. sichtbar gemacht werden durch Verbergen bzw. Sichtbarmachender Dokumente.

Die Konfiguration der General Deny Policy erfolgt im Constraint Management des ePA-Aktensystems.

A_24357 -ePA-Frontend des Versicherten: Verbergen von Dokumenten - Schnittstelle
Das ePA-Frontend des Versicherten MUSS zum Verbergen und sichtbar Machen von Dokumenten und Datenkategorien das Interface I_Constraint_Management_Insurant gemäß [I_Constraint_Management_Insurant] am ePA-Aktensystem aufrufen.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_26380 -ePA-Frontend des Versicherten: Verbergen von Dokumenten durch ConfidentialityCode "CON"
Das ePA-Frontend des Versicherten KANN es dem Nutzer ermöglichen, Dokumente direkt als verborgene Dokumente einzustellen (Verwendung des confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491)).**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_25144 -ePA-Frontend des Versicherten: Verbergen von Dokumenten – Hinweis auf mögliche versorgungsrelevante Folgen
Das ePA-Frontend des Versicherten MUSS dem Nutzer im Anwendungsfall "Verbergen von Dokumenten" vor dem Verbergen der Dokumente in der elektronischen Patientenakte einen Hinweis darauf geben, dass das Verbergen von Dokumenten Auswirkungen auf die Versorgung und die Patientensicherheit haben kann.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.2.7.1 Kategorienbasiertes Verbergen von Dokumenten

Das Verbergen einer Datenkategorie führt dazu, dass alle Dokumente und, falls vorhanden, alle in dieser Datenkategorie enthaltenen dynamischen Ordner (z. B. Mutterpass, DiGA) einschließlich der darin enthaltenen Dokumente für befugte Leistungserbringerinstitutionen nicht sichtbar sind. Die möglichen Datenkategorien zum Verbergen ergeben sich aus den Kategorien Dokumentenverwaltung (siehe A_19303*) außer eMP.

A_19685-01 -ePA-Frontend des Versicherten: Anzeige der zugehörigen Datenkategorie
Das ePA-Frontend des Versicherten MUSS dem Nutzer die dem Dokument zugeordnete Datenkategorie, die in den Anforderungen A_14761-* und A_19388-* aufgeführt sind, anzeigen können.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_19690 -ePA-Frontend des Versicherten: Optische Kennzeichnung der Datenkategorien
Das ePA-Frontend des Versicherten KANN dem Nutzer die zugeordnete Datenkategorie eines Dokumentes durch typografische Auszeichnung wie etwa Schriftfarbe, Hintergrundfarbe, Schriftart oder auch die Anordnung in Gruppen optisch kennzeichnen. **[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_24454-01 -ePA-Frontend des Versicherten: Anzeige der für den LEI verborgenen Datenkategorien
Das ePA-Frontend des Versicherten MUSS dem Nutzer anzeigen können, welche Datenkategorien für alle Leistungserbringerinstitutionen verborgen sind. **[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Damit kann der Nutzer vor dem Besuch einer Leistungserbringerinstitution sehen, welche Datenkategorien der ePA bei der LEI verborgen sind.

Das ePA-Aktensystem setzt die gesetzlichen Vorgaben zur Zugriffsbeschränkung von Berufsgruppen durch, siehe Legal Policy. Das ePA-Frontend des Versicherten unterstützt den Nutzer dabei, sich ein Bild zu verschaffen, auf welche Datenkategorien eine einzelne befugte Leistungserbringerinstitution prinzipiell zugriffsberechtigt ist.

A_24455 -ePA-Frontend des Versicherten: Anzeige der für eine befugte LEI prinzipiell geltenden Zugriffsregeln
Das ePA-Frontend des Versicherten MUSS dem Nutzer anzeigen können, welche der vom ePA-Aktensystem durchgesetzten Zugriffsregeln (Legal Policy) hinsichtlich Lesen, Schreiben, Aktualisieren und Löschen für eine einzelne Datenkategorie für eine einzelne Leistungserbringerinstitution gelten.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.7.2 Dokumentenspezifisches Verbergen von Dokumenten

Das Verbergen von Dokumenten erfolgt für alle Leistungserbringerinstitutionen gemeinsam.

Eine Auswahl einzelner Dokumente, die verborgen werden sollen, kann der Nutzer über 6.2.8.1.2- Dokumente suchen ermitteln.

Bei der Konfiguration der Policy wird der folgende Identifier eines Dokuments verwendet:

- XDS Document Service: das Metadatum referenceIdList mit "urn:gematik:iti:xds:2023:rootDocumentUniqueId" eines Dokuments, welches eine Referenz auf ein Dokument unabhängig von der Version des Dokuments darstellt.
- MHD Service: masterIdentifier des Dokuments im Status "current"

Es wird sichergestellt, dass das Verbergen eines Dokuments für alle Versionen, also auch für zukünftige Versionen wirksam wird.

A_24363-02 -ePA-Frontend des Versicherten: Verbergen von Dokumenten für alle Leistungserbringerinstitutionen
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, ein oder mehrere ausgewählte Dokumente für alle Leistungserbringerinstitutionen im ePA-Aktensystem zu verbergen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_27735-01 -ePA-Frontend des Versicherten: Verbergen von Dokumenten – Anhänge
Falls im Anwendungsfall "Verbergen von Dokumenten" ein Dokument in einer Anhangsbeziehung (Elterndokument, Anhang) dokumentenspezifisch verborgen werden soll, MUSS das ePA-Frontend des Versicherten dem Nutzer alle Dokumente, die mit diesem Dokument in einer Anhangsbeziehung sind, anzeigen und dem Nutzer die Möglichkeit gegeben werden, auch Dokumente in dieser Anhangsbeziehung zum Verbergen auszuwählen.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Hinweis zu A_27735:*
Ein Elterndokument kann mehrere Kinddokumente besitzen. Ein Kinddokument kann wiederum selbst über einen oder mehrere Anhänge verfügen. Dadurch können komplexe Anhangsketten (bzw. ein Anhangsbaum) entstehen, die dazu führen, dass beim Verbergen von Dokumenten alle in diesen Anhangsketten (bzw. Anhangsbaum) enthaltenen Dokumente dem Nutzer anzuzeigen sind.

A_24364 -ePA-Frontend des Versicherten: Sichtbar machen von Dokumenten für alle Leistungserbringerinstitution
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, ein oder mehrere ausgewählte für alle Leistungserbringerinstitutionen im ePA-Aktensystem verborgenen Dokumente sichtbar zu machen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_24362 -ePA-Frontend des Versicherten: Anzeige von verborgenen Dokumenten für alle Leistungserbringerinstitutionen
Das ePA-Frontend des Versicherten MUSS dem Nutzer die im ePA-Aktensystem für alle Leistungserbringerinstitutionen verborgenen Dokumente auflisten können.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.8 Medical Services

6.2.8.1 Document Services

Es können Dokumente in der ePA für Alle eingestellt, gesucht, heruntergeladen und gelöscht werden. Hierzu dienen der XDS Document Service und der MHD Service.

Der **MHD Service** ist der Document Service, der langfristig in der ePA für Alle unterstützt werden soll. Er setzt auf den HL7 FHIR-Standard sowie und das IHE ITI MHD-Profil auf und basiert auf einer REST API. Der MHD Service unterstützt den vollständigen Lebenszyklus von Dokumenten (d.h. Lesen, Einstellen, Aktualisieren, Löschen von Dokumenten sowie Aktualisierung von Metadaten). MHD Service-spezifische Anforderungen befinden sind in [gemIG_ePA_MHD].

Der **XDS Document Service** verwendet SOAP Web Services und wird in späteren ePA Releases nicht mehr unterstützt. Im ePA Release "ePA 27" können Dokumente über den XDS Document Servicefür eine Übergangszeit noch gesucht, eingestellt, aktualisiert, heruntergeladen und gelöscht werden. Die Aktualisierung von Metadaten wird nicht mehr unterstützt.

Im XDS Document Service vorgenommene Änderungen werden im MHD Service sichtbar, sodass Clients bei Verwendung des MHD Service einen vollständigen Überblick über alle Dokumente erlangen können. Dokumente, die über den MHD Service eingestellt werden, werden hingegen*nicht* in den XDS Document Service gespiegelt; Löschung und Metadatenaktualisierung sind jedoch weiterhin auch über XDS sichtbar. Details finden sich in [gemIG_ePA_MHD].

Das ePA-FdV nutzt den XDS Document Service ausschließlich nur noch für die folgenden Anwendungsfälle:

1. Verwaltung von DiGA-Dokumenten, die durch den MHD Service noch nicht unterstützt werden
2. Verwaltung von Notfalldatensatz und Datensatz Persönlicher Erklärung
3. Sichern von Mutterpass, Kinderuntersuchungsheft und Impfpass, siehe 5.4.5.1-Weiterentwicklung bzw. Ablösung von Sammlungen

A_30286 -ePA-Frontend des Versicherten: Einschränkungen zur Verwendung des XDS Document Service
Das ePA-Frontend des Versicherten MUSS sicherstellen, dass die Schnittstellen des XDS Document Service ausschließlich zur Verwaltung von Dokumenten mit folgendem DocumentEntry.formatCode genutzt werden:

- urn:gematik:ig:diga:v1.1
- urn:gematik:ig:Notfalldatensatz:r3.1
- urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1

[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.2.8.1.1 Dokumente einstellen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein Vertreter Dokumente in die ePA hochladen.

6.2.8.1.1.1 Dokumente einstellen - Document Service übergreifend
A_15286 -ePA-Frontend des Versicherten: Auswahl von Dokumenten
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, ein oder mehrere Dokumente aus lokal eingebundenem Speicher auszuwählen, um sie in die ePA einzustellen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_15461-02 -ePA-Frontend des Versicherten: Dokumente einstellen - Prüfung Dateigröße
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" die Größe jedes durch den Nutzer ausgewählten Dokuments prüfen und ablehnen, wenn das Dokument die Größe von 25 MB überschreitet.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Das bedeutet, dass Dokumente bis zu einer Größe von 25 MB = 25 * (1024)^2 Byte in die ePA hochgeladen werden. Grundlage für die Berechnung der Dokumentengröße ist das Dokument ohne Transportcodierung. Größere Dokumente können nicht hochgeladen werden.

Das ePA-Aktensystem lehnt beim Einstellen von Dokumenten Requests ab, wenn die Summe der Größe der Dokumente in einem Submission Set 250 MB überschreitet. Das ePA-Frontend des Versicherten kann Einstellversuche von Dokumentensets unterbinden, wenn diese von der Dokumentenverwaltung aufgrund der Größenbeschränkung abgelehnt würden.

A_15462 -ePA-Frontend des Versicherten: Dokumente einstellen - Eingabe der Metadaten zu Dokumenten

Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, zu jedem einzustellenden Dokument Metadaten einzugeben.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Für Festlegungen zur Eingabe von Metadaten siehe5.4.6.1- Metadaten für einzustellende Dokumente .

Das ePA-Frontend des Versicherten kann eine Prüfung der Metadaten auf Vollständigkeit und Korrektheit durchführen und den Nutzer bei fehlenden oder falschen Werten zur Korrektur auffordern.

Das ePA-Aktensystem unterstützt nur Dokumente mit bestimmten MIME Types. Die initial zulässigen Typen sind in A_14760* beschrieben. Der XDS Document Service prüft jedes Dokument anhand der Metadaten beim Hochladen der Dokumente und antwortet mit einem Fehler, wenn der Dokumenttyp nicht unterstützt wird.

A_15463-02 -ePA-Frontend des Versicherten: Dokumente einstellen - Prüfung Metadaten
Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" die Metadaten auf Vollständigkeit prüfen und bei fehlenden oder fehlerhaften Werten den Anwendungsfall abbrechen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.8.1.1.2 Dokumente einstellen - XDS Document Service spezifisch
A_24707 -ePA-Frontend des Versicherten: Dokumente einstellen
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen Dokumente in die Akte einzustellen unter Verwendung der Operation `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b` des XDS Document Service gemäß [XDSDocumentService].**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_16221-01 -ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-41] - Unterstützung MTOM/XOP
Das ePA-Frontend des Versicherten MUSS bei der Umsetzung der IHE XDS-Transaktion [ITI-41] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] gemäß [IHE-ITI-TF2]#V.8 verwenden.**[**Frontend_Vers_ePA,funkt. Eignung: Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA,<=**]**

6.2.8.1.2 Dokumente suchen

Mit diesem Anwendungsfall kann ein Versicherter oder ein Vertreter nach Dokumenten oder Dokumentensets im ePA-Aktensystem auf Basis der Metadaten der Dokumente suchen. Als Ergebnis der Suchanfrage liefert das ePA-Aktensystem eine Liste von Metadaten zu Dokumenten.

6.2.8.1.2.1 Dokumente suchen - Document Service übergreifend
A_15472 -ePA-Frontend des Versicherten: Ergebnisliste Dokumente anzeigen
Das ePA-Frontend des Versicherten MUSS dem Nutzer das Ergebnis der Suche nach Dokumenten anzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_15474 -ePA-Frontend des Versicherten: Suche verfeinern
Das ePA-Frontend des Versicherten MUSS die Ergebnisse einer Suchanfrage zusammen mit den zur Suche verwendeten Parameter anzeigen und es dem Nutzer ermöglichen, die Suchparameter anzupassen und die Suchanfrage erneut auszuführen.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_28647 -ePA-Frontend des Versicherten: Nutzerorientierte Anzeigenamen für IHE XDS Codes
Das ePA-Frontend des Versicherten KANN dem Nutzer ermöglichen, versichertenverständliche Anzeigenamen gemäß den veröffentlichten "EPA IHE XDS * FrontendVS" Value Sets in [gemIG_TI_Terminology] anstelle der heruntergeladenen,

originalen Display Names der IHE XDS Codes anzuzeigen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.8.1.2.2 Dokumente suchen - XDS Document Service spezifisch

A_24706 -ePA-Frontend des Versicherten: Dokumente suchen
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen Dokumente in der Akte zu suchen unter Verwendung der Operation `I_Document_Management_Insurant::RegistryStoredQuery` des XDS Document Service gemäß [XDSDocumentService].**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_17854-01 -ePA-Frontend des Versicherten: Nutzung des Anfragetyps "FindDocumentsByTitle"
Das ePA-Frontend des Versicherten MUSS den in [ITI-18] nicht enthaltenen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-ITI-TF2#3.18.4.1.2.3.7.1] in Verbindung mit dem zusätzlich zu [ITI-18] eingeführten Suchparameter`$XDSDocumentEntryTitle` sowie dem optionalen Parameter`$XDSDocumentEntryAuthorInstitution` nutzen können.
[Frontend_Vers_ePA,funkt. Eignung: Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA,<=**]**

Der zusätzliche Parameter "$XDSDocumentEntryTitle" filtert die Suchergebnismenge über das Attribut XDSDocumentEntry.title. Dabei ist die Angabe von Platzhaltern (wie für Suchanfragen über den Parameter $XDSDocumentEntryAuthorPerson) möglich, die sich verhält wie das SQL Schlüsselwort "`LIKE`" in Kombination mit den anzugeben Wildcard-Zeichen "%", um jedes beliebige Zeichen und "_", um ein einzelnes beliebiges Zeichen zu finden.

Der optionale Parameter "`$XDSDocumentEntryAuthorInstitution`" filtert die Suchergebnismenge über das Attribut XDSDocumentEntry.authorInstitution.

A_25190-01 -ePA-Frontend des Versicherten: Nutzung des Anfragetyps "FindDocumentsByComment"
Das ePA-Frontend des Versicherten MUSS den in [ITI-18] nicht enthaltenen zusätzlichen Anfragetyp "FindDocumentsByComment" mit der Query-ID "urn:uuid:2609dda5-2b97-44d5-a795-3e999c24ca99" und denselben Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß[IHE-ITI-TF2#3.18.4.1.2.3.7.1] in Verbindung mit den zusätzlich zu [ITI-18] eingeführten Suchparametern`$XDSDocumentEntryComments` oder`$XDSDocumentEntryComment` (deprecated) nutzen können.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Hinweis zu A_17854 und A_25190*:*
Die beiden Anforderungen sind dazu gedacht die erweiterten Funktionen des Aktensystems hinsichtlich der Suche im ePA FdV nutzbar zu machen. Diese Funktionen dienen der Optimierung und Vermeidung unnötiger Latenzen. Ein ePA FdV kann die Suche nach "Title" und "Comment" am ePA-Aktensystem auch auf andere Weise geeignet umsetzen.

A_15469 -ePA-Frontend des Versicherten: Suchparameter für Dokumente
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Suchparameter auf Basis der XDS-Metadaten für eine Suchanfrage einzugeben. Für Suchparameter mit fest vorgegebenem Wertebereich muss der Nutzer eine Auswahlliste nutzen können.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Das Ergebnis der Suche soll für den Nutzer sortierbar und filterbar dargestellt werden.

A_21134-01 -ePA-Frontend des Versicherten: Unscharfe Ergebnisse in Ergebnisliste kennzeichnen

Das ePA-Frontend des Versicherten SOLL etwaige unscharfe Suchergebnisse (siehe gemSpec_Aktensystem_ePAfuerAlle#A_24764*) in der Ergebnismenge als solche kennzeichnen können.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.2.8.1.3 Dokument herunterladen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein Vertreter Dokumente aus dem Aktenkonto zum Anzeigen oder lokalen Speichern herunterladen.

6.2.8.1.3.1 Dokument herunterladen - Document Service übergreifend

A_15475-01 -ePA-Frontend des Versicherten: Dokumente einer Suchanfrage verarbeiten
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Dokumente aus dem Ergebnis einer Suchanfrage zum herunterzuladen (bspw. für die Anzeige oder lokales Speichern).**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_23620-01 -ePA-Frontend des Versicherten: Information des Versicherten bei fehlerhaften medizinischen Dokumenten
Das ePA-Frontend des Versicherten MUSS den Nutzer mit einer Fehlermeldung informieren, wenn nach dem Download aus dem Aktensystem technisch fehlerhafte Dokumente bzw. Teildokumente einer Sammlung erkannt werden. Sofern es sich um eine fehlerhaftes Teildokument einer Sammlung handelt, MÜSSEN die korrekten Teildokumente der Sammlung trotzdem angezeigt werden.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_15478 -ePA-Frontend des Versicherten: Dokument lokal speichern
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, ein aus dem Aktenkonto heruntergeladenes Dokument im lokalen Speicher persistent abzulegen.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_15479 -ePA-Frontend des Versicherten: Dokument mit Standardprogramm anzeigen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, wenn für einen gegebenen Dateitypen ein Standardprogramm verfügbar ist, ein aus dem Aktenkonto heruntergeladenes Dokument mit dem Standardprogramm anzuzeigen.
[Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.2.8.1.3.2 Dokument herunterladen - XDS Document Service spezifisch

A_24708 -ePA-Frontend des Versicherten: Dokumente herunterladen
Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen Dokumente aus der Akte herunterzuladen unter Verwendung der Operation `I_Document_Management_Insurant::RetrieveDocumentSet` des XDS Document Service gemäß [XDSDocumentService].**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_16222-02 -ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-43] - MTOM unterstützen
Das ePA-Frontend des Versicherten MUSS bei der Umsetzung der IHE XDS-Transaktion [ITI-43] die Übertragung von Dokumenten mit MTOM/XOP [MTOM] unterstützen.
[Frontend_Vers_ePA,funkt. Eignung: Konformitätsbestätigung, funkt. Eignung: Test Produkt/FA,<=**]**

6.2.8.1.4 Dokumente im Aktenkonto löschen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein Vertreter Dokumente im Aktenkonto löschen. Die Dokumente sind damit unwiederbringlich aus dem ePA-Aktensystem entfernt.

6.2.8.1.4.1 Dokumente im Aktenkonto löschen - Document Service übergreifend

A_15480-05 -ePA-Frontend des Versicherten: Dokumente zum Löschen markieren

Falls ein zu löschendes Dokument in einer Anhangsbeziehung (Elterndokument, Kinddokument) verknüpft ist, MUSS das ePA-Frontend des Versicherten dem Nutzer die Möglichkeit geben, diese Dokumente ebenfalls zu löschen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Hinweis zu A_15480:*
Ein Elterndokument kann mehrere Kinddokumente besitzen. Ein Kinddokument kann wiederum selbst über einen oder mehrere Anhänge verfügen. Dadurch können komplexe Anhangsketten (bzw. ein Anhangsbaum) entstehen.

A_15482 -ePA-Frontend des Versicherten: Dokumente löschen - Bestätigung

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente löschen" vom Nutzer eine Bestätigung einholen, dass die markierten Dokumente gelöscht werden sollen und die Möglichkeit geben, das Löschen abzubrechen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_20722-01 -ePA-Frontend des Versicherten: Dokumente löschen – Hinweis auf mögliche versorgungsrelevante Folgen

Das ePA-Frontend des Versicherten MUSS dem Nutzer im Anwendungsfall "Dokumente löschen" vor dem Löschen von Dokumenten in der elektronischen Patientenakteeinen Hinweis darauf geben, dass das Löschen von Dokumenten Auswirkungen auf die Versorgung und die Patientensicherheit haben kann.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

A_24353 -ePA-Frontend des Versicherten: Dokumente löschen – Hinweis auf löschen

Das ePA-Frontend des Versicherten MUSS dem Nutzer im Anwendungsfall "Dokumente löschen" vor dem Löschen von Dokumenten in der elektronischen Patientenakte auf die Möglichkeit des Verbergens von Dokumenten und Datenkategorien hinweisen.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

Hinweis 1: Es reicht aus, dass der Hinweis auf Verbergen nur ein Mal während einer laufenden User-Session angezeigt wird.

Hinweis 2: LEIs dürfen nicht auf Dokumente gemäß § 25b SGB V (Dokumente der Kategorie "`health_risk_analysis`") zugreifen. Verbergen statt Löschen ist deshalb nicht relevant. Im Rahmen der UX ist es sinnvoll, wenn A_24353- in diesem konkreten Fall nicht zu einem Hinweis führt.*

6.2.8.1.4.2 Dokumente im Aktenkonto löschen - XDS Document Service spezifisch

A_24709 -ePA-Frontend des Versicherten: Dokumente löschen

Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen Dokumente in der Akte zu löschen unter Verwendung der Operation I_Document_Management_Insurant::RemoveMetadata des XDS Document Service gemäß [XDSDocumentService].**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

6.2.8.1.5 Metadaten von Dokumenten ändern

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein befugter Vertreter die Metadaten von Dokumenten in der ePA ändern. Das Ändern von Metadaten an Dokumenten erfolgt ausschließlich über Nutzung des MHD Service gemäß [gemIG_ePA_MHD].

6.2.8.2 Medication Service

Die elektronische Medikationsliste (eML) und der elektronische Medikationsplan (eMP) wird im ePA-Aktensystem durch den Medication Service umgesetzt. Ein Nutzer des FdV kann die in seinem Aktenkonto gespeicherten Medikationsdaten einsehen.Anforderungen an den Medication Service sind in [gemIG_ePA_Medication] spezifiziert.

6.2.8.3 MHD Service

Die ePA für alle unterstützt das Lesen, Speichern, Suchen und Löschen von Dokumenten und die Aktualisierung von Metadaten über den **ePA MHD Service** (kurz MHD Service). Anforderungen an den MHD Service sind in [gemIG_ePA_MHD] spezifiziert.

6.2.8.4 Patient Service

Das Speichern von Identitätsdaten des Versicherten wird über den Patient Service umgesetzt. Anforderungen an den Patient Service sind in [gemIG_ePA_Basic] spezifiziert.

6.2.9 Protokollverwaltung

Bei der Nutzung eines Aktenkontos durch verschiedene Akteure werden Aktivitäten protokolliert, damit der Aktenkontoinhaber oder ein Vertreter diese Aktivitäten nachvollziehen kann. Dazu zählen beispielsweise Zugriffe auf die Dokumente und seine Metadaten sowie auch Aktivitäten mit administrativem Charakter. Die Protokolldaten werden im Aktenkonto abgelegt und müssen für eine Anzeige unter Nutzung des Audit Event Service abgefragt werden.
Mit diesem Anwendungsfall kann ein Versicherter bzw. ein Vertreter die Protokolldaten über die Zugriffe auf das Aktenkonto des Versicherten einsehen.Anforderungen an den Audit Event Service sind in [gemIG_ePA_Basic] spezifiziert.

6.2.10 Geräteverwaltung

Die Geräteverwaltung erfolgt im ePA-Aktensystem durch das Device Management.

A_24792 -ePA-Frontend des Versicherten: registrierte Geräte anzeigen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die für den Nutzer registrierten Geräte unter Verwendung der Operation getAllDevices gemäß [I_Device_Management_Insurant] zu ermitteln und einschließlich des aktuellen Status anzuzeigen.**[**Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_24802 -ePA-Frontend des Versicherten: Anzeigename für registriertes Gerät ändern
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, den Anzeigenamen eines für den Nutzer registrierten Gerätes unter Verwendung der Operation updateDevice gemäß [I_Device_Management_Insurant] zu ändern.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_24803 -ePA-Frontend des Versicherten: registriertes Gerät löschen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, ein aus der Liste der registrierten Geräte ausgewähltes Gerät unter Verwendung der Operation removeOneDevice gemäß [I_Device_Management_Insurant] zu löschen.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

A_25237 -ePA-Frontend des Versicherten: registriertes Gerät bestätigen
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, den Geräteregistrierungscode (Confirmation Code) zur Bestätigung einer neuen Geräteregistrierung einzugeben und diesen mit der Operation `confirmDevice` gemäß [I_Device_Management_Insurant] an das Aktensystem senden.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25292 -ePA-Frontend des Versicherten - Eingabe eines falschen Geräteregistrierungscodes
Falls das Device Management dem ePA-FdV für den vom Versicherten am ePA-FdV eingegebenen Geräteregistrierungscode (Confirmation Code) in einer Fehlermeldung einen Fehlerzähler zurückmeldet, weil der Geräteregistrierungscode nicht zum deviceIdentifier passt, MUSS das ePA Frontend des Versicherten dem Versicherten ermöglichen, erneut einen Geräteregistrierungscode einzugeben und den Versicherten darauf hinweisen, dass sich die Anzahl der erlaubten Versuche zur Eingabe des Geräteregistrierungscodes reduziert hat.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_28416 -ePA-Frontend des Versicherten – Filtern nach Zusammenführung
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Protokolldaten bei der Anzeige nach Protokolleinträgen einer Zusammenführung zu filtern.
[Frontend_Vers_ePA,Sich.techn. Eignung: Produktgutachten,<=**]**

6.2.11 Verwaltung von E-Mail-Adressen

Dieses Kapitel beschreibt Anwendungsfälle zur Administration der E-Mail-Adresse eines Nutzers.

Die E-Mail-Adresse eines Nutzers wird am Home-AS verwaltet. Als Home-AS wird das ePA-Aktensystem desjenigen Betreibers bezeichnet, der vom Kostenträger des Versicherten beauftragt wurde.

Im ePA-Aktensystem wird die Verwaltung der E-Mail-Adresse im Email Management Service realisiert. Ein Nutzer kann nur seine eigene E-Mail-Adresse verwalten. Die E-Mail-Adresse ist Voraussetzung für die Geräteregistrierung, d.h. um ein ePA FdV nutzen zu können muss bei der ersten Nutzung durch das ePA FdV bereits eine E-Mail-Adresse für den Nutzer hinterlegt sein. Die aktuelle E-Mail-Adresse kann zur Anzeige abgerufen oder geändert werden.

In diesem Kapitel werden die folgenden Anwendungsfälle umgesetzt:

- die für den Nutzer hinterlegten E-Mail-Adressen anzeigen
- E-Mail-Adresse für den Nutzer ändern

A_25442-01 -ePA-Frontend des Versicherten: E-Mail-Verwaltung am Aktensystem - Nutzung Schnittstelle
Das ePA-Frontend des Versicherten MUSS beim Ändern und Anzeigen der E-Mail-Adresse am ePA-Aktensystem die Operationen der Schnittstelle`I_Email_Management` gemäß [I_Email_Management] verwenden.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25443-01 -ePA-Frontend des Versicherten: E-Mail-Adressen verwalten
Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, seine im Aktensystem hinterlegte E-Mail-Adresse einzusehen und die E-Mail-Adresse zu ändern.
[Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

A_25721 -ePA-Frontend des Versicherten: Hinweis auf Benachrichtigungsmail

Das ePA-Frontend des Versicherten MUSS den Nutzer beim Hinterlegen einer neuen E-Mail-Adresse am ePA-Frontend des Versicherten darauf hinweisen, dass ihm eine E-Mail an die neu hinterlegte E-Mail-Adresse gesendet wird und dass der Nutzer die im Aktensystem hinterlegte E-Mail-Adresse nochmals prüfen sollte, falls er die E-Mail nicht erhält.
[Frontend_Vers_ePA,Sich.techn. Eignung: Herstellererklärung,<=**]**

6.2.12 Push Notification

Aktivitäten eines Nutzers in der Akte eines Versicherten können durch Push Notification dem Versicherten auf seinem mobilen Gerät angezeigt werden. Der Versicherte kann beispielsweise darüber informiert werden, dass ein neues Dokument in seine Akte eingestellt wurde oder ein Dokument aktualisiert wurde. Solche Aktivitäten werden im Folgenden Channel genannt.

Push Notifications der ePA können ausschließlich durch Versicherte für Ereignisse ihres eigenen Aktenkontos genutzt werden. Der Erhalt von Benachrichtigungen aus dem Aktenkonto eines vertretenen Versicherten wird nicht unterstützt.

Damit ein Versicherter das Feature Push Notification mit seinem ePA-FdV nutzen kann muss dieser hierzu seine Einwilligung geben. Das ist eine Einwilligung, die typischerweise auf dem Endgerät (z.B. iOS oder Android Gerät) lokal im System gespeichert wird. Diese kann ggf. in den Systemeinstellungen des Betriebssystems widerrufen werden.

Das ePA-FdV wird durch eine app_id eindeutig identifiziert, registriert sich beim plattformspezifischen Push Provider und erhält dabei einen pushkey.

Die Nachrichteninhalte werden durch das ePA-Aktensystem verschlüsselt. Das ePA-FdV entschlüsselt die Nachrichteninhalte zur Anzeige für den Nutzer. Der hierfür erforderliche Schlüssel wird im ePA-FdV erzeugt und persistiert und bei der Registrierung der FdV-Instanz für app_id und pushkey in der Akte hinterlegt.

Im zweiten Schritt werden die Channel konfiguriert, für welche im ePA-Aktensystem Push Notification erzeugt werden und an das Push Gateway gesendet werden.

Das Konzept und die anwendungsübergreifenden Anforderungen für das Feature Push Notification werden in [gemF_PushNotification] beschrieben. Eine FdV-Instanz ist hierbei die konkrete Installation eines ePA-FdV auf dem Gerät des Nutzers.

Das Feature Push Notification ist im ePA-FdV ein optionales Feature. Anforderungen hierzu werden im Titel der Anforderung mit "(Push)" gekennzeichnet.

6.2.12.1 FdV-Instanz registrieren

A_27627 -ePA-Frontend des Versicherten (Push): FdV-Instanz für Push Notification registrieren
Falls das ePA-Frontend des Versicherten die Option Push Notification unterstützt, MUSS es für die Registrierung und Verwaltung der registrierten FdV-Instanzen am ePA-Aktensystem die Operationen gemäß [I_Push_Notification_Management] verwenden.**[**ePA-FdV_Option_PushNotification,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.12.2 Channel für FdV-Instanz konfigurieren

A_27628 -ePA-Frontend des Versicherten (Push): Channel für Push Notification konfigurieren
Falls das ePA-Frontend des Versicherten die Option Push Notification unterstützt, MUSS es für die Konfiguration und Verwaltung der Channel für jede der registrierten FdV-Instanzen

am ePA-Aktensystem die Operationen gemäß [I_Push_Notification_Management] verwenden.**[**ePA-FdV_Option_PushNotification,funkt. Eignung: Test Produkt/FA,<=**]**

6.2.12.3 Push Notification Historie

Eine Push Notification Historie ist ein optionales Feature und wird im ePA-Aktensystem nicht wie in Kapitel 5.4.2 Push Notification Historie [gemF_PushNotification] beschrieben, umgesetzt.

Der Audit Event Service bildet die vollständige Historie einer Akte ab. Über Referenzen, die auf einzelne Audit Event Einträge zeigen und vom ePA-Aktensystem beim Versenden einer Push Nachricht dem Push Gateway bereitgestellt werden, besteht prinzipiell die Möglichkeit dem Nutzer eines ePA-FdV eine Historie von gesendeten Push Notification anzubieten.

6.3 Testtreiber-Modul für ePA-Frontend des Versicherten

Für die automatisierten Tests des gematik im Kontext von Zulassungsverfahren des ePA-Frontend des Versicherten muss der Hersteller ein Testtreiber-Modul implementieren. Dieses ist entweder in ein Test-FdV zu integrieren oder es steuert die GUI des ePA-Frontends an. Vom Hersteller ist der gematik der Zugriff auf das Test-FdV bzw. zu testende ePA-Frontend über das Interface des Testtreibermoduls entsprechend [gemKPT_Test#9.1 Bereitstellung von Remote-Test-FdVs] zu ermöglichen.

Das Außeninterface des TesttreiberModuls [I_Test_Driver_FdV] wird im Fachportal der gematik und in GitHub als normativer Bestandteil der Spezifikation veröffentlicht.

A_18044-02 -ePA-Frontend des Versicherten: Testtreiber-Modul
Der Hersteller des ePa-Frontend des Versicherten MUSS ein Testtreiber-Modul mit dem Außeninterface laut [I_Test_Driver_FdV] implementieren. Das Testtreiber-Modul MUSS die durch das ePA-Frontend des Versicherten – dem Zulassungsgegenstand – über eine produktspezifische Schnittstelle angebotene Funktionalität nutzen, um die Operationen der Schnittstellen umzusetzen.**[**Frontend_Vers_ePA,funkt. Eignung: Test Produkt/FA,<=**]**

Das Testtreiber-Modul darf die Ausgaben des ePA-Frontend des Versicherten gemäß der technischen Schnittstelle aufarbeiten, aber darf die Inhalte nicht verfälschen.

A_18171 -ePA-Frontend des Versicherten: Keine Fachlogik in Testtreiber-Modul
Das Testtreiber-Modul DARF NICHT die fachliche Logik des ePA-Frontend des Versicherten umsetzen.**[**Frontend_Vers_ePA,funkt. Eignung: Herstellererklärung,<=**]**

Der Einsatz des Testtreiber-Moduls ist auf das Zulassungsverfahren beschränkt und darf nicht in Wirkbetriebs-Apps genutzt werden.

A_18071 -ePA-Frontend des Versicherten: Beschränkung Einsatz Testtreiber-Modul
Das Frontend des Versicherten DARF ein Testtreiber-Modul NICHT enthalten.
[Frontend_Vers_ePA,Sich.techn. Eignung: Herstellererklärung,<=**]**

7 Verteilungssicht

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

8 Anhang A – Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
AN	Arbeitsnummer
eGK	Elektronische Gesundheitskarte
ePA	Elektronische Patientenakte
ePA-ePS	ePA European Patient Summary
FdV	ePA-Frontend des Versicherten
FDZ	Forschungsdatenzentrum Gesundheit
FQDN	Fully-Qualified Domain Name
GdV	Gerät des Versicherten
IHE	Integrating the Healthcare Enterprise
KTR	Kostenträger
KVNR	Krankenversichertennummer
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
LP	Lieferpseudonym
MHD	Mobile access to Health Documents (FHIR-Service im Aktensystem u.a. für Volltextsuche)
MTOM	Message Transmission Optimization Mechanism
NFC	Near Field Communication
OWASP	Open Web Application Security Project
PDF	Portable Document Format

PIN	Personal Identification Number
Pseudonymisierungs-schablone, Pseudonymisierungs-vorgaben	MIO-, bzw. FHIR-Profil-spezifische Auflistung aller möglichen Elemente, welche in eine pseudonyme Repräsentation übernommen werden können, jeweils definiert als Fhir-Path-Angabe
PUK	Personal Unblocking Key
SOAP	Simple Object Access Protocol
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust-service Status List
VZD-FHIR-Directory	Verzeichnisdienst FHIR-Directory

8.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
Patienteninformation	Ist ein durch eine Leistungserbringerinstitution im Aktenkonto bereitgestelltes Dokument, welches vorrangig der Information von Versicherten dient. Das Dokument wird durch den Leistungserbringer als Versicherteninformation gekennzeichnet.
Versicherten-ID	Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen Krankenversichertennummer (KVNR).
Versichertendokument	Ist ein durch einen Versicherten (Aktenkontoinhaber oder Vertreter) im Aktenkonto bereitgestelltes Dokument
Versicherteninformation	siehe Patienteninformation

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

8.3 Abbildungsverzeichnis

Abbildung 1: Komponenten ePA-Frontend des Versicherten.....13
Abbildung 2: Authentisieren des Nutzers.....42

8.4 Tabellenverzeichnis

Tabelle 1: Akteure und Rollen....10
Tabelle 2: Schnittstellen des ePA-Aktensystems....11
Tabelle 3: Komponenten des FdV....13
Tabelle 4: IHE Akteure und Transaktionen....25
Tabelle 5: Parameter FdV....34
Tabelle 6: Tab_UX_KPI_Messung_ePA....37
Tabelle 7: FHIR Suche LEI....48
Tabelle 8: FHIR Suche DiGA....50
Tabelle 9: Vertretung am fremden FdV verwalten....61

8.5 Referenzierte Dokumente

8.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemKPT_ePAfuerAlle]	gematik: Grobkonzept der "ePA für alle"
[gemKPT_Test]	gematik: Testkonzept der TI
[gemSpec_Aktensystem_ePAfueralle]	gematik: Spezifikation Aktensystem ePA für alle
[gemSpec_IDP_Frontend]	gematik: Spezifikation Identity Provider - Frontend
[gemSpec_IDP_Sek]	gematik: Spezifikation Sektoraler Identity Provider
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_PKI]	gematik: Übergreifende Spezifikation PKI
[gemSpec_SigD]	gematik: Spezifikation Signaturdienst
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst

[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory
[gemSpec_X_509_TSP]	gematik: Spezifikation Trust Service Provider X.509
[I_Test_Driver_FdV]	gematik: I_Test_Driver_FdV Testtreiber-Schnittstellen GitHub: https://github.com/gematik/api-ePA-Testtreiber Path: src/openapi/I_Test_Driver_FdV.yaml
[gemIG_ePA_Basic]	gematik: FHIR Implementation Guide "ePA Basisfunktionalitäten" https://gematik.de/fhir/epa/ImplementationGuide/de.gematik.epa
[gemIG_ePA_Medication]	gematik: FHIR Implementation Guide "ePA Medication Service" https://gematik.de/fhir/epa-medication/ImplementationGuide/de.gematik.epa.medication
[gemIG_ePA_MHD]	gematik: FHIR Implementation Guide "ePA MHD Service" https://gematik.de/fhir/epa-mhd/ImplementationGuide/de.gematik.epa.mhd
[gemIG_TI_Terminology]	gematik: Implementation Guide "TI Terminology" https://gematik.de/fhir/terminology/ImplementationGuide/de.gematik.terminology
[ePA_Basic]	gematik: GitHub Repository "ePA-Basic" https://github.com/gematik/ePA-Basic
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung und impliziten Geräteregistrierung siehe [ePA_Basic] Path: src/openapi/I_Authorization_Service.yaml
[I_Entitlement_Management]	gematik: I_Entitlement_Management REST-Schnittstelle zur Verwaltung von Befugnissen und Befugnisausschlüssen siehe [ePA_Basic] Path: src/openapi/I_Entitlement_Management.yaml
[I_Entitlement_Management_EU]	gematik: I_Entitlement_Management_EU REST-Schnittstelle zur Verwaltung von Befugnissen als Erweiterung für EU-Zugriff siehe [ePA_Basic] Path: src/openapi/I_Entitlement_Management_EU.yaml
[I_Consent_Decision_Management]	gematik: I_Consent_Decision_Management REST-Schnittstelle zum Management der Widersprüche zu Versorgungsprozessen siehe [ePA_Basic] Path: src/openapi/I_Consent_Decision_Management.yaml
[I_Device_Management_Ins	gematik: I_Device_Management_Insurant.yaml

urant]	REST-Schnittstelle zur Geräteverwaltung siehe [ePA_Basic] Path: src/openapi/I_Device_Management_Insurant.yaml
[I_Email_Management]	gematik: I_Email_Management.yaml REST-Schnittstelle zur Verwaltung der Email Adresse siehe [ePA_Basic] Path: src/openapi/I_Email_Management.yaml
[I_Push_Notification_Management]	gematik: I_Push_Notification_Management REST-Schnittstelle zur Verwaltung der Pusher und Channel bei Push Notification siehe [ePA_Basic] Path: src/openapi/I_Push_Notification_Management.yaml
[ePA_XDS_Document]	gematik: GitHub Repository "ePA-xds-document" https://github.com/gematik/ePA-XDS-Document
[I_Constraint_Management_Insurant]	gematik: I_Constraint_Management_Insurant.yaml REST-Schnittstelle zum Verbergen und Sichtbarmachen von Dokumenten siehe [ePA_XDS_Document] Path: src/openapi/I_Constraint_Management_Insurant.yaml
[XDSDocumentService]	gematik: XDSDocumentService.wsdl IHE-Schnittstelle des XDSDocumentService siehe [ePA_XDS_Document] Path: src/schema
[gemSpec_IG_ePA]	gematik: Implementation Guides für strukturierte Dokumente GitHub: siehe [ePA_XDS_Document] Path: src/implementation_guides
[gemF_PushNotification]	gematik: Anwendungsübergreifende Push Notification
[Organization in gematik Directory]	Profil der Organization Ressource. https://simplifier.net/vzd-fhir-directory/organizationdirectory
[HealthcareService in gematik Directory]	Profil der HealthcareService Ressource. https://simplifier.net/vzd-fhir-directory/healthcareservicedirectory
[I_Tool_Convert_PDF_Insurant]	gematik: I_Tool_Convert_PDF_Insurant Schnittstelle für die PDF Formatkonvertierung siehe [ePA_XDS_Document] Path: src/openapi/ I_Tool_Convert_PDF_Insurant.yaml

2874 ### 8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-TF2]	IHE International (2025): IHE IT Infrastructure (ITI) Technical Framework,

	Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.2, https://profiles.ihe.net/ITI/TF/Volume2/
[IHE-ITI-RMD]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.6 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-RMU]	IHE International (2021): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.3 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[LVZ]	LÄNDERVERZEICHNIS für den amtlichen Gebrauch in der Bundesrepublik Deutschland https://www.auswaertiges-amt.de/blob/215256/e13a148b838b0734f6fca63b15029c9f/laenderverzeichnis-data.pdf
[OWASP Proactive Control]	OWASP Top Ten Proactive Controls Project OWASP Proactive Controls For Developers v3.0 https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf
[OWASP SAMM Project]	OWASP SAMM Project https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Browse_Online
[OWASPMobileTop10]	OWASP Mobile Security Project: Top 10 Mobile Risks https://owasp.org/www-project-mobile-top-10/
[OWASP MASVS]	OWASP Mobile Application Security Verification Service https://owasp.org/www-chapter-geneva/assets/slides/OWASP_Geneva-Chapter_Meeting-20161212_Jeremy_Matos-MASVS.pdf
[OWASP TTMC]	OWASP Mobile Security Project https://owasp.org/www-project-mobile-security/
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP https://tools.ietf.org/html/rfc6960
[INA]	INA - Interoperabilitäts-Navigator für digitale Medizin https://www.ina.gematik.de
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material),

	http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[XMLEnc-1.1]	XML Encryption Syntax and Processing, W3C Recommendation 11 April 2013, http://www.w3.org/TR/xmlenc-core1/
[NGP]	Schnittstelle des Nationalen Gesundheitsportal (gesund.bund.de) gemäß search.gesund.bund.de/documentation/gematik/
[rfc7515]	"JSON Web Signature (JWS)" RFC 7515 IETF Mai 2015
[rfc7519]	"JSON Web Token (JWT)" RFC 7519 IETF Mai 2015
[rfc4122]	"A Universally Unique Identifier (UUID) URN Namespace" RFC 4122 IETF Julli 2005
[BSI PVePAeRp]	BSI (2021): Prüfvorschrift für den Produktgutachter des „ePA-Frontend des Versicherten“ und des „E-Rezept-Frontend des Versicherten“ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/Pruefvorschrift_Produktgutachter_ePA-Frontend.html
[Nutzungszwecke des FDZ]	Nutzungszwecke des FDZ Gesundheit https://www.forschungsdatenzentrum-gesundheit.de/infoportal/antragsvorbereitung/nutzungszwecke

2875