Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
Aktensystem ePA für Alle

Version:	1.0.0
Revision:	832147
Stand:	30.01.2024
Status:	freigegeben
Klassifizierung:	öffentlich
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	30.01.24		ePA für alle	gematik

Inhaltsverzeichnis

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. Dokumentenlandkarte, 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 - 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 IDToken beim sektoralen IDP und die Erstellung oder Änderungen der Mailadresse für die Geräteverwaltung sowie die Aktivitäten im Unlock Service 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_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 zu User Agent sind in A_22470* definiert.

A_24816 - Aktenkontokennung 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-insurantId" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen.
[<=]

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

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 über DNS Service Discovery an 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).

Das 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 - 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) registrieren. Dies sind

- <host_epa>: Host und IP-Adresse für den Endpunkt I_Information_Service und der Services in der VAU
- <host_accounts>: Host und IP-Adresse für den Endpunkt I_Information_Service_Accounts

[<=]

Beispiele der Dienstlokalisierung

PU :
Aktensystem 1

```
_epa._tcp.epa4all.de    SRV   10 443 epa-hst1.prod.epa4all.de
_epa._tcp.epa4all.de    TXT   “txtvers=1“ "epa=/epa/" "info=/info/"
epa-hst1.prod.epa4all.de A 100.102.x1.y1


_accounts._tcp.epa4all.de    SRV   10 443 accounts-hst1.prod.epa4all.de
_accounts._tcp.epa4all.de    TXT   “txtvers=1“ "accounts=/accounts/"
accounts-hst1.prod.epa4all.de A 100.102.x1.y2
```

Aktensystem 2

```
_epa._tcp.epa4all.de    SRV   10 443 epa-hst2.prod.epa4all.de
_epa._tcp.epa4all.de    TXT   “txtvers=1“ "epa=/epa/" "info=/info/"
epa-hst2.prod.epa4all.de A 100.102.x2.y1


_accounts._tcp.epa4all.de    SRV   10 443 accounts-hst12prod.epa4all.de
_accounts._tcp.epa4all.de    TXT   “txtvers=1“ "accounts=/accounts/"
accounts-hst2.prod.epa4all.de A 100.102.x2.y2
```

TU :
Aktensystem 1

```
_epa._tcp.test.epa4all.de    SRV   10 443 epa-hst1.test.epa4all.de
_epa._tcp.test.epa4all.de    TXT   “txtvers=1“ "epa=/epa/" "info=/info/"
epa-hst1.test.epa4all.de A 172.30.x1.y1

...
```

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_22688-01 - Anbieter ePA-Aktensystem, Konfiguration Schnittstellen über /.well-known/
Der Anbieter des ePA-Aktensystems MUSS an seinen Access Gateway des Versicherten über den URL-Pfadnamen (bwz. 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

```
{
    "epa"   : "/epa/",
    "sgd1"  : "<pfad_Schlüsselgenerierungsdienst_typ1>"
    "sgd2"  : "<pfad_Schlüsselgenerierungsdienst_typ2>"
    ....
}
```
[<=]

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_17969-05 - Anbieter ePA-Aktensystem - Schnittstellenadressierung
Der Anbieter des ePA-Aktensystems MUSS alle nach außen angebotenen Dienste unter den folgenden URLs zur Verfügung stellen und eingehende SOAP- und REST-Nachrichten entsprechend verarbeiten:

- ePA-Clients über das zentrale Netz der TI:
  - https://<FQDN aus DNS Lookup>:443/accounts/I_Information_Service_Accounts
  - https://<FQDN aus DNS Lookup>:443/info/I_Information_Service
  - https://<FQDN aus DNS Lookup>:443/epa/<Schnittstellen der verschiedenen Services in der VAU>
- ePA-Frontend des Versicherten:
  - https://<FQDN lokaler Konfiguration des ePA-FdV>:443/epa/<Schnittstellen der verschiedenen Services in der VAU>

[<=]

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 zur Verfügbarkeit ergeben sich aus [gemSpec_Perf]. Die Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Komponenten des ePA-Aktensystems. In diesem Dokument werden zusätzliche Redundanzanforderungen spezifiziert, wenn die Anforderungen in [gemSpec_Perf] zur Verfügbarkeit nicht ausreichen.

Die Auswahl und der Zugriff auf Services des ePA-Aktensystems wird durch die Primärsysteme anhand der DNS-Einträge vorgenommen. Auf die Auswahl der Services des ePA-Aktensystems kann der Anbieter des ePA-Aktensystems durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn jedes Primärsystem oder andere Fachdienste (z.B. E-Rezept-Fachdienst, ein anderes ePA-Aktensystem, ...) die Möglichkeit haben, die Services des ePA-Aktensystems zu erreichen. Von der Versichertenseite aus erfolgt der Zugriff auf die Komponenten des ePA-Aktensystems durch das ePA-Frontend des Versicherte.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen Komponenten des ePA-Aktensystems 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 jede einzelne Komponente des ePA-Aktensystems im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

A_14921 - Anbieter ePA-Aktensystem - lokale Redundanz im Standort des ePA-Aktensystems
Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass bei Ausfall einer oder mehrerer Komponenten des ePA-Aktensystems die verbleibenden Komponenten des ePA-Aktensystems in demselben Standort den Datenverkehr aller Clients der ausgefallenen Komponente zusätzlich übernehmen, die Konsistenz der persistenten Daten erhalten bleibt und die Verfügbarkeit der Komponenten gemäß den geforderten SLAs in [gemSpec_Perf] weiterhin gegeben ist.**[<=]**

A_15245 - Anbieter ePA-Aktensystem - standortübergreifende Redundanz und Verfügbarkeit
Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass bei Ausfall eines Standorts (Rechenzentrum) die Konsistenz der persistenten Daten erhalten bleibt und die Verfügbarkeit der Komponenten gemäß der geforderten SLAs in [gemSpec_Perf] gegeben ist.**[<=]**

A_24862 - Anbieter ePA-Aktensystem – Georedundanz: Verfügbarkeit der Akten innerhalb von fünf Arbeitstagen
Der Betreiber des ePA-Aktensystems MUSS Maßnahmen zur Verfügbarkeit der Akten ergreifen, die sicherstellen, dass bei einem Großereignis aufgrund von Naturgewalten alle betroffenen Akten innerhalb von fünf Arbeitstagen in ihrer Kernfunktion wieder für die Versorgung genutzt werden können. Die Maßnahmen zur Erhaltung der Verfügbarkeit des Aktensystems müssen die Sicherheitsanforderungen für das ePA-Aktensystem erfüllen.
[<=]

Hinweis zu A_24862-*: Die Kernfuktionen des Aktensystems werden im Verlauf der Umsetzung des ePA-Aktensystems näher festgelegt werden.

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_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_15107-01 - 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 nach Freigabe durch den Versicherten oder einen Vertreter.**[<=]**

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-Aktennutzung entsprechend der Anforderung A_15154.**[<=]**

A_15154 - Anbieter ePA-Aktensystem - Ermittlung von Standard-Aktennutzung
Der Anbieter des ePA-Aktensystems MUSS mindestens einmal im Jahr Werte zu einer Standard-Aktennutzung 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-Aktennutzung
Der Anbieter des ePA-Aktensystems MUSS Zugriffe und Zugriffsmuster, die nicht einer Standard-Aktennutzung 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 - Anbieter ePA-Aktensystem – Versicherte über sensible Änderungen informieren
Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass der Versicherte über Änderungen in den folgenden Anwendungsfällen informiert wird,

- E-Mail-Adresse ändern,

- Aktenkonto schließen

und wenn der Anbieter des Aktensystems eine manuelle Änderung bezüglich einer Akte (Aktenverwaltung) im Auftrag eines Versicherten durchführt.**[<=]**

Hinweis: Dies kann z. B. durch eine Notifikations-E-Mail an den Versicherten erfolgen. Solche E-Mails dürfen keine Details über die Änderungen beschreiben, sondern nur einen Hinweis geben, dass eine Änderung gemacht wurde und dass der Versicherte die Änderungen in seinem Aktenkonto prüfen sollte.

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 - 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.OSIG
PolicyList	oid_fd_sig	oid_egk_sig	oid_smc_b_osig
intendedKeyUsage	digitalSignature	nonRepudiation	nonRepudiation
intendedExtendedKeyUsage	(leer)	(leer)	(leer)
OCSP-Graceperiod	24 Stunden	24 Stunden	24 Stunden
Offline-Modus	nein	nein	nein
Prüfmodus	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.
[<=]

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)

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.*

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 Validierungaktenkonten 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 den 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_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 diese 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 vorbei fließt, 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 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 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 Aktensystem MUSS den Tiger-Standalone-Proxy (und die damit verbunden 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_22470-04 - Definition Useragent
Das Produkt MUSS für das `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: ClientID = ein 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 zum Erhalt der ClientID: die ClientID wird durch die gematik vergeben und übermittelt, sobald sich ein (Client-)Produkthersteller (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 ClientID 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 den Useragent das spezifische Kostenträger-ePA-FdV erkennbar sein muss.

2.8 Datenmigration

Jeder Versicherter (vorbehaltlich eines Widerspruchs durch den Versicherten) erhält in ePA 3.0 ein neues, leeres Aktenkonto. Bei der Migration werden Daten und Vertreterberechtigungen aus ePA 2.6 in dieses Aktenkonto übertragen.

Für die Migration eines existierenden Aktenkontos der Version ePA-2.x wird vorausgesetzt, dass ein migriertes Aktenkonto sowohl die Schnittstellen der ePA für alle, als auch die Schnittstellen der bisherigen ePA-Version 2.x bereitstellt und simultan verarbeiten kann.

Die Migration eines existierenden Aktenkontos der ePA-Version 2.x erfordert die Entschlüsselung der existierenden Inhalte durch die Anwendung des aktenkontospezifischen Akten- und Kontextschlüssels und deren Überführung in die Verwaltungs- und Diensteeinheiten der im vorliegenden Dokument beschriebenen ePA-Version 3.x.

Aus einem existierenden Aktenkonto werden die folgenden Artefakte übernommen:

- Kategorien und Ordner, insoweit die Kategorien nicht abgekündigt sind. Ordner erhalten eine feste UUID.
- Dokumente, sowie deren Metadaten
- Protokolle

Die Vertraulichkeitsstufen für die Sichtbarkeit von Dokumenten werden nicht mehr unterstützt. Dokumente mit bisheriger Vertraulichkeitsstufe *confidential* werden bei der Migration der GlobalDenyPolicy des Constraint Managements zugeordnet.

Alle weiteren Nutzergruppen (LEI, Apotheken, usw) erhalten eine Befugnis zur Nutzung dediziert in einer Behandlungssituation oder durch direkte Befugnisvergabe durch den Versicherten oder einen Vertreter mittels ePA-FdV.

Für Versicherte, die keine ePA-FdV nutzen möchten oder können, ist eine Migration der Daten einer existierenden Akte nicht möglich, da die dafür notwendige Übertragung des bisherigen individuellen Akten- und Kontextschlüssels nicht erfolgen kann. Versicherte ohne ePA-FdV erhalten (vorbehaltlich eines Widerspruchs durch den Versicherten) ein neues, leeres Aktenkonto ohne Inhalten, die womöglich in ePA 2.6 existierten. Eine Befugnisvergabe für Leistungserbringerorganisationen ist in diesem Fall ausschließlich durch die Befugnisvergabe im Behandlungskontext möglich. Dieses erfordert eine LEI mit einem Client gemäß ePA-Version 3.x.

Es resultiert ein Aktenkonto, welches direkt durch den Versicherten, befugte Vertreter, den Kostenträger, die Ombudsstelle und den E-Rezept-Fachdienst genutzt werden kann.

2.8.1 Herstellerspezifische Umsetzung der Datenmigration

Die technische Umsetzung der Datenmigration obliegt grundsätzlich dem Hersteller des ePA-Aktensystems. Es muss jedoch sichergestellt werden, dass der Schutz der zu migrierenden Daten durchgehend gewährleistet wird.

A_24995 - Migration: Sicherheitskonzept für Datenmigration

Der Hersteller des ePA-Aktensystems MUSS ein Sicherheitskonzept zur Datenmigration erstellen, in welchem er beschreibt, mit welchen Maßnahmen die zu migrierenden Daten im gesamten Datenmigrationsprozess geschützt werden.**[<=]**

A_25000 - Migration: Stärke der Sicherheitsmaßnahmen für Datenmigration
Das ePA-Aktensystem MUSS sicherstellen, dass die zu migrierenden Daten im gesamten Datenmigrationsprozess mit technischen Maßnahmen geschützt werden, die auch gegen einzelne Innentäter beim Betreiber des ePA-Aktensystems wirken.**[<=]**

A_25049 - Migration: Migrationskonzept
Der Anbieter des ePA-Aktensystems MUSS ein Migrationskonzept erstellen, welches sowohl die Aktensystemmigration, als auch die Datenmigration, mitsamt der Bereitstellungs- und ggf. Außerbetriebnahme-Zeitpunkte der benötigten Komponenten berücksichtigt. Das Migrationskonzept MUSS dabei auch aufzeigen, welche Abhängigkeiten zu anderen TI-Diensten bestehen, wann und in welchem Umfang die Migration getestet wird und wie eventuelle Roll-Back-Szenarios aussehen.
[<=]

2.8.2 Durchführung der Migration

Das Aktenkonto muss durch den Anbieter für die Migration der Daten vorbereitet werden. Dabei müssen alle Maßnahmen umgesetzt werden, die im Zustand INITIALIZED eines neuen Aktenkontos vor der Aktivierung erforderlich sind (siehe 3.1.3- Anlage eines neuen Aktenkontos). Abweichend von den Maßnahmen für die Erstellung eines neuen Aktenkontos kann auf den Status INITIALIZED verzichtet werden und das Aktenkonto im Status ACTIVATED verbleiben.

Für ein zu migrierendes Aktenkonto sind alle Schritte anzuwenden, die auch für die Erstellung eines neuen Aktenkontos vor der Aktivierung erforderlich sind, insbesondere die Anlage der initialen Befugnisse für den Versicherten, den Kostenträger und die Ombudsstelle, sowie den E-Rezept-Fachdienst.

Im Anschluss an die Initialisierung erfolgt einmalig die Bereitstellung der Akten- und Kontextschlüssel durch ein ePA-FdV. Existierende Daten werden übertragen.

A_25148 - Migration: Information des Versicherten
Der Anbieter des ePA-Aktensystems MUSS den Versicherten über die Notwendigkeit und die Folgen einer Migration vor der eigentlichen Migration informieren, insbesondere darüber, welche Dokumentenformate und welche Berechtigungen übernommen und welche nicht übernommen werden, über die Freiwilligkeit einer Migration.**[<=]**

Die Entschlüsselung des Datenbestands für die Überführung in das vorbereitete Aktenkonto und die Migration der Berechtigungen der Vertreter wird durch die Nutzung eines ePA-FdV gemäß ePA-Version 3.x abgeschlossen. Bei der ersten Nutzung eines ePA-FdV durch den Versicherten mit dem zur Migration vorbereiteten Aktenkonto erfolgt die Migration über die vom ePA Aktensystem bereitgestellten Schnittstellen.

A_24922 - Migration: Schnittstellen zur Durchführung der Migration
Das ePA-Aktensystem MUSS für jedes Aktenkonto eine Migration von ePA 2.6 auf ePA 3.0 durchführen und geeignete Schnittstellen zum FdV anbieten, mit denen der Versicherte vom FdV das Entschlüsseln der verschlüsselten ePA 2.6-Akteninhalte anstoßen kann. **[<=]**

In der ePA für alle ist der Zugriff über einen Client der ePA-Version 2.x nicht mehr möglich, da sich die grundsätzliche Architektur und die Schnittstellen und Protokolle geändert haben.

2.8.3 Bereinigung von Registry und Repository im Zuge der Migration

A_24964 - XDS Document Service - Migration: Isolation der Migration
Der XDS Document Service MUSS die Verarbeitung von entschlüsselten Dokumenten, die im Rahmen der Migration durchgeführt werden, so technisch isolieren, dass kein Schaden für Aktenkonten oder das ePA-Aktensystem selbst entsteht.**[<=]**

Hinweis zu A_24964-: Hier kann z.B. eine Art Sandboxing oder eine separate VAU-Instanz verwendet werden, um die Isolation umzusetzen.*

A_25002 - XDS Document Service - Migration: Umbenennung von Ordnern
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 in den Werten von `Folder.codeList` die mit ePA 3.0 gegebenenfalls geänderten Kategoriennamen als Werte verwenden. **[<=]**

A_24562 - XDS Document Service - Migration: Auflösung abgekündigter Ordner
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 die abgekündigten Kategorien auflösen. Dabei MÜSSEN sämtliche Dokumente gemäß der Einordnungsregeln in A_19388-* neu Ordnern zugeordnet werden und die Ordner der abgekündigten Kategorien gelöscht werden.**[<=]**

A_25010 - XDS Document Service - Migration: Daten der Kategorie childsrecord verschieben
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 Daten, die dynamischen Folder der 2.6-Kategorie `childsrecord` zugeordnet sind, nur dann dem statischen Folder der 3.0-Kategorie `child` zugeordnet, wenn die Daten (des Kindes) dem Akteninhaber (der Kinderakte) zugeordnet werden können. Anderenfalls werden die Dokumente der dynamischen Folder der 2.6-Kategorie `childsrecord` dem Folder `other` zugeordnet.**[<=]**

Die in ePA 2 angelegten dynamischen Ordner der Kategorie `childsrecord` identifizieren Kinder, deren Daten nicht in ihren eigenen Akten gehalten wurden. Diese dynamischen Ordner sind nach folgender Regel in ePA 2 vom Primärsystem angelegt worden: Folder.title wurde mit dem Namen und Geburtsdatum des Kindes belegt. Bildungsregel: Nachname + ", " + 1. Vorname + " "Datum im Format TT.MM.YYYY. Beispiel: "Musterkind, Max 03.03.2017"

A_24963 - XDS Document Service - Migration: Keine Übernahme von Dokumenten mit unzulässigem Format
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 sämtliche Dokumente der ePA2.6 gemäß A_24864-* auf die zulässigen Dokumentenformate prüfen und Dokumente in einem nicht erlaubten Format nicht in die "ePA für alle" migrieren.**[<=]**

A_24966 - XDS Document Service - Migration: Konvertieren von PDF- in PDF/A-Dokumente
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 Dokumente im PDF-Format in ein PDF/A-Format konvertieren und ausschließlich das Dokument im PDF/A-Format in das Aktenkonto übernehmen.**[<=]**

A_25032 - XDS Document Service - Migration: Information des Versicherten zur Nichtübernahme von Dokumenten in bestimmten Formaten
Der Anbieter des ePA-Aktensystems MUSS den Versicherten darüber informieren, das Dokumente in der ePA2.6, die ein bestimmtes Format besitzen, nicht in die "ePA für alle" übernommen werden und informieren, um welche Formate es sich handelt.**[<=]**

A_24520 - XDS Document Service - Migration: Prüfsumme Dokument erzeugen
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 für jedes Dokument, das im Klartext vorliegt, die kryptographische Prüfsumme des

Dokumentes berechnen und in `DocumentEntry.hash` hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die Dokumentengröße für das Feld `DocumentEntry.size` berechnet und gesetzt werden. **[<=]**

A_24847 - XDS Document Service - Migration: Identifizieren und Auflösen von Dokumenten-Dubletten
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 zum Zeitpunkt der Entschlüsselung eine Dublettenerkennung durchführen. Dabei werden entschlüsselte Dokumente innerhalb und außerhalb von Sammlungen verglichen mit Dokumenten, die durch eine zwischenzeitliche Nutzung von ePA für alle in die Akte eingestellt worden sind. Dubletten werden anhand der Gleichheit des Hash-Wertes im Feld `documentEntry.hash` identifiziert. Das Dokument mit dem älteren Einstelldatum wird verworfen.**[<=]**

A_24851 - XDS Document Service - Migration: Dokumente und Ordner mergen
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf die ePA 3.0 zum Zeitpunkt der Entschlüsselung des Datenbestands die Ordnerinhalte einer Kategorie vergleichen, falls es neben den migrierten ePA 2.6-Akteninhalten durch eine ePA3-Aktennutzung ebenfalls Ordnerinhalte gibt. Unter Berücksichtigung der Dublettenprüfung werden alle Dokumente von zwei Ordnern derselben Kategorie (in ePA 2.6 bzw. 3.0 entstanden) in einen Ordner zusammengeführt. Dokumente und RPLC-Ketten, die durch die `documentEntry.uniqueId` erkennbar zusammen gehören, werden unter Wahrung der Abfolge der Einstelldaten zusammengeführt und das jüngste Dokument als aktives Dokument der Kette behandelt. Dokumente erhalten eine `rootDocumentUniqueId` gemäß A_24451-*, falls noch nicht vorhanden. **[<=]**

A_24848 - XDS Document Service - Migration: Auflösung von duplizierten dynamischen Ordnern
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf die ePA 3.0 anhand des Titels dynamischer Ordner erkennen, ob zwei dynamische Ordner zur selben Kategorie vorliegen, z.B. zur selben Schwangerschaft. In diesem Falle werden alle vorhandenen Einträge in einen der Odner hinein gemergt und der andere Ordner gelöscht.
[<=]

A_24522 - XDS Document Service - Migration: Erzeugen von Titeln für Dokumente
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf die ePA 3.0 sicherstellen, dass bei jedem Dokument das Metadatum `DocumentEntry.title` belegt ist. documentEntry.title=" " oder "" ist gleichbedeutend mit einem nicht vorhandenen Titel. Wenn title nicht belegt ist, MUSS`title` gemäß folgender Tabelle belegt werden.

Typ	Titel
Dokumente, die einem Implementation Guide zugeordnet sind	IG.displayName
andere Dokumententypen	Die gemäß A_24524-* bereinigte `DocumentEntry.URI` ohneExtension

[<=]

A_24523 - XDS Document Service - Migration: Löschen von ConfidentialityCodes
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 Dokumente und Ordner mit dem `confidentialityCode` "very restricted" auf die GlobalDenyPolicy setzen. Danach werden die confidentialityCodes gelöscht. **[<=]**

A_24817 - XDS Document Service - Migration: Normalisieren und Validieren der URI
Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 die ePA 3.0 für sämtliche Dokumente die `documentEntry.URI` gemäß A_24524-* und A_23447-* normalisieren und validieren.**[<=]**

A_24866 - Audit Event Service - Migration: Übernahme von Protokolldaten
Der Audit Event Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 sämtliche Protokolldaten des Versicherten in die migrierte Akte übernehmen. Für die Migration werden alte Dokumente in ein PDF/A überführt und in die Kategorie "patient" eingestellt. **[<=]**

2.8.4 Protokollierung der Migration

A_25029 - XDS Document Service - Protokollierung der Migration der medizinischen Daten
Der XDS Document Service MUSS den Vorgang der Migration der medizinischen Daten (Dokumente, Folder, Metdaten) gemäß A_24704* protokollieren. Dabei ist die Migration als atomares Ereignis zu betrachten und mit einem Protokolleintrag zu dokumentieren. Für den Protokolleintrag ist folgende Wertebelegung zu berücksichtigen:

Tabelle 2: Protokollierung der Migration der medizinischen Daten

Strukturelement	Wert	Erläuterung
AuditEvent.type	"object"	
AuditEvent.outcome	0	Migration war erfolgreich und ist abgeschlossen. Dieser Wert wird auch gesetzt, wenn einzelne Dokumente (z.b. Dokumente bestimmter Formate) nicht übernommen werden konnten.
	12	Migration wurde abgebrochen und wird ggf wiederholt, keine Datenübernahme ist erfolgt. In der AuditEvent.entity.detail Struktur werden keine Informationen hinterlegt.
AuditEvent.action	E	
AuditEvent.entity.name	"Migration"	
AuditEvent.entity.description	<Hinweistext>	

AuditEvent.entity.detail	**type**	**value[x]**	dieses Strukturelement ist zu versorgen, wenn einzelne Dokumente nicht übernommen werden konnten
	"DocumentTitle"	<DocumentEntry.title>	Name des Dokumentes, welches nicht übernommen werden konnte
	"DocumentUniqueId"	<Document.uniqueId>	ID des Dokumentes, welches nicht übernommen werden konnte
	"DocumentFormatCode"	<DocumentEntry.formatCode>	kodiert als Datentyp „Coded String“ gemäß [IHE-ITI- TF3].
	"DocumentMimeType"	<DocumentEntry.mimeType>	

[<=]

A_25031 - Audit Event Service - Protokollierung der Migration der Protokolldaten des Versicherten
Der Audit Event Service MUSS den Vorgang der Migration der Protokolldaten des Versicherten gemäß A_24704* protokollieren.
Dabei ist die Migration als atomares Ereignis zu betrachten und mit einem Protokolleintrag zu dokumentieren.
Für den Protokolleintrag ist folgende Wertebelegung zu berücksichtigen:

Tabelle 3: Protokollierung der Migration der Protokolldaten des Versicherten

Strukturelement	Wert	Erläuterung
AuditEvent.type	"object"	
AuditEvent.action	E	
AuditEvent.entity.name	"MigrationProtocol"	
AuditEvent.entity.description	<Hinweistext>	dieses Strukturelement ist nur zu versorgen, wenn bei der Migration Fehler aufgetreten sind

[<=]

2.9 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 Rohdatenlieferung 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 - Verarbeitung von UX-Messdaten
Das Aktensystem MUSS für die im zu betrachtenden Zeitintervall der Rohdatenlieferung (gemäß [gemSpec_Perf]) eingegangenen Messdaten je UX-Usecase und je ClientID 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 4: 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	Erfolgreicher Abschluss des Umzugs Widerspruch gegen die Nutzung der ePA	Unknown

	übertragen. Die Nutzung des Aktenkontos ist in diesem Zustand nicht möglich.	Der Bereitstellungszeitraum des Exportpakets ist abgelaufen.	Activated

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

A_24980 - Aktenkontoverwaltung – Protokollierung des Aktenkontostatus
Die Aktenkontoverwaltung MUSS bei Änderungen des Status eines Aktenkontos jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

Tabelle 5: Protokollierung von Änderungen des Aktenkontostatus

Strukturelement	Wert		Erläuterung
AuditEvent.type	"object"		
AuditEvent.action	E		Erste Aktivierung des Aktenkontos, Statuswechsel des Aktenkontos nach der ersten Aktivierung
AuditEvent.entity.name	"HealthRecordStatus"		Änderung des Aktenkontostatus
AuditEvent.entity.detail	**type**	**value[x]**	
	"previousRecordState"	<bisheriger Status des Aktenkontos>	Status des Aktenkontos vor der Änderung, beispielsweise "INITIALIZED"
	"RecordState"	<Status des Aktenkontos>	Zielstatus der Aktenkontos, beispielsweise "ACTIVATED"

[<=]

Hinweis: Der Statuswechsel von UNKNOWN auf INITIALIZED bei der Erstellung eines neuen Aktenkontos wird nicht protokolliert.

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 - Identifizerung 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_24302 - Anbieter ePA-Aktensystem - verpflichtende Nutzung von startRelocation
Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos durch Verwendung der Operation `startRelocation` gemäß [I_Information_Service_Accounts] auf Existenz eines Aktenkontos des Versicherten bei allen anderen Anbietern prüfen.**[<=]**

A_24790 - Anbieter ePA-Aktensystem - keine unbegründete Nutzung von startRelocation
Der Anbieter des ePA-Aktensystems DARF die Operation `startRelocation` gemäß [I_Information_Service_Accounts] für Zwecke abweichend der Vorgaben in A_24302* NICHT nutzen.**[<=]**

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.**[<=]**

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

A_15870-01 - Anbieter ePA-Aktensystem - Abbruch bei Nichtverfügbarkeit anderer Anbieter
Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen, wenn die Operation `startRelocation` gemäß `[I_Information_Service_Accounts]` mindestens bei einem anderen Anbieters eines ePA-Aktensystems eine technische Fehlermeldung liefert oder dieser nicht erreichbar ist.**[<=]**

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.**[<=]**

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.

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 Roll-out 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 Dokumente und 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_24359 - Anbieter ePA-Aktensystem - Löschen des Aktenkontos nach Widerspruch des Versicherten
Der Anbieter des ePA-Aktensystems MUSS das Aktenkonto eines Versicherten inklusive aller enthaltenen Daten löschen (sämtliche Dokumente, Schlüsselmaterial, Protokolle, Widerspruchsinformation, Befugnisse und Beschränkungen), wenn der Versicherte der grundsätzlichen Nutzung der ePA widerspricht. **[<=]**

A_24381 - Anbieter ePA-Aktensystem - Löschen des Aktenkontos nach Kündigung
Der Anbieter des ePA-Aktensystems MUSS das Aktenkonto eines Versicherten inklusive aller enthaltenen Daten nach Ablauf einer angemessenen oder gesetzlich bedingten Aufbewahrungsfrist löschen (sämtliche Dokumente, Schlüsselmaterial, Protokolle, Widerspruchsinformation, Befugnisse und Beschränkungen), wenn der Versicherte sein Aktenkonto gekündigt hat.**[<=]**

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 3.14.2- Information Service - Account).

A_24821 - Health Record Relocation Service - Suspendierung des Aktenkontos
Der Health Record Relocation Service MUSS sicherstellen, dass das Aktenkontos für die Erstellung eines Exportpakets auf den Status SUSPENDED gesetzt wird.**[<=]**

A_25191 - Health Record Relocation Service - Kein Exportpaket bei nicht migriertem ePA-2.x Aktenkonto
Falls das Aktenkonto ein bisher nicht migriertes ePA-2.x Aktenkonto ist, dann DARF das Aktenkonto NICHT in den Status SUSPENDED gesetzt werden und ein Exportpaket DARF NICHT erstellt werden.
[<=]

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 - 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 Mangement
- Constraint Management
- Audit Event Service
- Entitlement Management (außer Befugnisse für Versicherter, E-Rezept-Fachdienst, Kostenträger und Ombudsstelle).
- Device Management (nur KVNR / Mailaddressen der befugten Vertreter eines Aktenkontos)

[<=]

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

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_24787 - 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 aus der Anfrage zur Erstellung eines Exportpakets verwendet werden.**[<=]**

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 " CERTICATE_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 mit professionOID `oid_epa_mgmt` mittels des Zertifikats 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 Orginalwertes von DocumentEntry.URI aus dem alten Aktensystem dient.

[<=]

A_21548 - 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 FQDN des neuen Aktensystems des Versicherten informiert werden, so dass sie in der Lage sind, die erforderliche initiale Anmeldung und Geräteregistrierung durchzuführen.**[<=]**

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_24822 - Health Record Relocation Service - Löschen des Aktenkontos nach Umzug des Aktenkontos
Das Aktensystem MUSS sicherstellen, dass ein vorhandenes Aktenkonto eines Versicherten nach einem erfolgreichen Transfer zu einem anderen Anbieter, ggf. unter Einhaltung gesetzlicher Fristen, gelöscht wird.**[<=]**

A_24982 - 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 Wertebelegung zu berücksichtigen:

Tabelle 6 : Health Record Relocation Service Protokollierung

Strukturelement	Wert	Erläuterung
AuditEvent.type	"object"	
AuditEvent.action	E	Übertrag von Daten eines Aktenkontos von einem anderen Anbieter

AuditEvent.entity.name	"HealthRecordRelocation"		
AuditEvent.entity.detail	**type**	**value[x]**	
	"OriginName"	<Name des Kostenträgers>	Name des Kostenträgers, von welchem ein bestehendes Aktenkonto übernommen wird

[<=]

Hinweis: Statuswechsel des Aktenkontos im Kontext eines Wechsels des Anbieters erzeugen Protokolleinträge gemäß A_24980.*

Hinweis: Das Aktensystem des bisherigen Anbieters muss keine Protokolleintrag 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. dei Erstellung eines Exportpakets, ist in diesem Fall mangels eines existierenden Aktenkontos beim bisherigen Anbieter nicht erforderlich.

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

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

3.2.1.2 Abfrage existierendes Aktenkonto und Anfrage zum Transfer

Das Aktensystem (neu) fragt im Rahmen der Initialisierung des neuen Aktenkontos alle Aktensysteme der weiteren Betreiber an, ob bei diesen ein Aktenkonto für den Versicherten (KVNR) existiert. Schon bei dieser Anfrage an Aktensystem (alt) wird ein ENC-Zertifikat für die Verschlüsselung eines Exportpakets übermittelt. Das Aktensystem (alt), bei welchem das Aktenkonto existiert, bestätigt diese Anfrage zum Transfer mit einer Vorgangs-ID.

Starten des Transfers	
I_Information_Service_Accounts (bisheriges Aktensystem)	
`startRelocation`	Übergabe des ENC-Zertifikats, initiieren der Exportpaketerstellung

Existiert bei keinem Anbieter (alt) ein Aktenkonto des Versicherten, ist eine Datenübernahme nicht erforderlich und das Aktenkonto (neu) kann in den Status ACTIVATED überführt und der Transferprozess abgeschlossen werden.

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 übergibt das ENC-Zertifikat 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	
I_Health_Record_Relocation_Service_ (bisheriger Anbieter)	
`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 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	
I_Information_Service_Accounts (neues Aktensystem)	
`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	
I_Health_Record_Relocation_Service (neuer Anbieter)	
`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	
I_Information_Service_Accounts (bisheriges Aktensystem)	
`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		
I_Information_Service_Accounts (bisheriger Anbieter)		
`postExportPackageIncident`	Benachrichtigung zum Abbruch des Transfers	
	Incident	
	`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		
I_Information_Service_Accounts (bisheriges Aktensystem)		
`postExportPackageIncident`	Benachrichtigung zu Problemen beim Import des Exportpakets	
	Incident	
	`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) abzubrechen 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	
	Incident	
	`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	
	Incident	
	`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 - 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 VAU (genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- Privater Schlüssel der Verschlüsselungsidentität der VAU
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel
- Symmetrische Schlüssel für HMAC der VSDM-Prüfungsnachweise (jeweils einen pro VSD-Dienst-Betreiber)
- Symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)

- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU und ggf. für die Befugnisverifikations-VAU)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

A_24612 - 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 VAU
- Privater Schlüssel der Verschlüsselungsidentität der VAU
- Symmetrische Schlüssel für HMAC der VSDM-Prüfungsnachweise (jeweils einen pro VSD-Dienst-Betreiber)
- Symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU und ggf. für die Befugnisverifikations-VAU)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

A_24614 - 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 VAU
- Privater Schlüssel der Verschlüsselungsidentität der VAU
- Symmetrische Schlüssel für HMAC der VSDM-Prüfungsnachweise (jeweils einen pro VSD-Dienst-Betreiber)
- Symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU und ggf. für die Befugnisverifikations-VAU)
- 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.

A_24618 - ePA-Aktensystem - Zugriff auf Schlüssel und Informationen im VAU-HSM nur über Befugnisverifikations-Modul
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 ein Befugnisverifikations-Modul zugegriffen werden kann:

- Privater Schlüssel der Authentisierungsidentität der VAU (genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- Privater Schlüssel der Verschlüsselungsidentität der VAU

- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel
- Symmetrische Schlüssel für HMAC der VSDM-Prüfungsnachweise (jeweils einen pro VSD-Dienst-Betreiber)
- Symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU und ggf. für die Befugnisverifikations-VAU)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

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 integre und attestierte VAUs möglich. Die Prüfung der VAU-Attestierungstoken verbleibt in beiden Varianten im VAU-HSM (VAU-Token-Gate). 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 Aktenkontoverwaltung-VAU und die Befugnisverifikations-VAU möglich.

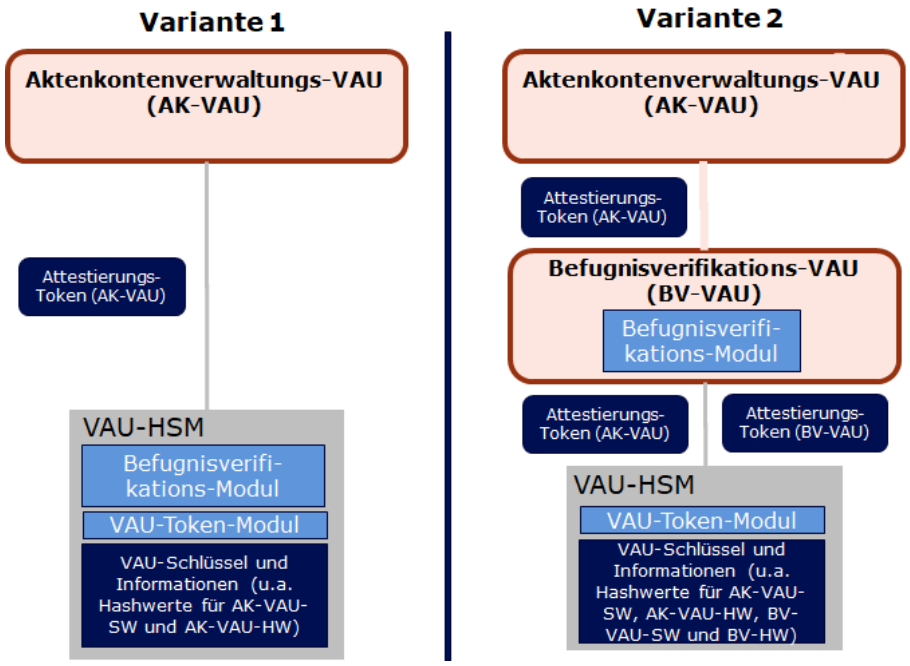

Abbildung 1 - Alternativen zur Ausführung des Befugnisverifikations-Moduls

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 Befugnisverifkations-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 - ePA-Aktensystem - VAU-Token-Modul nur durch Befugnisverifikations-Modul aufrufbar
Das ePA-Aktensystem MUSS sicherstellen, dass die Regeln des VAU-Token-Moduls ausschließlich von einem Befugnisverifikations-Modul aufgerufen werden.**[<=]**

Tabelle 7: Prüfregeln VAU Token

Regel	Beschreibung
hsm-r1	*Diese Regel dient zur Sicherung von Befugnissen mittels CMAC.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU

	• VAU-Attestierungstoken einer Befugnisverifikations_VAU (optional) • Befugnis = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum (opt.)) **Ausgangsdaten**: • Befugnis = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum (opt.)) gesichert mittels CMAC **Prüfschritte**: 1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen 1) - 3) erfolgreich waren, wird die übergebene Befugnis vom VAU-HSM mittels CMAC gesichert.
hsm-r2	*Diese Regel dient zur Ableitung der versichertenindividuellen Persistierungsschlüssel* **Eingangsdaten**: • KVNR • gewünschte Persistierungsschlüssel [Datenpersistierungsschlüssel und/oder Befugnispersistierungsschlüssel] • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) **Ausgangsdaten**: • falls in Eingangsdaten angefordert: versichertenindividueller Befugnispersistierungsschlüssel • falls in Eingangsdaten angefordert: versichertenindividueller Datenpersistierungsschlüssel **Prüfschritte**: 1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen 1) - 3) erfolgreich waren, wird der angeforderte versichertenindividuelle Befugnispersistierungsschlüssel und/oder versichertenindividuelle Datenpersistierungsschlüssel für die übergebene KVNR abgeleitet.
hsm-r3	*Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfungsnachweisen* **Eingangsdaten**:

	• Daten • Bezeichner des HMAC-Schlüssels • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) **Ausgangsdaten**: • HMAC der Daten mit dem symmetrischen Schlüssel, der zum übergebenen Bezeichner des HMAC-Schlüssels gehört **Prüfschritte**: 1. (opt.) prüfen der Signatur des VAU-Attestierungstokens für die Befugnisverifikations-VAU (herstellerspezifisch) 2. (opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen 1) - 2) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.
hsm-r4	*Diese Regel dient zur Nutzung des privaten Schlüssels der AUT-Identität der VAU* **Eingangsdaten**: • Challenge • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) **Ausgangsdaten**: • Challenge signiert mit privatem Schlüssel der AUT-Identität der VAU **Prüfschritte** 1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen in 1) bis 3) erfolgreich waren, wird die übergebene Challenge mit dem privatem Schlüssel der AUT-Identität der VAU signiert.
hsm-r5	*Diese Regel dient zur Nutzung des privaten Schlüssels der ENC-Identität der VAU* **Eingangsdaten**: • verschlüsselte Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) **Ausgangsdaten**: • entschlüsselte Daten **Prüfschritte** 1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-

	VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen in 1) bis 3) erfolgreich waren, werden die übergebenen verschlüsselten Daten mit dem privatem Schlüssel der ENC-Identität der VAU entschlüsselt.
hsm-r6	*Diese Regel dient zur Nutzung des CMAC-Schlüssels* **Eingangsdaten**: • Daten • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) **Ausgangsdaten**: • CMAC der Daten mit dem symmetrischen CMAC-Schlüssel **Prüfschritte**: 1. (opt.) prüfen der Signatur des VAU-Attestierungstokens für die Befugnisverifikations-VAU (herstellerspezifisch) 2. (opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen 1) - 2) erfolgreich waren, wird der CMAC über die Daten gebildet.

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.**[<=]**

3.4.2 Regeln des Befugnisverifikations-Moduls

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

Tabelle 8: Überblick über die Regeln des Befugnisverifikations-Moduls

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
rr1	Mit dieser Regel werden vom **Aktenkontoinhaber** am ePA-FdV erstellte **Befugnisse** 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 **Vertreter** am ePA-FdV erstellte **Befugnisse** für das Aktenkonto des Versicherten im Aktensystem registriert. Die im ePA-FdV erstellen	*Tab_AS_Entitlement_Registration_Rules*

	Befugnisse sind vom Vertreter mittels Signaturdienst signiert.	
rr3	Mit dieser Regel werden **Befugnisse** im Aktensystem registriert, die sich durch das **Stecken der eGK in einer Leistungserbringerumgebung** ergeben.	*Tab_AS_Entitlement_Registration_Rules*
rr4	Mit dieser Regel werden die **Befugnisse** für den Kostenträger und die zuständige Ombudsstelle bei der **Anlage eines Aktenkontos** im Aktensystem registriert.	*Tab_AS_Entitlement_Registration_Rules*
rr5	Mit dieser Regel werden die **Befugnisse** bei einem **betreiberübergreifenden Anbieterwechsel** im Aktensystem registriert.	*Tab_AS_Entitlement_Registration_Rules*
kr1	Diese Regel wird für die **Anmeldung** des **Aktenkontoinhabers** genutzt.	*Tab_AS_SDS-Key_Rules*
kr2	Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssels genutzt. Sie wird für die **Anmeldung** von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	*Tab_AS_SDS-Key_Rules*
kr3	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.	*Tab_AS_SDS-Key_Rules*
kr4	Diese Regel wird für die **Anmeldung** des **E-Rezept-Fachdienstes** verwendet.	*Tab_AS_SDS-Key_Rules*
autr	Diese Regel dient zum Nutzen des privaten Schlüssels der AUT-Identität der VAU.	*Tab_AS_AUT_ENC_Rules*
encr	Diese Regel dient zum Nutzen des privaten Schlüssels der ENC-Identität der VAU.	Tab_AS_AUT_ENC_Rules

A_24573 - ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls
Das Befugnisverifikations-Modul MUSS die in den Tabellen *Tab_AS_Entitlement_Registration_Rules*, *Tab_AS_SDS-Key_Rules* und *Tab_AS_AUT_ENC_Rules* definierten Regeln umsetzen.**[<=]**

Tabelle 9: Tab_AS_Entitlement_Registration_Rules - Regeln zur Registrierung von Befugnissen

Regel	Beschreibung
rr1	*Mit dieser Regel werden vom **Aktenkontoinhaber** am ePA-FdV erstellte Befugnisse im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token • Befugnis1 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) signiert vom Versicherten **Ausgangsdaten**: • Befugnis2 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) gesichert mittels CMAC **Prüfschritte**: 1. prüfen des ID-Tokens a. prüfen der Signatur gemäß A_25042-* (Zertifikatsprofil C.FD.SIG) b. prüfen, ob die professionOID im Signaturzertifikat `oid_idpd_sek` ist c. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt 2. prüfen der Befugnis1 a. prüfen der Signatur gemäß A_25042-* (Zertifikatsprofil C.CH.SIG) b. prüfen, ob die professionOID im Signaturzertifikat `oid_versicherter` ist c. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der "KVNR Aktenkonto" in der Befugnis1 übereinstimmt. d. prüfen, dass das JWT gemäß A_24587-* nicht abgelaufen ist (Feld: `exp`) 3. Falls die Prüfungen in 1) bis 2) erfolgreich waren, erstellt das Befugnisverifikations-Modul die Befugnis2. Die Inhalte werden aus Befugnis1 übernommen. 4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis2 a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

rr2	*Mit dieser Regel werden vom **Vertreter** 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.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • 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 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_idpd_sek` 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-* nicht abgelaufen ist (Feld: `exp`) 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befungnis3 vom Befugnisverifikations-Modul erstellt. Die Inhalte werden aus Befugnis1 übernommen. 3. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis3 a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis3 als Ergebnis des Regelaufrufs zurück.
rr3	*Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das **Stecken der eGK in einer Leistungserbringerumgebung** ergeben.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VSDM-Prüfungsnachweis signiert mit AUT-Identität der SMC-B **Ausgangsdaten**: • Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert

	mittels CMAC **Prüfschritte**: 1. prüfen der SMC-B-Signatur des signierten VSDM-Prüfungsnachweises gemäß A_25042-* (C.HCI.OSIG) 2. prüfen, dass das JWT gemäß A_24590-* nicht abgelaufen ist (Feld: exp) 3. prüfen, dass der Austellungszeitpunkt des VSDM-Prüfungsnachweises nicht länger als 20 Minuten zurückliegt 4. prüfen des HMAC des VSDM-Prüfungsnachweises mittels VAU-HSM Regel hsm-r3 a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 5. Falls die Prüfungen in 1) bis 4) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt: • Aktenkonto: die KVNR aus dem VSDM-Prüfungsnachweis • Telematik-ID: die Telematik-ID aus der SMC-B-Signatur • Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur. 6. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 7. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis als Ergebnis des Regelaufrufs zurück.
rr4	*Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der **Anlage eines Aktenkontos** im Aktensystem registriert.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Befugnis1 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) signiert mit SMC-B des Kostenträgers bzw. der Ombudsstelle **Ausgangsdaten**: • Befugnis2 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) gesichert mittels CMAC **Prüfschritte**: 1. Prüfen der Befugnis1 a. prüfen der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle gemäß A_25042-* (C.HCI.OSIG) b. prüfen, ob die professionOID im Signaturzertifikat `oid_kostentraeger` bzw. `oid_ombudsstelle` ist c. 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 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 erstellt. Die Inhalte der Befugnis2 sind: • Aktenkonto: die KVNR des Aktenkontos aus Befugnis1 • Telematik-ID: die Telematik-ID aus Befugnis1 3. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.
rr5	*Mit dieser Regel werden die **Befugnisse** bei einem **betreiberübergreifenden Anbieterwechsel** im Aktensystem registriert.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Befugnis1 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) signiert vom alten Aktensystembetreiber **Ausgangsdaten**: • Befugnis2 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) gesichert mittels CMAC **Prüfschritte**: 1. Prüfen der Befugnis1 a. prüfen der Signatur gemäß A_25042-* (C.FD.SIG) b. prüfen, ob im Signaturzertifikat C.FD.SIG der policyIdentifier `oid_epa_vau` ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 mit den Inhalten aus Befugnis1 erstellt. 3. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

A_24690 - 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 `aud` das ePA-Aktensystem eingetragen haben,
- das Feld `nonce` muss mit der ausgelösten Authentisierungsanfrage übereinstimmen.

[<=]

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 KVNR sein,
- das Feld `actorID` des JWT muss eine KVNR 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 10: Tab_AS_SDS-Key_Rules Key Rules - Regeln zur Ableitung der versichertenindividuellen Persistierungsschlüssel

Regel	Beschreibung
kr1	*Diese Regel wird für die Anmeldung des **Aktenkontoinhabers** genutzt.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token **Ausgangsdaten**: • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) • versichertenindividueller Befugnispersistierungsschlüssel (Secure Entitlement Storage Key) **Regelverhalten**: 1. Prüfen des ID-Tokens a. prüfen der Signatur gemäß A_25042-* (C.FD.SIG) b. prüfen, ob die professionOID im Signaturzertifikat `oid_idpd_sek` ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der

	KVNR aus dem ID-Token zur Ableitung von Befugnis- und Datenpersistierungsschlüssel aufgerufen. a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert die abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.
kr2	*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.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • KVNR (Aktenkonten-ID) **Ausgangsdaten**: • versichertenindividueller Befugnispersistierungsschlüssel (Secure Entitlement Storage Key) **Prüfschritte**: 1. Aufruf der VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der KVNR aus dem ID-Token zur Ableitung des Befugnispersistierungsschlüssels a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 2. Das Befugnisverifikations-Modul liefert den abgeleiteten Befugnispersistierungschlüssel als Ergebnis des Regelaufrufs zurück.
kr3	*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.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token • Befugnis = (KVNR Aktenkonto, BefugtenID (TID|KVNR), Gültigkeitszeitraum (opt.)) mit CMAC gesichert **Ausgangsdaten**: • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) **Prüfschritte**: 1. Prüfen des ID-Tokens a. prüfen der Signatur gemäß A_25042-* (C.FD.SIG) 2. Prüfen der Befugnis

	a. prüfen des CMAC der Befugnis mittels VAU-HSM Regel hsm-r6 i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. b. prüfen, ob die Nutzer-ID im ID-Token (KVNR oder Telematik-ID) mit der Befugten-ID in der Befugnis übereinstimmt. c. prüfen, ob die Befugnis noch gültig ist, falls die Befugnis zeitlich begrenzt ist (d. h. ein Gültigkeitszeitraum in der Befugnis enthalten ist). 3. Falls alle Prüfungen in 1) bis 2) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der KVNR aus dem ID-Token zur Ableitung des Datenpersistierungsschlüssels aufgerufen. a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. Das Befugnisverifikations-Modul liefert den abgeleiteten Datenpersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.
kr4	*Diese Regel wird für die Anmeldung des **E-Rezept-Fachdienstes** verwendet.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token • KVNR (Aktenkonten-ID) **Ausgangsdaten**: • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) • versichertenindividueller Befugnispersistierungsschlüssel (Secure Entitlement Storage Key) **Prüfschritte**: 1. Prüfen des ID-Tokens a. prüfen der Signatur gemäß A_25042-* (C.FD.SIG) b. prüfen, ob die professionOID im Signaturzertifikat oid_erp-vau ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der KVNR aus dem ID-Token zur Ableitung von Befugnis- und Datenpersistierungsschlüssel aufgerufen. a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert die abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.

Tabelle 11: Tab_AS_AUT_ENC_Rules Regeln für den Zugriff auf die privaten AUT- und ENC-Schlüssel der VAU

Regel	Beschreibung
autr	**Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Challenge **Ausgangsdaten**: • Challenge signiert mit privatem Schlüssel der AUT-Identität der VAU **Prüfschritte**: 1. Aufruf der VAU-HSM Regel hsm-r4 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der Challenge a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 2. Das Befugnisverifikations-Modul liefert die mit der AUT-Identität signierte Challenge als Ergebnis des Regelaufrufs zurück.
encr	**Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • verschlüsselte Daten **Ausgangsdaten**: • entschlüsselte Daten **Prüfschritte**: 1. Aufruf der VAU-HSM Regel hsm-r5 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und den verschlüsselten Daten a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 2. Das Befugnisverifikations-Modul liefert die mit der ENC-Identität entschlüsselten Daten als Ergebnis des Regelaufrufs zurück.

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.

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. **[<=]**

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. **[<=]**

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. **[<=]**

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.**[<=]**

3.5.1.3 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 authentisierte und vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen.**[<=]**

3.5.1.4 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 Betreibres notwendig werden.

Die Anforderungen zu den Betreiberprotokollen können im weiteren Verlauf der Umsetzung des ePA-Aktensystems

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.

[<=]

3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU

3.5.2.1 Schutz der Daten bei Verarbeitung in der VAU

A_24636 - ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen innerhalb einer VAU-Instanz
Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus ausschließen, dass sich innerhalb einer VAU-Instanz die Verarbeitungen eines Health Record Context oder einer User Session schadhaft auf die Verarbeitungen eines anderen Health Record Context oder einer anderen User Session auswirken können.
[<=]

Hinweis zu A_24636-*: Die Anforderung schließt eine Umsetzung mit Server-Threads, Worker und Ähnlichem nicht grundsätzlich aus, sofern die Sicherheitsleistung der Separation erbracht werden kann.

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_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_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 VAU

Die folgenden Anforderungen gewährleisten den Schutz der beim Betreiber des ePA-Aktensystems persistierten Daten. 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.**[<=]**

A_24853 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Informationen
Die VAU MUSS sicherstellen, dass alle Daten, die nicht mit dem versichertenindividuellen Daten- oder Befugnispersistierungsschlüssel verschlüsselt werden, vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems mit einem Schlüssel verschlüsselt werden, der nur über die VAU zugreifbar ist.**[<=]**

Hinweis: Hierzu gehören insbesondere die Informationen zum Device Management.

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-Aktenskystem - 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 authentisierte 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.**[<=]**

3.6 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.

3.7 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.

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).

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 SecureAdminStorageKey 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 3.14- 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 SecureAdminStorageKeys 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 3.12.1- XDS Document Service und 3.12.2- Medication Service) .

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

A_23874 - 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 12: 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-	Versorgungsprozess ("healthcareProcess")	"erp-submission"	"deny"/"permit"

Fachdienst			

[<=]

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 3.8.3- Befugnisausschluss (Blocked User Policy)).

Die Entscheidungen zu den widerspruchsfähigen Funktionen "medication' und "erp-submission" sind durch das Aktensystem abhängig assoziiert: Ein Widerspruch gegen die Nutzung der Funktion "erp-submission" setzt automatisch auch den Widerspruch gegen die Nutzung der Funktion "medication". Die Rücknahme eines Widerspruchs gegen die Funktion "medication" wird durch das Aktensystem abgelehnt, wenn gleichzeitig ein Widerspruch gegen die Nutzung von "erp-submission" vorliegt.

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 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 13: Consent Decision Management Protokollierung

Strukturelement	Wert		Erläuterung
AuditEvent.action	U		Update
AuditEvent.entity.name	"ConsentDecision"		Eintrag protokolliert eine Widerspruchsentscheidung
AuditEvent.entity.detail	**type**	**value[x]**	
	"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, dieses ist implizit mit der Protokollierung der Aktivierung bzw. Migration abgedeckt. Die spezifische Protokollierung erfolgt für Folgeänderungen.

3.8 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 - 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 (*)
Identifier des Aktenkontos (insurantId)	KVNR des Aktenkontos, für welches die Befugnis ausgestellt ist		ja
Identifier des befugten Nutzers (actorId)	Telematik-ID oder KVNR		ja
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 (tagesgenau) (letzter Tag der Gültigkeit, d.h eine heutige Befugnisvergabe für 3 Tage setzt für validTo das Datum	Eine unbegrenzt gültige Befugnis erhält den Wert 9999-12-31. Wird durch den Versicherten oder einen Vertreter oder das Entitlement Management gesetzt.	ja

	von übermorgen (aktueller Tag + 2 Tage). aktueller Tag ist inklusiv zu bewerten).		
Beginn der Gültigkeit, Ausstellungszeitpunkt (issued-at)	Datum und Zeitpunkt	Wird durch das Entitlement Management gesetzt.	nein
Identifier des Erstellers (issued-actorId)	Telematik-ID oder KVNR	Wird durch das Entitlement Management gesetzt.	nein
Name des Erstellers (issued-displayName)	Name der Institution, des Nutzers	Wird durch das Entitlement 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 - Entitlement Management - Erteilung von Befugnissen für berechtigte 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 berechtigte 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_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,
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 das Entitlement 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 3.8.3-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.

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_24504 - Entitlement Management - Löschen ungültiger Befugnisse
Das Entitlement Management MUSS vorhandene Befugnisse, deren Enddatum der Gültigkeit überschritten ist, unverzüglich aus dem Befugniskontext des Aktenkontos vollständig löschen.**[<=]**

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.**[<=]**

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_24987 - 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 Befugnisausschlüssen jeweils einen Protokolleintrag gemäß A_24704 erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

Tabelle 16: 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 Befugnisausschlüssen
	"EntitlementManagement"		Erteilen oder Entziehen von Befugnissen
AuditEvent.entity.detail	**type**	**value[x]**	
	"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"	<Identifier der Institution oder	ID der Institution oder des Nutzers für die eine

		des Vertreters>	Befugnis erteilt oder gelöscht wurden
	"entitledValidTo"	<Enddatum der Gültigkeit der Befugnis>	tagesgenaue Angabe des Endes einer erteilten Befugnis, Format: JJJJ-MM-TT

[<=]

Hinweis: Ein Update ("U") eines Entitlements liegt vor, wenn ein existierendes Entitlement aufgrund des längeren Gültigkeitszeitraums eines neuen Entitlements überschrieben wird.

3.8.1 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
Identifier 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
Identifier des Aktenkontos (insurantid)	KVNR des Versicherten	KVNR des Versicherten
Identifier 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

[<=]

A_24688 - Entitlement Management – Befugnisverifikation signierter initialer Befugnisse
Das Entitlement Management MUSS sicherstellen, dass die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle vor der Aktivierung des Aktenkontos 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.
[<=]

3.8.2 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` (Identifier des zu befugenden Nutzers), `kvnr` (Aktenkontold) 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.

3.8.2.1 Befugnisvergabe durch ein ePA-FdV

Ein ePA-FdV muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

A_24587 - 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"	Identifier (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 (tagesgenau)	2025-06-30

[<=]

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_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` = KVNR) ausschließlich durch den Versicherten erstellt oder gelöscht werden können. **[<=]**

A_24536 - Entitlement Management - Gültigkeitsdauer der Befugnisse für Vertreter
Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId` = KVNR) ausschließlichmit 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` = KVNR) eine E-Mail-Adresse des Vertreters für dessen Benachrichtigung angegeben wird.**[<=]**

A_24755 - Entitlement Management - Benachrichtigung des Vertreters bei Befugnisserstellung
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 MÜSSEN den Name des Versicherten enthalten sein. **[<=]**

A_25052 - Entitlement Management - Keine Benachrichtigung des Vertreters bei Befugnisersatz
Das Entitlement Management KANN auf die Benachrichtigung die Benachrichtigung des Vertreters durch eien E-Mail verzichten, wenn bei der Befugniserstellung eine existierende Befugnis des Vertreters ersetzt wird.**[<=]**

3.8.2.2 Befugnisvergabe durch ein Primärsystem

Ein Primärsystem muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

A_24590 - Entitlement Management - Befugnis durch ein Primärsystem
Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ein Primärsystem über die Schnittstelle I_Entitlement_Management durch 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

[<=]

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_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.**[<=]**

3.8.3 Befugnisausschluss (Blocked User Policy)

Das Entitlement Management erlaubt die Verwaltung von Widersprüchen des Versicherten oder eines Vertreters gegen die Nutzung des Aktenkontos durch spezifische Leistungserbringerinstitutionen.

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 - 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_institution-oegd
oid_institution-arbeitsmedizin

[<=]

Ein Eintrag der Blocked User Policy enthält Angaben gemäß der folgenden Tabelle: (Beispiel)

Tabelle 17: 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	2025-01-01T12:00:00Z

	Management gesetzt)	

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 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 das Zahnbonusheft der Datenkategorie "`dentalrecord`").
- 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_19303-12 - Legal Policy – gesetzlich vorgegebene Zugriffsrechte
Das Aktensystem MUSS alle in der folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

Tabelle 18: Legal Policy

Kategorie	Nutzergruppe										
Technischer Identifier	**Med**	**Apo**	**Pflege**	**GH**	**Physio**	**AM**	**KTR**	**OM**	**DiGA**	**eRP**	**Ver**
Medical Services (XDS Document Service)	**Zugriffsrecht gemäß § 352 SGB V**										
reports	CRUD	R	R	R	R	R	CU	-	-	-	RD
emp	CRUD	CRUD	R	R	R	R	-	-	-	-	RD
emergency	CRUD	R	R	R	R	R	-	-	-	-	RD
eab	CRUD	R	R	R	R	R	CU	-	-	-	RD
dental	CRUD	-	R	-	-	R	-	-	-	-	RD
child	CRUD	R	R	CRUD	R	R	-	-	-	-	RD (CU (*))
pregnancy_childbirth	CRUD	R	R	CRUD	R	R	-	-	-	-	RD
vaccination	CRUD	CRUD	R	R	-	CRUD	-	-	-	-	RD
patient	RD	R	R	R	R	R	-	-	-	-	CRUD
receipt	RD	RD	-	R	R	R	CU	-	-	-	RD
diga	R	R	R	R	R	R	-	-	CU	-	RD
care	CRUD	R	CRUD	R	R	R	-	-	-	-	RD
eau	CRUD	-	-	-	-	R	-	-	-	-	RD
rehab	CRU	-	-	-	-	-	-	-	-	-	RD

	D										
other	CRUD	-	-	-	-	R	-	-	-	-	RD
Medical Services (FHIR Data Service)	**Zugriffsrecht**										
medication	R	R	R	R	R	R	-	-	-	CU	R
Basic Services	**Zugriffsrecht**										
Consent Decisions	-	-	-	-	-	-	-	x	-	-	x
Constraints	-	-	-	-	-	-	-	-	-	-	x
Entitlements	x	x	x	x	x	x	-	-	-	-	x
Entitlements.Blocked User	-	-	-	-	-	-	-	x	-	-	x
Audit Events	-	-	-	-	-	-	-	x	-	-	x
Information	x	x	x	x	x	x	x	x	-	x	-
Devices	-	-	-	-	-	-	-	-	-	-	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_psychotherapeut oid_institution-oegd)
- Apo = Öffentliche Apotheke
  - (oid_öffentliche_apotheke)
- Pflege = Gesundheits-, Kranken- und Altenpflege
  - (oid_institution-pflege)
- GH = Geburtshilfe
  - (oid_institution-geburtshilfe)
- Physio = Physiotherapie
  - (oid_praxis-physiotherapeut)
- 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
- "-" = 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.

[<=]

Die folgende Tabelle erläutert die Kategorien aus A_19303-*:

Tabelle 19: Beschreibung der Kategorien

Technischer Identifier	**Beschreibung**
Medical Services	**XDS Document Service**
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 zum Nachweis der regelmäßigen Inanspruchnahme zahnärztlicher Vorsorgeuntersuchungen gemäß § 55 Absatz 1 in Verbindung mit § 92 Absatz 1 Satz 2 Nummer 2 (elektronisches Zahnbonusheft)
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)
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
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
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
Medical Services	**Medication Service**
medication	Verordnungs-, Dispensier- und Medikationsdaten in einer Elektronischen Medikationsliste (eML)

Basic Services	Account Management
Consent Decisions	Management der Entscheidungen zu widerspruchsfähigen Funktonen der ePA
Constraints	Management der Konfiguration der general Deny Policy und der User-specific 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 Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass Änderungen der Konfiguration der Legal Policy gemäß A_19303-* ausgeschlossen sind.**[<=]**

A_24548 - Legal Policy - Durchsetzung der Zugriffsrechte der Legal Policy
Das 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.**[<=]**

3.10 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 von Policies für jeden befugten Nutzer der betroffenen Nutzergruppen des Aktenkontos (zu den befugbaren Nutzern siehe auch 3.8- Entitlement Management).

Die folgend dargestellten Policies adressieren Nutzergruppen (professionOID) und spezifische Nutzer (Telematik-ID), sowie Metadaten der Daten. Bei jedem Zugriff auf Daten in Ordnern werden alle Policies mit einer Konfiguration bezüglich des betroffenen Dokuments, der Rolle und / oder ID eines Nutzers ausgewertet und durchgesetzt.

Die vorhandenen Policies sind:

General Deny Policy - verbirgt Dokumente, Kategorien oder Ordner für alle Leistungserbringerinstitutionen gemeinsam.

User-specific Deny Policy - verbirgt Dokumente, Kategorien oder Ordner für dedizierte Nutzer dieser Leistungserbringerinstitutionen.

Die folgende Anforderung zeigt eine Übersicht der Nutzergruppen und die mögliche Beschränkung von Zugriffen für Nutzer dieser Nutzergruppen durch die Policies.

A_24306 - Constraint Management- Policies für berechtigte Nutzergruppen und Nutzer
Das Constraint Management MUSS die Konfiguration von Policies und deren Anwendung auf die folgenden Nutzergruppen und Nutzer einschränken:

Nutzergruppe und Nutzer	Policies	
professionOID	General Deny Policy	User-specific Deny Policy
oid_praxis_arzt	x	x
oid_krankenhaus	x	x
oid_institution-vorsorge-reha	x	x
oid_zahnarztpraxis	x	x
oid_öffentliche_apotheke	x	x
oid_praxis_psychotherapeut	x	x
oid_institution-pflege	x	x
oid_institution-geburtshilfe	x	x
oid_praxis-physiotherapeut	x	x
oid_institution-oegd	x	x
oid_institution-arbeitsmedizin	x	x
oid_diga	x	x

Hinweis:
"x" bedeutet: diese Policy wird für die Nutzergruppe angewendet.
[<=]

A_24390 - Constraint Management- Anwendung der Policies
Das Constraint Management MUSS bei jedem Zugriff auf Daten durch den XDS Document Service durch befugte Nutzer oder Nutzergruppen die General Deny Policy und die User-specific Deny Policy anwenden und den Zugriff verhindern, wenn

- ein Dokument oder dessen assoziierter Ordner oder dessen assoziierte Datenkategorie in der General Deny Policy konfiguriert ist,
- ein Dokument oder dessen assoziierter Ordner oder dessen assoziierte Datenkategorie für den zugreifenden Nutzer in der User-specific Deny Policy konfiguriert ist.

[<=]

Dienste des Aktenkontos (Basic Services) können nicht verborgen werden. Hier gelten die Zugriffsregelungen gemäß Legal Policy und den Beschränkungen der Schnittstellen.

Datendienste (Medication Service) können nicht auf Daten- oder Ordnerebene verborgen werden. Hier gelten die Regelungen bezüglich des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA (siehe 3.7- 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 (siehe3.7- Consent Decision Management).

Die Operationen der Schnittstelle des Constraint Managements erlauben die Konfiguration der General Deny Policy und der User-specific 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 - Constraint Management - Protokolleinträge für Zugriffe auf das Constraint Management
Das Constraint Management MUSS für das Aufnehmen und Löschen von Einträgen in die General Deny bzw die User-Specific Deny Policy jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

Tabelle 20: 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 Ordnern)
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
	"User-specificDenyPolicy"		Eintrag für das Aufnehmen(Create) von Einträgen in die oder Löschen (Delete)

			von Einträgen aus der User sepcific Deny Policy
AuditEvent.entity.detail	**type**	**value[x]**	
	"DocumentTitle"	<XDSDocumentEntry.title>	wenn sich der Eintrag (Create oder Delete) der entsprechende Policy auf ein Dokument bezieht
	"RootDocumentId"	<rootDocumentId>	wenn sich der Eintrag (Create oder Delete) der entsprechende Policy auf ein Dokument bezieht
	"FolderTitle"	<XDSFolder.title>	wenn sich der Eintrag (Create oder Delete) der entsprechende Policy auf einen Folder bezieht
	"FolderEntryUUID"	<Folder.entryUUID>	wenn sich der Eintrag (Create oder Delete) der entsprechende Policy auf einen Folder bezieht
	"CategoryId"	<categoryId>	wenn sich der Eintrag (Create oder Delete) der entsprechende Policy auf eine Kategie bezieht
	"constrainedUserName"	<Name der LEI>	Name der LEI, auf die sich ein aufgenommener bzw gelöschter Eintrag der User specific Policy bezieht.
	"constrainedUserId"	<Telematik Id der LEI>	Telematik-ID der LEI, auf die sich ein aufgenommener bzw gelöschter Eintrag der User specific Policy

			bezieht.

[<=]

Für beide Policies gelten folgende Vorgaben.

A_24393 - Constraint Management - Initialisierung der Policies
Das Constraint Management MUSS für ein Aktenkonto eine General Deny Policy und eine User-specific Deny Policy, jeweils ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policies über die Schnittstelle `I_Constraint_Management_Insurant` gemäß [I_Constraint_Management_Insurant] ermöglichen.**[<=]**

A_24461 - Constraint Management - Konfiguration der Deny Policies anpassen nach Löschen von Dokumenten
Das Constraint Management MUSS Einträge aus der General Deny Policy oder User-specific Deny Policy entfernen, wenn diese ein spezifisches Dokument referenzieren und dieses Dokument aus dem Aktenkonto gelöscht wird.**[<=]**

A_24462 - Constraint Management - Konfiguration der Deny Policies anpassen nach Löschen von Ordnern
Das Constraint Management MUSS Einträge aus der General Deny Policy oder User-specific Deny Policy entfernen, wenn diese einen Ordner referenzieren und dieser Ordner aus dem Aktenkonto gelöscht wird.**[<=]**

A_24516 - Constraint Management - Speichern der Inhalte
Das Constraint Management MUSS Einträge aus der General Deny Policy und User-specific Deny Policy unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.**[<=]**

3.10.1 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 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. Enthält ein Eintrag der Policy einen Ordner oder eine Kategorie, so werden alle in diesem Ordner bzw. Kategorie enthaltenen Daten verborgen und von der Nutzung ausgeschlossen. Der Ordner bzw. die 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 (d. h. implizit dessen Daten) oder die Datenkategorie an sich verborgen werden. In letzterem Fall werden alle Daten in allen damit 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 21: Inhalt eines General Deny Policy Eintrags

Element		Inhalt	Erläuterung
policyType		"gdp"	General Deny Policy
denyType		"document" oder "folder" oder "category"	Art des zu verbergenden Inhalts,
parameter:			eine technische Referenz passend zu "denyType"
[choice]	rootDocumentId	documentEntry.referenceIdList, Item "rootDocumentUniqueId"	Identifier des zu verbergenden XDS Dokuments
	folderUUID	folder.entryUUID	Identifier des zu verbergenden dynamischen Ordners
	categoryId	categoryId	technischer Identifier der zu verbergenden Kategorie

Beispiel:

Tabelle 22: Verbergen eines Medical Service

General Deny Policy - Verbergen der Datenkategorie "Zahnbonusheft"		
policyType		"gdp"
denyType		"category"
parameters:		

	categoryId	"dentalrecord"

3.10.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes

Das Verbergen von Dokumenten kann auf Anweisung durch den Versicherten auch aus der Umgebung der Leistungserbringer erfolgen. Dazu wird durch den XDS Document Service beim Einstellen eines Dokuments der DocumentEntry.confidentialityCode der Dokumentmetadaten ausgewertet. Enthält der confidentialityCode beim Einstellen den Wert "CON" (constraint), wird durch das Aktensystem ein Eintrag in der General Deny Policy erzeugt.

Die Anforderungen zum Verbergen über den confidentialityCode sind im Kontext der Operationen des XDS Document Service definiert (siehe 3.12.1- XDS Document Service).

3.10.2 Nutzerspezifisches Verbergen (User-specific Deny Policy)

Das Aktensystem stellt für ein Aktenkonto eine User-specific Deny Policy bereit.

Die Konfiguration der User-specific Deny Policy erfolgt durch den Versicherten oder einen befugten Vertreter mittels ePA-FdV analog zur General Deny Policy und kann bestimmte Dokumente, Ordner oder Kategorien verbergen. Abweichend von der General Deny Policy sind Einträge der User-specific Deny Policy einem einzelnen, konkreten Nutzer zugeordnet, identifiziert über dessen Telematik-ID.

Die User-specific Deny Policy wird durch das Aktensystem für die in A_24306-* unter "User-specific Deny Policy" aufgeführten Nutzergruppen angewendet und durchgesetzt. Einträge der User-specific Deny Policy gelten dabei immer nur für den adressierten Nutzer.

Die User-specific Deny Policy ist bezüglich der Konfiguration der Einträge unabhängig von der General Deny Policy. Ein Dokument, ein Ordner oder eine Kategorie kann sowohl als Eintrag in der General Deny Policy als auch in der User-specific Deny Policy gleichzeitig enthalten sein. Gleichfalls können Einträge mit dem gleichen Dokument oder Ordner oder der gleichen Kategorie für verschiedene Nutzer gleichzeitig vorhanden sein.

Ein Eintrag der User-specific Deny Policy enthält Angaben gemäß der folgenden Tabelle:

Tabelle 23: Inhalt eines User-specificl Deny Policy Eintrags

Element		Inhalt	Erläuterung
policyType		"usdp"	User-specific Deny Policy
denyType		"document" oder "folder" oder "category"	Art des zu verbergenden Inhalts
parameter:			eine technische Referenz, passend zu "denyType"

[choice]	rootDocumentId	documentEntry.referenceIdList, Item "rootDocumentUniqueId"	Identifier des zu verbergenden Dokuments
	folderUUID	folder.entryUUID	Identifier des zu verbergenden dynamischen Ordners
	categoryId	categoryId	technischer Identifier der zu verbergenden Kategorie
	tid	Telematik-ID	Adressat der Beschränkung (Identifier)
	oid	profession-OID	Adressat der Beschränkung (Rolle)
	displayName	lesbarer Name / Bezeichnung	Name des Adressaten, definiert durch das ePA FdV, z. B. aus VZD-Eintrag

Beispiel:

Tabelle 24: Verbergen des Impfpasses für Apotheke "Musterapotheke"

User-specific Deny Policy - Verbergen der Datenkategorie "vaccination"		
policyType		"usdp"
denyType		"category"
parameters:		
	categoryId	"vaccination"
	tid	"3-xxxxxxxxxxxxxxx"
	oid	"1.2.276.0.76.4.54" (oid_öffentliche_apotheke)
	displayName	"Musterapotheke"

3.11 Geräteverwaltung

Die Geräteverwaltung ermöglicht ePA-FdVs die Registrierung und Verwaltung der vom Nutzer verwendeten Geräte und wird durch zwei Services realisiert.
Der Device Management Service stellt das API zum ePA-FdV für die Geräteverwaltung bereit und ist nur in einer VAU/User Session erreichbar.

Bei erstmaliger Nutzung des Gerätes wird eine Geräteregistrierung am ePA-Aktensystem im Rahmen der Nutzerauthentisierung gestartet, siehe auch 3.15.2- Anforderungen an den Authorization Service für die Authentisierung mit SMC-B . Der Device Management Service ermittelt die für den Nutzer im ePA-Aktensystem hinterlegte email-Adresse und übergibt diese dem Device Unlock Service.
Der Device Unlock Service befindet sich außerhalb der VAU, versendet bei der Geräteregistrierung eine E-Mail an den Nutzer zur Verifikation mit dem Bestätigungslink. Bestätigt ein Nutzer die Geräteregistrierung mittels Bestätigungslink, so empfängt und verarbeitet der Device Unlock Service diese Freischaltinformation.

A_24823 - Device Unlock Service - Erreichbarkeit
Das ePA-Aktensystem MUSS sicherstellen, dass der Device Unlock Service außerhalb von VAU/User Session erreichbar ist.**[<=]**

A_24824 - Device Unlock Service - Verification Information erzeugen
Der Device Unlock Service MUSS bei der Geräteregistrierung als Aufruf durch den Device Management Service einen deviceIdentifier (UUID) als eindeutigen Bezeichner für dieses Gerät und einen zugehörigen Verification Link erzeugen, im Device Unlock Service persistieren und an den Device Management Service zurückgeben. Der Verification Link MUSS genau diese Geräteregistrierung eindeutig adressieren und als URL aus dem Internet aufrufbar sein.**[<=]**

A_24974 - Device Unlock Service - Zufälligkeit des Verification Links
Der Device Unlock Service MUSS sicherstellen, dass der Verification Link eine Zufallszahl (base64-kodiert) mit mindestens 120 Bit Entropie und Erzeugung gemäß [gemSpec_Krypt#GS-A_4367] beinhaltet.**[<=]**

A_24825 - Device Unlock Service - E-Mail versenden
Der Device Unlock Service MUSS an alle E-Mail-Adressen, die bei der Geräteregistrierung übergeben werden, eine E-Mail für den Nutzer in einer verständlichen Form mit folgenden Informationen versenden:

- Verification Link
- Zweck der E-Mail.
- Zeitpunkt des Starts des Freischaltprozesses

[<=]

A_24826 - Device Unlock Service - Device Verification durchführen
Falls der Device Unlock Service einen gültigen Verification Link als Bestätigung des Nutzers zur Geräteregistrierung empfängt, MUSS das registrierte Gerät im Device Management Service als verifiziert gekennzeichnet werden. Anschließend MUSS der Device Unlock Service den Verification Link löschen. Ein ungültiger Verification Link führt ausschließlich zu einer für den Nutzer verständlichen Fehlermeldung.**[<=]**

Eine verständliche Fehlermeldung ist beispielsweise "Das Gerät kann nicht erneut registriert werden."

A_25167 - Device Unlock Service - Löschen der E-Mail-Adresse nach Versand Verification Link
Der Device Unlock Service MUSS die E-Mail-Adresse des Nutzers nach dem Versand der E-Mail mit dem Verification Link löschen.**[<=]**

A_24828 - Device Management Service - Realisierung der Schnittstelle I_Device_Management_Insurant
Der Device Management Service MUSS die Operationen der Schnittstelle `I_Device_Management_Insurant` gemäß [I_Device_Management_Insurant] umsetzen. **[<=]**

A_25164 - Device Management Service - Beschränkung der Schnittstellenoperationen auf Geräte des Nutzers
Der Device Management Service MUSS die Operationen der Schnittstelle `I_Device_Management_Insurant` gemäß [I_Device_Management_Insurant] auf die Geräte des aufrufenden Nutzers einschränken.**[<=]**

A_24975 - Geräteverwaltung – Protokollierung der Zugriffe auf Inhalte der Geräteverwaltung
Die Geräteverwaltung MUSS bei Anlage oder Änderungen von Einträgen zu registrierten Geräten des Versicherten oder eines Vertreters jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

Tabelle 25: Device Management Service Protokollierung

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die Api
	"object"		Bei Änderungen durch den Authorization Service oder die Geräteverwaltung selbst (Device Unlock Service)
AuditEvent.action	C		Erzeugen einer neuen Geräteregistrierung
	D		Löschen einer Geräteregistrierung durch den assoziierten Nutzer oder Löschen einer Geräteregistrierung nach Ablauf Wartezeit für Bestätigung
	U		Ändern des Status einer Geräteregistrierung durch den Device Unlock Service
AuditEvent.entity.name	"DeviceRegistration"		Setzen, Löschen und Anpassen von Geräteregistrierungen
AuditEvent.entity.detail	**type**	**value[x]**	
	"DeviceStatus"	<Status der	Status "pending" oder

		Registrierung>	"verified"
	"UserName"	<Name des Nutzers>	DisplayName des zugeordneten Nutzers des Geräts (Versicherter oder Vertreter)
	"UserId"	<KVNR>	KVNR des zugeordneten Nutzers des Geräts (Versicherter oder Vertreter)

[<=]

A_24979 - Device Management Service - Sichere Löschung von Geräten
Der Device Management Service MUSS beim Entfernen eines Gerätes sicherstellen, dass das Gerät gelöscht ist. **[<=]**

A_24917 - Device Management Service - Registrierung - E-Mail ermitteln
Der Device Management Service MUSS bei einer Geräteregistrierung die für diesen Nutzer hinterlegten E-Mail-Adressen ermitteln und an den Device Unlock Service übergeben.
[<=]

A_24918 - Device Management Service - Registrierung - deviceToken
Der Device Management Service MUSS bei einer Geräteregistrierung ein deviceToken erzeugen mit:

- Zufallszahl als String von 64 Zeichen mit einer Mindestentropie von 120 Bit gemäß [gemSpec_Krypt#GS-A_4367],
- eindeutig in der Menge aller für diese KVNR hinterlegten deviceToken.

[<=]

A_24920 - Device Management Service - Registrierung - Registrierung speichern
Der Device Management Service MUSS bei einer Geräteregistrierung die folgenden Inhalte für diesen Nutzer persistieren:

- createdAt (Zeitpunkt der Erzeugung)
- deviceToken (gemäß A_24918*)
- deviceIdentifier (gemäß A_24824*)
- status="pending" (Status der Registrierung als nicht verifiziert gekennzeichnet)
- displayName (vom Hersteller vergebener Gerätename)

[<=]

A_17947-03 - Device Management Service - Gültigkeitszeitraum und Löschung der Devicekennung
Der Device Management Service 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 hingeweisen wird und automatisch eine neue Registierung vom ePA-FdV am Aktensystem

ausgelöst wird.

A_14595 - Device Management Service - Pflegeprozess Geräteverwaltung
Der Device Management Service MUSS die interne Liste aller bekannten Geräte derart pflegen, dass ein Gerät nach spätestens 2 Jahren nach der letzten Nutzung des Gerätes automatisch aus der Liste der registrierten Geräte gelöscht wird.**[<=]**

A_14518 - Device Management Service - Freischaltprozess Freischalt-URL Transportsicherheit
Der Device Management Service MUSS in der generierten Freischalt-URL das https-Protokoll verwenden.
[<=]

A_14522-02 - Device Management Service - Freischaltprozess beenden
Der Device Management Service MUSS den Vorgang eines Freischaltprozesses zu `DeviceID` und Nutzer nach 6 Stunden Wartezeit beenden. Dieses beinhaltet auch die Löschung des Verification Links. Der ungültige Verification Link führt bei Nutzung ausschließlich zu einer für den Nutzer verständlichen Fehlermeldung.**[<=]**

3.12 Medical Services

3.12.1 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 3.10- Constraint Management).

3.12.1.1 Formatprüfung beim Einstellen von Dokumenten

A_24864 - 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-1a) (pdf)
- image/jpeg (jpeg oder jpg)
- image/png (png)
- image/tiff (tiff)
- text/plain (txt)
- application/xml (xml)
- application/hl7-v3 (xml)
- application/pkcs7-mime (p7)
- application/fhir+xml (xml)
- application/fhir+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.
[<=]

Hinweis 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.

A_25009 - 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-1a) (pdf)
- image/jpeg (jpeg oder jpg)
- image/png (png)
- image/tiff (tiff)
- text/plain (txt)
- application/xml (xml)
- application/fhir+xml (xml)

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.
[<=]

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.
[<=]

Hinweis zu A_24867-: Hier kann z.B. eine Art Sandboxing oder eine separate VAU-Instanz verwendet werden, um die Isolation umzusetzen.*

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.**[<=]**

3.12.1.2 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_14735 - XDS Document Service – Verpflichtende Nutzung des "mustUnderstand"-Attributs im SOAP Security Header
Der XDS Document Service MUSS SOAP 1.2-Nachrichten mit SAML 2.0 Assertions im SOAP Security Header mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren, sofern das SOAP 1.2 `mustUnderstand`-Attribut im SOAP Security Header nicht angegeben ist oder den Wert `false` bzw. `0` hat ([SOAP12#5.2.3] [WSS#5]).**[<=]**

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.

3.12.1.3 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
xacml	urn:oasis:names:tc:xacml:2.0:policy:schema:os
xdsb	urn:ihe:iti:xds-b:2007
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

3.12.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von Dokumenten

3.12.1.4.1 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 3.12.1.4.2-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 3.12.1.6 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.**[<=]**

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.**[<=]**

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 Authenticaton 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 "XDSDocument 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.**[<=]**

3.12.1.4.1.1 Gruppierungen mit anderen IHE ITI-Akteuren
A_15093-02 - XDS Document Service – Gruppierung RMU Update Responder mit Document Registry und X-Service Provider
Der XDS Document Service als RMU-Akteur "Update Responder" MUSS mit dem XDS-Akteur "Document Registry" gemäß [IHE-ITI-RMU] gruppiert sein.**[<=]**

3.12.1.4.1.2 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.**[<=]**

3.12.1.4.1.3 Gruppierungen mit anderen IHE ITI-Akteuren
A_14785 - XDS Document Service – Gruppierung XDS Document Registry mit APPC Content Consumer
Der XDS Document Service als XDS-Akteur "Document Registry" MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert sein.**[<=]**

3.12.1.4.1.4 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.**[<=]**

3.12.1.4.1.5 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.**[<=]**

3.12.1.4.2 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 26: 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 27: 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	X				

Source / Repository		
XDS On-Demand Document Source	X	
XDS Patient Identity Source	X	

3.12.1.4.3 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. **[<=]**

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.**[<=]**

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.**[<=]**

A_24451 - XDS Document Service - Automatisches initales 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.**[<=]**

3.12.1.4.3.1 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_15162-05 - 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)
- urn:ihe:iti:2007:AssociationType:APND (Append).

[<=]

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_23538 - XDS Document Service - vereinfachte Prüfung der Metadaten in DocumentEntry.eventCodeList

Der XDS Document Service KANN einen eventCode in DocumentEntry.eventCodeList ohne eine Prüfung, ob dieser eventCode im angegebenen Code System enthalten ist, akzeptieren, wenn das angegebene Code System eines der folgenden ist:

- ICD10gm (urn:oid:1.2.276.0.76.5.518)
- OPS (urn:oid:1.2.276.0.76.5.519)
- KDL (urn:oid:1.2.276.0.76.5.533).

[<=]

A_23123 - XDS Document Service – APND-Assoziation mit existierenden Dokument oder Dokument aus SubmissionSet

Der XDS Document Service MUSS bei APND-Assoziationen sowohl Verknüpfungen auf ein existierendes Dokument im Status "Approved" als auch auf ein Dokument aus dem übergebenen SubmissionSet ermöglichen.**[<=]**

A_23124 - XDS Document Service – Addendum nur mit einem Dokument verknüpfen

Der XDS Document Service DARF ein Addendum NICHT mit mehr als einem Dokument verknüpfen.**[<=]**

A_23125 - XDS Document Service – Kein automatisches "Deprecated" des Addendums

Der XDS Document Service DARF abweichend von [IHE-ITI-TF3#4.2.2.2.3] einem Addendum NICHT den availabilityStatus = Deprecated zuweisen, wenn das verknüpfte Dokument den availabilityStatus Depracated erhält.**[<=]**

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 - 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.**[<=]**

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 `XDSDuplicateFolder` 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 einem `MaxDocSizeExceeded`- 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 Verschlüsselung durch den Dokumentenschlüssel und ohne Transportcodierung. Größere Dokumente können nicht hochgeladen werden.

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.**[<=]**

3.12.1.4.3.2 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.UniqueId 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. **[<=]**

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.**[<=]**

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.**[<=]**

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.**[<=]**

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 die Komponente ePA-Dokumentenverwaltung 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.

3.12.1.4.3.3 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_14926-02 - XDS Document Service – Automatisiertes Löschen der Dokumente bei Remove Metadata
Der XDS Document Service MUSS bei zu löschenden DocumentEntry-Einträgen und assoziierten Dokumente im selben Zuge auch die über RPLC-assoziierten DocumentEntry-Einträge und Dokumente löschen.**[<=]**

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_21714-02 - XDS Document Service – Löschen von strukturierten Dokumenten durch ein ePA-FdV
Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners eines ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente 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 dem XDSRegistryError-Fehlercode zurückgeben werden. Werden einzelne strukturierte Dokumente der statischen Ordner vom Typ "vaccination", "dental", "child" gelöscht, MUSS der XDS Document Service diese Anfrage ebenso mit der o. g. Vorgabe ablehnen.
[<=]

A_21817-01 - XDS Document Service – Löschen von strukturierten Dokumenten durch ein Primärsystem
Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners eines Primärsystems ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente 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 XDSRegistryError-Fehlercode zurückgeben werden. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements der Wert "Anfragenachricht darf ausschließlich uniqueID für Folder beinhalten" belegt werden.**[<=]**

A_24663 - XDS Document Service – Bereinigung Deny Listen
Der XDS Document Service MUSS als Folge von erfolgreichen Löschanfragen alle Einträge der General Deny Policy und der User-specific 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).

3.12.1.4.3.4 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.**[<=]**

3.12.1.4.3.5 Restricted Update Document Set [ITI-92]
A_15061-03 - XDS Document Service – Ablauflogik für Restricted Update Document Set
Der XDS Document Service MUSS die Umsetzung der Operation `RestrictedUpdateDocumentSet` 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`, der identisch mit dem zu aktualisierenden `DocumentEntry` ist (inklusive entryUUID) und sich nur in den Metadaten gemäß A_15083* unterscheidet,
- 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.

Der XDS Document Service DARF die gesendete `Association` und das neue `SubmissionSet` NICHT dauerhaft speichern.**[<=]**

A_15082-02 - XDS Document Service – Validierung der Metadaten aus ITI Document Sharing-Profilen
Der XDS Document Service MUSS die übermittelten DocumentEntry-Metadaten der Operation `RestrictedUpdateDocumentSet` 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 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_15083-05 - XDS Document Service – Prüfung auf ausschließliche Aktualisierung der erlaubten Metadaten
Der XDS Document Service MUSS die übermittelten DocumentEntry-Metadaten der Operation `RestrictedUpdateDocumentSet` dahingehend prüfen, dass gegenüber den Bestandsdaten ausschließlich die folgenden Metadaten geändert werden:

- DocumentEntry.author
- DocumentEntry.classCode
- DocumentEntry.comments
- DocumentEntry.confidentialityCode
- 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 andere Aktualisierungen für die übermittelten Metadatenattribute in der Eingangsnachricht enthalten sind, MUSS der XDS Document Service diese ignorieren und ausschließlich die Aktualisierung der erlaubten Metadaten durchführen. 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_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 Operation `RestrictedUpdateDocumentSet` für Dokumente einer mixed- oder uniform-Sammlung aufgerufen wird MUSS der XDS Document Service das Aktualisieren der Metadatenattribute ablehnen, mit einem `XDSRepositoryMetadataError` quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements den Text "Metadata Update for MIOs not allowed" angeben.
[<=]

3.12.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen

A_24508 - 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, der General Deny Policy und der User-specific Deny Policy filtern, d. h. die Suchergebnismenge enthält ausschließlich XDS-Metadaten, die für einen angemeldeten Nutzer nicht diesen Policies widersprechen.**[<=]**

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 - XDS Document Service – Prüfung Herunterladen eines verborgenen Dokuments
Der XDS Document Service MUSS die Ausführung der Retrieve-Operation mit dem Fehlercode XDSDocumentUniqueIdError beenden, wenn für den angemeldeten Nutzer die Regeln der General Deny Policy und der User-specific Deny Policy nicht erfüllt sind.**[<=]**

A_24511 - XDS Document Service – Prüfung Löschen eines verborgenen Dokuments oder dynamischen Ordners
Der XDS Document Service MUSS die Ausführung der Remove-Operation mit dem Fehlercode XDSUnreferencedObjectException beenden, wenn für den angemeldeten Nutzer die Regeln der General Deny Policy und der User-specific Deny Policy nicht erfüllt sind.
Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die Liste der UUIDs der identifizierten Dokumente oder Ordner (DocumentEntry.entryUUID bzw. Folder.entryUUID) angegeben werden.**[<=]**

A_24512 - XDS Document Service – Prüfung Schreiben eines Dokuments in einen verborgenen dynamischen Ordner
Der XDS Document Service MUSS die Ausführung der Provide-Operation mit dem Fehlercode InvalidDocumentContent beenden, wenn für den angemeldeten Nutzer die Regeln der General Deny Policy und der User-specific Deny Policy nicht erfüllt sind.
Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die Liste der UUIDs der identifizierten Dokumente oder Ordner (DocumentEntry.entryUUID bzw. Folder.entryUUID) angegeben werden.**[<=]**

A_24513 - XDS Document Service – Prüfung Aktualisierung Metadaten eines verborgenen Dokuments
Der XDS Document Service MUSS die Ausführung der Update-Operation mit dem Fehlercode LocalPolicyRestrictionError beenden, wenn für den angemeldeten Nutzer die Regeln der General Deny Policy und der User-specific Deny Policy nicht erfüllt sind. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die Liste der UUIDs der identifizierten Dokumente oder Ordner (DocumentEntry.entryUUID bzw. Folder.entryUUID) angegeben werden.**[<=]**

3.12.1.5 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.**[<=]**

3.12.1.6 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_17969, 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.

3.12.1.6.1 Schnittstelle I_Document_Management

Weitere Vorgaben zu den Operationen befinden sich in 3.12.1.4.3- 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 28: 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	DocumentManagementService.wsdl	
XML Schema	• PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd	

[<=]

Durch die Legal Policy ist geregelt, welche Clients (professionOID) letztendlich zugreifen dürfen.

3.12.1.6.1.1 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.

A_14941-06 - 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 die folgenden Association Types nach [IHE-ITI-TF3#4.2.2] enthalten:

- `urn:ihe:iti:2007:AssociationType:XFRM` (Transform)
- `urn:ihe:iti:2007:AssociationType:XFRM_RPLC` (Transform and Replace)
- `urn:ihe:iti:2007:AssociationType:signs` (Digital Signature)
- `urn:ihe:iti:2010:AssociationType:IsSnapshotOf` (Snapshot of On-Demand document entry).

[<=]

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-Ordnern
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_13798-02 - 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 der 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`-Fehlercode 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_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 NDF- oder DPE-Dokument einzustellen, MUSS mit dem IHE-Error`InvalidDocumentContent` 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-Error `InvalidDocumentContent` abgebrochen werden. Es MUSS im `codeContext`-Attribut des zurückgegebenen `InvalidDocumentContent`-Elements der Text "Medical information object has to be unique" zurückgegeben werden.**[<=]**

A_24526 - XDS Document Service - Setzen der General Deny List
Falls beim Einstellen eines Dokuments das Metadatum confidentialityCode=CON gesetzt ist, MUSS der XDS Document Service die General Deny List so konfigurieren, dass das Dokument der Liste der zu verbergenden Dokumente bzw. Ordner hinzugefügt wird.**[<=]**

Zur Konfiguration der General Deny List wird die versionsübergreifende ID für Dokumente (siehe A_24451) verwendet.

A_24531 - Constraint Management - Verbergen von Dokumenten durch confidentialityCode
Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) eingestellt wird, nicht Bestandteil einer Sammlung, also eines Ordners der Ausprägung "mixed" oder "uniform" 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.**[<=]**

Aus der Umgebung der Leistungserbringer können auf diesem Weg Dokumente lediglich verborgen werden. Verborgene Inhalte können aus der Umgebung der Leistungserbringer nicht sichtbar gemacht werden. Diese Art des Verbergens ist nicht auf Dokumente anwendbar, die Bestandteil eines Ordners des Typs "mixed" oder "uniform" sind. Die dort enthaltenen MIOs oder strukturierten Dokumente können nur durch ein ePA-FdV kategorie- oder ordnerbasiert verborgen werden.

Die Anforderungen zum Verbergen über den confidentialityCode sind im Kontext der Operationen des XDS Document Service definiert.

3.12.1.6.1.2 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.

3.12.1.6.1.3 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.

3.12.1.6.1.4 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.

3.12.1.6.1.5 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 3.12.1.4.3.5- Restricted Update Document Set [ITI-92] .

3.12.1.6.2 Schnittstelle I_Document_Management_Insurant

Weitere Vorgaben zu den Operationen befinden sich in 3.12.1.4.3- 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 29: 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 in der Dokumentenverwaltung
	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	DocumentManagementService.wsdl	

XML Schema	• PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd

[<=]

3.12.1.6.2.1 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_21481-04 - XDS Document Service – Kein Einstellen von Ordnern und Associations
Die Komponente ePA-Dokumentenverwaltung 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
- APND

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_22400-01 - XDS Document Service - Ablehnung Upload bei abweichenden confidentialityCode
Der XDS Document Service MUSS Uploads, die als Resultat einen uneinheitlichen documentEntry.confidentialityCode über alle Dokumente in einer mixed- oder uniform-Sammlung haben, mit einem XDSRegistryMetadataError ablehnen.**[<=]**

Die Anforderung bezieht sich auf Einträge in documentEntry.confidentialityCode die nicht aus dem ValueSet zum Verbergen (confidentialityCode=CON), resultieren.

Diese Art des Verbergens mit confidentialityCode=CON ist nicht auf Dokumente anwendbar, die Bestandteil eines Ordners des Typs "mixed" oder "uniform" sind.

A_24797 - 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.**[<=]**

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. **[<=]**

3.12.1.6.2.2 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.

3.12.1.6.2.3 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.

3.12.1.6.2.4 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.

3.12.1.6.2.5 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 3.12.1.4.3.5- Restricted Update Document Set [ITI-92].

3.12.1.7 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 - 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
care	2d62bf9e-062a-4aa7-9951-9f33bbc665b5
eau	aa7d10d6-204a-47aa-be73-44bdcb77512f
other	605a9f3c-bfe8-4830-a3e3-25a4ec6612cb
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31
rehab	173f4204-fb93-4a1a-a1f6-316703b79539

[<=]

Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner vom Typ "pregnancy_childbirth", mit dem Folder.title für den Namen des Kindes bzw. ein Kennzeichen der Schwangerschaft (A_22515-).*

A_20216-03 - 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 von der Dokumentenverwaltung aktualisiert, sobald Dokumente in den Ordner eingestellt oder daraus gelöscht werden, siehe auch [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6].

[<=]

3.12.1.8 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.

3.12.1.8.1 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_14760-22 - 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	FV Edit
	PS	KTR	DS	FdV			
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 3.12.1.8.2-Metadaten der Dokumente und SubmissionSets 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 3.12.1.8.2-Metadaten der Dokumente und SubmissionSets (A_21209) genügen.	X
authorRole	0..n	0..n	0..0	0..n	Rolle des Autors	Der Wert MUSS einem Code des in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.authorRole entsprechen.	X
authorSpecialty	0..n	0..0	0..0	0..n	Fachliche Spezialisierung des Autors	Der Wert MUSS einem Code des in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.authorSpecialty entsprechen.	X
authorTelecommunication	0..n	0..0	0..0	0..n	Telekommunikationsdaten des Autors	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	X

availabilityStatus	0..0	0..0	1..1	0..0	Status des Dokuments ("Approved" oder "Deprecated")	Der Wert MUSS initial "`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" entsprechen.	
classCode	1..1	1..1	0..0	1..1	Grobe Klassifizierung des Dokuments	Der Wert MUSS einem Code des in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.classCode entsprechen. Sofern das Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.12.1.9-Strukturierte Dokumente genügen. PS-KTR MUSS ausschließlich den Code "`ADM`" (Administratives Dokument) aus dem in [gemSpec_Voc_ePA] definierten Value Set für DocumentEntry.classCode verwenden.	X
comments	0..1	0..1	0..0	0..1	Ergänzende Hinweise in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.4] genügen.	X
confidentialityCode	0..n	0..n	0..0	0..n	Vertraulichkeitskennzeichnung des Dokuments	Es sind die folgenden Codes unter der OID "`1.2.276.0.76.5.491`" mit dem Code System Name "`ePA-Vertraulichkeit`" definiert. Für `ProvideAndRegisterDocumentSet-b` gilt: Es MUSS für das Verbergen des Dokumentes der Codes • Code = "`CON`", Display Name = "`constraint`" aus dem Code System `1.2.276.0.76.5.491` (siehe auch [gemSpec_Voc_ePA]) gesetzt werden.	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 einem Code des in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.eventCode entsprechen.	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 zugreifenden System erlauben, im Vorfeld festzustellen, ob das Dokument verarbeitet werden kann.	Der Wert MUSS einem Code des in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.formatCode oder aus der Tabelle in der Anforderung A_14761-* entsprechen. Der Wert KANN `"urn:ihe:iti:xds:2017:mimeTypeSufficient"` (siehe [IHE-ITI-TF-3#4.2.3.2.9]) entsprechen, um anzuzeigen, dass über den MIME-Type hinaus keine genaueren Angaben zum Dokumentenformat gemacht werden können oder der MIME-Type ausreichend ist. Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.12.1.9-Strukturierte Dokumente genügen.	
hash	0..	0..	1..	0..	Kryptographische	Der Wert wird vom XDS	

	0	0	1	0	Prüfsumme des Dokuments	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 in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.healthcareFacilityTypeCode entsprechen. Das PS-KTR MUSS ausschließlich den Code "VER" (Versicherungsträger) aus dem in [gemSpec_Voc_ePA] definierten Value Set für DocumentEntry.healthcareFacilityTypeCode verwenden. 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 in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.languageCode entsprechen. Es MÜSSEN mindestens die in der Tabelle Tab_LanguageCodes angegebenen Codes unterstützt werden, alle weiteren Codes KÖNNEN unterstützt werden.	X
legalAuthenticator	0..1	0..0	0..0	0..1	Rechtlich Verantwortlicher für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.14] genügen. Das Attribut DARF NICHT gesetzt werden, falls es sich um ein automatisch erstelltes und nicht durch eine natürliche Person freigegebenes Dokument handelt.	

limitedMetadata	0..0	0..0	0..0	0..0	Markierungsattribut, dass das Metadatenelement DocumentEntry nicht den vollständigen Satz an Metadaten enthält.		
mimeType	1..1	1..1	0..0	1..1	MIME-Type des Dokuments	Ein Wert aus der folgenden Liste gemäß A_24864* und A_25009* MUSS als MIME-Type verwendet werden. Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.12.1.9-Strukturierte Dokumente genügen. Anmerkung: In Klammern sind die Extentions angegeben, die beim entsprechenden MIME-Type in DocumentEntry.URI für das URI-scheme "file„ zu verwenden sind.	
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	Der Wert MUSS einem Code des in [gemSpec_Voc_ePA] definierten Value Sets für	X

					Einrichtung, in der das dokumentiere Ereignis stattgefunden hat.	DocumentEntry.practiceSettingCode entsprechen. Die DiGA MUSS practiceSettingCode mit dem Wert "PAT" belegen.	
referenceIdList	0..n	0..0	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.	
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 `DocumentEntry.title=""` 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 in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.typeCode entsprechen. Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Inhalts- und Formatvorgaben aus Abschnitt 3.12.1.9-Strukturierte Dokumente genügen.	X
uniqueId	1..1	1..1	0..0	1..1	Eindeutige, aktenweite Kennung des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.26] genügen.	
URI	1..1	1..1	0..0	1..1	URI für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.27] genügen und mittels A_24524-* normalisiert werden. Die extension der DocumentEntry.URI MUSS wird dem mimetype gemäß A_23447-* angepasst, falls erforderlich.	
Metadaten für SubmissionSet							
author	1..n	1..1	0..0	1..1	Person oder System, welche(s) das Submission Set erstellt hat.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.1] genügen.	
authorPerson	0..1	0..1	0..0	1..1	Name der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus Abschnitt 3.12.1.8.2-Metadaten der Dokumente und	

							SubmissionSets genügen.	
	authorInstitution	1..1	1..1	0..0	0..0	Institution, welcher die einstellende Person oder das einstellende System zugeordnet ist.	Der Wert MUSS den Formatvorgaben aus Abschnitt 3.12.1.8.2-Metadaten der Dokumente und SubmissionSets (A_21209*) genügen.	
	authorRole	1..n	1..n	0..0	1..1	Rolle der einstellenden Person oder des einstellenden Systems	Der Wert MUSS einem Code des in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.authorRole entsprechen. Das PS-KTR MUSS den Code "105" (Kostenträgervertreter) aus dem in [gemSpec_Voc_ePA] definierten Value Set für DocumentEntry.authorRole verwenden. Das ePA-Frontend des Versicherten MUSS den Code "102" (der Patient selbst) aus dem in [gemSpec_Voc_ePA] definierten Value Set für DocumentEntry.authorRole verwenden. Die DiGA MUSS authorRole mit dem Code "12" (dokumentierendes Gerät) belegen.	
	authorSpecialty	0..n	0..0	0..0	0..n	Fachliche Spezialisierung der einstellenden Person oder des einstellenden Systems	Der Wert MUSS einem Code des in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.authorSpecialty entsprechen.	
	authorTelecommunication	0..n	0..0	0..0	0..n	Telekommunikationsdaten der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	

availabilityStatus	0..0	0..0	1..1	0..0	Status des Submission Sets ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
comments	0..1	0..1	0..0	0..1	Ergänzende Hinweise zum Submission Set in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.3] genügen.	X
contentTypeCode	0..1	0..1	0..0	0..1	Klinische Aktivität, die zum Einstellen des Submission Set geführt hat.	Der Wert MUSS einem Code des in [gemSpec_Voc_ePA] definierten Value Sets für SubmissionSet.contentTypeCode entsprechen.	
entryUUID	1..1	1..1	0..1	1..1	Intern verwendete, aktenweit eindeutige Kennung des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.5] genügen. 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.	
Metadaten für dynamische Folder							
availabilityStatus	1..1	n/a	0..0	n/a	Status des Ordners ("Approved")	Der Wert MUSS "`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" entsprechen.	
codeList	1..1	n/a	0..0	n/a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] genügen. Bei Folder.codeList=pregnancy_childbirth 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	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen.	

					eindeutige Kennung des Ordners	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	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.	
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.	
Metadaten für statische Folder							
availabilityStatus	n/a	n/a	1..1	n/a	Status des Ordners ("Approved")	Der Wert MUSS "`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" entsprechen.	
codeList	n/a	n/a	1..1	n/a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] genügen. 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	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.	
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)	nl-NL (niederländisch, Niederlande) nl-BE (niederländisch, Belgien)
es-ES (spanisch, Spanien)	no-NO (norwegisch, Norwegen)
et-EE (estnisch, Estland)	pl-PL (polnisch, Polen)
fi-FI (finnisch, Finnland)	pt-PT (portugiesisch, Portugal)
fr-FR (französisch, Frankreich) fr-CH (französisch, Schweiz) fr-LU (französisch, Luxemburg) fr-BE (französisch, Belgien)	rm-CH (rätoromanisch, Schweiz)
ga-IE (irisch, Irland)	ro-RO (rumänisch, Rumänien)
hr-HR (kroatisch, Kroatien)	sk-SK (slowakisch, Slowakei)
hu-HU (ungarisch, Ungarn)	sl-SI (slowenisch, Slowenien)
is-IS (isländisch, Island)	sv-SE (schwedisch, Schweden)

[<=]

3.12.1.8.2 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 (insbeondere 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 Zahnarztnummer (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 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

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^^^^`

[<=]

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^^^^`
- `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`**[<=]**

3.12.1.8.3 Metadaten für Datenkategorien

A_19388-18 - 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. Die Legal Policy gemäß Legal Policy MÜSSEN bei der Zuordnung generell durchgesetzt werden.

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 DocumentEntry, wenn nicht anders angegeben. Oder-Verknüpfungen, wenn nicht "und" angegeben)
receipt	healthcareFacilityTypeCode = VER und typeCode = ABRE
patient	Dokumente bei denen der Einsteller der Versicherte oder sein Vertreter ist
pregnancy_childbirth	healthcareFacilityTypeCode = HEB eventCodeList=SD070104 (KDL-Code Neugeborenenscreening)
eab	classCode = BRI
care	PracticeSettingCode = PFL

reports	classCode = ANF, ASM, BEF, BIL, DOK, DUR, LAB oder PLA
rehab	practiceSettingCode = REHA
dental	practiceSettingCode = MZKH, ORAL, KIEF oder PARO
emergency	eventCodeList = • ED110102 (KDL-Code Notfalldatenmanagement (NFDM)) • AU190104 (KDL-Code Notfalldatensatz) • AD020105 (KDL-Code Notfall-/Vertretungsschein)
other	Alle Dokumente, die in keine andere Kategorien eingeordnet werden können

[<=]

3.12.1.8.4 Weitere Metadatenvorgaben

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.**[<=]**

3.12.1.9 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 (3.12.1.9.2- 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_13798 bzw. A_14938-* antworten. **[<=]**

3.12.1.9.1 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_20577-05 - Definition und Zuweisung von Sammlungstypen
Der XDS Document Service MUSS jedem strukturierten Dokument 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-Fehlercode `BadFolderAssociation` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die UUID (DocumentEntry.entryUUID) des identifizierten Dokuments angegeben werden.**[<=]**

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_20581-02 - XDS Document Service – Löschen von Dokumenten aus Sammlungen der Typen "mixed" und "uniform"
Der XDS Document Service MUSS beim Löschen eines Dokuments der Sammlungstypen "mixed" und "uniform" über die Operation `I_Document_Management_Insurant::RemoveMetadata` sicherstellen, dass die Operation mit dem Fehler `ReferencesExistsException` abgebrochen wird, mit folgender 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.

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 einem `XDSRepositoryMetadataError` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `XDSRepositoryMetadataError`-Elements der Text „Version of submitted structured document is not supported“ zurückgegeben werden.**[<=]**

Hinweis: Die zeitliche Gültigkeit ergibt sich aus den Attributen "validFrom" und (optional) "clientReadOnlyFromDate" der Vorgaben in [gemSpec_IG_ePA].

3.12.1.9.2 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 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.

3.12.1.10 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.
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst	Alle vorhandenen Dokumente des Ordners "emp" (elektronischer Medikationsplan) werden gelöscht.

("erp-submission")	

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-Fachdiens" (Id == "erp-submission") auf "Widerspruch erklärt" ("deny") geändert wird.**[<=]**

A_23895 - 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 und Einstellen von Dokumenten des Ordners elektronischer Medikationsplan (codeSytem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") ablehnen. **[<=]**

A_25151 - XDS Document Service – Prüfung der Widersprüche bei Suchanfrage
Der XDS Document Service MUSS bei einer Suchanfrage die Suchergebnismenge filtern und sicherstellen, dass diese keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSytem = "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**[<=]**

3.12.1.11 Protokollierung von Zugriffen auf den XDS Document Service

A_24715 - XDS Document Service - Protokolleinträge für Zugriffe auf den XDS Document Service
Der XDS Document Service MUSS

- für die Operation ProvideAndRegisterDocumentSet-b durch eine LEI, Vertreter oder DiGA,
- für die Operation RegistryStoredQuery durch eine LEI oder Vertreter und
- für die Operationen RetrieveDocumentSet, RemoveMetadata, RestrictedUpdateDocumentSet

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.description	<Operation>		ein Wert aus {ProvideAndRegisterDocumentSet-b, RetrieveDocumentSet, RemoveMetadata, RestrictedUpdateDocumentSet, RegistryStoredQuery}
Parameterwerte für die Operationen ProvideAndRegisterDocumentSet-b, RetrieveDocumentSet und RemoveMetadata			
AuditEvent.entity.name	<XDSDocumentEntry.title>		wenn in der entity Struktur ein XDSDocument beschrieben wird *Hinweis: bei ProvideAndRegisterDocumentSet-b mit Replace Option, steht hier der Name des Dokumentes, welches ersetzt wird (targetObject)*
	<XDSFolder.title>		wenn in der entity Struktur ein XDSFolder beschrieben wird
AuditEvent.entity.detail	**type**	**value[x]**	
	"DocumentTitle"	<DocumentEntry.title>	wenn in der entity Struktur ein XDSDocument beschrieben wird *Hinweis: bei ProvideAndRegisterDocumentSet-b mit Replace Option, steht hier der Name des neu eingestellten Dokumentes (sourceObject)*
	"DocumentFormatCode"	<DocumentEntry.formatCode>	wenn in der entity Struktur ein XDSDocument 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 XDSDocument 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"
	"FolderEntryUUID"	<Folder.entryUUID>	wenn in der entity Struktur ein XDSFolder beschrieben wird
Parameterwerte für die Operation RegistryStoredQuery der Schnittstellen I_Document_Management und I_Document_Management_Insurant (nur Vertreter)			
AuditEvent.entity.name	"AdhocQuery"		fester Wert
AuditEvent.entity.detail	**type**	**value[x]**	
	"QueryId"	<Parameter Query ID>	Der Wert MUSS der Parameter Query ID gemäß [IHE-ITI-TF3]#3.18.4.1.2.4 entsprechen.
Parameterwerte für die Operation RestrictedUpdateDocumentSet			
Alle Metadaten, die **geändert** wurden, sind mit altem und neuem Wert mit den Parameternamen AuditEvent.entity.detail.**type** und .**value[x]** 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. z.b.Metadatum: DocumentEntry.formatCode ->Parameter value**type:** DocumentFormatCode und prevDocumentFormatCode. Attributunterstrukturen werden ebenfalls in gemischter Groß/Kleinschreibung zusammengesetzt(z.b. author.Person -> AuthorPerson).			

[<=]

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.**[<=]**

3.12.2 Medication Service

Der Medication Service ist ein FHIR Data Service und setzt im Rahmen des digital gestützten Medikationsprozesses eine elektronische Medikationsliste um.

A_24664 - Medication Service - Realisierung der Schnittstelle I_Medication_Service_FHIR
Der Medication Service MUSS die HTTP-Operationen der Schnittstelle I_Medication_Service_FHIR gemäß [I_Medication_Service_FHIR] umsetzen.**[<=]**

A_25175 - Medication Service - Realisierung der Nutzungsvorgaben für FHIR Operations
Der Medication Service MUSS die FHIR-Operationslogiken der Schnittstelle I_Medication_Service_FHIR gemäß [I_Medication_Service_FHIR_Operations] umsetzen.
[<=]

A_24863 - Medication Service - Realisierung der Schnittstelle I_Medication_Service_eML_Render
Der Medication Service MUSS die HTTP-Operationen der Schnittstelle I_Medication_Service_eML_Render gemäß [I_Medication_Service_eML_Render] umsetzen.
[<=]

A_24868 - Medication Service - Erzeugung eines xHTML-Exports
Der Medication Service MUSS die Erzeugung eines xHTML-Exports nach [XHTML] über die Schnittstelle I_Medication_Service_eML_Render gemäß [I_Medication_Service_eML_Render] umsetzen.

Dabei MUSS der nach Verordnungsdatum sortierte Export eine Tabelle über sämtliche Medikationslisteneinträge der letzten 12 Monate mit den folgenden Spalten beinhalten:

Spaltenkopf	Quelle	Bemerkung
Verordnungsdatum	https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication-request.authoredOn	
Dispensierdatum	https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication-dispense.whenHandedOver	
Wirkstoff	https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication.code.coding:pznCode https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication.code.text https://gematik.de/fhir/epa-medication/StructureDefinition/epa-	

	medication.ingredient https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication.ingredient.item[x]:itemCodeableConcept.coding:pznCode	
Handelsname	https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication.code.text https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication.ingredient.item[x]:itemCodeableConcept.text	
Wirkstärke	https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication.ingredient.strength	
Form	https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication.form.text	
M-M-A-N	https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication-request.dosageInstruction oder wenn verfügbar: https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication-dispense.dosageInstruction	
Grund		Dieser Wert wird vorbelegt mit "Keine Angabe".
Hinweis	https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication-request.note oder wenn verfügbar: https://gematik.de/fhir/epa-medication/StructureDefinition/epa-medication-dispense.note	
Verordnende Person	https://gematik.de/fhir/directory/StructureDefinition/PractitionerDirectory.name + " " + https://gematik.de/fhir/directory/StructureDefinition/OrganizationDirectory.name	
Status		Dieser Wert wird vorbelegt mit

		"Keine Angabe".

Der Medication Service MUSS sicherstellen, dass kein ausführbarer Code im Export enthalten ist.**[<=]**

A_24869 - Medication Service - Erzeugung eines PDF/A-Exports
Der Medication Service MUSS die Erzeugung eines PDF/A-Exports über die Schnittstelle I_Medication_Service_eML_Render gemäß [I_Medication_Service_eML_Render] umsetzen. Dabei MUSS sich die Erzeugung inhaltlich an der xHTML-Darstellung orientieren.**[<=]**

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_24841 - Medication Service - Schemavalidierung
Der Medication Service MUSS die im Body der HTTP-POST-Operation übertragenen Parameter gegen das jeweilige Schema der Operationsdefinition aus

- https://gematik.de/fhir/epa-medication/OperationDefinition/provide-prescription-erp-op
- https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-prescription-erp-op
- https://gematik.de/fhir/epa-medication/OperationDefinition/provide-dispensation-erp-op
- https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-dispensation-erp-op

prüfen und bei Nicht-Konformität das Ausführen der Operation mit dem HTTP Status Code 400 abbrechen, damit kein Schadcode und keine fachfremden Daten in den Medication Service hochgeladen werden.**[<=]**

A_24849 - Medication Service - Protokolleinträge für Zugriffe auf den Medication Service
Der Medication Service MUSS einen Protokolleintrag gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 37: Medication Service Protokollierung

Strukturelement	Operationen der Schnittstellen I_Medication_Service_FHIR und	Wert	Erläuterung

	I_Medication_Service_eML_Render		
AuditEvent.type	alle FHIR-Operationen, Nutzung der RESTful API, Abruf einer gerenderten eML	"rest"	
AuditEvent.action	$provide-prescription	C	Create
	$provide-dispensation	C	Create
	$cancel-prescription	U	Update
	$cancel-dispensation	U	Update
	renderEMLAsHTML	R	Read
	renderEMLAsPDF	R	Read
	listMedications	R	Read
	getMedicationById	R	Read
	FHIR Query/Search (Bundle:searchset)	R	Read
AuditEvent.entity.name		• "Medical Service" bei Operationen • <FHIR Resource Name> bei FHIR Query/Search	
AuditEvent.entity.description		Passend zur ausgeführten Operation ein Wert aus folgender Liste: • operation:provide-prescription • operation:provide-dispensation • operation:cancel-prescription • operation:cancel-dispensation • operation:render-eml-pdf • operation:render-eml-html • operation:list-medications • operation:get-medication-by-id • Bundle:searchset	

AuditEvent.entity.detail.type		search-parameters	Nur bei FHIR Query/Search
AuditEvent.entity.detail.value[x]		<ResourceName>?parameter1=<value>¶meter2=<value>& ...mehr	Nur bei FHIR Query/Search Suchkriterien in URL-Query-Notation

[<=]

3.13 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 - Audit Event Service - FHIR-Ressource AuditEvent
Der Audit Event Service MUSS die FHIR-Ressource AuditEvent gemäß der FHIR-Profilierung [gemSpec_EPAAuditEvent] unterstützen.**[<=]**

In der Struktur eines Protokolleintrages (AuditEvents) sind folgende Zugriffsinformationen hinterlegt:

Tabelle 38 : 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 - 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 39 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"
agent.type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets aus [gemSpec_EPAAuditEvent].	
	system	Das verwendete Codesystem	"http://terminology.hl7.org/CodeSystem/v3-RoleClass"
	code	Der verwendete Code aus dem Codesystem	"PROV"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"healthcare provider"
agent.who.identifier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Vaulue Sets aus [gemSpec_EPAAuditEvent]	
	system	Das verwendete Codesystem	a) "https://gematik.de/fhir/sid/telematik-id" b) "https://gematik.de/fhir/epa/sid/epa-telematikservice-identifier"
	value	<Telematik-Id> oder <KVNR> oder <Identifier> gemäß verwendetem Codesystem	a) "1-883110000092404" b) "ERP"

agent.	altId	<value> aus agent.who.identifier	a) "1-883110000092404" b) "ERP"
agent.	name	• <displayName> der Befugnis des Auslösers, • Bei Befugniserteilung in einer Behandlungssituation <displayName> der erstellten Befugnis, • "Elektronische Patientenakte Fachdienst" für intern ausgelöste AuditEvents	1) "John Doe" 2) "Musterpraxis" 3) "Elektronische Patientenakte Fachdienst"
agent.	requestor	Fest vorgegebener Wert "false"	"false"
source		Informationen zum auslösenden Service des Aktensystems	
source.observer.	display	Fester Wert "Elektronische Patientenakte Fachdienst"	"Elektronische Patientenakte Fachdienst"
source.type.		Der auslösende Service gemäß des zulässigen Value-Sets aus [gemSpec_EPAAuditEvent].	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/epa/CodeSystem/audit-event-source-type-cs"
	code	Der verwendete Code aus dem Codesystem	"CDMGMT"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Consent Decision Management"

[<=]

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 die Schnittstelle `I_Audit_Event`. Das ePA-FdV nutzt zur Abfrage der Protokolldaten als signiertes pdf die Schnittstelle `I_Audit_Event_Render_Insurant`.

A_24714 - Audit Event Service - Realisierung der Schnittstelle I_Audit_Event
Der Audit Event Service MUSS die Operationen der Schnittstelle `I_Audit_Event` gemäß gemäß [I_Audit_Event] umsetzen.**[<=]**

A_24750 - Audit Event Service - Realisierung der Schnittstelle I_Audit_Event_Render
Der Audit Event Service MUSS die Operationen der Schnittstelle `I_Audit_Event_Render_Insurant` gemäß [I_Audit_Event_Render_Insurant] umsetzen.
[<=]

A_25172 - Audit Event Service - Speicherung der Protokolldaten
Der Audit Event Service MUSS die Daten der Protokolleinträge im verschlüsselt im SecureDataStorage persistieren.**[<=]**

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 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 40: Audit Event Service Protokollierung

Strukturelement	Wert	Erläuterung
AuditEvent.type	"rest"	
AuditEvent.action	R	Read
AuditEvent.entity.name	"AuditEvent"	
AuditEvent.entity.descriptio	Passend zur ausgeführten Operation ein	

n	Wert aus folgender Liste: • listAuditEvents • getAuditEventById • renderAuditEventsToPDF		
AuditEvent.entity.detail	**type**	**value[x]**	
	parameters	parameter1=<value>¶meter2=<value>& ...mehr	Nur bei getAuditEventList
	identifier	<id> des AuditEvents	Nur bei getAuditEvent

[<=]

Hinweis: Zugriffe des Versicherten auf die Protokolle des Aktenkontos werden nicht protokolliert.

3.14 Information Service

3.14.1 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.**[<=]**

3.14.1.1 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").

3.14.1.2 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 2.9- Performance aus Anwendersicht definiert und vorgegeben.

3.14.2 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.
[<=]

3.15 Zusätzliche Anforderungen an den Authorization Service

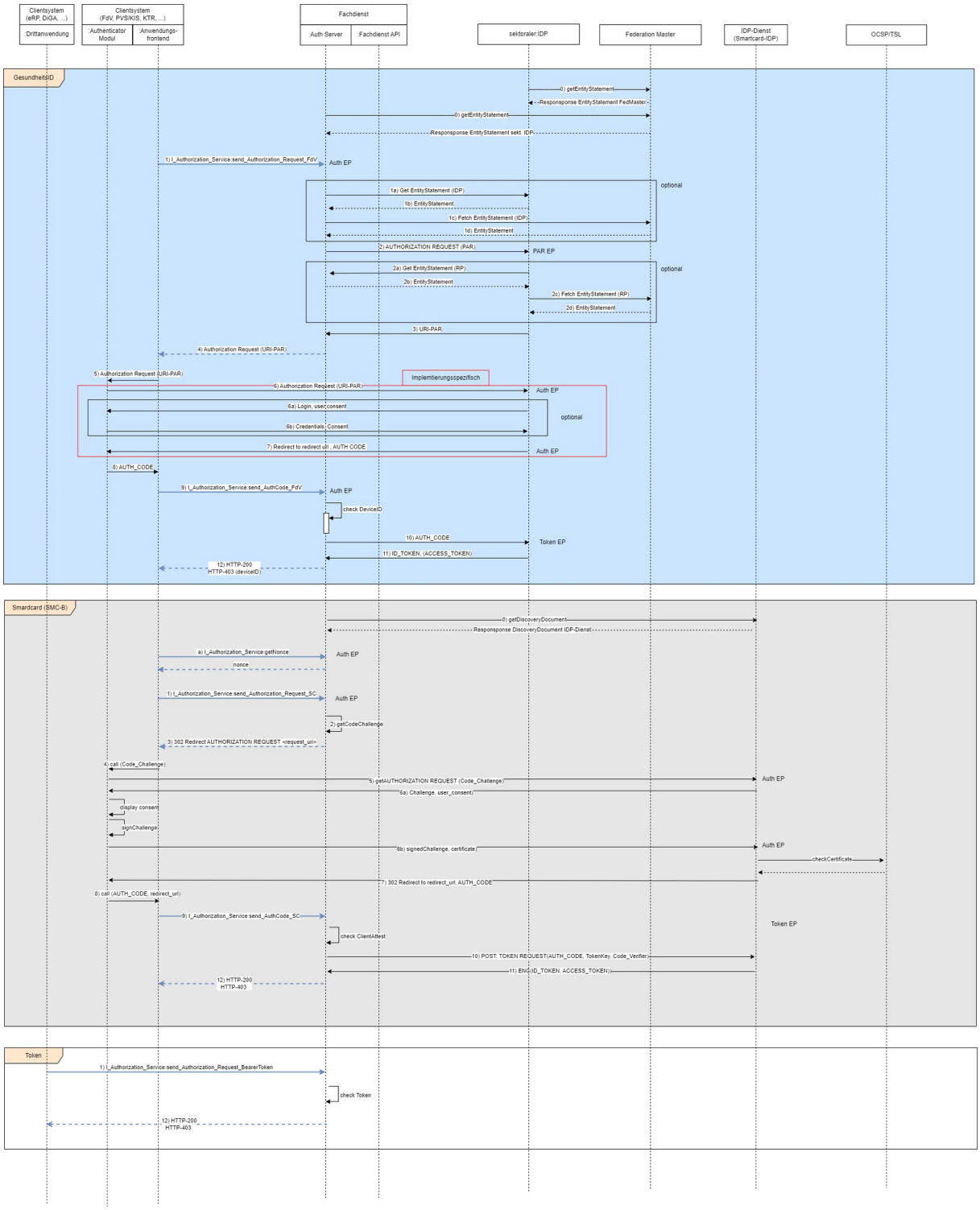

Abbildung 2: Ablauf der Authentifizierung von Versicherten über sektorale IDPs und Leistungserbringern über den Smartcard IDP

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].**[<=]**

3.15.1 Anforderungen an den Authorization Service für die Authentisierung von Versicherten (FdV)

Im Rahmen der Authentisierung des Versicherten erfolgt nach einer erfolgreichen Authentisierung, die Prüfung, ob das Gerät des Nutzers registriert ist. Ist dies nicht der Fall, so wird die Geräteregistrierung gestartet.

A_24877 - Authorization Service - ePA scopes und claims
Der Pushed Authorization Request (PAR) des ePA Authorization Service an den sektoralen IDP gemäß [gemSpec_IDP_FD#AF_10117] DARF als Parameter claims KEINE anderen als openid, amr, urn:telematik:display_name und urn:telematik:versicherter anfordern.**[<=]**

A_24878 - Authorization Service - Authentifizierung eines Versicherten am ePA-FdV des Vertreters
Falls der Eingangsparameter DeviceID = AUTHORIZE_REPRESENTATIVE der Operation `I_Authorization_Service::send_Authorization_Request_FdV` gesetzt ist MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:eGK` und `urn:telematik:auth:eID` belegt sein, um sicherzustellen, dass sich der Nutzer nur entweder über nPA+PIN oder eGK+PIN authentifizieren darf. **[<=]**

A_24937 - Authorization Service - Einschränkung bei AUTHORIZE_REPRESENTATIVE
Der Authorization Service MUSS sicherstellen, dass ein mit AUTHORIZE_REPRESENTATIVE authentisierter Nutzer ausschließlich Zugriff auf das Entitlement Management erhält.**[<=]**

A_24804 - Authorization Service - Prüfung auf registriertes Gerät
Der Authorization Service MUSS bei der Authentifizierung eines Versicherten prüfen, ob die in der Operation `I_Authorization_Service::send_AuthCode_FdV` übergebene DeviceID auf den authentifizierten Nutzer registriert und verifiziert ist, wenn der Wert `DeviceID` nicht `AUTHORIZE_REPRESENTATIVE` ist.**[<=]**

A_24914 - Authorization Service - Prüfung auf registriertes Gerät - kein registriertes Gerät
Falls keine bzw. unbekannte DeviceID übergeben wurde MUSS der Authorization Service:

- nach der Authentisierung des Nutzers die Geräteregistrierung in Service Device Management starten, welcher eine DeviceID (deviceIdentifier und deviceToken) erzeugt,
- die Operation send_AuthCode mit dem HTTP-Status 403 (Forbidden) mit ErrorCode = "unknownDevice", DeviceID mit deviceIdentifier und deviceToken abbrechen

[<=]

A_24936 - Authorization Service - keine Geräteregistrierung bei AUTHORIZE_REPRESENTATIVE

Falls DeviceID = AUTHORIZE_REPRESENTATIVE übergeben wird MUSS der Authorization Service sicherstellen, dass keine Geräteregistrierung erfolgt.**[<=]**

A_24915 - Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht verifiziert
Falls eine nicht verifizierte DeviceID in der Operation send_AuthCode übergeben wurde MUSS der Authorization Service die Operation mit HTTP-Status 403 (Forbidden) mit ErrorCode = "pendingDevice" abbrechen.**[<=]**

3.15.2 Anforderungen an den Authorization Service für die Authentisierung mit SMC-B

A_24880 - Authorization Service - Antwort des Authorization Service auf I_Authorization_Service::send_AuthCode_SC
Der Authorization Service MUSS auf einen Request `I_Authorization_Service::send_AuthCode_SC` aus einem Clientsystem, welches kein FdV ist, nach erfolgreichem Einlösen des AuthCode auf mit einem HTTP-200 antworten.**[<=]**

A_24805 - Authorization Service - Prüfung der Client-Attestation
Der Authorization Service MUSS bei der Authentifizierung eines Nutzers über den IPD-Dienst prüfen, ob die in der ClientAttest hinterlegte Client-Attestation mit einer Identität des authentifizierten Nutzer signiert ist und den passenden nonce enthält, und wenn dies nicht der Fall ist, die Authentifizierung mit dem HTTP-Status 403 (Forbidden) abbrechen. **[<=]**

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.**[<=]**

3.15.3 Anforderungen an den Authorization Service für die Authentisierung des E-Rezept-Fachdienstes

A_25165 - Authorization Service: JWT Bearer-Token des E-Rezept-Fachdienstes
Der Authorization Service MUSS bei der Authentifizierung des E-Rezept-Fachdienstes prüfen, dass das übermittelte JWT (vgl. [gemspec_Krypt#A_ 24658-*] mit mindestens folgenden Inhalten und den in A_24658-* definierten Inhalten erfolgt:

Befugnis	Claim Name	Claim	Beispiel
Protected Header			
	"typ"	"JWT"	

	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"iss"	URI des Token Ausstellers (issuer)	https://erezept.fachdien
	"sub"	Identifier (Telematik-ID)	9-E_Rezept_Fachdienst
	"iat"	Zeitstempel Ausgabezeitpunkt	1705674544
	"exp"	Verfalldatum, = "iat" + 20 min	1705675744
	"oid"	professionOid	1.2.276.0.76.4.258 (vgl. [gemSpec_OID#GS *] oid_erp-vau)
	"validTo"	Ende der Gültigkeit (tagesgenau)	2025-06-30

[<=]

Das Signaturzertifikat zu "x5c" (AUT-Zertifikat der E-Rezept-VAU) kommt aus der Komponenten-PKI der TI. 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.

3.16 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.**[<=]**

3.17 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.

3.17.1 Paketfilter

3.17.1.1 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_14019-01 - 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 nach A_15888 (vgl. Hinweis nach A_14019-01), 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_14019-01: 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 nach A_15888 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/ngx_http_ssl_module.html#ssl_stapling).

Um dies zu ermöglichen, muss der Paketfilter entsprechende stateful-Firewall-Regeln gemäß A_14019-01 und A_19126 definieren.

A_19126 - Access Gateway, OCSP-Status für das OCSP-Stapling
Der Paketfilter der Komponente Access Gateway MUSS bezüglich des OCSP-Stapling gemäß A_15888 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-Responsers 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) initiierter 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.**[<=]**

3.17.1.2 Redundanz

Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf#4.2]. 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.**[<=]**

3.17.1.3 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.

3.17.1.4 Adressierung

3.17.1.4.1 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.**[<=]**

3.17.1.4.2 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.

3.17.2 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.**[<=]**

3.17.3 Proxy Schlüsselgenerierungsdienst

Zur Nutzung der in [gemSpec_SGD_ePA] beschriebenen Schlüsselableitungsfunktionalität für den Schutz von Akten- und Kontextschlüssel einer ePA werden Aufrufe zu den Schlüsselgenerierungsdiensten SGD 1 und SGD 2 über den "Proxy Schlüsselgenerierungsdienst" ermöglicht.

Der Proxy SGD stellt sicher, dass ein ePA-FdV Aufrufe an den SGD 1 und SGD 2 durchführen kann.

Die Information, auf welche Anfragen (Pfade) des ePA-FdV der Proxy SGD aktiv wird ("/SGD1" für den SGD 1 und "/SGD2" für den SGD 2), sind in [gemSpec_SGD_ePA#2.2 Tabelle 2] angegeben.

A_17495 - Access Gateway, Zugriff auf den Schlüsselgenerierungsdienst
Der Proxy Schlüsselgenerierungsdienst der Komponente Access Gateway MUSS sicherstellen, dass das ePA-FdV auch ohne Authentisierung und Autorisierung Zugriff auf den SGD 1 und den SGD 2 erhält.
[<=]

3.17.4 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. [gemSpec_Aktensystem_ePA4All#4.6. 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 authentisierte 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.

3.17.5 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_15518-01 - Access Gateway, Verhalten des Authorization Proxy, Data Proxy
Die in der Komponente Access Gateway verwendeten Proxies Authorization Proxy und Data Proxy MÜSSEN als transparente Proxies umgesetzt werden.**[<=]**

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-Gefaehrdungen/DDoS/ddos_node.html.

A_14028 - Access Gateway, Verbindungen bei Komponentenausfall beenden
Die Komponente Access Gateway MUSS sicherstellen, dass

- alle bestehenden Verbindungen zum Access Gateway beendet werden und
- keine neuen Verbindungen zugelassen werden,

wenn am jeweiligen Access Gateway-Standort eine an der Weiterleitung der Daten zum ePA-Aktensystem beteiligte Komponente ausfällt und dadurch die Nutzung des ePA-Aktensystems nicht mehr möglich ist.**[<=]**

3.18 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.

3.18.1 Übersicht der Schnittstellen des Aktensystems

Tabelle 41: Übersicht der Schnittstellen des Aktensystems

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Consent_Decision_Management	
Schnittstelle des Consent Decision Managements gemäß [I_Consent_Decision_Management]	
`updateConsentDecision`	Diese Operation erlaubt dem FdV die Änderung des Zustand des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA für eine Funktion.
`getConsentDecisions`	Diese Operation erlaubt dem FdV das Lesen aller Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der ePA.
`getConsentDecision`	Diese Operation erlaubt dem FdV das Lesen eines Widerspruchs einer Funktion gegen die Nutzung von widerspruchsfähigen Funktionen.
I_Constraint_Management_Insurant	
Schnittstelle des Constraint Managements gemäß [I_Constraint_Management_Insurant]	
`getDenyPolicyAssignments`	Diese Operation gibt eine Liste aller konfigurierten Einträge der General Deny Policy und der User-specific Deny Policy aus.
`setPolicyAssignment`	Diese Operation fügt der General Deny Policy oder der User-specific Deny Policy einen neuen Eintrag hinzu.
`deletePolicyAssignment`	Diese Operation löscht einen bestimmten Eintrag der General Deny Policy oder der User-specific Deny Policy.
I_Entitlement_Management	
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.
`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.
I_Audit_Event_Render_Insurant	
Schnittstelle des Audit Event Service gemäß [I_Audit_Event_Render_Insurant] zum Abruf der Protokolldaten in lesbarer Form	
`renderAuditEventsToPDF`	Diese Operation erlaubt FdV und Ombudsstelle den Abruf der Protokolldaten als PDF.
I_Audit_Event	
Schnittstelle des Audit Event Service gemäß [I_Audit_Event] zum Abruf der Protokolldaten im FHIR-Format	
`listAuditEvents`	Diese Operation ermöglicht die Suche nach AuditEvent Instanzen.
`getAuditEventById`	Diese Operation ermöglicht das Lesen einer AuditEvent Instanz.
I_Health_Record_Relocation_Service	
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.

I_Device_Management_Insurant	
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.
I_Authorization_Service	
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
`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
I_Medication_Service_eML_Render	
`renderEMLAsHTML`	Diese Operation gibt die Medikationsliste im html-Format zurück.

renderEMLAsPDF	Diese Operation gibt die Medikationsliste im PDF/A-Format zurück.
I_Medication_Service_FHIR	
REST-Schnittstelle zum Abruf der Medikationsdaten im FHIR-Format	

Schnittstellen des Aktensystems (Nutzung ohne VAU-Kanal)	
I_Information_Service	
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 Performancedaten aus der Umgebung der Leistungserbringer.
getRecordStatus	Diese Operation fragt Existenz und Status eines bestimmten Aktenkontos bei einem Betreiber an.
I_Information_Service_Accounts	
Schnittstelle des Information Service gemäß [I_Information_Service_Accounts] für Anbieter Aktensystem im Kontext eines Aktenkontoumzugs	
getGeneralConsentDecision	Diese Operation dient der Abfrage eines Widerspurchs 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.

Die Schnittstellen (REST) und Operationen sind funktional in den Beschreibungen der jeweiligen Schnittstelle beschrieben. Darüber hinaus gelten die folgenden übergreifenden Anforderungen.

3.18.2 Übergreifende Festlegungen zu den Schnittstellen

A_23918 - Schnittstellen (OpenApi) - Prüfung der Befugnis
Das 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 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 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 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 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 Aktensystem MUSS nach der Ausführung der Operationen der REST-Schnittstellen eine 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
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
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
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
MIO	Medizinisches Informationsobjekt
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
W3C	World Wide Web Consortium
WS-I	Web-Services Interoperability Consortium
XCA	Cross-Community Access Profile
XDS	Cross-Enterprise Document Sharing ProfileGetAllDocumentKeys
XACML	eXtensible Access Control Markup Language

XDW	Cross-Enterprise Document Workflow Profile
XOP	XML-binary Optimized Packaging
XSPA	Cross-Enterprise Security and Privacy Authorization Profile

5.2 Glossar

Begriff	Erläuterung
Autneticator-Modul	Das Authenticator-Modul ist die Client-Komponente zum sektoralen Identity Provider. Über die das Authenticator-Modul authetifiziert 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

5.4 Tabellenverzeichnis

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: GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/implementation_guides
[gemSpec_Voc_ePA]	gematik: Vocabulary ePA GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/vocabulary
[gemSpec_EPAAuditEvent]	gematik: Datenstruktur für Audit-Protokolle im ePA-Aktensystem https://gematik.de/fhir/epa/StructureDefinition/audit-event
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_VZD_FHIR_Directory]	gematik: SpezifikationVerzeichnisdienst FHIR-

	Directory
[ValueSet-Speciality]	gematik: Value Set für Berechtigungskategorien GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/vocabulary/value_sets/vs-specialty-oth.xml
[I_Medication_Service_FHIR]	gematik: I_Medication_Service_FHIR REST-Schnittstelle (FHIR-Service) zum Abruf der FHIR-Instanzen der eML GitHub: https://github.com/gematik/ePA-Medication Path: src/openapi/I_Medication_Service_FHIR.yaml
[I_Medication_Service_FHIR_Operations]	gematik: Implementation Guide GitHub: https://github.com/gematik/ePA-Medication Path: src/doc/guides/erp-operations.md
[I_Medication_Service_eML_Render]	gematik: I_Medication_Service_eML_Render REST-Schnittstelle zum Abruf der gerenderten eML GitHub: https://github.com/gematik/ePA-Medication Path: src/openapi/I_Medication_Service_eML_Render.yaml
[I_Consent_Decision_Management]	gematik: I_Consent_Decision_Management REST-Schnittstell zum Management der Widersprüche zu Versorgungsprozessen GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Consent_Decision_Management.yaml
[I_Constraint_Management_Insurant]	gematik: I_Constraint_Management_Insurant.yaml REST-Schnittstelle zum Verbergen und Sichtbarmachen von Dokumenten GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Constraint_Management_Insurant.yaml
[I_Entitlement_Management]	gematik: I_Entitlement_Management REST-Schnittstelle zur Verwaltung von Befugnissen und Befugnisausschlüssen GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Entitlement_Management.yaml
[I_Device_Management_Insurant]	gematik: I_Device_Management_Insurant.yaml REST-Schnittstelle zur Geräteverwaltung GitHub: https://github.com/gematik/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 GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Health_Record_Relocation_Service.yaml
[Information_Service_Accounts]	Schnittstellenspezifikation Information Service für Betreiber GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Information_Service_Accounts.yaml

[I_Information_Service]	Schnittstellenspezifikation Information Service GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Information_Service.yaml
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung und impliziten Geräteregistrierung GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Authorization_Service.yaml
[I_Audit_Event_Render_Insurant]	gematik: I_Audit_Event_Render_Insurant REST-Schnittstelle (FHIR-Service) zum Abruf der gerenderten Protokolldaten GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Audit_Event_Render_Insurant.yaml
[I_Audit_Event]	gematik: I_Audit_Event REST-Schnittstelle (FHIR-Service) zum Abruf der Protokolldaten GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Audit_Event.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, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-RMU]	IHE International (2021): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.3 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf
[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, https://profiles.ihe.net/ITI/TF/Volume1/
[IHE-ITI-TF2]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume2/
[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, https://profiles.ihe.net/ITI/TF/Volume3/

[MIO-UH]	Kassenärztliche Bundesvereinigung (2022): Kinderuntersuchungsheft, https://mio.kbv.de/display/UH1X0X1
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://datatracker.ietf.org/doc/html/rfc2119
[RFC4122]	IETF (2005) A Universally Unique IDentifier (UUID) URN Namespace, RFC 4122 https://datatracker.ietf.org/doc/html/rfc4122
[RFC5246]	IETF (2008): The Transport Layer Security (TLS) Protocol Version 1.2 https://datatracker.ietf.org/doc/html/rfc5246
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231, https://datatracker.ietf.org/doc/html/rfc7231
[RFC7515]	IETF (2015): JSON Web Signature (JWS), RFC-7515 https://datatracker.ietf.org/doc/html/rfc7515
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), https://www.w3.org/TR/soap12-part1/
[WSA]	OASIS (2004): Web Services Addressing (WS-Addressing), https://www.w3.org/Submission/ws-addressing/
[WSIAP]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[WSIBSP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html

[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/
[XHTML]	W3C (2010): XHTML 1.1 - Module-based XHTML - Second Edition, https://www.w3.org/TR/xhtml1/