

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Spezifikation Aktensystem ePA für alle**

Version:	1.6.0 CC
Revision:	1298971
Stand:	15.07.2025
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_Aktensystem_ePAfueralle

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

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

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.01.2024		ePA für alle	gematik
1.1.0	28.03.2024		ePA für alle - Release 3.0.1	gematik
1.2.0	12.07.2024		ePA für alle - Release 3.0.2, Zuordnungen für Release E- Rezept 1.6.5	gematik
1.3.0	14.08.2024		ePA für alle - Release 3.1.0	gematik
1.4.0	28.02.2025		ePA für alle - Release 3.0.5	gematik
1.5.0	27.05.2025		ePA für alle - Release 3.1.2	gematik
1.6.0 CC	15.07.2025		ePA für alle - Release 3.1.2-1	gematik

---

## Inhaltsverzeichnis

---

*Please update the table of contents.*

---

## 1 Einführung

---

### 1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zur Herstellung, Test und Betrieb des Produkttyps ePA-Aktensystem.

### 1.2 Zielgruppe

Das Dokument richtet sich an Anbieter und Hersteller des Produkttyps ePA-Aktensystem sowie an Anbieter und Hersteller von Produkten, die die Schnittstellen des Produkttyps ePA-Aktensystem nutzen.

### 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

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps ePA-Aktensystem verzeichnet.

## 1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern 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.

---

## 2 Übergreifende Festlegungen

---

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.

### **A\_24986 -ePA-Aktensystem - Rollentrennung ePA-Aktensystem und IDP-Dienst**

Falls der Betreiber des ePA-Aktensystems auch den IDP-Dienst betreibt, MUSS der Betreiber sicherstellen, dass die Erstellung oder Änderungen von IDToken beim IDP-Dienst und die Verarbeitung und Prüfung der Client-Attestation im ePA-Aktensystem durch geeignete technische und organisatorische Maßnahmen so wirkungsvoll voneinander getrennt werden, dass ein einzelner Mitarbeiter des Betreibers nicht beide Aktivitäten durchführen kann.[<=]

### **A\_25149-01 -ePA-Aktensystem - Rollentrennung ePA-Aktensystem und sektoraler IDP**

Falls der Betreiber des ePA-Aktensystems auch einen sektoralen IDP betreibt, MUSS der Betreiber sicherstellen, dass die Erstellung oder Änderungen von ID-Token beim sektoralen IDP und die Erstellung oder Änderungen der Mailadresse für die Geräteverwaltung im ePA-Aktensystem durch geeignete technische und organisatorische Maßnahmen so wirkungsvoll voneinander getrennt werden, dass ein einzelner Mitarbeiter des Betreibers nicht die Aktivitäten in beiden Diensten durchführen kann.[<=]

### **A\_24673 -Zeitsynchronisation über Zeitdienst in der TI**

Das ePA-Aktensystem MUSS die Systemzeit über den Zeitdienst in der TI gemäß [gemSpec\_Net#6.2] synchronisieren  
[<=]

### **A\_25612 -ePA-Aktensystem - Authentisierung gegenüber einem Client innerhalb der TI**

Das ePA-Aktensystem MUSS sich beim Aufruf durch einen Client innerhalb der TI mit der TLS-Identität oid\_epa\_dvw und Zertifikatsprofil C.FD.TLS-S authentisieren.[<=]

### **A\_24676 -Useragent Information in HTTP Header außerhalb des VAU-Kanals**

Das ePA-Aktensystem MUSS sicherstellen, dass in der Kommunikation mit den ePA-Clients außerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "x-useragent" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen.  
[<=]

### **A\_24677 -Useragent Information in HTTP Header innerhalb des VAU-Kanals**

Das ePA-Aktensystem MUSS sicherstellen, dass in der Kommunikation mit den ePA-Clients innerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "x-useragent" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen.  
[<=]

Die Formatvorgaben zum Useragent sind in A\_22470\* definiert.

### **A\_24816-01 -Aktenkontokennung in HTTP Header innerhalb des VAU-Kanals**

Das ePA-Aktensystem MUSS sicherstellen, dass ePA-Clients in der Kommunikation mit den Medical Services der ePA innerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "x-insurantId" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen.[<=]

Hinweis: Das HTTP Header-Element mit dem Namen "x-insurantId", belegt mit einer KVNR, ist erforderlich, um die Zuordnung zu einer konkreten Akte gewährleisten zu können.

Hinweis: Das betrifft die Kommunikation mit dem XDS Document Service (SOAP) und dem FHIR Data Service (FHIR). Die Operationen aller weiteren Services definieren die Notwendigkeit des Parameters x-insurantId in der jeweiligen Schnittstellenbeschreibung (OpenApi).

#### **A\_27701 -Requestkennung in HTTP Header außerhalb des VAU-Kanals**

Falls in der Kommunikation mit den ePA-Clients außerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "X-Request-ID" gesendet wird MUSS das ePA-Aktensystem sicherstellen, dass der Wert von "X-Request-ID" eine UUID ist und andernfalls den Request mit HTTP-Fehler 400 ablehnen.【<=】

#### **A\_27702 -Requestkennung in HTTP Header innerhalb des VAU-Kanals**

Falls in der Kommunikation mit den ePA-Clients innerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "X-Request-ID" gesendet wird MUSS das ePA-Aktensystem sicherstellen, dass der Wert von "X-Request-ID" eine UUID ist und andernfalls den Request mit HTTP-Fehler 400 ablehnen.【<=】

#### **A\_27703 -Requestkennung in der Response**

Falls ein HTTP Header Element mit dem Namen "X-Request-ID" in einem Request an das ePA-Aktensystem gesendet wird MUSS das ePA-Aktensystem sicherstellen, dass die Response ein HTTP Header Element mit dem Namen "X-Request-ID" enthält und mit dem Wert aus dem Request belegt wird.【<=】

#### **A\_27712 -Requestkennung - betriebliche Protokollierung**

Falls ein HTTP Header Element mit dem Namen "X-Request-ID" in einem Request an das ePA-Aktensystem gesendet wird MUSS der Anbieter des ePA-Aktensystems sicherstellen, dass der Wert von "X-Request-ID" in der Protokollierung des Betreibers berücksichtigt wird.【<=】

#### **A\_27443 -Nutzung Terminologiepaket**

Das ePA-Aktensystem MUSS die relevanten Terminologien des Terminologiepakets gemäß [IG\_TI\_Terminology] verarbeiten und in der Kommunikation mit dem ePA-Aktensystem berücksichtigen.【<=】

Hinweis zu A\_27443:

Das Terminologiepaket wird als FHIR-Package bereitgestellt und enthält z.B. Vocabulary ePA und Value Set für Berechtigungskategorien.

#### **A\_27708 -ePA-Aktensystem - Festlegung zu Formatvorgabe für Datentyp datetime gemäß RFC3339**

Das ePA-Aktensystem MUSS bei der Verwendung des Datentyps datetime das Format gemäß RFC3339 wie folgt einschränken:

- Datum als <date> im Format YYYY-MM-DD (gemäß RFC3339 full-date)
- Zeit als <time> im Format hh:mm:ss (gemäß RFC3339 time-hour ":" time-minute ":" time-second)
- Zeitzonen als <zone> im Format "Z" oder time-numoffset (gemäß RFC3339 time-offset)
- <date>"T"<time><zone>
- „T“ und „Z“ Zeichen sind in Groß- bzw. Kleinschreibung zulässig

Diese Formatvorgabe betrifft nicht die Bestandsdatenlieferung.【<=】

Beispiele für Datentyp datetime:

2025-04-12T15:20:50Z

2025-06-30T23:59:59+01:00

#### **A\_27868 -ePA-Aktensystem - fehlerhafter URL-Pfad**

Falls ein URL-Pfad adressiert wird, der keinem für das Aktensystem spezifizierten Services zugeordnet werden kann, MUSS das ePA-Aktensystem den Aufruf mit dem HTTP-Statuscode 404 mit Errorcode pathNotFound ablehnen.

[<=]

## 2.1 Aktensystem- und Service-Lokalisierung

Die Lokalisierung der Services der ePA für alle für ePA-Clients, die über das zentrale Netz der TI auf die Anwendung zugreifen, erfolgt mittels der übergreifenden Domäne epa4all.de. Da nicht gesteuert werden kann, welchen DNS ein ePA-Client verwendet, kann diese Domäne sowohl im Internet als auch im DNS der TI aufgelöst werden und verweist immer auf IP-Adressen der TI. Für die verschiedenen Umgebungen der TI werden third-level Domänen eingerichtet: .ref (RU1), .dev (RU2), .test (TU) und .prod (PU).

Ein ePA-Client aus der TI kennt die FQDNs der ePA-Aktensysteme (diese werden hier fest definiert, vgl. A\_24592-\*). Das Vorgehen der festvorgegebenen FQDNs ist analog zum E-Rezept-Vorgehen.

Ein ePA-FdV kennt den FQDN seines ePA-Aktensystems und erhält die Information über die dort verwendeten Service-Endpunkte über den Abruf einer Konfigurationsdatei unter /.well-known. In dieser Datei sind die verschiedenen Pfade zu den Endpunkten hinterlegt.

Jedes ePA-FdV ruft an seinem ePA-Aktensystem auch eine Liste aus allen Namen der verschiedenen Kostenträger und den zuständigen FQDN ab, damit diese im Falle einer Vertretung genutzt werden können, um das entsprechende Aktensystem zu finden.

### A\_24592-02 -Anbieter ePA-Aktensystem -Registrierung an übergreifender ePA-Domäne

Der Anbieter des ePA-Aktensystems MUSS seine Hosts und IP-Adressen für Services, die über das zentrale Netz der TI angeboten werden, in der übergreifenden ePA-Domäne epa4all.de für die Sub-Domänen ref (RU1), dev (RU2), test (TU) und prod (PU) unter folgend aufgeführten DNS-Namen (FQDN) registrieren. Diese sind

1. Host und IP-Adressen für den Endpunkt I\_Information\_Service und der Services in der VAU:  
epa-as-<ePA-Anbieter-Zahl>.<Umgebung>.epa4all.de.
2. Host und IP-Adressen für den Endpunkt I\_Information\_Service\_Accounts:  
epa-asisa-<ePA-Anbieter-Zahl>.<Umgebung>.epa4all.de.

Die "ePA-Anbieter-Zahl" wird durch die gematik festgelegt.

[<=]

Folgende Zuordnungen der "ePA-Anbieter-Zahl" wurden vorgenommen:

ePA-Anbieter-Zahl	Anbieter / Betreiber
1	IBM
2	Bitmarck Technik

Sobald ein neuer Anbieter/Betreiber hinzukommt, wird diesem die kleinste, nicht belegte Ziffer (>0) durch die gematik zugewiesen.

### Beispiele der Dienstlokalisierung



## PU :

### Aktensystem A

epa-as-1.prod.epa4all.de A 100.102.x1.x2  
 ggf. ... weitere IP-Adressen für epa-as-1.prod.epa4all.de (DNS-Round-Robin)  
 ...  
 epa-asisa-1.prod.epa4all.de A 100.102.x3.x4

### Aktensystem B

epa-as-2.prod.epa4all.de A 100.102.x5.x6  
 epa-asisa-2.prod.epa4all.de A 100.102.x7.x8

## TU :

### Aktensystem 1

epa-as-1.test.epa4all.de A 172.30.x9.x10

...

D. h. ein ePA-Client aus der TI (Primärsystem) kennt die für ihn zwei relevanten FQDNs (PU: epa-as-1.prod.epa4all.de und epa-as-2.prod.epa4all.de) und verwendet diese um die beiden Aktensystem zu kontaktieren. Eine dynamisch konfigurierbare Anzahl der Anbieter in einem Primärsystem wird aktuell nicht in der Spezifikation gefordert.

### A\_14128-04 -Anbieter ePA-Aktensystem - Resource Records FQDN ePA

Der Anbieter des ePA-Aktensystems MUSS in seinen Nameservern im Internet den FQDN des Aktensystems für das ePA-FdV auflösen.

[<=]

### A\_22688-04 -Anbieter ePA-Aktensystem, Konfiguration Schnittstellen über /.well-known/

Der Anbieter des ePA-Aktensystems MUSS an seinen Access Gateway des Versicherten über den URL-Pfadnamen (bzw. die Datei) /.well-known/epa-configuration.json eine JSON-Repräsentation aller Pfade zu seinen Komponenten verfügbar machen.

D. h. der Aufrufende (ePA-FdV) MUSS wenn er diesen Pfad per HTTP-GET abfragt ein JSON-Objekt (also Content-Type "application/json") vom Access Gateway des Versicherten erhalten der Art

```
{
  "version" : "<Produkttypversion des Aktensystems im Format[0-9]{1,3}\.
[0-9]{1,3}\.[0-9]{1,3}>",
  ....
}
```

### A\_22687 -Aktensystem, Konfiguration Schnittstellen über /.well-known/

Das ePA-Aktensystem MUSS sicherstellen, dass dem Anbieter des ePA-Aktensystems die technische Möglichkeit bereitgestellt wird A\_22688-\* umzusetzen. [<=]

### A\_26814 -ePA-Aktensystem - Schnittstellenadressierung

Das ePA-Aktensystem MUSS die Schnittstellenadressierung (relative Pfade) gemäß der Schnittstellenspezifikationen umsetzen. [<=]

Schnittstellenspezifikationen für die fachlichen Requests erfolgen durch WSDL, OpenAPI und FHIR Implementation Guides.

Für Operationen, die innerhalb einer ePA-VAU aufgerufen werden, gelten die Schnittstellenspezifikationen für den inneren HTTP-Request.

Abgrenzend hierzu wird das VAU-Protokoll und die dabei verwendeten Pfade in [gemSpec\_Krypt#7] definiert.

### **A\_24801 -Aktensystem, Liste von FQDN im Internet**

Das ePA-Aktensystem MUSS dem ePA-FdV eine Liste aller Kostenträger und der FQDN, unter der deren ePA-Aktensystem im Internet erreichbar ist, bereitstellen. Die Liste setzt sich zusammen aus den selbst verwalteten Kostenträgern und den über I\_Information\_Service\_Accounts bezogenen Teillisten der anderen ePA-Aktensysteme.

[<=]

## **2.2 Redundanz**

Die Anforderungen an die Redundanzen des ePA-Aktensystems finden sich in gemSpec\_Perf.

## **2.3 Datenschutz und Sicherheit**

### **A\_15128 -Anbieter ePA-Aktensystem - Schutz der transportierten Daten im ePA-Aktensystem**

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die Vertraulichkeit und Integrität der innerhalb des ePA-Aktensystems transportierten Daten gewährleistet ist.

[<=]

Die folgenden Anforderungen verhindern Profilbildungen über Versicherte und Leistungserbringer(-institutionen) durch den Anbieter bzw. dessen Mitarbeiter.

### **A\_15103 -Anbieter ePA-Aktensystem - Konzept zur Verhinderung von Profilbildung**

Der Anbieter des ePA-Aktensystems MUSS ein Konzept erstellen und umsetzen, dass sicherstellt, dass Mitarbeiter des Anbieters die im ePA-Aktensystem verarbeiteten Daten nicht für Profilbildungen über Versicherte oder Leistungserbringer(-institutionen) nutzen können.[<=]

*Hinweis: Das Konzept kann Teil des Sicherheits- oder Datenschutzkonzeptes des Anbieters sein. Es ist nicht notwendigerweise ein eigenes Dokument erforderlich.*

### **A\_25722 -ePA-Aktensystem - Löschen von personenbezogenen Daten von Vertretern nach Wegfall der Notwendigkeit**

Das ePA-Aktensystem MUSS die personenbezogenen Daten eines Vertreters löschen, sofern der Vertreter kein Aktenkonto im ePA-Aktensystem besitzt und der Vertreter keine Versicherten im ePA-Aktensystem mehr vertritt.[<=]

### **A\_15104 -Anbieter ePA-Aktensystem - Ordnungsgemäße IT-Administration**

Der Anbieter des ePA-Aktensystems MUSS die Maßnahmen für erhöhten Schutzbedarf des BSI-Bausteins „OPS.1.1.2 Ordnungsgemäße IT-Administration“ [BSI-Grundschutz] während des gesamten Betriebs des ePA-Aktensystems umsetzen.[<=]

*Hinweis: Die Anforderungen des BSI-Bausteins sind entsprechend des dort genannten Schlüsselwortes (MUSS, DARF NICHT/ DARF KEIN, SOLLTE; SOLLTE NICHT/SOLLTE KEIN, KANN/DARF) umzusetzen.*

### **A\_15824 -Anbieter ePA-Aktensystem - Sichere Speicherung von Daten**

Unabhängig davon, ob die Daten schon verschlüsselt vorliegen, MUSS der Anbieter des ePA-Aktensystems die Daten des ePA-Aktensystems bei der Speicherung verschlüsseln.

[<=]

*Hinweis: Dies kann z. B. durch eine transparente Datenbankverschlüsselung oder eine Festplattenverschlüsselung erfolgen.*

#### **A\_24774 -Anbieter ePA-Aktensystem - Zwei-Faktor-Authentisierung von Administratoren**

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass sich Administratoren mindestens mit einer Zwei-Faktor-Authentisierung anmelden.[<=]

#### **A\_15107-02 -Anbieter ePA-Aktensystem - Keine unzulässige Weitergabe von Daten**

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die in seinem Aktensystem verarbeiteten Daten nicht weitergegeben werden, auch nicht in pseudonymisierter oder anonymisierter Form. Davon ausgenommen sind Weitergaben an berechtigte Nutzer der Aktenkonten, an einen durch den Versicherten gewählten Anbieter beim Anbieterwechsel sowie Übermittlungen an das Forschungsdatenzentrum Gesundheit soweit dagegen kein Widerspruch durch den Versicherten oder einen Vertreter vorliegt.[<=]

#### **A\_15119 -Anbieter ePA-Aktensystem - Löschkonzept**

Der Anbieter des ePA-Aktensystems MUSS in einem Löschkonzept für die im ePA-Aktensystem verarbeiteten personenbezogenen Daten mindestens folgende Aspekte beschreiben:

- die umgesetzten organisatorischen und technischen Löschmaßnahmen (dies beinhaltet insbesondere auch die Löschung von Backups, Protokollen etc.),
- die Löschregeln und Löschfristen zusammen mit einer nachvollziehbaren Begründung für die getroffenen Fristfestlegungen,
- wie sichergestellt wird, dass alle Auftragnehmer die Löschpflichten ihrerseits umsetzen.

[<=]

*Hinweis: Das Löschkonzept kann Teil des Sicherheits- oder Datenschutzkonzeptes des Anbieters sein. Es ist nicht notwendigerweise ein eigenes Dokument erforderlich.*

#### **A\_15169 -ePA-Aktensystem - Verbot von Werbe- und Usability-Tracking**

Die Komponenten des ePA-Aktensystems DÜRFEN im Produktivbetrieb ein Werbe- und Usability-Tracking NICHT verwenden.

Davon ausgenommen ist das Erfassen des standardmäßigen quantitativen Nutzerverhaltens zur Ermittlung der Standard-Aktenutzung entsprechend der Anforderung A\_15154.[<=]

#### **A\_15154 -Anbieter ePA-Aktensystem - Ermittlung von Standard-Aktenutzung**

Der Anbieter des ePA-Aktensystems MUSS mindestens einmal im Jahr Werte zu einer Standard-Aktenutzung von LE und Versicherten durch die Profilierung anonymer Zugriffsstatistiken auf das ePA-Aktensystem zum Zweck der Erkennung von Zugriffen gemäß A\_15155 ermitteln.[<=]

#### **A\_15155 -Anbieter ePA-Aktensystem - Abweichung von Standard-Aktenutzung**

Der Anbieter des ePA-Aktensystems MUSS Zugriffe und Zugriffsmuster, die nicht einer Standard-Aktenutzung entsprechen, erkennen und Maßnahmen zur Schadensreduzierung umsetzen.[<=]

*Hinweis: Diese Erkennung darf keine zusätzliche Persistierung von personenbezogenen Daten auslösen. Ausnahme sind hier nur die notwendigen Daten, falls ein Missbrauch erkannt wird.*

#### **A\_24778 -Anbieter ePA-Aktensystem - Einsatz zertifizierter HSM**

Der Anbieter des ePA-Aktensystems MUSS beim Einsatz eines HSM sicherstellen, dass dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria oder Federal Information Processing Standard (FIPS) in Frage.

Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3 oder

2. FIPS 140-3 Level 3 oder
  3. Common Criteria EAL 4+ (mit AVA\_VAN.5)
- entsprechen. [≤]

## **A\_15157 -Anbieter ePA-Aktensystem - Sicherer Betrieb und Nutzung eines HSMs**

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die auf dem HSM verarbeiteten privaten Schlüssel, Konfigurationen und eingesetzte Software nicht unautorisiert ausgelesen, unautorisiert verändert, unautorisiert ersetzt oder in anderer Weise unautorisiert benutzt werden können. [≤]

## **A\_15159 -Anbieter ePA-Aktensystem - Schutzmaßnahmen gegen die OWASP Top 10 Risiken**

Der Anbieter des ePA-Aktensystems MUSS in allen Komponenten des ePA-Aktensystems technische Maßnahmen zum Schutz vor den in der aktuellen Version genannten OWASP-Top-10-Risiken umsetzen. [≤]

## **A\_24780-01 -Anbieter ePA-Aktensystem - Versicherte über sensible Änderungen informieren**

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass der Versicherte informiert wird, wenn der Anbieter des Aktensystems eine manuelle Änderung bezüglich einer Akte (Aktenverwaltung) im Auftrag eines Versicherten durchführt. [≤]

*Hinweis: Ein Beispiel einer manueller Änderung durch den Anbieter des Aktensystems ist die manuelle Änderung einer E-Mail-Adresse auf Wunsch des Versicherten gegenüber dem Anbieter.*

## **A\_15163 -Anbieter ePA-Aktensystem - Angriffen entgegenwirken**

Der Anbieter des ePA-Aktensystems MUSS Maßnahmen zur Erkennung von Angriffen und zur Reduzierung bzw. Verhinderung von Schäden aufgrund von Angriffen in allen Komponenten des ePA-Aktensystems umsetzen. [≤]

## **A\_15167 -Anbieter ePA-Aktensystem - Social Engineering Angriffen entgegenwirken**

Der Anbieter des ePA-Aktensystems MUSS Maßnahmen zur Erkennung und Verhinderung von Social Engineering Angriffen umsetzen. [≤]

## **A\_24989 -Anbieter ePA-Aktensystem - Schutz vor Angriffen über die TI**

Die Anbieter des ePA-Aktensystems MUSS für alle über die TI erreichbaren Schnittstellen des ePA-Aktensystems Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS Lösungen verhindert werden. [≤]

## **A\_15168 -ePA-Aktensystem - Verbot vom dynamischen Inhalt**

Die Komponenten des ePA-Aktensystems DÜRFEN dynamischen Inhalt von Drittanbietern NICHT herunterladen und verwenden.  
[≤]

## **A\_17080 -Verhindern von Session Hijacking**

Die Komponenten des ePA-Aktensystems MÜSSEN geeignete Schutzmaßnahmen gegen Session-Hijacking implementieren.  
[≤]

## **A\_16323-01 -ePA-Aktensystem - Verbot von medizinisch irrelevantem Inhalt**

Der Anbieter des ePA-Aktensystems MUSS der Ablage von Dokumenten, die für die medizinische Versorgung oder für die Eigenorganisation medizinischer Belange des Versicherten oder zur Erstattung der Behandlungskosten irrelevant sind, mittels AGB auf Anbieterseite entgegenwirken.  
[≤]

## **A\_24781 -Sicherer Betrieb des Produkts nach Handbuch**

Der Anbieter eines ePA-Aktensystems MUSS die im Handbuch des eingesetzten ePA-Aktensystems beschriebenen Voraussetzungen für den sicheren Betrieb des Produktes gewährleisten. [≤]

#### **A\_18953 -Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch**

Der Hersteller des ePA-Aktensystems MUSS für sein Produkt im dazugehörigen Handbuch leicht ersichtlich darstellen, welche Voraussetzungen vom Betreiber und der Betriebsumgebung erfüllt werden müssen, damit ein sicherer Betrieb des Produktes gewährleistet werden kann. [≤]

#### **A\_19122-01 -Anbieter ePA-Aktensystem - Trennung zu anderen Mandanten**

Ein Betreiber eines ePA-Aktensystems MUSS sicherstellen, dass die Daten von unterschiedlichen Mandanten organisatorisch und technisch getrennt sind. [≤]

#### **A\_21106 -Anbieter ePA-Aktensystem - Signaturschlüssel für Protokolle**

Das ePA-Aktensystem MUSS für die Signatur von Listen von Protokollen des Versicherten Schlüsselmaterial der Ausstelleridentität ID.FD.SIG mit einem zugehörigen Zertifikat C.FD.SIG mit der Rolle oid\_epa\_logging gemäß [gemSpec\_OID] besitzen. [≤]

#### **A\_21107 -Anbieter ePA-Aktensystem - Speicherung Signaturschlüssel für Protokolle im HSM**

Das ePA-Aktensystem MUSS das private Schlüsselmaterial der Ausstelleridentität ID.FD.SIG für die Signatur von Listen von Protokollen des Versicherten in einem HSM speichern.  
[≤]

#### **A\_22409 -Anbieter ePA-Aktensystem - CA-Anbieterwechsel**

Der Anbieter des ePA-Aktensystems MUSS mindestens drei Monate vor dem Wechsel des CA-Anbieters für die Ausstellung der TLS-Zertifikate des Access Gateways die gematik darüber informieren, wer der alte Anbieter war und wer der neue Anbieter wird. [≤]

#### **A\_19118-01 -Komponenten des Aktensystems, Schutz vor XSW-Angriffen**

Die Komponenten des ePA-Aktensystems, die XML-Signaturen prüfen, MÜSSEN geeignete Maßnahmen gegen XSW-Angriffe umsetzen. Mindestens MÜSSEN sie die FastXPath-Auswertung der XML-Daten und XML-Signaturen gemäß [GJLS-2009] (vgl. auch [BSI-XSpRES]) umsetzen. [≤]

#### **A\_24783 -ePA-Aktensystem - Eingabevalidierung von Operationen**

Das ePA-Aktensystem MUSS alle Operationsaufrufe seiner Schnittstellen (Requests) sowie die Antwortmeldung auf seine Anfragen (Responses) auf Wohlgeformtheit und Zulässigkeit prüfen und bei Encoding-, Schema-, Semantik- oder Protokollverletzungen die Operation abbrechen. [≤]

*Hinweis: Eine Orientierung für die Validierung ist in [OWASP ASVS] Kapitel 5, Validation, Sanitization and Encoding beschrieben.*

#### **A\_24992 -ePA-Aktensystem - Zugriffe durch Versicherte übers Access Gateway**

Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session für einen Versicherten (NutzerID ist KVNR) ausschließlich über das Access Gateway erreichbar ist. [≤]

#### **A\_24993 -ePA-Aktensystem - Zugriffe übers Access Gateway ausschließlich für Versicherte**

Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session für einen Nutzer, dessen NutzerID keine KVNR ist (z.B. Leistungserbringerinstitutionen) nicht über das Access Gateway erreichbar ist. [≤]

#### **A\_25006 -ePA-Aktensystem - User Session bei Inaktivität Beenden**

Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session nach 20 Minuten Inaktivität beendet wird. [≤]

#### **A\_25022 -ePA-Aktensystem - Debug-Protokoll für Testbetrieb**

Das ePA-Aktensystem KANN im Testbetrieb ein Debug-Protokoll schreiben, welches eine erweiterte Protokollierung für Testzwecke ermöglicht. [≤]

*Hinweis: Die Anforderung beschränkt den Debug-Modus auf Testzwecke. Im Produktivbetrieb ist der Debug-Modus nicht zulässig.*

#### **A\_25023 -ePA-Aktensystem - Keine Echtdaten im Testbetrieb**

Das ePA-Aktensystem MUSS sicherstellen, dass im Testbetrieb keine Echtdaten verarbeitet werden. [≤]

#### **A\_25042 -ePA-Aktensystem - Prüfung von Signaturen**

Das ePA-Aktensystem MUSS bei der Prüfung von Signaturen

- das Signaturzertifikat gemäß A\_25040-\* prüfen,
- die Signatur prüfen (i. S. v. Verify()-Funktion des kryptographischen Signaturverfahrens ergibt "valid")

[≤]

#### **A\_25040-01 -ePA-Aktensystem - Prüfung Signaturzertifikate**

Das ePA-Aktensystem MUSS Signaturzertifikate gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit folgenden Parametern auf Gültigkeit prüfen:

**Tabelle 1: Tab\_Prüfung\_Signaturzertifikate Parameter Prüfung Signaturzertifikat**

Parameter	C.FD.SIG	C.CH.SIG	C.HCI.SIG	C.HCI.AUT
PolicyList	oid_fd_sig	oid_egk_sig	oid_smc_b_osig	oid_smc_b_auth
intendedKeyUsage	digitalSignature	nonRepudiation	nonRepudiation	digitalSignature
intendedExtendedKeyUsage	(leer)	(leer)	(leer)	id-kp-clientAuth
OCSP-Graceperiod	24 Stunden	24 Stunden	24 Stunden	24 Stunden
Offline-Modus	nein	nein	nein	nein
Prüfmodus	OCSP	OCSP	OCSP	OCSP

Das ePA-Aktensystem MUSS sicherstellen, dass die Prüfung des Signaturzertifikats nur erfolgreich ist, falls das Signaturzertifikat anhand der Zertifikatsprüfung für [Zertifikatsignatur "valid" UND zeitlich gültig UND online gültig ] befunden wird.

[≤]

#### **A\_27498 -Anbieter ePA-Aktensystem - Offline-Datensicherung**

Der Anbieter des ePA-Aktensystems MUSS Offline-Datensicherungen für die Aktenkonten umsetzen. [≤]

#### **A\_27497 -Anbieter ePA-Aktensystem - Rollenkonzept zum Schutz der permanenten Verfügbarkeit von Aktenkonten**

Der Anbieter des ePA-Aktensystems MUSS durch ein Rollenkonzept sicherstellen, dass ein einzelner Mitarbeiter die Verfügbarkeit der Akten nicht permanent zerstören kann, z.B. durch endgültiges Löschen von Masterkeys oder von Chiffren der Daten der Aktenkonten. Organisatorische Maßnahmen wie Dienstanweisungen sind alleine nicht ausreichend, um eine Rollentrennung zu etablieren.

[≤]



#### **A\_27499 -Anbieter ePA-Aktensystem - HSM-Backups im 4-Augen-Prinzip**

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die Erstellung der Backups der Masterkeys aus dem HSM sowie der Zugriff auf die HSM-Backups ausschließlich im 4-Augen-Prinzip erfolgen kann. [≤]

#### **A\_27500 -Anbieter ePA-Aktensystem - Rollentrennung Administratoren für Backup- und Produktionsdaten**

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass es eine Rollentrennung zwischen Backup-Administratoren und Administratoren der Produktivumgebung gibt. [≤]

## **2.4 Validierungsaktenkonto**

Die Architektur des ePA-Aktensystems verhindert eine Einsichtnahme des Betreibers in Daten von Versicherten. Ebenso ist ein Monitoring der Verfügbarkeit einzelner Schnittstellen und Operationen erschwert. Mit der Anlage eines Validierungsaktenkontos (auf Basis einer Validierungsidentität gem. gemSysL\_PK\_eGK) im ePA-Aktensystem kann die korrekte Funktionsweise in der Produktivumgebung validiert und überwacht werden. Ein Validierungsaktenkonto verhält sich dabei wie ein Konto eines echten Versicherten. Eine Validierungsidentität ist eine Identität mit Versichertenrolle, deren KVNR sich aufgrund ihrer festgelegten Bildungsvorschrift technisch von der eines echten Versicherten unterscheiden lässt. Die Bildungsvorschrift zur Erzeugung von KVNRn für Validierungskonten weicht dahingehend vom Standard ab, dass hier 4 (oder mehr) aufeinanderfolgende, gleiche Ziffern verwendet werden. Dadurch ist eine Überschneidung mit der Menge der "Echt"-KVNRn ausgeschlossen. Die Zuteilung von KVNR-Nummernkreisen, bzw. die Ausgabe einer KVNR in Form einer Prüfkarte, erfolgt durch die gematik.

Validierungsaktenkonten stehen der gematik, den Aktensystembetreibern selbst und Dritten (z. B. DVOs, Primärsystemhersteller ...) zur Verfügung. Für Dritte übernimmt die gematik die Anforderung der Validierungsaktenkonten bei den Aktensystembetreibern und vertreibt diese zusammen mit den dazugehörigen Prüfkarten. Für Validierungsaktenkonten von Dritten kann der Aktensystembetreiber nur eingeschränkten Support in Form von "Akte anlegen", "Akte zurücksetzen" und "Akte löschen" leisten. Über die Einschränkung sind die Nutzer durch die gematik zu informieren.

Folgende Anwendungsfälle sollen mit den Validierungsaktenkonten adressiert werden:

- Monitoring der Aktensystemfunktionalität
- Troubleshooting bei Störungsmeldungen (über FdV oder Primärsystem)
- Validierung der Konfiguration in der LEU
- Store-Review seitens der App-Store-Betreiber (über FdV)
- Validierung der EU-Anbindung

Die mittels der Validierungskonten in der Produktivumgebung realisierten Anwendungsfälle müssen sich möglichst auf die genannten, unbedingt jedoch auf spezifizierte Anwendungsfälle beschränken.

#### **A\_18168-01 -Anbieter des ePA-Aktensystem - Validierungsaktenkonto für gematik**

Nach Aufforderung durch die gematik MUSS der Anbieter des ePA-Aktensystems

- für die gematik ein Validierungsaktenkonto im ePA-Aktensystem für die von der gematik übergebene KVNR anlegen, wobei die KVNR die Festlegungen für die Versichertennummer [gem. gemSysL\_PK\_eGK] erfüllen muss.

- das durch die gematik angegebene Validierungsaktenkonto löschen, sofern die gematik dessen Anlage beantragt hatte.

[<=]

#### **A\_18169-02 -Anbieter des ePA-Aktensystem - Validierungsaktenkonto für eigene Zwecke**

Falls sich der Anbieter des ePA-Aktensystems ein Validierungsaktenkonto für eigene Zwecke anlegen möchte, MUSS er sicherstellen, dass nur eine Versichertennummer aus dem von der gematik für diesen Anbieter freigegebenen Nummernkreis [gem. gemSysL\_PK\_eGK] verwendet wird.

[<=]

#### **A\_22522-01 -Anbieter des ePA-Aktensystems - Validierungskonto für Dritte**

Der Anbieter des ePA-Aktensystems MUSS auf Antrag der gematik

- Validierungsaktenkonten für Dritte (z.B. DVO, PS-Hersteller) für eine vom Antragsteller übermittelte KVNR anlegen, sofern die KVNR die Festlegungen für die Versichertennummer [gem. gemSysL\_PK\_eGK] erfüllt ist.
- das durch einen Antragsteller angegebene Validierungsaktenkonto löschen, sofern der Antragsteller dessen Anlage beantragt hatte.

[<=]

Hinweis zu A\_22522-\*: Die Einrichtung der Validierungsaktenkonten für Dritte kann gegen Bezahlung erfolgen. Die Entscheidung *dafür obliegt dem Anbieter des ePA-Aktensystems*.

Im Design der ePA für alle wird die Initialisierung und Aktivierung durch den Kostenträger vorgenommen. Da es diese Rolle bei Validierungsaktenkonten nicht gibt, sind für diese speziellen Aktenkonten die folgenden Besonderheiten zu berücksichtigen:

#### **A\_26187 -Anlage von Validierungsaktenkonten**

Das ePA-Aktensystem MUSS die Anlage von Validierungsaktenkonten auch ohne KTR- und Ombudsstellen-Befugnisse zulassen.[<=]

#### **A\_26188 -Anbieter des ePA-Aktensystems -Aktivierung von Validierungsaktenkonten**

Der Anbieter des ePA-Aktensystems MUSS den Status von Validierungsaktenkonten, welche für die gematik (gem. A\_18168-\*) oder für Dritte (gem. A\_22522-\*) angelegt wurden, nach der Anlage auf ACTIVATED setzen.[<=]

Falls ein Antragsteller keine Löschung eines Validierungsaktenkontos beim Anbieter des ePA-Aktensystems beantragt, wird das Validierungsaktenkonto nach einer Lebensdauer von maximal 5 Jahren automatisch durch den Anbieter des ePA-Aktensystems gelöscht (ggf. früher aber nicht vor Ablauf der Gültigkeit der Prüf-eGK). Dies verhindert das Auftreten ungenutzter Validierungsaktenkonten im Aktensystem. Die maximale Lebensdauer eines Validierungsaktenkontos ist dabei an die maximale Gültigkeit der Zertifikate der Validierungsidentität gekoppelt, die maximal fünf Jahre betragen kann.

#### **A\_22524-01 -Anbieter des ePA-Aktensystems - Löschen von Validierungsaktenkonten nach 5 Jahren**

Der Anbieter des ePA-Aktensystems MUSS ein Validierungsaktenkonto spätestens fünf Jahre nach Anlage des Validierungsaktenkontos, frühestens jedoch nach Ablauf der Gültigkeit der dazugehörigen Prüf-eGK, löschen.[<=]

#### **A\_22684-01 -Validierungsaktenkonten im Store-Review der FdVs**

Der Anbieter/Hersteller des ePA-Aktensystems bzw. Hersteller des ePA-FdVs KANN - ausschließlich für dedizierte KVNRn von Validierungsaktenkonten zum Zwecke der Verwendung im Store-Review der FdVs - Vorkehrungen treffen, die es ermöglichen auf Gerätebindung, E-Mail-Validierung oder andere Aktivitäten des Registrierungs-/Anmeldeprozesses zu verzichten, um eine Prüfung der FdVs durch die App-Store-Betreiber zu ermöglichen. [<=]



### **A\_22942 -Besonderheiten bei Validierungsaktenkonten für StoreReviews**

Bei Validierungsaktenkonten, für die die Regelung gem. A\_22684-\* gilt [Validierungsaktenkonten im StoreReview der FdVs], MÜSSEN folgende Besonderheiten berücksichtigt werden:

- die entsprechenden Validierungsaktenkonten dürfen nur für den Zeitpunkt des Reviews aktiviert und erreichbar sein,
- die entsprechenden Validierungsaktenkonten sind unmittelbar nach dem Review zu leeren,
- es sind Zeitraum der Erreichbarkeit und eine eindeutige Referenz auf den Review (z.B. Vorgangsnummer) zu dokumentieren und auf Anforderung an die gematik zu übertragen

[<=]

### **A\_26209 -Prüfung auf Vertretungsberechtigung für Prüffidentität**

Das ePA-Aktensystem MUSS sicherstellen, dass bei der Vertreterbefugnis ausschließlich "echte" Vertreter für "echte" Konten befugt, bzw. auf Validierungsaktenkonten ausschließlich "Validierungs-Vertreter" eingerichtet werden können.[<=]

### **A\_24539 -Nutzung von Validierungsaktenkonten via FdV**

Der Anbieter des ePA-Aktensystems bzw. Hersteller des ePA-FdVs MUSS ein FdV bereitstellen, mit dem der Zugriff auf Validierungsaktenkonten möglich ist.[<=]

Die Bereitstellung dieser FdVs muss nicht unentgeltlich erfolgen, wenngleich eine Integration dieser Eigenschaft (Kompatibilität mit Validierungsaktenkonten) in das Standard-FdV anzustreben ist.

## **2.5 Tracing in Nichtproduktivumgebungen**

Ein gewonnener Erfahrungswert ist, dass es für die Fehlersuche in Nichtproduktivumgebungen -- insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase -- leistungsfähigere Mechanismen als zuvor geben muss. Gab es zunächst nur die Testschnittstelle ([gemKPT\_Test#A\_21193-\*]) in den ePA-Clients, so wurde mit ePA 2.0 ein Tracing im Aktensystem für Nichtproduktivumgebungen eingeführt und wird mit ePA für alle wie folgt umgesetzt:

1. Innerhalb des AS werden an die für die Fehlersuche in Nichtproduktivumgebungen wichtigen Stellen Sensoren platziert. Diese Sensoren streamen die aktuell transportierten Daten an bestimmte TCP-Ports am Access Gateway. Die Sensorpunkte liegen im AS immer hinter der TLS-Entschlüsselung. Fehlersuchende können sich zu diesen TCP-Ports am Access Gateway verbinden und lesen dann im Read-Only-Modus den aktuellen Datenverkehr, der an den Sensorpunkten vorbeifließt, mit.
2. ePA-Clients müssen in Nichtproduktivumgebungen beim VAU-Protokoll die symmetrischen Verbindungsschlüssel offenlegen [gemSpec\_Krypt#A\_24477-\*].

Damit wird es möglich, für die Fehlersuche in Nichtproduktivumgebungen den Datenverkehr zwischen einem ePA-Client und der VAU-Instanz im Aktensystem mitzulesen. Für ePA für alle konzentriert sich das Tracing auf genau diese Verbindungsstrecke, andere Sensorpunkte vor Services außerhalb der VAU sind optional.

Ein Aktensystem besitzt mehrere HTTPS-Schnittstellen, über die ein ePA-Client auf das Aktensystem zugreift. Die TLS-Sicherung endet vor den VAU-Instanzen. In den VAU-Instanzen möchte man die Trusted Computing Base (TCB) minimieren und setzt dort das VAU-Protokoll als extrem reduziertes TLS-Analogon ein. Der geforderte Sensorpunkt muss hinter der TLS-Terminierung und vor der VAU Instanz liegen.

**A\_21887-01 -Tracing, Sensorpunkt nahe vor den VAU-Instanzen (Nichtproduktivumgebungen)**

Ein ePA-Aktensystem MUSS sicherstellen, dass genau in Nichtproduktivumgebungen der Datenverkehr zur und von den VAU-Instanzen auf TCP-Ebene mitgeschnitten wird (Sensorpunkt). Der aktuell mitgeschnittene Datenverkehr MUSS auf einen TCP-Port im Access Gateway gestreamt werden (siehe A\_21890-\*). D. h. wenn ein Client sich zu diesem TCP-Port verbindet, MUSS er die aktuell auf dem Interface durchlaufenden Daten gestreamt lesen können.

[<=]

**A\_21891-01 -Tracing, Tiger-Standalone-Proxy**

Ein ePA-Aktensystem MUSS zum Mitschneiden und Streamen der Testdaten in Nichtproduktivumgebungen nach A\_21887-\* den von der gematik bereitgestellten aggregierenden Tiger-Standalone-Proxy (mindestens der Version 0.20) verwenden.[<=]

**A\_22581 -Tracing, Abschaltbarkeit**

Ein ePA-Aktensystem MUSS den Tiger-Standalone-Proxy (und die damit verbundenen Sensorpunkte) gemäß A\_21891-\* im Rahmen der Zulassungstests auf Wunsch der gematik aktivieren und insbesondere deaktivieren können.[<=]

*Hinweis: Die Aktivier- bzw. Deaktivierbarkeit nach A\_22581-\* kann dabei auch teilweise mit organisatorische Maßnahmen umgesetzt werden, d. h. es ist hier **kein** vollautomatisierter Mechanismus notwendig, der im Millisekunden-Bereich umschalten kann.*

## 2.6 Benutzerführung

Bietet der Anbieter des ePA-Aktensystems dem Versicherten die Aktenkontoeröffnung, die Änderung von Vertragsdaten und die Aktenkontoschließung auf einem elektronischen Weg an, dann muss die Bedienung für den Nutzer intuitiv gestaltet werden.

**A\_15842 -Anbieter ePA-Aktensystem - Ergonomie der Benutzerführung**

Der Anbieter des ePA-Aktensystems MUSS eine ergonomisch gestaltete Benutzerführung nach den Vorgaben zur Ergonomie in [DIN EN ISO 9241-171] anbieten.[<=]

**DIN-Normen und Verordnungen zur Beachtung:**

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.

Insbesondere soll der Fokus auf die nachfolgend aufgeführten Teile der ISO 9241 gerichtet sein:

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

- 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

## **BITV 2.0 - Barrierefreie Informationstechnik-Verordnung**

Die Umsetzung der Verordnung dient zur behindertengerechten Umsetzung von Webseiten und anderen grafischen Oberflächen.

Insbesondere sollen deshalb neben der Übernahme der international anerkannten Standards für barrierefreie Webinhalte, die Web Content Accessibility Guidelines (WCAG) 2.1, auch die Belange gehörloser, hör-, lern- und geistig behinderter Menschen berücksichtigt werden.

Die BITV 2.0 regelt unter anderem den sachlichen Geltungsbereich, die einzubeziehenden Gruppen behinderter Menschen und die anzuwendenden Standards.

Weitere Richtlinien und Empfehlungen zur digitalen Barrierefreiheit sind die EU-Richtlinie 2016/2102 für öffentliche Stellen und die europäische Norm EN 301 549 V2.1.2 mit dem Titel "Accessibility requirements for ICT products and services".

## **A\_15846 -Anbieter ePA-Aktensystem - Schnittstellen für die Unterstützung der barrierefreien Bedienungsmöglichkeit**

Der Anbieter des ePA-Aktensystems SOLL die Schnittstellen für die Unterstützung der barrierefreien Bedienungsmöglichkeit, welche vom Betriebssystem zur Verfügung gestellt werden, unterstützen.[<=]

## **2.7 Useragent**

### **A\_22470-06 -Definition x-useragent**

Das Produkt MUSS für das x-useragent-Element in Eingangs- oder Ausgangsparametern einer Operation folgende Formatvorgaben berücksichtigen:

- der Useragent umfasst 2 Informationen, welche als 1 String - getrennt durch "/" (Slash) - im Header übertragen werden
  - erster Teil: Client-ID = ein bis zu 20 Zeichen langer String (a-z A-Z 0-9, "-"), welcher im Rahmen der Produktregistrierung bei der gematik erzeugt wird,
  - zweiter Teil: Versionsnummer = bis zu 15 Zeichen langer String (a-z A-Z 0-9, "-"), ".") welcher die aktuelle Produktversion des Clients repräsentiert.

Beispiel: "CLIENTID1234567890AB/2.1.12-45"

Hinweis: gem. RFC7231 ist im http-Header ein Useragent einzutragen. Dieser RFC-Useragent enthält z.B. Angaben zum Betriebssystem oder zum Browser und ist nicht zu verwechseln mit dem hier definierten x-useragent. Dieser (x-useragent) muss deshalb im x-useragent-Parameter des http-Headers eingetragen werden, NICHT im Useragent-Parameter gem. RFC7231. Ein Beispiel für die Verwendung bieten die OpenAPI-Spezifikationen der fachlichen Aktensystem-Operationen.[<=]

*Hinweis zum Erhalt der Client-ID: die Client-ID wird durch die gematik vergeben und übermittelt, sobald sich ein (Client-)Produkthersteller (z.B. FdV oder Primärsystem) unter idp-registrierung@gematik.de registriert hat. Dazu ist im Rahmen dieser Registrierung der Name des Herstellers und der Name des zu registrierenden Produktes zu übermitteln. Sollte im Rahmen einer anderen TI-Anwendung bereits eine Registrierung vorgenommen worden sein, kann die Client-ID auch im ePA-Kontext genutzt werden (sofern es sich um das gleiche Softwareprodukt handelt).*

*Hinweis für FdV-Hersteller: Bei Entwicklung eines White-Label-Clients ist der Useragent Teil des kundenspezifischen Customizings, sodass über die Client-ID im Useragent das spezifische Kostenträger-ePA-FdV erkennbar sein muss.*

## 2.8 Performance aus Anwendersicht

Im Gegensatz zu den Performancevorgaben, welche in [gemSpec\_Perf] gemacht werden und welche lediglich die Aktivitäten im Aktensystem berücksichtigen, stellt sich die Leistungsfähigkeit und Nutzbarkeit in der Wahrnehmung der Clients oftmals anders dar. Aus diesem Grund werden die Endgeräte (Primärsystem und FdV) für definierte Anwendungsfälle (sogenannte UX-Usecases) dazu verpflichtet, eigene Messungen durchzuführen und diese Messwerte an eine definierte Schnittstelle im Aktensystem zu übermitteln. Das Aktensystem verarbeitet diese Informationen und leitet das konsolidierte Ergebnis im Rahmen der Betriebsdatenlieferung weiter an die gematik. Auf diese Weise erhalten sowohl die gematik (im Rahmen der Gesamt-Produktverantwortung) als auch die Anbieter der Aktensysteme Informationen darüber, wie die Anwendung ePA bei den Nutzern (insb. in der LEU und bei Versicherten) hinsichtlich bestimmter Kernfunktionalitäten wahrgenommen wird.

Die Anwendungsfälle umfassen dabei unter anderem das Login und das Hoch- bzw. Herunterladen von Dokumenten / Daten. Eine spezifische Beschreibung ist in der Spezifikation des FdVs bzw. im Implementierungsleitfaden für Primärsysteme zu finden.

Die Übermittlung der Messdaten erfolgt im Anschluss an den erfolgreichen Abschluss des Anwendungsfalles an das gleiche Aktensystem (unter Verwendung der Schnittstelle `InformationService.setUserExperienceResult`), bei dem auch der Anwendungsfall stattgefunden hat. Hierbei ist die Schnittstelle zur Lieferung der Messdaten an der Komponente "Information Service" nur für Primärsysteme normiert. Es steht dem Hersteller des Aktensystems frei, die Lieferschnittstelle für Messdaten von FdVs selbst oder nach dem Vorbild der PS-Schnittstelle zu implementieren.

Die eingegangenen Messergebnisse werden vom Aktensystem verarbeitet und anschließend gemäß der Vorgaben aus [gemSpec\_Perf] an die Betriebsdatenerfassung der gematik im Rahmen der Rohdatenlieferung übermittelt.

### **A\_24570-01 -Verarbeitung von UX-Messdaten**

Das ePA-Aktensystem MUSS für die im zu betrachtenden Zeitintervall der Betriebsdatenlieferung (gemäß [gemSpec\_Perf]) eingegangenen Messdaten je UX-Usecase, je Client-ID und je Client-Version folgende Werte ermitteln und gemäß [gemSpec\_Perf] übermitteln:

- Durchschnittswert der Messergebnisse
- Anzahl der berücksichtigten Messergebnisse
- Maximalwert
- Minimalwert[<=]

Die Versionsnummer des Useragents wird bei der Konsolidierung nicht weiter verarbeitet und dient dem Anbieter des ePA-Aktensystems zur Identifikation von möglichen Fehlerquellen im Rahmen des Eigenmonitorings und Troubleshootings.

---

## 3 Funktionsmerkmale

---

### 3.1 Aktenkonto eines Versicherten (Health Record)

Ein ePA-Aktenkonto wird durch den Kostenträger eines Versicherten als Anbieter der ePA für jeden Versicherten angelegt und für die Nutzung im Rahmen der gesetzlichen Vorgaben zur Verfügung gestellt. Die Anlage eines Aktenkontos erfordert keine Beantragung durch den Versicherten, dieser kann einer Anlage seines Aktenkontos jedoch widersprechen.

#### 3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte

Der Widerspruch des Versicherten gegen die grundsätzliche Nutzung der ePA kann jederzeit erfolgen. Wird dieser im Vorfeld der Anlage eines Aktenkontos erklärt, wird kein Aktenkonto für diesen Versicherten erzeugt. Existiert zum Zeitpunkt des Widerspruchs schon ein Aktenkonto (in einem beliebigen Zustand), so wird dieses gelöscht und alle enthaltenen Daten werden gelöscht.

Die Regelungen zum Widerspruch oder die Rücknahme des Widerspruchs gegen die grundsätzliche Nutzung der ePA sind durch den Anbieter der ePA eigenständig im Rahmen der gesetzlichen Vorgaben umzusetzen und sind nicht Bestandteil dieser Spezifikation.

Für die vereinfachte Prüfung auf einen bereits erteilten Widerspruch des Versicherten bei einem Wechsel des Kostenträgers muss die Information zu einem Widerspruch jedoch vermerkt und über die Schnittstelle `I_Information_Service_Account` [`I_Information_Service_Account`] abrufbar sein.

#### **A\_23886 -Anbieter ePA-Aktensystem - Keine Aktenkontoanlage bei Widerspruch des Versicherten**

Der Anbieter des ePA-Aktensystems DARF ein Aktenkonto für den Versicherten NICHT anlegen, wenn ein Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte vorliegt.[<=]

Der Widerspruch gegen die grundsätzliche Nutzung der ePA kann durch den Versicherten jederzeit zurückgenommen werden. In diesem Fall wird wie bei der Anlage eines neuen Aktenkontos für den Versicherten verfahren.

#### **A\_25181 -Anbieter ePA-Aktensystem - Aktenkontoanlage bei Zurücknahme des Widerspruchs des Versicherten**

Falls ein Versicherter den Widerspruch gegen die grundsätzliche Nutzung der ePA zurücknimmt MUSS der Anbieter des ePA-Aktensystems ein Aktenkonto für den Versicherten unverzüglich anlegen.[<=]

#### 3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger

Die Regelungen zum Widerspruch oder die Rücknahme des Widerspruchs gegen das Einstellen von Abrechnungsdaten des Kostenträgers in die ePA sind durch den Anbieter der ePA eigenständig im Rahmen der gesetzlichen Vorgaben umzusetzen und sind nicht Bestandteil dieser Spezifikation.

### 3.1.2 Lebenszyklus und Zustände eines Aktenkontos

Ein Aktenkonto durchläuft in seinem Lebenszyklus diverse Zustände. Einige dieser Zustände sind für rein administrative Vorgänge vorgesehen (Initialisierung, Umzug des Aktenkontos zu einem anderen Anbieter), andere für die Nutzung der Akte im Versorgungsprozess. Diese Nutzung für Versorgungsprozesse ist dabei auf den Zustand "Activated" eingeschränkt.

Eine Übersicht der unterschiedlichen Status und der Bedingungen für den Statusübergang sind in der folgenden Tabelle dargestellt.

**Tabelle 2: Zustandswechsel im Lebenszyklus eines Aktenkontos**

Zustand	Erläuterung	zulässige Transitionen	Folgezustand
UNKNOWN	Für einen Versicherten existiert kein Aktenkonto.	Konto initialisieren	Initialized
INITIALIZED	Ein neues Aktenkonto ist konfiguriert und für eine Aktivierung vorbereitet. Die initialen Befugnisse sind erstellt. Eine Nutzung des Aktenkontos im Versorgungsprozess und die Nutzung medizinischer Dokumente ist jedoch erst nach der Aktivierung möglich. Die Daten eines existierenden Aktenkontos werden importiert.	Widerspruch gegen die Nutzung der ePA	Unknown
		Explizite Aktivierung des Kontos durch den Anbieter. Bei existierendem Aktenkonto bei einem anderen Anbieter erfolgt die Aktivierung erst nach einem Import der Daten des Aktenkontos.	Activated
ACTIVATED	Das Aktenkonto ist aktiv und kann von befugten Nutzern und Nutzergruppen im Versorgungsprozess verwendet werden.	Vorbereitung des Umzugs des Aktenkontos zu einem anderen Anbieter (Erstellung des Exportpakets)	Suspended
		Widerspruch gegen die Nutzung der ePA	Unknown
SUSPENDED	Die Daten des Aktenkontos des Versicherten werden zu einem neuen Anbieter übertragen. Die Nutzung des Aktenkontos ist in	Erfolgreicher Abschluss des Umzugs Widerspruch gegen die Nutzung der ePA	Unknown
		Der Bereitstellungszeitraum	Activated



	diesem Zustand nicht möglich.	des Exportpakets ist abgelaufen.	
--	-------------------------------	----------------------------------	--

Die Anforderungen in den folgenden Kapiteln legen die zulässigen Zustandswechsel eines Kontos fest.

### 3.1.3 Anlage eines neuen Aktenkontos

Ein neues Aktenkonto wird für einen Versicherten bei seinem Anbieter automatisch angelegt, wenn der Versicherte der grundsätzlichen Nutzung der ePA nicht widerspricht oder einen zuvor gegebenen Widerspruch zurücknimmt und bei einem anderen Anbieter kein Aktenkonto für den Versicherten existiert.

Die Anlage eines neuen Aktenkontos erfolgt in zwei Stufen: der Initialisierung und der darauffolgenden Aktivierung.

Bei der Initialisierung wird ein neues Aktenkonto bei einem Betreiber eines ePA-Aktensystems für den Versicherten angelegt und die Dienste des Aktenkontos für die Nutzung vorbereitet. Die Identifikation eines Aktenkontos erfolgt dabei über die KVNR des Versicherten (unveränderlicher Anteil der Versichertennummer) im Aktensystem und gegenüber Clients bei Nutzung der ePA.

#### **A\_24336 -Anbieter ePA-Aktensystem - Identifizierung eines Aktenkontos**

Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos die KVNR des Versicherten zur Identifikation des Aktenkontos im Aktensystem verwenden und sicherstellen, dass diese Identifikation eines Aktenkontos nicht verändert werden kann.【<=】

#### **A\_23775 -Anbieter ePA-Aktensystem - Neues Aktenkonto anlegen**

Der Anbieter des ePA-Aktensystems MUSS für Versicherte jeweils ein Aktenkonto anlegen, wenn kein Widerspruch des Versicherten gegen die Nutzung der ePA vorliegt, und dabei die KVNR des Versicherten zur Identifikation eines Aktenkontos im Aktenkonto registrieren. Das initialisierte Aktenkonto MUSS den Status INITIALIZED erhalten.【<=】

Wechselt der Versicherte den Anbieter, so kann ein Widerspruch des Versicherten gegen die Nutzung der ePA auch bei diesem bisherigen schon vorliegen. In diesem Fall kann die Anlage eines Aktenkontos bei einem neuen Anbieter entfallen. Andernfalls kann bei dem bisherigen Anbieter ein Aktenkonto existieren, dessen Daten im Rahmen der Anlage eines Aktenkontos beim neuen Anbieter importiert werden müssen.

#### **A\_27343 -Anbieter ePA-Aktensystem - verpflichtende Prüfung auf Widerspruch gegen die Nutzung der ePA bei einem anderen Anbieter**

Der Anbieter des ePA-Aktensystems MUSS vor der Anlage eines Aktenkontos durch Verwendung der Operationen der Schnittstelle gemäß [I\_Information\_Service\_Accounts] prüfen, ob bei einem anderen Anbieter ein Widerspruch des Versicherten gegen die Nutzung der ePA vorliegt oder ein Aktenkonto des Versicherten existiert.【<=】

#### **A\_24789 -Anbieter ePA-Aktensystem - verpflichtender Import eines existierenden Aktenkontos**

Der Anbieter des ePA-Aktensystems MUSS die Inhalte eines existierenden Aktenkontos in ein neues, initialisiertes Aktenkonto vor dessen Aktivierung übernehmen.【<=】

#### **A\_24302-01 -Anbieter ePA-Aktensystem - verpflichtende Nutzung der Schnittstelle des Information Service Accounts**

Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos einen Import der Inhalte eines existierenden Aktenkontos von einem anderen Anbieter durch Verwendung der Operationen der Schnittstelle gemäß [I\_Information\_Service\_Accounts] veranlassen.【<=】

Der weitere Import eines existierenden Aktenkontos vor dessen Aktivierung erfolgt unter Verwendung des Health Record Relocation Service (3.2- Health Record Relocation Service ).

## **A\_24790-01 -Anbieter ePA-Aktensystem - keine unbegründeter Import eines Aktenkontos**

Der Anbieter des ePA-Aktensystems DARF den Import eines existierenden Aktenkontos von einem anderen Anbieter für Zwecke abweichend der Vorgaben in A\_24302-\* NICHT nutzen oder veranlassen. [≤]

## **A\_15870-02 -Anbieter ePA-Aktensystem - Abbruch bei Nichtverfügbarkeit anderer Anbieter**

Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen, wenn die Prüfung gemäß A\_27343-\* mindestens bei einem anderen Anbieters eines ePA-Aktensystems eine technische Fehlermeldung liefert oder dieser nicht erreichbar ist. [≤]

## **A\_27344 -Anbieter ePA-Aktensystem - Abbruch bei fehlgeschlagenem Import**

Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen, wenn ein Import von Daten eines Aktenkontos von einem bisherigen Anbieter erforderlich ist und dieser nicht erfolgreich abgeschlossen werden kann. [≤]

Hinweis zu A\_23744\*: Ein Import kann beispielsweise fehlschlagen, wenn schwerwiegende Fehler bei der Exportpaketerstellung oder bei der Übertragung auftreten (siehe 3.2- Health Record Relocation Service ).

Für die Geräteregistrierung bei Nutzung eines ePA-FdV durch den Versicherten ist eine E-Mail-Adresse des Versicherten für Bestätigung der Geräteregistrierung erforderlich. Falls vorhanden, kann diese E-Mail-Adresse bei der Anlage eines Aktenkontos im Device Management hinterlegt werden. Ansonsten muss eine E-Mail-Adresse bei der ersten Einrichtung eines ePA-FdV zur Nutzung des Aktenkontos hinterlegt werden. Eine E-Mail-Adresse muss vor der Übernahme in das Aktensystem validiert sein, beispielsweise durch Versand eines Bestätigungslink an diese E-Mail-Adresse.

## **A\_14996-01 -Anbieter ePA-Aktensystem - Manuelle Ergänzung E-Mail-Adresse**

Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten auf geeignetem Weg ermöglichen, die Registrierung einer E-Mail-Adresse für die Geräteverwaltung auch nachträglich vorzunehmen. [≤]

## **A\_14993-02 -Anbieter ePA-Aktensystem - Mailadresse validieren**

Der Anbieter des ePA-Aktensystems MUSS eine Mailadresse

- bei der ersten Hinterlegung im Aktensystem,
- bei einer Änderung der Mailadresse

auf Gültigkeit hin validieren. [≤]

## **A\_24369 -Anbieter ePA-Aktensystem - Initialisierung des Aktenkontos**

Der Anbieter des ePA-Aktensystems MUSS die Initialisierung der Bestandteile

- Consent Decision Management (initiale Entscheidungen)
- Constraint Management (Policies)
- Entitlement Management (initiale Befugnisse und Befugnisausschlüsse)
- Information Service (initiale Entscheidungen "Versorgungsprozess")
- XDS Document Service (statische Aktenkontoinhalte)
- Device Management
- Authorization Service
- Audit Event Service



- Medication Service

vor der Aktivierung eines Aktenkontos durchführen. Die genannten Bestandteile MÜSSEN nach der Aktivierung des Aktenkontos sofort nutzbar sein.【<=】

Im Zustand INITIALIZED obliegt es dem Anbieter, ein Aktenkonto mittels administrativer Eingriffe in die verschiedenen Bestandteile des Aktensystems und -kontos auf die Aktivierung vorzubereiten bzw. zu konfigurieren.

### **A\_26005 -ePA-Aktensystem - Optionale Schnittstelle zum Einbringen von initialen Befugnissen**

Das ePA-Aktensystem KANN eine Schnittstelle für Kostenträger anbieten, über die Kostenträger die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle ins ePA-Aktensystem einbringen können.【<=】

### **A\_26006 -ePA-Aktensystem - Nutzen der optionalen Schnittstelle zum Einbringen von initialen Befugnissen ausschließlich im Status INITIALIZED**

Falls das ePA-Aktensystem eine Schnittstelle für Kostenträger anbietet, über die Kostenträger die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle für ein Aktenkonto einbringen können, MUSS das ePA-Aktensystem sicherstellen, dass diese Schnittstelle ausschließlich genutzt werden kann, wenn sich das Aktenkonto im Status INITIALIZED befindet.

【<=】

Das Aktenkonto wird nach Abschluss der Initialisierung durch den Anbieter aktiviert und kann dann durch befugte Nutzer und Nutzergruppen verwendet werden. Eine Aktivierung erfolgt für den Rollout der ePA Version 3 im Kontext des ePA Go-Live-Termins und zu späteren, individuellen Zeitpunkten, wenn Versicherte als ePA-Nutzer neu dazu gekommen (bspw. Widerspruch wird zurückgenommen und ePA wird später angelegt oder Versicherte Person kommt erstmalig ins Gesundheitssystem im Falle eines Zuzugs oder eines Neugeborenen).

### **A\_24335 -Anbieter ePA-Aktensystem - Neues Aktenkonto aktivieren**

Der Anbieter des ePA-Aktensystems MUSS ein neues Aktenkonto nach Abschluss der Initialisierung aktivieren (Status ACTIVATED), wenn die gesetzliche Widerspruchsfrist abgelaufen ist.【<=】

## **3.1.4 Löschen eines Aktenkontos**

Die Löschung eines Aktenkontos bei einem Anbieter und aller darin enthaltenen Daten kann in folgenden Situationen erforderlich sein:

- Widerspruch des Versicherten gegen die Nutzung der ePA,
- nach erfolgreichem Wechsel des Anbieters durch den Versicherten und abgeschlossener Datenübernahme aus dem bisherigen Aktenkonto,
- nach Beendigung des Versicherungsverhältnisses des Versicherten bei seinem Kostenträger.

Ein Versicherter kann nach der Anlage eines Aktenkontos der grundsätzlichen Nutzung der ePA widersprechen. Liegt dieser erklärte Widerspruch vor, werden das Aktenkonto des Versicherten und sämtliche Inhalte durch den Anbieter des Aktenkontos gelöscht.

Bei einem Anbieterwechsel erfolgt die Übernahme der Daten des bisherigen Aktenkontos zu dem neuen Anbieter. Nach erfolgreichem Abschluss der Datenübernahme in das Aktenkonto des neuen Anbieters löscht der bisherige Anbieter das Aktenkonto des Versicherten und alle darin enthaltenen Daten.

Kündigt ein Versicherter das Vertragsverhältnis ohne Übernahme der Daten zu einem neuen Anbieter, löscht der Anbieter des Aktenkontos des Versicherten nach einer

angemessenen Wartezeit, bzw. nach Ablauf von vorgeschriebenen Bereitstellungs- und Aufbewahrungszeiträumen, das Aktenkonto und alle darin enthaltenen Daten.

Vor der Ausführung der endgültigen Löschung des Aktenkontos muss es dem Versicherten ermöglicht werden, die Protokolldaten (auch unter Einbindung der Ombudsstelle) für seinen eigenen Gebrauch außerhalb des Aktenkontos zu sichern. Dieses ist nicht erforderlich, wenn das Aktenkonto in Folge eines erfolgreichen Umzugs zu einem anderen Anbieter geschlossen wird.

#### **A\_25289 -Anbieter ePA-Aktensystem - Löschen des Aktenkontos durch den Kostenträger**

Der Anbieter des ePA-Aktensystems MUSS das Aktenkonto eines Versicherten inklusive aller enthaltenen Daten löschen (sämtliche Dokumente, Schlüsselmaterial, Protokolle, Widerspruchsinformation, Befugnisse und Beschränkungen), wenn dies durch den zuständigen Kostenträger beauftragt wird.【<=】

### **3.2 Health Record Relocation Service**

Transfer eines Aktenkontos zu einem neuen Anbieter (Aktenkontoumzug).

Wechselt der Versicherte den Kostenträger bzw. den Anbieter seines Aktenkontos, so erfolgt der Umzug der Inhalte seines bestehenden Aktenkontos vom bisherigen Anbieter zu einem neuen Anbieter weitestgehend automatisiert.

Seitens der Aktensysteme werden für einen Aktenkontoumzug zwei Schnittstellen angeboten: I\_Health\_Record\_Relocation\_Service zur Nutzung durch die Anbieter (alt und neu) für den Zugriff auf das Aktenkonto des Versicherten und I\_Information\_Service\_Accounts für die Interaktion der Aktensysteme (alt und neu) untereinander. Die notwendige Kommunikation der Kassen-Backends mit ihren Aktensystemen außerhalb der VAU erfolgt dabei in Absprache der Beteiligten und ist nicht Bestandteil der genannten Schnittstellen.

#### **A\_24786 -Health Record Relocation Service - Realisierung der Schnittstelle I\_Health\_Record\_Relocation\_Service**

Der Health Record Relocation Service MUSS die Operationen der Schnittstelle I\_Health\_Record\_Relocation\_Service gemäß [I\_Health\_Record\_Relocation\_Service] umsetzen.【<=】

*Hinweis: Zur Schnittstelle I\_Information\_Service\_Accounts siehe 3.15.2- Information Service - Account ).*

#### **A\_24821 -Health Record Relocation Service - Suspendierung des Aktenkontos**

Der Health Record Relocation Service MUSS sicherstellen, dass das Aktenkonto für die Erstellung eines Exportpakets auf den Status SUSPENDED gesetzt wird.【<=】

#### **A\_24827 -Health Record Relocation Service - Reaktivierung des Aktenkontos**

Der Health Record Relocation Service MUSS sicherstellen, dass ein Aktenkonto im Status SUSPENDED nach einem Abbruch eines Transfers von einem Anbieter zu einem anderen Anbieter aufgrund eines Fehlers (Datenübertrag ist nicht erfolgt) in den Status ACTIVATED gesetzt wird.【<=】

#### **A\_25005-03 -Health Record Relocation Service - Daten des Exportpakets**

Der Health Record Relocation Service MUSS sicherstellen, dass alle Daten des Aktenkontos in das Exportpaket übernommen werden aus:

- XDS Document Service
- Medication Service

- Consent Management
- Constraint Management
- Audit Event Service
- Entitlement Management (außer Befugnisse für Versicherter, E-Rezept-Fachdienst, Kostenträger, Ombudsstelle und NCPeH (EU-Zugriff)).
- E-Mail Management (die E-Mail-Adresse des Aktenkontoinhabers (falls vorhanden) sowie für alle Vertreter die E-Mail-Adressen, sofern sie die dem exportierenden Aktensystem bekannt sind).

Bei FHIR Data Services MUSS der Health Record Relocation Service sicherstellen, dass die jeweilige Resource.id aller FHIR-Instanzen ebenso in das Exportpaket einfließen, sodass nach einem Import die Identitäten der FHIR-Daten stabil bleiben.

[<=]

*Hinweis: Die Geräteregistrierungen des Versicherten oder der Vertreter werden nicht exportiert. Bei einem neuen Anbieter ist für den Versicherten eine erneute Geräteregistrierung erforderlich.*

#### **A\_25605 -Health Record Relocation Service - Erstellung des Exportpakets**

Der Health Record Relocation Service MUSS sicherstellen, dass das Exportpaket gemäß der Vorgaben in [HealthRecordMigration] bezüglich der Struktur, der Formate für die enthaltenen Daten und die Verschlüsselung erfolgt.[<=]

#### **A\_25012 -Health Record Relocation Service - Signatur der Befugnisse**

Der Health Record Relocation Service MUSS sicherstellen, dass die gemäß A\_23734-\* signierten Anteile einer Befugnis mit der Signaturidentität ID.FD.SIG (Rolle oid\_epa\_vau) signiert werden.[<=]

*Hinweis: Der CMAC einer Befugnis wird nicht ins Export-Paket übernommen.*

#### **A\_25719 -Health Record Relocation Service - JWT der Befugnis im Exportpaket**

Der Health Record Relocation Service MUSS sicherstellen, dass die Befugnisse im Exportpaket als gültig signierte JWT mit den dargestellten Inhalten abgelegt sind:

Befugnis	Claim Name	Claim	Beispiel
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.SIG	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	
	"exp"	Verfalldatum, = "iat" + 8Tage"	Mindestens für den gesamten Bereitstellungszeitraum des Exportpakets

	"insurantId"	KVNR des Aktenkontos	A123456789
	"actorId"	Identifizier (Telematik-id oder KVNR)	3-883110000092471
	"validTo"	Ende der Gültigkeit,	gemäß [RFC3339], z.B. 2025-06-30T21:59:59Z oder 2025-06-30T23:59:59+02:00

**[<=]**

Der Wert "ES256" (JWS-Parameters "alg") gilt auch für die Kurve "brainpoolP256r1" (also nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen."

#### **A\_24787-01 -Health Record Relocation Service - Verschlüsselung des Exportpaktes**

Der Health Record Relocation Service MUSS sicherstellen, dass Exportpakete ausschließlich verschlüsselt für den Download zu einem anderen Betreiber zur Verfügung stehen. Für die Verschlüsselung MUSS das kryptographische Material des ENC-Zertifikats verwendet werden, welches mittels der Regel hsm-r7 vom VAU-HSM abgerufen wurde.

**[<=]**

#### **A\_24942 -Health Record Relocation Service - Prüfung Provider ENC Zertifikat**

Der Health Record Relocation Service MUSS das übergebene Provider ENC-Zertifikat mittels TUC\_PKI\_018 (OCSP-Graceperiod=12h, PolicyList= oid\_fd\_enc, professionOID = oid\_epa\_vau ) prüfen und ungültige Zertifikate mit der Fehlermeldung " CERTIFICATE\_INVALID " ablehnen.**[<=]**

#### **A\_21750 -Health Record Relocation Service - Integritätsschutz Exportpaket**

Der Health Record Relocation Service MUSS das erstellte Exportpaket mit einem "Digest" HTTP Response Header (<https://tools.ietf.org/html/rfc5843>) als Integritätsschutz versehen und dabei als Digest Algorithmus SHA-256 verwenden.

Beispiel Digest-Header:

Digest: SHA-

256=MWVkmWQxYTRiMzk5MDQ0MzI3NGU5NDEyZTk5OWY1ZGFmNzgyZTJlODYzYjRjYzFhOTlmNTQwYzI2M2QwM2U2MQ==

**[<=]**

#### **A\_15051 -Health Record Relocation Service - Authentisierung gegenüber einem neuen Aktenanbieter**

Der Health Record Relocation Service, welcher das Exportpaket zur Verfügung stellt, MUSS sich beim Abruf des Exportpakets durch ein anderes ePA-Aktensystem mit der TLS-Identität oid\_epa\_mgmt und Zertifikatsprofil C.FD.TLS-S authentisieren.

**[<=]**

#### **A\_15048 -Health Record Relocation Service - Authentifizierung des neuen Aktenanbieters**

Der Health Record Relocation Service MUSS den Abruf des Exportpakets durch ein anderes ePA-Aktensystem ablehnen, wenn sich der abrufende Client nicht als ePA-Aktensystem in der Rolle oid\_epa\_mgmt in einem TLS-Zertifikat C.FD.TLS-C authentisiert.

**[<=]**

#### **A\_17236 -Health Record Relocation Service - Prüfung der TLS-Zertifikate**

Der Health Record Relocation Service MUSS bei der Authentifizierung eines anderen Aktensystems beim Abruf des Exportpakets die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC\_PKI\_018 durchführen. Zur Prüfung des TLS-Zertifikats C.FD-TLS-S sind

dabei die Parameter PolicyList=oid\_fd\_tls\_s, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-serverAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD-TLS-C sind dabei die Parameter PolicyList=oid\_fd\_tls\_c, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-clientAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden.

[<=]

#### **A\_15703 -Health Record Relocation Service - Verfügbarkeit Export-Paket**

Der Health Record Relocation Service MUSS ein erstelltes Export-Paket für maximal sieben Kalendertage zum Abruf durch einen anderen Anbieter eines ePA-Aktensystems bereithalten.[<=]

#### **A\_21239 -Health Record Relocation Service - Verhalten bei Nichtabholen des Exportpakets**

Der Health Record Relocation Service MUSS nach Ablauf des Bereithaltungszeitraums entsprechend A\_15703\* ein erstelltes Export-Paket löschen und den Status des Aktensystems von SUSPENDED auf ACTIVATED zurücksetzen.[<=]

*Hinweis: siehe dazu auch 3.2.1.7.3- Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter*

#### **A\_14905-04 -Health Record Relocation Service - Import des Exportpakets des vorhergehenden Aktenkontos**

Der Health Record Relocation Service MUSS das vom vorhergehenden Anbieter ePA-Aktensystem des Versicherten bezogene Exportpaket, in das neue Aktenkonto importieren und dazu:

- das Exportpaket mittels des privaten ENC-VAU-Schlüssels des neuen Betreibers entschlüsseln,
- den Digest gemäß A\_21750-\* prüfen,
- die Befugnisse mit Regel "rr5" (siehe Tab\_AS\_Entitlement\_Registration\_Rules im Aktensystem) registrieren und
- falls DocumentEntry.originalURI im Exportpaket vorhanden ist, wird für jedes Dokument eines SubmissionSet der Inhalt von DocumentEntry.URI durch den Inhalt von DocumentEntry.originalURI ersetzt. (Hinweis: DocumentEntry.originalURI darf nicht als eigenständiges Metadatum in die Registry übernommen werden, da es lediglich dem Transport des Originalwertes von DocumentEntry.URI aus dem alten Aktensystem dient.

[<=]

#### **A\_27616 -Health Record Relocation Service - Abbruch des Imports eines Exportpakets**

Der Health Record Relocation Service MUSS den Import eines Exportpakets vollständig abbrechen, wenn einzelne Elemente des Exportpakets aufgrund konstruktiver oder inhaltlicher Fehler nicht erfolgreich importiert werden können. Eventuell schon importierte Elemente desselben Exportpakets MÜSSEN im Falle eines Abbruchs entfernt werden.[<=]

*Hinweis: Das exportierende Aktensystem kann über den Abbruch durch ein Incident packageCorrupt benachrichtigt werden.*

*Hinweis: Eine zum Zeitpunkt des Imports eines Exportpaketes zeitlich nicht mehr gültige Befugnis aus dem Exportpaket ist kein Fehler im Sinne der Anforderung und führt nicht zu einem Abbruch. Das importierende Aktensystem kann eine solche Befugnis ignorieren.*

#### **A\_21548-02 -Health Record Relocation Service - Information der Vertreter über neuen FQDN nach Abschluss des Anbieterwechsels**

Der Health Record Relocation Service MUSS sicherstellen, dass alle Vertreter nach erfolgreichem Import des Exportpakets und somit Abschluss des Anbieterwechsels über Anbieterwechsel und den Bezeichner des neuen Anbieters des Versicherten informiert werden, so dass sie in der Lage sind, die erforderliche initiale Anmeldung durchzuführen und informiert sind, welche Art von personenbezogenen Daten vom Vertreter im Rahmen der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine Vertreterberechtigung widerrufen kann und gegenüber wem er seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann. [≤]

*Hinweis 1 zu A\_21548-\**: Für die Benachrichtigung derjenigen Vertreter, die dem importierenden Aktensystem nicht bekannt sind, werden die E-Mail-Adressen aus dem Exportpaket genommen. Für die Benachrichtigung der Vertreter, die dem importierenden Aktensystem bekannt sind, wird die im importierenden Aktensystem hinterlegte E-Mail-Adresse des Vertreters verwendet.

*Hinweis 2 zu A\_21548-\**: Der Bezeichner des neuen Anbieters muss dem Wert entsprechen der durch die Operation `getProviderList` geliefert wird.

### **A\_26257 -Health Record Relocation Service - Löschen der im Exportpaket enthaltenen E-Mail-Adressen der Vertreter**

Der Health Record Relocation Service MUSS sicherstellen, dass die im Exportpaket enthaltenen E-Mail-Adressen von Vertretern ausschließlich zur Information der Vertreter gemäß A\_21548-\* genutzt werden und nach Abschluss des Anbieterwechsels im importierenden Aktensystem gelöscht werden, d.h. nicht im importierenden Aktensystem gespeichert werden. [≤]

### **A\_24788 -Health Record Relocation Service - Löschen des Exportpakets nach Umzug des Aktenkontos**

Das Aktensystem MUSS sicherstellen, dass ein vorhandenes Exportpaket nach einem erfolgreichen Transfer eines Aktenkontos eines Versicherten von einem Anbieter zu einem anderen Anbieter gelöscht wird. [≤]

### **A\_24982-02 -Health Record Relocation Service - Protokollierung des Anbieterwechsels eines Aktenkontos**

Der Health Record Relocation Service des neuen (importierenden) Aktensystems MUSS nach der erfolgreichen oder einer abgebrochenen Übertragung der Inhalte eines Aktenkontos vom bisherigen Anbieter einen Protokolleintrag gemäß A\_24704\* erzeugen. Dabei ist folgende Wertbelegung zu berücksichtigen:

**Tabelle 3 : Health Record Relocation Service Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"object"		
AuditEvent.action	E		Übertrag von Daten eines Aktenkontos von einem anderen Anbieter
AuditEvent.agent.type	PAYOR		Umzug wurde ausgelöst vom Kostenträger.
AuditEvent.entity.name	"HealthRecordRelocation"		
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	

	"OriginName"	<Name des Kostenträgers>	Name des Kostenträgers, von welchem ein bestehendes Aktenkonto übernommen wird

[&lt;=]

*Hinweis: Das Aktensystem des bisherigen Anbieters muss keinen Protokolleintrag gemäß A\_24982\* erzeugen.*

### 3.2.1 Ablauf eines Aktenkontoumzugs

#### 3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter

Der Anbieter (neu) lässt im Aktensystem (neu) ein neues Aktenkonto anlegen. Dieses erhält den Status INITIALIZED. Hierfür gelten die Anforderungen gemäß 3.1.3- Anlage eines neuen Aktenkontos.

Falls der Versicherte schon einen Widerspruch gegen die Nutzung der ePA bei seinem bisherigen Kostenträger erklärt hat, kann die Initialisierung eines neuen Aktenkontos ggf. entfallen. Ein Transfer, bzw. die Erstellung eines Exportpakets, ist in diesem Fall mangels eines existierenden Aktenkontos beim bisherigen Anbieter nicht erforderlich.

Die Abfrage eines existierenden Widerspruchs des Versicherten bei einem anderen Anbieter ePA-Aktensystem erfolgt über dessen Information Service.

Abfrage eines existierenden Widerspruchs gegen die Nutzung der ePA	
<b>I_Information_Service_Accounts (bisheriges Aktensystem)</b>	
getGeneralConsentDecision	Abfrage des ggf. schon erteilten Widerspruchs gegen die Nutzung der ePA durch den Versicherten

#### 3.2.1.2 Start Transfer eines existierenden Aktenkontos

Hat der Versicherte bei keinem Anbieter einen Widerspruch gegen die Nutzung der ePA erklärt und existiert bei einem bisherigen Anbieter (alt) ein Aktenkonto, wird der Transfer der Daten durch das Aktensystem (neu) initiiert.

Das Aktensystem (alt), bei welchem das Aktenkonto existiert, bestätigt diese Anfrage zum Transfer mit einer Vorgangs-ID.

Starten des Transfers	
<b>I_Information_Service_Accounts (bisheriges Aktensystem)</b>	
startRelocation	initiiieren der Exportpaketerstellung



### 3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen Anbieter

Das Aktensystem (alt) informiert den Anbieter (alt) über die Anfrage zum Transfer und die Vorgangsnummer. Der Anbieter (alt) öffnet das existierende Aktenkonto des Versicherten und stößt in der VAU die Erzeugung des Exportpakets an. Der Health Record Relocation Service beantwortet diese Anfrage durch Rückgabe einer URL für den späteren Download des Exportpakets durch den neuen Anbieter und startet die Erzeugung des Exportpakets. Das Aktenkonto wird vor der Paketerstellung auf den Status SUSPENDED gesetzt, um weitere Aktivitäten seitens der Nutzer zu verhindern.

Erzeugen des Exportpakets	
<b>I_Health_Record_Relocation_Service_ (bisheriger Anbieter)</b>	
startPackageCreation	Starten der Erzeugung des Exportpakets in der VAU

In dieses Exportpaket werden alle Daten des Aktenkontos gemäß A\_25005\* übernommen. Das fertige Exportpaket wird mittels ENC-Zertifikat, welches im VAU-HSM eingebracht und gespeichert wurde, verschlüsselt und am vorbereiteten Downloadpunkt bereitgestellt.

### 3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den neuen Anbieter

Der Anbieter (alt) veranlasst nach Erhalt der Download-URL über das Aktensystem (alt) den Versand der URL an das Aktensystem (neu).

Das Aktensystem (alt) prüft vor der Übermittlung der Download-URL an das Aktensystem (neu), ob das Exportpaket für den Download bereitsteht, ggf. wird auf den Abschluss der Paketerstellung gewartet. Ist dieses der Fall, erfolgt die Benachrichtigung des Information\_Service des Aktensystem (neu) mit der Übergabe der URL

Übergabe der Download-URL für das Exportpaket	
<b>I_Information_Service_Accounts (neues Aktensystem)</b>	
putDownloadUrlForExportPackage	Übergabe der geprüften Download-URL

### 3.2.1.5 Import des Exportpakets durch den neuen Anbieter

Der Information Service des Aktensystems (neu) nimmt die Download-URL entgegen und übermittelt diese an den Kostenträger (neu). Dieser öffnet den Zugang zum Aktenkonto (neu) des Versicherten und veranlasst in der VAU den Import des Exportpakets.

Import und Integration des Exportpakets	
<b>I_Health_Record_Relocation_Service (neuer Anbieter)</b>	
startPackageImport	Starten des Imports der vorhandenen Daten

### 3.2.1.6 Abschluss des Transfers durch beide Anbieter

Das Aktensystem (neu) startet den Download des Exportpakets, entschlüsselt dieses und übernimmt die Daten in das initialisierte Aktenkonto des Versicherten. Nach



erfolgreichem Abschluss wird (kann) das Aktenkonto (neu) in den Status ACTIVATED überführt werden.

Unter Verwendung des Information Service wird das Aktensystem (alt) über den erfolgreichen Import und den Abschluss des Transfers informiert. Das Aktenkonto (alt) kann daraufhin, ggf. unter Einhaltung weiterer Bedingungen des Kostenträgers bzw. gesetzlicher Vorgaben, gelöscht werden (Status = UNKNOWN).

Abschluss des Transfers	
<b>I_Information_Service_Accounts (bisheriges Aktensystem)</b>	
deleteExportPackage	Beenden des Vorgangs (Löschen Exportpaket und ggf. bisheriges Aktenkonto)

### 3.2.1.7 Fehlersituationen und Handhabung

Der gesamte Austausch von Informationen zwischen Aktensystemen und Anbietern kann durch die in Schritt 1 erzeugte Vorgangs-ID genau einem konkreten Relocation Vorgang zugeordnet werden. Diese Vorgangsnummer wird auch verwendet, wenn das jeweils andere Aktensystem über Fehler im Ablauf benachrichtigt werden muss (Incidents).

#### 3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich oder derzeit nicht möglich

Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter (alt) das Exportpaket voraussehbar nicht importieren oder widerspricht der Versicherte nach der Initialisierung des Aktenkontos beim neuen Kostenträger der Nutzung der ePA, so kann durch Übertragung eines Incidents an das Aktensystem (alt) dieser Sachverhalt mitgeteilt werden, so dass der Transfervorgang abgebrochen und das Exportpaket nicht erzeugt oder wieder gelöscht wird.

Incident Abbruch des Transfers		
<b>I_Information_Service_Accounts (bisheriger Anbieter)</b>		
postExportPackageIncident	Benachrichtigung zum Abbruch des Transfers	
	<b>Incident</b>	
	relocationAborted	Abbruch aus Gründen bei Anbieter (neu). Transfer wird zu gegebener Zeit erneut gestartet

Das Aktenkonto wird bei Anbieter (alt) wieder in den Status ACTIVATED gesetzt, um eine weitere Nutzung zu ermöglichen.

Für einen Transfer zu einem späteren Zeitpunkt muss der Anbieter (neu) den Vorgang durch Anfrage bei den weiteren Anbietern (alt) und Übermittlung eines ENC-Zertifikats erneut starten.

### 3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter

Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter (alt) das Exportpaket unter Verwendung der übertragenen Download-URL nicht oder nicht vollständig laden oder die Inhalte des Exportpaketes aufgrund fehlerhafter Verschlüsselung oder fehlerhafter Struktur oder Inhalte nicht erfolgreich integrieren oder der Anbieter (neu) hat keine Download-URL vom Anbieter (alt) bezogen, so kann durch Übertragung eines Incidents an den Anbieter (alt) dieser Sachverhalt mitgeteilt werden.

Incident Fehler bei Import		
<b>I_Information_Service_Accounts (bisheriges Aktensystem)</b>		
postExportPackageIncident	Benachrichtigung zu Problemen beim Import des Exportpakets	
	<b>Incident</b>	
	importFailed	Exportpaket kann nicht vom Downloadpunkt geladen werden, ist unvollständig oder falsch verschlüsselt
	packageCorrupt	Exportpaket kann nicht verarbeitet werden (strukturelle Fehler oder inhaltliche Fehler)
	urlNotReceived	Download-URL nicht erhalten

Das Aktenkonto verbleibt beim neuen Anbieter in Status INITIALIZED. Die Incidentmeldung an den Anbieter (alt) kann durch Kommunikation der Anbieter und/oder Betreiber untereinander zum Zweck der Problemlösung ergänzt werden.

Der Anbieter (alt) meldet die Korrektur durch erneuten Versand einer Download-URL an den Anbieter (neu) für den unterbrochenen Vorgang.

Es obliegt dem Anbieter (alt), bei zeitlich aufwendigen Korrekturen das Aktenkonto zunächst für eine weitere Nutzung wieder zu aktivieren (Status ACTIVATED) und nach Abschluss der Korrektur wieder in den Status SUSPENDED zu überführen.

Es obliegt dem Anbieter (alt) auch, bei zeitlich aufwendigen Korrekturen den Transfer durch Senden des Incidents "relocationAborted" an den Anbieter (neu) abubrechen und das Aktenkonto zur weiteren Nutzung wieder zu aktivieren (Status ACTIVATED). Der Transfer muss dann durch den Anbieter (neu) erneut gestartet werden.

### 3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter

Ruft ein neuer Anbieter ein bereitgestelltes Exportpaket nicht ab oder erfolgt durch den neuen Anbieter keine Benachrichtigung über einen erfolgreichen Abschluss des Transfers oder einen Fehler beim Import des Exportpakets, dann kann eine Benachrichtigung an den neuen Anbieter erfolgen.

Incident Abbruch des Transfers durch bisherigen Anbieter		
I_Information_Service_Accounts (neuer Anbieter)		
postPackageDeliveryIncident	Benachrichtigung zum Abbruch des Transfers	
	<b>Incident</b>	
	noRelocationConfirmation	Nach Ablauf der Bereitstellungszeit gemäß A-15703-* wird der Transfer durch den Anbieter (alt) abgebrochen, da keine Bestätigung eines erfolgreichen Imports erfolgte.

Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei Anbieter (alt) auf den Status ACTIVATED gesetzt, um eine weitere Nutzung zu ermöglichen. Exportpaket und Downloadlink können gelöscht werden. Der Transfer muss durch den Anbieter (neu) erneut gestartet werden.

#### 3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter

Ein Anbieter (alt) kann den Abbruch eines angeforderten Transfers an den Anbieter (neu) signalisieren.

Incident Abbruch des Transfers durch bisherigen Anbieter		
I_Information_Service_Accounts (neuer Anbieter)		
postPackageDeliveryIncident	Benachrichtigung zum Abbruch des Transfers	
	<b>Incident</b>	
	relocationAborted	Das Exportpaket kann aufgrund von Ursachen seitens Anbieter (alt) nicht (länger) bereitgestellt werden. Der Transfer wird vorzeitig abgebrochen und muss erneut gestartet werden.

Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei Anbieter (alt) auf den Status ACTIVATED zurückgesetzt, wenn dieses schon den Status SUSPENDED hat, um eine weitere Nutzung zu ermöglichen. Exportpaket und Downloadlink können gelöscht werden. Der Transfer muss durch den Anbieter (neu) erneut gestartet werden.

### 3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM

Im Folgenden wird beschrieben, welche Informationen in einem HSM (als VAU-HSM bezeichnet) zu speichern sind.

Verständnishinweis: Die HMAC-Schlüssel (symmetrische Schlüssel) für die Prüfung der VSDM+-Prüfnachweise [gemSpec\_SST\_FD\_VSDM], [C\_11321] werden von den VSDM-Betreibern erzeugt und für die ePA-VAUs der ePA-Betreiber verschlüsselt exportiert. Die Schlüssel und auch die Export/Import-Vorgänge (Mehr-Augen-Prinzip) sind die gleichen wie sie auch für/bei der E-Rezept-VAU verwendet werden.

#### **A\_24611-06 -ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und Informationen für VAU-Betrieb**

Das ePA-Aktensystem MUSS sicherstellen, dass folgende, für den Betrieb der VAU notwendigen Schlüssel und Informationen in einem HSM (als VAU-HSM bezeichnet) gespeichert werden:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU (u.a. genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit professionOIDoid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Zertifikat C.ZD.SIG mit professionOID oid\_popp-token für die Token-Signatur-Identität des PoPP-Services
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und Überschlüsselung")
- symmetrische Schlüssel für die HMAC-Prüfung der VSDM-Prüfziffern (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

#### **[<=]**

Hinweis:

Es gelten die Anforderungen aus [gemSpec\_Krypt#3.18 VSDM-Prüfziffer Version 2] für ein ePA-Aktensystem in der Rolle "Prüfziffer Version 2 prüfendes System". Aus den ins HSM importierten gemeinsamen Geheimnissen erfolgt im HSM eine Schlüsselableitung (A\_27299-\*) der für die Entschlüsselung der Prüfziffer Version 2 benötigten AES/GCM-Schlüssel.

**A\_26109 -ePA-Aktensystem - Unterschiedliche private****Authentisierungsschlüssel für AK-, Befugnisverifikations- und Service-VAU**

Das ePA-Aktensystem MUSS sicherstellen, dass für die Authentisierungsidentitäten für Aktenkontoverwaltungs-VAUs, Befugnisverifikations-VAUs und Service-VAUs unterschiedliche private Schlüssel verwendet werden. [≤]

**A\_26110 -ePA-Aktensystem - Unterschiedliche private****Authentisierungsschlüssel für unterschiedliche Service-VAUs**

Das ePA-Aktensystem MUSS sicherstellen, dass für unterschiedliche Typen von Service-VAUs unterschiedliche private Schlüssel für die Authentisierung genutzt werden. [≤]

Hinweis zu A\_26110: Ein Typ einer Service-VAU könnte beispielsweise eine PDF-Konvertierungs-Service-VAU oder eine Pseudonymisierungs-Service-VAU für Daten zur Sekundärnutzung sein. Alle Instanzen einer PDF-Konvertierungs-Service-VAU nutzen denselben privaten Authentisierungsschlüssel. Die Instanzen der Pseudonymisierungs-Service-VAU dürfen den Authentisierungsschlüssel der PDF-Konvertierungs-Service-VAU jedoch nicht verwenden.

**A\_24612-05 -ePA-Aktensystem - Erzwingen von 4-Augen-Prinzip für Einbringen und Verwalten von Informationen ins VAU-HSM**

Das ePA-Aktensystem MUSS technisch erzwingen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip in das VAU-HSM eingebracht und verwaltet werden können:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit professionOID oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Zertifikat C.ZD.SIG mit professionOID oid\_popp-token für die Token-Signatur-Identität des PoPP-Services
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[≤]

**A\_24614-05 -ePA-Aktensystem - Einbringung von Informationen ins VAU-HSM im 4-Augen-Prinzip mit der gematik**

Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip ins VAU-HSM eingebracht und im VAU-HSM verwaltet werden, bei dem eine von der gematik benannte Person beteiligt ist:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs

- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit professionOIDoid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Zertifikat C.ZD.SIG mit professionOID oid\_popp-token für die Token-Signatur-Identität des PoPP-Services
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

### [<=]

Beim Einbringen der Hashwertrepräsentation der erlaubten VAU-Software ins VAU-HSM prüft die von der gematik benannte Person, dass die Hashwertrepräsentation des VAU-Images zuvor vom Hersteller des ePA-Aktensystems an die gematik übermittelt wurde und zulässig für den Produktivbetrieb ist.

Die von der gematik benannte Person prüft, dass das Zertifikat für die Token-Signatur-Identität des PoPP-Services gültig ist und die geforderten Inhalte enthält (Zertifikatsprofil oid\_zd\_sig (OID 1.2.276.0.76.4.287, "C.ZD.SIG"), technische Rolle oid\_popp-token (OID 1.2.276.0.76.4.320)).

### **A\_24618-05 -ePA-Aktensystem - Zugriff auf Schlüssel und Informationen im VAU-HSM**

Das ePA-Aktensystem MUSS sicherstellen, dass auf die folgenden, für den Betrieb der VAU notwendigen und im VAU-HSM gespeicherten Schlüssel und Informationen ausschließlich über attestierte VAU-Instanzen zugegriffen werden kann:

- privater Schlüssel der Authentisierungsidentität der VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU ausschließlich durch eine Befugnisverifikations-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität eines Service-VAU-Typs ausschließlich durch eine Service-VAU-Instanz dieses Service-VAU-Typs
- privater Schlüssel der Verschlüsselungsidentität der VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Signaturidentität der VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Zertifikat C.FD.ENC mit professionOIDoid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibersausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Zertifikat C.ZD.SIG mit professionOID oid\_popp-token für die Token-Signatur-Identität des PoPP-Services
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüsselausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz

- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüsselausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und Überschlüsselung") ausschließlich durch die Aktenkontoverwaltungs-VAU-Instanz oder durch eine dedizierte Überschlüsselungs-VAU
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden, ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse) ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz.

[<=]

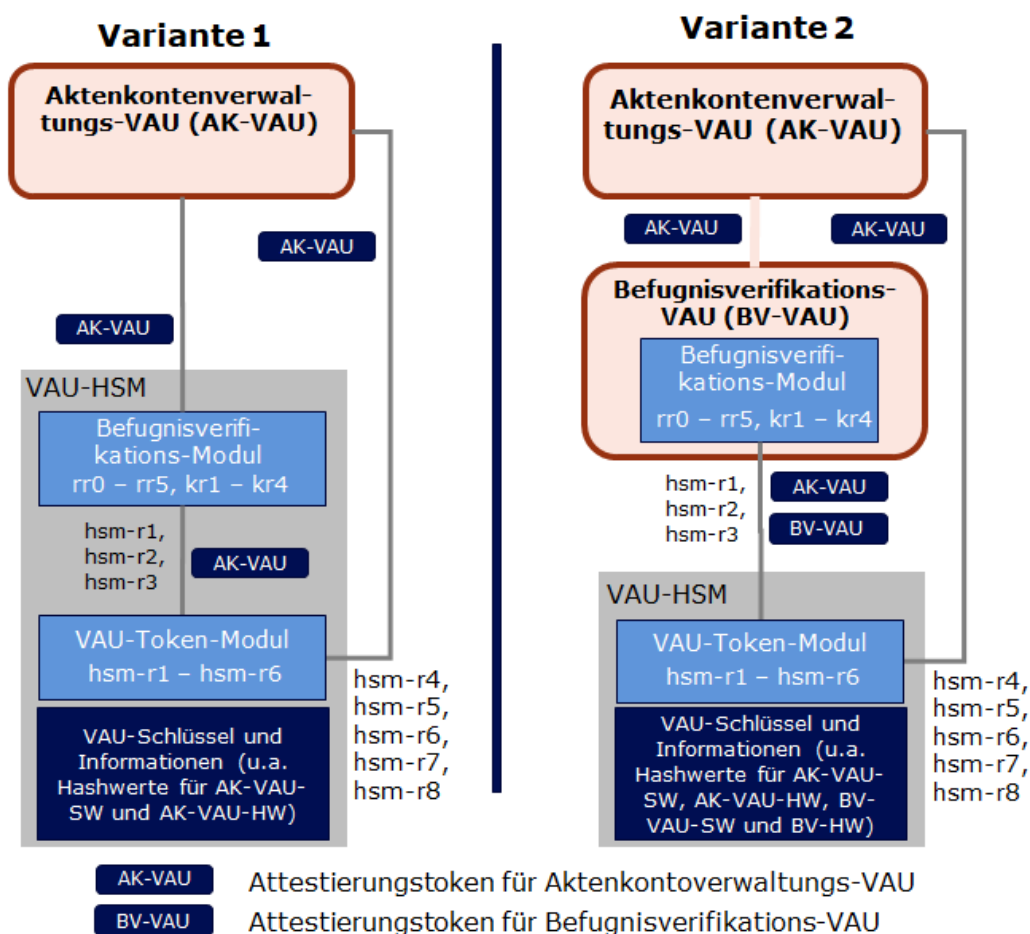
### 3.4 Befugnisverifikations-Modul

Das Befugnisverifikations-Modul enthält die Regeln zur Befugnisregistrierung (entitlement registration rules) und die Regeln zum Abruf der versichertenindividuellen Persistierungsschlüssel (key rules).

Die folgende Abbildung zeigt die zwei möglichen Architekturvarianten für die Ausführung des Befugnisverifikations-Moduls. In Variante 1 wird es direkt im VAU-HSM ausgeführt. In Variante 2 wird es in einer Befugnisverifikations-VAU ausgeführt, die zwischen einer Aktenkontoverwaltungs-VAU und einem VAU-HSM vermittelt und Prüfungen für das VAU-HSM übernimmt (z. B. prüfen der ID-Token oder registrieren neuer Befugnisse).

In beiden Varianten ist ein Zugriff auf die Schlüssel im VAU-HSM nur durch integrale und attestierte VAUs möglich. Die Prüfung der VAU-Attestierungstoken verbleibt in beiden Varianten im VAU-HSM (VAU-Token-Modul). Das VAU-HSM speichert in Variante 2 neben den Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der Aktenkontoverwaltung zusätzlich auch die Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der Befugnisverifikations-VAU. Ein Zugriff auf das HSM ist dann nur mit einem validen Attestierungstoken für die Aktenkontoverwaltungs-VAU und die Befugnisverifikations-VAU möglich.





**Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls**

#### **A\_25281 -ePA-Aktensystem - VAU-Token-Modul ausschließlich im HSM**

Das ePA-Aktensystem MUSS sicherstellen, dass ein VAU-Token-Modul ausschließlich in einem VAU-HSM ausgeführt wird. [≤]

#### **A\_24574 -ePA-Aktensystem - Befugnisverifikations-Modul im HSM oder Befugnisverifikations-VAU**

Das ePA-Aktensystem MUSS sicherstellen, dass ein Befugnisverifikations-Modul ausschließlich in einem VAU-HSM oder in einer Befugnisverifikations-VAU ausgeführt wird. [≤]

#### **A\_25050 -ePA-Aktensystem - 1:1-Beziehung zwischen Befugnisverifikations-VAU und Aktenkontoverwaltungs-VAU**

Das ePA-Aktensystem MUSS sicherstellen, dass eine 1:1-Beziehung zwischen einer Instanz einer Befugnisverifikations-VAU und einer Instanz einer Aktenkontoverwaltungs-VAU gibt. [≤]

### **3.4.1 VAU-Token-Modul**

Dieser Abschnitt enthält die Regeln zum Zugriff auf die Schlüssel im VAU-HSM. Diese werden von einem Befugnisverifikations-Modul genutzt.

#### **A\_24712-01 -ePA-Aktensystem - VAU-Token-Modul nur durch Befugnisverifikations-Modul oder Aktenkontoverwaltungs-VAU aufrufbar**

Das ePA-Aktensystem MUSS sicherstellen, dass die Regeln hsm-r1 bis hsm-r3 des VAU-Token-Moduls ausschließlich von einem Befugnisverifikations-Modul und die Regeln hsm-



r4 bis hsm-r7 ausschließlich von einer Aktenkontoverwaltungs-VAU aufgerufen werden.  
[<=]

#### A\_25282-02 -ePA-Aktensystem - Regeln des VAU-Token-Moduls

Das VAU-Token-Modul MUSS die in TabelleTab\_AS\_VAU-Token\_Modul\_Rules definierten Regeln umsetzen.[<=]

**Tabelle 4: Tab\_AS\_VAU-Token\_Modul\_Rules -Prüfregeln VAU Token**

Regel	Beschreibung
hsm-r1	<p><i>Diese Regel dient zur Sicherung von Befugnissen und HSM-ID-Token mittels CMAC.</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• VAU-Attestierungstoken einer Befugnisverifikations-VAU (optional)</li> <li>• Daten</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Daten gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur(en)des(r) VAU-Attestierungstoken (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> <li>3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <p>Falls die Prüfungen 1) - 3) erfolgreich waren, werden die übergebenen Daten mittels CMAC gesichert.</p>
hsm-r2	<p><i>Diese Regel dient zur Ableitung der versichertenindividuellen Persistierungsschlüssel</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• KVNR</li> <li>• gewünschte Persistierungsschlüssel [Label für Datenpersistierungs-Masterkey und/oder Label für Befugnispersistierungs-Masterkey]</li> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• falls in Eingangsdaten angefordert: versichertenindividueller Befugnispersistierungsschlüssel</li> <li>• falls in Eingangsdaten angefordert: versichertenindividueller Datenpersistierungsschlüssel</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur(en)des(r) VAU-Attestierungstoken (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-</li> </ol>

	<p>VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</p> <p>3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</p> <p>Falls die Prüfungen 1) - 3) erfolgreich waren, wird der angeforderte versichertenindividuelle Befugnispersistierungsschlüssel und/oder versichertenindividuelle Datenpersistierungsschlüssel für die übergebene KVNR von den durch die Label identifizierten Masterkeys abgeleitet.</p>
hsm-r3	<p><i>Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfziffern der Version 1 oder der Entschlüsselung der VSDM-Prüfziffern der Version 2</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)</li> <li>Szenario VSDM-Prüfziffer Version 1 <ul style="list-style-type: none"> <li>Daten</li> <li>Bezeichner des HMAC-Schlüssels</li> </ul> </li> <li>Szenario VSDM-Prüfziffer Version 2 <ul style="list-style-type: none"> <li>VSDM-Prüfziffer in Version 2</li> </ul> </li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>Szenario VSDM-Prüfziffer Version 1: HMAC der Daten mit dem symmetrischen Schlüssel, der zum übergebenen Bezeichner des HMAC-Schlüssels gehört</li> <li>Szenario VSDM-Prüfziffer Version 2: innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) bei erfolgreicher Entschlüsselung</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch)</li> <li>prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> <li>(opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <p>Szenario VSDM-Prüfziffer Version 1: Falls die Prüfungen 1) - 3) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.</p> <p>Szenario VSDM-Prüfziffer Version 2: Falls die Prüfungen 1) - 3) erfolgreich waren, wird die VSDM-Prüfziffer gemäß den Prüfschritten 4. und 5. aus A_27279-* geprüft und entschlüsselt. Bei erfolgreicher Entschlüsselung der VSDM-Prüfziffer wird die innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) zurückgeliefert, ansonsten ein Fehler.</p>
hsm-r4	<p><i>Diese Regel dient zur Nutzung der privaten Schlüssel der AUT-Identitäten der VAU</i></p>

	<p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Challenge</li> <li>• [VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU  VAU-Attestierungstoken einer Befugnisverifikations-VAU  VAU-Attestierungstoken eines Service-VAU-Typs]</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Challenge signiert mit privatem Schlüssel der AUT-Identität <ul style="list-style-type: none"> <li>• der Aktenkontoverwaltungs-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU übergeben wurde,</li> <li>• der Befugnisverifikations-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Befugnisverifikations-VAU übergeben wurde,</li> <li>• des Service-VAU-Typs, falls in den Eingangsdaten ein VAU-Attestierungstoken des Service-VAU-Typs übergeben wurde.</li> </ul> </li> </ul> <p><b>Prüfschritte</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und zum VAU-Typ passt.</li> </ol> <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, wird die übergebene Challenge mit dem privatem Schlüssel der zum VAU-Attestierungstoken gehörenden AUT-Identität signiert.</p>
hsm-r5	<p><i>Diese Regel dient zur Nutzung des privaten Schlüssels der ENC-Identität der VAU</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• verschlüsselte Daten</li> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• entschlüsselte Daten</li> </ul> <p><b>Prüfschritte</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind.</li> </ol> <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen verschlüsselten Daten mit dem privatem Schlüssel der ENC-Identität der VAU entschlüsselt.</p>
hsm-r6	<p><i>Diese Regel dient zur Nutzung des privaten Schlüssels der Signaturidentität der VAU</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• zu signierende Daten</li> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> </ul> <p><b>Ausgangsdaten:</b></p>

	<ul style="list-style-type: none"> <li>signierte Daten</li> </ul> <p><b>Prüfschritte</b></p> <ol style="list-style-type: none"> <li>prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</li> <li>prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen Daten mit dem privaten Schlüssel der Signaturidentität der VAU signiert.</p>
hsm-r7	<p><i>Diese Regel dient zum Auslesen des ENC-Zertifikats des anderen Aktensystembetreibers.</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>Verschlüsselungszertifikat C.FD.ENC des anderen Aktensystembetreibers</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</li> <li>prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <p>Falls die Prüfungen 1) - 2) erfolgreich waren, wird das ENC-Zertifikat des anderen Aktensystembetreibers zurückgeliefert.</p>
hsm-r8	<p>Diese Regel dient zum Ableiten von symmetrischen Schlüsseln für die Ver- bzw. Entschlüsselung von Daten</p> <p>Sie dient bspw. dazu, sogenannte Submissions für die Datenausleitung an das Forschungsdatenzentrum Gesundheit (FDZ) nach § 363 Absatz 1 SGB V außerhalb der VAU im Aktensystem zwischenspeichern, bis das Forschungsdatenzentrum diese Submissions abholt. Die Submissions sind dann über die über diese Regel abgeleiteten symmetrischen Schlüssel außerhalb der VAU kryptographisch gesichert.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder einer Service-VAU</li> <li>Ableitungsvektor <i>dv</i></li> <li>Label für Masterkey (opt.)</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>symmetrischer Schlüssel <i>symKey</i></li> <li>Label für Befugnis-Masterkey</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</li> <li>prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und es sich um die Attestierung einer Aktenkontoverwaltungs-VAU oder Service-VAU handelt</li> </ol>

	<p>3. falls ein Label für einen Masterkey In den Eingangsdaten enthalten ist, prüfen, ob das Label zu einem Befugnis-Masterkey gehört</p> <p>Falls alle Prüfungen erfolgreich waren, wird symKey wie folgt abgeleitet:</p> <p>Fall: Eingangsdaten enthalten ein Label mkey_label für einen Befugnis-Masterkey: Ableitung eines AES-Schlüssels [FIPS-197] symKey mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren auf Basis des Befugnis-Masterkeys mit Label mkey_label und dem Ableitungsvektor "eds: "+ dv. Ausgangsdaten sind der abgeleitete Schlüssel symKey und das Label mkey_label.</p> <p>(Verständnishinweis: eds steht für "External Data Storage". Das HSM erzwingt bei dieser Regeln, dass das Präfix "eds: " (also 5 Byte) dem vom Aufrufer übergebenen Ableitungsvektor (dv) vorangestellt wird.)</p> <p>Fall: Eingangsdaten enthalten kein Label für einen Befugnis-Masterkey: Ableitung eines AES-Schlüssels [FIPS-197] symKey mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#Abschnitt 2.4] zulässigen Verfahren auf Basis des aktuellen Befugnis-Masterkeys und dem Ableitungsvektor "eds: " + dv. Ausgangsdaten sind der abgeleitete Schlüssel symKey und das Label des aktuellen Befugnis-Masterkeys.</p>
--	--

#### A\_24667 -ePA-Aktensystem -VAU-HSM - Prüfen des VAU-Attestierungstokens

Das VAU-HSM MUSS bei der Prüfung eines VAU-Attestierungstokens sicherstellen, dass dieses zeitlich gültig ist und Replay-Attacken abwehren.【<=】

#### A\_26303 -ePA-Aktensystem - Abgeleitete Verschlüsselungsschlüssel sind ausschließlich einer VAU zugänglich

Das ePA-Aktensystem MUSS sicherstellen, dass ein mit Regel hsm-r8 abgeleiteter Schlüssel ausschließlich einer VAU zugänglich ist und ausschließlich mittels AES/GCM analog [gemSpec\_Krypt#GS-A\_4389] verwendet wird.【<=】

### 3.4.2 Regeln des Befugnisverifikations-Moduls

Die folgende Tabelle zeigt die Regeln des Befugnisverifikations-Moduls im Überblick.

**Tabelle 5: Überblick über die Regeln des Befugnisverifikations-Moduls**

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
rr0	Mit dieser Regel werden <b>ID-Token</b> im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.	Tab_AS_Entitlement_Registration_Rules
rr1	Mit dieser Regel werden vom <b>Aktenkontoinhaber</b> am ePA-FdV erstellte <b>Befugnisse</b> im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.	Tab_AS_Entitlement_Registration_Rules
rr2	Mit dieser Regel werden vom	Tab_AS_Entitlement_Registration_Rules

	<b>Vertreter</b> am ePA-FdV erstellte <b>Befugnisse</b> für das Aktenkonto des Versicherten im Aktensystem registriert. Die im ePA-FdV erstellen Befugnisse sind vom Vertreter mittels Signaturdienst signiert.	
rr3	Mit dieser Regel werden <b>Befugnisse</b> im Aktensystem registriert, die sich durch das <b>Stecken der eGK in einer Leistungserbringerumgebung</b> oder aufgrund eines <b>PoPP-Tokens</b> ergeben.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr4	Mit dieser Regel werden die <b>Befugnisse</b> für den Kostenträger und die zuständige Ombudsstelle bei der <b>Anlage eines Aktenkontos</b> im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr5	Mit dieser Regel werden die <b>Befugnisse</b> bei einem <b>betreiberübergreifenden Anbieterwechsel</b> im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
kr1	Diese Regel wird für die <b>Anmeldung des Aktenkontoinhabers</b> genutzt.	<i>Tab_AS_SDS-Key_Rules</i>
kr2	Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssels genutzt. Sie wird für die <b>Anmeldung</b> von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	<i>Tab_AS_SDS-Key_Rules</i>
kr3	Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die <b>Anmeldung</b> von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	<i>Tab_AS_SDS-Key_Rules</i>
kr4	Diese Regel wird für die <b>Anmeldung des E-Rezept-Fachdienstes</b> verwendet.	<i>Tab_AS_SDS-Key_Rules</i>
kr5	Diese Regel wird für die Überschlüsselung (ggf. mit Umschlüsselung einer	<i>Tab_AS_SDS-Key_Rules</i>

	Überschlüsselung) verwendet.	
--	------------------------------	--

### A\_24573-03 -ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls

Das Befugnisverifikations-Modul MUSS die in den Tabellen *Tab\_AS\_Entitlement\_Registration\_Rules* und *Tab\_AS\_SDS-Key\_Rules* definierten Regeln umsetzen. [≤]

**Tabelle 6: Tab\_AS\_Entitlement\_Registration\_Rules - Regeln zur Registrierung von Befugnissen**

Regel	Beschreibung
rr0	<p>Mit dieser Regel werden <b>ID-Token</b> im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>ID-Token mit NutzerID=x signiert durch einen sektoralen Identity Provider, den IDP-Dienst oder den E-Rezept-Fachdienst</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>HSM-ID-Token mit NutzerID=x gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>prüfen des ID-Tokens gemäß A_24690-* (C.FD.SIG) bei Token eines IDPs bzw. gemäß A_24658-* bei Token des E-Rezept-Fachdiensts (C.FD.AUT).</li> <li>Falls die Prüfung in 1) erfolgreich war, <ol style="list-style-type: none"> <li>erstellt das Befugnisverifikations-Modul ein HSM-ID-Token mit der NutzerID=x, einer Gültigkeitsdauer von 24 Stunden und der professionOID aus dem Signaturzertifikat (oid_idpd_sek, oid_idpd oder oid_erp-vau).</li> <li>ruft das Befugnisverifikations-Modul die VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und dem HSM-ID-Token auf. <ol style="list-style-type: none"> <li>Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> </ol> </li> <li>Das Befugnisverifikations-Modul liefert das mittels CMAC gesicherte HSM-ID-Token als Ergebnis des Regelaufrufs zurück.</li> </ol>
rr1	<p>Mit dieser Regel werden vom <b>Aktenkontoinhaber</b> am ePA-FdV erstellte Befugnisse im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>ID-Token oder HSM-ID-Token gesichert mit CMAC</li> <li>Befugnis1 = (KVNR Aktenkonto, Telematik-ID oder KVNR,</li> </ul>



	<p>Gültigkeitszeitraum) signiert vom Versicherten</p> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>Befugnis2 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> <li>prüfen, ob die professionOID im Signaturzertifikat oid_idpd_sek ist</li> <li>prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt oder prüfen des HSM-ID-Tokens</li> <li>Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens <ol style="list-style-type: none"> <li>Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>prüfen, ob die professionOID im HSM-ID-Token oid_idpd_sek ist</li> <li>prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt.</li> </ol> </li> <li>prüfen der Befugnis1 <ol style="list-style-type: none"> <li>prüfen der Signatur gemäß A_25042-* (Zertifikatsprofil C.CH.SIG)</li> <li>prüfen, ob die professionOID im Signaturzertifikat oid_versicherter ist</li> <li>prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der "KVNR Aktenkonto" in der Befugnis1 übereinstimmt.</li> <li>prüfen, dass das JWT gemäß A_24587-* zeitlich gültig ist (<math>iat - 15s \leq \text{aktuelle Zeit} \leq exp + 15s</math>)</li> </ol> </li> <li>Falls die Prüfungen in 1) bis 2) erfolgreich waren, erstellt das Befugnisverifikations-Modul die Befugnis2. Die Inhalte werden aus Befugnis1 übernommen mit folgender Ausnahme: Für eine Befugnis1 mit oid = oid_ncpeh wird die Gültigkeit validTo in Befugnis2 auf aktuelle Zeit + 1 Stunde gesetzt.</li> <li>Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis2 <ol style="list-style-type: none"> <li>Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.</li> </ol>
rr2	<p>Mit dieser Regel werden vom <b>Vertreter</b> am ePA-FdV erstellte Befugnisse für das Aktenkonto des Versicherten im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Vertreter mittels Signaturdienst signiert.</p>

**Eingangsdaten:**

- VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU
- ID-Token oder HSM-ID-Token gesichert mit CMAC
- Befugnis1 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) signiert vom Vertreter
- Befugnis2 = (KVNR Aktenkonto, KVNR Vertreter) gesichert mittels CMAC

**Ausgangsdaten:**

- Befugnis3 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC

**Prüfschritte:**

1. prüfen des ID-Tokens gemäß A\_24690-\* (Zertifikatsprofil C.FD.SIG)
  - a. prüfen, ob die professionOID im Signaturzertifikat oid\_idpd\_sek ist
  - b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt  
oder prüfen des HSM-ID-Tokens
  - c. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens
    - i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
  - d. prüfen, ob die professionOID im HSM-ID-Token oid\_idpd\_sek ist
  - e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt.
2. prüfen der Befugnis1 und Befugnis2
  - a. prüfen der Signatur von Befugnis1 gemäß A\_25042-\* (Zertifikatsprofil C.CH.SIG)
  - b. prüfen, ob die professionOID im Signaturzertifikat oid\_versicherter ist
  - c. prüfen des CMAC von Befugnis2
  - d. prüfen, dass die Telematik-ID in Befugnis 1 keine KVNR ist (Vertreter dürfen keine weiteren Vertreter befugen)
  - e. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der „KVNR Vertreter“ in der Befugnis2 übereinstimmt
  - f. prüfen, ob die „KVNR Aktenkonto“ in Befugnis 1 mit der „KVNR Aktenkonto“ in Befugnis2 übereinstimmt
  - g. prüfen, dass das JWT gemäß A\_24587-\* zeitlich gültig ist ( $iat - 15s \leq \text{aktuelle Zeit} \leq exp + 15s$ )
3. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis3 vom Befugnisverifikations-Modul erstellt. Die Inhalte werden aus Befugnis1 übernommen.

	<p>4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis3</p> <p>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> <p>5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis3 als Ergebnis des Regelaufrufs zurück.</p>
rr3	<p>Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das Stecken der eGK in einer Leistungserbringenumgebung oder aufgrund eines PoPP-Tokens ergeben.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>VSDM-Prüfziffer in Version 2 signiert mit AUT-Identität der SMC-B <b>oder</b> signiertes PoPP-Token</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC</li> <li>falls VSDM-Prüfziffer in Version 2, zusätzlich die innere Struktur der Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR)</li> </ul> <p><b>Prüfschritte:</b></p> <p><u>Szenario VSDM-Prüfziffer in Version 2:</u>  Falls enforce_popp_only = true, dann FAIL, ansonsten führe die folgenden Prüfschritte durch:</p> <ol style="list-style-type: none"> <li>prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A_25042-* (C.HCI.AUT)</li> <li>Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert.</li> <li>Aufruf von VAU-HSM Regel hsm-r3 mit der dekodierten VSDM-Prüfziffer <ol style="list-style-type: none"> <li>Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>prüfen der inneren Struktur nach Prüfschritt 6 gemäß A_27279-* (d.h. eGK ist nicht gesperrt)</li> <li>prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer (prüfziffer.iat) nicht länger als 20 Minuten zurückliegt (prüfziffer.iat - 30s &lt;= aktuelle Zeit &lt; prüfziffer.iat + 20 Minuten + 15s, Hinweis in der Prüfziffer gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben)</li> <li>prüfen des prüfziffer.hcv nach Prüfschritt 8 gemäß A_27279-* bzgl. des hcv im JWT</li> <li>Falls die Prüfungen in 1) bis 6) erfolgreich waren, und die VAU-HSM Regel hsm-r3 den Klartext der inneren Struktur der Prüfziffer zurückgeliefert hat, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:</li> </ol>

	<ul style="list-style-type: none"> <li>• Aktenkonto: KVNR, die als Ergebnis der VAU-HSM Regel hsm-r3 zurückgeliefert wird</li> <li>• Telematik-ID: die Telematik-ID aus der SMC-B-Signatur</li> <li>• Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur.</li> </ul> <p>8. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis</p> <p>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> <p>9. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis sowie die entschlüsselte innere Struktur der Prüfziffer im Klartext gemäß A_27278-* als Ergebnis des Regelaufrufs zurück.</p> <p><u>Szenario PoPP-Token:</u></p> <ol style="list-style-type: none"> <li>1. prüfen des PoPP-Tokens via TI-PKI gemäß Abschnitt "PoPP-Token Prüfung" in [gemSpec_PoPP_Service], wobei im HSM <u>bis auf den OCSP-Sperrstatus</u> keine Prüfung des Signaturzertifikats des PoPP-Tokens erfolgt, da das Signaturzertifikat kontrolliert im 4-Augenprinzip in das HSM eingebracht wird. Da das in das HSM eingebrachte TI-PKI-Signaturzertifikat genutzt wird, ist auch kein Bezug und keine Verarbeitung von Entity Statements im HSM erforderlich. Der Claim iss im PoPP-Token muss nicht geprüft werden.</li> <li>2. prüfen, dass der Ausstellungszeitpunkt des PoPP-Tokens (PoPP-Token.iat) nicht länger als 20 Minuten zurückliegt (<math>\text{PoPP-Token.iat} - 30s \leq \text{aktuelle Zeit} &lt; \text{PoPP-Token.iat} + 20 \text{ Minuten} + 15s</math>, Hinweis: im PoPP-Token gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben).</li> <li>3. prüfen, dass PoPP-Token.proofMethod keine Prüfmethode -* ist.</li> <li>4. Falls die Prüfungen in 1) bis 3) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt: <ul style="list-style-type: none"> <li>• Aktenkonto: KVNR aus PoPP-Token.patientId</li> <li>• Telematik-ID: Telematik-ID aus PoPP-Token.actorID</li> <li>• Gültigkeitszeitraum: ergibt sich aus PoPP-Token.actorProfessionOid.</li> </ul> </li> <li>5. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis <p>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> </li> <li>6. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis zurück.</li> </ol>
rr4	<p><i>Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der <b>Anlage eines Aktenkontos</b> im Aktensystem registriert.</i></p> <p><b>Eingangsdaten:</b></p>

	<ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>Befugnis1 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) signiert mit SMC-B des Kostenträgers bzw. der Ombudsstelle</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>Befugnis2 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>Prüfen der Befugnis1 <ol style="list-style-type: none"> <li>prüfen der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle gemäß A_25042-* (C.HCI.OSIG)</li> <li>prüfen, ob die professionOID im Signaturzertifikat oid_kostentraeger bzw. oid_ombudsstelle ist</li> <li>prüfen, ob die Telematik-ID im Signaturzertifikat C.HCI.OSIG der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle mit der Telematik-ID in der Befugnis1 übereinstimmt</li> </ol> </li> <li>Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 erstellt. Die Inhalte der Befugnis2 sind: <ul style="list-style-type: none"> <li>Aktenkonto: die KVNR des Aktenkontos aus Befugnis1</li> <li>Telematik-ID: die Telematik-ID aus Befugnis1</li> </ul> </li> <li>Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 <ol style="list-style-type: none"> <li>Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.</li> </ol>
rr5	<p>Mit dieser Regel werden die <b>Befugnisse</b> bei einem <b>betreiberübergreifenden Anbieterwechsel</b> im Aktensystem registriert.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>Befugnis1 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) signiert vom alten Aktensystembetreiber</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>Befugnis2 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>Prüfen der Befugnis1 <ol style="list-style-type: none"> <li>prüfen der Signatur gemäß A_25042-* (C.FD.SIG)</li> <li>prüfen, ob im Signaturzertifikat C.FD.SIG der</li> </ol> </li> </ol>

	<p>professionOIDoid_epa_vauist</p> <p>c. prüfen, dass das Signaturzertifikat C.FD.SIG nicht auf das importierende Aktensystem ausgestellt ist.</p> <p>2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 mit den Inhalten aus Befugnis1 erstellt.</p> <p>3. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2</p> <p>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> <p>4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.</p>
--	--

#### A\_24690-01 -ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen des ID-Tokens

Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung eines ID-Tokens durchführen:

- das ID-Token muss gemäß A\_25042-\* valide signiert sein durch einen sektoralen Identity Provider oder den IDP-Dienst (professionOID ist oid\_idpd\_sek oder oid\_idpd),
- das ID-Token muss zeitlich gültig sein (Felder: iat, exp),
- das ID-Token muss im Feld auid das ePA-Aktensystem eingetragen haben.

[<=]

#### A\_24691 -ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen von übers ePA-FdV erstellten Befugnissen

Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung einer von einem Versicherten bzw. Vertreter über das ePA-FdV eingestellten signierten Befugnis durchführen:

- die Befugnis muss gemäß A\_25042-\* valide signiert sein durch einen Versicherten bzw. Vertreter (C.CH.SIG, professionOID ist oid\_versicherter),
- das JWT für die Befugnis gemäß A\_24587-\* darf nicht abgelaufen sein (Feld: exp),
- das Feld insurantID des JWT muss eine KVN sein,
- das Feld actorID des JWT muss eine KVN oder eine Telematik-ID sein,
- das Feld validTo des JWT muss ein zeitliches Datum sein.

[<=]

Die folgenden Regeln dienen zum Abruf der versichertenindividuellen Daten- und Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel und die Ableitungsvorschriften sind in [gemSpec\_Krypt] in Abschnitt 3.15.2 festgelegt.

**Tabelle 7: Tab\_AS\_SDS-Key\_Rules Key Rules - Regeln zur Ableitung der versichertenindividuellen Persistierungsschlüssel**

Regel	Beschreibung
kr1	Diese Regel wird für die Anmeldung des <b>Aktenkontoinhabers</b> genutzt.

	<p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• ID-Token oder HSM-ID-Token gesichert mit CMAC</li> <li>• Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "&lt;current&gt;" für jüngsten im VAU-HSM verfügbaren).</li> <li>• Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "&lt;current&gt;" für jüngsten im VAU-HSM verfügbaren).</li> <li>• ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys</li> <li>• versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys</li> </ul> <p><b>Regelverhalten:</b></p> <ol style="list-style-type: none"> <li>1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> <li>a. prüfen, ob die professionOID im Signaturzertifikat oid_idpd_sek ist oder prüfen des HSM-ID-Tokens</li> <li>b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <ol style="list-style-type: none"> <li>i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>c. prüfen, ob die professionOID im HSM-ID-Token oid_idpd_sek ist</li> </ol> </li> <li>2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVN-R aus dem ID-Token und den Labeln der zu verwendenden Befugnispersistierungs- und Datenpersistierungs-Masterkeys zur Ableitung von Befugnis- und Datenpersistierungsschlüssel aufgerufen. <ol style="list-style-type: none"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>3. Das Befugnisverifikations-Modul liefert die abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.</li> </ol>
kr2	<p><i>Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssel genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> </ul>



	<ul style="list-style-type: none"> <li>• KVNR (Aktenkonten-ID)</li> <li>• Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> <li>• ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys</li> <li>• ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. Aufruf der VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR und dem Label des Befugnispersistierungs-Masterkeys zur Ableitung des Befugnispersistierungsschlüssels <ol style="list-style-type: none"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>2. Das Befugnisverifikations-Modul liefert den abgeleiteten Befugnispersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.</li> </ol>
kr3	<p><i>Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• ID-Token oder HSM-ID-Token gesichert mit CMAC</li> <li>• Befugnis = (KVNR Aktenkonto, BefugtenID (TID KVNR), Gültigkeitszeitraum (opt.)) mit CMAC gesichert</li> <li>• Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> <li>• ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys</li> <li>• ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen des ID-Tokens <ol style="list-style-type: none"> <li>a. gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) oder prüfen des HSM-ID-Tokens</li> <li>b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1</li> </ol> </li> </ol>

	<p>mit dem VAU-Attestierungstoken der Aktenkontoverwaltung</p> <ol style="list-style-type: none"> <li>i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> <ol style="list-style-type: none"> <li>2. Prüfen der Befugnis <ol style="list-style-type: none"> <li>a. prüfen des CMAC der Befugnis mittels VAU-HSM Regel hsm-r1 <ol style="list-style-type: none"> <li>i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>b. prüfen, ob die Nutzer-ID im ID-Token bzw. im HSM-ID-Token (KVNR oder Telematik-ID) mit der Befugten-ID in der Befugnis übereinstimmt.</li> <li>c. prüfen, ob die Befugnis noch gültig ist, falls die Befugnis zeitlich begrenzt ist (d. h. ein Gültigkeitszeitraum in der Befugnis enthalten ist).</li> </ol> </li> <li>3. Falls alle Prüfungen in 1) bis 2) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR aus dem ID-Token bzw. im HSM-ID-Token und dem Label für den Datenpersistierungs-Masterkey zur Ableitung des Datenpersistierungsschlüssels aufgerufen. <ol style="list-style-type: none"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>4. Das Befugnisverifikations-Modul liefert den abgeleiteten Datenpersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.</li> </ol>
kr4	<p><i>Diese Regel wird für die Anmeldung des <b>E-Rezept-Fachdienstes</b> verwendet.</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• ID-Token oder HSM-ID-Token gesichert mit CMAC</li> <li>• KVNR (Aktenkonten-ID)</li> <li>• Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> <li>• ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys</li> <li>• ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. Prüfen des ID-Tokens <ol style="list-style-type: none"> <li>a. prüfen der Signatur gemäß A_25042-* (C.FD.AUT)</li> <li>b. prüfen, ob die professionOID im Zertifikat C.FD.AUT gleich oid_erp-vauist</li> </ol> </li> </ol>

	<ul style="list-style-type: none"> <li>c. prüfen des ID-Tokens gemäß A_24658-* oder prüfen des HSM-ID-Tokens</li> <li>d. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <ul style="list-style-type: none"> <li>i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ul> </li> <li>e. prüfen, ob die professionOID im HSM-ID-Token oid_erp-vau ist</li> </ul> <p>2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR aus dem ID-Token bzw. dem HSM-ID-Token und dem Label für den Datenpersistierungs-Masterkey zur Ableitung des Datenpersistierungsschlüssels aufgerufen.</p> <ul style="list-style-type: none"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ul> <p>3. Das Befugnisverifikations-Modul liefert den abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.</p>
kr5	<p>Diese Regel wird für die Überschlüsselung verwendet (ggf. mit Umschlüsselung einer Überschlüsselung).</p> <p>Diese Regel kann von einer VAU (AK-VAU oder dedizierte Überschlüsselungs-VAU) verwendet werden um verschlüsselte Akten zu überschlüsseln (vgl. Abschnitt 3.6- Umschlüsselung und Überschlüsselung). Dabei kann es auch zu einer Umschlüsselung einer älteren Überschlüsselung kommen.</p> <p>Sei &lt;current&gt; ein spezielles Symbol was im VAU-HSM durch das Label des jüngsten Überschlüsselungsschlüssel ersetzt wird. Ein Aufruf braucht so das tatsächliche Label nicht zu kennen. (Der Hersteller ist frei "&lt;current&gt;" durch ein selbstgewählten Symbolnamen zu ersetzen.)</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder ggf. einer dedizierten Überschlüsselungs-VAU</li> <li>• KVNR (Aktenkonten-ID)</li> <li>• Labelliste: nicht leere Liste von Label-n von Überschlüsselungs-Masterkeys (im Regelfall enthält die Liste mindestens "&lt;current&gt;" als Element)</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Liste von Paaren: versichertenindividueller Überschlüsselungsschlüssel (Secure Data Storage Key), Label für verwendeten Überschlüsselungs-Masterkey</li> </ul> <p>(Hinweis: Die Liste enthält mindestens ein Element -- im Fall der ersten Überschlüsselung in Intervall 2 (vgl. Abschnitt 3.6 ))</p> <p><b>Ablauf:</b> Das VAU-HSM muss des VAU-Attestierungstoken prüfen, ob es sich um eine AK-VAU oder dedizierte Überschlüsselungs-VAU handelt. Falls nein, Abbruch.</p>

<p>Das VAU-HSM durchläuft die Label-Liste und führt mit dem entsprechenden Label verbundenen Überschlüsselungs-Masterkey und der KVNR eine Schlüsselableitung durch. Dabei wird im VAU-HSM das spezielle Symbol "&lt;current&gt;" durch das Label des jüngsten Überschlüsselungs-Masterkeys vor Abarbeitung ersetzt.</p> <p>In der Ergebnisse (siehe Ausgangsdaten) ist "&lt;current&gt;" ebenfalls so ersetzt. Die Reihenfolge in der Eingangsliste muss in der Ausgabeliste gleich bleiben.</p>
---

### 3.5 Vertrauenswürdige Ausführungsumgebung (VAU)

Eine Vertrauenswürdige Ausführungsumgebung (VAU) gewährleistet mit technischen Maßnahmen, dass Daten serverseitig im ePA-Aktensystem im Klartext verarbeitet werden können, ohne dass einzelne Mitarbeiter des Betreibers auf diese Daten zugreifen können.

Die Datenverarbeitungen der Aktenkontoverwaltung müssen in einer VAU ausgeführt werden. Diese VAU wird im folgenden als Aktenkontoverwaltungs-VAU bezeichnet. Des weiteren kann das Befugnisverifikations-Modul in einer VAU ausgeführt werden. Diese VAU wird im folgenden als Befugnisverifikations-VAU bezeichnet.

#### **A\_25716-02 -ePA-Aktensystem - Services ausschließlich in der VAU**

Das ePA-Aktensystem MUSS sicherstellen, dass die folgenden Services ausschließlich innerhalb einer VAU ausgeführt werden können und ein Zugriff auf die Schnittstellen ausschließlich über einen VAU-Kanal erfolgen kann:

- Consent Decision Management Service
- Entitlement Management
- Constraint Management
- Device Management
- E-Mail Management
- Audit Event Service
- Authorization Service
- Health Record Relocation Service
- alle Medical Services
- Data Submission Service
- Push Notification Management

#### **[<=]**

In den folgenden Abschnitten werden zunächst die Anforderungen an eine VAU beschrieben, die sowohl von einer Aktenkontoverwaltungs-VAU als auch einer Befugnisverifikations-VAU zu erfüllen sind. Die speziellen Anforderungen an eine Aktenkontoverwaltungs-VAU bzw. an eine Befugnisverifikations-VAU folgen darauf in separaten Abschnitten.

### 3.5.1 Übergreifende VAU-Anforderungen

#### 3.5.1.1 Schutz der Integrität der VAU

Die folgenden Anforderungen stellen die Integrität der VAU sicher.

##### **A\_24613 -ePA-Aktensystem - Bildung Hashwertrepräsentation des VAU-Images**

Der Hersteller des VAU-Images MUSS für seine zugelassenen VAU-Images Hashwertrepräsentationen bilden. Diese MÜSSEN signiert und die signierten Hashwertrepräsentationen an die gematik übermitteln. Dabei SOLLEN bezüglich der kryptographischen Vorgaben zur Signatur die Vorgaben aus [gemSpec\_Krypt] eingehalten werden. [≤]

Erläuterung zu A\_24613-\*:

Bei Intel-SGX sind die durch die Intel-Hardware erzeugten Signaturen RSA-3072-Bit-Signaturen, bei denen der öffentliche Exponent 3 ist. Dies entspricht nicht den Vorgaben in [gemSpec\_Krypt] für allgemeine RSA-Signaturen (also nicht im SGX-Kontext). Deshalb steht in A\_24613-\* diesbezüglich nur eine SOLL-Formulierung. Im Kontext SGX ist der öffentliche RSA-Exponent 3 zulässig.

##### **A\_24642 -ePA-Aktensystem - Ausschluss von Manipulationen an der Hardware der VAU**

Die VAU MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Betreiber des ePA-Aktensystems ausschließen. [≤]

##### **A\_24616 -ePA-Aktensystem - Attestierung des VAU-Images und der VAU-Hardware beim Start**

Das ePA-Aktensystem MUSS beim Start einer VAU das genutzte VAU-Image sowie die VAU-Hardware, auf der die VAU ausgeführt werden soll, kryptographisch attestieren und ein signiertes VAU-Attestierungstoken erzeugen, welches vom VAU-HSM geprüft werden kann. [≤]

##### **A\_24684 -ePA-Aktensystem - Hardwarebasierter Vertrauensanker für Attestierung der VAU**

Das ePA-Aktensystem MUSS sicherstellen, dass der kryptographische Vertrauensanker für die Attestierung des VAU-Images und der VAU-Hardware in einem hardwarebasierten sicheren Schlüsselspeicher gesichert ist. [≤]

##### **A\_24617 -ePA-Aktensystem - Betreiberunabhängiger Vertrauensanker für Attestierung der VAU**

Das ePA-Aktensystem MUSS sicherstellen, dass der kryptographische Vertrauensanker für die Attestierung des VAU-Images und der VAU-Hardware nicht in der Hoheit des Betreibers des Aktensystems liegt. [≤]

*Hinweis zu A\_24617: Mit der Anforderung soll die Bedrohung abgewehrt werden, dass sich einzelne Innentäter beim Betreiber des ePA-Aktensystems eigene VAU-Software oder VAU-Hardware mit Schwachstellen erstellen und sich für diese einen falschen Hashwert attestieren, der dem VAU-HSM bekannt ist.*

##### **A\_24620 -ePA-Aktensystem - Attestierung durch Systeme außerhalb der VAU zur Laufzeit**

Das ePA-Aktensystem MUSS technisch ermöglichen, dass Änderungen an der VAU-Software und der VAU-Hardware während der Laufzeit durch Systeme außerhalb der VAU automatisiert geprüft werden können. [≤]

*Hinweis: Die gematik soll regelmäßig die Integrität der Aktensysteme prüfen können.*

### 3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU

Die folgenden Anforderungen der VAU stellen sicher, dass die innerhalb der VAU verarbeiteten Daten technisch geschützt werden.

#### **A\_24621 -ePA-Aktensystem - Äußere Isolation der VAU von Datenverarbeitungsprozessen des Betreibers**

Die VAU MUSS die in ihr ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Betreibers technisch trennen und damit gewährleisten, dass der einzelne Mitarbeiter des Betreibers vom Zugriff auf die in der VAU verarbeiteten Daten technisch ausgeschlossen ist. [ $\leq$ ]

#### **A\_24638 -ePA-Aktensystem - Schutz der Daten vor physischem Zugang zu Systemen der VAU**

Die VAU MUSS mit technischen Mitteln sicherstellen, dass bei einem physischen Zugang zu Hardware-Komponenten der VAU keine Daten aus der VAU extrahiert oder manipuliert werden können. [ $\leq$ ]

#### **A\_24651 -ePA-Aktensystem - Betreiber ergreift Maßnahmen gegen physische Angriffe auf die VAU**

Der Betreiber des ePA-Aktensystems MUSS mit technischen und/oder organisatorischen Maßnahmen ausschließen, dass ein einzelner Innentäter beim Betreiber des ePA-Aktensystems physische Angriffe auf eine VAU ausführen kann. [ $\leq$ ]

#### **A\_24641 -ePA-Aktensystem - Löschen aller Daten beim Beenden einer VAU-Instanz**

Das ePA-Aktensystem MUSS sicherstellen, dass beim Beenden einer VAU-Instanz sämtliche Daten dieser VAU-Instanz aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [ $\leq$ ]

#### **A\_25244 -ePA-Aktensystem - x-insurantId nicht außerhalb des VAU-Kanals**

Das ePA-Aktensystem MUSS sicherstellen, dass das HTTP Header-Element mit dem Namen "x-insurantId" nicht außerhalb des VAU-Kanals gesendet wird. [ $\leq$ ]

### 3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU

#### **A\_26314 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Daten**

Das ePA-Aktensystem MUSS sicherstellen, dass eine VAU-Daten, die im System des Aktensystembetreibers gespeichert werden sollen und für die keine spezifischen Anforderungen zum Schutz der gespeicherten Daten existieren, ausschließlich verschlüsselt gespeichert werden und der verwendete Verschlüsselungsschlüssel mittels der Regel hsm-r8 vom VAU-HSM abgeleitet wird. [ $\leq$ ]

Hinweise zu A\_26314:

- Spezifische Anforderungen zum Schutz der gespeicherten Daten gibt es z.B. für die Aktenkontoverwaltungs-VAU in Abschnitt 3.5.2.2 und die durch die VAU für den Betrieb erstellten Protokolle in Abschnitt 3.5.1.5.
- Außerhalb der VAU verschlüsselt gespeicherte Daten der ePA3.0, die bisher nicht mit Regel hsm-r8 verschlüsselt sein konnten, sind beim Öffnen der Akte umzuschlüsseln und mit einem Schlüssel zu sichern, der mit Regel hsm-r8 abgeleitet wird. Eine Umschlüsselung ohne Öffnen der Akte ist nicht erforderlich.

#### **A\_26322 -ePA-Aktensystem - Unterschiedliche Schlüssel für die Verschlüsselung von außerhalb der VAU gespeicherten Daten bei unterschiedlichen Verarbeitungszwecken**

Falls Daten außerhalb der VAU im System des Aktensystembetreibers gespeichert werden, MUSS das ePA-Aktensystem sicherstellen, dass für die Verschlüsselung von Daten, die zu unterschiedlichen Zwecken verarbeitet werden, unterschiedliche Verschlüsselungsschlüssel genutzt werden. [ $\leq$ ]

Hinweis zu A\_26322: Verarbeitungszwecke für Daten sind beispielsweise die Verarbeitung von Daten zum Zwecke der Sekundärnutzung ( siehe Data Submission Service) oder die Verarbeitung von Daten für die Nutzerverwaltung im Aktensystem (insbesondere Geräteinformationen und E-Mail-Adressen).

### **3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM**

#### **A\_24653 -ePA-Aktensystem - Sichere Verbindung zwischen VAU und VAU-HSM**

Das ePA-Aktensystem MUSS technisch sicherstellen, dass zwischen einer VAU und einem VAU-HSM eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen. [≤]

### **3.5.1.5 Logging und Monitoring**

Hinweis: Die Anforderungen dieses Abschnitts könnten sich noch ändern, falls sich bei der Umsetzung des ePA-Aktensystems herausstellt, dass weitere Protokollierungen auf Seiten des Betreibers notwendig werden.

#### **A\_24910 -ePA-Aktensystem - Erlaubte Zwecke der Betreiberprotokolle**

Der Betreiber des Aktensystems MUSS sicherstellen, dass die durch die VAU für den Betrieb erstellten Protokolle des Betreibers ausschließlich zum Zwecke der Fehleranalyse und -behebung anlassbezogen sowie zum Zwecke des Security Monitorings verwendet werden. [≤]

#### **A\_24649 -ePA-Aktensystem - Datenschutzkonformes Logging und Monitoring der VAU**

Die VAU MUSS die für den Betrieb des ePA-Aktensystems erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dem Betreiber des ePA-Aktensystems vertrauliche oder zur unautorisierten Profilbildung geeignete Daten zur Kenntnis gelangen. [≤]

#### **A\_24695 -ePA-Aktensystem - Keine medizinische Informationen in VAU-Protokollen des Betreibers**

Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten Protokollen des Betreibers keine personenbezogenen medizinischen Informationen enthalten sind (u. a. medizinische Daten von Versicherten oder Informationen, aus denen sich ableiten lässt, bei welchen Leistungserbringerinstitutionen ein Versicherter in Behandlung ist).

[≤]

#### **A\_24909 -ePA-Aktensystem - Nicht KVNR und Telematik-ID gemeinsam protokollieren**

Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten Protokollen des Betreibers höchstens die KVNR oder höchstens die Telematik-ID enthalten ist, aber nicht eine Kombination aus KVNR und Telematik-ID und keine solche Verbindung über mehrere Protokolle hergestellt werden kann. [≤]

#### **A\_24719 -ePA-Aktensystem - Kein kryptographisches Schlüsselmaterial in VAU-Protokollen des Betreibers**

Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten Protokollen des Betreibers kein kryptographisches Schlüsselmaterial enthalten ist. [≤]

#### **A\_24911 -Löschfristen Protokolle**

Das ePA-Aktensystem MUSS sicherstellen, dass die

- zum Zwecke der Fehleranalyse erhobenen Protokolle nach Behebung des Fehlers unverzüglich gelöscht werden,



- zum Zwecke des Security Monitorings erhobenen Protokolle nach 3 Monaten gelöscht werden.

[<=]

#### **A\_26316 -Anbieter ePA-Aktensystem - Schutz der Protokolle des Betreibers**

Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die durch die VAU für den Betrieb erstellten Protokolle des Betreibers durch technische und organisatorische Maßnahmen vor einer missbräuchlichen Nutzung geschützt werden.[<=]

#### **gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik**

Hinweis zu A\_27336-\*: Der geheime Schlüssel für die Pseudonymisierung muss nicht im VAU-HSM gespeichert werden.

#### **A\_27333 -ePA-Aktensystem - Geheimer Schlüssel für Pseudonymisierung der gematik-Logdaten nur in VAU**

Das ePA-Aktensystem MUSS sicherstellen, dass der für die Pseudonymisierung der Logdaten gemäß A\_27332-\* benötigte geheime Schlüssel key\_pn\_log im Klartext ausschließlich innerhalb einer VAU-Instanz verarbeitet wird.[<=]

#### **A\_27336 -ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung im 4-Augen-Prinzip**

Das ePA-Aktensystem MUSS sicherstellen, dass der für die Pseudonymisierung der Logdaten gemäß A\_27332-\* benötigte geheime Schlüssel key\_pn\_log ausschließlich im 4-Augen-Prinzip ins ePA-Aktensystem eingebracht werden kann.[<=]

#### **A\_27334 -ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung der gematik-Logdaten im 4-Augen-Prinzip**

Der Betreiber des ePA-Aktensystems MUSS den für die Pseudonymisierung der Logdaten gemäß A\_27332-\* benötigten geheimen Schlüssel key\_pn\_log ausschließlich im 4-Augen-Prinzip mit der gematik ins ePA-Aktensystem einbringen.[<=]

#### **A\_27335 -ePA-Aktensystem - Wechsel des Schlüssels für Pseudonymisierung der gematik-Logdaten**

Der Betreiber des ePA-Aktensystems MUSS den für die Pseudonymisierung der Logdaten gemäß A\_27332-\* benötigten geheimen Schlüssel key\_pn\_log spätestens nach 1 Jahr wechseln.[<=]

### **3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU**

#### **3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU**

##### **A\_24636-01 -ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen innerhalb einer VAU-Instanz**

Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb einer VAU-Instanz zwischen Health Record Contexten bzw. User Sessions keine Informationsflüsse auftreten können.[<=]

##### **A\_27534 -ePA-Aktensystem - Kein gemeinsamer Speicher von Datenverarbeitungsprozessen innerhalb einer VAU-Instanz**

Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb einer VAU-Instanz von einem Health Record Context bzw. einer User Sessions nicht auf den Speicher anderer Health Record Contexte bzw. User Sessions zugegriffen werden kann.[<=]

Hinweis zu A\_24636-\* und A\_27534-\*: Die in den Anforderungen geforderten technischen Maßnahmen beziehen sich ausschließlich auf den Regelfall der Datenverarbeitung ("Gutfall").

#### **A\_27535 -ePA-Aktensystem - Maximale Lebensdauer von VAU-Instanzen**

Das ePA-Aktensystem MUSS sicherstellen, dass VAU-Instanzen einer Aktenkontoverwaltungs-VAU nach maximal 24 Stunden beendet werden. [≤]

#### **A\_24885 -ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen unterschiedlicher VAU-Instanzen**

Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der unabhängig vom Separationsmechanismus in A\_24636-\* ist, ausschließen, dass sich Verarbeitungen in einer VAU-Instanz schadhaft auf die Verarbeitungen einer anderen VAU-Instanz auswirken können.

[≤]

#### **A\_24637 -ePA-Aktensystem - Maximale Health Record Context in einer VAU-Instanz**

Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Health Record Context gleichzeitig in einer VAU-Instanz laufen können.

[≤]

#### **A\_25028 -ePA-Aktensystem - Keine Kommunikation zwischen Aktenkontoverwaltungs-VAUs**

Das ePA-Aktensystem MUSS sicherstellen, dass es keine direkte Kommunikation zwischen VAU-Instanzen von Aktenkontoverwaltungs-VAUs gibt. [≤]

#### **A\_26111 -ePA-Aktensystem - Keine Kommunikation zwischen Health Record Contexts**

Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer Aktenkontoverwaltungs-VAU-Instanz keine Kommunikation zwischen Health Record Contexts gibt. [≤]

#### **A\_24639 -ePA-Aktensystem - Löschen aller Daten beim Beenden eines Health Record Context**

Die VAU MUSS sicherstellen, dass beim Beenden eines Health Record Context sämtliche Daten dieses Health Record Context aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [≤]

#### **A\_24640 -ePA-Aktensystem - Löschen aller Daten beim Beenden einer User Session**

Die VAU MUSS sicherstellen, dass beim Beenden einer User Session sämtliche Daten dieser User Session aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [≤]

*Hinweis zu A\_24639-\*, A\_24640-\* und A\_24648-\*: Eine zeitliche Verzögerung des Löschens ist tolerabel, sofern ein sofortiges Löschen aufgrund der Architektur des Aktensystemherstellers aus Performanzgründen nicht sinnvoll ist. In diesem Fall ist ein geeigneter Kompromiss zwischen dem Löschzeitpunkt und der Performanz zu wählen.*

#### **A\_25231 -ePA-Aktensystem - Schließen des Health Record Context beim Beenden einer User Session**

Die VAU MUSS sicherstellen, dass beim Beenden einer User Session alle mit dieser User Session verknüpften Health Record Context beendet werden, wenn der jeweilige Health Record Context nicht mit mindestens einer weiteren User Session verknüpft ist. [≤]

#### **A\_25051 -ePA-Aktensystem - VAU-Kanal endet immer in einer Aktenkontoverwaltungs-VAU**

Die VAU MUSS sicherstellen, dass ein VAU-Kanal von einem Client der ePA (ePA-Client oder ePA-FdV) ausschließlich in einer Aktenkontoverwaltungs-VAU endet. [≤]

Hinweis: Der VAU-Kanal darf z.B. nicht in einer Befugnisverifikations-VAU enden.

### 3.5.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-VAU

Die folgenden Anforderungen gewährleisten den Schutz der beim Betreiber des ePA-Aktensystems persistierten Daten von Aktenkonten. Die Verschlüsselung der Daten eines Versicherten erfolgt mit seinem versichertenindividuellen Daten- und Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel sind in [gemSpec\_Krypt#3.15.2] festgelegt.

#### **A\_24643 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Daten mit dem Datenpersistierungsschlüssel**

Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten

1. Daten des FHIR-Data Service
2. Daten des XDS Document Service
3. Daten des Audit Event Service (Protokolle für den Versicherten zum Zwecke der Datenschutzkontrolle)
4. Daten des Constraint Managements (Policies zu verborgenen Daten)
5. Daten des Consent Managements (Widersprüche des Versicherten)

vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health Record Context mit dem zum Health Record gehörenden versichertenindividuellen Datenpersistierungsschlüssel verschlüsselt werden.

[<=]

#### **A\_24644 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Befugnissen mit dem Befugnispersistierungsschlüssel**

Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten Daten des Entitlement Managements, d. h. Befugnisse und Befugnisverbote, vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health Record Context mit dem zum Health Record gehörenden versichertenindividuellen Befugnispersistierungsschlüssel verschlüsselt werden.[<=]

### 3.5.2.3 Konsistenz des Systemzustands

#### **A\_24650 -ePA-Aktensystem - Konsistenter Systemzustand eines Health Record Context**

Die VAU MUSS sicherstellen, dass ein konsistenter Zustand eines Health Record Context auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw. wiederhergestellt werden kann.[<=]

#### **A\_24696 -ePA-Aktensystem - Konsistenz bei parallelen Zugriffen**

Die VAU MUSS auch bei parallelen Zugriffen auf dasselbe Aktenkonto durch mehrere Nutzer immer einen konsistenten Zustand des Aktenkontos gewährleisten.[<=]

### 3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU

Eine Befugnisverifikations-VAU ist eine spezielle VAU, in der ausschließlich das Befugnisverifikations-Modul ausgeführt wird.

#### **A\_24646 -ePA-Aktensystem - Befugnisverifikations-VAU verarbeitet ausschließlich ein Befugnisverifikations-Modul**

Das ePA-Aktensystem MUSS sicherstellen, dass in einer Befugnisverifikations-VAU ausschließlich ein Befugnisverifikations-Modul ausgeführt wird.[<=]

#### **A\_24647 -ePA-Aktensystem - Befugnisverifikations-VAU speichert keine Daten**

Eine Befugnisverifikations-VAU DARF die Daten, die sie im Rahmen der Regeln des Befugnisverifikations-Moduls verarbeitet, NICHT außerhalb der Befugnisverifikations-VAU speichern. [≤]

Eine Befugnisverifikations-VAU darf insbesondere die vom VAU-HSM abgeleiteten versichertenindividuellen Persistierungsschlüssel nicht speichern.

#### **A\_24648 -ePA-Aktensystem - Befugnisverifikations-VAU löscht Daten nach Regelbearbeitung**

Eine Befugnisverifikations-VAU MUSS sämtliche Daten, die sie im Rahmen eines Regelaufrufs des Befugnisverifikations-Moduls verarbeitet, sofort nach Abarbeitung der Regel sicher aus der Befugnisverifikations-VAU löschen bzw. einen Zugriff auf diese Daten technisch ausschließen. [≤]

#### **A\_24671 -ePA-Aktensystem - Sichere Verbindung zwischen VAU-Instanzen**

Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer VAU-Instanz einer Befugnisverifikations-VAU und einer VAU-Instanz einer Aktenkontoverwaltungs-VAU eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen. [≤]

#### **A\_24856 -ePA-Aktensystem - Private Authentisierungsschlüssel für sichere Verbindung zwischen VAU-Instanzen**

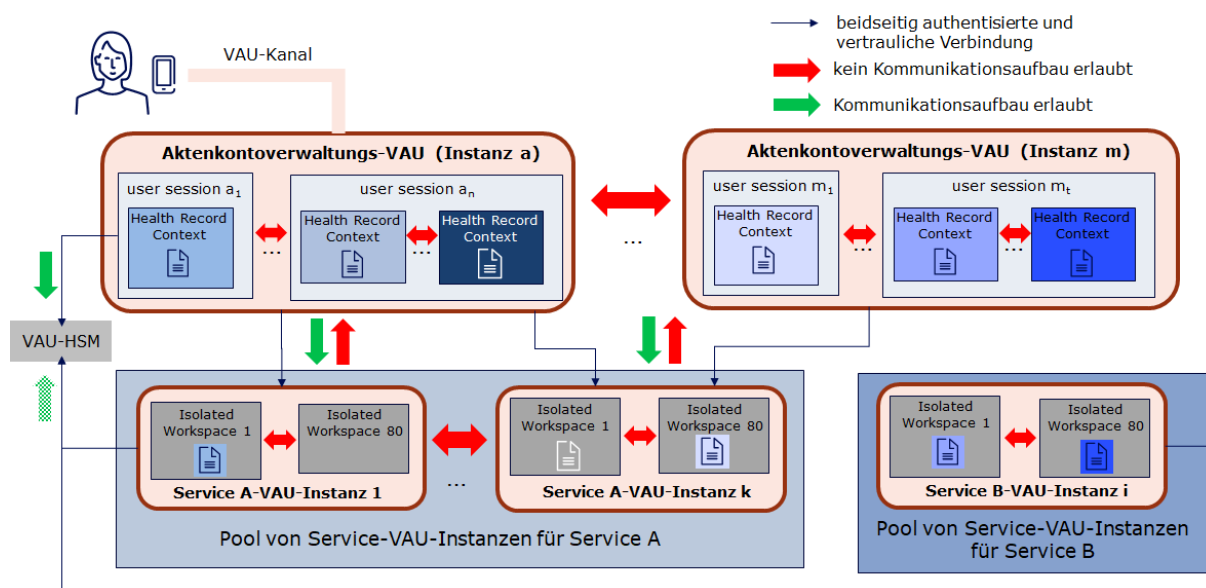
Das ePA-Aktensystem MUSS sicherstellen, dass sich die VAU-Instanzen bei einer Verbindung zwischen einer VAU-Instanz einer Befugnisverifikations-VAU und einer VAU-Instanz einer Aktenkontoverwaltungs-VAU mit privaten Schlüsseln authentisieren, die ausschließlich über die jeweilige VAU-Instanz nutzbar sind. [≤]

### **3.5.4 Zusätzliche Anforderungen an eine Service-VAU**

Spezielle Funktionen der “ePA für alle” können in eigenen, von den Aktenkontoverwaltungs-VAUs (AK-VAU) getrennten, VAUs ausgelagert und ausgeführt werden. Diese VAUs werden als **Service-VAUs** bezeichnet. Es kann Service-VAUs für unterschiedliche Funktionen geben, so dass es dementsprechend unterschiedliche **Typen von Service-VAUs** geben kann.

Service-VAU-Instanzen können durch den Betreiber des Aktensystems gestartet und in einem Pool verwaltet werden. AK-VAU-Instanzen können bei Bedarf auf Service-VAU-Instanzen zugreifen, wenn sie den Service nutzen möchten (in Abbildung 2 mit Service A dargestellt). Ein Kommunikationsaufbau von Service-VAU-Instanzen zu AK-VAU-Instanzen ist nicht möglich.

Eine Service-VAU-Instanz kann von mehreren AK-VAU-Instanzen gleichzeitig genutzt werden (die Service-VAU-Instanz zu AK-VAU-Instanz-Beziehung ist eine n:m-Beziehung).



**Abbildung 2 - Überblick Service-VAUs**

Innerhalb einer Service-VAU-Instanz erfolgt die Verarbeitung unterschiedlicher Service-Requests in voneinander getrennten **Isolated Workspaces**. Isolated Workspaces in Service-VAUs werden analog zu den Health Record Contexts in Aktenkontoverwaltungs-VAUs geschützt.

#### **A\_26112 -ePA-Aktensystem - Maximale Isolated Workspaces in einer Service-VAU-Instanz**

Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Isolated Workspaces gleichzeitig in einer Service-VAU-Instanz laufen können. [ $\leq$ ]

#### **A\_26113-01 -ePA-Aktensystem - Isolation zwischen Isolated Workspaces innerhalb einer Service-VAU-Instanz**

Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb einer Service-VAU-Instanz zwischen Isolated Workspaces keine Informationsflüsse auftreten können.

[ $\leq$ ]

#### **A\_27537 -ePA-Aktensystem - Kein gemeinsamer Speicher von Isolated Workspaces innerhalb einer Service-VAU-Instanz**

Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb einer Service-VAU-Instanz von einem Isolated Workspace nicht auf den Speicher anderer Isolated Workspaces zugegriffen werden kann. [ $\leq$ ]

#### **A\_26114 -ePA-Aktensystem - Isolation zwischen unterschiedlichen Service-VAU-Instanzen**

Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der unabhängig vom Separationsmechanismus in A\_26113-\* ist, ausschließen, dass sich Verarbeitungen in einer Service-VAU-Instanz schadhaft auf die Verarbeitungen einer anderen Service-VAU-Instanz auswirken können. [ $\leq$ ]

#### **A\_26115 -ePA-Aktensystem - Isolated Workspace verarbeitet maximal einen Request einer AK-VAU**

Nachdem ein Isolated-Workspace einen (1) Service-Request einer Aktenkontoverwaltungs-VAU-Instanz verarbeitet hat, MUSS das ePA-Aktensystem sicherstellen, dass alle Daten des Isolated-Workspaces sicher gelöscht werden, um den Isolated-Workspace für nachfolgende Service-Requests wieder neu zu initialisieren. [ $\leq$ ]

**A\_26116 -ePA-Aktensystem - In einem Isolated Workspace sind zu einem Zeitpunkt nur Daten eines Versicherten**

Das ePA-Aktensystem MUSS sicherstellen, dass in einem Isolated Workspace zu einem Zeitpunkt ausschließlich Daten eines Versicherten verarbeitet werden können, sofern die Auswahl der zu verarbeitenden Daten durch die Logik im ePA-Aktensystem bestimmt wird. [≤]

Hinweis zu A\_26116-\*: Falls Nutzer die Daten für die Service-VAU auswählen, ohne dass das ePA-Aktensystem auf diese Daten Einfluss hat (z.B. Nutzer wählt zu konvertierende PDF-Dokumente im ePA-FdV aus) kann es dazu kommen, dass zu einem Zeitpunkt auch Daten mehrerer Versicherter in einem Isolated Workspace verarbeitet werden.

**A\_26117 -ePA-Aktensystem - Keine Kommunikation zwischen Isolated Workspaces**

Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer Service-VAU-Instanz keine Kommunikation zwischen Isolated Workspaces gibt. [≤]

**A\_26118 -ePA-Aktensystem - Keine Kommunikation zwischen Service-VAU**

Das ePA-Aktensystem MUSS sicherstellen, dass es keine Kommunikation zwischen Instanzen von Service-VAUs gibt. [≤]

**A\_26119 -ePA-Aktensystem - Service-VAUs speichern keine Daten in Aktenkonten**

Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine Daten in einem Aktenkonto eines Versicherten persistieren. [≤]

**A\_26120 -ePA-Aktensystem - Service-VAUs verarbeiten keine Identitätstoken**

Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine Identitätstoken von Nutzern verarbeiten. [≤]

**A\_26123 -ePA-Aktensystem - Service-VAU-Instanzen haben maximale Lebensdauer**

Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen nach einer definierten Lebensdauer (abhängig von der Funktionalität der Services) keine neuen Service-Requests mehr annehmen können und, nachdem die laufenden Requests abgearbeitet wurden, beendet und neu gestartet werden. [≤]

**A\_26124 -ePA-Aktensystem - Information über neuen Service-VAU-Typ**

Der Hersteller des ePA-Aktensystems MUSS die gematik über die Absicht der Einführung eines neuen Service-VAU-Typs informieren und ggf. für diesen neuen Service-VAU-Typ zu erfüllende Rahmenbedingungen abstimmen. [≤]

Hinweis zu A\_26124-\*: Hierzu gehört z.B. auch die Festlegung der maximalen Lebensdauer für den neuen Service-VAU-Typ (siehe A\_26123-\*).

**A\_26125 -ePA-Aktensystem - Starten ausschließlich attestierter Service-VAUs**

Das ePA-Aktensystem MUSS sicherstellen, dass ausschließlich attestierte Service-VAU-Instanzen gestartet werden können. [≤]

**3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU****A\_26126 -ePA-Aktensystem - Gesicherte und authentifizierte Verbindung zwischen AK-VAU- und Service-VAU-Instanzen**

Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer Aktenkontoverwaltungs-VAU-Instanz und einer Service-VAU-Instanz eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen. [≤]

**A\_26127 -ePA-Aktensystem - Kein Kommunikationsaufbau von Service-VAU-Instanzen zu AK-VAU-Instanzen**



Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine Kommunikation zu einer AK-VAU-Instanz aufbauen kann.【<=】

#### **A\_26128 -ePA-Aktensystem - Kein Aufruf von Schnittstellen von AK-VAU-Instanzen durch Service-VAU-Instanzen**

Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine Schnittstellen/Services aufrufen kann, die in einer AK-VAU-Instanz ausgeführt werden. 【<=】

### **3.6 Umschlüsselung und Überschlüsselung**

Das Kerckhoffs'sche Prinzip von 1883 ist ein Grundpfeiler der Kryptographie. Es besagt u. a. dass die Sicherheit von kryptographischen Verfahren allein von der Geheimhaltung der Schlüssel abhängen darf, und dass Schlüssel leicht auswechselbar sein müssen. Damit kryptographische Schlüssel in der Praxis ihre Sicherheitseigenschaft behalten können müssen sie einen Lebenszyklus besitzen (vgl. bspw. [NIST-SP-800-57P1]), der den regelmäßigen Austausch (Wechsel) der Schlüssel vorsieht und umsetzt. Jährlich werden aus diesem Grunde die Masterkey für Aktdaten und die Masterkey für Befugnisse erneuert (vgl. A\_15745-\* und A\_20519-\* (beide aus [gemSpec\_Krypt])). Bei dieser Erneuerung muss eine Umschlüsselung durchgeführt werden:

- Schlüssel\_alt\_KVNR = Ableitung (MK\_alt, KVNR),
- Schlüssel\_neu\_KVNR = Ableitung (MK\_neu, KVNR),
- Umschlüsselung pro Akte: Schlüssel\_alt\_KVNR -> Schlüssel\_neu\_KVNR.

Falls eine AK-VAU Zugriff auf eine Akte besitzt und zu diesem Zeitpunkt feststellt neue Masterkeys (vgl. betreiberspezifische Schlüssel A\_15745-\*) existieren, muss sie eine Umschlüsselung durchführen (A\_20519-\*). Falls eine Akte länger nicht verwendet wird, kann eine AK-VAU keinen Zugang zu den Klartexten der Akte erhalten, da sie nur nach erfolgreicher Nutzerauthentisierung vom VAU-HSM die aktenspezifischen Ableitungsschlüssel erhält. Dann kann eine AK-VAU zunächst auch keine Umschlüsselung vornehmen. Aus diesem Grunde muss eine VAU (entweder eine AK-VAU oder eine dedizierte Überschlüsselungs-VAU) eine Überschlüsselung der Chiffre der Akte vornehmen. Dafür werden Überschlüsselungsschlüssel benötigt. Es gibt analog zu den anderen betreiberspezifischen Schlüssel (A\_15745-\*) Masterkeys für eine Schlüsselableitung für die Überschlüsselung der Chiffre einer Akte.

#### **A\_26197 -ePA-Aktensystem - betreiberspezifische Schlüssel: Überschlüsselungs-Masterkeys**

Ein ePA-Aktensystem MUSS sicherstellen, dass die Menge der betreiberspezifischen Schlüssel aus [gemSpec\_Krypt#A\_15745-\*] um die Kategorie Überschlüsselungs-Masterkeys erweitert wird. Für die Überschlüsselungsschlüssel MÜSSEN die gleichen Vorgaben wie für alle betreiberspezifischen Schlüssel gemäß A\_15745-\* gelten. Die betreiberspezifischen Schlüssel werden mindestens jährlich aktualisiert (A\_20519-\*), die alten Schlüssel MÜSSEN solange im VAU-HSM verfügbar sein, solange Chiffre im Aktensystem existieren (bspw. Daten einer Akte), die mit diesen Schlüsseln kryptographisch gesichert sind.【<=】

D. h. wie in Abschnitt 3.3 (bspw. A\_24611-\*) definiert, gibt es bei den Masterkeys drei Kategorien: (1) Aktenpersistierung, (2) Befugnispersistierung und (3) Überschlüsselung. Initial startet der Betrieb eines Aktensystems mit je einem Schlüssel in den ersten zwei Kategorien. Nach maximal einem Jahr (A\_20519-\*), oder anders formuliert im nächsten Intervall, werden diese beiden ersten Schlüssel zufällig neu erzeugt. Dabei muss nun ein neuer Überschlüsselungsmasterkey erzeugt werden. Die Anzahl der Schlüssel nach o. g. Kategorie ist anschließend (1) 2, (2) 2, (3) 1.

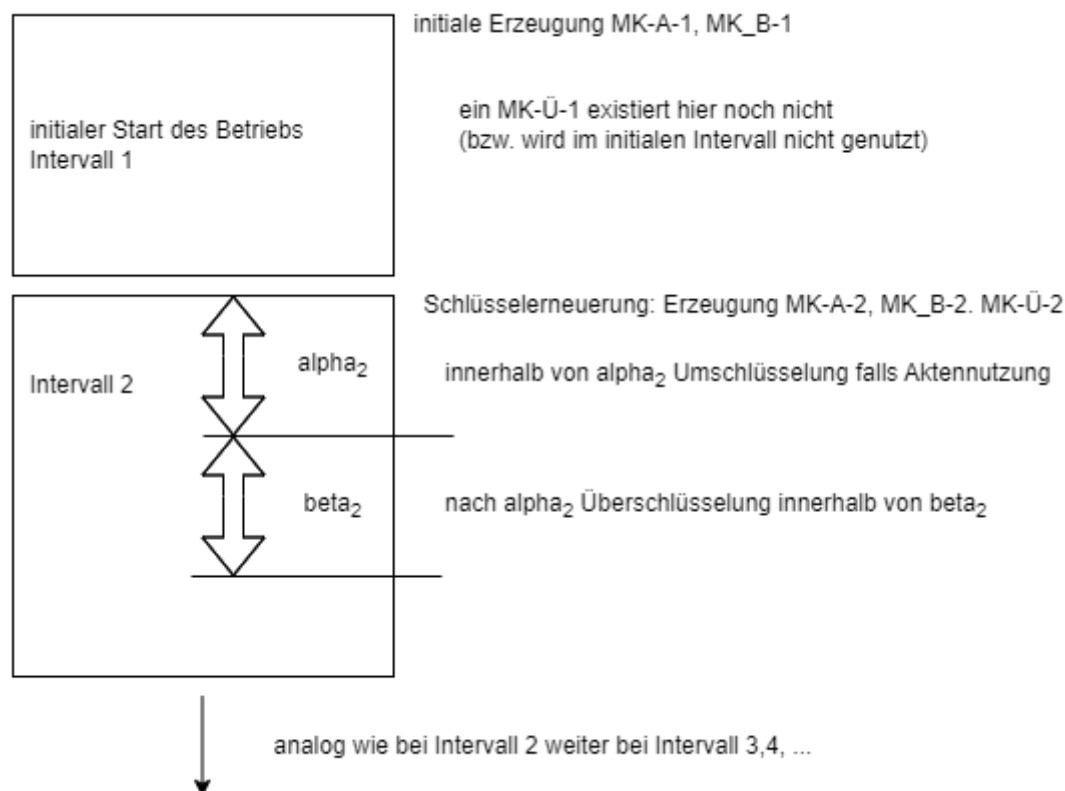


### A\_26198 -ePA-Aktensystem - neuer Überschlüsselungsschlüssel bei Erneuerung betreiberspezifischen Schlüssel

Ein ePA-Aktensystem MUSS sicherstellen, dass bei jeder Erneuerung der Masterkeys zur Aktenpersistierung ein weiterer neuer Überschlüsselungsmasterkey zufällig im VAU-HSM erzeugt wird.

[<=]

Bei einer Erneuerung der betreiberspezifischen Schlüssel gibt es verschiedene Zeitabschnitte:



**Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung**

### A\_26204 -ePA-Aktensystem - zeitliche Vorgaben zur Durchführung der Umschlüsselung und Überschlüsselung

Ein ePA-Aktensystem MUSS sicherstellen, dass es ein konfigurierbares Zeitintervall alpha gibt, so dass nach einer Schlüssel Erneuerung der betreiberspezifischen Schlüssel innerhalb von alpha bei einer Aktennutzung eine Umschlüsselung in einer AK-VAU vorgenommen wird, falls die Verschlüsselung der Akte auf einem älteren Masterkey basiert. Das Zeitintervall alpha startet jeweils direkt mit jedem neuen Intervall (Schlüssel Erneuerung der betreiberspezifischen Schlüssel).

Weiter MUSS es sicherstellen, dass es ein konfigurierbares Zeitintervall beta gibt beginnend direkt nach alpha, so dass nach ablaufen von alpha eine Überschlüsselung von Chiffren von Akten, bei denen keine Umschlüsselung (wegen Nichtaktennutzung innerhalb von alpha) durchgeführt werden konnte, vorgenommen wird.

Der Default-Wert für die Länge von alpha MUSS 100 Tage und für die Länge von beta 60 Tage betragen. ("Default-Wert" bedeutet, Wert wenn der AS-Betreiber dort keinen anderen Wert konfigurieren möchte.)

[<=]

Die folgenden zwei Anforderung geben weitere Details zu A\_26204-\*.

### **A\_26205 -ePA-Aktensystem - Umschlüsselung**

Ein ePA-Aktensystem MUSS sicherstellen, dass wenn die AK-VAU eine Akte verwendet und feststellt, dass diese Akte nicht überschlüsselt ist und die versichertenindividuelle Aktenverschlüsselung auf einem älteren Masterkey (i. S. v. eben nicht aus dem aktuellen Intervall kommend) basiert, die AK-VAU eine Umschlüsselung vornimmt. Die alten Chiffre der Akten (also die Chiffre die auf Basis eines älteren Masterkeys verschlüsselt sind), MÜSSEN im Aktensystem nach erfolgreicher Umschlüsselung gelöscht werden.

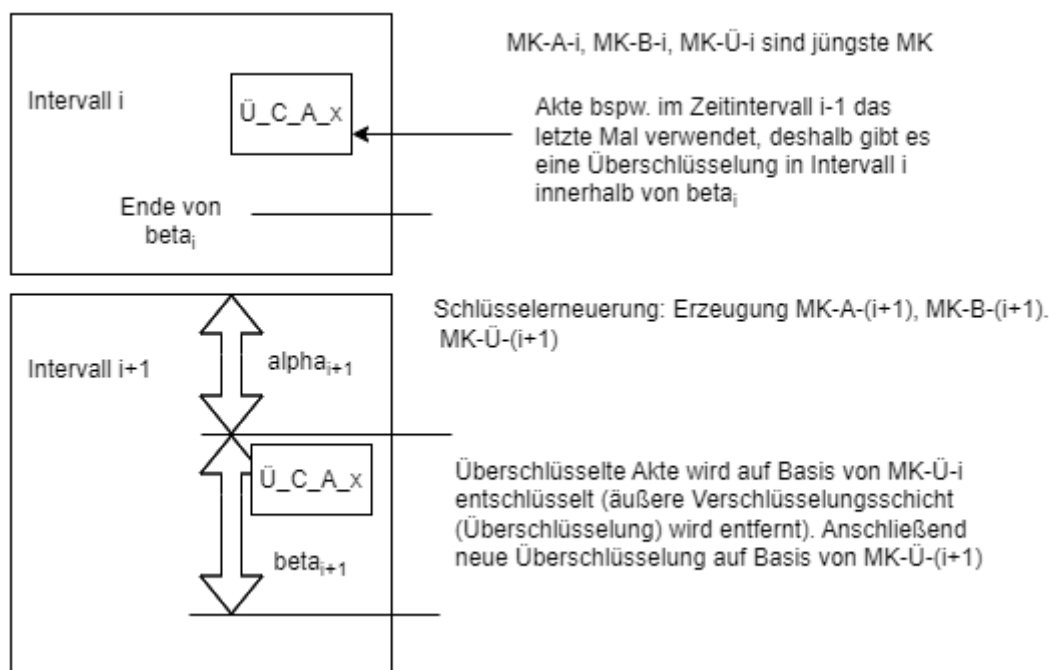
Wenn die AK-VAU eine Akte verwendet und feststellt, dass diese überschlüsselt ist, so MUSS die AK-VAU die Überschüsselung entschlüsseln und die nun verfügbare Chiffre der Akten auf Grundlage des aktuellen Masterkeys umschlüsseln. (Hinweis: nach Konstruktion muss die innere Aktenverschlüsselung auf einem älteren Masterkey basieren, ansonsten hätte keine Überschüsselung stattgefunden.) Nach erfolgreicher Umschlüsselung MÜSSEN die alten Chiffre (das Überschüsselungschiffre und das alte "innere" Chiffre der Akte) im Aktensystem gelöscht werden.【<=】

Hinweis zu A\_26205-\*: Die notwendigen aktenspezifischen Schlüssel liegen nun in der AK-VAU vor. Die Umschlüsselung muss nicht direkt sofort vor Nutzung der Akte erfolgen, sondern kann auch einige Minuten später erfolgen. Die konkrete Ausgestaltung liegt beim Hersteller.

### **A\_26206 -ePA-Aktensystem - Überschüsselung**

Ein ePA-Aktensystem MUSS sicherstellen, dass jeweils im aktuellen Intervall nach Ablauf des Zeitintervalls alpha Akten, die nicht überschlüsselt sind und deren Verschlüsselung auf einem älteren Masterkey (i. S. v. nicht aus dem aktuellen Zeitintervall) basiert, überschlüsselt werden auf Basis des aktuellen Überschüsselungs-Masterkeys. Diese Umschlüsselung MUSS jeweils innerhalb des Zeitintervalls beta für alle solche Akten abgeschlossen werden. Die "alten" Chiffre (Chiffre von solchen Akten vor der Überschüsselung) MÜSSEN im Aktensystem gelöscht werden.【<=】

Umschlüsselung einer Überschüsselung: Bei einer Akte, die länger nicht verwendet wird, kann es dazu kommen, dass überschlüsselte Akten wieder überschlüsselt werden müssen, weil alpha im nächsten Intervall abgelaufen ist. In diesem Fall wird eine Umschlüsselung mittels der Überschüsselung vorgenommen, d. h. die Verschlüsselungstiefe / -kette wird 2 nicht überschreiten -- es gibt maximal eine Überschüsselungsschicht.



**Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer Überschlüsselung**

#### **A\_26208 -ePA Aktensystem - Umschlüsselung einer Überschlüsselung**

Ein ePA-Aktensystem MUSS sicherstellen, dass jeweils in einem Intervall innerhalb von  $\beta$  überprüft wird, ob überschlüsselte Akten existieren, deren Überschlüsselung auf Basis eines alten Überschlüsselungs-Masterkeys (also aus einem früheren Intervall stammend) durchgeführt wurde. Die AK-VAU (oder eine dedizierte Überschlüsselungs-VAU) MUSS die überschlüsselten Akten umschlüsseln, d. h. die Überschlüsselung auf Grundlage eines älteren Überschlüsselungs-Masterkeys wird aufgehoben (äußere Verschlüsselungsschicht innerhalb der VAU entschlüsselt) und das Ergebnis (= Chiffre einer Akte) neu verschlüsselt auf Basis des aktuellen Überschlüsselungs-Masterkeys. Die alten Chiffre (also vor der Umschlüsselung der Überschlüsselung) MÜSSEN gelöscht werden. Das ePA-Aktensystem MUSS sicherstellen, dass nach Ablauf von  $\beta$  keine überschlüsselten Akten existieren, deren Überschlüsselung auf Basis eines Überschlüsselungsschlüssel, der nicht aus dem aktuellen Intervall stammt, durchgeführt wurde.

**[<=]**

Sollte durch irgendeinen Umstand die Sicherheitseigenschaft der Betreiberschlüssel (A\_15745-\*) in Frage stehen, so muss ein Aktensystembetreiber die Umschlüsselung bzw. die Überschlüsselung aktivieren/starten können.

#### **A\_26199 -ePA-Aktensystem - Notfall-Aktivierung Umschlüsselung/Überschlüsselung**

Ein ePA-Aktensystem MUSS sicherstellen, dass das ePA-Aktensystem es einem ePA-Betreiber ermöglicht eine Erneuerung der betreiberspezifischen Schlüssel zu starten/aktivieren. Es MUSS also dem ePA-Betreiber möglich sein neben der regelmäßigen Erneuerung der betreiberspezifischen Schlüssel (A\_205019-\*) eine Erneuerung zu initiieren.

**[<=]**

Nach A\_20519-\* muss es mindestens jährlich eine Schlüsselerneuerung geben. Mit 26199-\* kann ein ePA-Betreiber im Notfall sozusagen den Zyklus "beschleunigen" -- ein neues Intervall sofort einleiten/erzeugen.

Da die Chifftrate in einem ePA-Aktensystem mit Verschlüsselungsschlüsseln, die aus unterschiedlichen Masterkeys (aus unterschiedlichen Intervallen) abgeleitet werden, erzeugt werden können, muss an den äußeren Meta-Daten eines Chiffrats ersichtlich sein auf welchem Masterkeys sie basieren (vom welchem Masterkey sind sie abgeleitet sind).

#### **A\_26223 -ePA-Aktensystem - Metadaten von ePA-spezifischen Chiffraten**

Ein ePA-Aktensystem MUSS sicherstellen, dass bei ePA-spezifischen Daten (Datenpersistierung von Akten, überschlüsselte Aktenchifftrate, verschlüsselte Befugnisse etc.) an den äußeren (also unverschlüsselten) Meta-Daten des Chiffrat erkennbar ist mithilfe welches (oder welcher) Masterkeys die Chifftrate entschlüsselbar sind. [**<=**]

### **3.7 User Session und Health Record Context**

Die Verarbeitungen innerhalb einer VAU werden über User Sessions und Health Record Contexts voneinander getrennt.

Wenn ein ePA-Client einen VAU-Kanal zum Aktensystem aufbaut, wird dieser einer bestimmten VAU-Instanz zugeordnet, in welcher dann eine User Session für den Nutzer des ePA-Clients erzeugt wird. Nach erfolgreicher Authentifizierung des Nutzers unter Verwendung des sektoralen IDPs (Versicherte) oder des IDP-Dienstes (LEI) ist die User Session etabliert und kann durch den ePA-Client genutzt werden. Alle Verbindungen für diesen VAU-Kanal werden immer an dieselbe VAU-Instanz geleitet, die die User Session verwaltet. Eine VAU-Instanz kann mehrere User Sessions verwalten.

Wird durch den ePA-Client eine Operation für eine bestimmte Akte aufgerufen (Parameter x-insurantid) der Operation, wird in der User Session geprüft, ob diese Akte schon verwendet wird (ein anderer Nutzer gerade mit der Akte arbeitet) oder nicht. Sollte die Akte noch nicht verwendet werden, wird die Akte in einem Health Record Context geöffnet und kann durch den ePA-Client in dessen User Session verwendet werden. Existiert für die Akte schon ein geöffneter Health Record Context, darf es durch den parallelen Zugriff zu keinen Inkonsistenzen in der Akte kommen.

Innerhalb einer VAU-Instanz dürfen nur eine maximale Anzahl von Health Record Contexts gleichzeitig aufgebaut sein. Sollte diese Anzahl überschritten werden, wird der am längsten nicht genutzte Health Record Context geschlossen, um einen neuen Health Record Context öffnen zu können.

### **3.8 Consent Decision Management**

Das Consent Decision Management des Aktensystems verwaltet die Entscheidungen eines Versicherten oder eines Vertreters für oder gegen die Nutzung von definiert widerspruchsfähigen Funktionen gemäß gesetzlicher Vorgaben.

Außerdem werden im Consent Decision Management die Einschränkungen der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke durch das Forschungsdatenzentrum Gesundheit verwaltet (siehe 3.8.2- Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke ).

Der Widerspruch gegen die grundsätzliche Nutzung der ePA wird nicht im Consent Decision Management berücksichtigt. Die Existenz eines Aktenkontos für einen Versicherten impliziert, dass kein Widerspruch gegen die Nutzung der ePA erteilt wurde. Der Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger wird ebenfalls nicht hier verwaltet (siehe zu beiden Widersprüchen auch 3.1.1- Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte ).

### 3.8.1 Widersprüche für Funktionen der ePA

Die vorgehaltenen Entscheidungen zu einer Funktion umfassen dabei den Zustand "kein Widerspruch erklärt" ("permit") oder "Widerspruch erklärt" ("deny") und den Kontext einer Funktion. Der Kontext ordnet dabei die einzelnen widerspruchsfähigen Funktionen einem für die Umsetzung des Widerspruchs betroffenen Nutzerkreis zu und wird bei den zugreifenden Schnittstellen zur Filterung der Ausgabe verwendet.

Initial, also bei der Erstellung eines neuen Aktenkontos oder bei Übernahme eines existierenden ePA 2.x Aktenkontos, ist für keine widerspruchsfähige Funktion ein Widerspruch gegen die Nutzung erklärt. Ein Versicherter oder ein Vertreter kann im Verlauf der Nutzung des Aktenkontos aktiv der Verwendung von widerspruchsfähigen Funktionen widersprechen oder einen erteilten Widerspruch zurücknehmen.

Die aktuell erteilten Widersprüche können durch einen Versicherten oder einen Vertreter jederzeit über ein ePA-FdV eingesehen und geändert werden. Versicherte und Vertreter, die ein ePA-FdV nicht nutzen möchten, können eine Auskunft über die aktuell erteilten Widersprüche über die Ombudsstelle erhalten und dort auch Änderungen an den Entscheidungen im Aktenkonto veranlassen. Die Ansicht oder Änderung der Widersprüche erfolgt im Aktenkonto stets gesichert innerhalb der VAU, die aktuellen Entscheidungen zu den widerspruchsfähigen Funktionen der ePA sind versichertenindividuell mit dem SecureDataStorageKey verschlüsselt abgelegt.

Die Information über relevante erteilte oder nicht erteilte Widersprüche können Clients auf einfache Weise (ohne Authentisierung oder Etablierung eines VAU-Kanals) im Vorfeld einer Operation über den Information Service abfragen (siehe auch [3.15- Information Service](#) ).

Das Consent Decision Management des Aktenkontos spiegelt ("cached") die Entscheidungen zu den Widersprüchen für die schnelle Abfrage über den Information Service in einen Bereich, der ohne den Aufbau eines VAU-Kanals und Verwendung des versichertenindividuellen SecureDataStorageKey nutzbar ist.

Das Aktenkonto unterstützt die Durchsetzung eines erteilten Widerspruchs überall dort, wo Aktivitäten dediziert als Teil einer widerspruchsfähigen Funktion zugeordnet werden können. Beispielsweise wird das Einstellen neuer Verordnungs- und Dispensierdaten in die Ordner der Kategorie "medication" immer verhindert, wenn der Teilnahme am digital gestützten Medikationsprozess widersprochen wurde. Die konkreten Auswirkungen eines Widerspruchs sind in den jeweiligen Kapiteln zur Handhabung von Dokumenten und Daten des Aktenkontos dargestellt (siehe [3.13.1- XDS Document Service](#) und [3.13.2- FHIR Data Services](#) ).

Die jeweils berücksichtigten widerspruchsfähigen Funktionen sind wie folgt definiert. Diese Liste kann in folgenden Versionen der ePA ergänzt oder verändert werden.

#### **A\_23874-01 -Consent Decision Management - Definition der widerspruchsfähigen Funktionen der ePA**

Das Consent Decision Management MUSS die Attribute zu widerspruchsfähigen Funktionen der ePA gemäß der folgenden Tabelle verwenden.

**Tabelle 8: Widerspruchsfähige Funktionen der elektronischen Patientenakte**

Funktion (name)	Funktionsklasse (consent class)	Id der Funktion (id)	Entscheidung (consent decision)
Teilnahme am digital gestützten Medikationsprozess	Versorgungsprozess ("healthcareProcess")	"medication"	"deny"/"permit"

Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst	Versorgungsprozess ("healthcareProcess")	"erp- submission"	"deny"/"permit"
Sekundärdatennutzung durch das Forschungsdatenzentrum Gesundheit	Sekundärdatennutzung ("secondaryDataUsage")	"data- submission"	"deny"/"permit"

【<=】

*Hinweis: Die Bezeichnungen in () sind die Bezeichnungen in den Schnittstellen für den Abruf und die Verwaltung der Widersprüche. Eine widerspruchsfähige Funktion wird durch die ID der Funktion eindeutig identifiziert.*

*Hinweis: Die Verwaltung der Widersprüche gegen die Nutzung des Aktenkontos durch eine spezifische Leistungserbringerinstitution erfolgt über die Befugnisverwaltung (siehe 3.9.4- Befugnisausschluss (Blocked User Policy) ).*

Die Entscheidungen zu den widerspruchsfähigen Funktionen "medication" und "erp-submission" sind durch das Aktensystem dabei abhängig assoziiert:

#### **A\_25300 -Consent Decision Management - Untereinander abhängige Entscheidungen zu Widersprüchen**

Das Consent Decision Management MUSS durch interne Maßnahmen sicherstellen, dass bei Erteilung eines Widerspruchs gegen die Nutzung der Funktion der elektronischen Patientenakte 'erp-submission' ('deny') auch der Widerspruch gegen die Nutzung der Funktion 'medication' gesetzt wird ('deny') und dass bei der Rücknahme ('permit') des Widerspruchs gegen die Nutzung der Funktion 'medication' auch der Widerspruch gegen die Nutzung der Funktion 'erp-submission' zurückgenommen wird.【<=】

*Hinweis zu A\_25300\*: Die Änderung der Entscheidung zur Nutzung der "führenden" Funktion hat automatisch eine Entscheidung zur Nutzung der "abhängigen" Funktion zur Folge. Dieses gilt nur für die aufgeführten Entscheidungsänderungen. Alle weiteren, nicht aufgeführten, Änderungen zu Entscheidungen haben keine "abhängige" Auswirkung auf weitere Entscheidungen zu Funktionen. Beispiel: Wird die Entscheidung für 'medication' von 'permit' auf 'deny' gesetzt, so hat dieses keine weiteren Änderungen an Entscheidungen zur Folge.*

#### **A\_23766 -Consent Decision Management - Initialisierung der Widerspruchsinformation zur Nutzung von Funktionen der ePA**

Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen Patientenakte bei Erstellung eines neuen Aktenkontos oder bei Übernahme eines existierenden Aktenkontos einer älteren ePA-Version für alle Funktionen, gegen die der Versicherte nicht widersprochen hat mit der Entscheidung "kein Widerspruch erklärt" ("permit") initialisieren sowie alle Funktionen, gegen die der Versicherte widersprochen hat, mit "deny" initialisieren.

【<=】

#### **A\_24343 -Consent Decision Management - Speichern der Inhalte**

Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen Patientenakte unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.【<=】

#### **A\_23712 -Consent Decision Management - Übertrag der Widerspruchsinformation zur Nutzung von Funktionen der ePA für den Informationsdienst**



Das Consent Decision Management MUSS die aktuellen Entscheidungen zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen Patientenakte der Funktionsklassen

- Versorgungsprozess ("healthCareProcess")

sofort im Anschluss an eine Änderung der Entscheidung im Consent Decision Management für die Abfrage durch den Information Service des Aktensystems ohne Nutzung der VAU und des SecureAdminStorageKeys verfügbar machen.

[<=]

#### **A\_24040 -Consent Decision Management - Periodischer Übertrag der Widerspruchsinformation zur Nutzung von Funktionen der ePA für den Informationsdienst**

Das Consent Decision Management MUSS die aktuellen Entscheidungen zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen Patientenakte der Funktionsklassen

- Versorgungsprozess ("healthCareProcess")

bei jedem Start der VAU (des VAU-Kanals) für die Abfrage durch den Information Service des Aktensystems ohne Nutzung der VAU und des SecureAdminStorageKeys verfügbar machen, unabhängig von einer Änderung der Entscheidungen zu den Widersprüchen.

[<=]

Clients der Ombudsstelle und aus der Umgebung des Versicherten nutzen das Consent Decision Management über die Operationen der Schnittstelle I\_Consent\_Decision\_Management. Clients aus der Umgebung der LEI und der E-Rezept-Fachdienst nutzen für die schnelle Abfrage die Operation der Schnittstelle I\_Information\_Service.

#### **A\_23824 -Aktensystem - Realisierung der Schnittstelle I\_Consent\_Decision\_Management**

Das ePA-Aktensystem MUSS die Operationen der Schnittstelle I\_Consent\_Decision\_Management gemäß [I\_Consent\_Decision\_Management] umsetzen.

[<=]

#### **A\_23919 -Consent Decision Management - unveränderte Übernahme der Widerspruchsentscheidung**

Das Consent Decision Management MUSS die über Operationen der Schnittstellen des Consent Managements übermittelten Entscheidungen (consent decisions) zu widerspruchsfähigen Funktionen der ePA in das Aktenkonto übernehmen. Die Entscheidungen zu den in den Operationen nicht adressierten widerspruchsfähigen Funktionen MÜSSEN im Aktenkonto unverändert bleiben.[<=]

#### **A\_24844 -Consent Decision Management - Information über Änderungen der Widerspruchsinformation**

Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung einer Widerspruchsinformation, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber informieren, dass Widerspruchsinformationen geändert wurden, wann die Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind.[<=]

#### **A\_24055 -Consent Decision Management - Protokollierung geänderter Entscheidungen zu Widersprüchen**

Das Consent Decision Management MUSS Bei Änderungen von Entscheidungen zu den widerspruchsfähigen Funktionen der ePA jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen. Für die Wertebelegung ist A\_23874\* zu berücksichtigen und die Protokollstruktur entsprechend zu belegen:



**Tabelle 9: Consent Decision Management Protokollierung - Widersprüche für Funktionen der ePA**

Strukturelement	Wert		Erläuterung
AuditEvent.action	U		Update
AuditEvent.entity.name	"ConsentDecision"		Eintrag protokolliert eine Widerspruchsentscheidung
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"ConsentClass"	<consent class"	z.b. "healthcareProcess"
	"ConsentClassId"	<consent class Id>	z.b. "medication"
	"ConsentDecision"	<consent decision>	"deny" oder "permit"

**[<=]**

*Hinweis: Die initiale Entscheidung zu den Widersprüchen bei Anlage eines Aktenkontos wird nicht protokolliert. Die spezifische Protokollierung erfolgt für Folgeänderungen.*

Ein Aufruf der Operationen der Schnittstelle I\_ConsentDecisionManagement zur Änderung der Entscheidungen zu den Widersprüchen gegen die Nutzung von widerspruchsfähigen Funktionen der ePA kann erfolgreich beendet werden, ohne dass eine bisher gespeicherte Entscheidung zu diesen Widersprüchen im Aktensystem geändert wird. In diesem Fall erfolgt die Protokollierung gemäß A\_27883-\*.

#### **A\_27883 -Consent Decision Management - Protokollierung unveränderter Entscheidungen zu den widerspruchsfähigen Funktionen der ePA**

**Das Consent Decision Management MUSS für jede versuchte Änderung der Entscheidungen zu den Widersprüchen gegen die Sekundärnutzung von Daten, welche nicht durch einen Fehler abgelehnt wird und welche zu keiner Änderung einer gespeicherten Entscheidung führt ('leere' Änderung, keine Änderung der Einstellungen zu DataUsagePurposes ), einen Protokolleintrag gemäß A\_24704\* erzeugen:**

**Tabelle 10: Consent Decision Management Protokollierung - unveränderte Entscheidungen zu widerspruchsfähigen Funktionen der ePA**

Strukturelement	Wert	Erläuterung
AuditEvent.action	U	Update
AuditEvent.entity.name	"ConsentDecision"	Protokollierte Aktivität zuConsentDecisions
AuditEvent.entity.description	<operationId>	Id der verwendeten Operation (operationId gemäß Schnittstellenbeschreibung)

--	--	--

[&lt;=]

### 3.8.2 Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke

Wenn kein Widerspruch gegen die Sekundärdatennutzung durch das FDZ für das Aktenkonto erteilt wurde, kann durch den Versicherten oder einen Vertreter über das ePA FdV, bzw. durch die Ombudsstelle, die Verwendung der Daten auf die in § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszwecke im FDZ eingeschränkt werden.

Der initiale Zustand nach Aktivierung eines Aktenkontos ist für jeden Sekundärnutzungszweck "kein Widerspruch erteilt".

Eine Änderung der Widersprüche zu Verwendungszwecken führt dazu, dass diese Informationen an das Forschungsdatenzentrum Gesundheit übermittelt werden. Die Widersprüche des Versicherten in die Sekundärnutzungszwecke sind dort bindend für die Verarbeitung der übermittelten pseudonymisierten medizinischen Daten, siehe auch [3.20-Data Submission Service](#).

#### **A\_26286 -Consent Decision Management - Initialisierung der Sekundärnutzungszwecke**

Das Consent Decision Management MUSS jeden in § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszweck der elektronischen Patientenakte bei Erstellung eines neuen Aktenkontos oder bei Übernahme eines existierenden Aktenkontos einer älteren ePA-Version mit der Entscheidung "kein Widerspruch erklärt" ("permit") initialisieren.[<=]

#### **A\_26287 -Consent Decision Management - Speichern der Entscheidungen zu Sekundärnutzungszwecken**

Das Consent Decision Management MUSS die Entscheidungen zu Sekundärnutzungszwecken der elektronischen Patientenakte unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.[<=]

#### **A\_26288 -Consent Decision Management - Übertragen der Entscheidungen zu Sekundärnutzungszwecken an das FDZ**

Das Consent Decision Management MUSS die Entscheidungen zu Sekundärnutzungszwecken sofort im Anschluss an eine Änderung der Entscheidung im Consent Decision Management in das Paket zur Übermittlung von pseudonymisierten medizinischen Daten zu Sekundärnutzungszwecken an das FDZ aufnehmen.[<=]

#### **A\_26291 -Consent Decision Management - unveränderte Übernahme der Widerspruchsentscheidung zu Sekundärnutzungszwecken**

Das Consent Decision Management MUSS die über Operationen der Schnittstellen des Consent Managements [I\_Consent\_Decision\_Management] übermittelten Entscheidungen zu Sekundärnutzungszwecken in das Aktenkonto übernehmen.[<=]

#### **A\_26292 -Consent Decision Management - Information über Änderungen der Entscheidungen zu Sekundärnutzungszwecken**

Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung der Entscheidungen zu Sekundärnutzungszwecken, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber informieren, dass Entscheidungen zu Sekundärnutzungszwecken geändert wurden, wann die Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind.[<=]

#### **A\_26294 -Consent Decision Management - Weiterleitung von Widersprüchen gegen Sekundärnutzungszwecken an das FDZ**

Das Consent Decision Management MUSS die Information über einen erklärten Widerspruch gegen Sekundärnutzungszwecke über den Data Submission Service an das FDZ weiterleiten. [≤]

#### **A\_26310 -Consent Decision Management - Rücknahme des Widerspruchs gegen die Sekundärdatennutzung durch das FDZ**

Falls ein Widerspruch gegen die Sekundärdatennutzung durch das FDZ zurückgenommen wird MUSS das Consent Decision Management die Entscheidungen zu Sekundärnutzungszwecken über den Data Submission Service an das FDZ weiterleiten. [≤]

#### **A\_26308 -Consent Decision Management - Protokollierung geänderter Entscheidungen zu Sekundärnutzungszwecken**

Das Consent Decision Management MUSS bei jeder Änderung einer Widerspruchsentscheidung zur Verwendung der an das Forschungsdatenzentrum übermittelten Daten für bestimmte Sekundärnutzungszwecke einen Protokolleintrag gemäß A\_24704\* erzeugen.

**Tabelle 11: Consent Decision Management Protokollierung - Widersprüche zu Sekundärnutzungszwecken**

Strukturelement	Wert		Erläuterung
AuditEvent.action	U		Update
AuditEvent.entity.name	"DataUsagePurpose"		Eintrag protokolliert eine Widerspruchsentscheidung zu Sekundärnutzungszwecken
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	Liste aller geänderten Widersprüche zu Sekundärnutzungszwecken
	"Purpose"	<purpose Id>	Auswahl aus <purpose Id> mit den Werten: [Purpose1, Purpose2, Purpose3, Purpose4, Purpose5, Purpose6, Purpose7, Purpose8, Purpose9, Purpose10]
	"ConsentDecision"	<consent decision>	"deny" oder "permit"

[≤]

Ein Aufruf der Operationen der Schnittstelle I\_ConsentDecisionManagement zur Änderung der Entscheidungen zur den Widersprüchen gegen die Verwendung von Daten für Sekundärnutzungszwecke kann erfolgreich beendet werden, ohne dass eine bisher gespeicherte Entscheidung zu diesen Widersprüchen im Aktensystem geändert wird. In diesem Fall erfolgt die Protokollierung gemäß A\_27869-\*.

#### **A\_27869 -Consent Decision Management - Protokollierung unveränderter Entscheidungen zu Sekundärnutzungszwecken**

Das Consent Decision Management MUSS für jede versuchte Änderung der Entscheidungen zu den Widersprüchen gegen die Sekundärnutzung von Daten, welche nicht durch einen Fehler abgelehnt wird und welche zu keiner Änderung einer gespeicherten Entscheidung führt ('leere' Änderung, keine Änderung der Einstellungen zu DataUsagePurposes ), einen Protokolleintrag gemäß A\_24704\* erzeugen:

**Tabelle 12: Consent Decision Management Protokollierung - unveränderte Widersprüche zu Sekundärnutzungszwecken**

Strukturelement	Wert	Erläuterung
AuditEvent.action	U	Update
AuditEvent.entity.name	"DataUsagePurpose"	Protokollierte Aktivität zuDataUsagePurpose
AuditEvent.entity.description	<operationId>	Id der verwendeten Operation (operationId gemäß Schnittstellenbeschreibung)

[&lt;=]

**A\_26293 -Consent Decision Management - Weiterleitung von Widersprüchen gegen die Sekundärdatennutzung durch das FDZ**

Das Consent Decision Management MUSS die Information über einen erklärten Widerspruch gegen die Sekundärdatennutzung durch das FDZ über den Data Submission Service an das FDZ weiterleiten.[<=]

**3.8.3 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny Policy Medication)**

Ein Versicherter bzw. Vertreter kann den Zugriff auf den Medication Service für bestimmte LEI innerhalb seines Aktenkontos einschränken und diese Einschränkung auch wieder zurücknehmen. Durch das Setzen einer LEI auf eine User Specific Deny Policy Medication wird jeder Zugriff dieser LEI auf den Medication Service und auf die Dokumente der Kategorie "emp" des XDS Document Service für das Aktenkonto mit einem Fehler abgebrochen. Durch das Entfernen einer LEI von der User Specific Deny Policy Medication kann diese LEI Operationen des Medication Service (falls kein Widerspruch gegen "medication" vorliegt) wieder nutzen und auf die Dokumente der Kategorie "emp" des XDS Document Service zugreifen.

Die User Specific Deny Policy Medication wird durch das Aktensystem für die in A\_26406-\* aufgeführten Nutzergruppen angewendet und durchgesetzt.

Der initiale Zustand nach Aktivierung eines Aktenkontos ist eine leere Liste.

**A\_26400 -Consent Decision Management - Initialisierung der User Specific Deny Policy Medication**

Das Consent Decision Management MUSS für ein Aktenkonto eine User Specific Deny Policy Medication ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policy über die Schnittstelle I\_Consent\_Decision\_Management gemäß [I\_Consent\_Decision\_Management] ermöglichen.[<=]

**A\_26401 -Consent Decision Management - Speichern der Inhalte der User Specific Deny Policy Medication**

Das Consent Decision Management MUSS Einträge aus der User Specific Deny Policy Medication unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.[<=]

**A\_26403 -Consent Decision Management - Information über Änderungen der User Specific Deny Policy Medication**

Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung der Entscheidungen zu der User Specific Deny Policy Medication , sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber informieren, welche Änderungen der User Specific Deny Policy Medication vorgenommen wurden, wann die Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind. [≤]

#### **A\_26406-01 -Consent Decision Management - Policy für berechtigte Nutzergruppen und Nutzer**

Das Consent Decision Management MUSS die Konfiguration der User Specific Deny Policy Medication auf die folgenden Nutzergruppen einschränken:

Nutzergruppe [professionOID] der User Specific Deny Policy Medication
oid_praxis_arzt
oid_krankenhaus
oid_institution-vorsorge-reha
oid_zahnarztpraxis
oid_öffentliche_apotheke
oid_praxis_psychotherapeut
oid_institution-pflege
oid_institution-geburtshilfe
oid_praxis-physiotherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin
oid_praxis-ergotherapeut
oid_praxis-logopaede
oid_praxis-podologe
oid_praxis-ernaehrungstherapeut

[≤]

#### **A\_26405 -Consent Decision Management - Protokollierung geänderter Entscheidungen der User Specific Deny Policy Medication**

Das Consent Decision Management MUSS für jede Änderung der User Specific Deny Policy Medication einen Protokolleintrag gemäß A\_24704\* erzeugen:

**Tabelle 13: Consent Decision Management Protokollierung - User Specific Deny Policy Medication**

Strukturelement	Wert		Erläuterung
AuditEvent.action	C, D		Update
AuditEvent.entity.name	"UdpMedication"		Eintrag protokolliert eine Änderung der User Specific Deny Policy für Medication Service
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"UserId"	<Telematik-ID der LEI>	Telematik-ID der LEI, welche zur User Specific Deny Policy Medication hinzugefügt oder gelöscht wurde
	"UserName"	<displayName>	Name der LEI, welche zur User Specific Deny Policy Medication hinzugefügt oder gelöscht wurde

[&lt;=]

### 3.9 Entitlement Management

Befugnisse (Entitlements) werden individuell für jeden Nutzer des Aktenkontos erstellt (Versicherter, Vertreter, Leistungserbringerinstitutionen, Kostenträger, Ombudsstelle und Fachdienste). Eine erteilte Befugnis ist notwendige Voraussetzung für die Nutzung des Aktenkontos und zum internen Bezug des Datenpersistierungsschlüssels (SecureDataStorageKey) für den Zugriff auf die Dokumenten- und Datenverwaltung.

Eine Befugnis enthält folgende Informationen:

#### **A\_23734-01 -Entitlement Management - Definition einer Befugnis**

Das Entitlement Management MUSS für eine individuelle Befugnis die folgenden Daten nutzen und verwalten:

**Tabelle 14: Inhalt einer Befugnis**

Element	Inhalt	Anmerkung	signiertes Element (*)
Identifizier des Aktenkontos (insurantId)	KVNR des Aktenkontos, für welches die Befugnis ausgestellt ist		ja
Identifizier des befugten	Telematik-ID oder		ja

Nutzers (actorId)	KVNR		
Name des befugten Nutzers (displayName)	Name der Institution, des Nutzers		nein
Rolle des Nutzers (oid)	OID der Nutzerrolle (professionOID)		nein
Ende der Gültigkeit (validTo)	Datum und Zeitpunkt (letzter Tag der Gültigkeit, d.h. eine heutige Befugnisvergabe für 3 Tage setzt für validTo das Datum von übermorgen (aktueller Tag + 2 Tage). aktueller Tag ist inklusiv zu bewerten).	Wird gemäß [RFC3339] mit Zeitzone UTC (z.B.: 2024-04-12T22:59:59Z) bzw. Zeitzone-Offset (z.B.: 2024-04- 12T23:59:59+01:00) gespeichert. Eine unbegrenzt gültige Befugnis erhält das Datum 9999-12- 31T00:00:00Z. . Die Befugnisdauer der Befugnisse (Karte stecken), die durch das Aktensystem erstellt werden, werden auf das Ende des resultierenden Tages der aktuell gültigen Zeitzone in Deutschland gesetzt, z.B.: 2024-04- 12T23:59:59+01:00. Wird durch den Versicherten oder einen Vertreter oder das Entitlement Management gesetzt.	ja
Beginn der Gültigkeit, Ausstellungszeitpunkt (issued-at)	Datum und Zeitpunkt	Wird durch das Entitlement Management gesetzt.	nein
Identifizier des Erstellers (issued-actorId)	Telematik-ID oder KVNR	Wird durch das Entitlement Management Management gesetzt.	nein
Name des Erstellers (issued-displayName)	Name der Institution, des Nutzers	Wird durch das Entitlement Management Management Management gesetzt.	nein

**[<=]**

*Hinweis: Ein Nutzer ist der Adressat, für den die Befugnis ausgestellt wird. Der Ersteller ist der Nutzer, welcher die Befugnisausstellung veranlasst hat. Die Bezeichner in () sind die Bezeichner in den Schnittstellenbeschreibungen.*



*Hinweis (\*): A\_23734 definiert eine "vollständige" Befugnis, welche auch Daten enthält, die für eine Prüfung einer gültigen Befugnis im Kontext einer Schnittstellenoperation nicht notwendig sind. Für diesen Zweck wird nur der (HSM-) signierte Anteil als Ergebnis einer Befugnisverifikation verwendet (signiertes Element = ja). Eine gespeicherte Befugnis enthält jedoch alle Elemente für eine qualifizierte Verwaltung der Befugnisse durch einen Versicherten oder Vertreter.*

*Hinweis:* Befugnisse können durch das Aktensystem selbst (initiale Befugnisse), durch den Versicherten oder einen befugten Vertreter unter Verwendung eines ePA-FdV oder durch eine Leistungserbringerinstitution in einer Behandlungssituation erstellt werden.

Eine Befugnis kann nur für Nutzer und Nutzergruppen mit bestimmter Rolle erteilt werden. Nutzergruppen mit abweichenden Rollen können nicht befugt werden und erhalten keinen Zugriff auf das Aktenkonto.

Erfolgt die Befugniserteilung durch eine Leistungserbringerinstitution in einer Behandlungssituation, wird eine vorgegebene Gültigkeitsdauer der Rolle des Befugten entsprechend durch das Entitlement Management vergeben. Ein Versicherter oder ein befugter Vertreter kann den Gültigkeitszeitraum frei wählen (ausgenommen Vertreterbefugnisse).

#### **A\_23941-01 -Entitlement Management - Erteilung von Befugnissen für berechnigte Nutzergruppen und Nutzer**

Das Entitlement Management MUSS die Erteilung von Befugnissen in der jeweiligen Umgebung auf die folgenden Nutzergruppen und Nutzer einschränken:

**Tabelle 15: Befugnisse für berechnigte Nutzergruppen und Nutzer**

professionOID / Nutzergruppe und Nutzer	Umgebung			Standard- Befugnisdauer [Tage]	Befugnisdauer FdV [Tage]
	LEI	FdV	AS	durch das Entitlement Management bei Erteilung der Befugnis aus der Umgebung LEI	bei Erteilung der Befugnis aus der Umgebung FdV
oid_praxis_arzt	x	x	-	90	var
oid_krankenhaus	x	x	-	90	var
oid_institution-vorsorge-reha	x	x	-	90	var
oid_zahnarztpraxis	x	x	-	90	var
oid_öffentliche_apotheke	x	x	-	3	var
oid_praxis_psychotherapeut	x	x	-	90	var
oid_institution-pflege	x	x	-	90	var
oid_institution-geburtshilfe	x	x	-	90	var
oid_praxis-physiotherapeut	x	x	-	90	var

oid_praxis-ergotherapeut	x	x	-	90	var
oid_praxis-logopaede	x	x	-	90	var
oid_praxis-podologe	x	x	-	90	var
oid_praxis-ernaehrungstherapeut	x	x	-	90	var
oid_institution-oegd	x	x	-	3	var
oid_institution-arbeitsmedizin	x	x	-	3	var
oid_kostentraeger	-	-	x (statisch)	-	-
oid_ombudsstelle	-	-	x (statisch)	-	-
oid_erp-vau (E-Rezept vertrauenswürdige Ausführungsumgebung)	-	-	x (statisch)	-	-
oid_versicherter (Versicherter)	-	-	x (statisch)	-	-
oid_versicherter (Vertreter)	-	x	-	-	dauerhaft
oid_diga	-	x	-	-	dauerhaft

#### Hinweis:

'x' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung befugt werden

'-' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung nicht befugt werden

LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-Prüfungsnachweis (Prüfziffer),

FdV = Versicherter oder Vertreter,

KTR = Kostenträger

AS = Aktensystem (systemseitig erteilte Befugnisse)

Tage = Gültigkeit in Tagen: angegebener Wert ist einschließlich aktuellem Datum, z. B. 90 Tage bedeutet aktuelles Datum + 89 Tage.

dauerhaft = Befugnis unbegrenzt gültig (Enddatum = 9999-12-31)

statisch = Gültigkeit analog 'dauerhaft', Befugnis ist implizit vorhanden.

var = Gültigkeitsdauer von 1 Tag bis dauerhaft in jeweils ganzen Tagen[<=]

Befugnisse werden durch dasEntitlement Management mit dem SecureAdminStorageKey verschlüsselt und im Aktenkonto gesichert abgelegt.

Einzelne Nutzer können durch den Versicherten, einen befugten Vertreter oder die Ombudsstelle explizit von der Befugnisvergabe ausgeschlossen sein (siehe 3.9.4-Befugnisausschluss (Blocked User Policy) ). Eine Befugniserstellung ist dann weder für Leistungserbringerinstitutionen in einer Behandlungssituation, noch durch den Versicherten oder einen Vertreter möglich.

Die Befugnisse für den Versicherten und den E-Rezept-Fachdienst werden dabei nicht persistiert. Diese Befugnisse werden als implizit vorhanden und gültig angenommen.

Eine Besonderheit stellt hierbei eine Befugnis EU-Zugriff dar. Es gibt zu einem Zeitpunkt für ein Aktenkonto maximal eine Befugnis EU-Zugriff. Die Dauer dieser Befugnis wird durch das Aktensystem festgelegt und beträgt 1 Stunde. Das Ende der Gültigkeit (validTo) wird ermittelt vom Ausstellungszeitpunkt + 1 Stunde.

#### **A\_26167 -Entitlement Management (EU) - Erteilung der Befugnis EU-Zugriff**

Das Entitlement Management MUSS die Erteilung einer Befugnis EU-Zugriff in der jeweiligen Umgebung zusätzlich zu A\_23941-\* auf die folgenden Nutzergruppen und Nutzer einschränken:

**Tabelle 16: Befugnisse EU-Zugriff für berechnigte Nutzergruppen und Nutzer**

professionOID / Nutzergruppe und Nutzer	Umgebung			Standard- Befugnisdauer	Befugnisdauer FdV
	LEI	FdV	AS	durch das Entitlement Management bei Erteilung der Befugnis aus der Umgebung LEI	bei Erteilung der Befugnis aus der Umgebung FdV
oid_ncpeh	-	x	-	-	1 Stunde; wird durchgesetzt durch das Aktensystem

Hinweis:

'x' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung befugt werden

'-' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung nicht befugt werden

LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-Prüfungsnachweis (Prüfziffer),

FdV = Versicherter oder Vertreter,

AS = Aktensystem (systemseitig erteilte Befugnisse)[<=]

#### **A\_24371 -Entitlement Management - Verschlüsselung der Befugnisse**

Das Entitlement Management MUSS Befugnisse mit dem versichertenindividuellen SecureAdminStorageKey verschlüsseln und im Aktenkonto persistieren.[<=]

#### **A\_24372 -Entitlement Management - Keine persistente Ablage unverschlüsselter Befugnisse**

Das Entitlement Management MUSS sicherstellen, dass Befugnisse ausschließlich verschlüsselt unter Verwendung des versichertenindividuellen SecureAdminStorageKey im Aktenkonto gespeichert werden.[<=]

#### **A\_24687 -Entitlement Management - Keine Speicherung oder Verwendung nicht verifizierter Befugnisse**

Das Entitlement Management MUSS sicherstellen, dass ausschließlich Befugnisse persistiert oder für eine Befugnisprüfung verwendet werden, die erfolgreich durch das HSM unter Verwendung der adäquaten Regeln 'rr1 - rr4' gemäß A\_24573\* befugnisverifiziert sind. [≤]

#### **A\_23842 -Entitlement Management - Eindeutigkeit der Befugnisse im Befugniskontext**

Das Entitlement Management MUSS sicherstellen, dass im Befugniskontext keine zwei oder mehr Befugnisse existieren, die als Identifier des befugten Nutzers die gleiche Identifikation (actorId) aufweisen. [≤]

#### **A\_24785 -Entitlement Management - VSDM-Prüfungsnachweis kann höchstens einmal genutzt werden**

Das Entitlement Management MUSS sicherstellen, dass ein VSDM-Prüfungsnachweis (Prüfziffer) höchstens einmal zur Registrierung einer Befugnis genutzt werden kann. [≤]

#### **A\_27671 -Entitlement Management - PoPP-Token kann höchstens einmal genutzt werden**

Das Entitlement Management MUSS sicherstellen, dass ein PoPP-Token höchstens einmal zur Registrierung einer Befugnis genutzt werden kann. [≤]

#### **A\_27681 -Entitlement Management - Konfigurationsvariable enforce\_popp\_only**

Das Entitlement Management MUSS eine Konfigurationsvariable enforce\_popp\_only besitzen, die initial auf false gesetzt ist. [≤]

ePA-Clients nutzen zur Befugnisvergabe die Operationen der Schnittstelle I\_Entitlement\_Management gemäß [I\_Entitlement\_Management].

Die initialen Befugnisse des Aktenkontos werden auf organisatorischem Weg direkt im Aktenkonto erstellt.

#### **A\_24506 -Entitlement Management- Realisierung der Schnittstelle I\_Entitlement\_Management**

Das Entitlement Management MUSS die Operationen der Schnittstelle I\_Entitlement\_Management gemäß [I\_Entitlement\_Management] umsetzen. [≤]

#### **A\_26168 -Entitlement Management (EU)- Realisierung der Schnittstelle I\_Entitlement\_Management\_EU**

Das Entitlement Management MUSS die Operationen der Schnittstelle I\_Entitlement\_Management\_EU gemäß [I\_Entitlement\_Management\_EU] umsetzen. [≤]

#### **A\_24987-01 -Entitlement Management - Protokolleinträge für Zugriffe auf das Entitlement Management**

Das Entitlement Management MUSS für das Erteilen und Entziehen von Befugnissen und das Setzen und Löschen von Befugnisaußschlüssen jeweils einen Protokolleintrag gemäß A\_24704 erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

**Tabelle 17: Entitlement Management Protokollierung**

Strukturelement	Wert	Erläuterung
AuditEvent.type	"rest"	
AuditEvent.action	C, D, U	ein Code aus den genannten, je nach Operation
AuditEvent.entity.name	"UserBlocking"	Setzen und Löschen von Befugnisaußschlüssen

	"EntitlementManagement"		Erteilen oder Entziehen von Befugnissen
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"blockedUserName"	<Name der LEI>	Name der LEI, für die der Befugnisausschluss gesetzt bzw. der Ausschluss zurückgenommen wurde
	"blockedUserId"	<Telematik-ID der LEI>	Telematik-ID der LEI, für die der Befugnisausschluss gesetzt bzw. der Ausschluss zurückgenommen wurde
	"UserName"	<Name der Institution oder des Vertreters>	Name der Institution oder des Nutzers für die eine Befugnis erteilt oder gelöscht wurden
	"UserId"	<Identifizier der Institution oder des Vertreters>	ID der Institution oder des Nutzers für die eine Befugnis erteilt oder gelöscht wurden
	"entitledValidTo"	<Endzeitpunkt der Gültigkeit der Befugnis>	Angabe des Endes einer erteilten Befugnis, Format gemäß [RFC3339] YYYY-MM-DDThh:mm:ssZ oder YYYY-MM-DDThh:mm:ss+/-time zone

**[<=]**

*Hinweis: Ein Update ("U") eines Entitlements liegt vor, wenn ein existierendes Entitlement aufgrund des längeren Gültigkeitszeitraums eines neuen Entitlements überschrieben wird.*

### 3.9.1 Initiale Befugnisse (static Entitlements)

Einige grundsätzlich notwendige Befugnisse sind zum Zeitpunkt der Aktivierung eines Aktenkontos verfügbar.

Zu diesen initialen Befugnissen gehören die Befugnisse für den Versicherten, den E-Rezept-Fachdienst, den Kostenträger und die Ombudsstelle. Diese Befugnisse müssen in der Phase der Initialisierung eines Aktenkontos durch das Aktensystem erstellt werden.

Diese Befugnisse sind dauerhaft gültig und unveränderbar und können nicht gelöscht werden.

**A\_24145 -Entitlement Management - Implizite initiale (statische) Befugnisse**

Das Entitlement Management MUSS sicherstellen, dass der Versicherte (KVNR des Akteninhabers, oid\_versicherter), und der E-Rezept-Fachdienst (registrierte Telematik-ID, oid\_erp-vau) dauerhaft den versichertenindividuellen SecureDataStorageKey beziehen können und Zugriff auf die Dokumenten- und Datenverwaltung erhalten. Die Befugnisse MÜSSEN den Vorgaben der folgenden Tabelle entsprechen:

Element	Versicherter	E-Rezept-Fachdienst
Identifizier des befugten Nutzers (actorId)	KVNR des Versicherten (Aktenkontoinhaber)	Telematik-ID der E-Rezept vertrauenswürdigen Ausführungsumgebung
Name des befugten Nutzers (displayName)	Name des Versicherten	Name/ Bezeichnung des E-Rezept-Fachdienstes oder "Fachdienst E-Rezept"
Rolle des Nutzers (oid)	oid_versicherter	oid_erp-vau
Ende der Gültigkeit (validTo)	9999-12-31	9999-12-31

【<=】

**A\_24374 -Entitlement Management - Signierte initiale (statische) Befugnisse**

Das Entitlement Management MUSS sicherstellen, dass für den Kostenträger und die Ombudsstelle gültige Befugnisse mit unbegrenzter Gültigkeitsdauer zum Zeitpunkt der Aktivierung des Aktenkontos gemäß der Vorgaben der folgenden Tabelle vorliegen:

Element	Kostenträger	Ombudsstelle
Identifizier des Aktenkontos (insurantid)	KVNR des Versicherten	KVNR des Versicherten
Identifizier des befugten Nutzers (actorId)	Telematik-ID des Kostenträgers	Telematik-ID der Ombudsstelle
Name des befugten Nutzers (displayName)	Name des Kostenträgers	Name/ Bezeichnung der Ombudsstelle
Rolle des Nutzers (oid)	oid_kostentraeger	oid_ombudsstelle

Ende der Gültigkeit (validTo)	9999-12-31	9999-12-31
-------------------------------	------------	------------

[&lt;=]

**A\_24688-01 -Entitlement Management - Befugnisverifikation signierter initialer Befugnisse**

Das Entitlement Management MUSS sicherstellen, dass die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle spätestens beim ersten Zugriff auf das Aktenkonto durch das HSM unter Verwendung der Regel 'rr4' gemäß A\_24573\* befugnisverifiziert sind.[<=]

**A\_24533 -Entitlement Management - Keine Änderung statischer Befugnisse**

Das Entitlement Management MUSS sicherstellen, dass die dauerhaften Befugnisse des Versicherten, des E-Rezept-Fachdiensts, des Kostenträgers und der Ombudsstelle nicht verändert oder gelöscht werden können.[<=]

**A\_24784 -Entitlement Management - Höchstens eine Befugnis für KTR und Ombudsstelle pro Aktenkonto**

Das Entitlement Management MUSS sicherstellen, dass in einem Aktenkonto höchstens eine Befugnis für einen Kostenträger und höchstens eine Befugnis für eine Ombudsstelle hinterlegt ist.[<=]

**A\_24955 -Entitlement Management - Befugnis für KTR und Ombudsstelle nur bei Anlage und betreiberinterner Anbieterwechsel**

Das Entitlement Management MUSS sicherstellen, dass eine signierte Befugnis des Kostenträgers und eine signierte Befugnis der Ombudsstelle ausschließlich bei einer Anlage eines Aktenkontos (Initialisierung) oder bei einem betreiberinternen Anbieterwechsel in die Befugnisse des Aktenkontos aufgenommen werden.

[&lt;=]

**3.9.2 Erstellen einer Befugnis durch Clients**

Die Anforderung zur Vergabe einer neuen Befugnis erfolgt durch die Clients der ePA. Bei einer Befugnisvergabe aus der Umgebung der Leistungserbringer ist dieses das Primärsystem (PS), aus der Umgebung des Versicherten ist es das ePA-FdV.

Clients verwenden zur Befugnisvergabe signierte JSON Web Token (JWS). Das Token wird zur Verifikation an das HSM übergeben. Als Ergebnis der HSM Verarbeitung liegt eine bestätigte, CMAC gesicherte Befugnis mit den Elementen actorId (Identifizier des zu befugnenden Nutzers), kvnr (Aktenkontoid) und validTo (Gültigkeitszeitraum) für die spätere Befugnisprüfung vor. Das HSM Ergebnis wird mit den weiteren Daten gemäß A\_23734\* (oid, displayName, issued-\*) ergänzt und gemäß A\_24371\* mit dem SecureAdminStorageKey gesichert im Aktenkonto abgelegt.

**3.9.2.1 Befugnisvergabe durch ein ePA-FdV**

Ein ePA-FdV muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

**A\_24587-01 -Entitlement Management - Befugnis durch ein ePA-FdV**

Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ePA-FdV über die Schnittstelle I\_Entitlement\_Management durch Verwendung eines gültig signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:

Befugnis	Claim Name	Claim	Beispiel
----------	------------	-------	----------



Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.CH.SIG	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	
	"exp"	Verfalldatum, = "iat" + 20 min	
	"insurantId"	KVNR des Aktenkontos	A123456789
	"actorId"	Identifizier (Telematik-id oder KVNR)	3-883110000092471
	"oid"	professionOid	1.2.276.0.76.4.54
	"displayName"	Name des Befugten	Test-Apotheke
	"validTo"	Ende der Gültigkeit, (Bei unbegrenzter Gültigkeit ist 9999-12-31T00:00:00Z zu verwenden.)	gemäß [RFC3339], z.B. 2025-06-30T21:59:59Z oder 2025-06-30T23:59:59+02:00

#### 【<=】

Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve "brainpoolP256r1" basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

*Hinweis zu A\_24587\*: Im Falle der Befugnisvergabe für einen NCPeH (EU-Zugriff, "oid" == "oid\_ncpeh") wird durch das Aktensystem sichergestellt, dass die vorgeschriebene Gültigkeitsdauer für derartige Befugnisse angewendet wird. Dieses erfolgt durch die Befugnisverifikation gemäß Regel "rr1" im HSM. Die Angabe eines Gültigkeitsendes im "validTo"-Element des JWT wird daher für diesen Fall ignoriert, das Element selbst muss jedoch vorhanden sein.*

### **A\_24689 -Entitlement Management - Befugnisverifikation einer Befugnis durch ein ePA-FdV**

Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein ePA-FdV unter Verwendung der Regeln 'rr1' (Befugnisvergabe durch den Versicherten) bzw. 'rr2' (Befugnisvergabe durch einen Vertreter) des HSM eine Befugnisverifikation durchführen.【<=】

### **A\_24535 -Entitlement Management - Befugnisse für Vertreter**

Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (actorId = KVNVR) ausschließlich durch den Versicherten erstellt oder gelöscht werden können.  
[<=]

#### **A\_26698 -Entitlement Management - maximale Anzahl Befugnisse für Vertreter**

Das Entitlement Management MUSS sicherstellen, dass maximal fünf gültige Befugnisse für Vertreter gleichzeitig in einem Aktenkonto vorhanden sind.[<=]

#### **A\_24536 -Entitlement Management - Gültigkeitsdauer der Befugnisse für Vertreter**

Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (actorId = KVNVR) ausschließlich mit einer unbegrenzten Gültigkeit erstellt werden.[<=]

#### **A\_24754 -Entitlement Management - E-Mail-Adresse des Vertreters**

Das Entitlement Management MUSS sicherstellen, dass bei Befugnissen für Vertreter (actorId = KVNVR) eine E-Mail-Adresse des Vertreters für dessen Benachrichtigung angegeben wird.[<=]

Die in A\_24754 angegebene E-Mail-Adresse wird ausschließlich zur Benachrichtigung des Vertreters über die eingestellte Befugnis verwendet (vgl. A\_24755-\*), jedoch nicht für die Geräteregistrierung. Um eine Vertretung wahrnehmen zu können und hierfür Geräte zu registrieren, muss der Vertreter in seinem Home-AS eine E-Mail-Adresse hinterlegt haben.

#### **A\_24755-01 -Entitlement Management - Benachrichtigung des Vertreters bei Befugniserstellung**

Das Entitlement Management MUSS im Anschluss an die erfolgreiche, neue Befugniserstellung für einen Vertreter eine E-Mail an die E-Mail-Adresse des Vertreters senden, die diesen über die Befugniserstellung für das Aktenkonto des Versicherten geeignet informiert. In der Nachricht MUSS der Name des Versicherten enthalten sein und welche Art von personenbezogenen Daten vom Vertreter im Rahmen der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine Vertreterberechtigung widerrufen kann und gegenüber wem er seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann.[<=]

Hinweis: Unter Art der personenbezogenen Daten ist z.B. „Krankenversicherungsnummer, Name und E-Mail-Adresse“ gemeint, aber nicht die tatsächliche KVNVR des Vertreters, der tatsächliche Name oder die tatsächliche E-Mail-Adresse.

### **3.9.2.2 Befugnisvergabe durch ein Primärsystem**

#### **A\_27288-01 -Entitlement Management - Abgleich der KVNVR bei Erstellen einer Befugnis**

Das Entitlement Management MUSS sicherstellen, dass für die in setEntitlementPs bzw. setEntitlementsPsV2 vom Primärsystem in x-insurantid übergebene KVNVR folgendes gilt: die KVNVR in x-insurantid stimmt mit der KVNVR überein, die in der CMAC-gesicherten Befugnis enthalten ist, die als Ergebnis des Aufrufs der Regel rr3 mit der vom Primärsystem erhaltenen Befugnis (signiertes JWT) bzw. dem erhaltenen PoPP-Token vom HSM zurückgegeben wird.  
[<=]

Ein Primärsystem muss für die Befugnisvergabe mittels VSDM-Prüfziffer ein JWS gemäß folgender Vorgabe erstellen.

#### **A\_24590-03 -Entitlement Management - Befugnis durch ein Primärsystem**

Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ein Primärsystem über die Operation I\_Entitlement\_Management::setEntitlementPs durch die Verwendung eines gültig signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:

Befugnis	Claim Name	Claim
Protected Header		
	"typ"	"JWT"
	"alg"	"ES256" oder "PS256"
	"x5c"	Signaturzertifikat C.HCI.AUT
Payload		
	"iat"	Zeitstempel Ausgabezeitpunkt
	"exp"	Verfalldatum, = "iat" + 20 min
	"auditEvidence"	VSDM-Prüfziffer aus dem VSDM-Prüfungsnachweis, base64-kodiert.
	"hcv"	Hash check value, der als Ergebnis der Operation ReadVSD gemäß A_27352-* berechnet wird. Der berechnete hcv-Wert MUSS base64 kodiert werden.

[<=]

*Hinweis: Die Parameter "iat" und "exp" sind optional und werden durch das Entitlement Management nicht ausgewertet.*

Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

#### **A\_27321-01 -Entitlement Management - Abgleich hcv bei Erstellen einer Befugnis über VSDM-Prüfziffer in Version 2**

Falls vom Primärsystem in setEntitlementPs eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2 übergeben wird und das Ergebnis des Aufrufs der Regel rr3 eine interne Datenstruktur der VSDM-Prüfziffer zurückliefert, MUSS das Entitlement Management sicherstellen, dass der Wert im Attribut "hcv" des JWT mit dem Wert von hcv aus der VSDM-Prüfziffer übereinstimmt und ansonsten die Operation setEntitlementPs abbrechen.[<=]

#### **A\_27289 -Entitlement Management - Maximale Anzahl fehlerhafter Abgleiche der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer**

Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer Stunde maximal fünfmal eine Befugnis (signiertes JWT) über setEntitlementPs übermitteln kann, bei der die mitgelieferte KVNR in x-insurantId von der KVNR abweicht, die in der Prüfziffer der übermittelten Befugnis (signiertes JWT) enthalten ist, andernfalls für den Nutzer für diesen Zeitraum die Operation setEntitlementPs abbrechen.[<=]

#### **A\_27322 -Entitlement Management - Maximale Anzahl fehlerhafter Abgleiche der VSD-Update-Zeit bei Erstellen einer Befugnis über VSDM-Prüfziffer in Version 2**

Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer Stunde maximal fünfmal eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2 über setEntitlementPs übermitteln kann, bei der die Operation setEntitlementPs gemäß A\_27321-\* abbricht.【<=】

#### **A\_27679 -Entitlement Management - Telematik-ID im PoPP-Token ist gleich der Telematik-ID des angemeldeten Nutzers**

Das Entitlement Management MUSS bei der Befugnisvergabe durch ein Primärsystem unter Verwendung eines PoPP-Tokens sicherstellen, dass die Telematik-ID in PoPP-Token.actorID gleich der Telematik-ID des Nutzers der User Session ist.【<=】

#### **A\_24537 -Entitlement Management - Standardgültigkeitsdauer für Befugnisse**

Das Entitlement Management MUSS sicherstellen, dass neue Befugnisse, die unter Verwendung der Schnittstelle I\_Entitlement\_Management gemäß [I\_Entitlement\_Management] erstellt werden, eine vorgegebene, rollenspezifische Befugnisdauer gemäß A\_23941-\* erhalten.【<=】

### **3.9.3 Löschen von Befugnissen**

Erteilte Befugnisse werden grundsätzlich nach Erreichen des Endzeitpunkts ihrer Gültigkeit durch das Aktensystem gelöscht.

#### **A\_24504 -Entitlement Management - Löschen ungültiger Befugnisse**

Das Entitlement Management MUSS vorhandene Befugnisse, deren Enddatum der Gültigkeit überschritten ist, unverzüglich aus dem Befugniscontext des Aktenkontos vollständig löschen.【<=】

Das explizite Löschen von Befugnissen innerhalb ihres Gültigkeitszeitraums kann ausschließlich durch den Versicherten oder einen Vertreter mittels eines ePA-FdV erfolgen. Es können alle erteilten Befugnisse gelöscht werden, ausgenommen die initialen Befugnisse gemäß 3.9.1- Initiale Befugnisse (static Entitlements) .

Für das Löschen von Befugnissen durch einen Vertreter gilt darüber hinaus folgende Einschränkung:

#### **A\_25246 -Entitlement Management - Löschen von Befugnissen durch einen Vertreter**

Das Entitlement Management MUSS sicherstellen, dass eine erteilte Befugnis für einen Vertreter (actorIdder Befugnis == KVNR) durch einen Vertreter nur dann gelöscht werden kann, wenn die KVNR des löschenden Vertreters der KVNR der actorIdder zu löschenden Befugnis entspricht.【<=】

*Hinweis: Ein Vertreter darf nur seine eigene Befugnis löschen, nicht aber die Befugnis weiterer Vertreter.*

#### **A\_25269 -Entitlement Management - Benachrichtigung des Versicherten bei Löschen einer Vertreterbefugnis durch Vertreter**

Falls ein Vertreter seine eigene Vertreterbefugnis löscht MUSS das Entitlement Management für den Fall, dass für den Versicherten mindestens eine E-Mail-Adresse hinterlegt ist, den Versicherten über das Löschen der Vertreterbefugnis an alle seine hinterlegten E-Mail-Adressen informieren.【<=】

### **3.9.4 Befugnisausschluss (Blocked User Policy)**

Das Entitlement Management erlaubt die Verwaltung von Widersprüchen des Versicherten oder eines Vertreters gegen die Nutzung des Aktenkontos durch spezifische Leistungserbringereinstitutionen.

Ist ein Widerspruch gegen einen bestimmten Nutzer hinterlegt, so kann für diesen keine Befugnis erstellt werden, bis dieser Widerspruch zurückgenommen wird.

Die Umsetzung dieser Widerspruchsverwaltung bzw. des Befugnisausschlusses erfolgt durch eine Policy (Blocked User Policy). Die Konfiguration dieser Policy obliegt dem Versicherten oder einem befugten Vertreter mittels ePA-FdV oder der Ombudsstelle. Einträge können der Policy hinzugefügt oder entfernt werden. Zum Zeitpunkt der Erstellung des Aktenkontos enthält die Blocked User Policy keine Einträge.

Ein Eintrag in der Policy referenziert einen bestimmten Nutzer über seinen Identifier (Telematik-Id). Die Menge der Einträge ist nicht limitiert.

Jeder Eintrag der Blocked User Policy verhindert grundsätzlich die Erstellung einer Befugnis für den referenzierten Nutzer. Erfolgt der Widerspruch (Anlegen eines neuen Eintrags) bei bestehender Befugnis für den auszuschließenden Nutzer, wird die bestehende Befugnis gelöscht.

Bei Rücknahme eines Widerspruchs gegen die Nutzung des Aktenkontos für eine bestimmte Leistungserbringerinstitution wird der entsprechende Eintrag der Policy gelöscht. Anschließend kann dieser Nutzer befugt werden.

Ein Widerspruch gegen die Nutzung des Aktenkontos kann nur für Nutzer der folgenden Nutzergruppen erfolgen.

#### **A\_24463-01 -Entitlement Management - zulässige Rollen für den Widerspruch gegen die Nutzung durch eine Leistungserbringerinstitution**

Das Entitlement Management MUSS den Widerspruch gegen die Nutzung durch eine Leistungserbringerinstitution ausschließlich für Nutzer der folgenden Nutzergruppen zulassen:

professionOID / Nutzergruppe	
oid_praxis_arzt	
oid_krankenhaus	
oid_institution-vorsorge-reha	
oid_zahnarztpraxis	
oid_öffentliche_apotheke	
oid_praxis_psychotherapeut	
oid_institution-pflege	
oid_institution-geburtshilfe	
oid_praxis-physiotherapeut	
oid_praxis-ergotherapeut	
oid_praxis-logopaede	

oid_praxis-podologe
oid_praxis-ernaehrungstherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin

【<=】

Ein Eintrag der Blocked User Policy enthält Angaben gemäß der folgenden Tabelle:  
(Beispiel)

**Tabelle 18: Inhalt eines Blocked User Policy Eintrags**

Element	Inhalt	Beispiel
actorId	Telematik-Id	2-883110000099999
oid	professionOID	1.2.276.0.76.4.5
displayName	Name der Leistungserbringerinstitution	Zahnarztpraxis Dr. Beispiel
at	Zeitpunkt des Widerspruchs (wird durch das Entitlement Management gesetzt)	2025-01-01T12:00:00Z

#### **A\_25135 -Entitlement Management - Initialisierung der Blocked User Policy**

Das Entitlement Management MUSS für ein Aktenkonto eine Blocked User Policy ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policies über die Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` ermöglichen.【<=】

#### **A\_24514 -Entitlement Management - Keine Befugnis für von einer Befugnis ausgeschlossene Nutzer**

Das Entitlement Management MUSS sicherstellen, dass für keinen durch einen Eintrag der Blocked User Policy referenzierten Nutzer eine Befugnis existiert oder erstellt werden kann.【<=】

#### **A\_24515 -Entitlement Management- Verschlüsselung der Einträge der Blocked User Policy**

Das Entitlement Management MUSS Einträge der Blocked User Policy mit dem Befugnispersistierungsschlüssel (`SecureAdminStorageKey`) verschlüsseln und im Aktenkonto persistieren.【<=】

Die Konfiguration der Blocked User Policy erfolgt über die Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` durch ein ePA-FdV bzw. durch die Ombudsstelle.

#### **A\_24965 -Entitlement Management - Information über Änderungen der Blocked User Policy**

Das Entitlement Management MUSS den Aktenkontoinhaber bei einer Änderung der Blocked User Policy, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber informieren, dass ein Befugnisausschluss geändert wurde, wann die Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind.【<=】

### 3.9.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)

Die Erstellung von Befugnissen durch Primärsysteme der Leistungserbringerinstitutionen wird durch das Aktensystem mengenmäßig über einen Zeitraum begrenzt. Diese Maßnahme verhindert den massenhaften Zugriff auf Aktenkonten durch Fehlbedienung seitens eines Primärsystems oder durch unzulässige Nutzung der Aktensysteme.

Die maximal zulässige Befugnismenge ist dabei so bemessen, dass die intendierte Nutzung der ePA durch Leistungserbringerinstitutionen im Versorgungsalltag nicht eingeschränkt wird. Diese maximale Befugnismenge ist pro Nutzerrolle separat festgelegt.

Jedes Aktensystem führt dazu aktensystemweit Zähler für erteilte Befugnisse aus der Umgebung der Leistungserbringer pro Telematik-ID. Die Erfassung erfolgt somit pro Leistungserbringerinstitution separat. Die Zuordnung erfolgt zur Telematik-ID der befugnisstellenden Nutzer (nicht des zu befugnenden Nutzers). Die Befugnisvergabe aus der Umgebung des Versicherten mittels ePA-FdV wird nicht erfasst und geht nicht in die Zählerstände ein.

Das Entitlement Management wertet diese Menge der erfassten Befugnisvergaben im Falle einer weiteren Befugnisvergabe durch ein Primärsystem aus der Umgebung der LEI aus und verhindert die Befugniserstellung bei Erreichen der maximal zulässigen Befugnismenge.

Die zulässige Befugnisrate limitiert dabei einerseits die Menge der innerhalb einer Stunde erstellbaren Befugnisse, als auch die Menge der insgesamt monatlich erstellbaren. Die Zählung erfolgt aktensystemweit pro Aktensystem eines Herstellers und unabhängig vom adressierten Aktenkonto und berücksichtigt nur erfolgreiche Befugnisvergaben. Der Zeitraum pro Stunde, bzw. pro Monat, bezieht sich dabei auf den Zeitraum der aktuellen Stunde, bzw. des aktuellen Monats.

#### **A\_27311 -Entitlement Management - RateLimit-oid-List**

Das Entitlement Management MUSS eine *RateLimit-oid-List* führen, in der pro oid

- der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden Befugnisse innerhalb einer Stunde,
- der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden Befugnisse innerhalb eines Monats und
- der Zeitpunkt der letzten Änderung der Werte

gespeichert werden. [ $\leq$ ]

Initial ist die RateLimit-oid-List mit folgenden Werten zu belegen:

#### **A\_27290-01 -Entitlement Management - RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Stunde**

Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass eine LEI mit der Rolle

- oid\_praxis\_arzt maximal 200 Befugnisse
- oid\_krankenhaus maximal 1.000 Befugnisse
- oid\_institution-vorsorge-reha maximal 1.000 Befugnisse
- oid\_zahnarztpraxis maximal 200 Befugnisse
- oid\_öffentliche\_apotheke maximal 200 Befugnisse
- oid\_praxis\_psychotherapeut maximal 100 Befugnisse
- oid\_institution-pflege maximal 100 Befugnisse



- oid\_institution-geburtshilfe maximal 100 Befugnisse
- oid\_praxis-physiotherapeut maximal 100 Befugnisse
- oid\_praxis-ergotherapeut maximal 100 Befugnisse
- oid\_praxis-logopaede maximal 100 Befugnisse
- oid\_praxis-podologe maximal 100 Befugnisse
- oid\_praxis-ernaehrungstherapeut maximal 100 Befugnisse
- oid\_institution-oegd maximal 100 Befugnisse
- oid\_institution-arbeitsmedizin maximal 100 Befugnisse

innerhalb einer Stunde durch das Primärsystem im Aktensystem registrieren kann.  
[<=]

### **A\_27291-01 -Entitlement Management - RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Monat**

Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass

- oid\_praxis\_arzt maximal 10.000 Befugnisse
- oid\_krankenhaus maximal 200.000 Befugnisse
- oid\_institution-vorsorge-reha maximal 200.000 Befugnisse
- oid\_zahnarztpraxis maximal 10.000 Befugnisse
- oid\_öffentliche\_apotheke maximal 25.000 Befugnisse
- oid\_praxis\_psychotherapeut maximal 10000 Befugnisse
- oid\_institution-pflege maximal 10000 Befugnisse
- oid\_institution-geburtshilfe maximal 10000 Befugnisse
- oid\_praxis-physiotherapeut maximal 10000 Befugnisse
- oid\_praxis-ergotherapeut maximal 10000 Befugnisse
- oid\_praxis-logopaede maximal 10000 Befugnisse
- oid\_praxis-podologe maximal 10000 Befugnisse
- oid\_praxis-ernaehrungstherapeut maximal 10000 Befugnisse
- oid\_institution-oegd maximal 10000 Befugnisse
- oid\_institution-arbeitsmedizin maximal 10000 Befugnisse

innerhalb eines Monats durch das Primärsystem im Aktensystem registrieren kann.  
[<=]

Hinweis zu A\_27290-\* und A\_27291-\*: Die Stunde bzw. der Tag müssen sich nicht auf die aktuelle Stunde bzw. Kalendertag beziehen, sondern können auch je Leistungserbringerinstitution auf Requestzeitpunkte bezogen werden. Dann gilt für einen Monat 30 Tage.

### **A\_27318 -ePA-Aktensystem - RateLimit-oid-List: Maßnahmen zum Schutz der Konfiguration**

Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen umsetzen, die eine unautorisierte Änderung der *RateLimit-oid-List* verhindern.[<=]

### **A\_27312 -ePA-Aktensystem - RateLimit-oid-List: Konfiguration durch Betreiber**

Der Betreiber des ePA-Aktensystem MUSS sicherstellen, dass die Werte für die Anzahl der maximalen Befugnisse in der *RateLimit-oid-List* durch den Betreiber des ePA-Aktensystems ausschließlich im Vier-Augen-Prinzip konfigurierbar sind.[<=]

Stellen LEI Befugnisse mittels der Operation `setEntitlementsPs` über das Primärsystem in das ePA-Aktensystem ein, wird für diese LEI geprüft, ob diese bereits das zulässige Limit erreicht hat. Nur falls dies nicht der Fall ist, kann die Befugnis eingestellt werden. Hierzu erfasst das ePA-Aktensystem außerhalb der VAU wann ein Nutzer mit welcher Rolle eine Befugnis registriert hat. Für den Nutzer wird außerhalb der VAU ein Nutzerpseudonym geführt.

#### **A\_27313-01 -Entitlement Management - Prüfen der RateLimit-oid-List beim Einstellen von Befugnissen**

Das Entitlement Management MUSS bei Aufruf der Operation `setEntitlementsPs` oder `setEntitlementPsV2` prüfen, ob für das zur LEI gehörende Nutzerpseudonym und die oid der LEI bereits das in der `RateLimit-oid-List` vorgegebene maximale Limit pro Stunde oder Monat erreicht wurde. Falls ein Limit erreicht wurde, wird die Operation `setEntitlementsPs`, bzw. `setEntitlementPsV2`, mit einem Fehler abgebrochen. Falls kein Limit erreicht wurde, ist die Registrierung für das zur LEI gehörende Nutzerpseudonym zu vermerken. [ $\leq$ ]

#### **A\_27310 -ePA-Aktensystem - Erfassung der Nutzer zur Prüfung RateLimit-oid-List**

Das ePA-Aktensystem MUSS sicherstellen dass bei der Erfassung der Nutzerdaten außerhalb der VAU zur Prüfung der `RateLimit-oid-List` eine Profilierung über die Nutzer nicht möglich ist und zu diesem Zweck aus der TelematikId eines Nutzers ein Nutzerpseudonym abgeleitet wird, gemäß `gemSpec_Krypt#7.5` Routing auf VAU-Instanzen.

[ $\leq$ ]

### **3.9.6 EntitlementDenyList**

Ein Primärsystem einer Leistungserbringerinstitution (LEI) kann eine Befugnis für ein Aktenkonto eines Versicherten in einer Behandlungssituation ("Stecken" der eGK, VSDM-Prüfungsnachweis) eigenständig erstellen, wenn der Versicherte der Nutzung der ePA nicht widersprochen hat, für die konkrete Leistungserbringerinstitution im Aktenkonto kein Befugnisausschluss (3.9.4- Befugnisausschluss (Blocked User Policy) ) vorliegt und die Leistungserbringerinstitution einer grundsätzlich befugbaren Nutzergruppe angehört (3.9- Entitlement Management ).

Die bestimmte LEI deren Telematik-ID auf einer sogenannten `EntitlementDenyList` stehen, wird diese Funktionalität durch das Aktensystem unterbunden, in der Weise dass eine Befugnisvergabe durch das Aktensystem unterbunden wird.

Die Befugnisvergabe durch den Versicherten oder einen Vertreter mittel ePA-FdV ist durch die `EntitlementDenyList` nicht eingeschränkt. Über ein ePA-FdV können auch LEI befugt werden, die einen Eintrag in der `EntitlementDenyList` haben.

Die `EntitlementDenyList` wird durch das Aktensystem bei jedem Aufruf einer Operation zur Befugnisvergabe durch ein Primärsystem ausgewertet. Diese Operation wird mit einem Fehler beendet, wenn die zu befugende LEI Bestandteil der Liste ist. Eventuell vorhandene Befugnisse dieser LEI, etwa aus einer Befugnisvergabe mittels ePA-FdV, verbleiben im Fehlerfall der Operation unverändert.

Die `EntitlementDenyList` wird für alle Aktenkonten eines Aktensystems einheitlich verwaltet. Die Verwaltung erfolgt außerhalb der VAU, die Liste muss aber für Operationen der Befugnisvergabe innerhalb der VAU zugänglich sein.

#### **A\_27730 -ePA-Aktensystem - EntitlementDenyList außerhalb der VAU**

Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen umsetzen, die eine unautorisierte Änderung der `EntitlementDenyList` verhindern. [ $\leq$ ]

#### **A\_27731 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren**

Das ePA-Aktensystem MUSS sicherstellen, dass falls eine LEI (Telematik-ID) aus der EntitlementDenyList entfernt wird, in der VAU nach spätestens 24 Stunden die EntitlementDenyList aktualisiert wird. [≤]

## **A\_27732 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren - Ausschluss einer LEI**

Falls eine LEI der EntitlementDenyList hinzugefügt wird, MUSS der Betreiber des ePA-Aktensystems sicherstellen, dass die EntitlementDenyList in der VAU unverzüglich aktualisiert wird. [≤]

Hinweise zu A\_27732-\*:

- Die gematik übermittelt die komplette aktuelle EntitlementDenyList an den Anbieter des ePA-Aktensystems.
- Die gematik übermittelt die aufgrund von Sicherheitsgründen aktualisierte EntitlementDenyList über die etablierten Incident-Prozesse.

## **A\_27714 -Entitlement Management - setEntitlementPs in Abhängigkeit von EntitlementDenyList**

Falls der Nutzer auf der EntitlementDenyList enthalten ist, MUSS das Entitlement Management die Operation setEntitlementPs ohne Erzeugung einer Befugnis mit dem HTTP-Statuscode 409requestMismatch abbrechen.

[≤]

Technische Details zur Aktualisierung der EntitlementDenyList im Aktensystem:

Die gematik liefert regelmäßige Aktualisierungen der EntitlementDenyList an die Betreiber der ePA-Aktensysteme. Die gematik möchte automatisiert überwachen können, ob in den ePA-Aktensystemen jeweils die aktuelle Version der EntitlementDenyList geladen ist. In den ePA-Aktensystemen gibt es jeweils ein Enforcement-Point an dem die EntitlementDenyList technisch durchgesetzt wird. Mindestens bei Aktualisierung der EntitlementDenyList im ePA-Aktensystem soll solch ein Enforcement-Point Auskunft über eine BDE-Meldung darüber geben welche EntitlementDenyList ihm aktuell vorliegt. Dabei soll eine hohe Aussagekraft der Information erreicht werden, deshalb wird ein Hashwert über die TelematikIDs der aktuellen EntitlementDenyList erzeugt und dieser Hashwert wird über die BDE-Daten an die gematik (Betriebsüberwachung) übermittelt.

## **A\_27780 -Übertragungsformat der EntitlementDenyList (gematik->ePA-Aktensystem).**

Das ePA-Aktensystem MUSS sicherstellen, dass es eine EntitlementDenyList im JSON-Format von der gematik in folgender Art entgegen nehmen / auswerten kann.

```
{
  "type": "EntitlementDenyList",
  "version": <natürliche Zahl>,
  "iat": <Unix-Zeit als natürliche Zahl>,
  "separator": "<Trennsequenz>",
  "TelematikIDs": [
    "<TID_1>", ... "<TID_2>"
  ],
  "TruncatedHash": "Base64-kodierter 24-Byte-gekürzter-SHA256-Hashwert"
}
```

Die Attribute "version", "iat" dienen nur der Information, i. S. v. müssen von Aktensystem nicht notwendiger Weise technisch ausgewertet werden.

Ein ePA-Aktensystem KANN den TruncatedHash analog A\_27781-\* berechnen (es werden nur die ersten 192 Bit / 24 Byte verwendet) und für aktensysteminterne Zwecke verwendet.

Die Telematik-IDs im Array "TelematikIDs" (bspw. "1-1.12345678") sind in alphabetisch

aufsteigender Ordnung sortiert (werden also schon durch die gematik sortiert geliefert). Die JSON-Datei ist wie üblich UTF-8 kodiert.【<=】

Beispiel für eine EntitlementDenyList gemäß A\_27780-\*:

```
{
  "type": "EntitlementDenyList",
  "version": 6,
  "iat": 1749563839,
  "separator": "+++",
  "TelematikIDs": [
    "1-1.1234567890",
    "1-123456789",
    "1-12345678901234",
    "1-22345678901234",
    "3-06.2.1234567890.10.123",
    "3-07.2.1234567890.123",
    "3-14.2.1234567890.123"
  ],
  "TruncatedHash": "pee1nuX5TxSce3QSawdqs+Pf0L6UMCr8"
}
```

### **A\_27781 -Hashwertberechnung der Telematik-ID-Einträge in einer EntitlementDenyList**

Eine ePA-Aktensystem MUSS bei der Berechnung des Hashwertes für die BDE-Datenlieferung gemäß A\_22469-\*:

1. die Einträge in Array "TelematikIDs" alphabetisch aufsteigend sortieren,
2. die Einträge jeweils mit dem Inhalt von "separator" als Verbindungselement zu einer einzigen lange Bytefolge konkatenieren,
3. von dieser langen Bytefolge den SHA-256-Hashwert berechnen.

Der berechnete Hashwert MUSS Base64 kodiert werden. Das Ergebnis ist dann der Hashwert der für die BDE-Datenlieferung gemäß A\_22469-\* und A\_27782-\* zu verwenden ist.

【<=】

Beispiele für A\_27281-\*:

1)

Wäre separator="AAA" und TelematikIDs=["1", "2", "3"], dann wären die dtbh="1AAA2AAA3". Der Base64-kodierte Hashwert wäre dann NFtlcjAGzo8tL5goB6QMXpHkNCjDSFK5oTzILjXu8k=

2)

Mit den Daten aus dem oben aufgeführten Beispiel für A\_27780-\* würde ein Aktensystem pee1nuX5TxSce3QSawdqs+Pf0L6UMCr80uM3VYtVjdU= berechnen.

### **A\_27782 -EntitlementDenyList: Hashwertberechnung der Telematik-ID-Einträge im Aktensystem**

Ein ePA-Aktensystem MUSS sicherstellen, dass bei Aktualisierung der EntitlementDenyList-Daten am Enforcement-Point der EntitlementDenyList wie in A\_22467-\* definiert, eine Meldung an die BDE erzeugt und übermittelt wird. Dabei MUSS es den dabei zu übermittelnden Hashwert wie in A\_27781 definiert berechnen. (vgl. auch Hinweise zu A\_22782-\*)

【<=】

Hinweise zu A\_27782-\*:

Zum besseren Verständnis, falls der Enforcement-Point die VAU-Instanz ist, so muss beim initialen Starten der VAU-Instanz die EntitlementDenyList in die VAU-Instanz geladen werden. Diese gilt als Aktualisierung der EntitlementDenyList-Daten in der VAU-Instanz. Somit gilt dort A\_27782-\*.

### 3.10 Legal Policy

Die Legal Policy enthält die gesetzlich verbindlichen Regelungen der Zugriffsrechte bzgl. der Berufsgruppen und Datenkategorien gemäß § 341 Absatz 2 SGB V.

Für die Datenkategorien sind die grundsätzlichen Zugriffsrechte der Zugriffsoperationen (CRUD - create, read, update, delete) vorgegeben. Diese Zugriffsrechte wirken ausnahmslos für jeden befugten Nutzer.

Beispiele sind:

- Apotheker haben keinen Zugriff auf die zahnärztliche Dokumentation in der Datenkategorie "dental".
- Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen noch löschen.

Die Legal Policy wird durch das Aktensystem durchgesetzt und ist jederzeit vorhanden. Die Konfiguration kann durch Clients oder Bestandteile des Aktensystems nicht verändert werden.

#### A\_19303-23 -Legal Policy - gesetzlich vorgegebene Zugriffsrechte

Das ePA-Aktensystem MUSS alle in der folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

**Tabelle 19: Legal Policy**

Kategorie	Nutzergruppe										
Technischer Identifier	Med	Apo	Pflege	GH	HME	AM	KTR	OM	DiGA	eRP	Ver
<b>Medical Services (XDS Document Service)</b>	<b>Zugriffsrecht gemäß § 352 SGB V</b>										
reports	CRUD	R	R	R	CRUD	R	-	-	-	-	RD
emp	CRUD	CRUD	R	R	R	R	-	-	-	-	RD
emergency	CRUD	R	R	R	R	R	-	-	-	-	RD
eab	CRUD	R	R	R	R	R	-	-	-	-	RD
dental	CRU	-	R	-	-	R	-	-	-	-	RD

	D										
childsrecord	RD	R	R	RD	R	R	-	-	-	-	RD
child	CRU D	R	R	CRU D	R	R	-	-	-	-	RD (CU (*))
pregnancy_childbi rth	CRU D	R	R	CRU D	R	R	-	-	-	-	RD
vaccination	CRU D	CRU D	R	R	-	CRU D	-	-	-	-	RD
patient	RD	R	R	R	R	R	C	-	-	-	CRU D
receipt	RD	RD	-	R	R	R	CU	-	-	-	RD
health_risk_analys is	-	-	-	-	-	-	C	-	-	-	RD
diga	R	R	R	R	R	R	-	-	CU	-	RD
care	CRU D	R	CRUD	R	R	R	-	-	-	-	RD
eau	CRU D	-	-	-	-	R	-	-	-	-	RD
rehab	CRU D	-	-	-	-	-	-	-	-	-	RD
transcripts	CRU D	-	-	-	-	-	-	-	-	-	RD
other	CRU D	-	-	-	-	R	-	-	-	-	RD
<b>Medical Services (FHIR Data Services)</b>	<b>Zugriffsrecht</b>										
medication	R	R	R	R	R	R	-	-	-	CU	R
demographics	-	-	-	-	-	-	CU	-	-	-	R
documents	R	R	R	R	R	R	-	-	-	-	R
<b>Basic Services</b>	<b>Zugriffsrecht</b>										

Audit Events	-	-	-	-	-	-	-	X	-	-	X
Consent Decisions	-	-	-	-	-	-	-	X	-	-	X
Constraints	-	-	-	-	-	-	-	-	-	-	X
Devices	-	-	-	-	-	-	-	-	-	-	X
Entitlements	X	X	X	X	X	X	-	-	-	-	X
Entitlements.Blocked User	-	-	-	-	-	-	-	X	-	-	X
Information	X	X	X	X	X	X	X	X	X	X	-

#### Nutzergruppen:

- Med = Arztpraxis, Zahnarztpraxis, Krankenhaus, Psychotherapeut, Vorsorge- und Rehabilitation, Öffentlicher Gesundheitsdienst
  - (oid\_praxis\_arzt,, oid\_krankenhaus, oid\_institution-vorsorge-reha, oid\_zahnarztpraxis, oid\_praxis\_psychotherapeutoid\_institution-oegd)
- Apo = Öffentliche Apotheke
  - (oid\_öffentliche\_apotheke)
- Pflege = Gesundheits-, Kranken- und Altenpflege
  - (oid\_institution-pflege)
- GH = Geburtshilfe
  - (oid\_institution-geburtshilfe)
- HME = Heilmittelerbringer
  - (oid\_praxis-physiotherapeut, oid\_praxis-ergotherapeut, oid\_praxis-logopaede, oid\_praxis-podologe, oid\_praxis-ernaehrungstherapeut)
- AM = Arbeitsmedizin
  - (oid\_institution-arbeitsmedizin)
- KTR = Kostenträger
  - (oid\_kostentraeger)
- OM = Ombudsstelle
  - (oid\_ombudsstelle)
- DiGA = Digitale Gesundheitsanwendung
  - (oid\_diga)
- eRP = E-Rezept vertrauenswürdige Ausführungsumgebung
  - (oid\_erp-vau)
- Ver = Versicherter / Vertreter
  - (oid\_versicherter)

#### Legende:



- CRUD = create, read, update, delete; update: Aktualisierung von Metadaten, Aktualisierung eines Dokuments
- "-" = keine Zugriffsrechte;
- "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den Dienst (Service) definiert)
- "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung in einer zukünftigen Version der ePA vorgesehen.

Hinweise:

- (\*) Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann der Versicherte bzw. sein Vertreter oder eine Leistungserbringerinstitution gemäß der zuvor genannten Liste definierter professionOIDs sein. Sofern ein Versicherter/Vertreter der Einsteller der Elternnotiz ist, darf er abweichend von den oben aufgeführten Zugriffsunterbindungsregeln in die Datenkategorie mit dem technischen Identifier 'child' schreiben.

[<=]

#### **A\_26166-02 -Legal Policy (EU) - EU-Zugriff: gesetzlich vorgegebene Zugriffsrechte**

Das ePA-Aktensystem MUSS zusätzlich zu den Regeln aus A\_19303-\* alle in der folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

**Tabelle 20: Legal Policy - EU-Zugriff**

Kategorie	Nutzergruppe
<b>Technischer Identifier</b>	<b>NCPeH</b>
<b>Medical Services (XDS Document Service)</b>	<b>Zugriffsrecht gemäß § 352 SGB V</b>
reports	-
emp	-
emergency	R
eab	-
dental	-
child	-
childsrecord	-
pregnancy_childbirth	-

vaccination	-
patient	-
receipt	-
health_risk_analysis	-
diga	-
care	-
eau	-
rehab	-
transcripts	-
other	-
<b>Medical Services (FHIR Data Service)</b>	<b>Zugriffsrecht</b>
medication	-
<b>Basic Services</b>	<b>Zugriffsrecht</b>
Consent Decisions	-
Constraints	-
Entitlements	-
Entitlements.Blocked User	-
Audit Events	-
Information	x
Devices	-

Nutzergruppen:

- NCPeH = NCPeH-Fachdienst (oid\_ncpeh)

Legende:

- CRUD = create, read, update, delete; update: Aktualisierung von Metadaten, Aktualisierung eines Dokuments

- "-" = keine Zugriffsrechte;
- "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den Dienst (Service) definiert)
- "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung in einer zukünftigen Version der ePA vorgesehen.

[<=]

Die folgende Tabelle erläutert die Kategorien aus A\_19303-\* und A\_26166-\*:

**Tabelle 21: Beschreibung der Kategorien**

Technischer Identifier	Beschreibung
<b>Medical Services</b>	<b>XDS Document Service</b>
reports	Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen
emp	Elektronischer Medikationsplan
emergency	Daten der elektronischen Notfalldaten nach § 334 Absatz 1 Satz 2 Nummer 5 und 7
eab	Daten in elektronischen Briefen zwischen den an der Versorgung der Versicherten teilnehmenden Ärzten und Einrichtungen (elektronische Arztbriefe)
dental	Daten aus der zahnärztlichen Dokumentation
child	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
childsrecord	Archiv aus ePA 2.x: Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
pregnancy_childbirth	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass) sowie Daten, die sich aus der

	Versorgung der Versicherten mit Hebammenhilfe ergeben
vaccination	Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation)
patient	Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden
receipt	Bei Kostenträgern gespeicherte Daten über die in Anspruch genommenen Leistungen des Versicherten
health_risk_analysis	Ergebnisse datengestützter Auswertungen der Krankenkassen zu individuellen Gesundheitsrisiken gemäß SGB V § 25b.
diga	Daten des Versicherten aus digitalen Gesundheitsanwendungen des Versicherten nach § 33a.
care	Daten zur pflegerischen Versorgung des Versicherten nach den §§ 24g, 37, 37b, 37c, 39a und 39c und der Haus- oder Heimpflege nach § 44 des Siebten Buches und nach dem Elften Buch
eau	Daten nach § 73 Absatz 2 Satz 1 Nummer 9 ausgestellte Bescheinigung über eine Arbeitsunfähigkeit
rehab	Daten der Heilbehandlung und Rehabilitation nach § 27 Absatz 1 des Siebten Buches
transcripts	Elektronische Abschriften von der Patientenakte eines Primärsystems gemäß §630g Abs. 2 BGB
other	Sonstige von Leistungserbringern für Versicherten bereitgestellte Daten, insbesondere Daten, die sich aus der Teilnahme des Versicherten an strukturierten Behandlungsprogrammen bei chronischen Krankheiten gemäß § 137f ergeben
<b>Medical Services</b>	<b>FHIR Data Services</b>
medication	Verordnungs-, Dispensier- und Medikationsdaten in einer elektronischen Medikationsliste (eML) und einem elektronischen Medikationsplan (eMP)
demographics	Bereitstellung demographischer Daten des Versicherten für Medical Services
audit	Protokolle von Zugriffen aller Nutzer auf die Akte des Versicherten
documents	Suche & Bereitstellung (medizinischer) Dokumente aus dem XDS Document Service
<b>Basic Services</b>	<b>Account Management</b>

Consent Decisions	Management der Entscheidungen zu widerspruchsfähigen Funktionen der ePA
Constraints	Management der Konfiguration der General Deny Policy
Entitlements	Management der Befugnisse für Nutzer und Nutzergruppen
Audit Events	Abruf der Protokolleinträge eines Aktenkontos
Information	Informationen für nicht befugte Nutzer
Devices	Management der registrierten Geräte eines Nutzers

#### **A\_21211-01 -Legal Policy - Änderungen der Legal Policy nicht erlauben**

Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass Änderungen der Konfiguration der Legal Policy gemäß A\_19303-\* ausgeschlossen sind. [ $\leq$ ]

#### **A\_24548 -Legal Policy - Durchsetzung der Zugriffsrechte der Legal Policy**

Das ePA-Aktensystem MUSS sicherstellen, dass Operationen auf Daten und Operationen der Dienste eines Aktenkontos abgebrochen und mit einer Fehlermeldung beendet werden, wenn diese Operation durch die Vorgaben der Legal Policy gemäß A\_19303-\* für die Nutzergruppe des Aufrufers der Operation nicht zulässig ist. [ $\leq$ ]

### **3.11 Constraint Management**

Das Constraint Management des Aktenkontos stellt sicher, dass nur Zugriffe auf Daten in Ordnern des XDS Document Service über die Vorgaben der Legal Policy hinaus zugelassen werden, welche nicht vom Versicherten oder einem Vertreter unterbunden (verborgen) wurden.

Die Umsetzung dieser Beschränkungen erfolgt anhand der **General Deny Policy** für jeden befugten Nutzer der betroffenen Nutzergruppen des Aktenkontos.

Die General Deny Policy adressiert Nutzergruppen (professionOID) und Metadaten der Daten. Es können einzelne Dokumente, Kategorien oder Ordner verborgen werden. Bei jedem Zugriff auf Daten in Ordnern wird diese Policy bezüglich der Rolle eines Nutzers und der betroffenen Dokumente ausgewertet und durchgesetzt.

Die folgende Anforderung zeigt eine Übersicht der Nutzergruppen, für welche Dokumente durch Einträge in der General Deny Policy vor einem Zugriff verborgen werden können.

#### **A\_24306-02 -Constraint Management - Policy für berechtigte Nutzergruppen und Nutzer**

Das Constraint Management MUSS die Konfiguration der General Deny Policy auf die folgenden Nutzergruppen einschränken:

Nutzergruppe [professionOID] der General Deny Policy
oid_praxis_arzt

oid_krankenhaus
oid_institution-vorsorge-reha
oid_zahnarztpraxis
oid_öffentliche_apotheke
oid_praxis_psychotherapeut
oid_institution-pflege
oid_institution-geburtshilfe
oid_praxis-physiotherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin
oid_diga
oid_praxis-ergotherapeut
oid_praxis-logopaede
oid_praxis-podologe
oid_praxis-ernaehrungstherapeut

[<=]

#### **A\_24390-01 -Constraint Management- Anwendung der General Deny Policy**

Das Constraint Management MUSS bei jedem Zugriff auf Daten durch den XDS Document Service durch befugte Nutzer oder Nutzergruppen die General Deny Policy anwenden und den Zugriff verhindern, wenn ein Dokument oder dessen assoziierter Ordner oder dessen assoziierte Datenkategorie in der Policy konfiguriert ist.

[<=]

Dienste des Aktenkontos (Basic Services) können nicht verborgen werden. Hier gelten die Zugriffsregelungen gemäß Legal Policy und die Beschränkungen der Schnittstellen.

Datendienste (Medication Service) können nicht auf Daten- oder Ordner Ebene verborgen werden. Hier gelten die Regelungen bezüglich des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA (siehe [3.8- Consent Decision Management](#) ).

Die Kategorie "emp", bzw. einzelne Dokumente dieser Kategorie, des XDS Document Service dürfen nicht verborgen werden. Die Nutzung der Dokumente der Kategorie "emp" wird über das Consent Decision Management, bzw. einen erteilten Widerspruch gegen die widerspruchsfähige Funktion "medication" der ePA verhindert (siehe [3.8- Consent Decision Management](#) ).

Die Operationen der Schnittstelle des Constraint Managements erlauben die Konfiguration der General Deny Policy durch den Versicherten oder einen befugten Vertreter.

### **A\_24395 -Constraint Management - Realisierung der Schnittstelle**

#### **I\_Constraint\_Management\_Insurant**

Das Constraint Management MUSS die Operationen der Schnittstelle I\_Constraint\_Management\_Insurant gemäß [I\_Constraint\_Management\_Insurant] umsetzen.[<=]

### **A\_24887-01 -Constraint Management - Protokolleinträge für Zugriffe auf das Constraint Management**

Das Constraint Management MUSS für das Aufnehmen und Löschen von Einträgen in die General Deny Policy jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen. Dabei ist folgende Wertbelegung zu berücksichtigen:

**Tabelle 22: Constraint Management Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die API
	"object"		Bei intern ausgelösten Änderungen (XDS Document Service confidentiality code ("CON"), Löschen von Dokumenten oder Ordern)
AuditEvent.action	C, D		
AuditEvent.entity.name	"GeneralDenyPolicy"		Eintrag für das Aufnehmen(Create) von Einträgen in die oder Löschen (Delete) von Einträgen aus der General Deny Policy
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"DocumentTitle"	<XDSDocumentEntry.title>	wenn sich der Eintrag (Create oder Delete) der Policy auf ein Dokument bezieht
	"RootDocumentId"	<rootDocumentId>	wenn sich der Eintrag (Create oder Delete) der Policy auf ein Dokument bezieht



	"FolderTitle"	<XDSFolder.title>	wenn sich der Eintrag (Create oder Delete) der Policy auf einen Folder bezieht
	"FolderEntryUUID"	<Folder.entryUUID>	wenn sich der Eintrag (Create oder Delete) der Policy auf einen Folder bezieht
	"CategoryId"	<categoryId>	wenn sich der Eintrag (Create oder Delete) der Policy auf eine Kategorie bezieht

[<=]

Für die Policy gelten folgende Vorgaben.

#### **A\_24393-01 -Constraint Management - Initialisierung der General Deny Policy**

Das Constraint Management MUSS für ein Aktenkonto eine General Deny Policy ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policy über die Schnittstelle I\_Constraint\_Management\_Insurant gemäß [I\_Constraint\_Management\_Insurant] ermöglichen.[<=]

#### **A\_24462-01 -Constraint Management - Konfiguration der General Deny Policy anpassen nach Löschen von Ordnern**

Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn diese einen Ordner referenzieren und dieser Ordner aus dem Aktenkonto gelöscht wird. [<=]

#### **A\_24461-01 -Constraint Management - Konfiguration der General Deny Policy anpassen nach Löschen von Dokumenten**

Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn diese ein spezifisches Dokument referenzieren und dieses Dokument aus dem Aktenkonto gelöscht wird.[<=]

#### **A\_24516-01 -Constraint Management - Speichern der Inhalte der General Deny Policy**

Das Constraint Management MUSS Einträge aus der General Deny Policy unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.[<=]

### **3.11.1 Aktenkontoweites Verbergen (General Deny Policy)**

Die General Deny Policy wird durch das Aktensystem für die in A\_24306-\* unter "General Deny Policy" aufgeführten Nutzergruppen angewendet und durchgesetzt. Einträge der General Deny Policy gelten dabei immer für alle aufgeführten Nutzergruppen gemeinsam.

Die Konfiguration der General Deny Policy erfolgt durch den Versicherten oder einen befugten Vertreter mittels ePA-FdV. Einträge können hinzugefügt oder entfernt werden. Zum Zeitpunkt der Erstellung des Aktenkontos enthält die General Deny Policy keine Einträge.

Ein Eintrag in der General Deny Policy referenziert entweder ein bestimmtes Dokument, einen dynamischen Ordner oder eine Datenkategorie. Die Menge der Einträge ist nicht limitiert.

Jeder Eintrag der General Deny Policy verbirgt die betroffenen Daten und verhindert deren Nutzung durch Nutzergruppen gemäß A\_24306-\*. Enthält ein Eintrag der Policy einen dynamischen Ordner oder eine Kategorie, so werden alle in diesem Ordner bzw. Kategorie enthaltenen Daten verborgen und von der Nutzung ausgeschlossen. Ein dynamischer Ordner selbst wird ebenfalls verborgen und von der Nutzung ausgeschlossen, eine Kategorie selbst wird nicht verborgen. Verborgene Daten schränken die Anwendung der Datenoperationen ein, die konkreten Auswirkungen sind bei den jeweiligen Operationen definiert.

Beim kategorienbasierten Verbergen von dynamischen Ordnern kann ein einzelner Ordner oder die Datenkategorie an sich verborgen werden. In letzterem Fall werden alle assoziierten Ordner verborgen.

Bei Kategorien und Ordnern, die zusammengesetzte MIOs oder strukturierte Dokumente enthalten (MIOs oder strukturierte Dokumente, deren Inhalt über mehrere XDS Dokumente mit Zusammenhang verteilt ist - "Passdokumente") ist das Verbergen einzelner XDS Dokumente des MIOs nicht sinnvoll und daher nicht zulässig. In diesen Fällen erfolgt das Verbergen der Daten durch das Verbergen der Kategorie bzw. des dynamischen Ordners. Diese Einschränkung betrifft die Sammlungstypen "mixed" und "uniform".

Für das erfolgreiche Verbergen von Daten durch Einträge der General Deny Policy muss das adressierte XDS Dokument, der Ordner oder die Kategorie im Aktensystem vorhanden sein. Wird im Verlauf von Operationen ein XDS Dokument oder ein Ordner gelöscht, so werden auch die referenzierenden Policy-Einträge automatisch entfernt (siehe A\_24461-\* und A\_24662-\*).

Ein Eintrag der General Deny Policy enthält Angaben gemäß der folgenden Tabelle:

**Tabelle 23: Inhalt eines General Deny Policy Eintrags**

Element		Inhalt	Erläuterung
denyType		"document" oder "folder" oder "category"	Art des zu verbergenden Inhalts,
parameter:			eine technische Referenz passend zu "denyType"
[choice]	rootDocumentId	documentEntry.referenceIdList, Item "rootDocumentUniqueId"	Identifiziert das zu verbergende XDS Dokument
	folderUUID	folder.entryUUID	Identifiziert das zu verbergende dynamische Ordner
	categoryId	categoryId	technischer Identifizierer der zu verbergenden Kategorie

Beispiel:

Tabelle 24: Verbergen eines Medical Service

General Deny Policy - Verbergen der Datenkategorie "dental" (Daten aus der zahnärztlichen Dokumentation)		
denyType		"category"
parameters:		
	categoryId	"dental"

### 3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes

Das Verbergen über den confidentialityCode ist im Kontext der Operationen des XDS Document Service definiert und in 3.13.1.10- Verbergen von Dokumenten durch Verwendung des confidentialityCode beschrieben.

## 3.12 Device Management

Die Geräteverwaltung ermöglicht ePA-FdVs die Registrierung und Verwaltung der vom Nutzer verwendeten Geräte. Das Device Management stellt das API zum ePA-FdV für die Geräteverwaltung bereit und ist nur in einer VAU/authentisierten User Session erreichbar.

Im Folgenden wird als **Home-AS** eines Versicherten das ePA-Aktensystem desjenigen Betreibers bezeichnet, der vom Kostenträger des Versicherten beauftragt wurde. Falls der Versicherte der Anlage eines Aktenkontos nicht widersprochen hat, wird sein Aktenkonto im Home-AS verwaltet. Im Falle von Vertretern kann es vorkommen, dass das Home-AS des zu vertretenden Versicherten nicht das Home-AS des Vertreters ist.

Die E-Mail-Adressen und die Geräte eines Versicherten werden ausschließlich im Home-AS des Versicherten verwaltet. Für Vertreter, deren Home-AS nicht das Home-AS des Versicherten ist, können im Home-AS des Versicherten die im Home-AS des Vertreters registrierten Geräte nachgenutzt werden. Das ePA-Aktensystem bietet dem ePA-FdV eine Schnittstelle, über die die durch das Home-AS signierte Geräteinformationen abgerufen werden können.

Bei erstmaliger Nutzung des Gerätes initiiert das ePA-FdV die Geräteregistrierung und erhält dadurch eine DeviceID (bestehend aus deviceIdentifier und deviceToken), welche bei folgenden Verwendungen des ePA-FdV zur Identifizierung des Geräts verwendet wird. Eine neue Geräteregistrierung muss durch den Nutzer bestätigt werden. Der Zugriff auf ein Aktenkonto kann nur mit einem Gerät mit bestätigter Geräteregistrierung erfolgen.

Das Device Management ermittelt dazu die für den Nutzer im ePA-Aktensystem hinterlegte E-Mail-Adresse und versendet bei der Geräteregistrierung eine E-Mail an den Nutzer mit einem generierten Geräteregistrierungscode (confirmationCode). Der Nutzer sendet den Geräteregistrierungscode unter Verwendung des ePA-FdV zurück an das Device Management und bestätigt dadurch die Registrierung des neuen Geräts. Das Gerät kann nach der Bestätigung uneingeschränkt mit einem Aktenkonto genutzt werden.

### A\_24828 -Device Management - Realisierung der Schnittstelle

#### I\_Device\_Management\_Insurant

Das Device Management MUSS die Operationen der Schnittstelle

I\_Device\_Management\_Insurant gemäß [I\_Device\_Management\_Insurant] umsetzen.

[<=]

#### **A\_25164 -Device Management - Beschränkung der Schnittstellenoperationen auf Geräte des Nutzers**

Das Device Management MUSS die Operationen der Schnittstelle I\_Device\_Management\_Insurant gemäß [I\_Device\_Management\_Insurant] auf die Geräte des aufrufenden Nutzers einschränken.[<=]

#### **A\_26153 -Device Management - Nutzen von Device Management auch bei Widerspruch gegen Aktenkonto**

Das Device Management MUSS sicherstellen, dass das Device Management auch von Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben.[<=]

#### **A\_26154-01 -ePA-Aktensystem - Ausschließlich Nutzen von Email Management und Device Management bei Widerspruch**

Das ePA-Aktensystem MUSS sicherstellen, dass Versicherte, die einem Aktenkonto widersprochen haben, für sich selbst ausschließlich das Email Management und das Device Management nutzen können.[<=]

#### **A\_26155 -Device Management - Versicherte nutzen Device Management ausschließlich im Home-AS**

Das Device Management des ePA-Aktensystems MUSS sicherstellen, dass das Device Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-Aktensystem das Home-AS ist.[<=]

#### **A\_24979 -Device Management - Sicheres Löschen von Geräten**

Das Device Management MUSS beim Entfernen eines Gerätes sicherstellen, dass das Gerät gelöscht ist und dass das Gerät nicht mehr als verifiziertes Gerät genutzt werden kann.[<=]

#### **A\_17947-03 -Device Management - Gültigkeitszeitraum und Löschung der Devicekennung**

Das Device Management MUSS jede generierte und zu einem Nutzer gespeicherte Geräteregistrierung nach 2 Jahren löschen und darf Nutzeranfragen mit dieser Device-Kennung nach diesem Zeitpunkt nicht mehr akzeptieren.  
[<=]

Hinweis zu A\_17947-\*: Der Hersteller des ePA-FdVs kann die Nutzerführung seines ePA-FdVs so gestalten, dass der Versicherte auf ein baldiges Auslaufen der Registrierung hingewiesen wird und automatisch eine neue Registrierung vom ePA-FdV am Aktensystem ausgelöst wird.

#### **A\_14595-02 -Device Management - Pflegeprozess Geräteverwaltung**

Das Device Management MUSS die interne Liste aller bekannten Geräte derart pflegen, dass ein Gerät nach spätestens 1 Jahr nach der letzten Nutzung des Gerätes automatisch aus der Liste der registrierten Geräte gelöscht wird.[<=]

Hinweis zu A\_14595-\*: Der Abruf einer Device Attestation durch ein registriertes Gerät gilt ebenfalls als eine Nutzung dieses Geräts.

#### **A\_25270 -Device Management - Erzeugung von Geräteinformationen und Geräteregistrierungscode bei der Geräteregistrierung**

Das Device Management MUSS bei der Geräteregistrierung für das zu registrierende Gerät eines Nutzers

- einen deviceIdentifier als aktensystemweit eindeutigen Gerätebezeichner (uuid),
- ein deviceToken als eine Zufallszahl als String mit 64 Zeichen mit einer Mindestentropie von 120 Bit gemäß [gemSpec\_Krypt#GS-A\_4367] und
- eine zufällige sechsstellige natürliche Zahl als Geräteregistrierungscode erzeugen.[<=]

**A\_25271-01 -Device Management - Speicherung der Geräteinformationen**

Das Device Management MUSS bei einer Geräteregistrierung eines Geräts eines Nutzers folgende Inhalte für den Nutzer verschlüsselt persistieren:

- deviceIdentifizier
- deviceToken
- createdAt (Zeitpunkt der Erzeugung des deviceTokens)
- lastUse
- status
- displayName
- Geräteregistrierungscode,
- Fehlerzähler.

[<=]

Hinweis zu A\_25271-\*: Für die verschlüsselte Speicherung der Geräteinformationen sind die Anforderungen aus Abschnitt 3.5.1.3 zu berücksichtigen.

**A\_25272 -Device Management - Pseudonyme Speicherung der Geräteinformationen**

Das Device Management MUSS sicherstellen, dass die Zuordnung der außerhalb der VAU persistierten verschlüsselten Geräteinformationen zum Nutzer eindeutig ist und durch ein Pseudonym erfolgt.[<=]

Hinweis: Aus A\_25272 folgt, dass die Zuordnung der Speicherung der verschlüsselten Geräteinformationen nicht über die KVN der Nutzer erfolgen darf.

**A\_25273 -Device Management - Gültigkeitsdauer des Geräteregistrierungscodes**

Das Device Management MUSS sicherstellen, dass der bei der Geräteregistrierung erzeugte Geräteregistrierungscode maximal 6 Stunden nach Erzeugung der DeviceID (createdAt) für die Verifikation eines Gerätes genutzt werden kann.[<=]

**A\_25274 -Device Management - Löschen nach Gültigkeitsdauer des Geräteregistrierungscodes**

Das Device Management MUSS sicherstellen, dass die Geräteinformationen für eine nicht bestätigte Geräteregistrierung nach Ende der Gültigkeitsdauer des Geräteregistrierungscodes gelöscht werden.[<=]

**A\_25275 -Device Management - Versenden des Geräteregistrierungscodes per E-Mail**

Das Device Management MUSS bei der Geräteregistrierung für den Nutzer, für den das Gerät registriert werden soll, alle im Aktensystem hinterlegten E-Mail-Adressen ermitteln und an alle ermittelten E-Mail-Adressen eine E-Mail in einer für den Nutzer verständlichen Form mit folgenden Informationen versenden:

- Zweck der E-Mail,
- Geräteregistrierungscode,
- Gültigkeitsdauer des Geräteregistrierungscodes.

[<=]

**A\_25276 -Device Management - Bestätigung mittels Geräteregistrierungscodes**

Das Device Management MUSS für einen übergebenen Geräteregistrierungscode und eine übergebene DeviceID (deviceIdentifizier und deviceToken) prüfen, ob der vom Device Management bei der Geräteregistrierung erzeugte Geräteregistrierungscode für das angegebene Gerät (deviceIdentifizier, deviceToken) mit dem übergebenen

Gerätregistrierungscode übereinstimmt sowie der Gerätregistrierungscode zeitlich gültig ist und

1. bei Gleichheit und
  - a. zeitlicher Gültigkeit
    - den Status für die Gerätregistrierung wechseln, so das die erfolgreiche Bestätigung des Geräts aus dem Status hervorgeht,
    - den Gerätregistrierungscode und den Fehlerzähler aus den Geräteinformationen löschen und
    - den Zeitpunkt der erfolgreichen Bestätigung in lastUsed erfassen,
  - b. zeitlicher Ungültigkeit
    - alle Geräteinformationen zu diesem deviceIdentifizier löschen,
2. bei Ungleichheit den Fehlerzähler der Geräteinformation um eins erhöhen und
  - falls der Fehlerzähler größer oder gleich fünf ist,
  - alle Geräteinformationen zu diesem Gerät löschen.

**[<=]**

#### **A\_25277 -Device Management - Sperrung bei vermehrter Anzahl von abgebrochenen Gerätregistrierungen**

Falls für einen Nutzer innerhalb von 8 Stunden drei Gerätregistrierungen abgebrochen werden mussten, MUSS das Device Management sicherstellen, dass dieser Nutzer für 8 Stunden ab dem Zeitpunkt der dritten abgebrochenen Gerätregistrierung keine Geräte mehr registrieren darf.**[<=]**

#### **A\_25291 -ePA-Aktensystem - Health Record Context nur mit verifizierten Gerät**

Das ePA-Aktensystem MUSS sicherstellen, dass ein Versicherter (auch wenn er als Vertreter agiert) einen Health Record Context ausschließlich mit einem verifizierten Gerät öffnen kann, außer für den Fall, dass sich der Versicherte am ePA-FdV des Vertreters anmeldet (d.h. x-authorize-representative=True bei der Operation `I_Authorization_Service::sendAuthorizationRequestFdV`).**[<=]**

Eine Gerätregistrierung im Home-AS kann in einem anderen Aktensystem nachgenutzt werden. Hierzu kann ein ePA-FdV mittels `getDeviceAttestation` eine Device Attestation vom Home-AS abrufen, welche beim anderen Aktensystem genutzt werden kann.

#### **A\_26157 -Device Management - Device Attestation kann nur mit verifiziertem Gerät abgerufen werden**

Das Device Management MUSS sicherstellen, dass die Operation `getDeviceAttestation` ausschließlich nach erfolgreicher Authentifizierung des Nutzers und mit einem auf den Nutzer registrierten und verifizierten Gerät erfolgt.

**[<=]**

#### **A\_26156 -Device Management - Inhalte der Device Attestation**

Das Device Management MUSS sicherstellen, dass eine von einem ePA-FdV über die Operation `getDeviceAttestation` abgerufene Device Attestation folgende Inhalte enthält:

Attribut	Inhalt
actorId	KVNR aus dem ID-Token des angemeldeten Nutzers (bzw. der User Session)
iat	Zeitstempel Ausgabezeitpunkt

exp	Verfalldatum, = "iat" + 2 Stunden
-----	-----------------------------------

[<=]

#### **A\_26158 -Device Management - Signatur der Device Attestation**

Das Device Management MUSS sicherstellen, dass die über `getDeviceAttestation` abgerufene Device Attestation mit dem privaten Schlüssel der Signaturidentität der VAU des Home-AS signiert wird.[<=]

### **3.13 Medical Services**

#### **A\_25830-02 -Medical Services - Reihenfolge der Auswertung Legal Policy, Consent Decisions und Constraints**

Die Medical Services MÜSSEN bei der Ausführung von Operationen der Schnittstellen der Medical Services sicherstellen, dass die Prüfung zu Bedingungen

1. der Einschränkung der Rolle des Aufrufenden (oid),
2. der Existenz des Aktenkontos (Status UNKNOWN oder INITIALIZED),
3. des Zustands des Aktenkontos (Status ACTIVATED),
4. der Befugnis des Aufrufenden,
5. der Legal Policy,
6. der Entscheidungen zu widerspruchsfähigen Funktionen der ePA,
7. der Einträge der General Deny Policy
8. des Entscheidungen zum nutzerspezifischen Ausschluss von der Teilnahme am digital gestützten Medikationsprozess

in der dargestellten Reihenfolge erfolgt. Diese Reihenfolge MUSS auch eingehalten werden, wenn einzelne Prüfungen für eine Operation nicht anwendbar, bzw. nicht relevant, sind.[<=]

*Hinweis: Eine Operation kann nicht erfolgreich ausgeführt werden, weil dieses der Legal Policy widerspricht und weil ein Eintrag der General Deny Policy die Ausführung verhindert. Die Fehlermeldung zum Abbruch der Operation resultiert dann aus der Prüfung der Legal Policy, da die Bedingungen dieser gemäß der definierten Reihenfolge vor den Bedingungen der General Deny Policy geprüft werden müssen.*

#### **3.13.1 XDS Document Service**

Die gesetzlichen Vorgaben schränken den Zugriff Dritter auf Dokumente über berufsgruppenspezifische Vorgaben gemäß 341 Absatz 2 SGB V ein. Dazu verwendet der XDS Document Service festgelegte Datenkategorien, welche mit spezifischen Zugriffsrechten der grundlegenden Zugriffsoperationen (CRUD - create, read, update, delete) wirken.

Jedes eingestellte Dokument wird vom XDS Document Service mit einer automatischen Zuordnung zu einem statischen Ordner, welcher die Datenkategorie repräsentiert, erweitert. Diese statischen Ordner sind initial bei jedem Aktenkonto eines Versicherten existent. Die serverseitige Zuordnung in diese Ordner erfolgt anhand der XDS-Metadaten in Kombination mit der Nutzergruppe des Einstellers.

Das bedeutet weiterhin, dass das Anlegen von statischen Ordnern durch ePA-Clients nicht erlaubt ist, um eine zweifelsfreie Anwendung der Zugriffsregeln auf Grundlage der Datenkategorien zu gewährleisten.



Eine Ausnahme bilden bestimmte medizinische Informationsobjekte (MIOs), die eine weitere Gruppierung innerhalb der zugeordneten Datenkategorie erfordern. Ein Beispiel dafür ist der Mutterpass. Die Dokumente eines Mutterpasses müssen für die konkrete Schwangerschaft innerhalb der Kategorie separiert werden. Für die betroffenen Kategorien wird daher kein statischer Ordner vorbereitet, sondern der separierende, dynamische Ordner muss zeitgleich mit einer Dokumentenregistrierung durch den ePA-Client angelegt werden,

ePA-Clients, die Dokumente für MIOs einstellen, können die dem MIO zugeordnete Kategorie und die Art des Ordners (statisch, dynamisch) aus den Metadatenvorgaben für MIOs gemäß [Implementation-Guidelines] entnehmen.

Die Durchsetzung der Zugriffskontrolle auf die Kategorien, Ordner und Dokumente gemäß der gesetzlichen Vorgaben und ggf. weiterer Beschränkungen durch den Versicherten oder einen Vertreter erfolgt durch das Constraint Management (siehe 3.11- Constraint Management ).

### 3.13.1.1 Formatprüfung beim Einstellen von Dokumenten

#### **A\_25233 -XDS Document Service - erlaubte Formate für PDF-Dokumente**

Der XDS Document Service MUSS sicherstellen, dass ausschließlich die folgenden PDF/A-Formate unterstützt werden:

- PDF/A-1a
- PDF/A-1b
- PDF/A-2a
- PDF/A-2u
- PDF/A-2b

[<=]

#### **A\_24864-04 -XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten**

Der XDS Document Service MUSS beim Einstellen eines Dokumentes prüfen, dass das Dokument eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und den in Klammern angegebenen Dateiendungen (DocumentEntry.URI) besitzt

- application/pdf nur PDF/A gemäß A\_25233 (pdf)
- text/plain (txt)
- application/xml (xml)
- application/hl7-v3 (xml)
- application/pkcs7-mime (p7s oder p7)
- application/fhir+xml (xml)
- application/fhir+json (json)
- application/json (json)

sowie der tatsächliche Inhalt des Dokuments konform mit dem behaupteten MIME-Type ist. Falls die Prüfung nicht erfolgreich ist, muss das Einstellen des Dokumentes abgelehnt werden.[<=]

*Hinweise zu A\_24864-\*:*

- *Dokumente im PDF-Format werden vom XDS Document Service abgelehnt, da sie ausführbaren Code enthalten können. Daher müssen die Clients, falls sie Dokumente im PDF-Format einstellen wollen, diese zunächst in ein PDF/A konvertieren.*

- *p7s ist die Default-Dateiendung für Dokumente des mimetypes application/pkcs7-mime in der ePA und für Dokumente dieses mimetypes gemäß [gemSpec\_IG\_ePA] und für automatisierte Anpassungen von filename extensions bei Dokumentenupload (A\_23447-\*, A\_24451-\*) zu berücksichtigen.*

### **A\_25009-03 -XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten durch Versicherte**

Der XDS Document Service MUSS sicherstellen, dass Versicherte ausschließlich Dokumente eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und den in Klammern angegebenen Dateiendungen (DocumentEntry.URI) einstellen können:

- application/pdf nur PDF/A gemäß A\_25233 (pdf)
- text/plain (txt)
- application/fhir+xml (xml)
- application/json (json)

Ferner MUSS der XDS Document Service sicherstellen, dass ausschließlich die Elternnotiz des Kinderuntersuchungshefts als FHIR Document mit dem MIME-Type "application/fhir+xml" registriert werden kann - andere FHIR Documents sind nicht zulässig.

**[<=]**

*Hinweise zu A\_24864-\* und A\_25009-\*: Die Prüfung des zulässigen Dokumentenformats muss mindestens*

- *bei allen Formaten eine Prüfung auf Magic Bytes (soweit technisch möglich),*
- *bei txt-, XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es bei XML-Dokumenten kein valides UTF8 ist, prüfen auf "restriktives" ISO-8859-15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09, 0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind.",*
- *bei XML-, und JSON-Dokumenten eine Prüfung der XML- bzw. JSON-Validität mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet sind,*
- *auf den signierten Inhalt eines PKCS7-Dokuments sind die Regeln ebenfalls anzuwenden*

*umfassen. Eine alleinige Prüfung auf Basis der Magic Bytes ist für kein Format ausreichend. Werden keine zusätzlichen Prüfmaßnahmen durchgeführt, dürfen die Dokumente nicht in die Akte eingestellt werden können.*

*Für XML-Dokumente muss eine Schema-Validierung ausschließlich auf Basis bekannter, intern vorliegender XML Schema-Definitionen durchführen. Gegen nicht intern vorliegende XML Schema-Definitionen wird nicht validiert. Die Schema-Validierung kann innerhalb des Health Record Contexts ohne zusätzliche Isolation erfolgen.*

### **A\_24867 -XDS Document Service - Isolation der Formatprüfung**

Der XDS Document Service MUSS die Prüfung des Dateiformats (siehe A\_24864-\*) beim Einstellen eines Dokuments so technisch isolieren, dass kein Schaden für Aktenkonten oder das ePA-Aktensystem selbst entsteht.

**[<=]**

*Hinweise zu A\_24867-\*:*

*Hier kann z.B. eine Art Sandboxing oder eine separate VAU-Instanz verwendet werden, um die Isolation umzusetzen.*

Der in A\_24636-\* geforderte technische Separationsmechanismus zur Isolation von Health Record Contexten innerhalb einer VAU-Instanz kann ebenfalls zur Isolation der Formatprüfung in A\_24867-\* genutzt werden.

Findet eine Dokumentenformatprüfung innerhalb eines Health Record Context statt, wird durch den Isolationsmechanismus aus A\_24636-\* verhindert, dass sich die Dokumentenformatprüfung schadhaft auf andere Health Record Contexte auswirkt. Es verbleibt dann zur Umsetzung der A\_24867-\* noch zu gewährleisten, dass sich die Dokumentenformatprüfung nicht schadhaft auf den Health Record Context auswirkt, in dem die Dokumentenformatprüfung erfolgt.

Wenn Dokumentenprüfungen innerhalb eines Health Record Contexts ohne Isolation erfolgen, muss sichergestellt werden, dass sich diese Prüfungen nicht schadhaft auf den Health Record Context (oder andere) auswirken können. Dies ist vom Produktgutachter zu prüfen und im Produktgutachten zu dokumentieren.

Ein Ausschluss einer schadhaften Auswirkung auf den Health Record Context ist bei folgenden Prüfungen des Dokumentenformats denkbar, so dass diese innerhalb des Health Record Contexts ohne zusätzliche Isolationsmaßnahmen durchgeführt werden können und kein Verstoß gegen die Anforderung A\_24867-\* vorliegt:

- Prüfung der Magic Bytes des Dokuments (wo technisch möglich)
- bei txt-, XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es bei XML-Dokumenten kein valides UTF8 ist, eine Prüfung auf "restriktives" ISO-8859-15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09, 0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind.",
- bei XML- und JSON-Dokumenten: Parsen der Dokumente auf valides XML bzw. JSON mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu bestätigen.
- bei pkcs7-Dokumenten: Parsen der Dokumente mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu bestätigen.

Der Produktgutachter muss bei der Umsetzung der oben genannten Prüfungen bestätigen, dass der Ausschluss einer schadhaften Auswirkung auf den Health Record Context (oder andere) durch die Umsetzung im Produkt tatsächlich gegeben ist.

#### **A\_25285 -XDS Document Service - Sicheres Löschen von Dokumenten mit unzulässigem Format**

Falls der XDS Document Service bei der Prüfung des Dateiformats (siehe A\_24864-\*) beim Einstellen eines Dokuments ein unzulässiges Format erkennt, MUSS der XDS Document Service das Dokument sicher löschen.

[<=]

#### **A\_24943 -XDS Document Service - Formatprüfung exponiert keine Daten aus der VAU heraus**

Der XDS Document Service MUSS sicherstellen, dass bei der Formatprüfung (siehe A\_24864-\*) keine innerhalb der VAU verarbeiteten Daten die VAU verlassen.[<=]

### **3.13.1.2 Anforderungen zur Validierung**

#### **A\_15035 -XDS Document Service - Verwendung von SOAP Message Security 1.1**

Der XDS Document Service MUSS die Sicherheitsanforderungen aus SOAP Message Security 1.1 [WSS] für die Verarbeitung von SOAP 1.2-Nachrichten umsetzen.[<=]

#### **A\_15034 -XDS Document Service - Unterstützung von Profilen der Web Services Interoperability Organization (WS-I)**

Der XDS Document Service MUSS das WS-I Basic Profile V2.0 [WSIBP], das WS-I Basic Security Profile Version V1.1 [WSIBSP] sowie das WS-I Attachment Profile V1.0 [WSIAP] für die Kommunikation über Web Services berücksichtigen. [≤=]

#### **A\_15186 -XDS Document Service - Prüfung der Kombination von WS-Addressing Action und SOAP Body**

Der XDS Document Service MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-Eingangsnachrichten dahingehend prüfen, ob die angegebene WS-Addressing Action zum SOAP Body passt. Ist diese Kombination nicht passend, MUSS der XDS Document Service die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und die Verarbeitung der Nachricht abbrechen. [≤=]

#### **A\_15585 -XDS Document Service - Gleichheit von SOAP Action und WS-Addressing Action**

Der XDS Document Service MUSS SOAP 1.2-Eingangsnachrichten mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und die Verarbeitung der Nachricht abbrechen, falls die Werte aus SOAP Action (HTTP Header) und des Action-Elements [WSA] des SOAP Headers nicht übereinstimmen. [≤=]

#### **A\_14465-01 -XDS Document Service - XML Schema-Validierung für SOAP-Eingangsnachrichten**

Der XDS Document Service MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-Eingangsnachrichten einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen und gemäß [SOAP] verarbeiten. Sind Nachrichten nicht wohlgeformt oder ungültig, MUSS der XDS Document Service die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren. [≤=]

#### **A\_14809 -XDS Document Service - Keine Verwendung des "xsi:schemaLocation"-Attributs**

Der XDS Document Service MUSS SOAP 1.2-Eingangsnachrichten mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren, falls ein `xsi:schemaLocation`-Attribut gemäß [XMLSchema#2.6.3] enthalten ist. [≤=]

#### **A\_14811-01 -XDS Document Service - Ablehnung von SOAP 1.2-Nachrichten ohne UTF-8 Kodierung**

Der XDS Document Service MUSS SOAP 1.2-Nachrichten dahingehend prüfen, dass diese der Zeichenkodierung UTF-8 entsprechen, und andernfalls die Operation einem geeigneten HTTP-Statuscode gemäß [RFC7231] ablehnen. [≤=]

#### **A\_21200 -XDS Document Service und Clients - UTF-8 Kodierung von SOAP 1.2-Nachrichten**

Der XDS Document Service und Clients des XDS Document Service MÜSSEN sicherstellen, dass die XML-Inhalte der SOAP 1.2-Nachrichten, die sie senden, der Zeichenkodierung UTF-8 entsprechen. [≤=]

Es ist zu beachten, dass sich die Anzeige der verwendeten Kodierung in der Nachricht unterscheiden kann, z. B. in Nachrichten, in denen MTOM verwendet wird.

### **3.13.1.3 Namensräume**

Für die Spezifikation der Schnittstellen des XDS Document Service werden die folgenden XML-Präfixe verwendet, um den Namensraum bzw. das Vokabular des XML-Dokuments zu kennzeichnen.

Präfix	Namensraum
lcm	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0

rmd	urn:ihe:iti:rmd:2017
rs	urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0
wsa	http://schemas.xmlsoap.org/ws/2004/08/addressing
wss	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
xdsb	urn:ihe:iti:xds-b:2007
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

### 3.13.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von Dokumenten

#### 3.13.1.4.1 Anforderungen an IHE ITI-Akteure

In diesem Abschnitt werden Anforderungen und Einschränkungen an relevante IHE ITI-Akteure und -Transaktionen des XDS Document Service gestellt, um die geforderte IHE ITI-Semantik zum ePA-Aktensystem zu bewahren. Werden IHE ITI-Akteure mit weiteren Sub-Akteuren gruppiert, so werden die Anforderungen der Sub-Akteure zum gruppierten Akteur übernommen. Eine Übersicht und Herleitung der IHE ITI-Akteure ist [3.13.1.4.2-Überblick über gruppierte IHE ITI-Akteure und Optionen](#) zu entnehmen.

*Hinweis: Alle spezifizierten Anforderungen der IHE ITI-Akteure definieren das zu implementierende Verhalten an den Außenschnittstellen `I_Document_Management` sowie `I_Document_Management_Insurant`.*

#### **A\_17826-01 -XDS Document Service - Außenverhalten der IHE ITI-Implementierung**

Der XDS Document Service DARF NICHT vom Verhalten der definierten Außenschnittstellen `I_Document_Management`, sowie `I_Document_Management_Insurant` aus Abschnitt [3.13.1.6](#) abweichen. Dies schließt über die Anforderungslage hinausgehende Implementierungen von IHE ITI-Akteuren und Optionen innerhalb des XDS Document Service mit ein, sodass zusätzlich implementierte IHE-Funktionalitäten keine Auswirkungen an den definierten Außenschnittstellen aufweisen dürfen. [ $\leq$ ]

#### **A\_13806 -XDS Document Service - Implementierung des IHE ITI-Akteurs XDS Document Registry**

Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Registry" gemäß [IHE-ITI-TF1] implementieren. [ $\leq$ ]

#### **A\_14727 -XDS Document Service - Implementierung des IHE ITI-Akteurs XDS Document Repository**

Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]

Die § 291a-konforme Protokollierung von Zugriffen erfolgt mit Mechanismen außerhalb des IHE ITI-TF. Eine technische Protokollierung via ATNA kann gemäß der Anforderung A\_17826 dennoch erfolgen.

**A\_13809 -XDS Document Service - Keine Implementierung des IHE ITI-Akteurs ATNA Audit Record Repository**

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "ATNA Audit Record Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]

Die Mechanismen der IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure Application" zur Node Authentication werden über das Konzept "Vertrauenswürdige Ausführungsumgebung" (siehe 3.5- Vertrauenswürdige Ausführungsumgebung (VAU)) umgesetzt, sodass die Nutzung des Integrationsprofils ATNA diesbzgl. eingeschränkt wird.

**A\_17166 -XDS Document Service - Keine Implementierung der IHE ITI-Akteure ATNA Secure Node sowie ATNA Secure Application für Node Authentication**

Der XDS Document Service DARF zur Node Authentication die IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure Application" gemäß [IHE-ITI-TF1] NICHT implementieren. [≤]

Der Zeitdienst der Telematikinfrastruktur unterstützt das Network Time Protocol in Version 4. Das IHE ITI-TF verlangt hingegen, das Zeitsynchronisierungsprotokoll in Version 3.

**A\_14654 -XDS Document Service - Keine Implementierung des IHE ITI-Akteurs CT Time Client**

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "CT Time Client" gemäß [IHE-ITI-TF1] implementieren. [≤]

**A\_14665 -XDS Document Service - Keine Implementierung des IHE ITI-Akteurs XDS Document Source**

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Source" gemäß [IHE-ITI-TF1] implementieren. [≤]

**A\_14667 -XDS Document Service - Keine Implementierung des IHE ITI-Akteurs XDS Integrated Document Source/Repository**

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Integrated Document Source/Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]

**A\_14668 -XDS Document Service - Keine Implementierung des IHE ITI-Akteurs XDS Document Consumer**

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Consumer" gemäß [IHE-ITI-TF1] implementieren. [≤]

**A\_14666 -XDS Document Service - Keine Implementierung des IHE ITI-Akteurs XDS Patient Identity Source**

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Patient Identity Source" gemäß [IHE-ITI-TF1] implementieren. [≤]

**A\_14669 -XDS Document Service - Keine Implementierung des IHE ITI-Akteurs XDS On-Demand Document Source**

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS On-Demand Document Source" gemäß [IHE-ITI-TF1] implementieren. [≤]

**A\_14950 -XDS Document Service - Keine Angabe einer Fehlerlokalisierung im RegistryError-Element**

Der XDS Document Service DARF NICHT das location-Attribut im rs:RegistryError-Element in der IHE ITI-Ausgangsnachricht verwenden, sofern ein Fehler bei der



Verarbeitung einer IHE ITI-Eingangsnachricht auftritt. Diese Einschränkung gilt nur für Error Stack Traces bzw. der Offenbarung von Programmierdetails. [≤]

#### **A\_15081 -XDS Document Service - Implementierung des IHE ITI-Akteurs RMU Update Responder**

Der XDS Document Service MUSS den IHE ITI-Akteur "RMU Update Responder" gemäß [IHE-ITI-RMU] implementieren. [≤]

3.13.1.4.1.1 Gruppierungen mit anderen IHE ITI-Akteuren

#### **A\_15093-02 -XDS Document Service - Gruppierung RMU Update Responder mit Document Registry**

Der XDS Document Service als RMU-Akteur "Update Responder" MUSS mit dem XDS-Akteur "Document Registry" gemäß [IHE-ITI-RMU] gruppiert sein. [≤]

3.13.1.4.1.2 Optionen des IHE ITI-Akteurs

#### **A\_15094 -XDS Document Service - RMU Update Responder ohne "Forward Update"-Option**

Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option "Forward Update" unterstützen.  
[≤]

#### **A\_15095-02 -XDS Document Service - RMU Update Responder ohne "XCA Persistence"-Option**

Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option "XCA Persistence" unterstützen. [≤]

#### **A\_15096-02 -XDS Document Service - RMU Update Responder mit "XDS Persistence"-Option**

Der XDS Document Service als RMU-Akteur "Update Responder" MUSS die Option "XDS Persistence" unterstützen. [≤]

#### **A\_15097 -XDS Document Service - RMU Update Responder ohne "XDS Version Persistence"-Option**

Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option "XDS Version Persistence" unterstützen. [≤]

3.13.1.4.1.3 Gruppierungen mit anderen IHE ITI-Akteuren

3.13.1.4.1.4 Optionen des IHE ITI-Akteurs

#### **A\_14637 -XDS Document Service - XDS Document Registry ohne "Asynchronous Web Services Exchange"-Option**

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "Asynchronous Web Services Exchange" unterstützen. [≤]

#### **A\_14638 -XDS Document Service - XDS Document Registry mit "Reference ID"-Option**

Der XDS Document Service als XDS-Akteur "Document Registry" MUSS die Option "Reference ID" unterstützen. [≤]

#### **A\_14639 -XDS Document Service - XDS Document Registry ohne "Patient Identity Feed"-Option**

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "Patient Identity Feed" unterstützen.  
[≤]

#### **A\_14640 -XDS Document Service - XDS Document Registry ohne "Patient Identity Feed HL7v3"-Option**

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "Patient Identity Feed HL7v3" unterstützen. [≤]

#### **A\_14641 -XDS Document Service - XDS Document Registry ohne "On-Demand Documents"-Option**



Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "On-Demand Documents" unterstützen. [≤]

#### 3.13.1.4.1.5 Optionen des IHE ITI-Akteurs

#### **A\_14636 -XDS Document Service - XDS Document Repository ohne "Asynchronous Web Services Exchange"-Option**

Der XDS Document Service als XDS-Akteur "Document Repository" DARF NICHT die Option "Asynchronous Web Services Exchange" unterstützen. [≤]

#### 3.13.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen

Die folgende Tabelle fasst die oben definierten Anforderungen zu Gruppierungen und Optionen zusammen. Dabei wird die folgende Notation für Optionalitäten (Opt.) verwendet:

**Tabelle 25: Kennzeichnung von Optionalitäten**

Code	Bedeutung
R	Required - Mit "R" gekennzeichnete IHE ITI-Akteure oder Optionen MÜSSEN implementiert oder gruppiert werden.
X	Mit "X" gekennzeichnete IHE ITI-Akteure oder Optionen DÜRFEN NICHT implementiert oder gruppiert werden.

**Tabelle 26: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen des XDS Document Service**

IHE ITI-Akteur	Opt.			Umzusetzende Option des IHE ITI-Akteurs	Opt.
		Gruppierung mit anderem IHE ITI-Akteur	Opt.		
ATNA Audit Record Repository	X				
CT Time Client	X				
RMU Update Responder	R			Forward Update	X
				XCA Persistence	X
				XDS Persistence	R

			XDS Version Persistence	X
		Document Registry	R	
XDS Document Consumer	X			
XDS Document Registry	R		Asynchronous Web Services Exchange	X
			Document Metadata Update	X
			On-Demand Documents	X
			Patient Identity Feed	X
			Patient Identity Feed HL7v3	X
			Reference ID	R
		ATNA Secure Node oder Secure Application für Node Authentication	X	
XDS Document Repository	R		Asynchronous Web Services Exchange	X
		ATNA Secure Node oder Secure Application für Node Authentication	X	
XDS Document Source	X			
XDS Integrated Document Source / Repository	X			
XDS On-				

Demand Document Source	X	
XDS Patient Identity Source	X	

### 3.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen

#### **A\_17832 -XDS Document Service - Unterstützung MTOM/XOP**

Der XDS Document Service MUSS gemäß den Anforderungen von [IHE-ITI-TF2x#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] verwenden. [ $\leq$ ]

#### **A\_24524 -XDS Document Service - Migration, Upload: Normalisieren des URI**

Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten den `DocumentEntry.URI` normalisieren. Dies gilt für `FileURI`, z.

B. "<file:///C:/path/to/file.html#anchor>" oder `/C/path/to/file.html#anchor`". Die URI MUSS auf den reinen Dateinamen mit Extension (d. h. ohne Pfadangaben) reduziert werden, z. B. "file.html". Nach der Normalisierung MUSS eine Validierung der Extension gemäß A\_23447-\* erfolgen. [ $\leq$ ]

#### **A\_23447-01 -XDS Document Service - DocumentEntry.URI extension entspricht mimetype**

Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten das Metadatum `DocumentEntry.URI` daraufhin prüfen, ob `DocumentEntry.URI` eine filename extension aufweist, die nicht dem `DocumentEntry.mimetype` entspricht. Zuvor muss die URI mittels A\_24524-\* normalisiert worden sein. Danach MUSS der XDS Document Service sicherstellen, dass in `Document.URI` die filename extension dem `DocumentEntry.mimeType` entspricht. Im Falle einer Abweichung MUSS an die ursprüngliche `DocumentEntry.URI` die filename extension gemäß A\_24864-\*, bzw. A\_25009-\*, angehängt werden, die dem `mimeType` entspricht. Die Groß-/Kleinschreibung der filename extension ist bei der Prüfung nicht relevant. [ $\leq$ ]

#### **A\_24451-01 -XDS Document Service - Automatisches initiales Erzeugen einer versionsübergreifenden ID für Dokumente**

Der XDS Document Service MUSS beim initialen Einstellen eines Dokumentes die `DocumentEntry.uniqueId` als Eintrag einer `ReferenceID` in die `ReferenceIDList` in folgendem Format einstellen:

```
<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2023:rootDocumentUniqueId
```

Beim Upload einer neuen Version des Dokumentes DARF dieser Eintrag in der `ReferenceIDList`, d.h. die `rootDocumentUniqueId`, NICHT verändert werden. Er bleibt über alle Versionen des Dokumentes hinweg unverändert erhalten. Der Versuch eines Clients, die `rootDocumentUniqueId` durch ein Metadata-Update oder im Zuge des Einstellens einer neuen Dokumentenversion zu verändern, MUSS mit einem IHE-Error `XDSRegistryMetadataError` abgebrochen werden. Es MUSS im `codeContext`-Attribut des zurückgegebenen `XDSRegistryMetadataError`-Elements der Text „rootDocumentUniqueId must not be changed“ zurückgegeben werden. [ $\leq$ ]

#### **A\_14926-04 -XDS Document Service - Automatisiertes Löschen oder Verbergen von Dokumenten in RPLC-Ketten**

Der XDS Document Service MUSS bei zu löschenden oder zu verbergenden Dokumenten und `DocumentEntry`-Einträgen im selben Zuge auch alle mittels

urn:ihe:iti:2007:AssociationType:RPLC assoziierten DocumentEntry-Einträge und Dokumente löschen bzw. verbergen.[<=]

#### **A\_27683-01 -XDS Document Service - Maximale Länge von Anhangsketten**

Der XDS Document Service MUSS sicherstellen, dass beim Einstellen (über die Schnittstelle Provide and Register Document Set-b [ITI-41]) oder Kennzeichnen (über die Schnittstelle Restricted Update Document Set [ITI-92]) von neuen Anhängen die gesamte Anhangskette inklusive des neuen Anhangdokuments und inklusive des obersten Elterndokuments nicht mehr als fünf Dokumente enthält und ansonsten die Operation mit dem Fehler XDSMaxAttachmentsExceeded abbrechen.

[<=]

Der Abschnitt 6.1- Dokumentenanhänge enthält eine Illustration für diese Anforderung.

3.13.1.4.3.1 Provide and Register Document Set-b [ITI-41]

#### **A\_13715 -XDS Document Service - Ablauflogik für ProvideAndRegisterDocumentSet-b**

Der XDS Document Service MUSS die Umsetzung der Operation ProvideAndRegisterDocumentSet-b gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3 ] und [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3 ] implementieren.[<=]

#### **A\_15162-06 -XDS Document Service - Keine Registrierung bei Angabe von Document Entry Relationships in Metadaten**

Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem XDSRepositoryMetadataError-Fehlercode quittieren, sofern die Metadaten andere Association Types nach [IHE-ITI-TF3#4.2.2.2] als die Folgenden enthalten:

- urn:ihe:iti:2007:AssociationType:RPLC (Replace)

[<=]

#### **A\_14938-02 -XDS Document Service - Validierung der Metadaten aus ITI Document Sharing-Profilen**

Der XDS Document Service MUSS die SubmissionSet- sowie die DocumentEntry-Metadaten der eingehenden Nachricht vor einer Zugriffskontrolle gemäß Konformität zu den Nutzungsvorgaben in [A\_14760-\*] prüfen. Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem XDSRepositoryMetadataError quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht.[<=]

#### **A\_24521 -XDS Document Service - Erzeugen von Prüfsummen für Dokumente**

Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes Dokument seine kryptographische Prüfsumme berechnen und in DocumentEntry.hash hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die Dokumentengröße in DocumentEntry.size berechnet und gesetzt werden.[<=]

#### **A\_24988-01 -XDS Document Service - Dublettenprüfung für Dokumente**

Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes Dokument den hash-Wert vergleichen mit allen bereits in dieser Akte existierenden hash-Werten der Dokumente und bei einer Übereinstimmung das Einstellen mit dem Fehlercode XDSDuplicateDocument ablehnen. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die Liste der UUIDs (DocumentEntry.entryUUID) der identifizierten Dokumente angegeben werden. Der XDS Document Service MUSS diese Prüfung vor allen anderen Metadatenprüfungen durchführen.[<=]

Hintergrund ist, dass die Information, dass es sich um eine Dublette handelt, für das einstellende System hilfreicher und spezifischer ist als ein Metadatenfehler, dass bspw. die angelieferte uniqueId "falsch" ist.

#### **A\_24990 -XDS Document Service - Dublettenprüfung für dynamische Ordner**

Der XDS Document Service MUSS beim Anlegen dynamischer Folder prüfen, ob ein Ordner bereits existiert, der gemäß vom Titel her identisch ist mit demjenigen, den der Client einzustellen versucht. Im Falle eines identischen Titels MUSS der Einstellversuch mit dem Fehlercode XSDuplicateFolder abgelehnt werden. [≤]

#### **A\_14937 -XDS Document Service - Dokumentengröße prüfen**

Der XDS Document Service MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das SubmissionSet verarbeitet wird. Der XDS Document Service MUSS die Verarbeitung ablehnen und mit einemMaxDocSizeExceeded- bzw.MaxPkgSizeExceeded-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren, wenn die Gesamtgröße aller übermittelten Dokumente 250 MByte übersteigt oder die Größe mindestens eines einzelnen Dokuments 25 MByte übersteigt.

[≤]

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.

#### **A\_23098-01 -XDS Document Service - Keine Registrierung bei zeitlicher Ungültigkeit von strukturierten Dokumenten**

Der XDS Document Service MUSS beim Einstellen eines strukturierten Dokuments sicherstellen, dass die Vorgaben gemäß [gemSpec\_IG\_ePA] hinsichtlich der zeitlichen Gültigkeit erfüllt werden und andernfalls das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einemXDSRepositoryMetadataError quittieren. Es MUSS im codeContext-Attribut des zurückgegebenenXDSRepositoryMetadataError-Elements der Text „Version of submitted structured document is not supported“ zurückgegeben werden. [≤]

#### **A\_21610-03 -Sonderfälle Anlegen von Foldern durch Clientsysteme**

Der XDS Document Service MUSS sicherstellen, dass ausschließlich dynamische Ordner vom Typ "Schwangerschaft und Geburt" (Folder.Code = pregnancy\_childbirth) durch Clients angelegt werden können. [≤]

#### **A\_24797-04 -XDS Document Service - Ablehnung Upload bei veränderten Metadaten bei einer RPLC Assoziation**

Der XDS Document Service MUSS Uploads, die als Resultat ein zum Vorgängerdokument verändertes Metadatum enthalten, mit einem XDSRegistryMetadataError ablehnen. Einzige Ausnahmen sind:

- Metadatenattribut creationTime, entryUUID sowie uniqueId und confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491).
- Das Metadatenattribut DocumentEntry.referenceIdList DARF ohne die rootDocumentUniqueid gesendet werden; in dem Fall wird die rootDocumentUniqueid automatisch vom XDS Document Service gesetzt (Wert identisch zu dem des ersetzten Dokuments).

[≤]

#### **A\_27760-01 -XDS Document Service - Ablehnen von RPLC-Ersetzungen bei nicht erlaubten Dokumententypen**

Der XDS Document Service MUSS das Ersetzen von Dokumenten via RPLC-Associations mit dem Fehlercode XDSReplacementForbidden ablehnen, wenn das zu ersetzende Dokument nicht einen der folgenden DocumentEntry.formatCode-Werte besitzt:

Dokume nt	codeSystem	code
eMP	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:Medikationsplan:r3.1
NFD	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:Notfalldatensatz:r3.1
DPE	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:DatensatzPersoenlicheErklaerung en:r3.1
DiGA	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:diga:v1.1

oder das zu ersetzende Dokument nicht in einen der folgenden Ordner einsortiert ist:

Ordner-Kategorie	Folder.entryUUID	
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d	
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31	

【<=】

Seit ePA 3.1.2 ist das Ersetzen von Dokumenten via RPLC-Associations nur noch für die oben aufgeführten Dokumententypen bzw. -kategorien erlaubt. Der Versuch, andere Dokumententypen zu ersetzen, führt zu einem Fehler. Es kann Altdaten geben, die diese Regel noch missachten. Neue Ersetzung für diese Altdaten werden jedoch gleichermaßen fehlschlagen; d.h. neue Ersetzungen sind nur noch für die oben angegebenen Dokumententypen erlaubt.

#### **A\_27761 -XDS Document Service - Potentielle Dokumententypen (Elterndokumente) für Anhänge**

Der XDS Document Service MUSS das Anhängen von Dokumenten mit dem Fehlercode XDSAttachmentForbidden ablehnen, wenn das Dokument, an das angehängt wird, nicht die folgende Metadatenbelegung besitzt:

IHE- Metadaten	eventCodeList-Eintrag (KDL-Code)			
	Dokumente ntyp (informativ )	Code System	Code	
classCode="BRI" UND typeCode="BERI"	eventCodeList muss einen der folgenden Codes enthalten		1.2.276.0.76.5.552	ED110112
	eArztbrief	1.2.276.0.76.5	ED110104	

(beide Codes müssen angegeben sein)		.552	
	Anderer Arztbrief	1.2.276.0.76.5.552	AD0101*

【<=】

Hinweis 1: AD0101 bezeichnet Codes die mit den Zeichen "AD0101" beginnen, z. B. "AD010112" für den "Kurzarztbrief". Der Code "AD0101" als Level 2-Code in KDL ist selbst nicht Teil des Value Sets für eventCodeList, das nur die konkreteren Level 3 Codes enthält.

Hinweis 2: Die Anforderung schließt sowohl das Einstellen von Anhängen über die Operation Provide and Register Document Set-b [ITI-41] als auch Restricted Update Document Set [ITI-92] mit ein.

Hinweis 3: Die Dokumente, die als Anhang angehängt werden dürfen, werden über A\_27763 (RPLC-fähige Dokumente) und A\_27764 (Sammlungen) eingeschränkt.

#### **A\_27764 -XDS Document Service - Keine Anhangsbeziehungen mit Sammlungsdokumententypen**

Der XDS Document Service MUSS das Etablieren von Anhangsbeziehungen zu allen Dokumententypen, die in Sammlungen (mixed oder uniform) organisiert werden, unterbinden und mit dem Fehler XDSAttachmentForbidden ablehnen.

【<=】

#### **A\_27763-01 -XDS Document Service - Keine Anhangsbeziehungen mit RPLC-fähigen Dokumententypen**

Der XDS Document Service MUSS das Etablieren von Anhangsbeziehungen zu allen Dokumententypen, die in RPLC-Ketten verwendet werden dürfen (siehe A\_27760) oder die bereits aufgrund der Migration von Altdaten (siehe A\_27661) in RPLC-Beziehungen stehen, unterbinden und mit dem Fehler XDSAttachmentForbidden ablehnen.

【<=】

Das heißt, dass RPLC-fähige Dokumente (egal, ob sie bereits Teil einer RPLC-Kette sind oder nicht) nicht Teil einer Anhangskette sein dürfen, also weder als Anhang genutzt werden dürfen, noch als Dokument an das selbst angehängt wird. Das trägt der aktuellen Einschränkung Rechnung, dass alle RPLC-Dokumente in einer RPLC-Kette immer "identische" Metadaten besitzen und deshalb Anhänge (die über die Metadaten abgebildet werden) automatisch bei einer Ersetzung "mitvererbt" würden. Da dies fachlich potentiell zu Problemen führen kann, wird es auf diese Weise unmöglich gemacht, dass Dokumente gleichzeitig in einer RPLC- als auch in einer Anhangskette sein können.

Da diese Regelung in ePA 3.1.2 eingeführt wurde, können Altdaten noch über Anhänge verfügen, siehe auch Abschnitt zur [automatischen Datenanpassung](#).

Details zur grundsätzlichen Funktionsweise von Dokumentenanhängen finden sich in [diesem Abschnitt](#).

#### **A\_24531-04 -Constraint Management - Verbergen von Dokumenten durch confidentialityCode**

Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) durch eine Nutzergruppe der Rolleoid\_versichertereingestellt wird, nicht Bestandteil einer Sammlung, also eines Ordners der Ausprägung "mixed" oder "uniform" ist, und kein Dokument der Kategorie "emp" ist, dann MUSS der XDS Document Service sicherstellen, dass das Dokument durch einen Eintrag in der General Deny Policy verborgen wird. Es MUSS ein Eintrag mit denyType = "document" für die General Deny Policy erzeugt werden.【<=】



**A\_25856-02 -XDS Document Service - Fehlerhaftes Verbergen von Dokumenten durch confidentialityCode**

Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) nicht durch eine Nutzergruppe der Rolleoid\_versichertereingestellt wird, oder Bestandteil einer Sammlung, also eines Ordners der Ausprägung "mixed" oder "uniform" ist, dann MUSS der XDS Document Service die Operation abbrechen und mit einem Fehlercode ConstraintViolation beenden. [<=]

Das Verbergen von Dokumenten ist in Kapitel 3.13.1.10- Verbergen von Dokumenten durch Verwendung des confidentialityCode beschrieben.

**3.13.1.4.3.1.1 Dokumentenanhänge**

Für die Verwaltung von Anhängen wird ein Mechanismus basierend auf DocumentEntry.referencecldList verwendet. Zwei Dokumente werden verknüpft, indem in beiden dazugehörigen DocumentEntrys das jeweils andere Dokument als "Elterndokument" bzw. "Kinddokument" (=Anhang) eingetragen wird. Dies geschieht über die Auszeichnung der Referenzen mit den qualifizierenden Codesurn:gematik:iti:xds:2025:childDocument (Verweis auf ein Kinddokument) und urn:gematik:iti:xds:2025:parentDocument (Verweis auf ein Elterndokument).

Ein Verweis auf ein Elternformat hat also das Format:<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2025:parentDocument

Dabei muss das Dokument, auf das per Kind- oder Elternreferenz verwiesen wird, zusammen mit oder nach dem referenzierten Dokument eingestellt werden. Wenn z. B. das Elterndokument bereits im Aktensystem gespeichert ist und ein Kinddokument (Anhang) dazu hochgeladen wird, muss der DocumentEntry des Kinddokuments das Elterndokument in der referencecldList referenzieren. Die Markierung des Elterndokuments (mit dem Verweis auf das Kinddokument) wird dann vom Aktensystem automatisch vorgenommen. Damit wird vermieden, dass zwei Aufrufe notwendig sind (Einstellen gefolgt vom Aktualisieren der Metadaten), was zu inkonsistenten Zuständen im Aktensystem führen kann. Werden Eltern- und Kinddokument gemeinsam eingestellt, ist der Verweis auf mindestens entweder Elterndokument oder Kinddokument verpflichtend, da die jeweils andere Seite automatisch vom Aktensystem ergänzt werden kann.

Die Tiefe von Anhangsketten ist auf fünf Dokumente (inklusive dem obersten Elterndokument) begrenzt. Darüberhinaus ist die Verwendung von Anhängen nur für ausgewählte Dokumententypen erlaubt und kann dann jeweils weiteren Beschränkungen unterliegen.

Neben dem Anhängen während des Einstellens ist es auch möglich, über ein Metadatenupdate nachträglich zwei Dokumente miteinander über eine Anhangsbeziehung zu verbinden.

Anhänge, technisch umgesetzt über DocumentEntry.referencecldList, sind zu unterscheiden von RPLC (Replace/Ersetzungs)-Ketten, die über RPLC-Associations abgebildet werden. Ersetzte Dokumente stellen verschiedene Dokumentenversionen dar, während Anhänge in der Regel eine Ergänzung des Dokuments darstellen, an dem sie anhängen. Um die beiden Konzepte nicht zu vermischen (aktuell würden alle per RPLC-Associations verbundene Dokumente zwangsläufig aufgrund identischer Metadaten immer dieselben Anhänge besitzen), wird verboten, ein Dokument gleichzeitig in eine Ersetzungskette als auch in eine Anhangskette zu hängen. Dies geschieht über eine Beschränkung des RPLC-Mechanismus auf wenige ausgewählte Dokumententypen und der gezielten Verwendung von Anhängen für andere Dokumententypen.

Die letzte Einschränkung bedeutet auch, dass Anhänge nicht an beliebige Dokumente gehängt werden können. Ziel ist es, Anhänge nur in fachlich kontrollierter Form in der ePA zu verwenden und auf diese Weise die Datenqualität zu erhöhen.

Anhangsbeziehungen können gelöscht werden, in dem der entsprechende Verweis auf ein Anhangsdokument aus der `referenceIdList` (via `Restricted Update Document Set`) entfernt wird.

Es kann direkt an einem `DocumentEntry` erkannt werden, ob ein Dokument Anhangsbeziehungen zu anderen Dokumenten unterhält oder nicht. Um möglichst einfach (rekursiv) alle mit einem bestimmten Dokument verbundenen Dokumente zu finden, existiert eine spezielle Suche (siehe A\_27655), die alle entsprechenden `DocumentEntries` zurückliefert. Bei dieser und anderen Suchen werden Eltern- oder Kinddokumente zu einem zurückgegebenen `DocumentEntry`, die *nicht* für den Anfragenden sichtbar sind (z. B. aufgrund der Legal Policy oder da sie durch den Versicherten verborgen wurden), vom Aktensystem automatisch aus dem returnierten `DocumentEntry` bzw. dessen `referenceIdList` entfernt.

## Berechtigungen für Anhangsoperationen

Es gelten die Regelungen der Legal Policy für die zur Anhangsverwaltung notwendigen Operationen:

- **Lesen:** Um die Anhangsbeziehung zwischen beiden Dokumenten zu erkennen, müssen beide Dokumente für den Anfragenden lesbar (Berechtigung "R" für "Read") sein, ansonsten blendet das Aktensystem die Anhangsbeziehung in zurückgelieferten `DocumentEntries` aus. Auch wenn das referenzierte Dokument verborgen ist, wird die Anhangsbeziehung nicht angezeigt.
- **Einstellen:** Um Dokumente neu einzustellen und sie als Eltern- oder Kinddokument mit einem bestehenden (oder ebenfalls neuen) Dokument zu verknüpfen, wird das "C"-Recht ("Create") für das neue Dokument benötigt, um die `Provide and Register Document Set-b Operation` ausführen zu können. Zudem muss für das zu verbindende Dokument (sofern es nicht neu mit eingestellt wird) die Berechtigung zum Aktualisieren ("U") vorliegen. Auch in diesem Use Case müssen beide Dokumente für den Einstellenden sichtbar sein.
- **Aktualisieren:** Um zwei Dokumente, die bereits im Aktensystem vorliegen, zu verknüpfen oder zu entknüpfen, wird die Berechtigung "U" ("Update") zur Ausführung der Operation `Restricted Update Document Set` auf *beiden* Dokumenten benötigt. Beide Dokumente dürfen nicht vom Versicherten verborgen worden sein.
- **Löschen:** Wenn ein Dokument gelöscht werden soll muss die Berechtigung "D" für das zu löschende Dokument vorliegen. Der Verweis aus etwaigen Eltern/Kinddokumenten auf das gelöschte Dokument wird entfernt. Dazu ist beim referenzierten Dokument die Berechtigung "U" notwendig. Die "D"-Berechtigung selbst muss nur für das zu löschende Dokument vorliegen.

Eine wichtige Eigenschaft im Zusammenhang mit Anhängen ist es also, dass das Herstellen und Entfernen von Anhangsbeziehungen von Dokumenten das Update-Recht "U" benötigt (Ausnahme: für neu eingestellte nur Recht "C" notwendig). Das Anhängen oder Abhängen eines Dokuments in/aus einer Anhangskette wird also als Aktualisierung eines Dokuments verstanden.

## A\_27654 -XDS Document Service - Einstellen von neuen Anhängen oder Anhängen an neue Dokumente

Der XDS Document Service MUSS beim Registrieren und Speichern von Metadaten und Dokument(en) über die Operation `ProvideAndRegisterDocumentSet-b` die folgenden zusätzlichen Schritte durchführen, wenn das Feld `DocumentEntry.referenceIdList` einen Wert mit Identifier Type Code `urn:gematik:iti:xds:2025:parentDocument` (oder `urn:gematik:iti:xds:2025:childDocument`) enthält; im Folgenden ist der Fall

für urn:gematik:iti:xds:2025:parentDocument beschrieben, der Fall childDocument ist analog zu behandeln und jeweils in Klammern angegeben)

1. Prüfung, ob das dort als parentDocument (childDocument) adressierte Dokument (mit entsprechender DocumentEntry.uniqueId) entweder Teil des SubmissionRequests oder bereits im XDS Document Service vorhanden ist. Der XDS Document Service MUSS:
  - a. Wenn das Dokument nicht existiert oder für den Anfragenden nicht sichtbar ist, die Verarbeitung mit dem Fehler XDSNoSuchParent (XDSNoSuchChild) abbrechen;
  - b. Wenn das Dokument bereits vorhanden ist, prüfen ob der Anfragende gemäß Legal Policy die Berechtigung "U" für dieses Dokument besitzt und ansonsten die Verarbeitung mit dem Fehler XDSCannotLinkAttachment abbrechen und im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements als Text die DocumentEntry.uniqueId des referenzierten Dokuments angeben.
2. Prüfung, ob durch das Einstellen des Dokuments kein Verweiszirkel entsteht und ansonsten die Verarbeitung mit dem Fehler XDSAttachmentCycle abbrechen.
3. Prüfung, ob durch das Einstellen des Dokuments der zusätzliche Verweis nicht auf ein Elterndokument (Kinddokument) gemacht wird, das bereits Teil der Elternketten (Kindkette) ist und ansonsten die Verarbeitung mit dem Fehler XDSInvalidAttachmentHierarchy abbrechen.
4. Im referenzierten Dokument die DocumentEntry.uniqueId des einzustellenden Dokuments in die referencedList mit Identifier Codeurn:gematik:iti:xds:2025:childDocument (urn:gematik:iti:xds:2025:parentDocument) eintragen, wenn dies nicht bereits geschehen ist.

[<=]

Hinweis 1: Ein Verweiszirkel kann entstehen, wenn ein Kinddokument direkt oder indirekt (d.h. ggf. über eine Kette von Kinddokumenten hinweg) gegenüber seinem Elterndokument gleichzeitig auch selbst als Elterndokument auftritt.

Hinweis 2: Der Fehler XDSInvalidAttachmentHierarchy spiegelt die Situation wider, dass in einer Kette von Anhängen (wie 1<-2<-3) versucht wird, ein Kind (3) zusätzlich als Kind eines Vorfahren seines Elterndokuments (1) einzuführen.

Hinweis 3: Punkt 4 stellt sicher, dass das referenzierte Dokument passend markiert wird, egal ob es in der Anfrage enthalten ist oder bereits im Aktensystem hinterlegt ist.

Siehe auch [entsprechende Illustrationen im Anhang](#).

3.13.1.4.3.2 Registry Stored Query [ITI-18]

#### **A\_14913 -XDS Document Service - Ablauflogik für Registry Stored Query**

Der XDS Document Service MUSS die Umsetzung der Operation RegistryStoredQuery gemäß der definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3 ] implementieren.[<=]

#### **A\_24761 -XDS Document Service - Ermitteln verknüpfter Approved Documents für Registry Stored Query**

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "GetRelatedApprovedDocuments" mit der Query-ID "urn:uuid:1c1f1cea-ad3a-11ed-afa1-0242ac120002" mit denselben Parameternutzungsvorgaben der Registry Stored Query „GetDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.5] mit der Multiplizität 1 unterstützen. Das resultierende DocumentEntry Objekt MUSS

- mit dem Ergebnis von GetDocuments übereinstimmen, falls dieses sich im Zustand approved befindet;

- andernfalls über Associations ermittelt werden. Dabei wird jeweils ausgehend von der übergebenen DocumentEntry.EntryUUID oder DocumentEntry.Uniqueld über die Replace- Associations dasjenige DocumentEntry Objekt ermittelt, das sich im Zustand approved befindet.

Das wsa:Action-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery" besitzen. [ $\leq$ ]

#### **A\_24762 -XDS Document Service - Suchanfragen über das Metadatenattribut DocumentEntry.title**

Der XDS Document Service MUSS einen 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-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter \$XDSDocumentEntryTitle unterstützen, sodass eine Suchergebnismenge über das Attribut XDSDocumentEntry.title eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson. Das wsa:Action-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery" besitzen. [ $\leq$ ]

#### **A\_25183 -XDS Document Service - Suchanfragen über das Metadatenattribut DocumentEntry.comment**

Der XDS Document Service MUSS einen 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-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter \$XDSDocumentEntryComment unterstützen, sodass eine Suchergebnismenge über das Attribut XDSDocumentEntry.comment eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson. Das wsa:Action-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery" besitzen. [ $\leq$ ]

#### **A\_24763 -XDS Document Service - Suche über Author Institution bei Registry Stored Query**

Der XDS Document Service MUSS für den Anfragetyp "FindDocumentsByTitle" den weiteren optionalen Parameter \$XDSDocumentEntryAuthorInstitution verarbeiten können, sodass eine Suchergebnismenge über den authorInstitution-Slot der XDSDocumentEntry.author-Classification (Wertemenge des authorInstitution-Sub-Attributs) eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson. [ $\leq$ ]

#### **A\_24764 -XDS Document Service - Rückgabe unscharfer Suchergebnisse für Registry Stored Query**

Der XDS Document Service MUSS bei der Ermittlung der Ergebnisse einer Registry Stored Query bei Auswertung der folgenden Queries und deren Suchparametern beim Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d. h. bezogen auf das jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht abweichende Ergebnisse zurück liefern können:

- Query "FindDocuments" und Query "FindDocumentsByTitle" und Query "FindDocumentsByComment"
  - \$XDSDocumentEntryTitle
  - \$XDSDocumentEntryAuthorInstitution
  - \$XDSDocumentEntryAuthorPerson
  - \$XDSDocumentEntry.comment

- Query "FindSubmissionSets"
  - \$XDSSubmissionSetAuthorPerson

Dabei MUSS der XDS Document Service mindestens unscharfe Ergebnisse bezüglich Groß/Kleinschreibung unterstützen, also Groß/Kleinschreibung für die angegebenen Parameter der ausgewählten Query-Typen ignorieren.

[<=]

Das zur Ermittlung weiterer unscharfer Ergebnisse vom XDS Document Service einzusetzende Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu liefern, die ihm möglicherweise sonst wegen beispielsweise falscher Schreibweise eines Namens (z. B. "Meyer" vs. "Maier") vorenthalten worden wäre. Dabei sind Verfahren wie die Kölner Phonetik aber auch andere Mechanismen denkbar.

### **A\_27655 -XDS Document Service - Suche nach Anhangsketten**

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "GetDocumentAppendices" mit der Query-ID "urn:uuid:2a6b3197-8ea8-4245-a6de-daf71b469116" und denselben Parameternutzungsvorgaben der Registry Stored Query "GetDocumentsAndAssociations" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.8] unterstützen. Die Suchergebnismenge muss für jedes über \$XDSDocumentEntryEntryUUID oder \$XDSDocumentEntryUniqueld referenzierte Dokument die Ergebnismenge wie folgt ermitteln:

1. Start: Alle DocumentEntrys der Ergebnismenge hinzufügen, welche auf die uniqueld des Dokuments aus dem Eingangsparameter in der DocumentEntry.referenceIdList verweisen (ausgezeichnet als urn:gematik:iti:xds:2025:childDocument oder urn:gematik:iti:xds:2025:parentDocument) und sichtbar sind.
2. Kindkette: Für jeden im vorher durchgeführten Schritt identifizierten DocumentEntry D, der über den Eintrag urn:gematik:iti:xds:2025:childDocument identifiziert wurde, alle DocumentEntries der Ergebnismenge hinzufügen, welche die uniqueld von D wiederum als urn:gematik:iti:xds:2025:childDocument in der referenceIdList enthalten und sichtbar sind. Wenn ein DocumentEntry nicht sichtbar ist, wird dieser Teil der Kette nicht weiter verfolgt.
3. Elternkette: Für jeden im vorher durchgeführten Schritt identifizierten DocumentEntry E, der über den Eintrag urn:gematik:iti:xds:2025:parentDocument identifiziert wurde, alle DocumentEntries der Ergebnismenge hinzufügen, welche die uniqueld von E wiederum als urn:gematik:iti:xds:2025:parentDocument in der referenceIdList enthalten und sichtbar sind. Wenn ein DocumentEntry nicht sichtbar ist, wird dieser Teil der Kette nicht weiter verfolgt.
4. Rekursion: Schritte 2 und 3 jeweils wiederholen, bis keine weiteren DocumentEntries mehr gefunden werden können.

[<=]

Hinweis 1: "Sichtbar" im Kontext von Anhängen bedeutet hier, dass die Existenz eines Dokuments nicht durch fehlende Legal Policy-Berechtigung (Recht "R" ist notwendig), Verbergen durch den Versicherten, Zugriffsverbot für die zugreifenden Organisation über ("User Specific Deny Policy") oder gar Widerspruch ("Consent Decision") vor dem Zugreifenden versteckt werden muss.

Hinweis 2: Wenn als Eingabe eine entryUUID gegeben wird, muss der XDS Document Service die dazugehörige uniqueID ggf. intern selbst ermitteln. Zur Sichtbarkeit von Anhängen siehe Hinweis unter A\_27655.

Die Suche ermittelt also alle Dokumente, die über Anhangsketten mit dem gegebenen Dokument verbunden sind.

### **A\_27762 -XDS Document Service - Ausblenden nicht sichtbarer Anhänge**



Der XDS Document Service MUSS bei der Rückgabe eines DocumentEntries D im Rahmen einer Stored Query [ITI-18] jedes durch Anhangsbeziehungen in der DocumentEntry.referenceIdList (urn:gematik:iti:xds:2025:childDocument oder urn:gematik:iti:xds:2025:parentDocument) mit D verbundene Dokument E dahingehend prüfen, ob es für den Anfragenden sichtbar ist und wenn nicht, den entsprechenden Eintrag für E vor der Herausgabe an den Anfragenden aus der referenceIdList entfernen.

[<=]

#### 3.13.1.4.3.3 Remove Metadata [ITI-62]

##### **A\_14908-02 -XDS Document Service - Ablauflogik für Remove Metadata**

Der XDS Document Service MUSS die Umsetzung der Operation RemoveMetadata gemäß der definierten Ablauflogik in [IHE-ITI-RMD#3.62.4.1.2 und 3.62.4.1.3 ] implementieren.

[<=]

##### **A\_20701 -XDS Document Service - Unwiderrufliches Löschen bei Remove Metadata**

Der XDS Document Service MUSS sicherstellen, dass einmal gelöschte Dokumente und Metadatenobjekte nicht wiederhergestellt werden können.[<=]

##### **A\_21715 -XDS Document Service - Kein Löschen von "replaced"-Dokumenten im Status "Deprecated"**

Der XDS Document Service MUSS sicherstellen, dass keine Löschanfrage eines ePA-Client auf Dokumenten mit dem availabilityStatus = Deprecated ausgeführt werden darf.[<=]

##### **A\_21714-03 -XDS Document Service - Löschen von strukturierten Dokumenten durch ein ePA-FdV**

Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die Nachricht mit demXDSRegistryError-Fehlercode zurückgeben werden.Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt werden.

[<=]

##### **A\_21817-02 -XDS Document Service - Löschen von strukturierten Dokumenten durch ein Primärsystem**

Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein Primärsystem ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die Nachricht mitXDSRegistryError-Fehlercode zurückgeben werden. Es MUSS im codeContext-Attribut des zurückgegebenenrs:RegistryError-Elements der Wert "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt werden.

[<=]

##### **A\_24663-01 -XDS Document Service - Bereinigung der General Deny Policy**

Der XDS Document Service MUSS als Folge von erfolgreichen Löschanfragen alle Einträge der General Deny Policy entfernen, welche die betroffenen Dokumente oder dynamischen Ordner referenzieren.[<=]

##### **A\_24765 -XDS Document Service - Kein Löschen von statischen Ordnern und Associations**

Der XDS Document Service MUSS sicherstellen, dass eine Löschanfrage keine statischen Ordner und Assoziationen löschen darf. Dies gilt nicht für dynamische Ordner. Der XDS Document Service MUSS bei Löschung eines Dokumentes die Assoziation zum Folder löschen.[<=]

Dynamische Ordner sind beispielsweise Mutterpass (folderCode = pregnancy\_childbirth) oder DiGA (folderCode = diga).

#### **A\_20579-01 -XDS Document Service - Löschen von Ordnern**

Der XDS Document Service MUSS Requests, die darauf abzielen, einen statischen Folder direkt zu löschen, mit einem XDSRegistryMetadataError ablehnen. [**<=**]

#### **A\_27656-01 -XDS Document Service - Löschen von Anhangsreferenzen beim Löschen von Dokumenten**

Der XDS Document Service MUSS beim Löschen eines Dokuments D, das in der DocumentEntry.referenceIdList ein Dokument E via  
urn:gematik:iti:xds:2025:childDocument oder  
urn:gematik:iti:xds:2025:parentDocument referenziert,

- für jedes Dokument E, das nicht ebenfalls gelöscht werden soll, prüfen, ob E für den Anfragenden sichtbar ist:
  - Wenn ja, für Dokument E prüfen, ob E für den Anfragenden gemäß Legal Policy das "U"-Recht besitzt, und ansonsten die Verarbeitung mit dem FehlerXDSCannotUnlinkAttachment abbrechen und im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements als Text die DocumentEntry.uniqueId des referenzierten Dokuments angeben;
  - Wenn nein, die Verarbeitung mit dem FehlerXDSCannotUnlinkAttachment abbrechen ohne die DocumentEntry.uniqueId des referenzierten Dokuments E preiszugeben.
- im Dokument E, das nicht ebenfalls gelöscht werden soll, die dazu passende rückwärtige Referenz auf D aus E's referenceIdList entfernen.

[**<=**]

Die Anforderung stellt sicher, dass keine "toten" Eltern- und Kindreferenzen im XDS Document Service verbleiben.

Hinweis: Zum Begriff "sichtbar" siehe analogen Hinweis unter A\_27655.

Hinweis 2: Ein Dokument kann also nicht gelöscht werden, wenn etwaige Anhangsreferenzen ("Backlinks") in den referenzierten Dokumenten nicht gelöscht werden können.

#### 3.13.1.4.3.4 RetrieveDocumentSet [ITI-43]

#### **A\_14914 -XDS Document Service - Ablauflogik für Retrieve Document Set**

Der XDS Document Service MUSS die Umsetzung der Operation RetrieveDocumentSet gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3 ] und [IHE-ITI-TF2b#3.43.4.2.2 und 3.43.4.2.3 ] implementieren. [**<=**]

#### **A\_16201 -XDS Document Service - Prüfung der zurückgegebenen Paketgröße**

Der XDS Document Service MUSS anhand der übergebenen DocumentUniqueIds die Gesamtgröße ermitteln und bei Überschreitung von 250 MByte die Verarbeitung ablehnen und die Nachricht mit einem MaxPkgSizeExceeded-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. [**<=**]

#### 3.13.1.4.3.5 Restricted Update Document Set [ITI-92]

#### **A\_15061-08 -XDS Document Service - Ablauflogik für Restricted Update Document Set**

Der XDS Document Service MUSS die Umsetzung der OperationRestrictedUpdateDocumentSet gemäß der definierten Ablauflogik in [IHE-ITI-RMU#3.92.4.1.2 und 3.92.4.1.3] implementieren und sicherstellen, dass (nur) die folgenden Metadatenobjekte gesendet werden:

- ein neues SubmissionSet,



- einen DocumentEntry inklusive der entryUUID des zu ändernden DocumentEntry-Objekts. Das übermittelte DocumentEntry-Objekt kann sowohl alle vollständigen Metadatenattribute als auch nur zu ändernde Metadatenattribute enthalten. In jedem Fall dürfen Änderungen ausschließlich gemäß A\_15083-\* angenommen und durchgeführt werden.
- für das Hinzufügen, Ändern oder Löschen eines einzelnen oder mehrerer Werte in DocumentEntry.author, DocumentEntry.confidentialityCode, DocumentEntry.eventCodeList und DocumentEntry.referenceIdList gilt darüber hinaus:
  - es MÜSSEN alle und nicht nur die zu ändernden Werte (z. B. Autoren) über ihre jeweiligen <classification classificationScheme="urn:uuid:...>-XML-Elemente im gewünschten Soll-Zustand gesendet werden.
  - das Löschen aller Werte (z. B. Autoren) MUSS durch Übertragung ein einzelnen, komplett leeren <classification="urn:uuid:...>-XML-Elements signalisiert werden.
- eine SS-DE HasMember-Association, die das SubmissionSet mit dem geschickten DocumentEntry verbindet.
- die „lid“ (logicalID) DARF NICHT gesendet werden.
- der Slot "PreviousVersion" MUSS immer mit dem Wert "1" gesendet werden.
- der Slot „AssociationPropagation“ MUSS auf „no“ gesetzt werden. Zusätzlich MUSS der alternative Slot-Name "associationPropagation" akzeptiert werden.

Der XDS Document Service DARF die gesendete Association und das neue SubmissionSet NICHT dauerhaft speichern.【<=】

Der alternative Slot-Name "associationPropagation" wird unterstützt, da alte Versionen von ePA fälschlicherweise, abweichend von [IHE-ITI-RMU] diesen Wert gefordert haben.

#### **A\_15082-02 -XDS Document Service - Validierung der Metadaten aus ITI Document Sharing-Profilen**

Der XDS Document Service MUSS die übermittelten DocumentEntry-Metadaten der OperationRestrictedUpdateDocumentSet dahingehend prüfen, dass gegenüber den Bestandsdaten die geänderten Metadaten konform zu den Nutzungsvorgaben in [A\_14760-\*] geändert werden. Der XDS Document Service MUSS das Aktualisieren der Metadatenattribute ablehnen und mit einemXDSRepositoryMetadataError quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. Es MUSS im codeContext-Attribut des zurückgegebenenrs:RegistryError-Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht.【<=】

#### **A\_15083-09 -XDS Document Service - Prüfung auf ausschließliche Aktualisierung der erlaubten Metadaten**

Der XDS Document Service MUSS die übermittelten DocumentEntry-Metadaten der OperationRestrictedUpdateDocumentSet dahingehend prüfen, dass gegenüber den Bestandsdaten ausschließlich die folgenden Metadaten geändert werden:

- DocumentEntry.author
- DocumentEntry.classCode
- DocumentEntry.comments
- DocumentEntry.confidentialityCode(confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) ist nicht erlaubt)
- DocumentEntry.creationTime
- DocumentEntry.eventCodeList

- DocumentEntry.formatCode
- DocumentEntry.healthcareFacilityTypeCode
- DocumentEntry.languageCode
- DocumentEntry.legalAuthenticator
- DocumentEntry.practiceSettingCode
- DocumentEntry.referenceIdList
- DocumentEntry.serviceStartTime
- DocumentEntry.serviceStopTime
- DocumentEntry.title
- DocumentEntry.typeCode
- DocumentEntry.URI

Wenn das Metadatum DocumentEntry.referenceIdList ohne rootDocumentUniqueId gesendet wird, MUSS der XDS Document Service den Wert automatisch setzen (identisch zu rootDocumentId in DocumentEntry.referenceIdList des ersetzten Dokuments). Wenn die rootDocumentUniqueId gesendet wird, MUSS der XDS Document Service sicherstellen, dass der Wert dem ansonsten automatisch gesetzten Wert entspricht.

Werden unerlaubte Metadatenänderungen geschickt, muss die Operation mit einem LocalPolicyRestrictionError-Fehlercode abgebrochen werden. Werden Metadatenattribute mit leeren Werten übermittelt, signalisiert dies ein Löschen des Metadatums (z.B. DocumentEntry.comments). Es müssen die Kardinalitäten in A\_14760-\* berücksichtigt bzw. dürfen nicht verletzt werden (Ausnahme für Altdaten: eventCodeList darf mehr als einen DMP- oder KDL-Code in der eventCodeList enthalten, wenn der alte Metadatensatz bereits dieselben DMP- und KDL-Codes führt). Das Metadatum DocumentEntry.referenceIdList MUSS dabei mindestens die rootDocumentUniqueId enthalten.

Wenn in der Eingangsnachricht keine Aktualisierung für die erlaubten Metadaten enthalten ist, ist die Weiterverarbeitung abzubrechen und die Nachricht mit einem LocalPolicyRestrictionError-Fehlercode zu quittieren. [≤]

#### **A\_27657-01 -XDS Document Service - Anhänge hinzufügen oder entfernen mit Restricted Update Document Set**

Der XDS Document Service MUSS beim Aktualisieren eines DocumentEntries die folgenden Regeln durchsetzen (der Text bezieht sich auf das Einfügen oder Entfernen eines parentDocument; die analoge Handlungsanweisung für childDocument ist jeweils in Klammern angegeben):

- Wenn die DocumentEntry.referenceIdList vor der Aktualisierung auf ein überurn:gematik:iti:xds:2025:parentDocument (urn:gematik:iti:xds:2025:childDocument) ausgezeichnetes Dokument verweist, dieses aber für den Anfragenden nicht sichtbar ist, MUSS der XDS Document Service den entsprechenden Eintrag für die weitere Bearbeitung automatisch wieder hinzufügen.
- Wenn dem Feld DocumentEntry.referenceIdList ein Wert mit der Auszeichnung urn:gematik:iti:xds:2025:parentDocument (urn:gematik:iti:xds:2025:childDocument) hinzugefügt wird, MUSS der XDS Document Service prüfen,
  - ob das vom Anfragenden dort referenzierte Dokument nicht existent oder für das anfragende System nicht sichtbar ist und in diesem Fall die Operation mit dem Fehler XDSNoSuchParent (XDSNoSuchChild) abbrechen,

- ob für beide betroffenen Dokumente die Berechtigung "U" (gemäß Legal Policy) vorliegt und ansonsten die Verarbeitung mit dem Fehler `XDSCannotLinkAttachment` abbrechen und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements als Text die `DocumentEntry.uniqueId` des referenzierten Dokuments angeben,
- ob die Kennzeichnung des Dokuments als Anhang einen Verweiszirkel verursachen würde und ggf. die Operation mit dem Fehler `XDSAttachmentCycle` abbrechen;
- ob durch das Markieren des Dokuments der zusätzliche Verweis nicht auf ein Elterndokument (Kinddokument) gemacht wird, das bereits Teil der Elternketten (Kindkette) ist und ansonsten die Verarbeitung mit dem Fehler `XDSInvalidAttachmentHierarchy` abbrechen.
- Wenn aus dem Feld `DocumentEntry.referenceIdList` ein Wert mit der Auszeichnung `urn:gematik:iti:xds:2025:parentDocument(urn:gematik:iti:xds:2025:childDocument)` entfernt wird, MUSS der XDS Document Service prüfen,
  - ob für beide betroffenen Dokumente die Berechtigung "U" (gemäß Legal Policy) vorliegt und ansonsten die Verarbeitung mit dem Fehler `XDSCannotUnLinkAttachment` abbrechen und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements als Text die `DocumentEntry.uniqueId` des referenzierten Dokuments angeben,
  - und ansonsten im dort referenzierten Dokument den passenden `urn:gematik:iti:xds:2025:childDocument(urn:gematik:iti:xds:2025:parentDocument)`-Eintrag aus der `referenceIdList` entfernen.

#### 【<=】

Das Hinzufügen oder Entfernen von bestehenden Anhängen wird also immer entweder über den Verweis auf ein Eltern- oder Kinddokument vorgenommen; das referenzierte Dokument selbst wird immer automatisch angepasst. Wird über RMU die `referenceIdList` so gesetzt, dass die Eltern- und Kinddokumentauszeichnungen unverändert bleiben, ist A\_27657 nicht relevant.

Zum Begriff "sichtbar" siehe analogen Hinweis unter A\_27655. Die spezielle Behandlung für nicht sichtbare Dokumente ist notwendig, da eine Dokumentensuche eine solche Anhangsbeziehung zum verbundenen Dokument gemäß A\_27762 aus der `DocumentEntry.referenceIdList` entfernt. Eine anschließende Aktualisierung des Dokuments kann also in aller Regel auch den Verweis auf das nicht sichtbare Eltern- oder Kinddokument nicht enthalten. Wenn der Anfragende es dennoch mitliefert (aus welcher Quelle auch immer), gilt wie in der Anforderung beschrieben, dass der gesamte Aufruf mit dem Fehler `XDSNoSuchParent` bzw. `XDSNoSuchChild` abgelehnt werden muss (nicht etwa mit `XDSInvalidAttachmentHierarchy`).

Falls das Ändern der Metadaten zur Folge hat, dass ein Dokument in eine andere Dokumentenkategorie gemäß Legal Policy fällt, wird durch den XDS Document Service bewertet, ob der Anfragende überhaupt Dokumente in diese Kategorie einstellen darf. In dem Zusammenhang ist auch zu bewerten, ob alle per `referenceIdList` "geforderten" Anhänge des Dokuments überhaupt in dieser neuen Kategorie angehängt werden können (Berechtigung "U") und ob auch die Regeln zum Einstellen von Anhängen im Allgemeinen (darf der Dokumententyp bspw. Anhänge besitzen) eingehalten werden. Beispiel: Für einen PDF/A-Arztbrief mit Anhängen wird der `classCode` auf "ADM" (administratives Dokument) geändert. Das Dokument ist damit nicht mehr als Arztbrief identifizierbar (A\_27761) und sofern es nicht als anderer Dokumententyp erkannt wird, für den Anhänge erlaubt sind, ist das Metadatenupdate abzulehnen. Der passenden Fehler wäre in dem Fall wie oben angegeben "XDSCannotLinkAttachment". Ein Client kann ggf. nur zuerst Dokumente "abhängen" und dann die Operation neu starten.

**A\_21533 -XDS Document Service - Kein Anlegen von Versionen für Restricted Update Document Set**

Der XDS Document Service DARF eine echte Versionierung NICHT umsetzen, d. h. er DARF den alten DocumentEntry NICHT speichern. Insbesondere DARF der XDS Document Service DocumentEntry.version NICHT anlegen und verwalten.[<=]

**A\_21783-03 -XDS Document Service - Vererbung der geänderten Metadaten für Restricted Update Document Set**

Der XDS Document Service MUSS die neu gesetzten Metadaten ebenfalls auf alle mit dem geänderten Dokument assoziierten Dokumente setzen. Als assoziierte Dokumente sind im Sinne dieser Anforderung Dokumente einer RPLC-Kette zu betrachten.[<=]

Metadaten von Dokumenten einer mixed- oder uniform-Sammlung dürfen nicht geändert werden.

**A\_25173 -XDS Document Service - Restricted Update Document Set nicht für MIOs**

Falls die OperationRestrictedUpdateDocumentSet für Dokumente einer mixed- oder uniform-Sammlung aufgerufen wird MUSS der XDS Document Service das Aktualisieren der Metadatenattribute ablehnen, mit einemXDSRepositoryMetadataError quittieren und im codeContext-Attribut des zurückgegebenenrs:RegistryError-Elements den Text "Metadata Update for MIOs not allowed" angeben.  
[<=]

*3.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen***A\_24508-01 -XDS Document Service - Prüfung der Policies bei Suchanfrage**

Der XDS Document Service MUSS bei einer Suchanfrage für einen angemeldeten Nutzer die Suchergebnismenge entsprechend der Legal Policy und der General Deny Policy filtern, d. h. die Suchergebnismenge enthält ausschließlich XDS-Metadaten, die für einen angemeldeten Nutzer nicht diesen Policies widersprechen.[<=]

**A\_26222 -XDS Document Service (EU) - Prüfung Zugriffscode bei Suchanfrage EU-Zugriff**

Der XDS Document Service MUSS für einen angemeldeten Nutzer mit der Rolle oid\_ncpeh bei jeder Suchanfrage und jeder Retrieve-Operation prüfen, dass der im SOAP-Header der Operation übergebene Zugriffscode identisch ist mit dem im Entitlement Management für diesen Nutzer hinterlegten Zugriffscode und andernfalls die Operation mit dem Fehlercode AccessCodeViolation beenden.[<=]

**A\_24509 -XDS Document Service - Prüfung der Legal Policy außer Suchanfragen**

Der XDS Document Service MUSS die Ausführung einer Operation mit dem Fehlercode LegalPolicyViolation beenden, wenn für den angemeldeten Nutzer die Regeln der Legal Policy nicht erfüllt sind und es sich nicht um eine Suchanfrage handelt.  
Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die Liste der UUIDs (DocumentEntry.entryUUID) der identifizierten Dokumente angegeben werden.[<=]

**A\_24510-02 -XDS Document Service - Prüfung Herunterladen eines verborgenen oder nicht vorhandenen Dokuments**

Der XDS Document Service MUSS die Ausführung der Retrieve-Operation mit dem Fehlercode XDSDocumentUniqueldError beenden, wenn das assoziierte Dokument nicht vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.[<=]

**A\_24511-01 -XDS Document Service - Prüfung Löschen eines verborgenen Dokuments oder dynamischen Ordners**

Der XDS Document Service MUSS die Ausführung der Remove-Operation mit dem Fehlercode XDSDocumentUniqueldError beenden, wenn für den angemeldeten Nutzer die

Regeln der General Deny Policy nicht erfüllt sind.  
[<=]

#### **A\_24512-02 -XDS Document Service - Prüfung Schreiben eines Dokuments in einen nicht vorhandenen oder verborgenen dynamischen Ordner**

Der XDS Document Service MUSS die Ausführung der Provide-Operation mit dem Fehlercode UnresolvedReferenceException beenden, wenn der Ordner nicht existiert oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.  
[<=]

#### **A\_24513-02 -XDS Document Service - Prüfung Aktualisierung Metadaten eines verborgenen oder nicht vorhandenen Dokuments**

Der XDS Document Service MUSS die Ausführung der Update-Operation mit dem Fehlercode UnresolvedReferenceException beenden, wenn das assoziierte Dokument nicht vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind. [<=]

### **3.13.1.5 Fehlerbehandlung in Schnittstellenoperationen**

#### **A\_22516-02 -XDS Document Service - Alternative Verwendung von XDSRegistryMetadataError anstelle von XDSRepositoryMetadataError**

Der XDS Document Service KANN alternativ zum Fehler "XDSRepositoryMetadataError" den Fehler "XDSRegistryMetadataError" verwenden. [<=]

#### **A\_23148-01 -XDS Document Service - Festlegung zu http-Statuscode bei IHE-Responses**

Der XDS Document Service MUSS für den Fall, dass eine IHE-Response in der HTTP-Response enthalten ist, den http-Statuscode 200 zurückgeben. Das gilt auch, wenn die IHE-Response einen IHE-Fehler überträgt. [<=]

#### **A\_26324-01 -XDS Document Service - Aktenkonto im Umzug**

Falls sich ein Aktenkonto im Zustand SUSPENDED befindet MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem StatusMismatch-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. <=[<=]

#### **A\_26325-01 -XDS Document Service - Aktenkonto unbekannt oder im Zustand INITIALIZED**

Falls sich ein Aktenkonto im Zustand UNKNOWN oder INITIALIZED befindet MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem NoHealthRecord-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. <=[<=]

#### **A\_25683-01 -XDS Document Service - Prüfung auf Befugnis**

Falls keine gültige Befugnis für den aufrufenden Nutzer vorliegt MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem NotEntitled-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. [<=]

#### **A\_26459 -XDS Document Service - keine Authentisierung des Nutzers**

Falls keine erfolgreiche Authentifizierung des Nutzers vorliegt MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem InvalidAuth-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. <=[<=]

#### **A\_27541 -XDS Document Service - keine Geräteregistrierung des Nutzers**

Falls der Nutzer der Versicherte oder ein Vertreter ist (oid\_versicherter) und keine Geräteregistrierung des Nutzers vorliegt, MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem UnregisteredDevice-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. [<=]

### 3.13.1.6 Schnittstellen im XDS Document Service

In diesem Abschnitt wird die Außenschnittstelle des XDS Document Service festgelegt. Einzelne Umsetzungsanforderungen suggerieren eine vermischte Verarbeitung von Funktionalitäten, welche bei IHE ITI originär getrennt von einer Document Registry und einem Document Repository (bzw. den Responding Gateways) durchgeführt werden. Da die Außenschnittstelle des XDS Document Service nicht zwischen Document Registry und Document Repository unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit differenzierten Pfaden, siehe A\_26814-\*, werden sonst bei IHE ITI explizite Operationen zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne Umsetzung angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-Nachricht kann an IHE ITI-konforme Akteure ausgerichtet werden.

#### 3.13.1.6.1 Schnittstelle I\_Document\_Management

Weitere Vorgaben zu den Operationen befinden sich in [3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen](#).

### A\_14152-02 -XDS Document Service - Implementierung der Schnittstelle I\_Document\_Management

Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle für den Zugriff von ePA-Clients, die über das zentrale Netz zugreifen implementieren.

**Tabelle 27: Schnittstelle I\_Document\_Management**

Schnittstelle	I_Document_Management	
Version	2.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	ProvideAndRegisterDocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Metadata	Löschen von Dokumenten oder Ordnern
	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
WSDL	[XSDDocumentService]	
XML Schema	<ul style="list-style-type: none"> <li>PRPA_IN201301UV02.xsd</li> </ul>	



	<ul style="list-style-type: none"> <li>• PRPA_IN201302UV02.xsd</li> <li>• PRPA_IN201304UV02.xsd</li> <li>• MCCI_IN000002UV01.xsd</li> <li>• query.xsd</li> <li>• rs.xsd</li> <li>• lcm.xsd</li> <li>• rim.xsd</li> <li>• XDS.b_DocumentRepository.xsd</li> </ul>
--	--

**[<=]**

Durch die Legal Policy ist geregelt, welche Clients (professionOID) letztendlich zugreifen dürfen.

3.13.1.6.1.1 Operation I\_Document\_Management::ProvideAndRegisterDocumentSet-b  
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "ProvideAndRegisterDocumentSet-b" [ITI-41] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner gesammelt. Das Anlegen eines DiGA-Ordners erfolgt durch den XDS Document Service unter der Voraussetzung, dass es eine gültige Befugnis für die DiGA gibt. Der DiGA-Ordner wird vom XDS Document Service mit der Telematik-ID der DiGA verknüpft. Die Zuordnung von DiGA-Dokumenten beim Schreiben erfolgt implizit über die TelematikID aus dem IDToken des Nutzers. Da ein DiGA-Ordner im Titel immer den Namen der DiGA enthält kann ein Client (z.B. LEI) darüber die relvante DiGA auswählen und auf die Dokumente der DiGA, sofern eine Befugnis für den Nutzer vorliegt, lesend zugreifen.

Ein Update eines bestehenden Dokuments mit der bekannten DocumentEntry.entryUUID kann durch einen DiGA-Client erfolgen. Hierzu ist es erforderlich, dass ein DiGA-Client die DocumentEntry.entryUUID persistiert und keine symbolischen IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] verwendet.

**A\_21512-04 -XDS Document Service - dynamisches Anlegen von DiGA-Ordern**

Falls eine gültige Befugnis für eine konkrete DiGA vorliegt, MUSS der XDS Document Service beim erstmaligen Einstellen eines Dokumentes für diese DiGA in die Akte des Versicherten (Operation I\_Document\_Management::ProvideAndRegisterDocumentSet-b()) sicherstellen, dass genau ein Ordner für den Versicherten mit den folgenden Eigenschaften angelegt ist:

- DiGA-Ordner der Kategorie diga gemäß A\_19388 (Belegung Folder.codeList) unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A\_14760 (Belegung der restlichen Metadatenfelder).
- Folder.title wird entsprechend des Attributs "organizationName" aus dem IDToken der zugreifenden DiGA belegt.
- Folder.comment wird belegt mit "urn:gematik:diga:<Telematik-ID>", wobei die Telematik-ID dem Attribut "idNummer" des ID-Token entspricht.
- Folder.EntryUUID wird mit einer aus der TelematikID abgeleiteten UUID belegt.

Die folder.EntryUUID MUSS wie folgend dargestellt aus der TelematikID der DiGA erzeugt werden:

- Algorithmus: Name-Based UUID gemäß [RFC4122#4.3], Version 3 (MD5)
- Namensraum-UUID: "e2310a38-0b62-415e-8b44-994dc8312965"



- Name: "<TelematikId>"

Eine konkrete DiGA wird identifiziert durch die TelematikID und ist als DiGA durch die professionOID gekennzeichnet.

[<=]

#### **A\_22994-01 -XDS Document Service - automatische Folder-Zuordnung für DiGA**

Der XDS Document Service MUSS beim Einstellen eines DiGA-Dokumentes in die Akte des Versicherten (Operation I\_Document\_Management::ProvideAndRegisterDocumentSet-b()) sicherstellen, dass das DiGA-Dokument in den durch die TelematikID referenzierten DiGA-Ordner abgelegt wird. Die TelematikID des zu adressierenden Ordners entspricht dem Attribut "idNummer" des ID-Token .[<=]

#### **A\_21713-03 -XDS Document Service - Kein Einstellen von Ordnern**

Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) über die Schnittstelle I\_Document\_Management::ProvideAndRegisterDocumentSet-b ablehnen und mit einem XDSRegistryMetadataError-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder enthalten sind. Ausnahme: Folder der Kategorie pregnancy\_childbirth in Folder.codeList.[<=]

#### **A\_24497 -XDS Document Service - Verwendung der korrekten Telematik-ID beim Einstellen**

Der XDS Document Service MUSS die Telematik-ID aus dem ID-Token der aktuellen User Session abgleichen mit der Telematik-ID aus SubmissionSet.authorInstitution und das Abweichen der Telematik-Ids mit einem XDSRepositoryMetadataError-Fehlercode quittieren und im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements den Text "Telematik-ID does not match" angeben.[<=]

#### **A\_24456 -XDS Document Service - Durchsetzung von Uniqueness beim Einstellen von Notfalldaten**

Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien "emergency" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein einzelnes NFD- und ein einzelnes DPE-Dokument im Status "approved" gibt. Der Versuch, innerhalb dieses Ordners ein zweites NFD- oder DPE-Dokument einzustellen, MUSS mit dem IHE-ErrorInvalidDocumentContent abgebrochen werden. Es MUSS im codeContext-Attribut des zurückgegebenen InvalidDocumentContent-Elements der Text "Medical information object has to be unique" zurückgegeben werden.[<=]

#### **A\_25137 -XDS Document Service - Durchsetzung von Uniqueness beim Einstellen vom Medikationsplan**

Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien "emp" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein einzelnes eMP-Dokument im Status "approved" gibt. Der Versuch, innerhalb dieses Ordners ein zweites eMP-Dokument einzustellen, MUSS mit dem IHE-ErrorInvalidDocumentContent abgebrochen werden. Es MUSS im codeContext-Attribut des zurückgegebenen InvalidDocumentContent-Elements der Text "Medical information object has to be unique" zurückgegeben werden.[<=]

##### **3.13.1.6.1.2 Operation I\_Document\_Management::RegistryStoredQuery**

Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

##### **3.13.1.6.1.3 Operation I\_Document\_Management::RemoveMetadata**

Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

#### 3.13.1.6.1.4 Operation I\_Document\_Management::RetrieveDocumentSet

Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

#### 3.13.1.6.1.5 Operation I\_Document\_Management::RestrictedUpdateDocumentSet

Weitere Details zur Ausgestaltung dieser Operation finden sich bezüglich der dazugehörigen IHE ITI-Transaktion "RestrictedUpdateDocumentSet" [ITI-92] in [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x].

Weitere Anforderungen zur Umsetzung der Operation RestrictedUpdateDocumentSet befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92] .

#### 3.13.1.6.2 Schnittstelle I\_Document\_Management\_Insurant

Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen .

### A\_14478-01 -XDS Document Service - Implementierung der Schnittstelle I\_Document\_Management\_Insurant

Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle für den Zugriff des ePA-FdV implementieren .

**Tabelle 28: Schnittstelle I\_Document\_Management\_Insurant**

Schnittstelle	I_Document_Management_Insurant	
Version	2.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente im XDS Document Service
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Metadata	Löschen ein oder mehrerer Dokumente oder Folder
	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
WSDL	[XDSDocumentService]	
XML Schema	<ul style="list-style-type: none"> <li>PRPA_IN201301UV02.xsd</li> <li>PRPA_IN201302UV02.xsd</li> </ul>	

	<ul style="list-style-type: none"> <li>• PRPA_IN201304UV02.xsd</li> <li>• MCCI_IN000002UV01.xsd</li> <li>• query.xsd</li> <li>• rs.xsd</li> <li>• lcm.xsd</li> <li>• rim.xsd</li> <li>• XDS.b_DocumentRepository.xsd</li> </ul>
--	---

[<=]

#### **A\_26460 -XDS Document Service - Zugriff über I\_Document\_Management\_Insurant mit nicht registriertem Gerät**

Falls Operationen von I\_Document\_Management\_Insurant ohne registriertes Gerät aufgerufen werden MUSS der XDS Document Service die Verarbeitung ablehnen und mit einemUnregisteredDevice-Fehlercode quittieren.[<=]

##### 3.13.1.6.2.1 Operation

I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b

Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Provide And Register Document Set-b" [ITI-41] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

#### **A\_21481-05 -XDS Document Service - Kein Einstellen von Ordnern und Associations**

Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) über die Schnittstelle

I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b() ablehnen und mit einem XDSRegistryMetadataError-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder oder andere als die folgenden Assoziationen

- SS-DE
- SS-HM
- FD-DE
- RPLC

enthalten sind.[<=]

Das Referenzieren bestehender Ordner ist davon nicht berührt, wie dies z. B. beim Einstellen von Dokumenten in Sammlungen der Fall ist (z. B. Einstellen eines Dokuments in einen Mutterpass).

#### **A\_23144 -XDS Document Service - Automatische Ablage von Dokumenten im Ordner "technical"**

Der XDS Document Service MUSS sicherstellen, dass Dokumente mit einem formatCode mit der codeSystem OID "2.25.154081344090540725127779452347992051720", unabhängig von weiteren Metadaten, im statischen Ordner "technical" abgelegt werden. [<=]

##### 3.13.1.6.2.2 Operation I\_Document\_Management\_Insurant::RegistryStoredQuery

Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Registry Stored Query" [ITI-18] sind [IHE-ITI-TF2a], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.2.3 Operation `I_Document_Management_Insurant::RemoveMetadata`  
 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.2.4 Operation `I_Document_Management_Insurant::RetrieveDocumentSet`  
 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RetrieveDocumentSet" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.2.5 Operation  
`I_Document_Management_Insurant::RestrictedUpdateDocumentSet`  
 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RestrictedUpdateDocumentSet" [ITI-92] sind [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

Weitere Anforderungen zur Umsetzung der Operation `RestrictedUpdateDocumentSet` befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92].

### 3.13.1.6.3 Schnittstelle `I_Document_Management_Ncpeh`

Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen.

## A 27300-01 -XDS Document Service (EU) - Implementierung der Schnittstelle `I_Document_Management_Ncpeh`

Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle für den Zugriff durch den NCPeH-FD implementieren.

**Tabelle 29: Schnittstelle `I_Document_Management_Ncpeh`**

Schnittstelle	<code>I_Document_Management_Ncpeh</code>	
Version	2.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
WSDL	[XDSDocumentService]	
XML Schema	<ul style="list-style-type: none"> <li>PRPA_IN201301UV02.xsd</li> <li>PRPA_IN201302UV02.xsd</li> <li>PRPA_IN201304UV02.xsd</li> <li>MCCI_IN000002UV01.xsd</li> <li>query.xsd</li> </ul>	

	<ul style="list-style-type: none"> <li>• rs.xsd</li> <li>• lcm.xsd</li> <li>• rim.xsd</li> <li>• XDS.b_DocumentRepository.xsd</li> </ul>
--	--

### [<=]

3.13.1.6.3.1 Operation I\_Document\_Management\_Ncpeh::RegistryStoredQuery  
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.3.2 Operation I\_Document\_Management\_Ncpeh::RetrieveDocumentSet  
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

### 3.13.1.7 Statische Metadaten

Statische Inhalte werden vor der ersten Nutzung des XDS Document Service angelegt, d. h. bevor auf XDS Metadaten zugegriffen wird. Sie sind unveränderlich.

#### A\_24491-02 -XDS Document Service - Anlegen von statischen Ordnern

Der XDS Document Service MUSS nach der erfolgreichen Anlage der Akte des Versicherten die Kategorienordner unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A\_14760\* (Belegung der restlichen Metadatenfelder) für den Versicherten gemäß der folgenden Tabelle anlegen. Alle statischen Kategorienordner werden mit jeweils einem Ordner pro Kategorie angelegt. Alle statischen Ordner sind nach dem Anlegen initial leer.

Das Anlegen von Submission Sets und zugehöriger Associations zu den statischen Ordnern ist nicht vorgegeben. Das XDS-Informationsmodell MUSS allerdings hinsichtlich der Folder-DocumentEntry- sowie SubmissionSet-HasMember-Associations bei einer Verarbeitung durch die Document Consumer (z. B. Querying) erfüllt werden.

**Tabelle 30: Festlegung Folder.entryUUID zu statischen Ordnern**

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
reports	b878db05-49e4-4f74-a329-b3bcdd8082c4
emp	7c1054ea-a4df-4a1b-8e10-209f6d8812ee
emergency	a7bb6be7-d756-46dd-90d4-4020ed55b777
eab	2ed345b1-35a3-49e1-a4af-d71ca4f23e57
dental	af547321-b8e8-4e1d-b9af-51bb4a990bda

child	2c898452-4667-40e3-9d3e-c09d7385b527
vaccination	9c3edaf3-a978-46fe-8e6e-021ff4aca60b
patient	d236c9a2-ab01-4902-a00a-1e1dff439fe7
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d
health_risk_analysis	840a59c7-61d4-4caa-80a7-1857af2f166f
care	2d62bf9e-062a-4aa7-9951-9f33bbc665b5
eau	aa7d10d6-204a-47aa-be73-44bdc77512f
other	605a9f3c-bfe8-4830-a3e3-25a4ec6612cb
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31
rehab	173f4204-fb93-4a1a-a1f6-316703b79539
transcripts	6A8E383D-8705-4B0E-A140-39A5F144501D

**[<=]**

*Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner vom Typ "pregnancy\_childbirth" und verwenden als Folder.title ein Kennzeichen der Schwangerschaft (A\_22515-\*).*

#### **A\_20216-04 -XDS Document Service - Unveränderlichkeit von statischen Akteninhalten**

Der XDS Document Service DARF die Metadaten eines statischen Aktenobjekts gemäß A\_24491 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen. Dabei gelten folgende Ausnahmen:

- Folder.lastUpdateTime - Folder.lastUpdateTime wird automatisch vom XDS Document Service aktualisiert, sobald Dokumente in den Ordner eingestellt (siehe auch [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6]), daraus gelöscht oder darin aktualisiert werden.

**[<=]**

### 3.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten

Für den XDS Document Service werden Vorgaben bezüglich zu verwendender IHE XDS-Metadatenattribute auf Ebene von Submission Set, Document Entry sowie Folder vorgenommen. Diese Nutzungsvorgaben referenzieren größtenteils Value Sets der IHE Deutschland Arbeitsgruppe "XDS Value Sets" [IHE-ITI-VS] und sind für die ePA-Fachanwendung verbindlich. Diese XDS-Value Sets sind teilweise von IHE-Deutschland als "offen" gekennzeichnet, um Erweiterungen flexibel einbringen zu können. Für die ePA-Fachanwendung gelten jedoch definierte Vorgaben, wie neue Codes und Value Sets sicher über eine Konfigurationsschnittstelle eingebracht werden können. Daher sind die in dieser Spezifikation beschriebenen Nutzungsvorgaben für Value Sets als fest anzusehen bzw. die Offenheit der XDS Value Sets wird nicht unterstützt.

#### 3.13.1.8.1 Allgemeine Metadatenvorgaben

Die Spalten der unten dargestellten, tabellarischen Übersichten für die Metadaten von Dokumenten (IHE XDS.b Document Entry) und Übertragungspaketen (IHE XDS.b Submission Set) haben die folgenden Bedeutungen:

- Die Spalte "Metadatenattribut XDS.b" listet alle aus dem IHE ITI TF vorgesehenen Metadaten für Document Entry- und Submission Set-Elemente auf.
- Die Spalten "Mult. PS" (Multiplizität Primärsystem; alle Primärsysteme außer PS-KTR), "Mult. KTR" (Multiplizität "PS-KTR"), "Mult. DS" (Multiplizität "Document Service"), "Mult. FV" (Multiplizität "ePA-Frontend des Versicherten") kennzeichnen die Multiplizität des Metadatenattributs beim Erzeugen oder Verarbeiten durch das jeweilige System.  
Die Angabe der jeweiligen Spalte entspricht einem Wertebereich. Die Zeichen [...] für Wertebereich wurden zum Zwecke der besseren Darstellbarkeit weggelassen.
- Die Spalte "Kurzbeschreibung" beschreibt kurz die Bedeutung des Metadatenattributs.
- Die Spalte "Nutzungsvorgabe" macht Bedingungen für die Verwendung eines Metadatenattributs (z. B. erlaubte Wertebereiche und Formatangaben), welche über die im IHE ITI TF definierten Vorgaben hinausgehen.
- Die Spalte "FV Edit" beschreibt, ob ein bestimmtes Metadatenattribut beim Einstellen eines Dokuments über das ePA-FdV durch den Versicherten veränderbar gestaltet werden muss. Es sollten dabei immer nur die für den aktuellen Workflow relevanten Metadatenattribute angezeigt werden, um die Komplexität für den Versicherten gering zu halten. Veränderbar gestaltete Metadatenattribute müssen mit sinnvollen Default-Werten vorbelegt werden.

#### A\_14760-27 -Nutzungsvorgaben für die Verwendung von XDS-Metadaten

Der XDS Document Service MUSS sicherstellen, dass Primärsysteme und das ePA-Frontend des Versicherten zur Registrierung von Dokumenten die nachstehenden Nutzungsvorgaben für Metadaten berücksichtigen. Der XDS Document Service MUSS diese Metadaten verarbeiten können und diese Metadaten ggf. während des Registriervorgangs ergänzen. Metadaten können über die Operationen

- `I_Document_Management::ProvideAndRegisterDocumentSet-b` sowie
- `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b`

registriert oder über die Operationen

- `I_Document_Management::RestrictedUpdateDocumentSet`
- `I_Document_Management_Insurant::RestrictedUpdateDocumentSet`

geändert werden.

Für den Produkttyp DiGA gelten die gleichen Vorgaben wie für die Primärsysteme sofern unter Nutzungsvorgaben keine abweichenden Bedingungen definiert werden.



Tabelle 31: Nutzungsvorgaben für Metadatenattribute XDS

Metadaten- attribut XDS.b	Multiplizität				Kurz-beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
Metadaten für DocumentEntry							
author	1. .n	1. .1	0. .0	0. .n	Person oder System, welche(s) das Dokument erstellt hat	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.1] genügen. Das Primärsystem MUSS mindestens das Subattribut authorPerson oder authorInstitution inhaltlich belegen.	
authorPerson	0. .1	0. .1	0. .0	0. .1	Name des Autors	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt <u>3.13.1.8.2-Metadaten der Dokumente und SubmissionSets</u> genügen.	X
authorInstitution	0. .n	0. .n	0. .0	0. .n	Institution, die dem Autor zugeordnet ist	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt <u>3.13.1.8.2-Metadaten der Dokumente und SubmissionSets</u> (A_21209) genügen.	X
authorRole	0. .n	0. .n	0. .0	0. .n	Rolle des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS aus [IG_TI_Terminology] entsprechen.	X
authorSpecialty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorSpecialty VS aus [IG_TI_Terminology] entsprechen.	X
authorTelecommunication	0. .n	0. .0	0. .0	0. .n	Telekommunikationsdaten des Autors	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	X
availabilityStatus	0. .0	0. .0	1. .1	0. .0	Status des Dokuments ("Approved" oder "Deprecated")	Der Wert MUSS initial "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" sein.	

						ed" entsprechen.	
classCode	1. .1	1. .1	0. .0	1. .1	Grobe Klassifizierung des Dokuments	<p>Der Wert MUSS einem Code des Value Sets EPAXDSCClassCodeVS aus [IG_TI_Terminology] entsprechen.</p> <p>Sofern das Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt <u>3.13.1.9- Strukturierte Dokumente</u> genügen.</p> <p>PS-KTR MUSS für Dokumente</p> <ul style="list-style-type: none"> <li>• der Kategorie receipt ausschließlich den Code "ADM" (Administratives Dokument) verwenden</li> <li>• und für solche der Kategorie health_risk_analysis den Code "ASM" (Assessment) verwenden.</li> </ul>	X
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.4] genügen.	X
confidentialityCode	0. .n	0. .n	0. .1	0. .n	Vertraulichkeitskennzeichnung des Dokuments	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3# 4.2.3.2.5] genügen und einem Code des Value Sets EPAXDSCConfidentialityCodeVS aus [IG_TI_Terminology] entsprechen.</p> <p>Für ProvideAndRegisterDocumentSet-b MUSS für das Verbergen des Dokumentes der Code</p> <ul style="list-style-type: none"> <li>• Code = "CON", Display Name = "constraint"</li> </ul> <p>aus dem Code System 1.2.276.0.76.5.491 (siehe auch Value Set EPAXDSCConfidentialityCodeVS aus [IG_TI_Terminology]) gesetzt werden.</p>	X

creationTime	1. .1	1. .1	0. .0	1. .1	Erstellungszeitpunkt des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.6] genügen und DARF NICHT in der Zukunft liegen. Bei der Prüfung ist eine Toleranz von 5 Minuten zulässig.	X
entryUUID	1. .1	1. .1	0. .1	1. .1	Intern verwendete, aktenweit eindeutige Kennung des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.7] genügen.  Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.	
eventCodeList	0. .n	0. .0	0. .0	0. .n	Ereignisse, die zur Erstellung des Dokuments geführt haben.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.8] genügen und Codes des Value Set EPAXDSEventCodeVS aus [IG_TI_Terminology] entsprechen.  Der Wert darf höchstens einen KDL-Code ("Klinische Dokumentenklassen-Liste") und höchstens einen DMP-Code ("Disease Management Programm") enthalten.  Hinweis: Frühere Versionen der ePA für alle haben das Einstellen von mehreren KDL- bzw. DMP-Codes in die eventCodeList nicht unterbunden. Deshalb kann es Altdaten geben, die noch mehr als einen Code der entsprechenden Code-Systeme in der eventCodeList enthalten.	X
formatCode	1. .1	1. .1	0. .0	1. .1	Global eindeutiger Code für das Dokumentenformat.  Zusammen mit dem DocumentEntry.typeCode eines Dokuments soll es einem potentiellen	Der Wert MUSS einem Code des Value Sets EPAXDSFormatCode aus [IG_TI_Terminology] entsprechen. Der Wert KANN "urn:ihe:iti:xds:2017:mimeTypeSufficient" (siehe [IHE-ITI-TF-3#4.2.3.2.9]) entsprechen, um anzuzeigen, dass über den MIME-Type hinaus keine genaueren	

					zugreifenden System erlauben, im Vorfeld festzustellen, ob das Dokument verarbeitet werden kann.	Angaben zum Dokumentenformat gemacht werden können oder der MIME-Type ausreichend ist.  Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9-Strukturierte Dokumente genügen.	
hash	0. .0	0. .0	1. .1	0. .0	Kryptographische Prüfsumme des Dokuments	Der Wert wird vom XDS Document Service beim Einstellen des Dokuments in die Akte berechnet.	
healthcareFacilityTypeCode	1. .1	1. .1	0. .0	1. .1	Art der Einrichtung, in der das dokumentierte Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSHealthcareFacilityTypeCodeVS aus [IG_TI_Terminology] entsprechen. Das PS-KTR MUSS healthcareFacilityTypeCode ausschließlich mit dem Wert "VER" (Versicherungsträger) belegen. Die DiGA MUSS healthcareFacilityTypeCode mit dem Wert "PAT" belegen.	X
homeCommunityId	0. .1	0. .1	0. .0	0. .1		n/a Eine optional übertragene homeCommunityId wird nicht gespeichert.	
languageCode	1. .1	1. .1	0. .0	1. .1	Sprache, in der das Dokument abgefasst ist.	Der Wert MUSS einem Code des Value Sets EPAXDSLLanguageCodeVS aus [IG_TI_Terminology] entsprechen. Es MÜSSEN mindestens die in der Tabelle Tab_LanguageCodes angegebenen Codes unterstützt werden, alle weiteren Codes KÖNNEN unterstützt werden.	X
legalAuthentication	0.	0.	0.	0.	Rechtlich	Der Wert MUSS den	

r	.1	.0	.0	.1	Verantwortlicher für das Dokument	<p>Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.14] genügen.</p> <p>Das Attribut DARF NICHT gesetzt werden, falls es sich um ein automatisch erstelltes und nicht durch eine natürliche Person freigegebenes Dokument handelt.</p>	
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierungsattribut, dass das Metadatenelement DocumentEntry nicht den vollständigen Satz an Metadaten enthält.		
contentType	1. .1	1. .1	0. .0	1. .1	MIME-Type des Dokuments	<p>Ein Wert aus der folgenden Liste gemäß A_24864* und A_25009* MUSS als MIME-Type verwendet werden.</p> <p>PS-KTR MUSS für Dokumente der Kategorie health_risk_analysis ausschließlich den Wert "application/pdf" gemäß A_25009-* verwenden. Als formatCode ist dann entsprechend "urn:ihe:iti:xds:2017:mimeTypeSufficient" zu verwenden</p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9-Strukturierte Dokumente genügen. <u>Anmerkung:</u> In Klammern sind die Extensions angegeben, die beim entsprechenden MIME-Type in DocumentEntry.URI für das URI-scheme "file," zu verwenden sind.</p>	
objectType	1. .1	1. .1	0. .0	1. .1	Typ des Dokuments	Der Wert MUSS immer "urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"	

						betragen. Dieser Wert steht für stabile Dokumente im IHE ITI XDS.b-Profil [IHE-ITI-TF3#4.2.5.2].	
patientId	1. .1	1. .1	0. .0	1. .1	Systemweit eindeutige Kennung des Patienten	Der Wert MUSS den Inhalts- und Formatvorgaben aus A_14974* genügen.  Außerdem MUSS der Wert der Identität des Akteninhabers entsprechen und MUSS vom XDS Document Service dahingehend bei Registrierung der Metadaten geprüft werden.	
practiceSettingCode	1. .1	0. .0	0. .0	1. .1	Art der Fachrichtung der erstellenden Einrichtung, in der das dokumentierte Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSPracticeSettingCodeV S aus [IG_TI_Terminology] entsprechen. Die DiGA MUSS practiceSettingCode mit dem Wert "PAT" belegen.	X
referenceIdList	0. .n	0. .1	1. .1	0. .n	Liste von IDs, mit denen das Dokument assoziiert wird.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.28] genügen.  Wenn KTR-Clients einen Wert übertragen, muss es sich um die rootDocumentId im Rahmen einer RMU-Operation (Aktualisierung) oder dem Ersetzen (RPLC) eines Dokuments handeln.	
repositoryUniqueId	0. .1	0. .1	1. .1	0. .1	Kennung des Document Repository, in welches das Dokument eingestellt wird/wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.18] genügen.	
serviceStartTime	0. .1	0. .1	0. .0	0. .1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis begonnen wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.19] genügen.	X

serviceStopTime	0. .1	0. .1	0. .0	0. .1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis beendet wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.20] genügen.	X
size	0. .0	0. .0	1. .1	0. .0	Größe des Dokuments in Bytes	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.21] genügen.  Der XDS Document Service MUSS die Größe des Dokuments berechnen und in den Metadaten während des Registriervorgangs setzen (vgl. [IHE-ITI-TF2b#3.41.4.1.3]).	
sourcePatientId	0. .1	0. .0	0. .0	0. .0	Kennung des Patienten im Quellsystem	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.22] genügen.	
sourcePatientInfo	0. .n	0. .0	0. .0	0. .0	Demographische Daten zum Patienten im Quellsystem	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.23] genügen.	
title	1. .1	1. .1	1. .1	1. .1	Titel des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.24] genügen. Ein leeres Feld <code>DocumentEntry.title=""</code> bzw. ausschließlich mit nicht druckbaren Zeichen befüllt ist nicht erlaubt.	X
typeCode	1. .1	1. .1	0. .0	1. .1	Art des Dokuments	Der Wert MUSS einem Code des Value Sets EPAXDSTypeCodeVS aus [IG_TI_Terminology] entsprechen.  PS-KTR MUSS für Dokumente der Kategorie <code>health_risk_analysis</code> ausschließlich den Code "GRIS" verwenden  Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Inhalts-	X



						und Formatvorgaben aus Abschnitt <u>3.13.1.9-Strukturierte Dokumente</u> genügen.	
uniqueId	1. .1	1. .1	0. .0	1. .1	Eindeutige, aktenweite Kennung des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.26] genügen.	
URI	1. .1	1. .1	0. .0	1. .1	URI für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.27] genügen und mittels A_24524-* normalisiert werden. Die extension der DocumentEntry.URI MUSS wird dem mimetype gemäß A_23447-* angepasst, falls erforderlich.	
<b>Metadaten für SubmissionSet</b>							
author	1. .n	1. .1	0. .0	1. .1	Person oder System, welche(s) das Submission Set erstellt hat.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.1] genügen.	
authorPerson	0. .1	0. .1	0. .0	0. .1	Name der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus Abschnitt <u>3.13.1.8.2-Metadaten der Dokumente und SubmissionSets</u> genügen. ePA-FdV: Das ePA-Aktensystem MUSS die KVNR mit den Inhalten der User Session auf Übereinstimmung prüfen. Eine Gleichheit liegt vor, wenn die KVNR aus der XCN-Struktur des Autors nach den Vorgaben von A_14762-* mit dem entsprechenden Wert aus der User Session übereinstimmt. Ist authorPerson nicht gesetzt, MUSS das ePA Aktensystem das Metadatenattribut authorPerson für Versicherte entsprechend der Vorgaben aus A_14762-* unter	

						Verwendung der entsprechenden Informationen aus der User Session (KVNR, family_name und given_name) setzen. Das ePA Aktensystem KANN in einer übergebenen authorPerson den Nachnamen und Vornamen mit Informationen aus der User Session überschreiben. PS/DiGAs können hier im Bedarfsfall Einträge für Software-Komponente bzw. Gerät als Autor entsprechend A_14762-* vornehmen.	
authorInstitution	0. .1	0. .1	0. .0	0. .0	Institution, welcher die einstellende Person oder das einstellende System zugeordnet ist.	Der Wert MUSS den Formatvorgaben aus Abschnitt 3.13.1.8.2- <u>Metadaten der Dokumente und SubmissionSets</u> (A_21209*) genügen. Das ePA-Aktensystem MUSS die Identität von TelematikID-basierten Identitäten mit den Inhalten aus authorInstitution prüfen. Eine Gleichheit liegt vor, wenn Telematik-ID aus der XCN-Struktur des Autors nach den Vorgaben von A_14763-* bzw. A_21511-* mit dem entsprechenden Wert aus der User Session übereinstimmt. Ist authorInstitution nicht gesetzt, MUSS das ePA Aktensystem das Metadatenattribut authorInstitution entsprechend der Vorgaben aus A_14763-* bzw. A_21511-* unter Verwendung der entsprechenden Informationen aus der User Session (organizationName und idNummer) setzen.	

authorRole	1. .n	1. .n	0. .0	1. .1	Rolle der einstellenden Person oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS aus [IG_TI_Terminology] entsprechen. Das PS-KTR MUSS den Code "105" (Kostenträgervertreter) verwenden. Das ePA-Frontend des Versicherten MUSS den Code "102" (der Patient selbst) verwenden. Die DiGA MUSS authorRole mit dem Code "12" (dokumentierendes Gerät) verwenden.	
authorSpecialty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung der einstellenden Person oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorSpecialtyVS aus [IG_TI_Terminology] entsprechen.	
authorTelecommunication	0. .n	0. .0	0. .0	0. .n	Telekommunikationsdaten der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	
availabilityStatus	0. .0	0. .0	1. .1	0. .0	Status des Submission Sets ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise zum Submission Set in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.3] genügen.	X
contentTypeCode	0. .1	0. .1	0. .0	0. .1	Klinische Aktivität, die zum Einstellen des Submission Set geführt hat.	Der Wert MUSS einem Code des Value Sets EPAXDSContentCodeVS aus [IG_TI_Terminology] entsprechen.	
entryUUID	1. .1	1. .1	0. .1	1. .1	Intern verwendete, aktensystemweit eindeutige Kennung des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.5] genügen.  Der XDS Document Service MUSS symbolische IDs	

						gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
intendedRecipient	0. .n	0. .0	0. .0	0. .n	Vorgesehener Adressat des Submission Set	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.7] genügen.	
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierung, welche anzeigt, dass das Submission Set nicht den durch das IHE ITI TF vorgegebenen Satz an Metadaten enthält.		
patientId	1. .1	1. .1	0. .0	1. .1	Patienten-ID, zu der das Submission Set gehört	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
sourceId	0. .0	0. .0	0. .0	0. .0	Weltweit eindeutige, unveränderliche Kennung des einstellenden Systems		
submissionTime	1. .1	1. .1	0. .0	1. .1	Zeit, zu der das Submission Set zusammengestellt wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.10] genügen. Der XDS Document Service MUSS prüfen, ob der Wert der aktuellen Systemzeit entspricht. Sollte diese von der lokalen Zeit über mehr als eine Minute abweichen, MUSS der Wert mit der aktuellen Systemzeit ersetzt werden. Diese Systemzeit MUSS dabei synchron zur Systemzeit des Produkttyps Zeitdienst gemäß A_24673 sein.	
title	0. .1	0. .1	0. .0	0. .1	Titel des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.11] genügen.	X

uniqueId	1. .1	1. .1	0. .0	1. .1	Eindeutige Kennung des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.3.12] genügen.	
<b>Metadaten für dynamische Folder</b>							
availabilityStatus	1. .1	n/ a	0. .0	n/ a	Status des Ordners ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approv ed" entsprechen.	
codeList	1. .1	n/ a	0. .0	n/ a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI- TF3#4.2.3.4.2] und einem Code des Value Sets EPADataCategoryOtherVS aus [IG_TI_Terminology] entsprechen. Bei Folder.codeList=pregnancy_c hildbirth MUSS das Primärsystem diese Codes angeben.	
comments	0. .1	n/ a	0. .0	n/ a	Freitextkommentar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen.	
entryUUID	1. .1	n/ a	1. .1	n/ a	Intern verwendete, aktenweit eindeutige Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI- TF2b#3.42.4.1.3.7] auflösen.	
homeCommunity Id	siehe Vorgaben zu DocumentEntry.homeCommunityId						
lastUpdateTime	0. .0	n/ a	1. .1	n/ a	Zeitstempel, an dem der Ordner das letzte mal geändert wurde	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.6] genügen. Der XDS Document Service MUSS den Wert automatisch gemäß [IHE-ITI- TF2b#3.42.4.1.3.6] aktuell halten.  Zudem MUSS der XDS Document Service den Wert aktualisieren, wenn ein	

						Dokument aus dem Ordner gelöscht oder dessen Metadaten aktualisiert wurden.	
limitedMetadata	Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden.						
patientId	1. .1	n/ a	0. .0	n/ a	Patienten ID, zu der der Ordner gehört.	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
title	1. .1	n/ a	0. .0	n/ a	Titel des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.8] genügen.	
uniqueId	1. .1	n/ a	0. .0	n/ a	Eindeutige, aktenweite Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.9] genügen.	
<b>Metadaten für statische Folder</b>							
availabilityStatus	n/ a	n/ a	1. .1	n/ a	Status des Ordners ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
codeList	n/ a	n/ a	1. .1	n/ a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] und einem Code des Value Sets EPADataCategoryOtherVS und EPADataCategoryMedicalVS aus [IG_TI_Terminology] entsprechen. Der XDS Document Service MUSS codeList gemäß A_19388* setzen.	
comments	n/ a	n/ a	0. .1	n/ a	Freitextkommentar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen.	
entryUUID	n/ a	n/ a	1. .1	n/ a	Intern verwendete, aktenweit eindeutige Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen.  Der XDS Document Service	

						MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
lastUpdateTime	n/a	n/a	1. .1	n/a	Zeitstempel, an dem der Ordner das letzte mal geändert wurde	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.6] genügen.</p> <p>Der XDS Document Service MUSS den Wert automatisch gemäß [IHE-ITI-TF2b#3.42.4.1.3.6] aktuell halten. Zudem MUSS der XDS Document Service den Wert aktualisieren, wenn ein Dokument aus dem Ordner gelöscht oder dessen Metadaten aktualisiert wurden.</p>	
limitedMetadata	Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden.						
patientId	n/a	n/a	1. .1	n/a	Patienten ID, zu der der Ordner gehört.	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
title	n/a	n/a	1. .1	n/a	Titel des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.8] genügen. Der Wert MUSS redundant gefüllt werden mit Folder.Codelist.Code.displayName.	
uniqueId	n/a	n/a	1. .1	n/a	Eindeutige, aktenweite Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.9] genügen.	

**Tabelle 32: Tab\_LanguageCodes - Mindestanforderung an zu unterstützende Language Codes**

Language / Country Code Kombination	Language / Country Code Kombination
bg-BG(bulgarisch, Bulgarien)	it-IT(italienisch, Italien) it-CH (italienisch, Schweiz)
cs-CZ(tschechisch, Tschechien)	lt-LT(litauisch, Litauen)



da-DK(dänisch, Dänemark)	lb-LU(luxemburgisch, Luxemburg)
de-AT(deutsch, Österreich) de-DE (deutsch, Deutschland) de-CH (deutsch, Schweiz) de-LI (deutsch, Liechtenstein) de-LU (deutsch, Luxemburg)	lv-LV(lettisch, Lettland)
el-GR(griechisch, Griechenland)	mt-MT(maltesisch, Malta)
en-GB(englisch, Vereinigtes Königreich)	n1-NL(niederländisch, Niederlande) n1-BE (niederländisch, Belgien)
es-ES(spanisch, Spanien)	no-NO(norwegisch, Norwegen)
et-EE(estnisch, Estland)	pl-PL(polnisch, Polen)
fi-FI(finisch, Finnland)	pt-PT(portugiesisch, Portugal)
fr-FR(französisch, Frankreich) fr-CH (französisch, Schweiz) fr-LU (französisch, Luxemburg) fr-BE (französisch, Belgien)	rm-CH(rätoromanisch, Schweiz)
ga-IE(irisches, Irland)	ro-RO(rumänisch, Rumänien)
hr-HR(kroatisch, Kroatien)	sk-SK(slowakisch, Slowakei)
hu-HU(ungarisch, Ungarn)	sl-SI(slowenisch, Slowenien)
is-IS(isländisch, Island)	sv-SE(schwedisch, Schweden)

【<=】

### 3.13.1.8.2 Metadaten der Dokumente und SubmissionSets

#### **A\_23369-02 -XDS Document Service - Verpflichtender Dokumententitel in DocumentEntry.title**

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Metadaten an Dokumenten `DocumentEntry.title` befüllen. Der Titel des Dokumentes soll eine fachliche Beschreibung des Dokumentes enthalten. Bei `DocumentEntry.title` MÜSSEN führende und endende Leerzeichen entfernt werden. In `DocumentEntry.title` DARF NICHT leer sein (`!= ""`) (insbesondere auch nicht nach etwaigen Entfernen von Leerzeichen vorne und hinten). In `Document.title` DÜRFEN keine nicht-druckbaren Zeichen enthalten sein.【<=】

#### **A\_25188 -XDS Document Service - Input Sanitization**

Der XDS Document Service MUSS sicherstellen, dass bei Anlage und Aktualisierung (Ändern) von Metadaten:

1. führende (leading) und endende (trailing) Whitespace von den Attributen automatisch entfernt werden.

2. die notwendigen Attribute nichtleer sind (insbesondere auch noch Whitespace-Entfernung aus 1.) und
3. Die Attribute nur druckbare Zeichen enthalten.

[<=]

#### **A\_14762-05 -XDS Document Service - Nutzungsvorgabe für authorPerson als Teil von DocumentEntry.author und SubmissionSet.author**

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an authorPerson unterhalb von DocumentEntry.author und SubmissionSet.author neben [IHE-ITI-TF3#4.2.3.1.4.2] auch die folgenden Vorgaben beachten.

#### **Bei Leistungserbringer als Autor:**

1. Lebenslange Identifikationsnummer eines Arztes (Lebenslange Arztnummer - LANR 9 Stellen) oder im Falle eines Zahnarztes die Zentrale Zahnarzt Nummer (ZANR)- sofern die ZANR bekannt ist
2. "^"
3. Nachname
4. "^"
5. Vorname
6. "^"
7. Weiterer Vorname
8. "^"
9. Namenszusatz
10. "^"
11. Titel
12. "^^^&" - sofern LANR oder ZANR angegeben, ansonsten "^^^"
13. "1.2.276.0.76.4.16" - sofern LANR angegeben oder "1.2.276.0.76.4.296", falls ZANR angegeben
14. "&ISO" - sofern LANR oder ZANR angegeben

Beispiele:

165746304^Weber^Thilo^^^Dr.^^^&1.2.276.0.76.4.16&ISO  
^Zahnschmerz^Eberhard^^^Dr.^^^

#### **Bei Versichertem als Autor:**

1. Der unveränderbare Teil der KVNR (10 Stellen)
2. "^"
3. Nachname
4. "^"
5. Vorname
6. "^"
7. Weiterer Vorname
8. "^"

9. Namenszusatz

10. "^"

11. Titel

12. "^^^&"

13. "1.2.276.0.76.4.8"

14. "&ISO"

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

Sowohl beim LE als auch beim Versicherten müssen Vorname und Nachname belegt werden.

### Software-Komponente bzw. Gerät als Autor

Beim (automatisierten) Einstellen von Dokumenten MUSS der max. 256-Zeichen lange Name der Software-Komponente bzw. des Geräts als Nachname und ggf. als Vorname(n) eingetragen werden.

Beispiel: ^PHR-Gerät-XY^PHR-Software-XY

Im Falle einer DiGA MUSS das Feld Autor folgendermaßen aufgebaut sein:

1. Telematik-ID der DiGA
2. "^"
3. Name der DiGA (Name der Verordnungseinheit)
4. "^"
5. Name des DiGA-Herstellers
6. "^"
7. optionale Ergänzung der Bezeichnung der SW
8. "^"
9. optionale Ergänzung der Bezeichnung der SW
10. "^"
11. optionale Ergänzung der Bezeichnung der SW
12. "^^^&"
13. <OID für DiGAs, wie in professionOID>
14. "&ISO"

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

### A\_14763-03 -XDS Document Service - Nutzungsvorgabe für SubmissionSet.authorInstitution

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an SubmissionSet.authorInstitution neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

1. Name der Leistungserbringereinstitution oder Name des Kostenträgers
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)

4. "&ISO^^^^"

5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

Beispiele:

- Arztpraxis Dr. Thilo Weber^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-e518
- gematik Betriebskrankenkasse^^^^&1.2.276.0.76.4.188&ISO^^^^8-34923902a

[<=]

#### **A\_21511-01 -Nutzungsvorgabe SubmissionSet.authorInstitution für DiGAs**

Der XDS Document Service MUSS sicherstellen, dass DiGAs beim Upload von Dokumenten, die folgenden Nutzungsvorgaben für das Metadatenattribut DocumentEntry.authorInstitution sowie SubmissionSet.authorInstitution berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.1.4.1] genügen und ist inhaltlich nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen.

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

[<=]

#### **A\_21209-02 -XDS Document Service - Nutzungsvorgabe für DocumentEntry.authorInstitution**

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an DocumentEntry.authorInstitution neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

Die Komponenten 2.-5. sind nur anzugeben, wenn die Telematik ID (5.) der Autoreninstitution bekannt ist oder ad-hoc ermittelt werden kann, bspw. über den Verzeichnisdienst der TI-Plattform (VZD). Ansonsten wird ausschließlich der Name gesetzt.

Beispiele:

- Arztpraxis Dr. Thilo Weber^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-e518
- gematik Betriebskrankenkasse^^^^&1.2.276.0.76.4.188&ISO^^^^8-34923902a
- Arztpraxis Dr. Wiebke Werner

[<=]

#### **A\_22408-02 -XDS Document Service - DocumentEntry.authorInstitution ohne Telematik-ID**

Der XDS Document Service MUSS Nachrichten zum Registrieren von Dokumenten bei fehlender Telematik-ID in `DocumentEntry.authorInstitution` akzeptieren und daraufhin alle Zeichen hinter dem Namen der `authorInstitution` abschneiden und verwerfen. [≤]

#### **A\_14974-02 -XDS Document Service - Nutzungsvorgabe für `DocumentEntry.patientId` und `SubmissionSet.patientId`**

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten die folgenden Nutzungsvorgaben für `DocumentEntry.patientId` und `SubmissionSet.patientId` berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.2.16] bzw. [IHE-ITI-TF3#4.2.3.3.8] genügen und ist inhaltlich nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen:

1. Der unveränderbare Teil der KVNR des Akteninhabers (10 Stellen)
2. "^^^&"
3. "1.2.276.0.76.4.8" (OID zur Kennzeichnung einer unveränderbaren KVNR)
4. "&ISO"

Beispiel: G995030566^^^&1.2.276.0.76.4.8&ISO [≤]

#### **A\_27759 -XDS Document Service - Verarbeitung von Code System Version**

Der XDS Document Service MUSS Metadaten vom Typ Coded Attribute im Slot "codingScheme" bei Angabe einer System URL oder Canonical URL eine per Pipe-Symbol (|) angehängte Version akzeptieren und für eine Terminologievalidierung verwenden. [≤]

Beispiel: <http://dvmd.de/fhir/CodeSystem/kdl|2025>

### *3.13.1.8.3 Metadaten für Datenkategorien*

#### **A\_19388-21 -Nutzungsvorgaben für die Verwendung von Datenkategorien**

Der XDS Document Service MUSS beim Einstellen eines Dokuments und beim Ändern von Metadaten die folgende Zuordnung zu einer Datenkategorie (d. h. Assoziierung mit einem bestimmten Folder) vornehmen. Dabei haben Auswertungs- und Zuordnungsregeln, die sich aus A\_14761-\* und damit verbunden aus [gemSpec\_IG\_ePA] ableiten, immer den Vorrang gegenüber anderen Auswertungsregeln. Ferner MUSS der XDS Document Service sicherstellen, dass bei einer Aktualisierung eines Dokuments derselbe Ordner des zu ersetzenden Dokuments zugeordnet wird.

Für eine eindeutige Zuordnung zu einer Datenkategorie MUSS die Auswertung der Metadatenvorgaben in der Reihenfolge der folgend dargestellten Einsortierungskriterien erfolgen:

**Tabelle 33: Einsortierung\_Datenkategorien**

Datenkategorie/Technischer Identifier/Foldercode	Einsortierkriterium (anzuwenden auf <code>DocumentEntry</code> , wenn nicht anders angegeben. Oder-Verknüpfungen, wenn nicht "und" angegeben)
receipt	healthcareFacilityTypeCode = VER und typeCode = ABRE und <code>DocumentEntry.authorRole</code> =105 und <code>SubmissionSet.authorRole</code> = 105
health_risk_analysis	healthcareFacilityTypeCode = VER und typeCode = GRIS und <code>DocumentEntry.authorRole</code> =105 und

	Submissionset.authorRole = 105
patient	Dokumente bei denen der Einsteller der Versicherte oder sein Vertreter ist: Submissionset.authorRole = 102 Dokumente bei denen der Einsteller der Kostenträger ist: Submissionset.authorRole = 105
pregnancy_childbirth	healthcareFacilityTypeCode = HEB eventCodeList=SD070104 (KDL-Code Neugeborenenenscreening)
eab	classCode = BRI
care	PracticeSettingCode = PFL*
rehab	practiceSettingCode = REHA
dental	practiceSettingCode = MZKH*
emergency	eventCodeList = <ul style="list-style-type: none"> <li>• ED110102 (KDL-Code Notfalldatenmanagement (NFDMM))</li> <li>• AU190104 (KDL-Code Notfalldatensatz)</li> <li>• AD020105 (KDL-Code Notfall-/Vertretungsschein)</li> </ul>
transcripts	eventCodeList = <ul style="list-style-type: none"> <li>• UB999997 (KDL-Code Gesamtdokumentation stationäre Versorgung) oder</li> <li>• UB999998 (KDL-Code Gesamtdokumentation ambulante Versorgung)</li> </ul>
reports	classCode = ANF, ASM, BEF, BIL, DOK, DUR, LAB oder PLA
other	Alle Dokumente, die in keine andere Kategorien eingeordnet werden können

\*Falls Basiskonzepte angegeben werden, dann gelten automatisch alle Subkonzepte, z.B. gilt für die Kategorie "care" die Einsortierregel bei PracticeSettingCode = PFL wie auch für die Sub-Konzepte ALT (Altenpflege) und KIN (Kinderpflege).【<=】

#### 3.13.1.8.4 Automatisches Umschreiben von Daten

Dieser Abschnitt enthält Vorgaben für Datenanpassungen, die für bestehende Daten im XDS Document Service vorgenommen werden müssen (z. B. wenn sie durch Änderungen im Rahmen einer neuen Version des XDS Document Service notwendig werden).

### **A\_27482-01 -XDS Document Service - Metadatenkorrektur bei vorhandenen elektronischen Arztbriefen**

Der XDS Document Service MUSS die Metadaten (DocumentEntry) von bestehenden Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief) gemäß [gemSpec\_IG\_ePA] derartig anpassen, dass DocumentEntry.eventCodeList zusätzlich um den KDL-Code (code: ED110104, codeSystem: 1.2.276.0.76.5.552, displayName: eArztbrief) erweitert wird, wenn dieser nicht bereits vorhanden ist. [≤=]

#### **A\_27661 -XDS Document Service - Umwandeln von APND-Assoziationen**

Der XDS Document Service MUSS sobald möglich Associations vom Typ "urn:ihe:iti:2007:AssociationType:APND" wie folgt ersetzen:

1. Wenn ein Association.sourceObject oder Association.targetObject auf ein DocumentEntry im Status "deprecated" zeigt, oder auf einen DocumentEntry, der zu einer Sammlung (mixed oder uniform) gehört, wird nur Schritt 4 durchgeführt (Association wird gelöscht), ansonsten weiter bei Schritt 2.
2. Der DocumentEntry, auf den Association.sourceObject zeigt (der "Anhang"), MUSS in DocumentEntry.referenceIdList mit dem mittelsurn:gematik:iti:xds:2025:parentDocument ausgezeichneten Wert der DocumentEntry.uniqueId desjenigen Dokuments ergänzt werden, auf das Association.targetObject zeigt.
3. Der DocumentEntry, auf den Association.targetObject zeigt (der "Hauptdokument"), MUSS in DocumentEntry.referenceIdList mit dem mittelsurn:gematik:iti:xds:2025:childDocument ausgezeichneten Wert der DocumentEntry.uniqueId desjenigen Dokuments ergänzt werden, auf das Association.sourceObject zeigt.
4. Anschließend ist die APND-Association zu löschen.

[≤=]

APND-Associations werden mit ePA Version 3.1.2 durch einen Anhangsmechanismus mittels DocumentEntry.referenceIdList abgelöst. Beim automatischen Umschreiben der APND-Associations auf die DocumentEntry.referenceIdList können Anhangsketten entstehen, die länger als insgesamt fünf Dokumente sind. Das ist über das Einstellen von Dokumenten über Provide and Register Document Set [ITI-41] oder Restricted Update Document Set [ITI-92] nicht möglich. Entsprechend lange Ketten können also nur aus der Anpassung von Altdaten entstehen.

Wie aus A\_27661 hervorgeht, werden Anhänge von "deprecated"-Dokumenten (d.h. durch Ersetzen via RPLC-Association durch neue Versionen ersetzte Dokumente) abgetrennt. Das ist notwendig, da die identischen Metadateneinträge der Dokumente in der RPLC-Dokumentenketten bei jedem Dokument zwangsläufig auf identische Anhänge zeigen müssen. Das kleinere Übel ist hier, die Anhänge für die aktuellste Version zumindest intakt zu halten. Neue Ersetzungen in Verbindung mit Anhängen verhindert das Aktensystem ab Version 3.1.2, da die Menge an RPLC-fähigen Dokumenten und die Dokumente, die Anhangsbeziehungen eingehen können, disjunkt spezifiziert sind.

#### **3.13.1.9 Strukturierte Dokumente**

Die elektronische Patientenakte unterstützt unterschiedliche sogenannte "strukturierte Dokumente", deren Aufbau über Implementation Guides genau vorgegeben ist. Der Umfang der unterstützten strukturierten Dokumente wird durch den Umfang der veröffentlichten Implementation Guides festgelegt (3.13.1.9.2- Konfigurierbarkeit). Für alle strukturierten Dokumente gelten spezifische Metadatenvorgaben, um sie eindeutig zu identifizieren und gezielt verarbeiten zu können.

#### **A\_14761-08 -Nutzungsvorgaben für die Verwendung von IHE ITI XDS-Metadaten bei strukturierten Dokumenten**

Der XDS Document Service MUSS die Nutzungsvorgaben für strukturierte Dokumente unter [gemSpec\_IG\_ePA] berücksichtigen. Dabei ist das Format des Dokuments, welches



über einen Code des Metadatenattributs `formatCode` ausgedrückt wird, führend. Das bedeutet, bei Registrierung eines strukturierten Dokuments mit einem `formatCode` MÜSSEN die weiteren Metadatenattribute `classCode`, `typeCode`, `mimeType` sowie `eventCodeList` entsprechend belegt werden. Der XDS Document Service MUSS eine solche Registrierung diesbzgl. prüfen und im Fehlerfall analog zu A\_14938-\* antworten. [`<=`]

#### 3.13.1.9.1 Sammlungstypen

Je nach Art ihrer Zusammensetzung und ihrer Handhabung existieren unterschiedliche Typen strukturierter Dokumente, sogenannte medizinische Informationsobjekte. Ein medizinisches Informationsobjekt (MIO) ist eine **Sammlung** von Informationen zu medizinischen, strukturellen oder administrativen Sachverhalten, die in sich geschlossen oder entsprechend verschachtelt vorliegt. Zudem ist ein MIO eine klar definierte Vorgabe, wie diese Informationssammlung in der elektronischen Patientenakte gespeichert wird, damit semantische und syntaktische Interoperabilität gewährleistet werden. Die Festlegung dieser Vorgaben ist gemäß SGB V Aufgabe der KBV. Beispiele für medizinische Informationsobjekte sind der Impfpass, das Kinderuntersuchungsheft, der Mutterpass, das zahnärztliche Bonusheft, oder DiGA. MIOs werden über Sammlungen und Sammlungstypen umgesetzt.

Einige strukturierte Dokumente sind für sich genommen vollständig und schlüssig wie z. B. ein Elektronischer Arztbrief. Sie sind ohne Zuhilfenahme weiterer Dokumente in der ePA für einen Benutzer sinnvoll zu verwenden. Andere Typen strukturierter Dokumente müssen hingegen fast immer in Kombination betrachtet werden, z. B. Impfpassdokumente. Bei letzteren spiegelt jedes Impfpassdokument ein oder mehrere Impfungen wieder. Ein Impfpass, wie er in der analogen Welt geläufig und als logisches Konstrukt sinnvoll ist, besteht immer aus der gemeinsamen Betrachtung aller Impfpassdokumente und somit aller vorhandenen Impfeinträge. Die Kombination ein oder mehrerer strukturierter Dokumente ergeben eine Sammlung.

Eine Sammlungsinstanz (z. B. der Mutterpass der ersten Schwangerschaft der Patientin Martha Mustermann) ist eine konkrete Ausprägung der Information, die zwischen den beteiligten Akteuren ausgetauscht wird. Nicht jede Sammlung besteht zwangsläufig aus Dokumenten desselben Formats: Ein Kinderuntersuchungsheft beispielsweise besteht aus Dokumenten mit drei verschiedenen strukturierten Dokumenttypen. Zentral für alle Sammlungstypen ist immer mindestens ein strukturiertes Dokument mit einem festgelegten Dokumentenformat. Für eine technische Umsetzung sind die Sammlungstypen "mixed" und "uniform" zu unterscheiden, die technisch unterschiedlich umgesetzt werden und zum Teil unterschiedliche Operationen erlauben.

Der Sammlungstyp "mixed" fasst semantisch zusammengehörige, strukturierte Dokumente unterschiedlicher Struktur mittels Ordner zu einer Sammlung zusammen. Der Sammlungstyp "uniform" wird ebenfalls intern über Ordner abgebildet. Dies stellt sicher, dass zukünftige Versionen dieser strukturierten Dokumente/Pässe oder DiGA verlässlich verarbeitet werden können. Ordner gelten als "statische Ordner", bis auf Sammlungen der Kategorie Mutterpass und DiGA ("dynamische Ordner"). Der dynamische Ordner für einen konkreten Mutterpass wird durch den Client angelegt, weil es aus Gründen, die nur der Client kennt (Anzahl der Schwangerschaften), mehrere Ordner dieses Typs geben kann ("nicht-statische Ordner", vgl. A\_21610-\*). Die Version der Struktur eines Dokuments ist am Format Code erkennbar.

#### **A\_20577-06 -Definition und Zuweisung von Sammlungstypen**

Der XDS Document Service MUSS jeder Sammlung einen von zwei Sammlungstypen zuweisen:

**Tabelle 34: TAB\_EPA\_Sammlungstypen**

Sammlungstyp	Definition
mixed	Ordner, die einer Sammlung des Typs "mixed" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) mit einem für die Sammlung festgelegten Code in der Folder.codeList abgelegt werden.
uniform	Ordner, die einer Sammlung des Typs "uniform" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) abgelegt werden.

Es gelten die Metadaten für strukturierte Dokumente gemäß [gemSpec\_IG\_ePA]. In den unter [gemSpec\_IG\_ePA] gemachten Vorgaben werden auch Ordner-Kardinalitäten für spezifische Sammlungen festgelegt. Diese Angaben sagen aus, wie viele Instanzen einer Sammlung (d. h. minimal und maximal) registriert werden können. [**<=**]

#### **A\_20707-04 -XDS Document Service - Keine unpassenden Dokumente in nicht-statische Ordner**

Falls das Dokument nicht den Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec\_IG\_ePA] entspricht, MUSS der XDS Document Service das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-FehlercodeBadFolderAssociation quittieren. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die UUID (DocumentEntry.entryUUID) des identifizierten Dokuments angegeben werden. [**<=**]

#### **A\_20581-06 -XDS Document Service - Löschen von Dokumenten aus Sammlungen der Typen "mixed" und "uniform" durch ein ePA-FdV**

Der XDS Document Service MUSS beim Löschen eines Dokuments der Sammlungstypen "mixed" und "uniform" durch das ePA-FdV sicherstellen, dass die Operation mit dem Fehler ReferencesExistException abgebrochen wird, wenn die Löschanfrage nicht alle Dokumente der Sammlung enthält. Es besteht folgende Ausnahme: Das Löschen einer Elternnotiz im Kinderuntersuchungsheft ist erlaubt. [**<=**]

Nur Leistungserbringern ist es erlaubt, einzelne Dokumente aus Sammlungen der Typen "mixed" und "uniform" zu löschen, um die medizinische Interpretation der gesamten Sammlungsinstanz nicht zu gefährden.

*Hinweis: Die zeitliche Gültigkeit ergibt sich aus den Attributen "validFrom" und (optional) "clientReadOnlyFromDate" der Vorgaben in [gemSpec\_IG\_ePA].*

### **3.13.1.9.2 Konfigurierbarkeit**

#### **A\_17546-02 -Konfigurierbarkeit von strukturierten Dokumenten**

Der XDS Document Service MUSS die Liste strukturierter Dokumente konfigurierbar machen, indem dieser die Unterstützung strukturierter Dokumente unter Angabe folgender Eigenschaften ermöglicht:

- Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec\_IG\_ePA] konfigurativ hinzufügen bzw. entfernen,
- Sammlungen zu TAB\_EPA\_Sammlungstypen gemäß [gemSpec\_IG\_ePA] konfigurativ hinzufügen bzw. entfernen.

[**<=**]

Das Entfernen der Unterstützung von strukturierten Dokumenten oder Sammlungen bedeutet, dass diese zu einem früheren Zeitpunkt in das Aktensystem geschrieben werden konnten, aber durch Erreichen von "clientReadOnlyFromDate" nicht mehr geschrieben werden dürfen. Das Schreiben umfasst das Aktualisieren oder neu Anlegen. Das Lesen ist weiterhin erlaubt.

#### **A\_17551-01 -Prüfanforderungen zur Konfigurierbarkeit von Value Sets**

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die zu konfigurierenden Value Sets des XDS Document Service gemäß der Anforderung A\_17546-\* den folgenden Prüfkriterien unterliegen, bevor bestehende, im XDS Document Service verarbeitete Value Sets verändert werden:

- Es DÜRFEN KEINE Codes der Value Sets gelöscht werden, lediglich das Hinzufügen von Codes zu existierenden Value Sets ist aus Kompatibilitätsgründen erlaubt.
- Neue Codes MÜSSEN den Formatvorgaben gemäß Tabelle 4.2.3.1.7-2 in [IHE-ITI-TF3#4.2.3.1.7] entsprechen und gegenüber einer internen Referenzliste validiert werden. Dies schließt auch Prüfungen zur Zeichenkodierung, der Datentypen als auch zu den Längenbeschränkungen ein.

[<=]

#### **A\_21212-01 -Restriktionen zur Konfigurierbarkeit von Metadaten für strukturierte Dokumente und Sammlungen**

Der XDS Document Service MUSS durch technische Maßnahmen sicherstellen, dass Änderungen an den in den Implementierungsvorgaben in [gemSpec\_IG\_ePA] spezifizierten Codes ausgeschlossen sind.[<=]

#### **A\_21214-03 -Konfiguration strukturierter Dokumente im Rahmen der Veröffentlichung durch die gematik**

Der Anbieter des ePA-Aktensystems MUSS durch organisatorische Maßnahmen sicherstellen, dass die Konfiguration im Aktensystem zur Unterstützung strukturierter Dokumente aus [gemSpec\_IG\_ePA] ausschließlich im Rahmen der Veröffentlichung der Implementation Guides durch die gematik erfolgt.[<=]

Bei Einführung neuer strukturierter Dokumente werden die beschriebenen Konfigurationsmöglichkeiten so verwendet, dass eine Erweiterung der Spezifikation und daraus resultierend eine Änderung des ePA-Aktensystems mit erneuter Zulassung nicht erforderlich sind.

#### *3.13.1.9.3 Verarbeitungsvorgaben für spezifische Dokumente*

#### **A\_27686 -Einstellen des eArztbriefs mit Dokumentenanhängen**

Der XDS Document Service MUSS beim Einstellen eines eArztbriefs (gemäßig-eab.json in [gemSpec\_IG\_ePA]) sicherstellen,

- dass alle zusätzlich in der Anfrage enthaltenen Dokumente mit dem enthaltenen eArztbrief-Dokument über die Kennzeichnung als Anhang verbunden werden (urn:gematik:iti:xds:2025:childDocument/parentDocument),
- dass kein Dokument (via urn:gematik:iti:xds:2025:parentDocument ) auf ein Elterndokument referenziert, dass nicht der eArztbrief selbst ist.

und ansonsten die Verarbeitung mit dem Fehler XDSInvalidAttachmentHierarchyabbrechen.

[<=]

Unter anderem müssen also die Anhänge immer direkt unter den Arztbrief "gehängt" werden; ein "Anhang am Anhang" ist nicht erlaubt.

#### **A\_27765 -Nachträgliches Anhängen an einen eArztbrief**

Der XDS Document Service MUSS ein Anhängen von Dokumenten an einen eArztbrief (gemäßig-eab.json in [gemSpec\_IG\_ePA]) mit dem Fehler XDSAttachmentForbidden ablehnen, wenn die Anhangsbeziehung nicht mit demselben SubmissionSet hergestellt wird, mit dem der eArztbrief eingestellt wird.

[<=]

Hierdurch wird ein nachträgliches Anhängen von Dokumenten an einen bestehenden Arztbrief über die Operationen Provide and Register Document Set-b oder Restricted Update Document Set unterbunden.

#### **A\_27758 -XDS Document Service - Metadatenerweiterung bei neuen elektronischen Arztbriefen**

Der XDS Document Service MUSS die Metadaten (DocumentEntry) von neuen Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief) gemäß [gemSpec\_IG\_ePA] derartig anpassen, dass DocumentEntry.eventCodeList zusätzlich um den aktuellen KDL-Code nach [IG\_TI\_Terminology] mit den Werten

- code: ED110104,
- codeSystem: [http://dvmd.de/fhir/CodeSystem/kdl/\[version\]](http://dvmd.de/fhir/CodeSystem/kdl/[version]) (präferiert) oder die entsprechende OID,
- displayName: eArztbrief

erweitert wird, wenn dieser nicht bereits vorhanden ist.

[<=]

Dabei muss bei obiger Anforderung "[version]" mit der aktuellen Version der KDL belegt werden, z.B.:

#### **Canonical URL für Version 2025**

<http://dvmd.de/fhir/CodeSystem/kdl|2025>

#### **OID für Version 2025**

1.2.276.0.76.5.553

### **3.13.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode**

Der Versicherte oder ein Vertreter kann vorhandene Dokumente des Aktenkontos durch die Verwendung der General Deny Policy des Constraint Managements verbergen oder sichtbar machen.

Der Versicherte oder ein Vertreter kann ein neues Dokument auch direkt beim Einstellen in das Aktenkonto verbergen. Dazu wird durch den XDS Document Service beim Einstellen bzw. Aktualisieren (Replace) eines Dokuments der DocumentEntry.confidentialityCode der Dokumentmetadaten ausgewertet. Enthält der confidentialityCode beim Einstellen bzw. Aktualisieren den Wert "CON" (constraint), wird durch das Aktensystem ein Eintrag in der General Deny Policy erzeugt und das Dokument verborgen.

Diese zusätzliche Art des direkten Verbergens ist dabei grundsätzlich nur auf Dokumententypen anwendbar, welche durch einen Versicherten oder einen Vertreter über ein ePA-FdV eingestellt werden können (keine MIOs oder strukturierten Dokumente).

Das Metadatum DocumentEntry.confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491:

1. Führt beim Einstellen und Replace eines Dokuments zum Verbergen des Dokuments, d.h. das Dokument wird auf die General Deny Policy des Aktenkontos gesetzt.

2. Wird im Aktensystem nicht persistiert sondern über dort intern über eine General Deny Policy umgesetzt.
3. Wird im ePA-FdV nicht zur Anzeige gebracht und kann dort auch nicht geändert werden.
4. Eine LEI darf DocumentEntry.confidentialityCode = "CON" nicht verwenden.

### 3.13.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die Dokumente des Aktenkontos

Wird ein Widerspruch gegen die Nutzung einer Funktion der ePA erklärt, verhindert der XDS Document Service, abhängig von der jeweils widersprochenen Funktion, deren weitere Nutzung.

Im Falle eines Widerspruchs gilt:

**Tabelle 35: Auswirkungen bei Widerspruch gegen eine Funktion der ePA**

widerspruchsfähige Funktion	Auswirkung bei erteiltem Widerspruch
Teilnahme am digital gestützten Medikationsprozess ("medication")	Das Einstellen, Verändern, Lesen oder Suchen von Dokumenten des Ordners "emp" (elektronischer Medikationsplan) wird durch den XDS Document Service abgelehnt. Ausgenommen hiervon sind der Versicherte und befugte Vertreter.
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst ("erp-submission")	Alle vorhandenen Dokumente des Ordners "emp" (elektronischer Medikationsplan) werden gelöscht.

*Hinweis zum Medikationsprozess: Dadurch wird verhindert, dass Leistungserbringer im Versorgungsprozess veraltete oder unvollständige Daten verwenden.*

#### A\_23860 -XDS Document Service - Löschen der Dokumente des Medikationsprozesses

Der XDS Document Service des Aktensystems MUSS alle Dokumente aus dem Ordner elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") löschen, wenn der Status der widerspruchsfähigen Funktion "Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst" (Id == "erp-submission") auf "Widerspruch erklärt" ("deny") geändert wird. [≤]

#### A\_23895-02 -XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch

Falls ein Widerspruch zur widerspruchsfähigen Funktion "Teilnahme am Medikationsprozess" (Id = "medication" und status = "deny") vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für alle Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid\_versicherter), ablehnen und die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.

[≤]

#### A\_25151-01 -XDS Document Service - Prüfung der Widersprüche bei Suchanfrage

Der XDS Document Service MUSS bei einer Suchanfrage die Suchergebnismenge für alle Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid\_versicherter), filtern und sicherstellen, dass diese keinerlei XDS-Metadaten von Dokumenten des Ordners

elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält, wenn ein Widerspruch gegen die widerspruchsfähige Funktion "Teilnahme am digital gestützten Medikationsprozess" (Id = "medication" und status = "deny") vorliegt.

[<=]

### 3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI auf die Dokumente des Aktenkontos

Wird ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI erklärt, verhindert der XDS Document Service, dass auf die Dokumente der Kategorie "emp" zugegriffen werden kann.

#### A\_26429 -XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für diese LEI, ablehnen und die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.

[<=]

#### A\_26430 -XDS Document Service - Prüfung des Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI bei Suchanfrage

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service bei einer Suchanfrage die Suchergebnismenge für diese LEI filtern und sicherstellen, dass die Suchergebnismenge keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält.

[<=]

### 3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service

#### A\_24715-02 -XDS Document Service - Protokolleinträge für Zugriffe auf den XDS Document Service

Der XDS Document Service MUSS für die Operationen

- ProvideAndRegisterDocumentSet-b,
- RetrieveDocumentSet,
- RemoveMetadata,
- RestrictedUpdateDocumentSet,
- RegistryStoredQuery (entfällt, wenn Nutzung durch den Versicherten erfolgt)

Protokolleinträge gemäß A\_24704\* erzeugen und dabei folgende Wertebelegung berücksichtigen:

**Tabelle 36: XDS Document Service Protokollierung**

Strukturelement	Wert	Erläuterung
AuditEvent.type	"document"	



AuditEvent.action	C	Für ProvideAndRegisterDocumentSet-b ohne Replace Option
	U	Für ProvideAndRegisterDocumentSet-b mit Replace Option
	U	Für RestrictedUpdateDocumentSet
	R	Für RegistryStoredQuery
	R	Für RetrieveDocumentSet
	D	Für Zugriffe mit RemoveMetadata
AuditEvent.entity.name	"XDS Document Service"	Service Name
AuditEvent.entity.description	<Operation>	ein Wert aus {ProvideAndRegisterDocumentSet-b, RetrieveDocumentSet, RemoveMetadata, RestrictedUpdateDocumentSet, RegistryStoredQuery}

**Parameterwerte für die Operationen ProvideAndRegisterDocumentSet-b, RetrieveDocumentSet und RemoveMetadata**

AuditEvent.entity.detail	type	value[x]	
	"DocumentFormatCode"	<DocumentEntry.formatCode>	wenn in der entity Struktur ein XSDDocument beschrieben wird. kodiert als Datentyp „Coded String“ gemäß [IHE-ITI- TF3]. Wenn es sich beim Wert von DocumentEntry.formatCode um den Code urn:ihe:iti:xds:2017:mimeTypeSufficient (Code System 1.3.6.1.4.1.19376.1.2.3) handelt, MUSS stattdessen der Wert von DocumentEntry.mimeType hier eingetragen werden.
	"DocumentUniqueid"	<Document.uniqueid>	wenn in der entity Struktur ein XSDDocument beschrieben wird
	"DocumentEntryTitle"	<DocumentEntry.title>	wenn in der entity Struktur ein XSDDocument beschrieben wird
	"FolderTitle"	<Folder.title>	wenn in der entity Struktur ein XDSFolder beschrieben wird
	"FolderCodeList"	<Folder.codeList>	wenn in der entity Struktur ein XDSFolder beschrieben wird kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3] z.B. "pregnancy_childbirth^^^&1.2.276.0



			.76.5.512&ISO"
	"FolderEntryUID"	<Folder.entryUUID>	wenn in der entity Struktur ein XDSFolder beschrieben wird
<b>Parameterwerte für die Operation RegistryStoredQuery der Schnittstellen I_Document_Management und I_Document_Management_Insurant (nur Vertreter)</b>			
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"QueryId"	<Parameter Query ID>	Der Wert MUSS der Parameter Query ID gemäß [IHE-ITI-TF2]#3.18.4.1.2.4 und für das Aktensystem definierten Anfragetypen entsprechen.
<b>Parameterwerte für die Operation RestrictedUpdateDocumentSet</b>			
<p>Alle Metadaten, die <b>geändert</b> wurden, sind mit altem und neuem Wert mit den Parameternamen AuditEvent.entity.detail.<b>type</b> und <b>.value[x]</b> zu protokollieren. In A_15083* sind die Metadaten genannt, die geändert werden können. Der Parameter type ist ein Kompositum aus Objekt (Document) + Attribut in Groß/Kleinschreibung. Wird das geänderte Metadatum adressiert, wird noch der Präfix "prev" ergänzt.</p> <p>z.B. Metadatum: DocumentEntry.formatCode -&gt;Parameter value<b>type</b>: DocumentFormatCode und prevDocumentFormatCode.</p> <p>Attributunterstrukturen werden ebenfalls in gemischter Groß/Kleinschreibung zusammengesetzt(z.B. author.Person -&gt; AuthorPerson).</p>			

**[<=]**

*Hinweis: In der AuditEvent.entity Struktur sind Dokumente und/oder Folder zu berücksichtigen, die in der zu protokollierenden Operation referenziert werden.*

#### **A\_24925 -XDS Document Service - Protokolleinträge für Zugriffe gleicher Art**

Werden mehrere XDS Dokumente bzw Folder in der zu protokollierenden Operation referenziert und die Zugriffe sind gleicher Art (AuditEvent.action) KANN der XDS Document Service einen Protokolleintrag erzeugen, der mehreren AuditEvent.entity Strukturen enthält.**[<=]**

Das bedeutet, wenn in einer ProvideAndRegisterDocumentSet-b Operation zehn Dokumente eingestellt werden, kann für diesen Zugriff ein AuditEvent mit zehn Entity Strukturen erzeugt werden. Werden zehn Dokumente eingestellt und das zehnte Dokument ersetzt ein bereits vorhandenes, kann in einem Protokolleintrag das Einstellen (Create) mit neun Entity Strukturen dokumentiert und muss in einem weiteren Protokolleintrag ein Ersetzen (Update) (zehnte Dokument) protokolliert werden.

#### **A\_25007 -XDS Document Service - Nicht zu protokollierende Zugriffe**

Werden mit der Operation RestrictedUpdateDocumentSet keine geänderten Metadaten eines referenzierten DocumentEntry gesendet, d.h. die gesendeten Metadateninhalte unterscheiden sich nicht von bereits persistierten Werten, DARF der XDS Document Service diesen Zugriff NICHT protokollieren.**[<=]**

#### **A\_27253-01 -XDS Document Service - Nicht zu protokollierende Zugriffe auf Ordner "technical"**

Der XDS Document Service DARF Zugriffe auf den statischen Ordner "technical" oder dessen Inhalte NICHT protokollieren.**[<=]**

**A\_27254-01 -XDS Document Service - Protokollierung von Nutzerzugriffen auf den Ordner "technical"**

Der XDS Document Service MUSS Nutzerzugriffe auf den Ordner "technical" dann protokollieren, wenn durch den Zugriff Dokumente Protokolldokumente einer ePA-2.6 Aktenkontomigration betroffen sind. Diese Protokollierung MUSS gemäß der Vorgaben in A\_24715-\* erfolgen.[<=]

**3.13.1.14 Unterstützungsleistung für das ePA-FdV**

Der XDS Document Service akzeptiert aus Sicherheitsgründen nur bestimmte Dokumentenformate. Das schränkt auch das Format PDF auf bestimmte PDF/A-Varianten ein (siehe auch A\_25233\*). Daher müssen PDF-Dokumente des Versicherten unter Umständen vor dem Einstellen in die ePA konvertiert werden.

Um das ePA-FdV dabei zu entlasten und Komplexität aus dem ePA-FdV zu nehmen, wird eine Funktion angeboten, durch die ein PDF in ein PDF/A konvertiert werden kann. Das ePA-FdV muss aber berücksichtigen, dass die Konvertierung ggf. technisch nicht durchgeführt werden kann oder das Ergebnis der Konvertierung durch ein geändertes Layout ggf. nicht verwendbar ist.

**A\_25456 -XDS Document Service - Keine negativen Auswirkungen auf Folgekonvertierungen von PDF zu PDF/A**

Der XDS Document Service MUSS sicherstellen, dass eine Konvertierung eines PDF-Dokuments sich nicht schädlich auf folgende Konvertierungen auswirken kann.[<=]

Hinweis zu A\_25456\*: Die Anforderung soll erreichen, dass ein potentiell über ein PDF-Dokument eingebrachter Schadcode nach der Konvertierung gelöscht wird, z.B. durch Zurücksetzen der Sandbox oder der VAU-Instanz

**A\_25455 -XDS Document Service - Isolation der Konvertierung von PDF zu PDF/A**

Der XDS Document Service MUSS die Verarbeitung von PDF-Dokumenten, die im Rahmen der Konvertierung in ein PDF/A durchgeführt wird, in einer separaten VAU-Instanz durchführen, die ausschließlich eine Verbindung zu einem ePA-FdV besitzen darf.[<=]

**A\_25454 -XDS Document Service - Realisierung der Schnittstelle****I\_Tool\_Convert\_PDF\_Insurant**

Der XDS Document Service MUSS die Operationen der Schnittstelle I\_Tool\_Convert\_PDF\_Insurant gemäß [I\_Tool\_Convert\_PDF\_Insurant] umsetzen.[<=]

**A\_26129 -ePA-Aktensystem - Rahmenbedingungen bei Nutzung einer Service-VAU für PDF-Konvertierung**

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die vom ePA-FdV übermittelten PDF-Dokumente in der Aktenkontoverwaltungs-VAU ausschließlich weitergeleitet aber ansonsten nicht verarbeitet werden. Gleiches gilt für die von der Service-VAU an das ePA-FdV übermittelten konvertierten PDF/A-Dokumente.[<=]

**A\_26130 -ePA-Aktensystem - maximale Lebensdauer einer Service-VAU für PDF-Konvertierung**

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die Lebensdauer einer solchen Service-VAU-Instanz maximal 12 Stunden beträgt.[<=]

**A\_26131 -ePA-Aktensystem - Keine Speicherung von in der Service-VAU für PDF-Konvertierung verarbeiteten Daten**

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass weder die vom

ePA-FdV übermittelten und zu konvertierenden PDF-Dokumente noch die daraus konvertierten PDF/A-Dokumente von der "PDF-VAU" im ePA-Aktensystem gespeichert werden. [≤]

#### **A\_26121 -ePA-Aktensystem - Keine Verarbeitung von Geräteinformationen**

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass keine Geräteinformationen (Device Management) von Nutzern verarbeitet werden. [≤]

### **3.13.2 FHIR Data Services**

#### **3.13.2.1 Patient Service**

##### **A\_26252-03 -Patient Service - Realisierung der Schnittstelle des FHIR IG ePA Basisfunktionalitäten**

Der Patient Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide ePA Basisfunktionalitäten (Patient Service) gemäß [IG\_Basic] umsetzen. [≤]

##### **A\_26254-01 -Patient Service - Protokolleinträge für Zugriffe auf den Patient Service**

Der Patient Service MUSS einen Protokolleintrag gemäß A\_24704\* erzeugen und dabei folgende Wertebelegung berücksichtigen:

**Tabelle 37: Patient Service Protokollierung**

Strukturelement	Wert	Erläuterung
AuditEvent.type	"rest"	
AuditEvent.action	U	Update
AuditEvent.entity.name	Patient	Service Name
AuditEvent.entity.description	upsertPatient	operationId der zu ausgeführten Operation

[≤]

#### **3.13.2.2 Medication Service**

##### **A\_26253-01 -Medication Service - Realisierung der Schnittstellen des FHIR IG Medication Service**

Der Medication Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide für den Medication Service [IG\_Medication\_Service] umsetzen. [≤]

##### **A\_26317 -Medication Service - Erzeugung eines xHTML-Exports**

Der Medication Service MUSS gemäß den Vorgaben von [IG\_Medication\_Service] für die Generierung der Medikationsliste im xHTML-Format nach [XHTML] sicherstellen, dass kein ausführbarer Code im Export enthalten ist. [≤]

##### **A\_24820 -Medication Service - Ablehnung von Request bei vorliegendem Widerspruch**

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID != oid\_erp-vau, oid\_versicherter mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("medication") die Entscheidung ("deny") gesetzt ist. [≤]

#### **A\_25152 -Medication Service - Ablehnung neuer Daten bei vorliegendem Widerspruch**

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID == oid\_erp-vau mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny") gesetzt ist. [≤]

#### **A\_25153 -Medication Service - Löschen der Daten des Medication Service**

Der Medication Service MUSS alle vorhandenen fachlichen Daten des Medication Service löschen, wenn im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny") gesetzt wird. [≤]

#### **A\_26399 -Medication Service - Ablehnung von Request bei vorliegendem Widerspruch gegen die Nutzung durch eine spezifische LEI**

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID gemäß A\_26406-\* mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management die LEI der User Session in der User Specific Deny Policy des Medication Service enthalten ist. [≤]

#### **A\_24841-03 -Medication Service - Schemavalidierung**

Der Medication Service MUSS im Body der HTTP-POST-Operation die übertragenen Parameter auf Schadcode prüfen und fachfremde Daten (d.h. Schemavalidierung) prüfen und im Fehlerfall das Ausführen der Operation mit dem HTTP Status Code 400 abbrechen. [≤]

#### **A\_27894 -Medication Service - Nutzung der FHIR-Operationen durch den E-Rezept-Fachdienst**

Der Medication Service MUSS sicherstellen, dass die folgenden FHIR-Operationen ausschließlich durch den E-Rezept-Fachdienst mit der professionOID oid\_erp-vau genutzt werden dürfen:

- providePrescription\_MedicationSvc
- cancelPrescription\_MedicationSvc
- provideDispensation\_MedicationSvc
- cancelDispensation\_MedicationSvc.

[≤]

#### **A\_24849-05 -Medication Service - Protokolleinträge für Zugriffe auf den Medication Service**

Der Medication Service MUSS einen Protokolleintrag gemäß A\_24704\* erzeugen und dabei folgende Wertbelegung berücksichtigen:

**Tabelle 38: Medication Service Protokollierung**

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung

type		"rest"	
action	OperationId: providePrescription_M edicationSvc	"C"	Einstellen von Verschreibungsda ten
	OperationId: provideDispensation_ MedicationSvc	"C"	Einstellen einer Medikamentenab gabe
	OperationId: cancelPrescription_Me dicationSvc	"U"	Stornieren von Verschreibungsda ten
	OperationId: cancelDispensation_M edicationSvc	"U"	Stornieren einer Medikamentenab gabe
	OperationId: getMedicationList_Me dicationSvc	"R"	Abruf der Medikationsliste
	OperationId: renderMedicationListT oHTML_MedicationSvc	"R"	Abruf der Medikationsliste im HTML-Format
	OperationId: renderMedicationListT oPDF_MedicationSvc	"R"	Abruf der Medikationsliste im PDF-Format
	OperationId: listMedications_Medic ationSvc	"R"	Abruf von Medikamentenin formationen
	OperationId: listMedicationDispens es_MedicationSvc	"R"	Abruf von Medikamentenab gabeinformatio nen
	OperationId: listMedicationRequest s_MedicationSvc	"R"	Abruf von Verschreibungsinf ormationen
	OperationId: addEMLEntry_Medicati onSvc	"C"	Eintrag in Medikationsliste hinzufügen
	OperationId: updateEMLEntry_Medi cationSvc	"U"	Eintrag in Medikationsliste aktualisieren
	OperationId:	"C"	Eintrag in

	addEMPEntry_MedicationSvc		Medikationsplan hinzufügen
	OperationId: updateEMPEntry_MedicationSvc	"U"	Eintrag in Medikationsplan aktualisieren
	OperationId: linkEMP_MedicationSvc	"U"	Eintragsverknüpfung Medikationsplan/ Medikationsliste
	OperationId: unlinkEMP_MedicationSvc	"U"	Aufhebung Eintragsverknüpfung Medikationsplan/ Medikationsliste
	OperationId: renderMedicationListToPDF_MedicationSvc	"R"	Abruf des Medikationsplans im PDF-Format
	OperationId: getMedicationPlan_MedicationSvc	"R"	Abruf des Medikationsplans
entity.name		"Medication Service"	Service Name
entity.description		<operationId>	operationId der ausgeführten Operation
Nur bei FHIR Query API:			
entity.detail.type		"search-parameters"	
entity.detail.value[x]		<ResourceName>? parameter1=<value>¶meter2=<value>& ...mehr	Suchkriterien in URL-Query-Notation

Falls ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF der Medication Service einen Protokolleintrag NICHT erzeugen.【<=】

Ereignisse, die gemäß A\_26298\* zu einer Übertragung neuer oder geänderter Daten an das FDZ führen, erzeugen grundsätzlich einen eigenen Protokolleintrag für den Vorgang gemäß der Vorgaben in A\_24849\*. Liegt kein Widerspruch des Versicherten gegen die Übermittlung der Daten an das FDZ vor und ist eine Übertragung der Daten des Ereignisses aufgrund der Pseudonymisierbarkeit dieser Daten möglich, so folgt auf das ursächliche Ereignis automatisch der Export der pseudonymisierten Daten.

Diese Übertragung der Daten muss für einen Versicherten aus der Protokollierung ersichtlich sein. Anstelle eines dedizierten Protokolleintrags für die Datenübertragung wird die Datenübertragung als ergänzendes entity.detail des auslösenden Ereignisses

protokolliert. Aus dem Protokolleintrag des Ereignisses ist dann ersichtlich, ob die betroffenen Daten in pseudonymisierter Form auch der sekundären Datennutzung zugeführt wurden.

#### **A\_27188 -Medication Service - Protokollierung des Datenexports an das FDZ**

Der Medication Service MUSS einen Protokolleintrag gemäß A\_24849\* um das folgend aufgeführte `entity.detail` mit dem Wert `true` ergänzen, wenn aus der Operation eine Übertragung von Daten an das FDZ folgt. Diese Ergänzung MUSS entweder den Wert `false` haben oder entfallen, wenn aus der Operation keine Übertragung von Daten an das FDZ folgt.

Strukturelement		Wert	Erläuterung
<code>entity.detail.type</code>		"data-submission"	Export an das Forschungsdatenzentrum
<code>entity.detail.value[x]</code>		"true" oder "false"	

[<=]

### **3.13.2.3 MHD Service**

#### **A\_27667-01 -MHD Service - Realisierung der Schnittstellen des FHIR IG MHD**

Der MHD Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide für den MHD Service [IG\_MHD\_Service] umsetzen.[<=]

Hinweis zu A\_27667-\*: Auch für den MHD Service sind die übergreifenden Anforderungen A\_15159 zum Schutz gegen die OWASP Risiken und A\_24783 zur Eingabvalidierung zu berücksichtigen, um zu verhindern, dass Schadcode über Suchanfragen ins Aktensystem eingebracht werden kann.

#### **A\_27892 -MHD Service - Durchsetzen der Zugriffskontrolle für XDS Document Service**

Der MHD Service MUSS bei einer Suchanfrage durch einen Nutzer alle Zugriffsregeln durchsetzen, die für den Zugriff dieses Nutzers bzgl. des XDS Document Service gelten.

[<=]

Hinweis zu A\_27892-\*: Nutzer dürfen durch den MHD Service keinen Zugriff auf Dokumente erhalten, auf den sie über den XDS Document Service nicht zugreifen dürften. So dürfen Nutzer mittels des MHD Services keinen Zugriff auf Dokumente einer Dokumentenkategorie erhalten, auf die sie nach der Legal Policy nicht zugreifen dürfen. Genauso dürfen sie über den MHD Service keine Dokumente finden, die auf der General Deny Policy stehen.

#### **A\_27668 -MHD Service - Filtern von verborgenen Metadaten und Dokumenten**

Der MHD Service MUSS bei einer Suchanfrage bei jedem Dokument einer verborgenen Datenkategorie die Metadaten (bzw. korrespondierende FHIR-Ressource `DocumentReference` filtern sowie den Dokumentenabruf `ausDocumentReferences.content.attachment.url` verhindern (HTTP Code 404 not found).

[<=]

#### **A\_27669 -MHD Service - Protokolleinträge für Zugriffe auf den MHD Service**

Der MHD Service MUSS einen Protokolleintrag gemäß A\_24704\* erzeugen und dabei folgende Wertbelegung berücksichtigen:



Tabelle 39: MHD Service Protokollierung

Strukturelement [AuditEvent.]	Operationen der FHIR Query API	Wert	Erläuterung
type		"rest"	
action	OperationId: findDocumentReferences_MHDSvc	"R"	Suche von Dokumenten
	OperationId: retrieveDocument_MHDSvc	"R"	Abruf eines Dokuments
entity.name		"MHD Service"	
entity.detail.type		"search-parameters"	
entity.detail.value[x]		<ResourceName>? parameter1=<value>&parameter2=<value>& ...mehr	Suchkriterien in URL-Query-Notation

Falls ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF der MHD Service NICHT einen Protokolleintrag erzeugen. [≤=]

### 3.13.2.4 Dienstübergreifende Festlegungen

#### A\_27886 -FHIR Data Service - Durchführung von Datenbestandsmigrationen

Wenn Migrationsvorgaben für den Datenbestand eines FHIR Data Services für verschiedene Versionen des Services existieren, MUSS der FHIR Data Service alle bislang nicht angewandten Datenbestandsmigrationsvorgaben in der richtigen Reihenfolge (d.h. nacheinander die jeweils für die Version benannten Migrationsschritte beginnend mit der kleinsten Versionsnummer hin zur höchsten Versionsnummer) ausführen oder, alternativ eine Migration der Daten vornehmen, die zum selben Ergebnis führt.

[≤=]

## 3.14 Audit Event Service

Ereignisse und Zugriffe auf die ePA eines Versicherten werden im ePA Aktensystem protokolliert. Die Protokollierung dient der Datenschutzkontrolle für den Versicherten.

Der Audit Event Service ist ein FHIR Data Service und ermöglicht dem Versicherten, befugten Vertretern bzw. der Ombudsstelle den Zugriff auf diese Protokollinformationen.

#### **A\_24704-02 -Audit Event Service - Realisierung der Schnittstelle des FHIR IG ePA Basisfunktionalitäten**

Der Audit Event Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide ePA Basisfunktionalitäten (Audit Event Service) gemäß [IG\_Basic] umsetzen.【<=】

In der Struktur eines Protokolleintrages (AuditEvents) sind folgende Zugriffsinformationen hinterlegt:

**Tabelle 40 : Inhaltliche Definitionen eines AuditEvent**

Information	Strukturelement
Wann ist der Zugriff erfolgt bzw. hat das Ereignis stattgefunden?	AuditEvent.recorded
Wer war der Akteur/Auslöser?	AuditEvent.agent
Welcher Art Service wurde angefragt?	AuditEvent.type
Worauf wurde zugegriffen?	AuditEvent.source
Welcher Art war der Zugriff?	AuditEvent.action
War der Zugriff erfolgreich?	AuditEvent.outcome
Informationen zu Daten/Dokumente/Objekte	AuditEvent.entity

Die spezifische Befüllung eines Audit Events gemäß A\_24704\* wird durch die jeweiligen Services vorgegeben. Allgemeine Elemente sind wie folgt zu befüllen:

#### **A\_25154-04 -ePA-Aktensystem - Befüllung der Elemente recorded, agent und source eines Audit Events**

Das ePA-Aktensystem MUSS die Audit Event Elemente AuditEvent.recorded, AuditEvent.agent und AuditEvent.source wie folgt befüllen.

**Tabelle 41 Befüllung AuditEvent**

Element [AuditEvent.]	Beschreibung	Beispiel
recorded	Systemzeit bei Erstellung des AuditEvents im Format YYYY-MM-DDThh:mm:ssZ	"2025-01-15T14:52:04.928Z"
purposeOfEvent	Zweck(e) des protokollierten Ereignisses gemäß des zulässigen Value-Sets. Nur zu belegen, wenn explizit bei entsprechender Protokollierungsanforderung gefordert.	
	syste	Das verwendete Codesystem
		" <a href="https://gematik.de/fhir/epa/">https://gematik.de/fhir/epa/</a>

	m		<a href="#">ValueSet/epa-auditevent-purpose-of-event-vs</a> "
	code	Der verwendete Code aus dem Codesystem	"EXPORTFDZ"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Export für das Forschungsdatenzentrum Gesundheit"
agent[client].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem; Fest vorgegebener Wert: "http://dicom.nema.org/resources/ontology/DCM"	"http://dicom.nema.org/resources/ontology/DCM"
	code	Der verwendete Code aus dem Codesystem; Fest vorgegebener Wert: "110150"	"110150"
	display	Der Bezeichner zur Anzeige aus dem Codesystem; Fest vorgegebener Wert: "Application"	"Application"
agent[client].who.identifier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/sid/telematik-id"
	value	<Telematik-Id>	"1-883110000092404"
agent[client].	altId	<value> aus agent.who.identifier	"1-883110000092404"
agent[client].	name	<ul style="list-style-type: none"> <li>&lt;display_name&gt; des auslösenden Akteurs aus dem ID-Token der UserSession</li> <li>"Elektronische Patientenakte Fachdienst" für intern ausgelöste</li> </ul>	1) "E-Rezept-Fachdienst" 2) "Elektronische Patientenakte Fachdienst" 3) "Portugal" (Beispiel EU-Zugriff)

		AuditEvents	
agent[client].	requestor	Fest vorgegebener Wert "false"	"false"
agent[user].type .coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	" <a href="http://terminology.hl7.org/CodeSystem/v3-RoleClass">http://terminology.hl7.org/CodeSystem/v3-RoleClass</a> "
	code	Der verwendete Code aus dem Codesystem	"PROV"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"healthcare provider"
agent[user].who. identifier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/sid/ telematik-id"
	value	<Telematik-Id> oder <KVNR>	1) "2-121212121212121" 2) "Z123456789"
agent[user].	altId	<value> aus agent.who.identifier	1) "2-121212121212121" 2) "Z123456789"
agent[user].role. coding		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthProfessionalRole.	
	system	Das verwendete Codesystem	"urn:oid:1.3.6.1.4.1.12559.11. 10.1.3.2.2.2"
	code	Der verwendete Code aus dem Codesystem	"Resident Physician"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Resident Physician"
agent[user].extension		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthcareFacilityType; extension mit url="https://gematik.de/fhir/de v-epa/StructureDefinition/epa-	

		healthcare-facility-type-extension">	
	system	Das verwendete Codesystem	"urn:oid:2.16.840.1.113883.2.9.6.2.7"
	code	Der verwendete Code aus dem Codesystem	"221"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Medical Doctors"
agent[user].	name	Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: <leiName> / <healthProfessionalName> Andernfalls: <display_name> des auslösenden Akteurs aus dem ID-Token der UserSession	EU-Zugriff: "Dr. Manuel Dos Santos / Clínica de Dos Santos" Andernfalls: "John Doe"
agent[user].	requestor	Fest vorgegebener Wert "false"	false
agent[internal].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	" <a href="https://gematik.de/fhir/epa/CodeSystem/epa-auditevent-sourcetype-cs">https://gematik.de/fhir/epa/CodeSystem/epa-auditevent-sourcetype-cs</a> "
	code	Der verwendete Code aus dem Codesystem	"DATASUBSVC"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Data Submission Service"
agent[internal].	altId	Fest vorgegebener Wert "ePA"	"ePA"
agent[internal]	name	Fest vorgegebener Wert "ePA"	"ePA"
agent[internal].	requestor	Fest vorgegebener Wert "false"	"false"
source		Informationen zum auslösenden Service des Aktensystems	
source.observer.	display	Fester Wert "Elektronische	"Elektronische Patientenakte"

	ay	Patientenakte Fachdienst"	Fachdienst"
source.type.		Der auslösende Service gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	" <a href="https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs">https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs</a> "
	code	Der verwendete Code aus dem Codesystem	"CDMGMT"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Consent Decision Management"

Hinweis:

agent[client]: Angaben zur Applikation, z. B. eRezept-Fachdienst, NCPeH

agent[user]: Angaben zu LEI oder Vertreter oder Versicherter

agent[internal]: Angaben zu systemeigenen Prozessen, z. B. Datenexport für das FDZ  
[<=]

#### **A\_27689 -Protokollierung von nicht erfolgreichen Zugriffen**

Falls für eine Operation ein Protokolleintrag gefordert ist und mit einem Fehler abgebrochen wird, MUSS der Audit Event Service jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen. Darüberhinaus und ergänzend zu den Vorgaben aus dem Profil EPAAuditEvent gemäß [IG\_Basic] sind folgende Werte entsprechend zu belegen:

**Tabelle 42 Audit Event Management Protokollierung - Fehler**

Strukturelement	Wert	Erläuterung
AuditEvent.action	C, R, U, D	Create   Read   Update   Delete
AuditEvent.entity.name	<service name>	Service Name, wie für Protokollierung im Service gefordert
AuditEvent.entity.description	<operationId>	OperationId der mit einem Fehler abgebrochenen Operation, z. B. "providePrescription_MedicationSvc"
<b>Nur bei FHIR Query API:</b>		
entity.detail.type	"search-parameters"	
entity.detail.value[x]	<ResourceName>? parameter1=<value>parameter2=<value>	Suchkriterien in URL-Query-Notation

	>& ...mehr	
--	------------	--

Falls ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF bei nicht erfolgreichen Zugriffen ein Protokolleintrag NICHT erzeugt werden.

Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A\_25172\* entfällt, wenn ein Protokolleintrag mangels eines befugten Nutzers (kein Bezug des SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann.

[<=]

#### **A\_24503 -ePA-Aktensystem - Aufbewahrungsdauer der Protokolleinträge**

Das ePa-Aktensystem MUSS die zum Zwecke der Datenschutzkontrolle für den Versicherten erstellten Protokolleinträge für drei Jahre aufbewahren. Danach sind sie vom Aktensystem automatisch zu löschen.[<=]

Die Protokolleinträge können durch den Versicherten oder durch einen befugten Vertreter mittels ePA-FdV eingesehen werden. Versicherte ohne ePA-FdV können bei ihrer zuständigen Ombudsstelle beantragen, die Protokolldaten zur Verfügung gestellt zu bekommen.

Für eine Abfrage der Protokolleinträge als strukturierte Einträge nutzen ein ePA-FdV und die Ombudsstelle den Audit Event Service [IG\_Basic].

#### **A\_24714-01 -Audit Event Service - Realisierung der Query API: AuditEvent**

Der Audit Event Service MUSS die "Query API: AuditEvent" des FHIR Implementation Guide für den Audit Event Service [IG\_Basic] umsetzen.[<=]

#### **A\_24750-02 -Audit Event Service - Realisierung der Render API: PDF Audit**

Der Audit Event Service MUSS die "Render API: PDF Audit" des FHIR Implementation Guide für den Audit Event Service [IG\_Basic] umsetzen.[<=]

#### **A\_25172 -Audit Event Service - Speicherung der Protokolldaten**

Der Audit Event Service MUSS die Daten der Protokolleinträge verschlüsselt im SecureDataStorage persistieren.[<=]

Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A\_25172\* entfällt, wenn ein Protokolleintrag mangels eines befugten Nutzers (kein Bezug des SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann.

#### **A\_25018 -Audit Event Service - PAdES-Signatur in renderAuditEventsToPDF**

Der Audit Event Service MUSS bei der Operation renderAuditEventsToPDF beim Signieren eines Protokolls im PDF/A-Format eine PAdES-Signatur gemäß [PAdES-3] und [PAdES Baseline Profile] erstellen. Bei der Signaturerstellung ist das Attribut signing certificate reference gemäß den Vorgaben aus [PAdES-3] Kapitel 4.4.3 „Signing Certificate Reference Attribute“ anzulegen.[<=]

Durch die Baseline-Profilierung [PAdES Baseline Profile] wird festgelegt, wie der Signaturzeitpunkt, gemessen als Systemzeit des ePA-Aktensystems, in die Signatur eingebracht wird.

#### **A\_24991 -Audit Event Service - Protokollierung von Zugriffen auf die Protokolldaten**

Der Audit Event Service MUSS für die Zugriffe der Ombudsstelle oder eines Vertreters auf die protokollierten Daten jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen.

**Tabelle 43: Audit Event Service Protokollierung**

Strukturelement	Wert	Erläuterung



AuditEvent.type	"rest"		
AuditEvent.action	R		Read
AuditEvent.entity.name	"AuditEvent"		Service Name
AuditEvent.entity.description	Passend zur ausgeführten Operation ein Wert aus folgender Liste: <ul style="list-style-type: none"> <li>• listAuditEvents</li> <li>• getAuditEventById</li> <li>• renderAuditEventsToPDF</li> </ul>		operationId der zu protokollierenden Operation
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	parameters	parameter1=<value>&parameter2=<value>& ...mehr	Nur bei getAuditEventList
	identifizier	<id> des AuditEvents	Nur bei getAuditEvent

[&lt;=]

*Hinweis: Zugriffe des Versicherten auf die Protokolle des Aktenkontos werden nicht protokolliert.*

## 3.15 Information Service

### 3.15.1 Information Service

Der Information Service ist ohne die Nutzung eines VAU-Kanals nutzbar. Die über den Information Service genutzten Daten sind ausschließlich persistierte Daten des Aktenkontos, die weder mit dem SecureAdminStorageKey noch mit dem SecureDataStorageKey gesichert sind.

Der Zugang erfolgt durch Nutzung der Schnittstelle I\_Information\_Service.

#### **A\_24344 -Information Service - Realisierung der Schnittstelle I\_Information\_Service**

Der Information Service MUSS die Operationen der Schnittstelle I\_Information\_Service gemäß [I\_Information\_Service] umsetzen.[<=]

#### **A\_24345 -Information Service - Kein Zugriff auf verschlüsselte Daten des Aktenkontos**

Der Information Service DARF NICHT auf Daten zugreifen, die nicht explizit für die Verwendung durch den Informationsdienst bereitgestellt wurden. Dazu gehören

insbesondere alle Daten des Aktenkontos, die mit den versichertenindividuellen Schlüsseln zur Daten- oder Befugnispersistierung (SecureDataStorageKey oder SecureAdminStorageKey) gesichert sind. [≤]

### 3.15.1.1 Informationen zu Widersprüchen (Consent Decisions)

Die Widersprüche eines Versicherten gegen die Nutzung von Funktionen der elektronischen Patientenakte werden durch das Consent Decision Management gesichert administriert. Änderungen an den Widersprüchen erfolgen dort.

Der Information Service bietet für die Nutzergruppen der ePA eine einfache Abfragemöglichkeit der aktuell erteilten oder nicht erteilten Widersprüche auch ohne die Nutzung des Consent Decision Managements an. Liegt ein Widerspruch gegen die Nutzung einer Funktion vor, kann auf die Ausführung der zur Nutzung dieser Funktion notwendigen Aktionen mit der ePA eines Versicherten durch den Client verzichtet werden.

Für diese vereinfachte Abfragemöglichkeit der aktuellen Widersprüche verwendet der Information Service den durch das Consent Decision Management persistent übertragenen Zustand der Widersprüche ("Cache" des Zustands der Widersprüche). Berücksichtigt wird dabei die Widerspruchsinformation, für die eine vereinfachte Abfrage vorgesehen ist (Widersprüche der Klasse "Versorgungsprozess").

### 3.15.1.2 Informationen zur Anwenderperformance (UX Performance)

Der Information Service stellt für die Umgebung der Leistungserbringer die Operation zur Sammlung der Messwerte zu den Anwendungsfällen der Nutzererfahrung zur Verfügung. Die Weiterverarbeitung der gesammelten Daten ist in 2.8- Performance aus Anwendersicht definiert und vorgegeben.

## 3.15.2 Information Service - Account

Die Operationen der Information Service - Account werden für den Umzug eines existierenden Aktenkontos zu einem neuen Anbieter verwendet. Die Nutzung der Operationen erfolgt exklusiv durch die Aktensystembetreiber.

Die Verwendung der einzelnen Operationen erfolgt im Verbund mit den Operationen der Schnittstelle I\_Health\_Record\_Relocation\_Service für die Umsetzung der Anwendungsfälle eines automatischen Aktenkontoumzugs und sind in 3.2- Health Record Relocation Service erläutert.

### A\_24424 -Information Service Account - Realisierung der Schnittstelle

#### I\_Information\_Service\_Accounts

Der Information Service MUSS die Operationen der Schnittstelle

I\_Information\_Service\_Accounts gemäß [I\_Information\_Service\_Accounts] umsetzen.

[≤]

### A\_24665 -Information Service Account - Nutzung beidseitig authentisiertes TLS

Der Information Service MUSS sicherstellen, dass die Operationen der Schnittstelle I\_Information\_Service\_Accounts ausschließlich unter Verwendung einer beidseitig authentisierten TLS-Verbindung zwischen den beteiligten Aktensystemen genutzt werden und die Operationen ansonsten abgebrochen und mit einer Fehlermeldung gemäß Vorgaben in [I\_Information\_Service\_Accounts] beantwortet werden. [≤]

### A\_25054 -Information Service Account - Gegenseitige Authentisierung Aktensysteme

Die Information Service Account Dienste der Aktensysteme MÜSSEN sich mit der TLS-Identität mit professionOID `oid_epa_mgmt` mittels des Zertifikats `C.FD-TLS-S` gegenseitig authentisieren.

[≤]

**A\_25053 -Information Service Account - Prüfung der TLS-Zertifikate**

Der Information Service Account MUSS bei der Authentifizierung eines jeweils anderen Aktensystems die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC\_PKI\_018 durchführen. Zur Prüfung des TLS-Zertifikats C.FD-TLS-S sind dabei die Parameter PolicyList=oid\_fd\_tls\_s, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-serverAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD-TLS-C sind dabei die Parameter PolicyList=oid\_fd\_tls\_c, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-clientAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden.

[<=]

### 3.16 Email Management

Das Email Management ermöglicht einem FdV-Nutzer die Verwaltung seiner E-Mail-Adresse und einem Kostenträger die Verwaltung von E-Mail-Adressen von Versicherten, die bei diesem Kostenträger versichert sind.

Die Schnittstelle zum Verwalten der E-Mail-Adressen durch den Kostenträger dient dem ausschließlichen Zweck des Einstellens, Lesens und der Änderung von E-Mail-Adressen auf Verlangen des Versicherten. Dies ermöglicht dem Kostenträger, seinen Versicherten die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte auf Berichtigung und Auskunft bzgl. der im Aktensystem verarbeiteten E-Mail-Adresse zu gewährleisten.

Für einen Versicherten kann nur genau eine E-Mail Adresse hinterlegt werden.

**A\_25435 -Email Management - Realisierung der Schnittstelle****I\_Email\_Management**

Das Email Management MUSS die Operationen der Schnittstelle I\_Email\_Management gemäß [I\_Email\_Management] umsetzen.[<=]

**A\_25438 -Email Management - Beschränkung der Schnittstellenoperationen auf E-Mail-Adressen des FdV-Nutzers**

Das Email Management MUSS die Operationen der Schnittstelle I\_Email\_Management gemäß [I\_Email\_Management] auf die E-Mail-Adresse des aufrufenden Nutzers einschränken, sofern der Nutzer ein FdV-Nutzer ist.[<=]

**A\_26161 -Email Management - Nutzen von Email Management auch bei Widerspruch**

Das Email Management MUSS sicherstellen, dass das Email Management auch von Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben.[<=]

**A\_26162 -Email Management - Versicherte nutzen Email Management ausschließlich im Home-AS**

Das Email Management des ePA-Aktensystems MUSS sicherstellen, dass das Email Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-Aktensystem das Home-AS ist.[<=]

Hinweis: Für das Email Management ist auch Anforderung A\_26154\* umzusetzen.

**A\_25439 -Email Management - Kostenträger kann ausschließlich E-Mail-Adressen der eigenen Versicherten verwalten**

Das Email Management MUSS sicherstellen, dass ein Kostenträger mittels der Operationen der Schnittstelle I\_Email\_Management gemäß [I\_Email\_Management] ausschließlich E-Mail-Adressen von Versicherten verwalten kann, die beim Kostenträger versichert sind.[<=]

**A\_25440-01 -Email Management - Benachrichtigung bei Änderung der E-Mail-Adresse**

Falls eine E-Mail-Adresse a) ersetzt oder b) ergänzt wird, MUSS das Device Management bei a) eine E-Mail an die alte und die neue E-Mail-Adresse senden und bei b) eine E-Mail an die neue E-Mail-Adresse senden, in der bei a) über die Ersetzung bzw. bei b) die Ergänzung einer E-Mail-Adresse informiert wird. In der E-Mail MUSS darüber informiert werden, wann und ob der FdV-Nutzer selbst oder der Kostenträger die E-Mail ersetzt bzw. ergänzt hat. [≤]

#### **A\_25441 -Email Management - Information bzgl. der Ergänzung bei E-Mail-Adressen**

Das Email Management MUSS sicherstellen, dass der FdV-Nutzer für eine im Email Management hinterlegte E-Mail-Adresse erkennen kann, wann und von wem diese E-Mail-Adresse ergänzt wurde. [≤]

#### **A\_25968-01 -Email Management - Maximale Anzahl E-Mail-Adressen**

Das Email Management MUSS sicherstellen, dass für einen Nutzer maximal eine E-Mail-Adresse hinterlegt werden kann. [≤]

#### **A\_26163 -Email Management - Keine Persistierung einer im Rahmen der Vertretereinrichtung übergebenen E-Mail-Adresse**

Das Email Management MUSS sicherstellen, dass eine im Rahmen des Anwendungsfalls der Vertretereinrichtung vom Nutzer übermittelte E-Mail-Adresse nicht persistiert und spätestens bei Beendigung der User Session gelöscht wird. [≤]

#### **A\_26164 -Email Management - Keine Geräteregistrierung mit der im Rahmen der Vertretereinrichtung übergebenen E-Mail-Adresse**

Das Email Management MUSS sicherstellen, dass keine E-Mail-Adressen zur Übermittlung eines Geräteregistrierungscodes genutzt werden, die dem ePA-Aktensystem im Rahmen des Anwendungsfalls der Vertretereinrichtung übermittelt wurden. [≤]

Hinweis zu A\_26163 und A\_26164: Die im Rahmen des Anwendungsfalls der Vertretereinrichtung übermittelte E-Mail-Adresse wird ausschließlich zur Information des Vertreters über die Einrichtung der Vertretung genutzt (vgl. A\_24755-\*).

### **3.17 Zusätzliche Anforderungen an den Authorization Service**

Der ePA Authorization Service wird sowohl für die Authentisierung der Versicherten über das FdV als auch für die Authentisierung von Leistungserbringern und Kostenträgern über deren Primärsystem benötigt. Ebenso muss die Zugriffsautorisierung für andere Fachdienste wie z.B. E-Rezept geprüft werden. Die Festlegungen für den Authorization Server finden sich in [gemSpec\_IDP\_FD]. Dieser Abschnitt des vorliegenden Dokuments enthält spezifische Anforderungen, die vom Authorization Service des Aktensystems zusätzlich umzusetzen sind.

#### **A\_24923 -Authorization Service - I\_Authorization\_Service**

Der Authorization Service MUSS die Operationen der Schnittstelle `I_Authorization_Service` implementieren gemäß [I\_Authorization\_Service]. [≤]

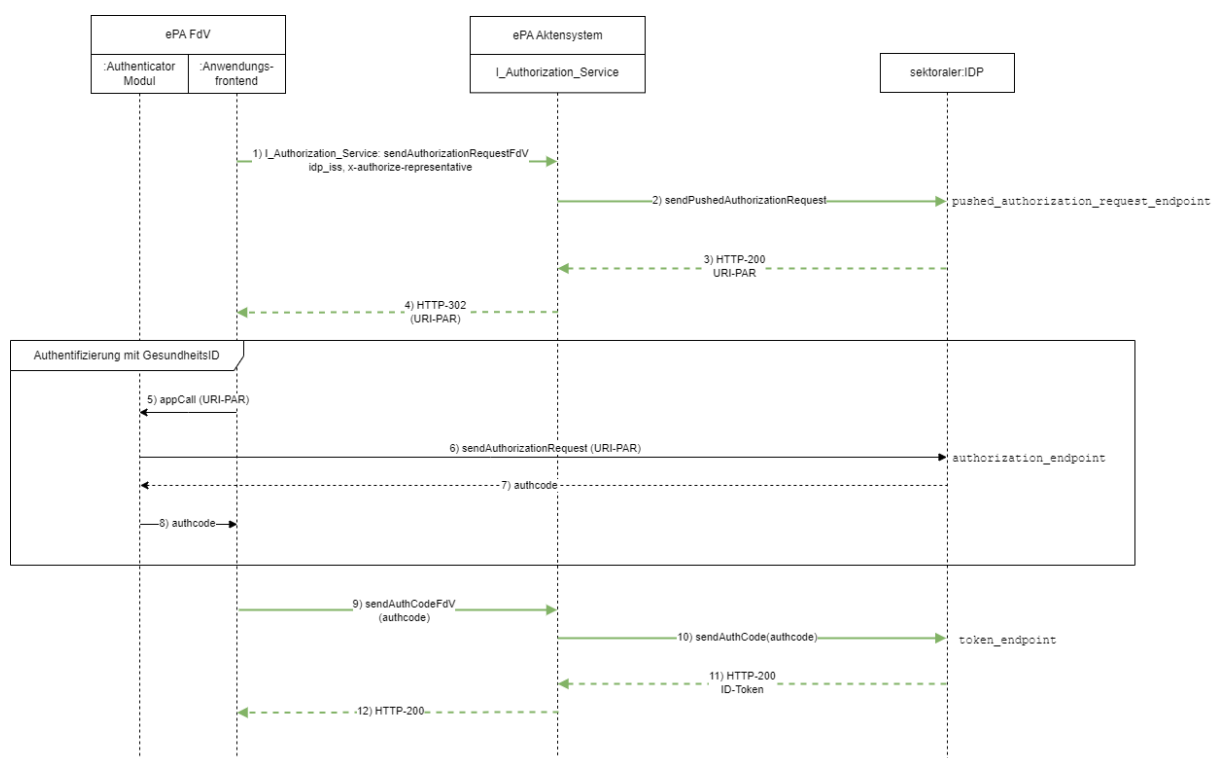
#### **A\_25283 -Authorization Service - Konvertieren von ID-Token**

Der Authorization Service MUSS sicherstellen, dass für ein nach erfolgreicher Authentifizierung des Nutzers vorliegendes ID-Token mittels Regel `rr0` gemäß *Tab\_AS\_Entitlement\_Registration\_Rules* ein HSM-ID-Token erstellt wird, bevor das ID-Token zeitlich ungültig ist. [≤]

### 3.17.1 Anforderungen an den Authorization Service für die Authentisierung von Versicherten (FdV)

Im Rahmen der Authentisierung des Versicherten erfolgt die Prüfung der Geräteregistrierung (Verifikation) direkt. Das Gerät muss dafür die Geräteparameter eines zuvor ausgeführten und bestätigten Registrierungsprozesses verwenden

Bisher nicht registrierte Geräte, bzw. Geräteparameter einer bisher nicht bestätigten Geräteregistrierung, können unter Verwendung des Device Management registriert, bzw. bestätigt werden (siehe Kapitel 3.12- Device Management).



**Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP**

#### A\_25717-03 -Authorization Service - Pushed Authorization-Request des Authorization Service an sektorale Identity Provider

Der ePA Authorization Service MUSS den Pushed Authorization Request (PAR) an durch den vom ePA-FdV übergebenen Parameter idp-iss adressierten sektoralen IDP gemäß [gemSpec\_IDP\_FD#AF\_10117] mit folgenden Parametern aufrufen:

Parameter	Wert	Anmerkung
scope	"openid urn:telematik:display_name urn:telematik:versicherter urn:telematik:family_name urn:telematik:given_name"	Notwendige Scopes für den Zugriff für die Autorisierung von Nutzern am ePA-Aktensystem
acr_values	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung

redirect_uri	Inhalt des Parameters x-redirecturi [sendAuthorizationRequestFdV in I_Authorization_Service], an dem falls eine herstellerspezifische Standard-redirect_uri.	Diese URI muss unter dem claim redirect_uris im Entity Statement des Authorization Service enthalten sein. Mandanten, welche eine eigene redirect_uri verwenden [sendAuthorizationRequestFdV in I_Authorization_Service], müssen diese im Rahmen des Registrierungsprozesses beim Authorization Service bekannt geben.
--------------	--	--

**[<=]**

Hinweis 1: An die redirect\_uri im Pushed Authorization Request sendet der sektorale IDP den ausgestellten Authorization Code (siehe [gemSpec\_IDP\_Sek])

Hinweis 2: Der Redirectaufruf, der vom Authenticator Modul an die redirect\_uri ausgeführt wird, wird vom ePA-FdV über Plattformmechanismen (deeplink/universallink) gefangen und stellt selbst einen POST-Request an den Endpunkt des Authorization Service.

#### **A\_26584 -Authorization Service - Liste der redirect\_uris im Entity Statement**

Der Authorization Service MUSS in seinem Entity Statement im claim redirect\_uris die redirect\_uris aller Mandanten auflisten, welche bei der Registrierung an einem beliebigen ePA Authorization Service eine eigene redirect\_uri angegeben haben. Über Änderungen des claim redirect\_uris MUSS der Anbieter des Federation Master vor produktiver Verwendung informiert werden**[<=]**

Hinweis: Im Registrierungsprozess eines Mandanten mit eigener redirect\_uri muss sichergestellt sein,

- dass alle Anbieter von ePA Authorization Servern (ePA Aktensystem Anbieter) entsprechend informiert sind und das Entity Statement anpassen
- dem Hersteller des Federation Master über ein ITSM Change bekannt gemacht wird, dass sich die Entity Statements aller ePA Authorization Server ändern

#### **A\_27145 -Synchronisation "redirect\_URI" mit Marktteilnehmer - E-Mail-Adresse**

Der Anbieter ePA-Aktensystem MUSS der gematik eine E-Mail-Adresse mitteilen, über welche er die eigenverantwortliche Registrierung (von redirect-URLs im Entity-Statement) durchführt und über die der Anbieter bei Änderungen erreichbar ist.

Hinweis: Diese E-Mail-Adressen werden durch das Provider Management der gematik anschließend unter den relevanten Anbietern verteilt bzw. können dort erfragt werden. Die Änderung der E-Mail-Adressen ist ebenfalls zu kommunizieren.

Hintergrund: Für Stellvertretung via ePA-FdV ist eine Synchronisierung der redirect\_URLs notwendig.**[<=]**

#### **A\_27186 -Synchronisation "redirect\_URI" mit Marktteilnehmer - Information**

Der Anbieter ePA-Aktensystem MUSS bei Änderungen der redirect\_URLs im eigenen Entity Statement allen anderen Marktteilnehmern des gleichen Fachdiensttyps diese Änderung innerhalb 24 Stunden mitteilen.**[<=]**

#### **A\_27187 -Synchronisation "redirect\_URI" mit Marktteilnehmer - Aktualisierung**

Der Anbieter ePA-Aktensystem MUSS nach dem Empfang der Mitteilungen über Änderungen der Redirect URLs in einem externen Entity Statement diese Änderung binnen 24 Stunden in den Redirect URLs des eigenen Entity Statement synchronisieren.

Hinweis: Diese Änderung erfordert anschließend keine Information nach A\_27186. [≤]

#### **A\_24878-01 -Authorization Service - Authentifizierung eines Versicherten am ePA-FdV des Vertreters**

Falls der Eingangsparameter x-authorize-representative=True der Operation I\_Authorization\_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der Authorization Service im PAR als Parameter amr mit den Werten urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [≤]

#### **A\_26189-01 -Authorization Service - Authentifizierung eines Versicherten im Gastmodus mit eGK und PIN**

Falls der Eingangsparameter x-authorize-egk=True der Operation I\_Authorization\_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der Authorization Service im PAR als Parameter amr mit den Werten urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [≤]

#### **A\_24937-01 -Authorization Service - Einschränkung bei Authentifizierung eines Versicherten am ePA-FdV des Vertreters**

Der Authorization Service MUSS sicherstellen, dass ein mit x-authorize-representative=True authentisierter Nutzer ausschließlich Zugriff auf das Entitlement Management erhält. [≤]

#### **A\_26159 -Authorization Service - Prüfen der Device Attestation**

Der Authorization Service MUSS sicherstellen, dass von einem anderen ePA-Aktensystem signierte Device Attestations ausschließlich akzeptiert werden, wenn

- die Device Attestation gemäß A\_25042-\* valide von einer Signaturidentität der VAU eines anderen ePA-Aktensystems signiert wurde,
- die KVNR in der Device Attestation mit der KVNR im ID-Token des angemeldeten Nutzers übereinstimmt,
- die Device Attestation zeitlich gültig ist.

[≤]

#### **A\_26160 -Authorization Service - Keine Persistierung der Device Attestation**

Der Authorization Service MUSS sicherstellen, dass die von einem anderen ePA-Aktensystem signierte Device Attestation und deren Inhalte spätestens bei Beendigung der User Session gelöscht und nicht persistiert werden. [≤]

#### **A\_25310-01 -Authorization Service - Einschränkung bei Authentifizierung mit einem unregistrierten Gerät**

Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wird und der Nutzer nicht mit x-authorize-representative=True authentisiert wurde, MUSS der Authorization Service sicherstellen, dass der Nutzer ausschließlich Zugriff auf das Device Management erhält. [≤]

Hinweis:

Ein vollständiger Zugriff eines authentisierten Nutzers auf alle Dienste des Aktensystems kann nur mit einem Gerät erfolgen, dessen Geräteregistrierung bei der Authentifizierung des Nutzers erfolgreich verifiziert wurde.

Ein Nachweis einer Geräteregistrierung ist entweder DeviceID (deviceIdentifier und deviceToken), die für den Nutzer im Aktensystem bekannt sind oder die vom Client übergebene Device Attestation (deviceAttestation), die zuvor am Device Management des Home Aktensystems durch den Client abgerufen wurde.

#### **A\_24804-01 -Authorization Service - Prüfung auf registriertes Gerät**



Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des Vertreters handelt und im Operationsaufruf

`I_Authorization_Service::sendAuthCodeFdV` eine DeviceID (deviceIdentifier und deviceToken) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer registriert und bestätigt ist und übereinstimmt. [ $\leq$ ]

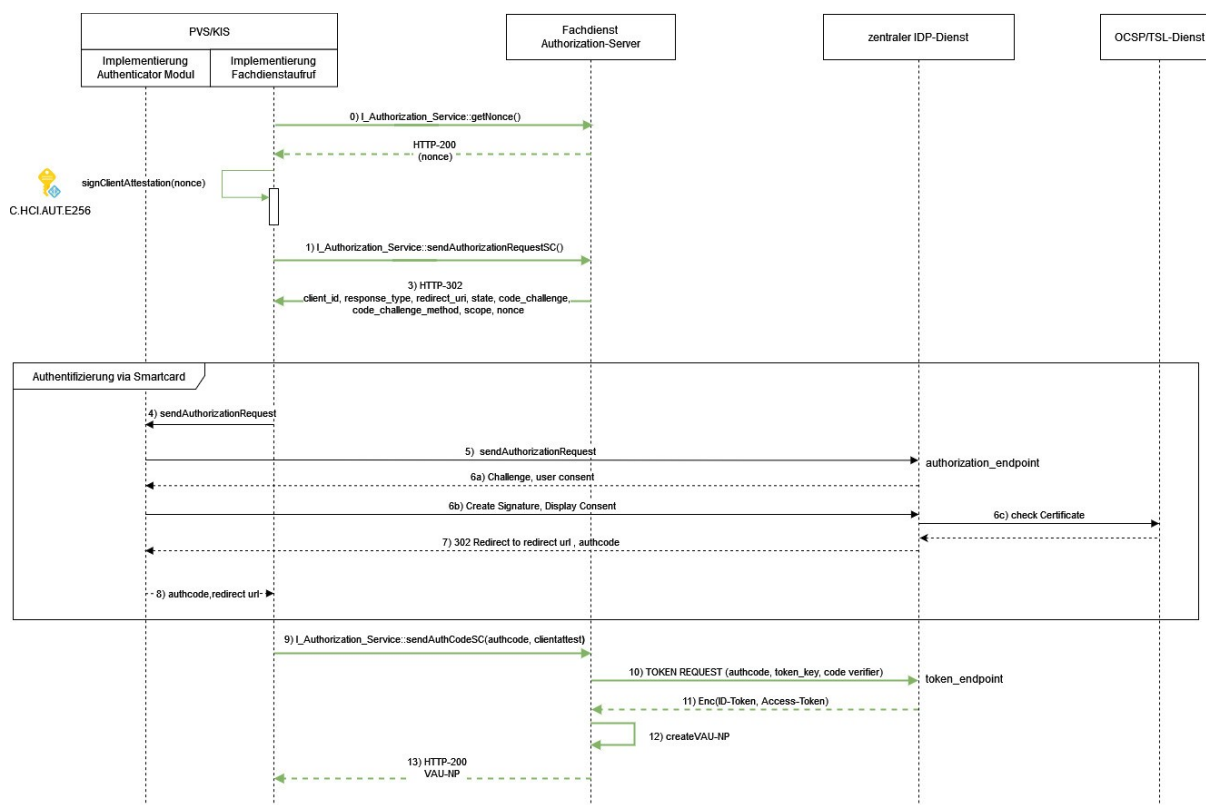
#### A\_24914-03 -Authorization Service - Prüfung auf registriertes Gerät - kein registriertes Gerät

Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wurde, MUSS der Authorization Service die Operation `sendAuthCodeFdV` mit einer Fehlermeldung abbrechen und die User Session beenden. [ $\leq$ ]

#### A\_24915-01 -Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht bestätigt

Falls als Nachweis einer Geräteregistrierung eine DeviceID (deviceIdentifier und deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status == 'pending'), MUSS der Authorization Service die Operation `sendAuthCodeFdV` mit einer Fehlermeldung abbrechen und die User Session beenden. [ $\leq$ ]

### 3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B



**Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP**

**A\_24717 -Authorization Service: IDToken vom IDP-Dienst nur mit Client-Attestation nutzbar**

Der Authorization Service MUSS sicherstellen, dass ein vom IDP-Dienst abgerufenes ID-Token für Nutzer "TelematikID\_X" nur dann akzeptiert wird, falls im Authorization Service auch eine Client-Attestation vom Nutzer "TelematikID\_X" vorliegt. [≤]

**A\_24718 -Authorization Service: Client-Attestation nur einmal nutzbar (Replay Angriffe)**

Der Authorization Service MUSS sicherstellen, dass eine Client-Attestation eines Nutzers im Authorization Service mit dem ID-Token nur einmalig für die Aktivierung einer User Session verwendet wird. [≤]

**A\_25444-01 -Authorization Service - JWT Client Attestation**

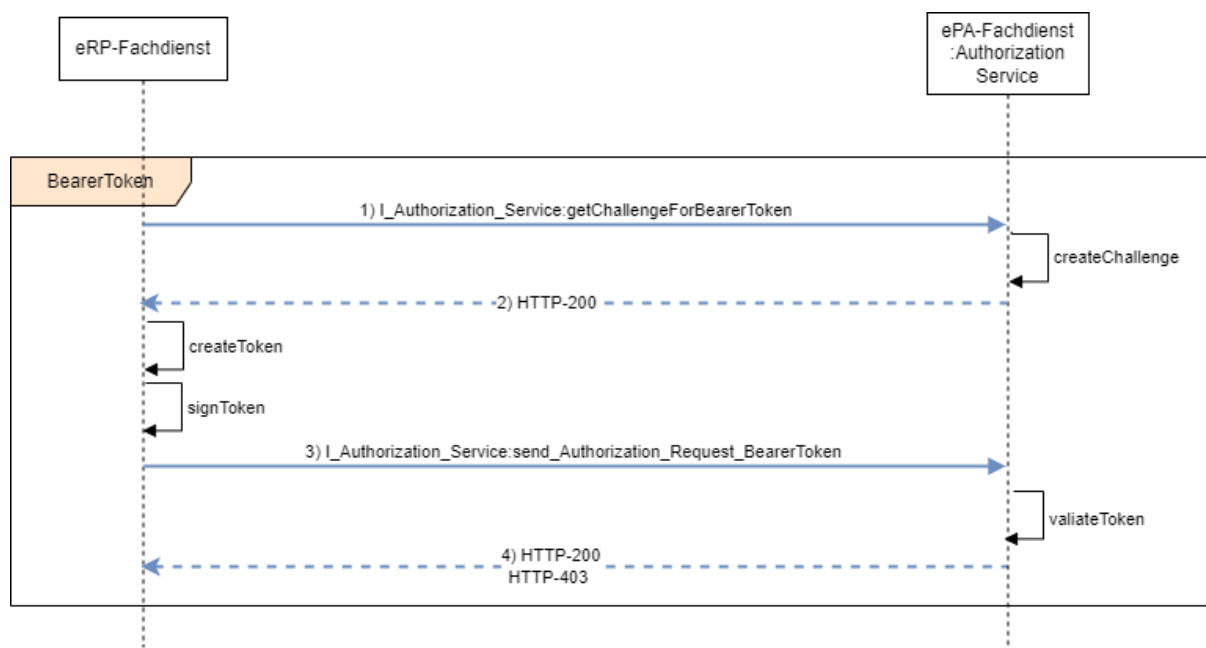
Der Authorization Service MUSS bei der Authentifizierung einer Leistungserbringerinstitution prüfen, dass das übermittelte JWT der Client Attestierung mindestens die folgenden Inhalte aufweist.

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256" oder "PS256"	
	"x5c"	Signaturzertifikat C.HCI.AUT	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"exp"	Verfalldatum, = "iat" + 20 min	Beispiel: "1705675744"
	"nonce"	Nonce aus einer getNonce Operation	siehe [I_Authorization_Service]

[≤]

Für das Signaturzertifikat zu "x5c" (AUT-Zertifikat der SMC-B) gilt: Basiert der öffentlichen Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

### 3.17.3 Anforderungen an den Authorization Service für die Authentisierung des E-Rezept-Fachdienstes



**Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes**

#### **A\_25165-03 -Authorization Service: JWT Bearer-Token des E-Rezept-Fachdienstes**

Das Authorization Service MUSS sicherstellen, dass die Authentifizierung des E-Rezept-Fachdienstes über die Schnittstelle `I_Authorization_Service` durch Verwendung eines gültig signierten JWT Bearer Token mit den dargestellten Mindest-Inhalten und Prüfung durch Regel 'rr0' des Befugnisverifikations-Moduls erfolgt. Die Claims in 'Payload' MÜSSEN dazu die Vorgaben aus [gemSpec\_Krypt], A\_24658\* befolgen.

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"

	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Krypt]
	"sub"	Telematik-ID des E-Rezept-Fachdienstes	

[<=]

Das Signaturzertifikat zu "x5c" (AUT-Zertifikat der E-Rezept-VAU) kommt aus der Komponenten-PKI der TI. Basiert der öffentliche Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

### 3.18 Anbindung Verzeichnisdienst FHIR-Directory

#### A\_25176 -ePA-Aktensystem - Anbindung Verzeichnisdienst FHIR-Directory

Das ePA-Aktensystem MUSS bei der Suche des Versicherten nach Einträgen im Verzeichnisdienst FHIR-Directory und bei der initialen Anlage einer Akte den Anwendungsfall "AF\_10219\* - Versicherter sucht Einträge im FHIR-Directory" gemäß [gemSpec\_VZD\_FHIR\_Directory] als Fachdienst unterstützen und dabei für die Client-Anfrage von search-access\_token die Operation getFHIRVZDtoken gemäß [I\_Authorization\_Service.yaml] bereitstellen.[<=]

### 3.19 Access Gateway

Das Access Gateway ermöglicht den Versicherten bzw. deren berechtigten Vertretern den Zugang zum zugehörigen Aktensystem über das Internet. Auf der einen Seite dient es der Abschottung des ePA-Aktensystems in Richtung Internet, auf der anderen Seite regelt es den kontrollierten Zugriff der Versicherten auf das Aktensystem mit seinen funktionalen Komponenten.

#### 3.19.1 Paketfilter

##### 3.19.1.1 Funktion

Der Paketfilter stellt die Anbindung des ePA-Aktensystems an das Internet her und gewährleistet die Abschottung des ePA-Aktensystems in Richtung Internet.

#### A\_14017 -Access Gateway, Sicherung zum Transportnetz Internet durch Paketfilter

Das ePA-Aktensystem MUSS zum Transportnetz Internet durch einen Paketfilter (ACL) gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der Paketfilter der Komponente Access Gateway MUSS frei konfigurierbar sein auf der Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport.[<=]

#### A\_14018 -Access Gateway, Platzierung des Paketfilters Internet

Der Paketfilter der Komponente Access Gateway, zum Schutz in Richtung Transportnetz Internet, DARF NICHT auf den anderen, zum Access Gateway gehörenden, physischen Komponenten implementiert werden.[<=]

#### A\_14019-02 -Access Gateway, Richtlinien für den Paketfilter zum Internet

Der Paketfilter der Komponente Access Gateway MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

1. HTTPS, und
2. OCSP-Zugriffe für das OCSP-Stapling (vgl. Hinweis nach A\_14019-02), ggf. notwendige DNS Anfragen (und Antworten).

Ein Verbindungsaufbau aus dem ePA-Aktensystem über das Access Gateway in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 .[<=]

*Hinweis zu A\_14019-02: Der Aktensystem-Anbieter muss für seine HTTPS-Schnittstelle ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-Zertifikate also über einen aktuellen Webbrowser prüfbar ist, vgl. A\_14776). Für dieses TLS-Zertifikat fragt das Access Gateway (die HTTPS-Schnittstelle ist Teil davon) regelmäßig für das OCSP-Stapling (vgl. [gemSpec\_Krypt#A\_24913-\*]) den OCSP-Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält das Access Gateway eine OCSP-Response. Diese wird nach A\_19126 geprüft und anschließend von der HTTPS-Schnittstelle verwendet (vgl.*

*<https://tools.ietf.org/html/rfc6066#section-8> und bspw.*

*[http://nginx.org/en/docs/http/nginx\\_http\\_ssl\\_module.html#ssl\\_stapling](http://nginx.org/en/docs/http/nginx_http_ssl_module.html#ssl_stapling) ).*

Um dies zu ermöglichen, muss der Paketfilter entsprechende stateful-Firewall-Regeln gemäß A\_14019-\* und A\_19126 definieren.

## **A\_19126-02 -Access Gateway, OCSP-Status für das OCSP-Stapling**

Der Paketfilter der Komponente Access Gateway MUSS bezüglich des OCSP-Stapling (vgl.A\_24913-\*) folgende Vorgaben umsetzen:

1. Für das vom Aktensystem-Anbieter erworbene TLS-Zertifikat (vgl. Hinweis zu A\_14019-01) MUSS die Komponente initial die IP-Adresse (ggf. die IP-Adressen) des entsprechenden OCSP-Responers ermitteln.
2. Diese IP-Adresse(n) MÜSSEN gemäß A\_14019-01 per stateful-Firewalling Verbindungen von der HTTPS-Schnittstelle an den OCSP-Responder erlaubt werden.
3. Gemäß OCSP-Stapling (<https://tools.ietf.org/html/rfc6066#section-8> ) MUSS die Komponente regelmäßig eine OCSP-Response vom entsprechenden OCSP-Responder beziehen (Die Regelmäßigkeit wird vom zertifikatsausgebenden TSP und der Gültigkeitsdauer dessen OCSP-Responses bestimmt).
4. Die OCSP-Responses MÜSSEN von der Komponente geprüft werden (Signaturprüfung, CertID in der OCSP-Response passt zum angefragten Zertifikat). Falls eine der Prüfung ein nicht-positives Ergebnis liefert, so MUSS die erhaltene OCSP-Response verworfen werden.
5. Sollte die letzte in der Komponente vorhandene OCSP-Response zeitlich nicht mehr gültig sein (bspw. der OCSP-Responder im Internet war länger nicht erreichbar), so MUSS diese OCSP-Response verworfen werden und ein von einem Klienten (ePA FdV) initiiertes TLS-Verbindungsaufbau der HTTPS-Schnittstelle ohne OCSP-Stapling durchgeführt werden.

[<=]

## **A\_14776 -Access Gateway, Richtlinien zum TLS-Verbindungsaufbau**

Die Komponente Access Gateway MUSS sich beim TLS-Verbindungsaufbau gegenüber dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren. Das Zertifikat MUSS an die Schnittstelle der Proxy-Komponente gebunden werden.[<=]

### 3.19.1.2 Redundanz

Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec\_Perf#3.18.1.3]. Die Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Access Gateways.

Die Auswahl der Access Gateways wird durch das ePA-Frontend des Versicherten aus einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des Access Gateways kann der Anbieter des ePA-Aktensystems durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn jeder Versicherte mit existierendem Konto beim Anbieter des ePA-Aktensystems oder dessen berechtigter Vertreter die Möglichkeit zum Verbindungsaufbau hat.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen Access Gateways ist über grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern einzusetzen, so dass jedes einzelne Access Gateway im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

#### **A\_14026 -Access Gateway, Redundanz der Paketfilter im Access Gateway**

Die Komponente Access Gateway MUSS sicherstellen, dass bei Ausfall eines von mehreren Paketfiltern die verbleibenden Paketfilter in demselben Standort den Datenverkehr aller Mandanten des ausgefallenen Paketfilters zusätzlich übernehmen können.[<=]

### 3.19.1.3 Konfiguration

#### **A\_14030 -Access Gateway, Verhalten des Access Gateways bei Vollauslastung**

Die Komponente Access Gateway MUSS den Paketfilter Internet so konfigurieren, dass bei Vollauslastung der Systemressourcen im ePA-Aktensystem keine weiteren Verbindungen angenommen werden.[<=]

Durch die Zurückweisung von Verbindungen wird sichergestellt, dass das ePA-Frontend des Versicherten einen Verbindungsaufbau mit einem anderen Access Gateway des jeweiligen ePA-Aktensystems versucht, bei dem die erforderlichen Ressourcen zur Verfügung stehen.

### 3.19.1.4 Adressierung

#### *3.19.1.4.1 Access Gateway zum Transportnetz Internet*

#### **A\_14031 -Access Gateway, IPv4-Adressierung der Internetschnittstellen des Access Gateways**

Der Anbieter des ePA-Aktensystems MUSS jedem Access Gateway genau eine öffentliche IPv4-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentlichen IP-Adressen des Access Gateways MÜSSEN vom Anbieter des ePA-Aktensystems zur Verfügung gestellt werden.[<=]

#### **A\_14032 -Access Gateway, IPv6-Adressierung der Internetschnittstellen des Access Gateways**

Der Anbieter des ePA-Aktensystems SOLL jedem Access Gateway eine IPv6-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentliche IPv6-Adresse MUSS vom Anbieter des Access Gateways zur Verfügung gestellt werden.[<=]

#### 3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz

Die Adressen des ePA-Aktensystems am Übergang zur TI werden vom Anbieter des Zentralen Netzes aus dem Adressblock TI\_Zentral zugewiesen.

### 3.19.2 Proxy für das VAU-Protokoll

Das Access Gateway leitet Anfragen vom ePA-FdV über den VAU-Kanal an die zuständige VAU-Instanz weiter, damit diese dort in der User Session des Versicherten verarbeitet werden können.

#### **A\_24331 -Access Gateway - Data Proxy**

Das Access Gateway MUSS die VAU-Protokoll-Kommunikation des ePA-Frontend des Versicherten an die zuständige VAU-Instanz weiterleiten.【<=】

### 3.19.3 Tracing in Nichtproduktivumgebungen

Für die Fehlersuche - insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase - hat es sich als notwendig erwiesen, dass ein Fehlersuchender den Klartext der Kommunikation zwischen ePA-Client und VAU-Instanz mitlesen kann. (vgl. auch 2.5- Tracing in Nichtproduktivumgebungen )

Das Access Gateway stellt Informationen über die aktuell verfügbaren Sensorpunkte im AS bereit. Weiterhin exponiert das Access Gateway die Daten der Sensorpunkte über TCP (i. S. v. nicht TLS-gesichert) bspw. über Port 8001,...,8009. Die dort von den Sensorpunkten ge-streamten Daten sind nur Testdaten, also keine Echtdaten, d. h. sie haben keinen Schutzbedarf bezüglich Vertraulichkeit. Um die exponierten Sensordaten-Punkte vor DoS-Angriffen zu schützen, erlaubt das Access Gateway im Fall der Fälle die TCP-Ports auf IP-Layer über Firewall-Regeln abzusichern.

#### **A\_21890-01 -Access Gateway, Sensorpunkt für Nichtproduktivumgebungen**

Die Komponente Access Gateway MUSS genau in Nichtproduktivumgebungen:

- die Daten der Sensorpunkte des Aktensystems auf TCP-Ports (bspw. ab Port 8000) öffentlich (ggf. auch ohne TLS-Sicherung) im Internet zur Verfügung stellen, indem die aktuell an den Sensorpunkten auflaufenden Daten auf dem TCP-Port am Access Gateway öffentlich gestreamt werden.
- die Möglichkeit bieten, den Zugriff auf diese TCP-Ports durch Firewall-Einstellungen auf IP-Layer zu beschränken.

Weiterhin MUSS das Access Gateway über die URL /tracingpoints Informationen über die aktuell im AS verfügbaren und damit auch im Access Gateway öffentlich exponierten Sensorpunkt-Daten als JSON-Array (=> Response-Type 'application/json') der folgenden Form bereitstellen:

```
[
  {
    "name" : "zentraler Tigerproxy",
    "port" : 8001,
    "DoS-protection-type" : „secret_url“
    "DoS-protection-port" : „udp/46789“
  },
  {
    "name" : "Extra Senor VAU RZ2/B1/R1",
    "port" : 8002,
    "DoS-protection-type" : „ssh_tunnel“
    "DoS-protection-port" : „tcp/46790“
  },
  ...
]
```



Sollten keine Sensorpunkte aktuell im AS aktiviert sein (bspw. bei Lasttests) so ist das Array leer: [ ].

Sollte es keinen optionalen DoS-Schutzmechanismus gemäß A\_22582-\* geben, so fallen die DoS-\* Attribute in der o. g. Datenstruktur weg (sind nicht existent).

Die einzelnen Felder des Arrays sind associative array (oder auch maps oder dictionaries genannt). Diese KÖNNEN neben "name" und "port" beliebige vom AS definierbare, weitere key-value-Paare enthalten. Der Eintrag "port" gibt an, an welchem öffentlich erreichbaren TCP-Port des Access Gateway die Sensordaten des entsprechenden Sensors abrufbar sind (gestreamt werden).

**[<=]**

*Hinweis zu A\_21890-\*: Die semistatische JSON-Datei, welche ein Client unter dem Pfad „/tracingpoints“ erhalten kann, ist eine einfache Form von Service-Discovery. Damit kann ein Client (Fehlersuchende(r)) erfahren, welche Tracing-Quellen es aktuell im AS gibt i. S. v. welche Tracing-Quellen ein Client zur Fehlersuche aktuell verwenden kann.*

### **A\_22582 -Tracing in Nichtproduktivumgebungen, DoS-Schutz**

Die Komponente Access Gateway KANN Sicherheitsmechanismen bereitstellen und aktivieren, die es genau in Nichtproduktivumgebungen ermöglichen, temporär, automatisiert und nur nach erfolgreicher Authentifizierung die TCP-Ports für das Streaming der Sensorpunkte für Clients nach A\_21890-\* freizuschalten. **[<=]**

*Hinweis zu A\_22582-\*: In den Nichtproduktivumgebungen darf es keine Echtdaten geben. Es dürfen sich dort nur Daten befinden, deren Schutzbedarf bezüglich Vertraulichkeit niedrig ist. Der optionale Schutzmechanismus nach A\_22582-\* braucht nur einen einfachen DoS-Schutz leisten gegen einen Angreifer mit niedrigen Angriffspotential. Der Anbieter ist, sofern er einen solchen Mechanismus einsetzen möchte, frei, dafür den Mechanismus selbst zu wählen. Er wählt dann bei "DoS-protection-type" (vgl. A\_21890-\*) einen selbstdefinierten (möglichst sprechenden) Namen.*

Beispiele für Umsetzungsmöglichkeiten:

1. Es gibt im Access Gateway eine geheime URL (bspw. /tracing/964b059de83d20581f43dd1b867d740c). Ein Client kennt das Geheimnis und ruft diese URL auf. Daraufhin wird im Access Gateway für die IP-Adresse des Clients die Tracing-Quelle im Access Gateway frei geschaltet (TCP-Port 8000, ... ).
2. Die gematik stellt eine Beispielimplementierung zur Verfügung. Dort gibt es einen UDP-Server (Access Gateway) und einen UDP-Client (Fehlersuchende), die beide ein gemeinsames HMAC-Geheimnis teilen. Wenn der Client die aktuelle Zeit und dessen IP-Adresse per HMAC authentisiert dem UDP-Server sendet, so schaltet der UDP-Server nach erfolgreicher Prüfung des HMACs den entsprechenden TCP-Port für die authentifizierte IP-Adresse des Clients frei.
3. Auf dem Access Gateway läuft ein SSH-Daemon. Der öffentliche Authentisierungsschlüssel eines Clients ist dort als gültiger Nutzer konfiguriert (Login-Shell: /bin/false). Die Tracing-Quellen im Access Gateway sind so konfiguriert, dass sie nur mittels authentisierten SSH-Port-Forwarding (<https://www.ssh.com/academy/ssh/tunneling/example>) erreichbar sind.

## **3.19.4 Übergreifende Festlegungen**

### **A\_14249 -Komponente Access Gateway - Separierung der Schnittstellen für verschiedene Umgebungen**

Die Komponente Access Gateway MUSS die Bereitstellung von Schnittstellen für die Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen Umgebungen der TI (RU/TU, PU) sicherstellen und voneinander separieren. **[<=]**

### **A\_14034 -Access Gateway, Übergang des ePA-Aktensystems zur TI**

Die Komponente Access Gateway MUSS sicherstellen, dass der Zugriff auf Dienste der TI ausschließlich über einen Sicheren Zentralen Zugangspunkt (SZZP) erfolgt. [≤]

**A\_14036 -Access Gateway, Synchronisierung der Komponenten mit den Stratum-1-NTP-Servern der TI**

Die Komponente Access Gateway MUSS alle Komponenten seines Access Gateways mit den Stratum-1-NTP-Servern der TI synchronisieren. [≤]

**A\_13879 -Access Gateway, Serverseitige Authentisierung**

Die Komponente Access Gateway MUSS sich gegenüber dem ePA-Frontend des Versicherten beim Aufbau der TLS-Session durch sein ExtendedValidation-Zertifikat authentisieren. Die Beschaffung des Zertifikats erfolgt durch den Anbieter über eine öffentliche CA. [≤]

**A\_14033 -Access Gateway, TLS Verschlüsselung**

Die Komponente Access Gateway MUSS sicherstellen, dass jede Kommunikation mit dem ePA-Frontend des Versicherten TLS verschlüsselt erfolgt. [≤]

Die Verwendung der SoapAction ermöglicht einer Reverse-Proxy-Komponente innerhalb des Access Gateways, die Nachrichten zu verarbeiten, ohne die http-Payload zu untersuchen.

**A\_13876 -Access Gateway, Kein direkter Zugriff auf Dienste der zentralen TI-Plattform**

Die Komponente Access Gateway MUSS einen direkten Zugriff aus dem Internet auf Dienste der zentralen TI-Plattform verhindern. [≤]

**A\_14016 -Access Gateway , Schutz vor Angriffen aus dem Internet**

Die Komponente Access Gateway MUSS für alle vom Internet erreichbaren Schnittstellen Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS Lösungen verhindert werden. [≤]

**A\_15196 -Access Gateway, Schutz vor volumetrischen DoS-Angriffen**

Die Komponente Access Gateway MUSS bei Beauftragung eines qualifizierten Dienstleisters zum Schutz vor volumetrischen DoS-Angriffen Kriterien des BSI zur Auswahl qualifizierter Dienstleister umsetzen. [≤]

Als Maßnahme gegen volumetrische Denial-of-Service-Angriffe wird die Verwendung von DNS- oder BGP-Routing-Diensten empfohlen. Hinweise des BSI:

[https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos_node.html).

## 3.20 Data Submission Service

Die Daten der elektronischen Patientenakten sollen nach § 363 Absatz 1 SGB V für die in § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszwecke zugänglich gemacht und hierfür in pseudonymisierter Form automatisiert von den ePA-Aktensystemen an das Forschungsdatenzentrum Gesundheit (FDZ) nach § 303d SGB V übermittelt werden, sofern Versicherte dem nicht widersprochen haben.

Neben dem FDZ und den ePA-Aktensystemen ist die Vertrauensstelle (VST) nach § 303c SGB V im Prozess involviert. Deren Aufgabe ist es, die von den ePA-Aktensystemen erhaltenen Lieferpseudonyme in periodenübergreifende Pseudonyme umzuwandeln und diese an das FDZ zu übermitteln.

Der Data Submission Service im Aktensystem übernimmt in der Übermittlung der pseudonymisierten medizinischen Daten folgende Aufgaben:

- Erstellung der Lieferpseudonyme (auf Basis der KVNR) und der Arbeitsnummern

- Registrierung der Arbeitsnummer mit dem zugehörigen Lieferpseudonym bei der Vertrauensstelle
- Pseudonymisierung der medizinischen Daten
- Verknüpfung der pseudonymisierten medizinischen Daten mit der Arbeitsnummer
- Übermittlung der pseudonymisierten medizinischen Daten und der zugehörigen Arbeitsnummern an das Forschungsdatenzentrum Gesundheit

Die Übermittlung der Daten erfolgt blockweise. D.h. es wird ein Paket von pseudonymisierten medizinischen Daten mit zugehörigen Arbeitsnummern aus verschiedenen Aktenkonten zusammengestellt (Datenpaket FDZ) und alle für dieses Paket benötigten Arbeitsnummern und Lieferpseudonyme mit einem Mal bei der VST registriert (Datenpaket VST). Die Datenpakete haben eine anbieterübergreifend eindeutige SubmissionID und die SubmissionID zusammengehöriger Datenpakete VST und FDZ ist identisch.

Für die Übermittlung wird zwischen Aktensystem und VST, sowie Aktensystem und FDZ jeweils ein beidseitig authentisierter VAU-Kanal aufgebaut, auf dem sich die Dienste VST und FDZ mit einer Identität ID.FD.AUT mit ihren entsprechenden Rollen authentisieren.

Der Versicherte kann mit Hilfe seines ePA-FdVs oder über die Ombudsstelle des Kostenträgers der Übermittlung seiner pseudonymisierten medizinischen Daten an das FDZ widersprechen oder die möglichen Sekundärnutzungszwecke seiner übermittelten pseudonymisierten medizinischen Daten im FDZ einschränken. Dies erfolgt über das Consent Decision Management im Aktensystem.

### 3.20.1 Erstellung von Arbeitsnummern und Lieferpseudonymen

Der Data Submission Service erzeugt eindeutige Arbeitsnummern und Lieferpseudonyme, um die pseudonymisierten medizinischen Daten in der Übermittlung an das FDZ eindeutig zuordnen zu können.

#### **A\_26211 -Data Submission Service - Erstellung des Lieferpseudonyms**

Der Data Submission Service MUSS das Lieferpseudonym des Versicherten gemäß [I\_VST] unter Verwendung der KVNR des Versicherten erstellen.[<=]

#### **A\_26409 -Data Submission Service - keine Erstellung von LP für Validierungsaktenkonten**

Der Data Submission Service DARF KEINE Lieferpseudonyme für KVNRn von Validierungsaktenkonten erstellen.[<=]

#### **A\_26212 -Data Submission Service - Erstellung der Arbeitsnummer**

Der Data Submission Service MUSS für die Arbeitsnummer einen Zufallswert mit einer Mindestentropie von 120 Bit erzeugen und die Kodierung aus [I\_VST] verwenden.[<=]

#### **A\_26410 -Data Submission Service - keine Erstellung von AN für Validierungsaktenkonten**

Der Data Submission Service DARF KEINE Arbeitsnummern für Daten aus Validierungsaktenkonten erstellen.[<=]

#### **A\_26255 -Data Submission Service - Verwendungsdauer von Lieferpseudonymen und Arbeitsnummern**

Der Data Submission Service MUSS für jedes in einem Datenpaket FDZ übermittelte pseudonymisierte medizinische Datum zu einer KVNR eine neue Arbeitsnummer und ein neues Lieferpseudonym generieren.[<=]

#### **A\_26256 -Data Submission Service - Registrierung von Arbeitsnummern**

Der Data Submission Service MUSS jede Arbeitsnummer zusammen mit dem zugehörigen Lieferpseudonym in das entsprechende Datenpaket VST aufnehmen und an die Vertrauensstelle übermitteln.【<=】

### 3.20.2 Auswahl von medizinischen Daten

Der Data Submission Service muss bestimmte neue und geänderte FHIR-Ressourcen an den FDZ übertragen. Dies betrifft im ersten Schritt die Medikationsdaten aus der E-Medikationsliste und wird subsequent weiter ausgebaut.

Der Medication Service, als Quelle der Medikationsdaten zur Übertragung an den FDZ, erlaubt flexible, datenbasierte Operationen auf einzelnen FHIR-Ressourcen. Dies erfordert entsprechende Implementierung um effizient und zuverlässig die neuen und geänderten Ressourcen identifizieren können um daraus die Auswahl für die zu übertragende FHIR-Ressourcen treffen zu können.

#### **A\_26296 -Data Submission Service - Übertragung neuer und geänderter FHIR-Ressourcen**

Der Data Submission Service MUSS neue und geänderte FHIR-Ressourcen identifizieren können und daraus die Auswahl für die Übermittlung der Daten an FDZ treffen können. 【<=】

#### **A\_26297 -Data Submission Service - Einschränkung der FHIR-Ressourcen nach Änderungsdatum**

Der Data Submission Service MUSS den Zeitpunkt der letzten Übermittlung (lastSubmissionTimestamp) merken und in nachfolgenden Übermittlungen nur die Ressourcen, die sich seit diesem Zeitpunkt geändert haben, berücksichtigen. Hierfür ist das FHIR-Element meta.lastUpdated in der jeweiligen FHIR-Ressource zu verwenden.【<=】

*Hinweis: Ressourcen, die im Rahmen eines Anbieterwechsels in ein Aktenkonto übernommen werden, sind nicht erneut zu übermitteln.*

#### **A\_26298 -Data Submission Service - FHIR-Ressourcen zur Übermittlung an FDZ**

Der Data Submission Service MUSS die FHIR-Ressourcen gemäß der Tabelle "Auswahl der zu übertragenden FHIR-Ressourcen" an FDZ übertragen, dabei sind die Filter-Bedingungen (Spalte 'Filter Expression') und zu inkludierende referenzierte Ressourcen zu berücksichtigen (Spalte 'Include' sowie Tabelle "Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen").【<=】

**Tabelle 44: Auswahl der zu übertragenden FHIR-Ressourcen**

Ressourcentyp /Profil	Filter Expression	Include
MedicationRequest \${epa-medication}/epa-medication-request	status != 'active' and identifier.where(system='https://gematik.de/fhir/epa-medication/sid/rx-prescription-process-identifier').hasValue()	MedicationRequest:medication
MedicationDispense \${epa-medication}/e	status != 'in-progress' and extension('https://gematik.de/fhir/epa-medication/StructureDefinition/rx-prescription-process-identifier-	MedicationDispense:medication

pa-medication-response	extension').hasValue()	
------------------------	------------------------	--

**Tabelle 45: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen**

Ressourcentyp/Profil	Anmerkung
Medication \${epa-medication}/epa-medication	Referenziert durch MedicationRequest, MedicationDispense

### 3.20.3 Protokollierung des Datenexports an das FDZ

Ein Datenexport erfolgt immer in Verbindung mit dem Einstellen neuer oder der Änderung existierender Daten für ein Aktenkonto. Ein Datenexport nach Auswahl der Daten gemäß A\_26298 wird als Bestandteil der Protokollierung des auslösenden Ereignisses protokolliert (siehe dazu: [3.13.2.2- Medication Service](#) )

### 3.20.4 Pseudonymisierung von medizinischen Daten

Bevor medizinische Daten an das FDZ übermittelt werden dürfen, müssen diese pseudonymisiert werden und Daten mit direktem Personenbezug entfernt werden.

#### **A\_26300 -Data Submission Service - Pseudonymisierung von medizinischen Daten**

Der Data Submission Service MUSS an das FDZ zu übermittelnde medizinische Daten gemäß der Vorgaben aus [DataPseudonymization] pseudonymisieren. [ $\leq$ ]

#### **A\_26408 -Data Submission Service - keine Pseudonymisierung von Daten aus Validierungsaktenkonten**

Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem. Kapitel 2.4) pseudonymisieren. [ $\leq$ ]

#### **A\_26315 -Data Submission Service - Randomisierung der Reihenfolge des Datenpakets FDZ**

Das ePA-Aktensystem MUSS sicherstellen, dass in einem Datenpaket FDZ vor der Übermittlung die Einträge nach Arbeitsnummer (AN) aufsteigend sortiert werden. Die Arbeitsnummer (32-Byte Zufallswert, A\_26212-\*) wird dabei als natürliche Zahl (byteorder=big) interpretiert. [ $\leq$ ]

Verständnishinweis:

Die Akten werden regelmäßig nach zu übermittelnden Daten vom ePA-Aktensystem durchsucht. Dabei kann es passiert, dass in einer Akte mehrere Daten zur Übermittlung anfallen, die nach der Pseudonymisierung in einer Reihenfolge in das Datenpaket FDZ gelangen. Deshalb kann die Reihenfolge der Einträge im Datenpaket FDZ statistisch relevante Informationen über den Zusammenhang von Einträgen geben. Durch eine Randomisierung der Reihenfolge der Einträge innerhalb des Datenpakets wird dies verhindert. Die AN werden zufällig erzeugt, eine Sortierung nach AN ist deshalb eine Randomisierung der Reihenfolge.

### 3.20.5 Übermittlung der pseudonymisierten medizinischen Daten

Die Übermittlung von Datenpaketen an VST und FDZ erfolgt gemäß den Vorgaben des RKI (VST) und BfArM (FDZ) und deren Schnittstellenspezifikationen.

Die Übermittlung der pseudonymisierten Daten eines Aktenkontos für Sekundärnutzungszwecke erfolgt automatisch, sofern kein Widerspruch gegen Sekundärdatennutzung vorliegt. Die Voreinstellung ist dabei "kein Widerspruch erteilt" (siehe: 3.8.1- Widersprüche für Funktionen der ePA ). Vor der allerersten Übermittlung solcher Daten wird dem Versicherten daher eine Frist gewährt, gegebenenfalls einen Widerspruch gegen diese Sekundärdatennutzung zu formulieren.

#### **A\_26462 -Data Submission Service - Übermittlung Datenpaket nach Ablauf der Widerspruchsfrist**

Der Data Submission Service MUSS sicherstellen, dass vor der erstmaligen Übermittlung von Daten eines Aktenkontos die Widerspruchsfrist gemäß den Vorgaben des Kostenträgers abgelaufen ist. [ <= ]

Hinweis: Die erste Datenübermittlung ist die erste automatisiert mögliche Übermittlung (nach Aktivierung des Aktenkontos) und nicht die erste Datenübermittlung nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung.

Hinweis: Für eine Übermittlung nach Ablauf dieser Widerspruchsfrist oder nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung werden immer nur ab diesem Zeitpunkt neu angefallene Daten berücksichtigt, Es erfolgt keine Übermittlung von vorhandenen Daten des Aktenkontos.

#### **A\_26214 -Data Submission Service - Erstellung der SubmissionID**

Der Data Submission Service MUSS für zusammengehörige Datenpakete VST und FDZ eine gemeinsame anbieterübergreifend eindeutige SubmissionID erzeugen und diese mit den Datenpaketen übertragen. [ <= ]

#### **A\_26304 -Data Submission Service - Zufällige SubmissionID**

Der Data Submission Service MUSS sicherstellen, dass die SubmissionID ein zufällig gewählter 256-Bit Wert mit einer Mindestentropie von 120 Bit ist. [ <= ]

#### **A\_26215 -Data Submission Service - Übermittlung Datenpaket VST**

Der Data Submission Service MUSS das Datenpaket VST gemäß [I\_VST] an die Vertrauensstelle übermitteln. [ <= ]

#### **A\_26407 -Data Submission Service - keine Übermittlung von Daten aus Validierungsaktenkonten**

Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem. Kapitel 2.4) an das Forschungsdatenzentrum übermitteln. [ <= ]

#### **A\_26216 -Data Submission Service - Realisierung der Schnittstelle**

##### **I\_Data\_Submission\_Service**

Der Data Submission Service MUSS die Operationen der Schnittstelle I\_Data\_Submission\_Service gemäß [I\_Data\_Submission\_Service] umsetzen. [ <= ]

#### **A\_26217 -Data Submission Service - Verbindung zur Vertrauensstelle**

Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des Datenpakets VST ausschließlich über einen VAU-Kanal erfolgt in dem sich die Vertrauensstelle über ein Zertifikat C.FD.AUT mit professionOID gleich oid\_epa\_vst authentisiert hat. [ <= ]

#### **A\_26218 -Data Submission Service - Verbindung zum Forschungsdatenzentrum Gesundheit**

Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des Datenpakets FDZ ausschließlich über einen VAU-Kanal erfolgt in dem sich das Forschungsdatenzentrum Gesundheit über ein Zertifikat C.FD.AUT mit professionOID gleich oid\_epa\_fdz authentisiert hat. [ <= ]



**A\_26299 -Data Submission Service - Wechsel des Verschlüsselungsschlüssels für Datenpakete**

Falls die Datenpakete VST und FDZ außerhalb der VAU im System des Aktensystembetreibers gespeichert werden, MUSS der Data Submission Service sicherstellen, dass ein Schlüssel für die Verschlüsselung der Datenpakete VST bzw. FDZ maximal 4 Wochen genutzt werden kann und danach ein neuer Verschlüsselungsschlüssel mittels der Regel hsm-r8 mit Hilfe eines geänderten Ableitungsvektors abgeleitet wird. [≤]

**A\_26312 -Data Submission Service - Timeout in der Übermittlung**

Der Data Submission Service MUSS die Übermittlung der Pakete VST und FDZ erneut starten, wenn das Datenpaket FDZ nicht innerhalb von 30 Minuten nach erfolgreicher Übermittlung des Datenpakets VST abgerufen wird. [≤]

**A\_26313 -Data Submission Service - Konfiguration der Intervalle und maximalen Größe eines Datenpakets**

Der Data Submission Service MUSS folgende Parameter konfigurierbar gestalten:

- das Intervall in dem Datenpakete VST und FDZ übermittelt werden
- eine maximale Größe eines Datenpakets FDZ bei deren Erreichen die Datenpakete übermittelt werden

[≤]

**A\_26244 -Data Submission Service - Löschen von Datenpaketen nach Übermittlung**

Der Data Submission Service MUSS nach erfolgreicher Übermittlung des Datenpakets FDZ an das Forschungsdatenzentrum Gesundheit das übermittelte Datenpaket FDZ und das zugehörige Datenpaket VST lokal löschen. [≤]

**A\_26245 -Data Submission Service - Löschen von Datenpaketen bei Nicht-Übermittlung**

Der Data Submission Service MUSS das Datenpaket FDZ und das zugehörige Datenpaket VST lokal löschen, wenn das Datenpaket FDZ länger als 72 Stunden nicht an das Forschungsdatenzentrum Gesundheit übermittelt werden konnte. Die enthaltenen Widersprüche MÜSSEN in die aktuell in Erstellung befindlichen Datenpakete VST und FDZ übernommen werden. [≤]

*Hinweis: Wenn Widersprüche in ein neues Datenpaket übernommen werden, muss für jeden der Widersprüche eine neue Arbeitsnummer (AN) und ein Lieferpseudonym (LP) erstellt werden, da die bisherigen AN und LP im Kontext des zu löschenden Paketes stehen.*

**A\_26246 -Data Submission Service - Aufnahme von Widersprüchen**

Der Data Submission Service MUSS Widersprüche gegen die Freigabe von Daten zur Sekundärnutzung durch das FDZ oder Änderungen zu Sekundärnutzungszwecken, aus dem Consent Decision Management, in die aktuell in Erstellung befindlichen Datenpakete VST und FDZ übernehmen. Es MUSS sichergestellt werden, dass in einem Datenpaket FDZ für eine KVNR immer nur die zuletzt erklärten Widersprüche gegen die Übermittlung von Daten zur Sekundärnutzung durch das FDZ bzw. zu Sekundärnutzungszwecken enthalten sind. [≤]

*Hinweis: Sollte während der Erstellung eines Datenpakets FDZ mehrfach die Widersprüche für eine KVNR geändert werden, wird immer nur der letzte Stand übermittelt.*

**A\_26307 -Data Submission Service - Durchsetzung von Widersprüchen**

Falls für ein Aktenkonto ein Widerspruch gegen die Übermittlung an das FDZ eingestellt wird, MUSS der Data Submission Service sicherstellen, dass in allen zukünftig zu übermittelnden Datenpaketen VST und FDZ außer den Daten für den Widerspruch keine



Daten für dieses Aktenkonto enthalten sind.

[<=]

*Hinweis zu A\_26307:* Zum Zeitpunkt des Eingangs des Widerspruchs im Aktensystems bereits in der Übermittlung befindliche Datenpakete sind von der Anforderung ausgeschlossen. Betroffen sind jedoch auch die aktuell in Erstellung befindlichen Datenpakete VST und FDZ, bei denen die Übermittlung an die VST bzw. das FDZ noch nicht begonnen hat.

## 3.21 Push Notification Management

Nutzer von Anwendungen für Versicherte (ePA-FdV) können mittels Push Notifications direkt über Ereignisse in bestimmten Fachdiensten der TI oder des Kostenträgers auf ihren Endgeräten informiert werden. Diese Notifications erreichen einen Nutzer auch außerhalb aktiver Anmeldungen in diesen Fachdiensten. Die Ereignisse von Interesse zur Benachrichtigung des Nutzers sind dabei individuell abonnierbar.

Der Versand einer Push Notification erfolgt stets durch die einzelnen Fachdienste für Ereignisse ihrer Domäne. Die Übertragung in das Endgerät des Nutzers unter Einbindung der plattformspezifischen, externen Push-Dienste und betreiberspezifischen Push-Gateways wird für alle beteiligten Fachdienste gemeinsam durch ein Push Notification System realisiert. Dieses anwendungsübergreifende System und seine Komponenten für Push Notifications im Gesundheitswesen sind in [gemF\_PushNotification] und [PushNotificationConcept] detailliert beschrieben.

Dort sind auch die normativen Vorgaben für unterstützende Anwendungen und Fachdienste in Bezug auf Registrierung von Applikationen und Ereignissen für Push Nachrichten, Schnittstellen, sicherheitstechnische Anforderungen und notwendige Artefakte für einen interoperablen Betrieb formuliert.

### 3.21.1 Push Notification Management des ePA-Aktensystems

Das Push Notification Management des ePA-Aktensystems ist als ein spezifischer Fachdienst in dieses übergreifende System eingebunden und bedient die in [gemF\_PushNotification] geforderten und in [PushNotificationConcept] beschriebenen Schnittstellen und Verfahren.

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.

Der Nutzung des Push Notification Managements der ePA kann nicht widersprochen werden. Dieser Dienst gehört nicht zu den widerspruchsfähigen Funktionen der ePA. Versicherte, die keine Benachrichtigungen der ePA erhalten möchten, können die Benachrichtigungen durch Abwahl der Benachrichtigungskanäle oder auch generell durch den Verzicht des ePA-FdV auf eine Registrierung für Push Notifications unterbinden.

Schnittstellen, die das Push Notification Management der ePA zur Nutzung durch Clients (ePA-FdV) anbietet, sind um ePA-spezifische Verfahren und Anforderungen ergänzt und als OpenApi gemäß [I\_Push\_Notification\_Management] verfügbar.

#### **A\_27637 -Push Notification Management - Realisierung der Schnittstelle**

##### **I\_Push\_Notification\_Management**

Das Push Notification Management MUSS die Operationen der Schnittstelle I\_Push\_Notification\_Management gemäß [I\_Push\_Notification\_Management] umsetzen.

[<=]

### 3.21.2 Registrierung eines ePA-FdV als Pusher

(siehe auch: [gemF\_PushNotification]#Kapitel "Pusher registrieren")

Ein Versicherter kann registrierte Geräte (im Sinne des Device Managements gemäß 3.12-Device Management ) zur Nutzung seiner aktivierten elektronischen Patientenakte auch für den Erhalt von Push Nachrichten nutzen, sofern das übergreifende Push Notification System die technologische Infrastruktur für Benachrichtigungen an den Geräte-, bzw. Betriebssystemtyp des Versichertengeräts unterstützt. Dazu kann die ePA-FdV-Anwendung jedes dieser Geräte als ePA-FdV Instanz, bzw. 'Pusher', im eigenen Aktenkonto des Versicherten registriert werden.

Die ePA-FdV Instanz Registrierung eines Gerätes als Pusher erfolgt immer durch und für das auf diesem Gerät installierte ePA-FdV und unter Nutzung der Schnittstelle [I\_Push\_Notification\_Management]. Über diese Schnittstelle werden existierende Registrierungen auch aktualisiert und wieder entfernt.

Die Daten der Registrierungen, inklusive des kryptographischen Materials der Schlüsselableitungen und der Auswahl der Benachrichtigungskanäle, sind Bestandteil des Aktenkontos und werden dort gespeichert. Pro registriertem Gerät kann jeweils nur eine ePA-FdV Instanz im Aktenkonto hinterlegt sein und eine Registrierung gilt immer nur für genau eine bestimmte ePA-FdV Instanz. Eine ePA-FdV Instanz Registrierung ist daher fest an eine Device Registration gebunden.

#### **A\_27638 -Push Notification Management- Speicherung der Daten**

Das Push Notification Management MUSS alle Daten des Dienstes für einen Versicherten im SecureDataStorage des Aktenkontos des Versicherten speichern. [≤]

#### **A\_27640 -Push Notification Management - automatisches Löschen der Registrierung einer ePA-FdV Instanz**

Das Push Notification Management MUSS sicherstellen, dass eine existierende Registrierung einer ePA-FdV Instanz und die dazugehörigen Daten vollständig und automatisch gelöscht werden, wenn die Device Registration des assoziierten Geräts im Device Management des Aktensystems gelöscht wird. [≤]

#### **A\_27639 -Push Notification Management - eindeutiger pushKey**

Das Push Notification Management MUSS sicherstellen, dass der pushKey einer Registrierung einer ePA-FdV Instanz eindeutig ist und es keine zwei oder mehr Registrierungen mit gleichem pushKey gibt. [≤]

Bei jedem Versand einer Push Nachricht an das Push Gateway kann dieses in den Rückgabewerten der Push Operation einen Eintrag oder eine Liste veralteter, bzw. ungültiger pushKeys melden. Eine weitere Nutzung solcher Registrierungen, bzw. pushKeys, soll unterbleiben. Die assoziierten Registrierungen von ePA-FdV-Instanzen werden daher aus dem Aktenkonto entfernt.

#### **A\_27682 -Push Notification Management - Entfernen ungültiger pushKeys**

Das Push Notification Management MUSS Registrierungen von ePA-FdV-Instanzen löschen, wenn pushKeys dieser Registrierungen durch das Push Gateway als ungültig gemeldet werden. [≤]

*Hinweis: Es werden nur Registrierungen aus dem versendenden Aktenkonto entfernt. Eventuelle Rückmeldungen des Push Gateways zu pushKeys, die nicht oder nicht mehr mit dem versendenden Aktenkonto verbunden sind, werden ignoriert.*

### 3.21.3 Push Notification Channels

(siehe auch: [gemF\_PushNotification]#Kapitel "Channel/ Trigger Konfiguration")

Das ePA-Aktensystem bietet eine Auswahl an Channels zu Ereignissen, über deren Aktivität ein Versicherter durch Push-Benachrichtigungen informiert werden kann. Der jeweilige Nachrichteninhalt beschreibt dabei in Kurzform das auslösende Ereignis.

Die Grundeinstellung für den Versand von Push-Benachrichtigungen an neu erstellten Registrierungen für ePA-FdV-Instanzen lautet für jeden Channel zunächst deaktiviert ('disabled' - keine Benachrichtigung für diesen Kanal). Ein Versicherter kann diese Grundeinstellung individuell für jede seiner ePA-FdV-Instanzen jederzeit ändern und die Benachrichtigung pro Channel aktivieren ('enabled' - Benachrichtigungen für diesen Kanal), bzw. auch wieder deaktivieren.

Die Verwaltung der individuellen Channelkonfiguration des ePA-Aktenkontos für eine registrierte ePA-FdV-Instanz erfolgt über die Schnittstelle [I\_Push\_Notification\_Management].

#### **A\_27641-01 -Push Notification Management - Push Notification Channels**

Das Push Notification Management MUSS ausschließlich für die folgenden Ereignisse Push Nachrichten erstellen können, wenn das Ereignis durch einen Nutzer der definierten Nutzergruppe ausgelöst wird und die damit verbundene Operation erfolgreich (nicht durch einen Fehler abgebrochen) ist.

Ereignis	channelId	Beschreibung	Nutzergruppen
Neues Dokument eingestellt	xds.put	Ein Dokument wurde durch einen Nutzer neu eingestellt.	alle, außer Versicherter
Dokument aktualisiert	xds.update	Ein aktualisiertes Dokument wurde durch einen Nutzer eingestellt.	alle, außer Versicherter
Befugnis erstellt	entitle.put	Eine Befugnis wurde durch das ePA-FdV erstellt.	nur Vertreter
Befugnis gelöscht	entitle.del	Eine existierende Befugnis wurde durch das ePA-FdV gelöscht.	nur Vertreter
Befugniserstellung im Behandlungskontext	entitle.ps	Eine Befugnis wurde mittels VSDM-Prüfnachweis, bzw. PoPP, erstellt.	alle, außer FdV Nutzer
Verbergen aufgehoben (Dokument)	constraint.del	Ein zuvor verborgenes Dokument ist wieder sichtbar.	nur Vertreter
Verbergen aufgehoben (dynamischer Ordner)		Ein zuvor verborgener dynamischer Ordner ist wieder sichtbar.	nur Vertreter
Verbergen aufgehoben (Kategorie)		Eine zuvor verborgene Kategorie wieder	nur Vertreter

		sichtbar.	
--	--	-----------	--

[&lt;=]

### 3.21.4 Push Notification Nachrichteninhalte

(siehe auch: [gemF\_PushNotification]#Kapitel "Operation Notify")

Für jedes ausgelöste Ereignis eines Push Channels wird eine Push Notification erstellt. Die Nachrichtendaten für ein Ereignis werden strukturiert gemäß Schema angeordnet und nach den Vorgaben in [gemF\_PushNotification#A\_27610-\*] auf konstante Länge aufgefüllt.

#### A\_27645 -Push Notification Management - Push Notification Datenstruktur

Das Push Notification Management MUSS die Nachrichtendaten einer Push Nachricht für den Versand gemäß [Schema\_PushNotifications] strukturieren.[<=]

Es gibt eine maximal erlaubte Größe für Nachrichteninhalte, die durch das Push Notification System [gemF\_PushNotification] vorgegeben wird. Es muss sichergestellt werden, dass erzeugte Nachrichteninhalte diese Größe nicht übersteigen.

#### A\_27673 -Push Notification Management - Verkürzung der Nachrichteninhalte

Falls der erzeugte Nachrichtinhalt die maximal erlaubte Größe für Nachrichteninhalte übersteigt MUSS das Push Notification Management die Elemente actor, title, who, folderTitle so verkürzen, dass die maximal erlaubte Größe für Nachrichteninhalte gerade nicht überschritten wird.[<=]

*Hinweis: Es müssen nicht alle aufgeführten Elemente gleichzeitig verkürzt werden.*

#### A\_27674 -Push Notification Management - Art der Verkürzung

Falls Elemente einer Nachricht verkürzt werden, dann sollen diese so verkürzt werden, dass:

- am Ende der Zeichenkette Zeichen entfernt werden
- die Verkürzung mit "..." angezeigt wird.

[&lt;=]

*Hinweis: Es kann sinnvoll sein, nur das längste kürzbare Element zu kürzen. Es wird empfohlen eine Mindestlänge von 50 Bytes nicht zu unterschreiten.*

### 3.21.5 Versenden von Push Nachrichten

(siehe auch: [gemF\_PushNotification]#Kapitel "Operation Notify" und [PushNotificationConcept]#Concept: "Verschlüsselung des Benachrichtigungsinhalts")

Eine erstellte Push Nachricht wird an jede ePA-FdV-Instanz mit einer Registrierung im Aktenkonto gesendet, wenn für diese der assoziierte Kanal abonniert wurde (Konfiguration channelId == enabled).

Die längenkorrigierte Nachricht wird jeweils mit dem für den aktuellen Monat gültigen SchlüsselAES/CGM-Schlüssel-Jahr-Monat der Registrierung für jede adressierte ePA-FdV-Instanz verschlüsselt. Das Verschlüsselungsergebnis ist der Inhalt von ciphertext der notification für den Versand ([I\_Push\_Gateway]).

#### A\_27651 -Push Notification Management - verpflichtende Verschlüsselung der Nachrichteninhalte

Das Push Notification Management MUSS sicherstellen, dass ausschließlich verschlüsselte Nachrichteninhalte als Push Nachricht versendet werden.[<=]

Jedes einer Push Nachricht zugrundeliegenden Ereignis erzeugt auch einen Protokolleintrag im Audit Event Service. Die Menge der korrespondierenden Protokolleinträge ergibt dadurch im Aktenkonto ein Archiv der Push Ereignisse. Damit Clients ein Push Ereignis zu einem späteren Zeitpunkt, also nachdem die Push Nachricht im Client selbst schon gelöscht ist, restaurieren können, wird jeder Push Nachricht auch der Identifier des Protokolleintrags angehängt.

#### **A\_27644 -Push Notification Management - Referenz auf Protokolleintrag**

Das Push Notification Management MUSS den eindeutigen Identifier Resource.id des zu einem Push Notification Ereignis gehörenden Protokolleintrags (AuditEvent) des Aktenkontos im Feld notification/identifizier einer Push Notification angeben.【<=】

### **3.21.6 Protokollierung**

#### **A\_27636 -Push Notification Management- Protokollierung der ePA-FdV-Instanz-Registrierung**

Das Push Notification Management MUSS für Erstellung und Änderung (CUD) von ePA-FdV-Instanz-Registrierungen jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen. Dabei ist folgende Wertbelegung zu berücksichtigen:

**Tabelle 46: Constraint Management Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die API
	"object"		Bei intern ausgelösten Änderungen (internes Löschen einer ePA-FdV-Instanz-Registrierung nach Löschen Device Registration)
AuditEvent.action	C, U, D		
AuditEvent.entity.name	"PushNotificationManagement"		
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"DisplayNamePusher"	<device_display_name aus der Pusher Registrierung>	
	"DisplayNameDevice"	<displayName der Device Registration>	

【<=】

*Hinweis: DisplayNamePusher und DisplayNameDevice können gleich lauten.*

## A\_27662 -Push Notification Management- Protokollierung von Änderungen der Channel Konfiguration

Das Push Notification Management MUSS für Änderungen der Channel-Konfiguration jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

**Tabelle 47: Constraint Management Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die API
	"object"		Bei intern ausgelösten Änderungen (internes Löschen einer ePA-FdV-Instanz-Registrierung nach Löschen Device Registration)
AuditEvent.action	U		
AuditEvent.entity.name	"PushNotificationManagement"		
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"channelId"	<[enabled, disabled]>	value wird auf den neuen Wert gesetzt
	Die Kardinalität der <channelId>   <value> Paare ist 1 .. *. Für jeden geänderte Wert eines Channels ist ein Eintrag erforderlich. Erfolgt der Protokolleintrag aufgrund Löschung eines Pushers, so sind die Channels zu erfassen, die vor der Löschung den Wert enabled hatten		
	"DisplayNamePusher"	<device_display_name aus der Pusher Registrierung>	
	"DisplayNameDevice"	<displayName der Device Registration>	

**[<=]**

*Hinweis: Die Speicherung von Protokolleinträgen erfordert einen berechtigten Benutzer, um den Zugriff auf den sicheren Datenspeicher zu gewährleisten. Daher wird die Erstellung von Protokolleinträgen immer übersprungen und es wird kein Protokolleintrag gespeichert, wenn diese Bedingung nicht erfüllt ist.*

## 3.22 Schnittstellen (OpenAPI)

Hinweis: Die Vorgaben in den beschreibenden Dateien der REST-Schnittstellen (yaml) sind normativ für den Anbieter der Schnittstellen. Die Anforderungen im vorliegenden Dokument ergänzen diese Vorgaben, insbesondere, wenn diese für sicherheitstechnische Gutachten erforderlich sind.

### 3.22.1 Übersicht der Schnittstellen des Aktensystems

**Tabelle 48: Übersicht der Schnittstellen des Aktensystems**



<b>Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)</b>	
<b>I_Consent_Decision_Management</b>	
Schnittstelle des Consent Decision Managements gemäß [I_Consent_Decision_Management]	
updateConsentDecision	Diese Operation erlaubt dem FdV und der Ombudsstelle die Änderung des Zustand des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA für eine Funktion.
getConsentDecisions	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen aller Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der ePA.
getConsentDecision	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen eines Widerspruchs einer Funktion gegen die Nutzung von widerspruchsfähigen Funktionen.
updateDataUsagePurposes	Diese Operation erlaubt dem FdV und der Ombudsstelle die Änderung der Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden.
getDataUsagePurposes	Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht der aktuellen Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden bzw. wurden.
getUserSpecificMedicationDenyList	Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht, welche LEI keinen Zugriff auf den Medication Service haben.
setUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI in die Liste der LEIs aufzunehmen, die keinen Zugriff auf den Medication Service haben.
getUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine bestimmte LEI aus der Liste der LEIs anzuzeigen, die keinen Zugriff auf den Medication Service haben.

deleteUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI aus der Liste der LEIs zu entfernen, damit diese LEI wieder Zugriff auf den Medication Service haben kann.
<b>I_Constraint_Management_Insurant</b>	
Schnittstelle des Constraint Managements gemäß [I_Constraint_Management_Insurant]	
getDenyPolicyAssignments	Diese Operation gibt eine Liste aller konfigurierten Einträge der General Deny Policy aus.
setPolicyAssignment	Diese Operation fügt der General Deny Policy einen neuen Eintrag hinzu.
deletePolicyAssignment	Diese Operation löscht einen bestimmten Eintrag der General Deny Policy.
<b>I_Entitlement_Management</b>	
Schnittstelle des Entitlement Management gemäß [I_Entitlement_Management] zur Vergabe von Befugnissen und Befugnisausschlüssen	
setEntitlementPs	Diese Operation fügt eine Befugnis für eine Leistungserbringerinstitution in einer Behandlungssituation hinzu (VSDM Prüfnachweis).
setEntitlementPsV2	Diese Operation fügt eine Befugnis für eine Leistungserbringerinstitution in einer Behandlungssituation hinzu (PoPP).
getEntitlements	Diese Operation erlaubt dem FdV den Abruf aller aktuellen Befugnisse.
getEntitlement	Diese Operation erlaubt dem FdV den Abruf einer bestimmten Befugnis.
setEntitlement	Diese Operation erlaubt dem FdV das Setzen einer Befugnis für einen Nutzer.
deleteEntitlement	Diese Operation erlaubt dem FdV den Abruf das Löschen einer existierenden Befugnis.
getBlockedUserPolicyAssignments	Diese Operation erlaubt dem FdV den Abruf der aktuell vorhandenen Befugnisausschlüsse.

setBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Befugnisausschluss für einen Nutzer.
getBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Abruf eines bestimmten Befugnisausschlusses.
deleteBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV die Aufhebung eines Befugnisausschlusses.
<b>I_Entitlement_Management_EU</b>	
Schnittstelle des Entitlement Management EU-Zugriff gemäß [I_Entitlement_Management_EU] zur Verwaltung Befugnis EU-Zugriff	
setEntitlementEu	Diese Operation erlaubt dem FdV das Setzen einer Befugnis EU-Zugriff für einen Versicherten.
getAccessCode	Diese Operation erlaubt dem FdV den Abruf des Zugriffscodes für die Befugnis EU-Zugriff.
<b>Render API: PDF Audit</b>	
Schnittstelle des Audit Event Service gemäß [IG_Basic] zum Abruf der Protokolldaten in lesbarer Form	
renderAuditEventsToPDF	Diese Operation erlaubt FdV und Ombudsstelle den Abruf der Protokolldaten als PDF.
<b>Query API: AuditEvent</b>	
Schnittstelle des Audit Event Service gemäß [IG_Basic] zum Abruf der Protokolldaten im FHIR-Format	
listAuditEvents_AuditEventSvc	Diese Operation ermöglicht die Suche nach AuditEvent Instanzen.
getAuditEventById_AuditEventSvc	Diese Operation ermöglicht das Lesen einer AuditEvent Instanz.
<b>I_Health_Record_Relocation_Service</b>	
Schnittstelle zur Steuerung des Aktenumzugs aus der Umgebung des Kostenträgers	
startPackageCreation	Diese Operation initiiert die Erstellung eines Export Pakets für den Umzug

	eines Aktenkontos zu einem neuen Anbieter.
--	--

startPackageImport	Diese Operation initiiert den Import eines Export Pakets in ein neu erstelltes Aktenkonto.
<b>I_Device_Management_Insurant</b>	
Schnittstelle zur Geräteverwaltung aus der Umgebung des Versicherten	
getDevice	Diese Operation ruft eine bestimmte Geräteregistrierung ab.
getDevices	Diese Operation ruft alle Geräteregistrierungen ab.
updateDevice	Diese Operation ändert den Displayname einer Geräteregistrierung.
deleteDevice	Diese Operation löscht eine bestimmte Geräteregistrierung.
registerDevice	Diese Operation erzeugt eine neue Geräteregistrierung und neue Geräteparameter
confirmPendingDevice	Diese Operation bestätigt eine neue Geräteregistrierung mit einem Geräteregistrierungscode
getDeviceAttestation	Diese Operation ruft die Bestätigung einer Geräteregistrierung am Home-AS ab.
<b>I_Authorization_Service</b>	
Schnittstelle der Autorisierung für den Login	
getFHIRVZDtoken	Diese Operation bezieht das search-access-token für den Zugriff auf den FHIR VZD vom Aktensystem
getNonce	Diese Operation bezieht einen eindeutigen einmalig generierten Zufallswert für die Client Attestierung
sendAuthorizationRequestSC	Diese Operation initiiert die Authentifizierung eines Leistungserbringers
sendAuthorizationRequestFdV	Diese Operation initiiert die Authentifizierung eines ePA-FdV
getFreshnessParameter	Diese Operation erzeugt einen

	Frischeparameter für die Authentisierung mittels Bearer Token
--	--

sendAuthorizationRequestBearerToken	Diese Operation initiiert die Authentifizierung über Bearer Token
sendAuthCodeSC	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
sendAuthCodeFdV	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
logoutFdV	Diese Operation beendet aktiv die Sitzung
<b>I_Medication_Service_eML_Render</b>	
renderEMLasHTML	Diese Operation gibt die Medikationsliste im html-Format zurück.
renderEMLasPDF	Diese Operation gibt die Medikationsliste im PDF/A-Format zurück.
<b>I_Medication_Service_FHIR</b>	
REST-Schnittstelle zum Abruf der Medikationsdaten im FHIR-Format	
<b>I_Email_Management</b>	
getEmailaddress	Diese Operation ruft die hinterlegte E-Mail-Adresse des Versicherten ab.
replaceEmailAddress	Diese Operation setzt oder ändert die E-Mail Adresse für einen Versicherten ab.
<b>I_Tool_Convert_PDF_Insurant</b>	
Schnittstelle des XDS Document Managements gemäß [I_Tool_Convert_PDF_Insurant]	
convertPDF	Diese Operation konvertiert ein PDF in ein PDF/A Format
<b>I_Data_Submission_Service</b>	
Schnittstelle des Data Submission Service gemäß [I_Data_Submission_Service]	
getSubmissionPackage	Diese Operation stellt dem FDZ ein Datenpaket für eine bestimmte SubmissionID bereit.



<b>I_Push_Notification_Management_Insurant</b>	
Schnittstelle des Push Notification Managements gemäß [I_Push_Notification_Management]	
getPushers	Diese Operation gibt alle Pusher Registrierungen eines Aktenkontos aus
updatePusher	Diese Operation setzt, aktualisiert oder löscht eine Pusher Registrierung
getChannelsOfPusher	Diese Operation gibt die aktuelle Konfiguration der Push Notification Channels für einen Pusher aus
updateChannelsOfPusher	Diese Operation aktualisiert die Auswahl der Push Notification Channels für einen Pusher
getChannels	Diese Operation gibt die möglichen Push Notification Channels der ePA aus

Schnittstellen des Aktensystems (Nutzung ohne VAU-Kanal)	
<b>I_Information_Service</b>	
Schnittstelle des Informationsdienstes gemäß [I_Information_Service]	
getConsentDecisionInformation	Diese Operation liest den aktuellen Zustand der Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der Funktionsklasse "Versorgungsprozess" aus.
setUserExperienceResult	Die Operation dient der Sammlung von Client Performedaten aus der Umgebung der Leistungserbringer.
getRecordStatus	Diese Operation fragt Existenz und Status eines bestimmten Aktenkontos bei einem Betreiber an.
<b>I_Information_Service_Accounts</b>	
Schnittstelle des Information Service gemäß [I_Information_Service_Accounts] für Anbieter Aktensystem im Kontext eines Aktenkontoumzugs	
getGeneralConsentDecision	Diese Operation dient der Abfrage eines Widerspruchs gegen die Nutzung der ePA bei einem anderen Aktensystemanbieter.
startRelocation	Diese Operation initiiert die Erstellung eines Export Pakets für die Relocation.
deleteExportPackage	Diese Operation schließt den Vorgang der Relocation erfolgreich ab.
postExportPackageIncident	Diese Operation erhält Benachrichtigungen zum Relocation-Prozess.
putDownloadUrlForExportPackage	Diese Operation initiiert den Import eines Export Packages.
postPackageDeliveryIncident	Diese Operation erhält Benachrichtigungen zum Relocation-Prozess.
getProviderList	Diese Operation gibt eine Liste von FQDNs der Versicherungen / ePA-Anbieter aus

Die Schnittstellen (REST) und Operationen sind funktional in den Beschreibungen der jeweiligen Schnittstelle beschrieben. Darüber hinaus gelten die folgenden übergreifenden Anforderungen.

### 3.22.2 Übergreifende Festlegungen zu den Schnittstellen

#### **A\_23918 -Schnittstellen (OpenApi) - Prüfung der Befugnis**

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) eine vorhandene und gültige Befugnis (entitlement) für den Nutzer der Operation fordern und diese nicht vorliegt. [≤]

*Hinweis: A\_23918 deckt auch die Fehlersituationen "kein VAU-Kanal" und "keine User Session" ab, da diese eine Vorbedingung für den Nachweis einer gültigen Befugnis sind.*

#### **A\_24365 -Schnittstellen (OpenApi) - Prüfung des Aktenkontos**

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) die Existenz des adressierten Aktenkontos fordern und diese nicht für den Operationsaufruf verwendet wird. [≤]

*Hinweis A\_24365 deckt auch die Fehlersituation "kein Health Record Context" ab, da dieses nur infolge eines nicht vorhandenen Aktenkontos auftritt.*

#### **A\_24538 -Schnittstellen (OpenApi) - Prüfung des Aktenkontostatus**

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) einen vorgegebenen Status des Aktenkontos fordern und dieser nicht vorhanden ist. [≤]

#### **A\_24366 -Schnittstellen (OpenApi) - Prüfung der Rolle**

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) die Zulässigkeit der Operation auf bestimmte Rollen (professionOID) einschränken und der Nutzer der Operation diese nicht nachweist. [≤]

#### **A\_24367 -Schnittstellen(OpenApi) - Prüfung des Identifiers**

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) die Zulässigkeit der Operation auf bestimmte Identifier (KVNR oder Telematik-ID) einschränken und der Nutzer der Operation diese nicht nachweist. [≤]

#### **A\_24580 -Schnittstellen (OpenApi) - Protokollierung der Operationen**

Das ePA-Aktensystem MUSS nach der Ausführung der Operationen der REST-Schnittstellen einen Protokolleintrag erstellen, wenn die Protokollierung in den Nachbedingungen (Postconditions) der Operationen gefordert ist (log-entry). [≤]

---

## 4 Informationsmodelle

---

Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten wird nicht benötigt.

---

## 5 Anhang A - Verzeichnisse

---

### 5.1 Abkürzungen

Kürzel	Erläuterung
AdV	Anwendungen des Versicherten
AN	Arbeitsnummer in der Übermittlung von Daten zur Sekundärnutzung
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BGP	Border Gateway Protokoll
BPPC	Basic Patient Privacy Consents
CRUD	Create Read Update Delete
DiGA	Digitale Gesundheitsanwendung
ePA-FdV	ePA-Frontend des Versicherten
ePA-FdV AdV	ePA-Frontend des Versicherten im KTR-AdV-Terminal
FDZ	Forschungsdatenzentrum Gesundheit
HL7	Health Level Seven
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IHE ITI TF	IHE IT Infrastructure Technical Framework
JWT	JSON-Web-Token
JWS	signiertes JSON-Web-Token

KTR	Kostenträger
LP	Lieferpseudonym in der Übermittlung von Daten zur Sekundärnutzung
MIO	Medizinisches Informationsobjekt
MHD	Mobile access to Health Documents (FHIR-Service im Aktensystem u.a. für Volltextsuche)
MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
PDSG	Patientendaten-Schutz-Gesetz
PHR	Personal Health Record
RMU	Restricted Metadata Update Profile
SAML	Security Assertion Markup Language
TLS	Transport Layer Security
UUID	Universally Unique Identifier
VAU	Vertrauenswürdige Ausführungsumgebung
VST	Vertrauensstelle Elektronische Patientenakte für Datenausleitung an das FDZ
W3C	World Wide Web Consortium
WS-I	Web-Services Interoperability Consortium
XCA	Cross-Community Access Profile
XDS	Cross-Enterprise Document Sharing Profile
XDW	Cross-Enterprise Document Workflow Profile
XOP	XML-binary Optimized Packaging
XSPA	Cross-Enterprise Security and Privacy Authorization Profile

## 5.2 Glossar

Begriff	Erläuterung
Authenticator-Modul	Das Authenticator-Modul ist die Client-Komponente zum sektoralen Identity Provider. Über die das Authenticator-Modul authentifiziert sich der Versicherte gegenüber des sektoralen IDP. Das Authenticator-Modul kann in ein App (z.B. Service-App einer Krankenkasse oder ePA-FdV) integriert oder als eigenständige App implementiert werden (siehe auch [gemSpec_IDP_Sek]).

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

## 5.3 Abbildungsverzeichnis

*Please update the table of figures.*

## 5.4 Tabellenverzeichnis

*Please update the table of figures.*

## 5.5 Referenzierte Dokumente

### 5.5.1 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"
[gemSpec_FdV_ePA]	gematik: Spezifikation ePA-Frontend des Versicherten
[gemSpec_IDP_Sek]	gematik: Spezifikation des sektoralen IDP (GesundheitsID)
[gemSpec_IDP_FD]	gematik: Spezifikation der Fachdienste der TI-Föderation
[gemSpec_IDP_Frontend]	gematik: Spezifikation der Frontendkomponenten für Fachdienste der TI-Föderation



[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform
[gemSpec_IG_ePA]	gematik: Implementation Guides für strukturierte Dokumente GitHub: siehe [ePA_XDS_Document] Path: src/implementation_guides
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory
[ePA_Basic]	gematik: GitHub Repository "ePA-Basic" <a href="https://github.com/gematik/ePA-Basic/tree/ePA-3.1.2">https://github.com/gematik/ePA-Basic/tree/ePA-3.1.2</a>
[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_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 EU-Zugriff siehe [ePA_Basic] Path: src/openapi/I_Entitlement_Management_EU.yaml
[I_Device_Management_Insurant]	gematik: I_Device_Management_Insurant.yaml REST-Schnittstelle zur Geräteverwaltung siehe [ePA_Basic] Path: src/openapi/I_Device_Management_Insurant.yaml
[I_Health_Record_Relocation_Service]	gematik: I_Health_Record_Relocation_Service REST-Schnittstelle zum Aktenumzug siehe [ePA_Basic] Path: src/openapi/I_Health_Record_Relocation_Service.yaml

[I_Information_Service_Accounts]	Schnittstellenspezifikation Information Service für Betreiber siehe [ePA_Basic] Path: src/openapi/I_Information_Service_Accounts.yaml
[I_Information_Service]	Schnittstellenspezifikation Information Service siehe [ePA_Basic] Path: src/openapi/I_Information_Service.yaml
[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_Email_Management]	gematik: I_Email_Management REST-Schnittstelle zum Management von E-Mail-Adressen eines Versicherten siehe [ePA_Basic] Path: src/openapi/I_Email_Management.yaml
[ePA_XDS_Document]	gematik: GitHub Repository "ePA-xds-document" <a href="https://github.com/gematik/ePA-XDS-Document/tree/ePA-3.1.2">https://github.com/gematik/ePA-XDS-Document/tree/ePA-3.1.2</a>
[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
[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
[XDSDocumentService]	gematik: XDSDocumentService.wsdl IHE-Schnittstelle des XDSDocumentService siehe [ePA_XDS_Document] Path: src/schema
[HealthRecordMigration]	gematik: ref-ePA-HealthRecordMigration Referenzimplementierung und Vorgaben für das Exportpaket bei einem Anbieterwechsel GitHub: <a href="https://github.com/gematik/ref-ePA-HealthRecordMigration/tree/ePA-3.1">https://github.com/gematik/ref-ePA-HealthRecordMigration/tree/ePA-3.1</a>
[IG_Basic]	gematik: FHIR Implementation Guide "ePA Basisfunktionalitäten" <a href="https://gematik.de/fhir/epa/1.1.5">https://gematik.de/fhir/epa/1.1.5</a>

[IG_Medication_Service]	gematik: FHIR Implementation Guide "ePA Medication Service" <a href="https://gematik.de/fhir/epa-medication/1.1.5">https://gematik.de/fhir/epa-medication/1.1.5</a>
[IG_MHD_Service]	gematik: FHIR Implementation Guide "ePA MHD Service" <a href="https://gematik.de/fhir/epa-mhd/1.0.0">https://gematik.de/fhir/epa-mhd/1.0.0</a>
[IG_TI_Terminology]	gematik: Implementation Guide "TITerminology" <a href="https://gematik.de/fhir/terminology/1.0.6">https://gematik.de/fhir/terminology/1.0.6</a>
[DataPseudonymization]	gematik: epa-research Vorgaben zur Pseudonymisierung von Daten zur Sekundärnutzung GitHub: <a href="https://github.com/gematik/epa-research/tree/ePA-3.1">https://github.com/gematik/epa-research/tree/ePA-3.1</a> Path: docs/leitfaden_pseudonymisierung.md
[I_Data_Submission_Service]	gematik: I_Data_Submission_Service Schnittstelle für den Abruf eines Datenpaketes FDZ siehe [ePA_Basic] Path: src/openapi/ I_Data_Submission_Service.yaml
[I_Push_Notification_Management]	gematik: I_Push_Notification_Management_Insurant REST-Schnittstelle zum Management des Benachrichtigungsdienstes der ePA siehe [ePA_Basic] Path: src/openapi/I_Push_Notification_Management_Insurant.yaml
[gemF_PushNotification]	gematik: Anwendungsübergreifende Push Notification
[PushNotificationConcept]	gematik: Push Notification Concept Repository mit Artefakten und Vorgaben für anwendungsübergreifende Push Notification GitHub: <a href="https://gematik.github.io/gem-push-notifications-concept/1.0.0/#concept/concept.html">https://gematik.github.io/gem-push-notifications-concept/1.0.0/#concept/concept.html</a> und <a href="https://gematik.github.io/gem-push-notifications-concept/1.0.0/#concept/concept.html%23_priorit%C3%A4t">https://gematik.github.io/gem-push-notifications-concept/1.0.0/#concept/concept.html%23_priorit%C3%A4t</a>
[I_Push_Gateway]	gematik: Push Gateway API REST-Schnittstelle des Push Gateways zum Versand von Push Nachrichten GitHub: <a href="https://gematik.github.io/gem-push-notifications-concept/1.0.0/#push_gateway_openapi.html">https://gematik.github.io/gem-push-notifications-concept/1.0.0/#push_gateway_openapi.html</a>

[Schema_PushNotifications]	gematik: PushNotificationSchema Strukturvorgaben für Nachrichteninhalte des Push Notification Managements siehe [ePA_Basic] Path: src/schema/PushNotificationSchema.yaml
----------------------------	---

### 5.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-RMD]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.6 – Trial Implementation, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf</a>
[IHE-ITI-RMU]	IHE International (2021): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.3 – Trial Implementation, <a href="https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf">https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf</a>
[IHE-ITI-TF1]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Profile definition, use-case analysis, actor definition, and use of transactions and content, Revision 20.0, <a href="https://profiles.ihe.net/ITI/TF/Volume1/">https://profiles.ihe.net/ITI/TF/Volume1/</a>
[IHE-ITI-TF2]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.0, <a href="https://profiles.ihe.net/ITI/TF/Volume2/">https://profiles.ihe.net/ITI/TF/Volume2/</a>
[IHE-ITI-TF3]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Document Sharing Metadata and Content Profiles, Revision 20.0, <a href="https://profiles.ihe.net/ITI/TF/Volume3/">https://profiles.ihe.net/ITI/TF/Volume3/</a>
[I_VST]	Vertrauensstelle ePA – Pseudonymisierungskonzept Datenausleitung ePA zu Forschungszwecken Version 2.0 (12.07.2024), Herausgeber: Robert Koch-Institut, Nordufer 20,13353 Berlin
[MIO-UH]	Kassenärztliche Bundesvereinigung (2022): Kinderuntersuchungsheft, <a href="https://mio.kbv.de/display/UH1X0X1">https://mio.kbv.de/display/UH1X0X1</a>
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, <a href="https://www.w3.org/TR/soap12-mtom/">https://www.w3.org/TR/soap12-mtom/</a>

[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, <a href="https://datatracker.ietf.org/doc/html/rfc2119">https://datatracker.ietf.org/doc/html/rfc2119</a>
[RFC3339]	IETF (2002): Date and Time on the Internet: Timestamps, RFC 3339, <a href="https://datatracker.ietf.org/doc/html/rfc3339">https://datatracker.ietf.org/doc/html/rfc3339</a>
[RFC4122]	IETF (2005): A Universally Unique Identifier (UUID) URN Namespace, RFC 4122 <a href="https://datatracker.ietf.org/doc/html/rfc4122">https://datatracker.ietf.org/doc/html/rfc4122</a>
[RFC5246]	IETF (2008): The Transport Layer Security (TLS) Protocol Version 1.2 <a href="https://datatracker.ietf.org/doc/html/rfc5246">https://datatracker.ietf.org/doc/html/rfc5246</a>
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231, <a href="https://datatracker.ietf.org/doc/html/rfc7231">https://datatracker.ietf.org/doc/html/rfc7231</a>
[RFC7515]	IETF (2015): JSON Web Signature (JWS), RFC-7515 <a href="https://datatracker.ietf.org/doc/html/rfc7515">https://datatracker.ietf.org/doc/html/rfc7515</a>
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), <a href="https://www.w3.org/TR/soap12-part1/">https://www.w3.org/TR/soap12-part1/</a>
[WSA]	OASIS (2004): Web Services Addressing (WS-Addressing), <a href="https://www.w3.org/Submission/ws-addressing/">https://www.w3.org/Submission/ws-addressing/</a>
[WSIAP]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, <a href="http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html">http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html</a>
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), <a href="http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html">http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html</a>
[WSIBSP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, <a href="http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html">http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html</a>
[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), <a href="http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf">http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf</a>

[XMLSchema ]	W3C (2004): XML Schema Part 1: Structures Second Edition, <a href="http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/">http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/</a>
[XHTML]	W3C (2010): XHTML 1.1 - Module-based XHTML - Second Edition, <a href="https://www.w3.org/TR/xhtml1/">https://www.w3.org/TR/xhtml1/</a>

---

## 6 Anhang B - Erläuternde Informationen

---

Dieser Anhang enthält nicht normative Informationen, die dazu dienen, das Verständnis der Spezifikation zu vereinfachen.

### 6.1 Dokumentenanhänge

Der vorliegende Abschnitt enthält einige Abbildungen, die das Konzept der Dokumentenanhänge in der ePA für alle visuell erläutern und damit leichter verständlich machen sollen.

#### 6.1.1 Überblick

Die folgende Abbildung zeigt fünf Dokumente (bzw. DocumentEntries), die teilweise über Anhangsbeziehungen miteinander verbunden sind:



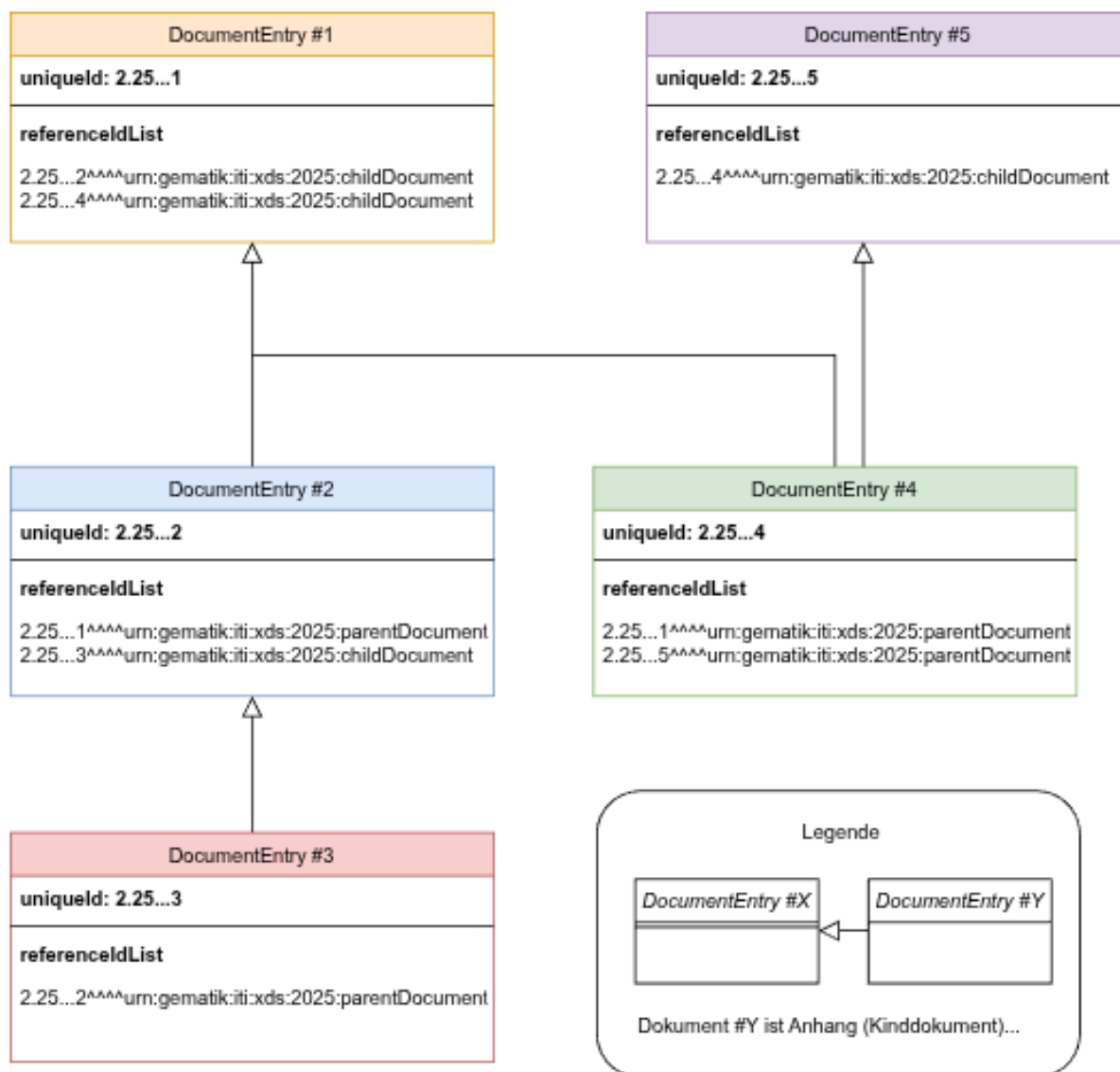


Abbildung 8: Dokumente mit Anhangsbeziehungen

```

3CmxGraphModel%3E%3Croot%3E%3CmxCell%20id%3D%220%22%2F%3E
%3CmxCell%20id%3D%221%22%20parent%3D%220%22%2F%3E%3CmxCell
%20id%3D%222%22%20value%3D%22DocumentEntry%20%231%22%20style
%3D%22swimlane%3BfontStyle%3D0%3Balign%3Dcenter
%3BverticalAlign%3Dtop%3BchildLayout%3DstackLayout
%3Bhorizontal%3D1%3BstartSize%3D26%3BhorizontalStack
%3D0%3BresizeParent%3D1%3BresizeLast%3D0%3Bcollapsible
%3D1%3BmarginBottom%3D0%3Brounded%3D0%3Bshadow
%3D0%3BstrokeWidth%3D1%3BfillColor%3D%23ffe6cc%3BstrokeColor
%3D%23d79b00%3B%22%20vertex%3D%221%22%20parent%3D%221%22%3E
%3CmxGeometry%20x%3D%22239%22%20y%3D%2270%22%20width%3D
%22290%22%20height%3D%22138%22%20as%3D%22geometry%22%3E
%3CmxRectangle%20x%3D%22130%22%20y%3D%22380%22%20width%3D
%22160%22%20height%3D%2226%22%20as%3D%22alternateBounds%22%2F
%3E%3C%2FmxGeometry%3E%3C%2FmxCell%3E%3CmxCell%20id%3D
%223%22%20value%3D%22uniqueId%3A%202.25...2%22%20style%3D
%22text%3Balign%3Dleft%3BverticalAlign%3Dtop%3BspacingLeft
%3D4%3BspacingRight%3D4%3Boverflow%3Dhidden%3Brotatable
%3D0%3Bpoints%3D%5B%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D
%3BportConstraint%3Deastwest%3BfontStyle%3D1%22%20vertex%3D
%221%22%20parent%3D%222%22%3E%3CmxGeometry%20y%3D
%2226%22%20width%3D%22290%22%20height%3D%2226%22%20as%3D
%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell%20id%3D
%224%22%20value%3D%22%22%20style%3D%22line%3Bhtml
%3D1%3BstrokeWidth%3D1%3Balign%3Dleft%3BverticalAlign%3Dmiddle
%3BspacingTop%3D-1%3BspacingLeft%3D3%3BspacingRight
%3D3%3Brotatable%3D0%3BlabelPosition%3Drigh%3Bpoints%3D%5B%5D
%3BportConstraint%3Deastwest%3B%22%20vertex%3D%221%22%20parent
%3D%222%22%3E%3CmxGeometry%20y%3D%2252%22%20width%3D
%22290%22%20height%3D%2228%22%20as%3D%22geometry%22%2F%3E%3C
%2FmxCell%3E%3CmxCell%20id%3D%225%22%20value%3D
%22referenceIdList%22%20style%3D%22text%3Balign%3Dleft
%3BverticalAlign%3Dtop%3BspacingLeft%3D4%3BspacingRight
%3D4%3Boverflow%3Dhidden%3Brotatable%3D0%3Bpoints%3D%5B
%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D%3BportConstraint%3Deastwest
%3BfontStyle%3D1%22%20vertex%3D%221%22%20parent%3D%222%22%3E
%3CmxGeometry%20y%3D%2260%22%20width%3D%22290%22%20height%3D
%2226%22%20as%3D%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell
%20id%3D%226%22%20value%3D%222.25...2%5E%5E%5E%5Eurn%3Agematik
%3Aiti%3Aaxds%3A2025%3AchildDocument%26%2310%3B2.25...4%5E%5E
%5E%5Eurn%3Agematik%3Aiti%3Aaxds%3A2025%3AchildDocument
%22%20style%3D%22text%3Balign%3Dleft%3BverticalAlign%3Dtop
%3BspacingLeft%3D4%3BspacingRight%3D4%3Boverflow%3Dhidden
%3Brotatable%3D0%3Bpoints%3D%5B%5B0%2C0.5%5D%2C%5B1%2C0.5%5D
%5D%3BportConstraint%3Deastwest%3B%22%20vertex%3D
%221%22%20parent%3D%222%22%3E%3CmxGeometry%20y%3D
%2286%22%20width%3D%22290%22%20height%3D%2234%22%20as%3D
%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell%20id%3D

```

```

%227%22%20value%3D%22DocumentEntry%20%232%22%20style%3D
%22swimlane%3BfontStyle%3D0%3Balign%3Dcenter%3BverticalAlign
%3Dtop%3BchildLayout%3DstackLayout%3Bhorizontal
%3D1%3BstartSize%3D26%3BhorizontalStack%3D0%3BresizeParent
%3D1%3BresizeLast%3D0%3Bcollapsible%3D1%3BmarginBottom
%3D0%3Brounded%3D0%3Bshadow%3D0%3BstrokeWidth%3D1%3BfillColor
%3D%23dae8fc%3BstrokeColor%3D%236c8ebf%3B%22%20vertex%3D
%221%22%20parent%3D%221%22%3E%3CmxGeometry%20x%3D%2278%22%20y
%3D%22313%22%20width%3D%22290%22%20height%3D%22138%22%20as%3D
%22geometry%22%3E%3CmxRectangle%20x%3D%22130%22%20y%3D
%22380%22%20width%3D%22160%22%20height%3D%2226%22%20as%3D
%22alternateBounds%22%2F%3E%3C%2FmxGeometry%3E%3C%2FmxCell%3E
%3CmxCell%20id%3D%228%22%20value%3D%22uniqueId%3A
%202.25...%22%20style%3D%22text%3Balign%3Dleft
%3BverticalAlign%3Dtop%3BspacingLeft%3D4%3BspacingRight
%3D4%3Boverflow%3Dhidden%3Brotatable%3D0%3Bpoints%3D%5B
%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D%3BportConstraint%3Deastwest
%3BfontStyle%3D1%22%20vertex%3D%221%22%20parent%3D%227%22%3E
%3CmxGeometry%20y%3D%2226%22%20width%3D%22290%22%20height%3D
%2226%22%20as%3D%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell
%20id%3D%229%22%20value%3D%22%22%20style%3D%22line%3Bhtml
%3D1%3BstrokeWidth%3D1%3Balign%3Dleft%3BverticalAlign%3Dmiddle
%3BspacingTop%3D-1%3BspacingLeft%3D3%3BspacingRight
%3D3%3Brotatable%3D0%3BlabelPosition%3Drigh%3Bpoints%3D%5B%5D
%3BportConstraint%3Deastwest%3B%22%20vertex%3D%221%22%20parent
%3D%227%22%3E%3CmxGeometry%20y%3D%2252%22%20width%3D
%22290%22%20height%3D%228%22%20as%3D%22geometry%22%2F%3E%3C
%2FmxCell%3E%3CmxCell%20id%3D%2210%22%20value%3D
%22referenceIdList%22%20style%3D%22text%3Balign%3Dleft
%3BverticalAlign%3Dtop%3BspacingLeft%3D4%3BspacingRight
%3D4%3Boverflow%3Dhidden%3Brotatable%3D0%3Bpoints%3D%5B
%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D%3BportConstraint%3Deastwest
%3BfontStyle%3D1%22%20vertex%3D%221%22%20parent%3D%227%22%3E
%3CmxGeometry%20y%3D%2260%22%20width%3D%22290%22%20height%3D
%2226%22%20as%3D%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell
%20id%3D%2211%22%20value%3D%22.25...1%5E%5E%5E%5Eurn
%3Agematik%3Aiti%3Aaxds%3A2025%3AparentDocument%22%20style%3D
%22text%3Balign%3Dleft%3BverticalAlign%3Dtop%3BspacingLeft
%3D4%3BspacingRight%3D4%3Boverflow%3Dhidden%3Brotatable
%3D0%3Bpoints%3D%5B%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D
%3BportConstraint%3Deastwest%3B%22%20vertex%3D%221%22%20parent
%3D%227%22%3E%3CmxGeometry%20y%3D%2286%22%20width%3D
%22290%22%20height%3D%2226%22%20as%3D%22geometry%22%2F%3E%3C
%2FmxCell%3E%3CmxCell%20id%3D%2212%22%20value%3D
%22DocumentEntry%20%234%22%20style%3D%22swimlane%3BfontStyle
%3D0%3Balign%3Dcenter%3BverticalAlign%3Dtop%3BchildLayout
%3DstackLayout%3Bhorizontal%3D1%3BstartSize
%3D26%3BhorizontalStack%3D0%3BresizeParent%3D1%3BresizeLast

```

%3D0%3Bcollapsible%3D1%3BmarginBottom%3D0%3Brounded  
%3D0%3Bshadow%3D0%3BstrokeWidth%3D1%3BfillColor%3D  
%23d5e8d4%3BstrokeColor%3D%2382b366%3B%22%20vertex%3D  
%221%22%20parent%3D%221%22%3E%3CmxGeometry%20x%3D%22428%22%20y  
%3D%22313%22%20width%3D%22290%22%20height%3D%22138%22%20as%3D  
%22geometry%22%3E%3CmxRectangle%20x%3D%22130%22%20y%3D  
%22380%22%20width%3D%22160%22%20height%3D%2226%22%20as%3D  
%22alternateBounds%22%2F%3E%3C%2FmxGeometry%3E%3C%2FmxCell%3E  
%3CmxCell%20id%3D%2213%22%20value%3D%22uniqueId%3A  
%202.25...4%22%20style%3D%22text%3Balign%3Dleft  
%3BverticalAlign%3Dtop%3BspacingLeft%3D4%3BspacingRight  
%3D4%3Boverflow%3Dhidden%3Brotatable%3D0%3Bpoints%3D%5B  
%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D%3BportConstraint%3Deastwest  
%3BfontStyle%3D1%22%20vertex%3D%221%22%20parent%3D%2212%22%3E  
%3CmxGeometry%20y%3D%2226%22%20width%3D%22290%22%20height%3D  
%2226%22%20as%3D%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell  
%20id%3D%2214%22%20value%3D%22%22%20style%3D%22line%3Bhtml  
%3D1%3BstrokeWidth%3D1%3Balign%3Dleft%3BverticalAlign%3Dmiddle  
%3BspacingTop%3D-1%3BspacingLeft%3D3%3BspacingRight  
%3D3%3Brotatable%3D0%3BlabelPosition%3Dright%3Bpoints%3D%5B%5D  
%3BportConstraint%3Deastwest%3B%22%20vertex%3D%221%22%20parent  
%3D%2212%22%3E%3CmxGeometry%20y%3D%2252%22%20width%3D  
%22290%22%20height%3D%228%22%20as%3D%22geometry%22%2F%3E%3C  
%2FmxCell%3E%3CmxCell%20id%3D%2215%22%20value%3D  
%22referenceIdList%22%20style%3D%22text%3Balign%3Dleft  
%3BverticalAlign%3Dtop%3BspacingLeft%3D4%3BspacingRight  
%3D4%3Boverflow%3Dhidden%3Brotatable%3D0%3Bpoints%3D%5B  
%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D%3BportConstraint%3Deastwest  
%3BfontStyle%3D1%22%20vertex%3D%221%22%20parent%3D%2212%22%3E  
%3CmxGeometry%20y%3D%2260%22%20width%3D%22290%22%20height%3D  
%2226%22%20as%3D%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell  
%20id%3D%2216%22%20value%3D%222.25...1%5E%5E%5E%5Eurn  
%3Agematik%3Aiti%3Aaxds%3A2025%3AparentDocument%22%20style%3D  
%22text%3Balign%3Dleft%3BverticalAlign%3Dtop%3BspacingLeft  
%3D4%3BspacingRight%3D4%3Boverflow%3Dhidden%3Brotatable  
%3D0%3Bpoints%3D%5B%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D  
%3BportConstraint%3Deastwest%3B%22%20vertex%3D%221%22%20parent  
%3D%2212%22%3E%3CmxGeometry%20y%3D%2286%22%20width%3D  
%22290%22%20height%3D%2226%22%20as%3D%22geometry%22%2F%3E%3C  
%2FmxCell%3E%3CmxCell%20id%3D%2217%22%20value%3D%222.25...1%5E  
%5E%5E%5Eurn%3Agematik%3Aiti%3Aaxds%3A2025%3AparentDocument  
%22%20style%3D%22text%3Balign%3Dleft%3BverticalAlign%3Dtop  
%3BspacingLeft%3D4%3BspacingRight%3D4%3Boverflow%3Dhidden  
%3Brotatable%3D0%3Bpoints%3D%5B%5B0%2C0.5%5D%2C%5B1%2C0.5%5D  
%5D%3BportConstraint%3Deastwest%3B%22%20vertex%3D  
%221%22%20parent%3D%2212%22%3E%3CmxGeometry%20y%3D  
%22112%22%20width%3D%22290%22%20height%3D%2226%22%20as%3D  
%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell%20id%3D

```

%2218%22%20value%3D%22DocumentEntry%20%233%22%20style%3D
%22swimlane%3BfontStyle%3D0%3Balign%3Dcenter%3BverticalAlign
%3Dtop%3BchildLayout%3DstackLayout%3Bhorizontal
%3D1%3BstartSize%3D26%3BhorizontalStack%3D0%3BresizeParent
%3D1%3BresizeLast%3D0%3Bcollapsible%3D1%3BmarginBottom
%3D0%3Brounded%3D0%3Bshadow%3D0%3BstrokeWidth%3D1%3BfillColor
%3D%23f8cecc%3BstrokeColor%3D%23b85450%3B%22%20vertex%3D
%221%22%20parent%3D%221%22%3E%3CmxGeometry%20x%3D%2278%22%20y
%3D%22533%22%20width%3D%22290%22%20height%3D%22138%22%20as%3D
%22geometry%22%3E%3CmxRectangle%20x%3D%22130%22%20y%3D
%22380%22%20width%3D%22160%22%20height%3D%2226%22%20as%3D
%22alternateBounds%22%2F%3E%3C%2FmxGeometry%3E%3C%2FmxCell%3E
%3CmxCell%20id%3D%2219%22%20value%3D%22uniqueId%3A
%202.25...%3%22%20style%3D%22text%3Balign%3Dleft
%3BverticalAlign%3Dtop%3BspacingLeft%3D4%3BspacingRight
%3D4%3Boverflow%3Dhidden%3Brotatable%3D0%3Bpoints%3D%5B
%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D%3BportConstraint%3Deastwest
%3BfontStyle%3D1%22%20vertex%3D%221%22%20parent%3D%2218%22%3E
%3CmxGeometry%20y%3D%2226%22%20width%3D%22290%22%20height%3D
%2226%22%20as%3D%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell
%20id%3D%2220%22%20value%3D%22%22%20style%3D%22line%3Bhtml
%3D1%3BstrokeWidth%3D1%3Balign%3Dleft%3BverticalAlign%3Dmiddle
%3BspacingTop%3D-1%3BspacingLeft%3D3%3BspacingRight
%3D3%3Brotatable%3D0%3BlabelPosition%3Drigh%3Bpoints%3D%5B%5D
%3BportConstraint%3Deastwest%3B%22%20vertex%3D%221%22%20parent
%3D%2218%22%3E%3CmxGeometry%20y%3D%2252%22%20width%3D
%22290%22%20height%3D%2228%22%20as%3D%22geometry%22%2F%3E%3C
%2FmxCell%3E%3CmxCell%20id%3D%2221%22%20value%3D
%22referenceIdList%22%20style%3D%22text%3Balign%3Dleft
%3BverticalAlign%3Dtop%3BspacingLeft%3D4%3BspacingRight
%3D4%3Boverflow%3Dhidden%3Brotatable%3D0%3Bpoints%3D%5B
%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D%3BportConstraint%3Deastwest
%3BfontStyle%3D1%22%20vertex%3D%221%22%20parent%3D%2218%22%3E
%3CmxGeometry%20y%3D%2260%22%20width%3D%22290%22%20height%3D
%2226%22%20as%3D%22geometry%22%2F%3E%3C%2FmxCell%3E%3CmxCell
%20id%3D%2222%22%20value%3D%22.25...2%5E%5E%5E%5Eurn
%3Agematik%3Aiti%3Aaxds%3A2025%3AparentDocument%22%20style%3D
%22text%3Balign%3Dleft%3BverticalAlign%3Dtop%3BspacingLeft
%3D4%3BspacingRight%3D4%3Boverflow%3Dhidden%3Brotatable
%3D0%3Bpoints%3D%5B%5B0%2C0.5%5D%2C%5B1%2C0.5%5D%5D
%3BportConstraint%3Deastwest%3B%22%20vertex%3D%221%22%20parent
%3D%2218%22%3E%3CmxGeometry%20y%3D%2286%22%20width%3D
%22290%22%20height%3D%2226%22%20as%3D%22geometry%22%2F%3E%3C
%2FmxCell%3E%3CmxCell%20id%3D%2223%22%20value%3D%22%22%20style
%3D%22endArrow%3Dblock%3BendSize%3D10%3BendFill%3D0%3Bshadow
%3D0%3BstrokeWidth%3D1%3Brounded%3D0%3Bcurved%3D0%3BedgeStyle
%3DelbowEdgeStyle%3Belbow%3Dvertical%3BexitX%3D0.5%3BexitY
%3D0%3BexitDx%3D0%3BexitDy%3D0%3B%22%20edge%3D%221%22%20source

```



```
%3D%227%22%20target%3D%222%22%20parent%3D%221%22%3E
%3CmxGeometry%20width%3D%22160%22%20relative%3D%221%22%20as%3D
%22geometry%22%3E%3CmxPoint%20x%3D%22488%22%20y%3D
%22360%22%20as%3D%22sourcePoint%22%2F%3E%3CmxPoint%20x%3D
%22378%22%20y%3D%22258%22%20as%3D%22targetPoint%22%2F%3E%3C
%2FmxGeometry%3E%3C%2FmxCell%3E%3CmxCell%20id%3D
%2224%22%20value%3D%22%22%20style%3D%22endArrow%3Dblock
%3BendSize%3D10%3BendFill%3D0%3Bshadow%3D0%3BstrokeWidth
%3D1%3Brounded%3D0%3Bcurved%3D0%3BedgeStyle%3DelbowEdgeStyle
%3Belbow%3Dvertical%3BexitX%3D0.5%3BexitY%3D0%3BexitDx
%3D0%3BexitDy%3D0%3B%22%20edge%3D%221%22%20source%3D
%2212%22%20target%3D%222%22%20parent%3D%221%22%3E%3CmxGeometry
%20width%3D%22160%22%20relative%3D%221%22%20as%3D%22geometry
%22%3E%3CmxPoint%20x%3D%22233%22%20y%3D%22323%22%20as%3D
%22sourcePoint%22%2F%3E%3CmxPoint%20x%3D%22384%22%20y%3D
%22210%22%20as%3D%22targetPoint%22%2F%3E%3C%2FmxGeometry%3E%3C
%2FmxCell%3E%3CmxCell%20id%3D%2225%22%20value%3D%22%22%20style
%3D%22endArrow%3Dblock%3BendSize%3D10%3BendFill%3D0%3Bshadow
%3D0%3BstrokeWidth%3D1%3Brounded%3D0%3Bcurved%3D0%3BedgeStyle
%3DelbowEdgeStyle%3Belbow%3Dvertical%3B%22%20edge%3D
%221%22%20source%3D%2218%22%20target%3D%227%22%20parent%3D
%221%22%3E%3CmxGeometry%20width%3D%22160%22%20relative%3D
%221%22%20as%3D%22geometry%22%3E%3CmxPoint%20x%3D%22583%22%20y
%3D%22323%22%20as%3D%22sourcePoint%22%2F%3E%3CmxPoint%20x%3D
%22394%22%20y%3D%22218%22%20as%3D%22targetPoint%22%2F%3E%3C
%2FmxGeometry%3E%3C%2FmxCell%3E%3C%2Froot%3E%3C%2FmxGraphModel
%3Dazu einige Hinweise:
```

- Dokument #1
  - besitzt zwei Anhänge (Dokumente #2 und #4)
  - ist selbst an kein Dokument angehängt.
- Dokument #2
  - besitzt einen Anhang (Dokument #3).
- Dokument #3
  - besitzt keine Anhänge.
  - ist selbst an Dokument #2 angehängt.
- Dokument #4
  - besitzt keine Anhänge.
  - ist selbst an zwei Dokumente angehängt (Dokumente #1 und #5)
- Dokument #5
  - besitzt einen Anhang (Dokument #4).

## Notation

Jedes Dokument verweist auf Dokumentenanhänge über einen Eintrag in seiner `referencedList`  
 (<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2025:childDocument), wobei

DocumentEntry.uniqueId sich auf die eindeutige Kennung des Anhangsdokuments bezieht. In der Spezifikation wird der Anhang manchmal als Kinddokument bezeichnet, und das Dokument, an dem es hängt als Elterndokument. In diesem Sinne ist Dokument #3 bspw. das Kinddokument von Dokument #2.

### Anzahl Anhänge

Wie aus der Abbildung hervorgeht, kann ein Dokument mehrere Anhänge besitzen; im Beispiel verfügt Dokument über zwei Anhänge. Umgekehrt kann auch jeder Anhang an mehr als einem Dokument hängen (im Beispiel ist Dokument #4 Anhang sowohl für Dokument #1 also auch Dokument #5).

Die Beziehung zwischen Eltern- und Kinddokumenten ist also m:n: Ein Dokument kann beliebig viele Anhänge besitzen und ein Anhang kann an beliebig vielen Dokumenten anhängen.

## 6.1.2 Ungültige Anhänge

Dieser Abschnitt illustriert einige nicht erlaubte Anhangsszenarien.

### 6.1.2.1 Verweiszirkel und doppelte Eltern

Die folgende Abbildung demonstriert Anhänge, wie sie nicht in den XDS Document Service eingebracht werden können:

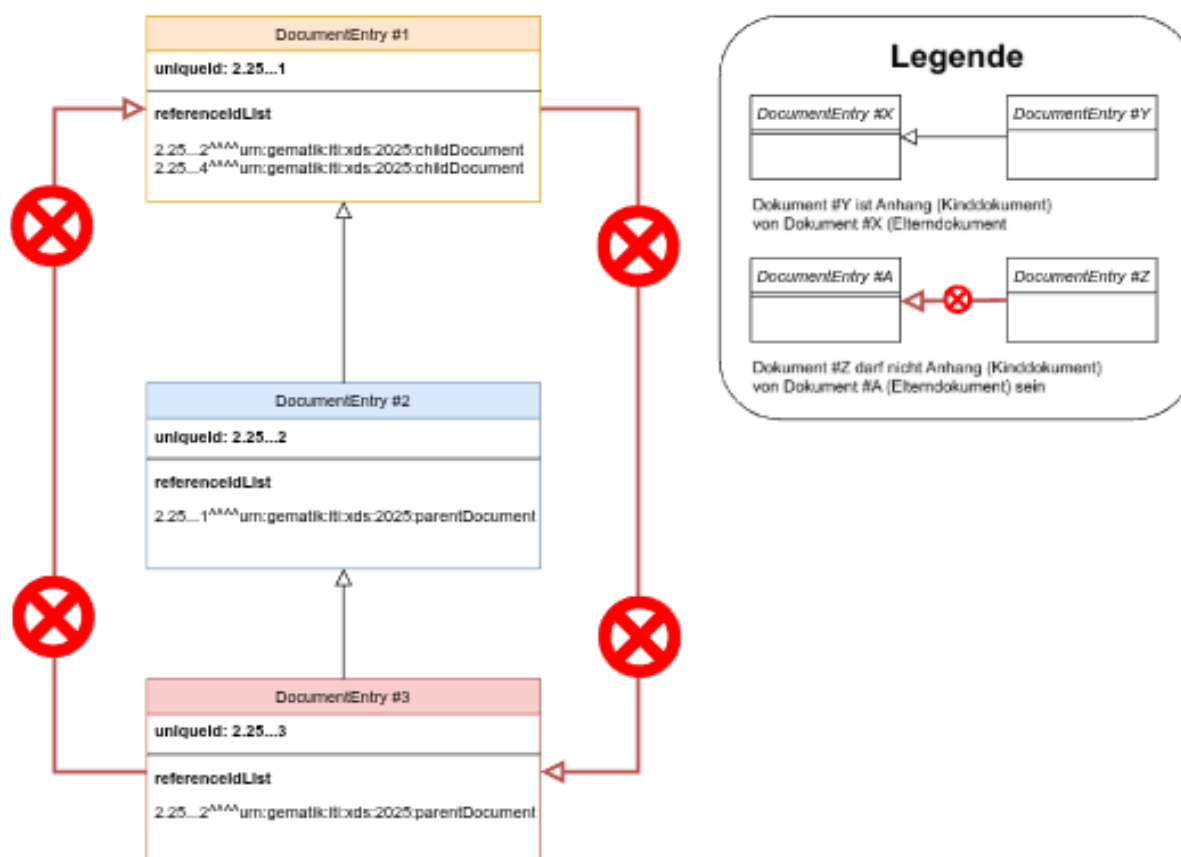


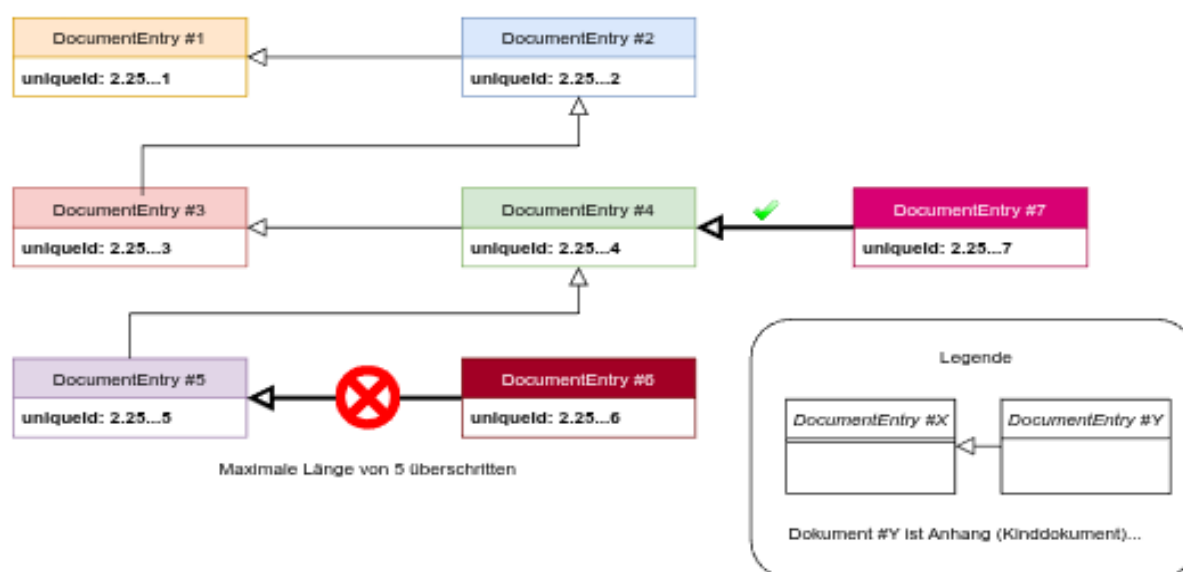
Abbildung 9: Beispiel Verweiszirkel und doppelte Eltern



- Ausgangssituation (unproblematisch):
  - Dokument #3 ist Anhang zu Dokument #2.
  - Dokument #2 ist Anhang zu Dokument #1.
- Falls nun anschließend versucht wird, Dokument #3 als Kind von Dokument #1 einzutragen (roter Pfeil auf der linken Seite), ist dies nicht erlaubt, da ein Dokument nicht Anhang zu zweien seiner "Vorfahren" in der Anhangskette sein darf (denn Dokument #3 ist bereits Anhang von Dokument #2, das wiederum an Dokument #1 hängt).
- Auch der Versuch, Dokument #1 als Anhang zu Dokument #3 zu markieren schlägt fehl, denn es würde ein Verweiszirkel entstehen, in dem ein Kinddokument gleichzeitig Elterndokument für eines seiner Vorfahren ist.

### 6.1.2.2 Anhangskette zu lang

Die maximale Länge der Anhangsketten ist auf fünf beschränkt. Die folgende Abbildung zeigt, in welchem Fall das Hinzufügen eines weiteren Anhangs zu Problemen führt (und wann nicht):



**Abbildung 10: Beispiel Anhangskette zu lang**

- Ausgangssituation (Dokumente #1-#5) unproblematisch. Länge der Anhangskette ist fünf.
- Wenn versucht wird, Dokument #6 einzufügen, ist die Anhangskette zu lang.
  - Das würde auch gelten, wenn der Einstellende bspw. Dokumente #1 und #2 gar nicht sehen könnte (Legal Policy, Verbergen)
  - Es würde ein Fehler zurückgegeben.
- Das Einstellen von Dokument #7 wäre unproblematisch.
  - Die Anhangskette von Dokument #7 hätte fünf Dokumente, Dokument #6 gehört also nicht mit dazu.
  - Das Dokument könnte auf diese Weise als Anhang an Dokument #4 eingestellt werden.

