Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation
Aktensystem ePA für alle

Version:	2.0.0 CC
Revision:	1762413
Stand:	15.10.2026
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_Aktensystem_ePAfueralle_V2.0.0_CC

Dokumentinformationen

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

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.01.2024		ePA für alle	gematik
1.1.0	28.03.2024		ePA für alle - Release 3.0.1	gematik
1.2.0	12.07.2024		ePA für alle - Release 3.0.2, Zuordnungen für Release E-Rezept 1.6.5	gematik
1.3.0	14.08.2024		ePA für alle - Release 3.1.0	gematik
1.4.0	28.02.2025		ePA für alle - Release 3.0.5	gematik
1.5.0	27.05.2025		ePA für alle - Release 3.1.2	gematik
1.6.0	12.09.2025		ePA für alle - Release 3.1.3 (inkl.Release 3.1.2-1)	gematik
1.7.0	15.12.2025		ePA für alle - Release 3.1.3-1	gematik
1.8.0	23.03.2026		ePA für alle - Release 3.1.3-2	gematik
1.8.1	24.03.2026		Anpassung Prozess Client-ID-/product-id-Registrierung	gematik
1.8.2	14.07.2026		ePA für alle - Release ePA_3_1_3-4	gematik

2.0.0 CC	15.10.2026		ePA für alle 27	gematik

Inhaltsverzeichnis

1 Einführung 7
1.1 Zielsetzung 7
1.2 Zielgruppe 7
1.3 Geltungsbereich 7
1.4 Abgrenzungen 7
1.5 Methodik 8
2 Übergreifende Festlegungen 9
2.1 Aktensystem- und Service-Lokalisierung 12
2.2 Redundanz 14
2.3 Datenschutz und Sicherheit 14
2.4 Validierungsaktenkonto 19
2.5 Tracing in Nichtproduktivumgebungen 22
2.6 Benutzerführung 23
2.7 Useragent 24
2.8 Performance aus Anwendersicht 25
3 Funktionsmerkmale 26
3.1 Aktenkontoverwaltung 26
3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte 27
3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger 27
3.1.2 Anlage eines neuen Aktenkontos 27
3.1.3 Löschen eines Aktenkontos 31
3.1.4 Verschiebung der Informationen eines Aktenkontos 31
3.1.4.1 Erzeugen von Exportpaketen 33
3.1.4.2 Import von Exportpaketen 35
3.1.5 Anlage einer Akte bei Rücknahme eines Widerspruchs gegen die ePA 37
3.1.6 Lebenszyklus und Zustände einer Akte 37
3.1.7 Akte ist zeitweise nicht nutzbar 39
3.1.8 Aktenzusammenführung (Health Record Merge) 41
3.1.8.1 Zusammenführung der Ressourcen des Medication Service 43
3.1.8.1.1 Keine Zusammenführung bei Widerspruch 44
3.1.8.1.2 Sonderfall exklusive Nutzung einer der beiden Akten 44
3.1.8.1.3 Zusammenführung verteilter Ressourcen 44
3.1.8.1.4 Vereinfachte Auswahl eines Datenbestands (Fallback-Lösung) 47
3.2 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM 49
3.3 Befugnisverifikations-Modul 53

3.3.1 VAU-Token-Modul....54
3.3.2 Regeln des Befugnisverifikations-Moduls....61
3.4 Vertrauenswürdige Ausführungsumgebung (VAU)....76
3.4.1 Übergreifende VAU-Anforderungen....79
3.4.1.1 Schutz der Integrität der VAU....79
3.4.1.2 Schutz der Daten bei Verarbeitung in der VAU....80
3.4.1.3 Schutz der Daten bei Speicherung außerhalb der VAU....81
3.4.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM....81
3.4.1.5 Logging und Monitoring....81
3.4.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU....83
3.4.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU....83
3.4.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-VAU....84
3.4.2.3 Konsistenz des Systemzustands....85
3.4.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU....85
3.4.4 Zusätzliche Anforderungen an eine Service-VAU....86
3.4.4.1 Zusätzliche Anforderungen an eine Zusatzfunktion-Service-VAU....88
3.4.4.2 Kommunikation zwischen AK-VAU und Service-VAU....88
3.4.5 Temporäres Speichern von Daten und spätere Aufnahme ins Aktenkonto....89
3.5 Umschlüsselung....94
3.6 User Session und Health Record Context....96
3.7 Consent Decision Management....96
3.7.1 Widersprüche für Funktionen der ePA....97
3.7.2 Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke....100
3.7.3 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny Policy Medication)....101
3.8 Entitlement Management....103
3.8.1 Initiale Befugnisse (static Entitlements)....108
3.8.2 Erstellen einer Befugnis durch Clients....110
3.8.2.1 Befugnisvergabe durch ein ePA-FdV....110
3.8.2.2 Befugnisvergabe durch ein Primärsystem....112
3.8.3 Löschen von Befugnissen....114
3.8.4 Befugnisausschluss (Blocked User Policy)....115
3.8.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)....117
3.8.6 EntitlementDenyList....119
3.9 Legal Policy....122
3.10 Constraint Management....130
3.10.1 Aktenkontoweites Verbergen (General Deny Policy)....132
3.10.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes 134
3.11 Device Management....134
3.12 Medical Services....138
3.12.1 XDS Document Service....139
3.12.1.1 Formatprüfung beim Einstellen von Dokumenten....139
3.12.1.2 Anforderungen zur Validierung....142
3.12.1.3 Namensräume....143
3.12.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von Dokumenten....144
3.12.1.4.1 Anforderungen an IHE ITI-Akteure....144
3.12.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen....146

3.12.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen.....148
3.12.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen.....160
3.12.1.5 Fehlerbehandlung in Schnittstellenoperationen.....161
3.12.1.6 Schnittstellen im XDS Document Service.....163
3.12.1.6.1 Schnittstelle I_Document_Management.....163
3.12.1.6.2 Schnittstelle I_Document_Management_Insurant.....166
3.12.1.7 Statische Metadaten.....168
3.12.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten.....170
3.12.1.8.1 Allgemeine Metadatenvorgaben.....170
3.12.1.8.2 Metadaten der Dokumente und SubmissionSets.....186
3.12.1.8.3 Metadaten für Datenkategorien.....191
3.12.1.8.4 Automatisches Umschreiben von Daten.....192
3.12.1.9 Strukturierte Dokumente.....194
3.12.1.9.1 Sammlungstypen.....194
3.12.1.9.2 Konfigurierbarkeit.....196
3.12.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode 197
3.12.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die Dokumente des Aktenkontos.....198
3.12.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI auf die Dokumente des Aktenkontos.....199
3.12.1.13 Protokollierung von Zugriffen auf den XDS Document Service.....199
3.12.1.14 Unterstützungsleistung für das ePA-FdV.....199
3.12.2 FHIR Data Services.....200
3.13 Audit Event Service.....200
3.14 Information Services.....201
3.14.1 Information Service.....201
3.14.1.1 Informationen zu Widersprüchen (Consent Decisions).....201
3.14.1.2 Informationen zur Anwenderperformance (UX Performance).....201
3.14.2 Information Service - Account.....201
3.14.3 EHR Information Service.....202
3.15 Email Management.....203
3.16 Zusätzliche Anforderungen an den Authorization Service.....204
3.16.1 Anforderungen an den Authorization Service für die Authentisierung von Versicherten (FdV).....204
3.16.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B 209
3.16.3 Anforderungen an den Authorization Service für die Authentisierung über JWT Bearer Token.....210
3.17 Anbindung Verzeichnisdienst FHIR-Directory.....213
3.18 Access Gateway.....214
3.18.1 Paketfilter.....214
3.18.1.1 Funktion.....214
3.18.1.2 Redundanz.....215
3.18.1.3 Konfiguration.....216
3.18.1.4 Adressierung.....216
3.18.1.4.1 Access Gateway zum Transportnetz Internet.....216
3.18.1.4.2 ePA-Aktensystem zum Zentralen Netz.....216

3.18.2 Proxy für das VAU-Protokoll....216
3.18.3 Tracing in Nichtproduktivumgebungen....216
3.18.4 Übergreifende Festlegungen....218
3.19 Data Submission Service....219
3.19.1 Erstellung von Arbeitsnummern und Lieferpseudonymen....220
3.19.2 Auswahl von medizinischen Daten....221
3.19.3 Protokollierung des Datenexports an das FDZ....222
3.19.4 Pseudonymisierung von medizinischen Daten....222
3.19.5 Übermittlung der pseudonymisierten medizinischen Daten....223
3.20 Push Notification Management....225
3.20.1 Push Notification Management des ePA-Aktensystems....225
3.20.2 Registrierung eines ePA-FdV als Pusher....226
3.20.3 Push Notification Channels....227
3.20.4 Push Notification Nachrichteninhalte....228
3.20.5 Versenden von Push Nachrichten....229
3.21 Backendseitige Zusatzfunktionen....230
3.21.1 Zugriffsmodell für backendseitige Zusatzfunktionen....231
3.21.2 Zusatzfunktion-Manager für backendseitige Zusatzfunktionen....232
3.22 Schnittstellen (OpenAPI)....236
3.22.1 Übersicht der Schnittstellen des Aktensystems....236
3.22.2 Übergreifende Festlegungen zu den Schnittstellen....245
4 Informationsmodelle....246
5 Anhang A – Verzeichnisse....247
5.1 Abkürzungen....247
5.2 Glossar....249
5.3 Abbildungsverzeichnis....249
5.4 Tabellenverzeichnis....249
5.5 Referenzierte Dokumente....251
5.5.1 Dokumente der gematik....251
5.5.2 Weitere Dokumente....255

1 Einführung

1.1 Zielsetzung

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

1.2 Zielgruppe

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

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

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

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

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet. Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

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

2 Übergreifende Festlegungen

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

Hinweis: Wenn in dieser Spezifikation vom E-Rezept-Fachdienst gesprochen wird, dann ist damit der Nutzer gemeint, der sich mit der Rolle oid_erp-vau authentisiert hat. Dies kann der E-Rezept-Fachdienst oder der TI-Flow-Fachdienst in seiner Rolle als E-Rezept-Fachdienst sein.

A_24986 -ePA-Aktensystem - Rollentrennung ePA-Aktensystem und IDP-Dienst
Falls der Betreiber des ePA-Aktensystems auch den IDP-Dienst betreibt, MUSS der Betreiber sicherstellen, dass die Erstellung oder Änderungen von IDToken beim IDP-Dienst und die Verarbeitung und Prüfung der Client-Attestation im ePA-Aktensystem durch geeignete technische und organisatorische Maßnahmen so wirkungsvoll voneinander getrennt werden, dass ein einzelner Mitarbeiter des Betreibers nicht beide Aktivitäten durchführen kann.**[<=]**

A_25149-01 -ePA-Aktensystem - Rollentrennung ePA-Aktensystem und sektoraler IDP
Falls der Betreiber des ePA-Aktensystems auch einen sektoralen IDP betreibt, MUSS der Betreiber sicherstellen, dass die Erstellung oder Änderungen von ID-Token beim sektoralen IDP und die Erstellung oder Änderungen der Mailadresse für die Geräteverwaltung im ePA-Aktensystem durch geeignete technische und organisatorische Maßnahmen so wirkungsvoll voneinander getrennt werden, dass ein einzelner Mitarbeiter des Betreibers nicht die Aktivitäten in beiden Diensten durchführen kann.**[<=]**

A_24673 -Zeitsynchronisation über Zeitdienst in der TI
Das ePA-Aktensystem MUSS die Systemzeit über den Zeitdienst in der TI gemäß [gemSpec_Net#6.2] synchronisieren
[<=]

A_25612 -ePA-Aktensystem - Authentisierung gegenüber einem Client innerhalb der TI
Das ePA-Aktensystem MUSS sich beim Aufruf durch einen Client innerhalb der TI mit der TLS-Identität oid_epa_dvw und Zertifikatsprofil C.FD.TLS-S authentisieren.**[<=]**

A_24676 -Useragent Information in HTTP Header außerhalb des VAU-Kanals
Das ePA-Aktensystem MUSS sicherstellen, dass in der Kommunikation mit den ePA-Clients außerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "x-useragent" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen.
[<=]

A_24677 -Useragent Information in HTTP Header innerhalb des VAU-Kanals
Das ePA-Aktensystem MUSS sicherstellen, dass in der Kommunikation mit den ePA-Clients innerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "x-useragent" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen.
[<=]

Die Formatvorgaben zum Useragent sind in A_22470* definiert.

A_24816-01 -Aktenkontokennung in HTTP Header innerhalb des VAU-Kanals
Das ePA-Aktensystem MUSS sicherstellen, dass ePA-Clients in der Kommunikation mit den Medical Services der ePA innerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "x-insurantId" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen.**[<=]**

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

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

A_27701 -Requestkennung in HTTP Header außerhalb des VAU-Kanals
Falls in der Kommunikation mit den ePA-Clients außerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "X-Request-ID" gesendet wird MUSS das ePA-Aktensystem sicherstellen, dass der Wert von "X-Request-ID" eine UUID ist und andernfalls den Request mit HTTP-Fehler 400 ablehnen.**[<=]**

A_27702 -Requestkennung in HTTP Header innerhalb des VAU-Kanals
Falls in der Kommunikation mit den ePA-Clients innerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "X-Request-ID" gesendet wird MUSS das ePA-Aktensystem sicherstellen, dass der Wert von "X-Request-ID" eine UUID ist und andernfalls den Request mit HTTP-Fehler 400 ablehnen.**[<=]**

A_27703 -Requestkennung in der Response
Falls ein HTTP Header Element mit dem Namen "X-Request-ID" in einem Request an das ePA-Aktensystem gesendet wird MUSS das ePA-Aktensystem sicherstellen, dass die Response ein HTTP Header Element mit dem Namen "X-Request-ID" enthält und mit dem Wert aus dem Request belegt wird.**[<=]**

A_27712 -Requestkennung - betriebliche Protokollierung
Falls ein HTTP Header Element mit dem Namen "X-Request-ID" in einem Request an das ePA-Aktensystem gesendet wird MUSS der Anbieter des ePA-Aktensystems sicherstellen, dass der Wert von "X-Request-ID" in der Protokollierung des Betreibers berücksichtigt wird.**[<=]**

A_27443-01 -Nutzung Terminologiepaket
Das ePA-Aktensystem MUSS die relevanten Terminologien des Terminologiepakets gemäß [gemIG_TI_Terminology] verarbeiten und in der Kommunikation mit dem ePA-Aktensystem berücksichtigen. Weiterhin MUSS das ePA-Aktensystem die Registrierung von Daten und Dokumenten ablehnen, falls ein Code den Status "inactive" besitzt.**[<=]**

Hinweise zu A_27443-*:

1. Das Terminologiepaket wird als FHIR-Package bereitgestellt und enthält z.B. Vocabulary ePA und Value Set für Berechtigungskategorien. Falls ein Code in einem Code System als "inactive" gekennzeichnet wird, wird der Code über eine entsprechende "Property" gekennzeichnet. Der folgende Ausschnitt zeigt ein Beispiel (FHIR JSON-Format):
```
{
"code": "1",
"display": "Arzt in Facharztausbildung",
"property": [{
    "code": "status",
    "valueCode": "inactive"
  }]
},
```
2. Die Registrierung von Daten und Dokumenten mit dem Code im Status "deprecated" wird vom ePA-Aktensystem akzeptiert. Die Kennzeichnung erfolgt analog über property.code="status" und valueCode="deprecated".

A_28834 -Nutzung ausgewählter Code Systems im Status "Deprecated"

Das ePA-Aktensystem MUSS an den an Stellen, an denen gemäß [gemIG_TI_Terminology] die Verwendung von Codes aus folgenden versionierten Code Systems erlaubt sind, auch Codes der jeweils angegebenen alten Version desselben Code System akzeptieren (inklusive der/des ggf. angegebenen alternativen Namen):

Name	Code System Identifier und Version Status "Active" (gemäß [gemIG_TI_Terminology] zu unterstützen)	Code System Identifier und Version Status "Deprecated" (zusätzlich zu unterstützen)
KDL	http://dvmd.de/fhir/CodeSystem/kdl Version 2025	http://dvmd.de/fhir/CodeSystem/kdl(preferred) Version 2024 Alternativer Name: 1.2.276.0.76.5.552

Die Umsetzung erfolgt zunächst nur für Codes im Metadatum DocumentEntry.eventCodeList.
[<=]

Der Hinweis "preferred" wird in A_28834 nicht benötigt, kann jedoch bei Bedarf von anderen Anforderungen referenziert werden.

Die hier gelisteten Code Systems werden als "deprecated" markiert. Sie können nach wie vor wie "aktive" Code Systems und deren Codes durch Clients genutzt werden (bspw. beim Einstellen von neuen Dokumenten bzw. DocumentEntries). Mit der Kennzeichnung wird jedoch angedeutet, dass zukünftige Versionen von ePA für Alle die entsprechenden Codes möglicherweise entfernen werden (Status "inactive"). Dann können sie nicht mehr für neue Daten genutzt werden.

A_27708 -ePA-Aktensystem – Festlegung zu Formatvorgabe für Datentyp datetime gemäß RFC3339
Das ePA-Aktensystem MUSS bei der Verwendung des Datentyps datetime das Format gemäß RFC3339 wie folgt einschränken:

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

Diese Formatvorgabe betrifft nicht die Bestandsdatenlieferung.**[<=]**

Beispiele für Datentyp datetime:
`2025-04-12T15:20:50Z`
`2025-06-30T23:59:59+01:00`

Der FHIR-Datentyp `dateTime` ist von der obigen Regelung nicht betroffen; dessen Format wird über die entsprechenden Vorgaben des FHIR-Standards oder darüber hinaus gehende Einschränkungen innerhalb der FHIR-Profile geregelt.

A_27868 -ePA-Aktensystem – fehlerhafter URL-Pfad
Falls ein URL-Pfad adressiert wird, der keinem für das Aktensystem spezifizierten Services zugeordnet werden kann, MUSS das ePA-Aktensystem den Aufruf mit dem HTTP-

Statuscode 404 mit Errorcode `pathNotFound`ablehnen.
[<=]

2.1 Aktensystem- und Service-Lokalisierung

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

Ein ePA-Client aus der TI kennt die FQDNs der ePA-Aktensysteme (diese werden hier fest definiert, vgl. A_24592-*). Das Vorgehen der festvorgegebenen FQDNs ist analog zum E-Rezept-Vorgehen.

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

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

A_24592-02 -Anbieter ePA-Aktensystem -Registrierung an übergreifender ePA-Domäne
Der Anbieter des ePA-Aktensystems MUSS seine Hosts und IP-Adressen für Services, die über das zentrale Netz der TI angeboten werden, in der übergreifenden ePA-Domäne `epa4all.de` für die Sub-Domänen ref (RU1), dev (RU2), test (TU) und prod (PU) unter folgend aufgeführten DNS-Namen (FQDN) registrieren. Diese sind

1. Host und IP-Adressen für den Endpunkt I_Information_Service und der Services in der VAU:
   `epa-as-<ePA-Anbieter-Zahl>.<Umgebung>.epa4all.de.`
2. Host und IP-Adressen für den Endpunkt I_Information_Service_Accounts:
   `epa-asisa-<ePA-Anbieter-Zahl>.<Umgebung>.epa4all.de.`

Die "ePA-Anbieter-Zahl" wird durch die gematik festgelegt.
[<=]

Die "ePA-Anbieter-Zahl" für einen Aktensystembetreiber ist unter https://wiki.gematik.de/spaces/EPA/pages/729781779/Liste+von+Aktensystemen+f%C3%BCr+Aktenlokalisierung veröffentlicht.

Beispiele der Dienstlokalisierung

PU :
Aktensystem A

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

Aktensystem B

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

TU :
Aktensystem 1
`epa-as-1.test.epa4all.de A 172.30.x9.x10`

...

D. h. ein ePA-Client aus der TI (Primärsystem) kennt die für ihn relevanten FQDNs (z.B. PU: epa-as-1.prod.epa4all.de) und verwendet diese um die Aktensysteme zu kontaktieren.

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_22688-06 -Anbieter ePA-Aktensystem, Konfiguration Schnittstellen über /.well-known/
Der Anbieter des ePA-Aktensystems MUSS an seinen Access Gateway des Versicherten über den URL-Pfadnamen (bzw. die Datei) /.well-known/epa-configuration.json eine JSON-Repräsentation der Produkttypversion verfügbar machen.
D. h. der Aufrufende (ePA-FdV) MUSS wenn er diesen Pfad per HTTP-GET abfragt ein JSON-Objekt (also Content-Type "application/json") vom Access Gateway des Versicherten erhalten der Art

```
{
    "version" : "<Produkttypversion des Aktensystems im Format^(?:[1-9]\
d?|\d)\.(?:[1-9]\d?|\d)\.(?:[1-9]\d?|\d)(?:-(?:[1-9]\d?|\d))?$>",
    ....
}
```

[<=]

Hinweis: Die JSON-Datei kann auch weitere Informationen für das ePA-FdV enthalten, welche aber nicht interoperabel gehalten sind.

A_22687 -Aktensystem, Konfiguration Schnittstellen über /.well-known/
Das ePA-Aktensystem MUSS sicherstellen, dass dem Anbieter des ePA-Aktensystems die technische Möglichkeit bereitgestellt wird A_22688-* umzusetzen.**[<=]**

A_26814 -ePA-Aktensystem - Schnittstellenadressierung
Das ePA-Aktensystem MUSS die Schnittstellenadressierung (relative Pfade) gemäß der Schnittstellenspezifikationen umsetzen. **[<=]**

Schnittstellenspezifikationen für die fachlichen Requests erfolgen durch WSDL, OpenAPI und FHIR Implementation Guides.
Für Operationen, die innerhalb einer ePA-VAU aufgerufen werden, gelten die Schnittstellenspezifikationen für den inneren HTTP-Request.
Abgrenzend hierzu wird das VAU-Protokoll und die dabei verwendeten Pfade in [gemSpec_Krypt#7] definiert.

A_24801 -Aktensystem, Liste von FQDN im Internet
Das ePA-Aktensystem MUSS dem ePA-FdV eine Liste aller Kostenträger und der FQDN, unter der deren ePA-Aktensystem im Internet erreichbar ist, bereitstellen. Die Liste setzt sich zusammen aus den selbst verwalteten Kostenträgern und den über I_Information_Service_Accounts bezogenen Teillisten der anderen ePA-Aktensysteme.
[<=]

2.2 Redundanz

Die Anforderungen an die Redundanzen des ePA-Aktensystems finden sich in gemSpec_Perf.

2.3 Datenschutz und Sicherheit

A_15128 -Anbieter ePA-Aktensystem - Schutz der transportierten Daten im ePA-Aktensystem
Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die Vertraulichkeit und Integrität der innerhalb des ePA-Aktensystems transportierten Daten gewährleistet ist. **[<=]**

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

A_15103 -Anbieter ePA-Aktensystem - Konzept zur Verhinderung von Profilbildung
Der Anbieter des ePA-Aktensystems MUSS ein Konzept erstellen und umsetzen, dass sicherstellt, dass Mitarbeiter des Anbieters die im ePA-Aktensystem verarbeiteten Daten nicht für Profilbildungen über Versicherte oder Leistungserbringer(-institutionen) nutzen können.**[<=]**

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

A_25722-01 -ePA-Aktensystem - Löschen von personenbezogenen Daten von Vertretern nach Wegfall der Notwendigkeit
Das ePA-Aktensystem MUSS es ermöglichen, dass personenbezogene Daten von Vertretern ohne eigene Akte in ihrem Home-AS auf Verlangen des Vertreters gelöscht werden können. Der Hersteller des ePA-Aktensystems kann hierfür eine herstellerspezifische VAU-Schnittstelle umsetzen.**[<=]**

Hinweis zu A_25722-*: Die Löschung kann auch durch den Kostenträger des Vertreters ausgelöst werden, falls der Vertreter die Löschung gegenüber seinem Kostenträger verlangt hat.

A_15104 -Anbieter ePA-Aktensystem - Ordnungsgemäße IT-Administration
Der Anbieter des ePA-Aktensystems MUSS die Maßnahmen für erhöhten Schutzbedarf des BSI-Bausteins „OPS.1.1.2 Ordnungsgemäße IT-Administration“ [BSI-Grundschutz] während des gesamten Betriebs des ePA-Aktensystems umsetzen.**[<=]**

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

A_15824 -Anbieter ePA-Aktensystem - Sichere Speicherung von Daten
Unabhängig davon, ob die Daten schon verschlüsselt vorliegen, MUSS der Anbieter des ePA-Aktensystems die Daten des ePA-Aktensystems bei der Speicherung verschlüsseln. **[<=]**

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

A_24774 -Anbieter ePA-Aktensystem - Zwei-Faktor-Authentisierung von Administratoren
Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass sich Administratoren mindestens mit einer Zwei-Faktor-Authentisierung anmelden.**[<=]**

A_15107-02 -Anbieter ePA-Aktensystem - Keine unzulässige Weitergabe von Daten
Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die in seinem Aktensystem verarbeiteten Daten nicht weitergegeben werden, auch nicht in pseudonymisierter oder anonymisierter Form. Davon ausgenommen sind Weitergaben an berechtigte Nutzer der Aktenkonten, an einen durch den Versicherten gewählten Anbieter beim Anbieterwechsel sowie Übermittlungen an das Forschungsdatenzentrum Gesundheit soweit dagegen kein Widerspruch durch den Versicherten oder einen Vertreter vorliegt.**[<=]**

A_15119 -Anbieter ePA-Aktensystem - Löschkonzept
Der Anbieter des ePA-Aktensystems MUSS in einem Löschkonzept für die im ePA-Aktensystem verarbeiteten personenbezogenen Daten mindestens folgende Aspekte beschreiben:

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

[<=]

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

A_15169 -ePA-Aktensystem - Verbot von Werbe- und Usability-Tracking
Die Komponenten des ePA-Aktensystems DÜRFEN im Produktivbetrieb ein Werbe- und Usability-Tracking NICHT verwenden.
Davon ausgenommen ist das Erfassen des standardmäßigen quantitativen Nutzerverhaltens zur Ermittlung der Standard-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_24780-01 -Anbieter ePA-Aktensystem – Versicherte über sensible Änderungen informieren
Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass der Versicherte informiert wird, wenn der Anbieter des Aktensystems eine manuelle Änderung bezüglich einer Akte (Aktenverwaltung) im Auftrag eines Versicherten durchführt.**[<=]**

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

A_15163 -Anbieter ePA-Aktensystem - Angriffen entgegenwirken
Der Anbieter des ePA-Aktensystems MUSS Maßnahmen zur Erkennung von Angriffen und zur Reduzierung bzw. Verhinderung von Schäden aufgrund von Angriffen in allen Komponenten des ePA-Aktensystems umsetzen.**[<=]**

A_15167 -Anbieter ePA-Aktensystem - Social Engineering Angriffen entgegenwirken
Der Anbieter des ePA-Aktensystems MUSS Maßnahmen zur Erkennung und Verhinderung von Social Engineering Angriffen umsetzen.**[<=]**

A_24989 -Anbieter ePA-Aktensystem - Schutz vor Angriffen über die TI
Die Anbieter des ePA-Aktensystems MUSS für alle über die TI erreichbaren Schnittstellen des ePA-Aktensystems Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS Lösungen verhindert werden.**[<=]**

A_15168 -ePA-Aktensystem - Verbot vom dynamischen Inhalt
Die Komponenten des ePA-Aktensystems DÜRFEN dynamischen Inhalt von Drittanbietern NICHT herunterladen und verwenden.
[<=]

A_17080 -Verhindern von Session Hijacking
Die Komponenten des ePA-Aktensystems MÜSSEN geeignete Schutzmaßnahmen gegen Session-Hijacking implementieren.
[<=]

A_16323-01 -ePA-Aktensystem - Verbot von medizinisch irrelevantem Inhalt
Der Anbieter des ePA-Aktensystems MUSS der Ablage von Dokumenten, die für die medizinische Versorgung oder für die Eigenorganisation medizinischer Belange des Versichertenoder zur Erstattung der Behandlungskosten irrelevant sind, mittels AGB auf Anbieterseite entgegenwirken.
[<=]

A_24781 -Sicherer Betrieb des Produkts nach Handbuch
Der Anbieter eines ePA-Aktensystems MUSS die im Handbuch des eingesetzten ePA-Aktensystems beschriebenen Voraussetzungen für den sicheren Betrieb des Produktes gewährleisten.**[<=]**

A_18953 -Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch
Der Hersteller des ePA-Aktensystems MUSS für sein Produkt im dazugehörigen Handbuch leicht ersichtlich darstellen, welche Voraussetzungen vom Betreiber und der Betriebsumgebung erfüllt werden müssen, damit ein sicherer Betrieb des Produktes gewährleistet werden kann.**[<=]**

A_19122-01 -Anbieter ePA-Aktensystem – Trennung zu anderen Mandanten
Ein Betreiber eines ePA-Aktensystems MUSS sicherstellen, dass die Daten von unterschiedlichen Mandanten organisatorisch und technisch getrennt sind.**[<=]**

A_21106 -Anbieter ePA-Aktensystem – Signaturschlüssel für Protokolle
Das ePA-Aktensystem MUSS für die Signatur von Listen von Protokollen des Versicherten Schlüsselmaterial der Ausstelleridentität ID.FD.SIG mit einem zugehörigen Zertifikat C.FD.SIG mit der Rolle oid_epa_logging gemäß [gemSpec_OID] besitzen.**[<=]**

A_21107 -Anbieter ePA-Aktensystem – Speicherung Signaturschlüssel für Protokolle im HSM
Das ePA-Aktensystem MUSS das private Schlüsselmaterial der Ausstelleridentität ID.FD.SIG für die Signatur von Listen von Protokollen des Versicherten in einem HSM speichern.
[<=]

A_22409 -Anbieter ePA-Aktensystem - CA-Anbieterwechsel
Der Anbieter des ePA-Aktensystems MUSS mindestens drei Monate vor dem Wechsel des CA-Anbieters für die Ausstellung der TLS-Zertifikate des Access Gateways die gematik darüber informieren, wer der alte Anbieter war und wer der neue Anbieter wird.**[<=]**

A_19118-01 -Komponenten des Aktensystems, Schutz vor XSW-Angriffen
Die Komponenten des ePA-Aktensystems, die XML-Signaturen prüfen, MÜSSEN geeignete Maßnahmen gegen XSW-Angriffe umsetzen. Mindestens MÜSSEN sie die FastXPath-Auswertung der XML-Daten und XML-Signaturen gemäß [GJLS-2009] (vgl. auch [BSI-XSpRES]) umsetzen.**[<=]**

A_24783 -ePA-Aktensystem - Eingabevalidierung von Operationen
Das ePA-Aktensystem MUSS alle Operationsaufrufe seiner Schnittstellen (Requests) sowie die Antwortmeldung auf seine Anfragen (Responses) auf Wohlgeformtheit und Zulässigkeit prüfen und bei Encoding-, Schema-, Semantik- oder Protokollverletzungen die Operation abbrechen.**[<=]**

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

A_24992 -ePA-Aktensystem - Zugriffe durch Versicherte übers Access Gateway
Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session für einen Versicherten (NutzerID ist KVNR) ausschließlich über das Access Gateway erreichbar ist.**[<=]**

A_24993 -ePA-Aktensystem - Zugriffe übers Access Gateway ausschließlich für Versicherte
Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session für einen Nutzer, dessen NutzerID keine KVNR ist (z.B. Leistungserbringerinstitutionen) nicht über das Access Gateway erreichbar ist.**[<=]**

A_25006 -ePA-Aktensystem - User Session bei Inaktivität Beenden
Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session nach 20 Minuten Inaktivität beendet wird.**[<=]**

A_25022 -ePA-Aktensystem - Debug-Protokoll für Testbetrieb
Das ePA-Aktensystem KANN im Testbetrieb ein Debug-Protokoll schreiben, welches eine erweiterte Protokollierung für Testzwecke ermöglicht.**[<=]**

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

A_25023 -ePA-Aktensystem - Keine Echtdaten im Testbetrieb
Das ePA-Aktensystem MUSS sicherstellen, dass im Testbetrieb keine Echtdaten verarbeitet werden.**[<=]**

A_25042 -ePA-Aktensystem - Prüfung von Signaturen
Das ePA-Aktensystem MUSS bei der Prüfung von Signaturen

- das Signaturzertifikat gemäß A_25040-* prüfen,
- die Signatur prüfen (i. S. v. Verify()-Funktion des kryptographischen Signaturverfahrens ergibt "valid")

[<=]

A_25040-01 -ePA-Aktensystem - Prüfung Signaturzertifikate
Das ePA-Aktensystem MUSS Signaturzertifikate gemäß [gemSpec_PKI#TUC_PKI_018] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat

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

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

A_27498 -Anbieter ePA-Aktensystem - Offline-Datensicherung
Der Anbieter des ePA-Aktensystems MUSS Offline-Datensicherungen für die Aktenkonten umsetzen.**[<=]**

A_27497 -Anbieter ePA-Aktensystem - Rollenkonzept zum Schutz der permanenten Verfügbarkeit von Aktenkonten
Der Anbieter des ePA-Aktensystems MUSS durch ein Rollenkonzept sicherstellen, dass ein einzelner Mitarbeiter die Verfügbarkeit der Akten nicht permanent zerstören kann, z.B. durch endgültiges Löschen von Masterkeys oder von Chiffraten der Daten der Aktenkonten. Organisatorische Maßnahmen wie Dienstanweisungen sind alleine nicht ausreichend, um eine Rollentrennung zu etablieren.
[<=]

A_27499 -Anbieter ePA-Aktensystem - HSM-Backups im 4-Augen-Prinzip

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

A_27500 -Anbieter ePA-Aktensystem - Rollentrennung Administratoren für Backup- und Produktionsdaten
Der Anbieter des ePA-Aktensystems MUSS sicherstellen, das es eine Rollentrennung zwischen Backup-Administratoren und Administratoren der Produktivumgebung gibt.**[<=]**

A_30420 -ePA-Aktensystem - Restore einzelner Aktenkonten
Das ePA-Aktensystem SOLL die Möglichkeit schaffen, dass einzelne Aktenkonten aus einem bestehenden Backup wiederhergestellt werden können.**[<=]**

A_28333 -ePA-Aktensystem - zulässige Operationen im Aktenkontostatus SUSPENDED
Das ePA-Aktensystem MUSS sicherstellen, dass die Nutzung des Aktensystems im Status SUSPENDED außer für den Anbieterwechsel sowie das Auslesen der Auditprotokolle des Versicherten nicht möglich ist.
[<=]

2.4 Validierungsaktenkonto

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

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

Folgende Anwendungsfälle sollen mit den Validierungsaktenkonten adressiert werden:

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

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

A_18168-01 -Anbieter des ePA-Aktensystem - Validierungsaktenkonto für gematik
Nach Aufforderung durch die gematik MUSS der Anbieter des ePA-Aktensystems

- für die gematik ein Validierungsaktenkonto im ePA-Aktensystem für die von der gematik übergebene KVNR anlegen, wobei die KVNR die Festlegungen für die Versichertennummer [gem. gemSysL_PK_eGK] erfüllen muss.
- das durch die gematik angegebene Validierungsaktenkonto löschen, sofern die gematik dessen Anlage beantragt hatte.

[<=]

A_18169-02 -Anbieter des ePA-Aktensystem - Validierungsaktenkonto für eigene Zwecke
Falls sich der Anbieter des ePA-Aktensystems ein Validierungsaktenkonto für eigene Zwecke anlegen möchte, MUSS er sicherstellen, dass nur eine Versichertennummer aus dem von der gematik für diesen Anbieter freigegebenen Nummernkreis [gem. gemSysL_PK_eGK] verwendet wird.
[<=]

A_22522-01 -Anbieter des ePA-Aktensystems - Validierungskonto für Dritte
Der Anbieter des ePA-Aktensystems MUSS auf Antrag der gematik

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

[<=]

Hinweis zu A_22522-*: Die Einrichtung der Validierungsaktenkonten für Dritte kann gegen Bezahlung erfolgen. Die Entscheidung *dafür obliegt dem Anbieter des ePA-Aktensystems.*

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

A_26187 -Anlage von Validierungsaktenkonten
Das ePA-Aktensystem MUSS die Anlage von Validierungsaktenkonten auch ohne KTR- und Ombudsstellen-Befugnisse zulassen.**[<=]**

A_26188 -Anbieter des ePA-Aktensystems -Aktivierung von Validierungsaktenkonten
Der Anbieter des ePA-Aktensystems MUSS den Status von Validierungsaktenkonten, welche für die gematik (gem. A_18168-*) oder für Dritte (gem. A_22522-*) angelegt wurden, nach der Anlage auf ACTIVATED setzen.**[<=]**

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

A_22524-01 -Anbieter des ePA-Aktensystems - Löschen von Validierungsaktenkonten nach 5 Jahren

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

A_22684-01 -Validierungsaktenkonten im Store-Review der FdVs
Der Anbieter/Hersteller des ePA-Aktensystems bzw. Hersteller des ePA-FdVs KANN - ausschließlich für dedizierte KVNRn von Validierungsaktenkonten zum Zwecke der Verwendung im Store-Review der FdVs – Vorkehrungen treffen, die es ermöglichen auf Gerätebindung, E-Mail-Validierung oder andere Aktivitäten des Registrierungs-/Anmeldeprozesses zu verzichten, um eine Prüfung der FdVs durch die App-Store-Betreiber zu ermöglichen. **[<=]**

A_22942 -Besonderheiten bei 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 dem Review zu leeren,
- es sind Zeitraum der Erreichbarkeit und eine eindeutige Referenz auf den Review (z.B. Vorgangsnummer) zu dokumentieren und auf Anforderung an die gematik zu übertragen

[<=]

A_26209 -Prüfung auf Vertretungsberechtigung für Prüfidentität
Das ePA-Aktensystem MUSS sicherstellen, dass bei der Vertreterbefugnis ausschließlich "echte" Vertreter für "echte" Konten befugt, bzw. auf Validierungsaktenkonten ausschließlich "Validierungs-Vertreter" eingerichtet werden können.**[<=]**

A_24539 -Nutzung von Validierungsaktenkonten via FdV
Der Anbieter des ePA-Aktensystems bzw. Hersteller des ePA-FdVs MUSS ein FdV bereitstellen, mit dem der Zugriff auf Validierungsaktenkonten möglich ist.**[<=]**

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

2.5 Tracing in Nichtproduktivumgebungen

Ein gewonnener Erfahrungswert ist, dass es für die Fehlersuche in Nichtproduktivumgebungen -- insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase -- leistungsfähigere Mechanismen als zuvor geben muss. Gab es zunächst nur die Testschnittstelle ([gemKPT_Test#A_21193-*]) in den ePA-Clients, so wurde mit ePA 2.0 ein Tracing im Aktensystem für Nichtproduktivumgebungen eingeführt und wird mit ePA für alle wie folgt umgesetzt:

1. Innerhalb des AS werden an die für die Fehlersuche in Nichtproduktivumgebungen wichtigen Stellen Sensoren platziert. Diese Sensoren streamen die aktuell transportierten Daten an bestimmte TCP-Ports am Access Gateway. Die Sensorpunkte liegen im AS immer hinter der TLS-Entschlüsselung. Fehlersuchende können sich zu diesen TCP-Ports am Access Gateway verbinden und lesen dann im Read-Only-Modus den aktuellen Datenverkehr, der an den Sensorpunkten vorbeifließt, mit.

2. ePA-Clients müssen in Nichtproduktivumgebungen beim VAU-Protokoll die symmetrischen Verbindungsschlüssel offenlegen [gemSpec_Krypt#A_24477-*].

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

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

A_21887-01 -Tracing, Sensorpunkt nahe vor den VAU-Instanzen (Nichtproduktivumgebungen)
Ein ePA-Aktensystem MUSS sicherstellen, dass genau in Nichtproduktivumgebungen der Datenverkehr zur und von den VAU-Instanzen auf TCP-Ebene mitgeschnitten wird (Sensorpunkt). Der aktuell mitgeschnittene Datenverkehr MUSS auf einen TCP-Port im Access Gateway gestreamt werden (siehe A_21890-*). D. h. wenn ein Client sich zu diesem TCP-Port verbindet, MUSS er die aktuell auf dem Interface durchlaufenden Daten gestreamt lesen können.
[<=]

A_21891-01 -Tracing, Tiger-Standalone-Proxy
Ein ePA-Aktensystem MUSS zum Mitschneiden und Streamen der Testdaten in Nichtproduktivumgebungen nach A_21887-* den von der gematik bereitgestellten aggregierenden Tiger-Standalone-Proxy (mindestens der Version 0.20) verwenden.**[<=]**

A_22581 -Tracing, Abschaltbarkeit
Ein ePA-Aktensystem MUSS den Tiger-Standalone-Proxy (und die damit 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_22470-06 -Definition x-useragent
Das Produkt MUSS für das x-useragent-Element in Eingangs- oder Ausgangsparametern einer Operation folgende Formatvorgaben berücksichtigen:

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

Beispiel: "CLIENTID1234567890AB/2.1.12-45"
Hinweis: gem. RFC7231 ist im http-Header ein Useragent einzutragen. Dieser RFC-Useragent enthält z.B. Angaben zum Betriebssystem oder zum Browser und ist nicht zu verwechseln mit dem hier definierten x-useragent. Dieser (x-useragent) muss deshalb im x-useragent-Parameter des http-Headers eingetragen werden, NICHT im Useragent-Parameter gem. RFC7231. Ein Beispiel für die Verwendung bieten die OpenAPI-Spezifikationen der fachlichen Aktensystem-Operationen.**[<=]**

Hinweis zum Erhalt der Client-ID: Die Client-ID wird durch die gematik vergeben und übermittelt, sobald sich ein (Client-)Produkthersteller unter https://fachportal.gematik.de/formulare-product-id/neuanlage registriert hat. Dazu ist im Rahmen dieser Registrierung der Name des Herstellers und der Name des zu registrierenden Produktes zu übermitteln. Sollte für eine andere TI-Anwendung bereits eine Registrierung vorgenommen worden sein, kann die Client-ID auch im ePA-Kontext genutzt werden (sofern es sich um das gleiche Softwareprodukt handelt). In diesem Fall sollte eine Anpassung der Verwendungszwecke der Client-ID/product-id unter https://fachportal.gematik.de/formulare-product-id/aenderung-zwecke-der-product-id vorgenommen werden. Die Versionsnummer kann im Rahmen der erlaubten Zeichen vom Hersteller frei gewählt werden und sollte bei ePA-relevanten Änderungen des Produkts aktualisiert werden. In den Formularen ist immer von "product-id" die Rede, da der Useragent zukünftig aus product-id und Versionsnummer bestehen wird - es ändert sich dabei aber nur der Name.

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

2.8 Performance aus Anwendersicht

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

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

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

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

A_24570-01 -Verarbeitung von UX-Messdaten
Das ePA-Aktensystem MUSS für die im zu betrachtenden Zeitintervall der Betriebsdatenlieferung (gemäß [gemSpec_Perf]) eingegangenen Messdaten je UX-Usecase, je Client-ID und je Client-Version folgende Werte ermitteln und gemäß [gemSpec_Perf] übermitteln:
- Durchschnittswert der Messergebnisse
- Anzahl der berücksichtigten Messergebnisse
- Maximalwert
- Minimalwert**[**<=**]**

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

3 Funktionsmerkmale

3.1 Aktenkontoverwaltung

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. In einem Aktenkonto ist entweder der Widerspruch des Versicherten gegen die ePA hinterlegt oder eine Akte für den Versicherten. Die Verwaltung eines Aktenkontos und der darin enthalten Akte oder Widerspruch durch den Kostenträger erfolgt über das Account Management.

Die ITSG stellt im Auftrag des GKV-SV ein System bereit, das über ein Token attestiert, dass ein bestimmter Kostenträger berechtigt ist eine KVNR zu verwalten und damit auch die ePA für diese KVNR zu verwalten. Dieses ITSG-Token wird in der Aktenkontoverwaltung genutzt, um Aktionen des Kostenträgers zu berechtigen. Festlegungen zu Inhalten, Format und Signatur des ITSG-Token sind in den "Richtlinien zum Aufbau und zur Vergabe einer Krankenversichertennummer (KVNR) und Regelungen des Krankenversichertennummernverzeichnis nach § 290 SGB V einschließlich der dazugehörigen Anlagen" [RL_KVNR], in der Anlage 4 zu finden.

A_30369 -Account Management - Realisierung der Schnittstelle I_Account_Management
Das Account Management MUSS die Operationen der Schnittstelle `I_Account_Management` gemäß [I_Account_Management] umsetzen.**[<=]**

A_30356 -Anbieter ePA-Aktensystem - Anlage eines Aktenkontos für den Versicherten
Der Anbieter des ePA-Aktensystems MUSS für seine Versicherten ein Aktenkonto im ePA-Aktensystem über die Schnittstellen [I_Account_Management] anlegen und verwalten. **[<=]**

A_24336 -Anbieter ePA-Aktensystem - Identifizierung eines Aktenkontos
Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos die KVNR des Versicherten zur Identifikation des Aktenkontos im Aktensystem verwenden und sicherstellen, dass diese Identifikation eines Aktenkontos nicht verändert werden kann.**[<=]**

A_30359 -Anbieter ePA-Aktrensystem - Anlage Aktenkonto erst nach Ablauf einer Widerspruchsfrist
Der Anbieter des ePA-Aktensystems DARF ein neues Aktenkonto NICHT anlegen, bevor die gesetzliche Widerspruchsfrist abgelaufen ist es sei denn, es liegt ihm ein Widerspruch gegen die Nutzung der ePA vor.**[<=]**

A_30373 -Account Management - Prüfung auf Berechtigung des Kostenträgers
Das Account Management MUSS sicherstellen, dass Operationen zum Erstellen eines Aktenkontos, Erstellen einer Akte oder hinterlegen eines Widerspruchs nur durchgeführt werden können, wenn der handelnde Kostenträger ein gültiges ITSG-Token vorweisen kann, das ihn als berechtigten Kostenträger für die betreffende KVNR ausweist.**[<=]**

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 keine Akte für diesen Versicherten erzeugt und der Widerspruch im Aktenkonto hinterlegt. Existiert zum Zeitpunkt des Widerspruchs schon eine Akte (in einem beliebigen Zustand), so wird dieses gelöscht, alle enthaltenen Daten werden gelöscht und der Widerspruch wird im Aktenkonto hinterlegt.

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.

A_30357 -Anbieter ePA-Aktensystem - Hinterlegung eines Widerspruchs im ePA-Aktensystem
Der Anbieter des ePA-Aktensystems MUSS einen Widerspruch gegen die ePA im Aktenkonto im ePA-Aktensystem hinterlegen. Eine bestehende Akte wird dann durch das ePA-Aktensystem gelöscht.**[<=]**

A_30358 -Anbieter ePA-Aktensystem - Hinterlegung des Rücknahme eines Widerspruchs
Der Anbieter des ePA-Aktensystems MUSS bei Rücknahme eines Widerspruchs gegen die ePA eine Akte im Aktenkonto anlegen, wodurch der Widerspruch im Aktenkonto des ePA-Aktensystems gelöscht.**[<=]**

A_30374 -Account Management - Übermittlung eines Widerspruchs an das FDZ bei Widerspruch gegen die ePA
Das Account Management MUSS vor der Löschung einer Akte aufgrund eines hinterlegten Widerspruchs gegen die Nutzung der ePA, ein Widerspruch gegen die Datenausleitung zu Sekundärnutzungszwecken für diese Akte an den Data Submission Service übergeben, sofern der Widerspruch gegen die Datenausleitung nicht schon im Consent Decision Management vorliegt.**[<=]**

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 Anlage eines neuen Aktenkontos

Ein neues Aktenkonto wird für einen Versicherten bei seinem Anbieter automatisch angelegt und darin entweder der Widerspruch gegen die grundsätzlichen Nutzung der ePA gespeichert oder bei fehlendem Widerspruch eine Akte angelegt. Innerhalb der Gesamtsystems ePA darf es zu einem Versicherten (zu einer KVNR) nur ein Aktenkonto geben. Bei einem Wechsel des Kostenträgers werden die Informationen eines Aktenkontos zum neuen Kostenträger verschoben.

Bei Anlage eines Aktenkontos wird erst geprüft, ob lokale oder auf anderen ePA-Aktensystemen schon ein Aktenkonto zur KVNR existiert. Sollte mehr als ein ePA-Aktensystem Informationen zu einer KVNR melden, wird der Vorgang abgebrochen und die Situation über die beteiligten Kostenträger aufgeklärt. Existiert schon ein Aktenkonto, so werden dessen Informationen in das lokale ePA-Aktensystem verschoben, bzw., wenn

das Aktenkonto schon lokal existiert, die Befugnisse für den zuständigen Kostenträger und die zuständige Ombudsstelle aktualisiert.

Nachfolgend ist der generelle Ablauf der Anlage eines Aktenkontos mit möglicher Verschiebung von Informationen aus einem bestehenden Aktenkonto dargestellt.

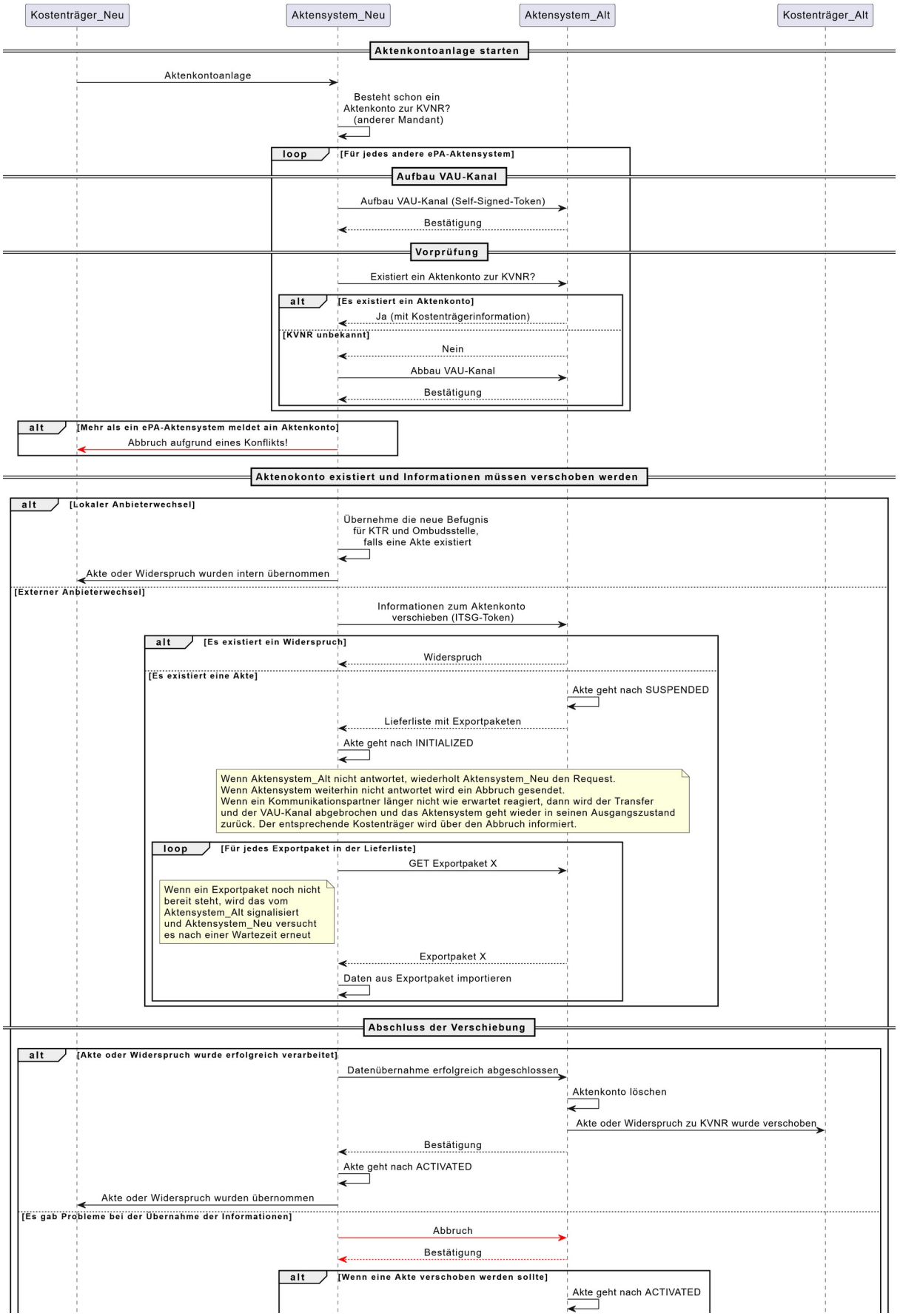

Kostenträger_Neu
Aktensystem_Neu
Aktensystem_Alt
Kostenträger_Alt
Aktenkontoanlage starten
Aktenkontoanlage
Besteht schon ein Aktenkonto zur KVNR? (anderer Mandant)
loop
[Für jedes andere ePA-Aktensystem]
Aufbau VAU-Kanal
Aufbau VAU-Kanal (Self-Signed-Token)
Bestätigung
Vorprüfung
Existiert ein Aktenkonto zur KVNR?
alt
[Es existiert ein Aktenkonto]
Ja (mit Kostenträgerinformation)
[KVNR unbekannt]
Nein
Abbau VAU-Kanal
Bestätigung
alt
[Mehr als ein ePA-Aktensystem meldet ain Aktenkonto]
Abbruch aufgrund eines Konflikts!
Aktenokonto existiert und Informationen müssen verschoben werden
alt
[Lokaler Anbieterwechsel]
Übernehme die neue Befugnis für KTR und Ombudsstelle, falls eine Akte existiert
Akte oder Widerspruch wurden intern übernommen
[Externer Anbieterwechsel]
Informationen zum Aktenkonto verschieben (ITSG-Token)
alt
[Es existiert ein Widerspruch]
Widerspruch
[Es existiert eine Akte]
Akte geht nach SUSPENDED
Lieferliste mit Exportpaketen
Akte geht nach INITIALIZED
Wenn Aktensystem_Alt nicht antwortet, wiederholt Aktensystem_Neu den Request.
Wenn Aktensystem weiterhin nicht antwortet wird ein Abbruch gesendet.
Wenn ein Kommunikationspartner länger nicht wie erwartet reagiert, dann wird der Transfer und der VAU-Kanal abgebrochen und das Aktensystem geht wieder in seinen Ausgangszustand zurück. Der entsprechende Kostenträger wird über den Abbruch informiert.
loop
[Für jedes Exportpaket in der Lieferliste]
GET Exportpaket X
Wenn ein Exportpaket noch nicht bereit steht, wird das vom Aktensystem_Alt signalisiert und Aktensystem_Neu versucht es nach einer Wartezeit erneut
Exportpaket X
Daten aus Exportpaket importieren
Abschluss der Verschiebung
alt
[Akte oder Widerspruch wurde erfolgreich verarbeitet]
Datenübernahme erfolgreich abgeschlossen
Aktenkonto löschen
Akte oder Widerspruch zu KVNR wurde verschoben
Bestätigung
Akte geht nach ACTIVATED
Akte oder Widerspruch wurden übernommen
[Es gab Probleme bei der Übernahme der Informationen]
Abbruch
Bestätigung
alt
[Wenn eine Akte verschoben werden sollte]
Akte geht nach ACTIVATED

Abbildung 1 : Ablauf der Anlage eines Aktenkontos

Die Festlegungen und die Beschreibung der Verschiebung von Informationen eines Aktenkontos sind im Kapitel "Verschiebung der Informationen eines Aktenkontos" beschrieben.

A_30375 -Account Management - Prüfung der KVNR bei Anlage eines Aktenkontos
Das Account Management MUSS bei Anlage eines Aktenkontos lokal und beim Account Management auf allen anderen ePA-Aktensystemen prüfen, ob schon ein Aktenkonto zur entsprechenden KVNR existiert.**[<=]**

A_30376 -Account Management - Abbruch der Anlage eines Aktenkontos bei Konflikt
Das Account Management DARF ein Aktenkonto NICHT anlegen, wenn auf mehr als einem ePA-Aktensystem schon ein Aktenkonto zur entsprechenden KVNR existiert.**[<=]**

A_30401 -Account Management - Absicherung der Kommunikation über einen VAU-Kanal
Das Account Management MUSS die Kommunikation mit den Accounts Managements der anderen ePA-Aktensysteme über einen VAU-Kanal absichern. Für die Authentisierung am anderen ePA-Aktensystem wird das Self-Signed-Token des Kostenträgers verwendet.**[<=]**

A_30377 -Account Management - Information des Kostenträgers zum Abbruch der Anlage eines Aktenkontos
Das Account Management MUSS den zuständigen Kostenträger über den Abbruch der Anlage des Aktenkontos und den Grund dafür informieren. Dabei MUSS es dem zuständigen Kostenträger Informationen zu den am Konflikt beteiligten anderen ePA-Aktensystemen und Kostenträgern mitteilen.**[<=]**

A_30402 -Account Management - Sicherstellung lokaler Konsistenz
Das Account Management MUSS sicherstellen, dass es zu einer KVNR im ePA-Aktensystem immer nur ein Aktenkonto geben kann und dass in einem Aktenkonto immer nur genau ein Widerspruch oder genau eine Akte existiert.**[<=]**

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.**[<=]**

3.1.3 Löschen eines Aktenkontos

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

- nach Wechsel des Anbieters durch den Versicherten zu einem Anbieter, der die ePA seinen Versicherten nicht anbietet,
- nachdem der Versicherte das generell das System der ePA verlassen hat, da er z.B. ins Ausland verzogen ist oder verstorben ist.

Kündigt ein Versicherter das Vertragsverhältnis ohne Übernahme der Daten zu einem neuen Anbieter, löscht der Anbieter des Aktenkontos des Versicherten nach einer angemessenen Wartezeit, bzw. nach Ablauf von vorgeschriebenen Bereitstellungs- und Aufbewahrungszeiträumen, das Aktenkonto und alle darin enthaltenen Daten.

Vor der Ausführung der endgültigen Löschung des Aktenkontos muss es dem Versicherten ermöglicht werden, die Protokolldaten (auch unter Einbindung der Ombudsstelle) für seinen eigenen Gebrauch außerhalb des Aktenkontos zu sichern.

Bei der Löschung eines Aktenkontos muss der Anbieter die Administrationsgewalt über die entsprechende KVNR nicht über ein ITSG-Token nachweisen, da er dieses in bestimmten Anwendungsfällen (z.B. Wechsel des Versicherten zu einem Anbieter ohne ePA) nicht abrufen kann. Die Löschung erfolgt Risiko des löschenden Kostenträgers.

A_30403 -Account Management - Löschung eines Aktenkontos
Das Account Management MUSS den Auftrag zur Löschung eines Aktenkontos vom zuständigen Kostenträger unverzüglich ausführen und alle Informationen im Aktenkonto (Verwaltungsinformationen und Akte / Widerspruch) sicher löschen.**[<=]**

3.1.4 Verschiebung der Informationen eines Aktenkontos

Wird bei der Anlage eines Aktenkontos für einen Kostenträger festgestellt, dass es zu der entsprechenden KVNR schon ein Aktenkonto bei einem anderen Kostenträger gibt, so werden die Informationen daraus zum aktuellen Kostenträger verschoben. Dabei kann es sich um eine lokale Verschiebung innerhalb eines ePA-Aktensystems handeln oder um die Verschiebung aus einem anderen ePA-Aktensystem.

Das Account Management agiert im Zusammenhang mit der Verschiebung der Informationen eines Aktenkontos in zwei Rollen. Zum einen agiert das Account Management beim Anlegen eines Aktenkontos als Client der Informationen von einem anderen ePA-Aktensystem abruft. Zum anderen agiert das Account Management auf dem abgebenden ePA-Aktensystem als Server, der Informationen zum Widerspruch bereitstellt oder die Daten einer Akte in Exportpaketen zusammen- und bereitstellt.

Für die Verschiebung der Information eines Widerspruchs ist kein Exportpaket nötig, da diese an der Schnittstelle unmittelbar bereitgestellt wird.

Der Ablauf einer Verschiebung ist wie folgt (siehe auch Abbildung "Ablauf der Anlage eines Aktenkontos"):

1. Das lokale ePA-Aktensystem startet den Vorgang beim anderen ePA-Aktensystem
2. Das andere ePA-Aktensystem liefert entweder einen Widerspruch oder eine Liste von Exportpaketen. Falls es ein Widerspruch ist, wird dieser übernommen und der Vorgang abgeschlossen.

3. Falls eine Liste von Exportpaketen geliefert wurde, so wird diese nacheinander abgearbeitet indem
   a. ein Exportpaket von der Liste durch das lokale ePA-Aktensystem geholt wird
   b. der Inhalt des Exportpakets in die Akte des lokalen ePA-Aktensystems importiert wird
4. Nachdem das letzte Exportpaket geholt und erfolgreich importiert wurde, wird der Vorgang abgeschlossen
5. Die lokale Akte geht in den Status Activated und das Aktenkonto auf der abgebenden Seite wird gelöscht

In dieser Spezifikation werden die Aktivitäten des Account Managements, die sich um das Erstellen von Exportpaketen und dem Import von Daten aus einem Exportpaket in einem internen virtuellen Health Record Relocation Service zusammengefasst. Dieser Service hat keine Schnittstellen außerhalb der VAU und dient nur einer fachlichen Gruppierung von Anforderungen. Nach außen hin werden diese Leistungen vom Account Management erbracht.

A_30412 -Account Management - Abbruch bei Inaktivität der aufnehmenden Seite
Das Account Management der abgebenden Seite MUSS das Verschieben von Informationen abbrechen und wieder in den Ausgangszustand zurückkehren, wenn das Account Management der aufnehmenden Seite mehr als 60 Minuten kein neues Request schickt, obwohl die Verschiebung der Informationen noch nicht abgeschlossen ist.**[<=]**

A_30413 -Account Management - Abbruch bei Inaktivität der abgebenden Seite
Das Account Management der aufnehmenden Seite MUSS, wenn das Account Management der abgebenden Seite auch nach 4 Retries im Prozess der Verschiebung nicht antwortet, die Verschiebung abbrechen, den VAU-Kanal abbauen und das lokale Aktenkonto löschen.**[<=]**

A_30414 -Account Management - Unklare Situation bei Abschluss der Verschiebung
Das Account Management der aufnehmenden Seite MUSS, wenn das Account Management der abgebenden Seite den Abschluss der Verschiebung nach 4 Retries im Prozess der Verschiebung nicht bestätigt, eine mögliche lokale Akte in den Status INACCESSIBLE setzen und den zuständigen Kostenträger über das Problem beim Abschluss der Verschiebung informieren.
[<=]

A_30416 -Account Management - Aktenkonto eingefroren bei unklarer Situation bei Abschluss der Verschiebung
Das Account Management DARF für Aktenkonten, bei denen die Verschiebung von Informationen aufgrund von Inaktivität der abgebenden Seite beim Abschluss nicht erfolgreich abgeschlossen werden konnte, NICHT eine weitere Verschiebung unterstützen.**[<=]**

A_30415 -Account Management - Erfolgreicher Abschluss, falls erste Antwort verloren ging
Das Account Management der aufnehmenden Seite MUSS, wenn es auf einen Retry der Abschlusses der Verschiebung die Antwort erhält, dass das Aktenkonto unbekannt ist, die Verschiebung als erfolgreich abgeschlossen betrachten.**[<=]**

3.1.4.1 Erzeugen von Exportpaketen

Als abgebendes ePA-Aktensystem müssen die Daten einer Akte in ein interoperables Austauschformat gebracht werden, damit das aufnehmende ePA-Aktensystem diese versteht und verarbeiten kann. Dieses Austauschformat wird über die Festlegungen zum Exportpaket definiert. Nachfolgend finden sich die Festlegungen zur Erstellung und zum Inhalt des Exportpakets.

Hinweis: Aktuell werden die Daten aller Services in einem Exportpaket zusammengefasst. Zukünftig ist es mit steigender Größe einer Akte für das exportierenden ePA-Aktensystem möglich, die Daten auf mehrere Exportpakete aufzuteilen, um lange Wartezeiten an der Schnittstelle zu vermeiden. Die Schnittstelle und die hier definierten Anforderungen sind schon daraufhin festgelegt, dass sie auch die Aufteilung in mehrere Pakete unterstützen.

A_25005-05 -Health Record Relocation Service - Daten des Exportpakets
Der Health Record Relocation Service MUSS sicherstellen, dass alle Daten einer Akte aus den nachfolgenden Services in ein oder mehrere Exportpakete übernommen werden. Die Daten eines Services MÜSSEN sich dabei immer in einem einzelnen Exportpaket befinden.

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

Bei FHIR Data Services MUSS das Account Management sicherstellen, dass die jeweilige Resource.id aller FHIR-Instanzen ebenso in das Exportpaket einfließen, sodass nach einem Import die Identitäten der FHIR-Daten stabil bleiben.
[<=]

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

A_25605-02 -Health_Record_Relocation_Service - Erstellung des Exportpakets
Der Health Record Relocation Service MUSS sicherstellen, dass das Exportpaket gemäß der Vorgaben in [Exportpaket] bezüglich der Struktur, der Formate für die enthaltenen Daten und die Verschlüsselung erfolgt.**[<=]**

A_25012 -Health Record Relocation Service - Signatur der Befugnisse
Der Health Record Relocation Service MUSS sicherstellen, dass die gemäß A_23734-* signierten Anteile einer Befugnis mit der Signaturidentität ID.FD.SIG (Rolle `oid_epa_vau`) signiert werden.**[<=]**

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

A_25719 -Health Record Relocation Service - JWT der Befugnis im Exportpaket
Der Health Record Relocation Service MUSS sicherstellen, dass die Befugnisse im Exportpaket als gültig signierte JWT mit den dargestellten Inhalten abgelegt sind:

Tabelle 2 : Inhalte des JWT der Befugnisse im Exportpaket

Befugnis	Claim Name	Claim	Beispiel
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.SIG	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	
	"exp"	Verfalldatum, = "iat" + 8Tage"	Mindestens für den gesamten Bereitstellungszeitraum des Exportpakets
	"insurantId"	KVNR des Aktenkontos	A123456789
	"actorId"	Identifier (Telematik-id oder KVNR)	3-883110000092471
	"validTo"	Ende der Gültigkeit,	gemäß [RFC3339], z.B. 2025-06-30T21:59:59Z oder 2025-06-30T23:59:59+02:00

[<=]

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

A_24821-01 -Health Record Relocation Service - Suspendierung des Aktenkontos
Der Health Record Relocation Service MUSS sicherstellen, dass die Akte für die Erstellung eines Exportpakets auf den Status SUSPENDED gesetzt wird.**[<=]**

A_24827-01 -Health Record Relocation Service - Reaktivierung des Aktenkontos
Der Health Record Relocation Service MUSS sicherstellen, dass eine Akte 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_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-256verwenden.
Beispiel Digest-Header:
Digest: SHA-256=MWVkMWQxYTRiMzk5MDQ0MzI3NGU5NDEyZTk5OWY1ZGFmNzgyZTJlODYzYjRjYzFhOTlmNTQwYzI2M2QwM2U2MQ==
[<=]

3.1.4.2 Import von Exportpaketen

Beim Import eines Exportpakets werden die darin enthaltenen Daten in das lokale ePA-Aktensystem integriert. Dabei sind bestimmte Regeln einzuhalten. Die entsprechenden Vorgaben sind in diesem Kapitel dargestellt.

A_14905-05 -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:

- den Digest gemäß A_21750-* prüfen,
- die Befugnisse mit Regel "rr5" (siehe Tab_AS_Entitlement_Registration_Rules im Aktensystem) registrieren und
- falls DocumentEntry.originalURI im Exportpaket vorhanden ist, wird für jedes Dokument eines SubmissionSet der Inhalt von DocumentEntry.URI durch den Inhalt von DocumentEntry.originalURI ersetzt. (Hinweis: DocumentEntry.originalURI darf nicht als eigenständiges Metadatum in die Registry übernommen werden, da es lediglich dem Transport des Originalwertes von DocumentEntry.URI aus dem alten Aktensystem dient.

[<=]

A_28045-01 -Health Record Relocation Service - Übernahme von Widersprüchen
Der Health Record Relocation Service MUSS sicherstellen, dass beim Import von Widersprüchen zur Sekundärdatennutzung berücksichtigt wird, ob das Feature in der abgebenden Akte bzw. in der aufnehmenden Akte unterstützt wird. Dabei MUSS wie folgt vorgegangen werden:

- neu unterstützt: Die Widersprüche werden unverändert übernommen.
- neu nicht unterstützt: Die Widersprüche werden als "erteilt" gesetzt (decision = deny).

Bei Veränderung der Entscheidung MUSS dem Sekundärnutzungszweck als Zeitpunkt der Änderung der feste Wert "2025-01-15T00:00:00Z" und als Akteur "system" zugeordnet werden.
[<=]

Hinweis:
Die Verschiebung von einem Kostenträger, der das Feature Sekundärdatennutzung nicht unterstützt zu einem Kostenträger, der das Feature Sekundärdatennutzung unterstützt führt zu einem Opt-In für dieses Feature. D.h. für eine Sekundärdatennutzung muss ein

Versicherter bzw. Vertreter nach der Verschiebung aktiv der Sekundärdatennutzung zustimmen, was durch geeignete Prozesse des Kostenträgers unterstützt wird.

A_27616 -Health Record Relocation Service - Abbruch des Imports eines Exportpakets
Der Health Record Relocation Service MUSS den Import eines Exportpakets vollständig abbrechen, wenn einzelne Elemente des Exportpakets aufgrund konstruktiver oder inhaltlicher Fehler nicht erfolgreich importiert werden können. Eventuell schon importierte Elemente desselben Exportpakets MÜSSEN im Falle eines Abbruchs entfernt werden.**[<=]**

Hinweis: Das exportierende Aktensystem wird über den Abbruch durch ein `abort` an der Schnittstelle informiert.
Hinweis: Eine zum Zeitpunkt des Imports eines Exportpaktes zeitlich nicht mehr gültige Befugnis aus dem Exportpaket ist kein Fehler im Sinne der Anforderung und führt nicht zu einem Abbruch. Das importierende Aktensystem kann eine solche Befugnis ignorieren.

A_21548-02 -Health Record Relocation Service - Information der Vertreter über Bezeichner des neuen Abieters nach Abschluss des Anbieterwechsels
Der Health Record Relocation Service MUSS sicherstellen, dass alle Vertreter nach erfolgreichem Import aller Exportpakete und somit Abschluss der Verschiebung der Akte über Anbieterwechsel und den Bezeichner des neuen Anbieters des Versicherten informiert werden, so dass sie in der Lage sind, die erforderliche initiale Anmeldung durchzuführen und informiert sind, welche Art von personenbezogenen Daten vom Vertreter im Rahmen der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine Vertreterberechtigung widerrufen kann und gegenüber wem er seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann.**[<=]**

Hinweis 1 zu A_21548-: Für die Benachrichtigung derjenigen Vertreter, die dem importierenden Aktensystem nicht bekannt sind, werden die E-Mail-Adressen aus dem Exportpaket genommen. Für die Benachrichtigung der Vertreter, die dem importierenden Aktensystem bekannt sind, wird die im importierenden Aktensystem hinterlegte E-Mail-Adresse des Vertreters verwendet.*

Hinweis 2 zu A_21548-: Der Bezeichner des neuen Anbieters muss dem Wert entsprechen der durch die Operation getProviderList geliefert wird.*

A_26257 -Health Record Relocation Service - Löschen der im Exportpaket enthaltenen E-Mail-Adressen der Vertreter
Der Health Record Relocation Service MUSS sicherstellen, dass die im Exportpaket enthaltenen E-Mail-Adressen von Vertretern ausschließlich zur Information der Vertreter gemäß A_21548-* genutzt werden und nach Abschluss des Anbieterwechsels im importierenden Aktensystem gelöscht werden, d.h. nicht im importierenden Aktensystem gespeichert werden.**[<=]**

A_24788 -Health Record Relocation Service - Löschen des Exportpakets nach Umzug des Aktenkontos
Das Aktensystem MUSS sicherstellen, dass ein vorhandenes Exportpaket nach einem erfolgreichen Transfer eines Aktenkontos eines Versicherten von einem Anbieter zu einem anderen Anbieter gelöscht wird.**[<=]**

3.1.5 Anlage einer Akte bei Rücknahme eines Widerspruchs gegen die ePA

Besteht für einen Versicherten ein Aktenkonto mit einem Widerspruch und wird dieser Widerspruch zurückgenommen, so muss der zuständige Kostenträger für diesen Versicherten eine Akte im Aktenkonto anlegen.

Dafür stellt der Kostenträger die selbst-signierten Befugnisse für sich und die Ombudsstelle bereit, der Widerspruch wird im Aktenkonto gelöscht und die Akte wird initialisiert. Nach erfolgreicher Initialisierung geht der Status der Akte nach Activated über und die Akte ist in der Versorgung nutzbar.

A_30390 -Account Management - Anlage einer Akte in einem bestehenden Aktenkonto
Das Account Management MUSS bei der Anlage einer Akte in einem Aktenkonto den bestehenden Widerspruch löschen, die Befugnisse für den zuständigen Kostenträger und die Ombudsstelle übernehmen, die Akte initialisieren und nachfolgend die Akte in den Status ACTIVATED setzen.**[<=]**

3.1.6 Lebenszyklus und Zustände einer Akte

Eine Akte 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 3: Zustandswechsel im Lebenszyklus einer Akte

Zustand	Erläuterung	zulässige Transitionen	Folgezustand
UNKNOWN	Für einen Versicherten existiert keine Akte.	Akte initialisieren	INITIALIZED
INITIALIZED	Eine neue Akte ist konfiguriert und für eine Aktivierung vorbereitet. Die initialen Befugnisse sind erstellt. Eine Nutzung der Akte im Versorgungsprozess und die Nutzung medizinischer Dokumente ist jedoch erst nach der Aktivierung möglich.Die Daten einer existierenden Akte werden importiert.	Widerspruch gegen die Nutzung der ePA	UNKNOWN
		Explizite Aktivierung des Kontos durch das ePA-Aktensystem. Bei existierender Akte bei einem anderen Anbieter erfolgt die Aktivierung erst nach einem Import der Daten der Akte.	ACTIVATED
		Der Status konnte nicht auf ACTIVATED gewechselt werden, da eine weitere aktivierte Akte gefunden wurde.	INACCESSIBLE

ACTIVATED	Die Akte ist aktiv und kann von befugten Nutzern und Nutzergruppen im Versorgungsprozess verwendet werden.	Vorbereitung des Umzugs der Akte zu einem anderen Anbieter (Erstellung des Exportpakets)	SUSPENDED
		Widerspruch gegen die Nutzung der ePA	UNKNOWN
		Die Akte soll aus Wartungsgründen nicht durch befugte Nutzer und Nutzergruppen verwendet werden	INACCESSIBLE
SUSPENDED	Die Daten der Akte des Versicherten werden zu einem neuen Anbieter übertragen.Die Nutzung der Akte ist in diesem Zustand nicht möglich.	Erfolgreicher Abschluss des UmzugsWiderspruch gegen die Nutzung der ePA	UNKNOWN
		Der Umzug der Akte wurde abgebrochen.	ACTIVATED
		Der Status konnte nicht auf ACTIVATED gewechselt werden, da eine weitere aktivierte Akte gefunden wurde.	INACCESSIBLE
INACCESSIBLE	Die Akte kann derzeit nicht verwendet werden.Dies kann z. B. der Fall sein, wenn Datenmigrationen bei der Aktualisierung auf eine neuere ePA-Versionen noch nicht durchgeführt werden konnte oder in Verbindung mit Widersprüchen gegen die ePA, bei denen das erforderliche Vertrauensniveau ohne weitere Maßnahmen nicht erreicht wird.	Die Anlässe für diesen Zustand sind entfallen (z.B. Datenmigration wurde erfolgreich durchgeführt)	ACTIVATED
		Widerspruch gegen die Nutzung der ePA	UNKNOWN
		Der Status konnte nicht auf ACTIVATED gewechselt werden, da eine weitere aktivierte Akte gefunden wurde.	INACCESSIBLE

A_28686 -Prüfung vor Wechsel in den Status ACTIVATED
Das ePA-Aktensystem MUSS unmittelbar vor dem Wechsel in den Status ACTIVATED prüfen, ob bei einem anderen ePA-Aktensystem für die verwendete KVNR schon ein Aktenkonto im Status ACTIVATED vorliegt und im Fall des Fundes eines solchen Aktenkontos den Statuswechsel abbrechen, den Status INACCESSIBLE mit der Ursache "fehlgeschlagener Statuswechsel ACTIVATED" setzen und die Situation durch den Anbieter oder Betreiber des ePA-Aktensystems auflösen lassen.**[<=]**

A_24369-02 -ePA-Aktensystem - Initialisierung einer Akte
Das 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
- MHD Service
- Patient Service
- EHR Information Service

vor der Aktivierung einer Akte durchführen. Die genannten Bestandteile MÜSSEN nach der Aktivierung der Akte sofort nutzbar sein.**[<=]**

3.1.7 Akte ist zeitweise nicht nutzbar

Während der aktiven Nutzung einer Akte kann es zu Problemen kommen, bei der die Nutzung temporär nicht möglich ist und Maßnahmen ergriffen werden müssen, um eine Akte zu reparieren oder wieder nutzbar zu machen. In diesem Fall setzt das Aktensystem die Akte in den Aktenstatus INACCESSIBLE und weist im betrieblichen Log auf das Problem und seine Ursache hin. Zusätzlich wird die Ursache für den Statuswechsel gespeichert. Es ist auch möglich, dass im Aktenstatus INACCESSIBLE weitere Ursachen ergänzt werden, die für eine Beibehaltung des Aktenstatus sorgen. Der Anbieter oder Betreiber kann nun Maßnahmen ergreifen, um die Ursachen zu adressieren. Adressierte Ursachen werden gelöscht. Nachdem alle Ursachen gelöscht wurden, wird die Akte wieder in den Aktenstatus ACTIVATED gesetzt. Damit wird ermöglicht, dass die ergriffenen Maßnahmen bei der nächsten Nutzung der Akte auf die Daten des Aktenkontos wirken können.

HINWEIS: Der Aktenstatus wird nicht aufgrund temporärer betrieblicher Probleme (z.B. Datenbank nicht erreichbar) gewechselt sondern nur, wenn explizite Maßnahmen für diese spezifische Akte ergriffen werden müssen, die einige Zeit in Anspruch nehmen. Temporäre betrieblich Probleme werden über die entsprechenden Fehlercodes ggü. dem Client signalisiert, welche dann zu einem erneuten Versuch zu einem späteren Zeitpunkt führen.

HINWEIS: Sollte in der Spezifikation im Zusammenhang mit dem STATUS INACCESSIBLE eine konkrete Ursache benannt sein, dann ist dies immer als eine semantische Ursache zu verstehen und muss nicht über den genannten Wortlaut im Produkt repräsentiert werden.

A_28493-01 -ePA-Aktensystem – Verwaltung der Deaktivierung einer Akte durch Aktensystem
Das ePA-Aktensystem KANN eine Akte in den Aktenstatus *INACCESSIBLE* versetzen bzw. für eine Akte im Zustand *INACCESIBLE* weitere Ursachen für den Verbleib im Aktenstatus *INACCESSIBLE* ergänzen oder Ursachen, die durch das Aktensystem behoben sind löschen. Die Ursache des Statuswechsel wird in der Akte gespeichert.
[<=]

A_28494-01 -ePA-Aktensystem – Verwaltung der Deaktivierung einer Akte durch Anbieter
Der Anbieter des ePA-Aktensystems KANN eine Akte in den Aktenstatus *INACCESSIBLE* versetzen bzw. für eine Akte im Zustand *INACCESIBLE* weitere Ursachen für den Verbleib im Aktenstatus *INACCESSIBLE* ergänzen oder Ursachen die behoben sind löschen.
[<=]

A_28495-01 -ePA-Aktensystem – Reaktivierung einer Akte
Das ePA-Aktensystem MUSS bei einer Akte im Aktenstatus *INACCESSIBLE,* bei dem keine Ursache mehr für den Aktenstatus vorliegt, in den Aktenstatus ACTIVATED wechseln.
[<=]

A_28496-01 -ePA-Aktensystem – Optionale Schnittstelle zur Aktualisierung
Das ePA-Aktensystem KANN eine Schnittstelle für Kostenträger anbieten, über die der zuständige Kostenträger eine Akte zur Verarbeitung in die VAU laden kann, damit das ePA-Aktensystem Daten der Akte korrigieren kann.
[<=]

A_28497-01 -ePA-Aktensystem – Abgrenzung der optionalen Schnittstelle zur Aktualisierung
Das ePA Aktensystem MUSS sicherstellen, dass die optionale Schnittstelle gemäß A_28496-*

- ausschließlich durch Kostenträger nutzbar ist,
- keine fachlichen Eingangs- oder Ausgangsparameter besitzt,
- ausschließlich technische Operationen zur Korrektur oder Aktualisierung einer Akte auslösen kann.

[<=]

HINWEIS: Die Schnittstelle dient zum Öffnen einer Akte zu einem vom Kostenträger wählbaren Zeitpunkt, um im Aktensystem implementierte technische Operationen zur Korrektur oder Aktualisierung einer Akte automatisch auszuführen, deren Ausführung eine geöffnete Akte benötigen. Die technischen Operationen sind durch das Aktensystem festgelegt, d.h. der Kostenträger hat keine Möglichkeit die Operationen über die optionale Schnittstelle selbst zu steuern oder zu beeinflussen.

3.1.8 Aktenzusammenführung (Health Record Merge)

Die Zusammenführung von zwei Akten desselber Versicherten aus verschiedenen Aktenkonten erfolgt genauso, wie die Verschiebung einer Akte. Sie unterscheiden sich nur darin, dass die Akte im Aktenkonto der abgebenden Seite einen anderen Status haben muss und der Health Record Relocation Service auf der aufnehmenden Seite die Daten aus den zwei beteiligten Akten gemäß festgelegter Regeln zusammenführen muss.

A_28412-01 -Health Record Relocation Service - Regeln für eine Zusammenführung
Der Health Record Relocation Service des neuen (importierenden) Aktensystems MUSS bei der Zusammenführung zweier Akten für Objekte `obj_export` im zu importierenden Exportpaket die folgenden Regeln umsetzen:

Daten im Exportpaket	Regel für die Zusammenführung

XDS Document Service `obj_export` = Replace-Kette bestehend aus 1...n Dokumenten (n>= 1) `obj_export[1]` bezeichnet das aktuellste Dokument der Kette	Bemerkung; ein Dokument `obj` ist im Aktensystem*vorhanden*, falls es ein Dokument `obj'` im Aktensystem mit selber entryUUID, uniqueID oder selbem Hash-Wert gibt. **wenn** im importierenden AS kein Dokument von `obj_export` vorhanden ist, **dann** ergänze `obj_export` **wenn** im importierenden AS mindestens ein Dokument von**`obj_export`** vorhanden ist und das aktuellste Dokument `obj_export[1]` ist nicht vorhanden, **dann** ergänze `obj_export[1]`und verwerfe den Rest der Kette`obj_export[2..n]`, **sonst** verwerfe `obj_export`
XDS Document Service `obj_export` = Unique-Dokument (z.B. NFD, DPE)	**wenn** im importierenden AS das Unique-Dokument `obj_export` nicht vorhanden ist, **dann** ergänze `obj_export` **sonst** verwerfe `obj_export`
XDS Document Service `obj_export` = dynamischer Folder	Bemerkung; ein Folder`obj` ist im Aktensystem*vorhanden*, falls es einen Folder`obj'` im Aktensystem mit dem selbem Foldertitel gibt. **wenn** im importierenden AS der Folder `obj_export` nicht vorhanden ist, **dann** 1. ergänze `obj_export` und 2. generiere für `obj_export` eine neue entryUUID bzw. neue uniqueId, falls die entryUUID bzw. uniqeId von`obj_export` bereits im importierenden AS existieren. **wenn** im importierenden AS der Folder**`obj_export`**vorhanden ist und SubmissionSet.submissionTime von**`obj_export`** älter als das SubmissionSet.submissionTime des vorhandenen Folders ist,**dann** übernimmSubmissionSet.submissionTimevon **`obj_export`** für den vorhandenen Folder **sonst** verwerfe `obj_export`
XDS Document Service `obj_export` = Anhangs-Graph bestehend aus 1...n Dokumenten (n>= 1)	**wenn**im importierenden AS kein Dokument von `obj_export` vorhanden ist,**dann ergänze** `obj_export` **wenn** im importierenden AS mindestens ein Dokument von **`obj_export`** vorhanden ist, **dann** 1. entferne alle APND-Assoziationen zwischen den Dokumenten aus**`obj_export`** und 2. ergänze ein Dokument von**`obj_export`** im importierenden AS, falls das Dokument im

	importierenden AS nicht vorhanden ist.
Patient Service `obj_export = FHIR-Datum`	*Es erfolgt keine Zusammenführung durch das Aktensystem.*

Consent Decision Management
`obj_export = ConsentDecision,`
`obj_export = DataUsagePurpose`
	wenn das importierende AS die Art des Widerspruchs unterstützt, **und**
	das Änderungsdatum des existierenden Objekts älter ist,
	dann übernehme`obj_export`,
	sonst verwerfe `obj_export`

Consent Decision Management `obj_export = Eintrag in der User-specific deny Policy Medication`	**wenn** `obj_export` im importierenden AS nicht vorhanden ist, **dann** ergänze `obj_export`, **sonst** verwerfe `obj_expor`
Entitlement Management `obj_export = Eintrag auf der Blocked User Policy`	**wenn** `obj_export` im importierenden AS nicht vorhanden ist, **dann** ergänze `obj_export` und lösche eine ggf. vorhandene Befugnis für die in`obj_export` identifzierte LEI, **sonst** verwerfe `obj_export`
Entitlement Management `obj_export = Befugnis`	**wenn** `obj_export` = Vertreter-Befugnis und `obj_export` im importierenden AS nicht vorhanden ist, **dann** ergänze `obj_export`, **sonst** verwerfe `obj_export`
Constraint Management `obj_export = Eintrag in General Deny Policy`	**wenn** `obj_export` im importierenden AS nicht vorhanden ist (nach Import aller Dokumente aus dem Export-Paket) und das in`obj_export` referenzierte Objekt im importierenden AS vorhanden ist, **dann** ergänze `obj_export`, **sonst** verwerfe `obj_export`
Audit Event Service `obj_export = Protokolleintrag`	**wenn** `obj_export` im importierenden AS nicht vorhanden ist, **dann** ergänze `obj_export` mit folgender Erweiterung in entyity.detail mit entity.detail.type="System-Zusammenführung" und entity.detail.value[x]= true, **sonst** verwerfe `obj_export`
E-Mail Management `obj_export = E-Mail-Adresse`	*Es erfolgt keine Zusammenführung durch das Aktensystem.*

[<=]

A_28414 -ePA-Aktensystem – Information des Versicherten über Zusammenführung durch Anbieter

Der Anbieter des ePA-Aktensystems MUSS den Versicherten über eine anstehende Zusammenführung seiner Akte informieren, sofern durch die Zusammenführung ein Zustand der Akte enstehen könnte, den der Versicherte überprüfen sollte.**[<=]**

Hinweis zu A_28414-*: In der Kommunikation mit den Versicherten kann der Anbieter eine eigene Sprachregelung wählen, es muss gegenüber dem Versicherten nicht von einer "Zusammenführung" gesprochen werden.

A_28415 -Health Record Relocation Service – Information des Versicherten über Zusammenführung per Mail
Falls der Versicherte eine E-Mail-Adresse im neuen (importierenden) Aktensystem hinterlegt hat oder eine E-Mail-Adresse des Versicherten im Export-Paket vorhanden ist, MUSS der Health Record Relocation Service bei der Operation startPackageMergeImport eine E-Mail an alle bekannten E-Mail-Adressen des Versicherten mit folgenden Hinweisen senden:

- Information über die Tatsache der Zusammenführung,
- ggf. Information, dass sich durch die Zusammenführung Daten oder Einstellungen in der Akte geändert haben und diese Änderungen in den Protokollen nachvollzogen werden können,
- ggf. könnten Protokolle durch die Zusammenführung inkonistent wirken.

[<=]

3.1.8.1 Zusammenführung der Ressourcen des Medication Service

Es erfolgt keine einfache Zusammenführung fehlender Daten des Medication Service aufgrund der komplexen Beziehungen der enthaltenen FHIR-Ressourcen untereinander zur Abbildung der Sichten "elektronische Medikationsliste (eML)" und "elektronischer Medikationsplan (eMP)" mit zeitlichem Zusammenhang. Stattdessen werden die eML-relevanten Ressourcen mit dem Ziel einer vollständigen eML in der weiterzuführenden Akte zusammengestellt. Vorhandene eMP-Ressourcen werden gelöscht, wenn durch die Zusammenführung von Ressourcen Anpassungen an eMP-Ressourcen erforderlich werden oder eMP-Ressourcen zusammengeführt werden müssten. Ein eMP ist dann in der weiterzuführenden Akte nicht mehr vorhanden.

Die eML-Ressourcen sind Ressourcen auf Basis der Profile `EPAMedication`, `EPAMedicationStatement`, `EPAMedicationRequest` und `EPAMedicationDispense`, sowie `OrganizationDirectory`, `PractitionerDirectory`, `PractitionerRole` und `EPAActivityProvenance`(Änderungseintrag eML), inklusive aller enthaltenen Daten.

Die eMP-Ressourcen sind Ressourcen auf Basis der Profile `EMPMedication` und `EMPMedicationRequest`, sowie `EMPChronologyProvenance`, `TIOrganization` und `EPAActivityProvenance`(Änderungseintrag eMP), inklusive aller enthaltenen Daten.

Sind im Zuge der Zusammenführung oder der vereinfachten Auswahl des Datenbestandes für die weiterzuführende Akte Ressourcen aus der weiterzuführenden Akte zu löschen, dann werden diese vollständig entfernt (kein "logisches" Löschen).

3.1.8.1.1 Keine Zusammenführung bei Widerspruch

Die Zusammenführung von Daten des Medication Service entfällt, wenn der resultierende Datenbestand des Consent Decision Managements der zusammengeführten Akte einen Widerspruch gegen die Funktion 'erp-submission' aufweist und die Daten des Medication Service gelöscht sein müssen. In diesem Fall sind auch alle Daten des Medication Service in der weiterzuführenden Akte zu löschen.

3.1.8.1.2 Sonderfall exklusive Nutzung einer der beiden Akten

Eine Zusammenführung der Daten entfällt auch, wenn es keinerlei Verteilung der Ressourcen über die doppelten Akten gibt, also Änderungen am Datenbestand des Medication Service lediglich in einer der Akten vorgenommen wurden. Falls diese Änderungen nicht in der weiterzuführenden Akte enthalten sind, erfolgt die einfache Übertragung der Ressourcen des Medication Service in diese Akte.

Dieser Fall liegt vor, wenn der Datenbestand (des Medication Service) der einen Akte schon vollständig im Datenbestand der anderen Akte vorhanden ist. Der Datenbestand mit der größeren Anzahl Ressourcen ist dann der weiterzuführende. Für den Vergleich sind alle Versionen aller Ressourcen des Datenbestands zu berücksichtigen.

Die Bewertung der Datenbestände bezüglich Änderung und Abweichung kann dabei auf ein zeitliches Intervall eingegrenzt werden, wenn ein Zeitpunkt der Separation (Relocation) der beiden Akten existiert und bekannt ist und vor diesem Zeitpunkt die Datenbestände der beiden Akten identisch sind.

A_30421 -Health Record Relocation Service - Auswahl des Datenbestands des Medication Service für die weitere Nutzung bei nicht verteilten Ressourcen
Wenn Ressourcen des Medication Service einer Akte bei einer anstehenden Zusammenführung von Ressourcen des Medication Service vollständig im Datenbestand der anderen Akte enthalten sind, dann MUSS der Health Record Relocation Service den Datenbestand der enthaltenden Akte vollständig im Medication Service der weiterzuführenden Akte verfügbar machen.**[<=]**

3.1.8.1.3 Zusammenführung verteilter Ressourcen

Sind eML-Ressourcen zusammenzuführen, dann werden bisher nicht vorhandene Ressourcen und Versionen von Ressourcen in die weiterzuführende Akte übertragen. Der Übertrag von Unikat-Ressourcen entfällt, wenn bereits eine inhaltsgleiche Ressource in der weiterzuführenden Akte existiert. In diesem Fall werden Referenzen in übertragenen Ressourcen angepasst, wenn sie auf diese Unikate referenzieren.

A_30422 -Health Record Relocation Service -Zusammenführung von Ressourcen und Ressourcenversionen des Medication Service
Der Health Record Relocation Service MUSS bei einer Zusammenführung von Ressourcen des Medication Service die Ressourcen der Profile`EPAMedication`, `EPAMedicationStatement`, `EPAMedicationRequest`, `EPAMedicationDispense` und `EPAActivityProvenance` (Änderungseintrag eML), inklusive aller Inhalte und mit allen Versionen in die weiterführende Akte übertragen, wenn diese dort nicht vorhanden sind oder weniger Versionen aufweisen.**[<=]**

A_30423 -Health Record Relocation Service -Zusammenführung von Unikat-Ressourcen des Medication Service
Der Health Record Relocation Service MUSS bei einer Zusammenführung von Ressourcen des Medication Service die Ressourcen der Profile`PractitionerDirectory`, `OrganizationDirectory` und `PractitionerRole` der eML in die weiterzuführende Akte übertragen, wenn es dort keine dieser Unikat-Ressourcen mit gleichem Inhalt gibt.
Der Health Record Relocation Service MUSS die Übertragung dieser Ressourcen unterlassen, wenn es in der weiterzuführenden Akte bereits Ressourcen mit gleichem Inhalt gibt. Referenzen auf die nicht übertragenen Unikat-Ressourcen in den übertragenen weiteren Ressourcen des Medication Service MÜSSEN in Referenzen auf die im Bestand vorhandenen Ressourcen geändert werden.
Zwei Ressourcen des Profils `PractitionerDirectory` oder `OrganizationDirectory` sind

gleichen Inhalts, wenn die enthaltene Telematik-ID übereinstimmt.
Zwei Ressourcen des Profils `PractitionerRole` sind gleichen Inhalts, wenn in den referenzierten Ressourcen `PractitionerDirectory` und `OrganizationDirectory` jeweils die Telematik-ID übereinstimmt.**[<=]**

Hinweis: Die Anpassung einer Referenz auf eine schon vorhandene Unikat-Ressource erfordert keine neuen Versionen von Ressourcen und keine Anlage einer EPAActivityProvenance.

Wenn durch die Zusammenführung von eML-Ressourcen eine Anpassung von im Bestand vorhandenen eMP-Ressourcen erforderlich würde (Erstellen von Verknüpfungen eML-eMP) oder in beiden Akten eMP-Ressourcen angelegt oder verändert wurden (simultanes Kuratieren des eMP), dann wird der eMP, bzw. werden die eMP-Ressourcen, in der weiterzuführenden Akte entfernt und keine eMP-Ressourcen in diese Akte übertragen.

A_30424 -Health Record Relocation Service - Löschen des eMP bei Zusammenführung von Ressourcen
Der Health Record Relocation Service MUSS bei einer Zusammenführung von Ressourcen des Medication Service die Ressourcen des eMP (`EMPMedication`, `EMPMedicationRequest`, `EMPChronologyProvenance`, `TIOrganization` und `EPAActivityProvenance` (Änderungseintrag eMP) in der weiterzuführenden Akte löschen, wenn:

- in beiden Akten eMP-Einträge erstellt oder geändert wurden, oder
- in der weiterzuführenden Akte nach einer Zusammenführung von eML-Einträgen zur Erstellung eines konsistenten Datenbestands Änderungen an existierenden eMP-Ressourcen erforderlich werden.

[<=]

A_30425 -Health Record Relocation Service - Löschen von eML-eMP Verknüpfungen
Der Health Record Relocation Service MUSS bei einer Zusammenführung von Ressourcen des Medication Service alle eML-eMP-Verknüpfungen aus den eML-Ressourcen der weiterzuführenden Akte löschen, wenn eMP-Ressourcen dieser Akte entfernt wurden.
Der Health Record Relocation Service MUSS alle Extensions der Indikation "LINKING_NOT_SUCCESFULL" aus den`EPAMedicationStatements` entfernen.
Für jede Änderung an Ressourcen des Profils `EPAMedicationStatement` MUSS eine Ressource `EPAActivityProvenance` mit ausführendem Dienst 'MEDICATIONSVC' erzeugt werden.**[<=]**

Hinweis: Eine eML-eMP-Verknüpfung wird vollständig entfernt, der Inhalt von based0n der Ressourcen `EPAMedicationStatement` und `EPAMedicationRequest` wird dazu gelöscht.

Hinweis: Diese Änderungen sind durch die Zusammenführung der Ressourcen bedingte Korrekturen und stellen keine Änderung eines eML-Eintrags dar. Eine gesonderte Protokollierung ist nicht erforderlich.

Durch die Zusammenführung können Daten des eMP verloren gehen. Dieses können sowohl eMP-Einträge aus dem Bestand der weiterzuführenden Akte, als auch aus der anderen Akte sein. Zur Information und weiteren Verwendung durch den Versicherten wird daher jeweils ein aktueller Medikationsplan der Akten in gerenderter Form im Format PDF/A als Dokument in der Akte des Versicherten abgelegt.

Durch die Zusammenführung wird die eML in der weiterzuführenden Akte um Einträge erweitert. Zur Information und weiteren Verwendung durch den Versicherten wird daher jeweils eine aktuelle Medikationsliste der Akten in gerenderter Form im Format PDF/A als

Dokument in der Akte des Versicherten abgelegt. Diese Dokumente geben den Zustand vor der Zusammenführung von eML-Einträgen wieder.

A_30426 -Health Record Relocation Service - Archivierung der Daten des Medication Service als Dokument
Der Health Record Relocation Service MUSS bei einer Zusammenführung von Ressourcen des Medication Service jeweils ein Dokument für beide Akten im Format PDF/A für den letzten Zustand des eMP und der eML des Medication Service erstellen und in der weiterzuführenden Akte des Versicherten ablegen und die Ablage der Dokumente protokollieren. Die Dokumente MÜSSEN den Vorgaben für Dokumente im Format PDF/A bei Abruf über die Render API "Medikationsplan abrufen (eMP)", bzw. "Medikationsliste abrufen (eML), entsprechen. Der Abruf der Dokumente MUSS nicht protokolliert werden. Für die Dokumente gilt:

- Ablage im Ordner "`patient`" des XDS Document Service
- DocumentEntry.title =
  - eMP der weiterzuführenden Akte: "Medikationsplanung vor Löschung durch Aktenzusammenführung - KEIN GÜLTIGER MEDIKATIONSPLAN!"
  - eMP der anderen Akte: "Gelöschte Medikationsplanung der Akte <Kostenträgername> aus Aktenzusammenführung - KEIN GÜLTIGER MEDIKATIONSPLAN!"
  - eML der weiterzuführenden Akte: "Medikationsliste vor Aktenzusammenführung - KEINE GÜLTIGE MEDIAKTIOSNLISTE!"
  - eML der anderen Akte: "Übernommene Medikationsliste der Akte <Kostenträgername> aus Aktenzusammenführung - KEINE GÜLTIGE MEDIAKTIOSNLISTE!
- mimetype = "application/pdf"
- formatCode = "`urn:ihe:iti:xds:2017:mimeTypeSufficient`

[<=]

Hinweis: Die Ablage der Dokumente ist gemäß der Vorgaben aus IG-EPA89078Y44- zu protokollieren.*

Hinweis: Dokumente müssen nicht erstellt werden, wenn diese keine Einträge enthalten ("empty list").

Hinweis: Die Dokumente für Daten der nicht weitergeführten Akte (der "anderen" Akte) können durch diese erstellt und als Bestandteil des Exportpaktes übertragen werden.

A_30427 -Health Record Relocation Service - Protokollierung der Zusammenführung des Datenbestands des Medication Service in eine Akte
Der Health Record Relocation Service MUSS die Zusammenführung von Ressourcen in die weiterzuführende Akte des Versicherten protokollieren. Die Protokollierung MUSS folgende Aktionen berücksichtigen, wenn diese angewendet wurden:

- Löschen des eMP in der weiterzuführenden Akte,
- Übertragung von eML-Ressourcen in die weiterzuführende Akte.

[<=]

Hinweis: Die Protokollierung erfolgt gemäß IG-EPA83763PTC-.*

A_30428 -Health Record Relocation Service - Validierung der Änderungen

Der Health Record Relocation Service MUSS in der weiterzuführenden Akte überprüfen, dass die Änderungen zu

- Löschen des eMP
- Löschen von Referenzen für eML-eMP-Verknüpfunge
- Löschen von Extensions
- Ergänzen von Ressourcen, Ressourcenversionen
- Korrektur von Referenzen auf Unikat-Ressourcen

technisch konsistent und korrekt umgesetzt wurden und der resultierende Datenbestand durch die Operationen des Medication Service erfolgreich nutzbar ist.**[<=]**

3.1.8.1.4 Vereinfachte Auswahl eines Datenbestands (Fallback-Lösung)

In Ausnahmefällen kann die Zusammenführung der Daten des Medication Service aus technischen Gründen fehlschlagen. Eine Ursache können beispielsweise simultan veränderte Versionen einer Ressource sein: in beiden Akten gibt es die Ressource "abc" in der Version "x", aber "abc.x" der Akte 1 ist ungleich "abc.x" der Akte 2, oder nicht validier- und korrigierbare Endzustände des weiterzuführenden Datenbestands.

In solchen Fällen, wenn die technische Stabilität nicht herstellbar ist - wird auf die Zusammenführung von Ressourcen verzichtet. Stattdessen wird der Datenbestand des Medication Service einer der beiden Akten vollständig in der weiterzuführenden Akte verfügbar gemacht. Abhängig von der Verteilung der eMP- und eML-Ressourcen gehen dadurch Teile des eMP und/oder der eML verloren, zugunsten eines technisch validen Datenbestands, welcher für die weitere Nutzung durch Clientsysteme geeignet ist.

Der Anteil des eMP im ausgewählten Datenbestand für die weiterzuführende Akte - so vorhanden - bleibt dabei erhalten.

Für die Auswahl des weiterzuführenden Datenbestands wird die größere Anzahl eML-Einträge favorisiert.

A_30429 -Health Record Relocation Service - Auswahl des Datenbestands bei vereinfachter Auswahl (Fallback-Lösung)
Der Health Record Relocation Service MUSS bei der Anwendung der vereinfachten Auswahl des weiterzuführenden Datenbestands des Medication Service diese Auswahl aufgrund der Anzahl der aktuell vorhandenen Ressourcen des Medication Service treffen. Die Anzahl wird für beide Akten getrennt ermittelt. Für die Berechnung gilt:

- Ressourcen des Profils `EPAMedicationStatement` gehen als Repräsentation eines eML-Eintrags in die Berechnung ein.
- Andere Ressourcen werden nicht gezählt
- Eine Ressource mit mehreren Versionen wird als eine Ressource gezählt

Der Health Record Relocation Service MUSS den Datenbestand mit der größeren Anzahl als Datenbestand für die weiterzuführende Akte auswählen. Bei gleicher Anzahl wird der aktuelle Datenbestand der weiterzuführenden Akte gewählt.

Der Health Record Relocation Service MUSS sicherstellen, dass die weiterzuführende Akte genau den ausgewählten Datenbestand vollständig enthält**[<=]**

Hinweis: Ein gemäß der Beschreibung in Kapitel 3.2.3.1.2 "Sonderfall exklusive Nutzung einer der beiden Akten" festgestellter Zeitpunkt der Separation kann auch hier zur Einschränkung der relevanten Ressourcenmenge angewendet werden.

Durch die vereinfachte Auswahl geht der Datenbestand einer Akte verloren. Zur Information und weiteren Verwendung durch den Versicherten wird daher jeweils eine aktuelle Medikationsliste und ein aktueller Medikationsplan in gerenderter Form im Format PDF/A als Dokument in der Akte des Versicherten abgelegt. Diese Dokumente geben den Zustand des nicht weitergeführten Datenbestandes wieder. Für den weiterzuführenden Datenbestand entfällt die Erstellung dieser Dokumente.

A_30430 -Health Record Relocation Service - Archivierung der Daten des Medication Service als Dokument bei vereinfachter Auswahl (Fallback-Lösung)
Der Health Record Relocation Service MUSS jeweils ein Dokument für den nicht weiterzuführenden Datenbestand im Format PDF/A für den letzten Zustand des eMP und der eML des Medication Service erstellen und in der weiterzuführenden Akte des Versicherten ablegen und die Ablage der Dokumente protokollieren. Die Dokumente MÜSSEN den Vorgaben für Dokumente im Format PDF/A bei Abruf über die Render API "Medikationsplan abrufen (eMP)", bzw. "Medikationsliste abrufen (eML), entsprechen. Der Abruf der Dokumente MUSS nicht protokolliert werden.
Für die Dokumente gilt:

- Ablage im Ordner "`patient`" des XDS Document Service
- DocumentEntry.title =
  - eMP: "Gelöschte Medikationsplanung aus Aktenzusammenführung - KEIN GÜLTIGER MEDIKATIONSPLAN!"
  - eML: "Gelöschte Medikationsliste aus Aktenzusammenführung - KEINE GÜLTIGE MEDIKATIONSLISTE!"
- mimetype = "application/pdf"
- formatCode = "`urn:ihe:iti:xds:2017:mimeTypeSufficient`"

[<=]

Hinweis: Die Ablage der Dokumente ist gemäß der Vorgaben aus IG-EPA89078Y44- zu protokollieren.*

Hinweis: Dokumente müssen nicht erstellt werden, wenn diese keine Einträge enthalten ("empty list").

3.2 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] werden von den VSDM-Betreibern erzeugt und für die ePA-VAUs der ePA-Betreiber verschlüsselt exportiert. Die Schlüssel sowie die Export-/Import-Vorgänge (Mehr-Augen-Prinzip) sind die gleichen wie sie auch für die E-Rezept-VAU verwendet werden.

A_24611-10 -ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und Informationen für VAU-Betrieb

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

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU (u.a. genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Paare (kid, C.ZD.SIG) für die Zertifikate C.ZD.SIG mit professionOID `oid_popp-token` für die aktuelle Token-Signatur-Identität des PoPP-Services und ggf. die vorherige Token-Signatur-Identität des PoPP-Services. Der Wert kid für ein Zertifikat C.ZD.SIG ergibt sich aus dem JWK-Set, welches der PoPP-Service veröffentlicht.
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel
- symmetrische Schlüssel für die HMAC-Prüfung der VSDM-Prüfziffern (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Paare (sn, Root-Zertifikat) für das aktuelle und das vorherige (sofern nicht kompromittiert) Root-Zertifikat (Vertrauensanker) für die Prüfung der Signatur von ITSG-Token. Der Identifier sn bezeichnet die Seriennummer des Root-Zertifikats,
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

Hinweis:
Es gelten die Anforderungen aus [gemSpec_Krypt#3.20 VSDM-Prüfziffer Version 2] für ein ePA-Aktensystem in der Rolle "Prüfziffer Version 2 prüfendes System". Aus den ins HSM importierten gemeinsamen Geheimnissen erfolgt im HSM eine Schlüsselableitung (A_27299-*) der für die Entschlüsselung der Prüfziffer Version 2 benötigten AES/GCM-Schlüssel.

Hinweis: Das ITSG-Trust Center veröffentlicht die Root-Zertifikate für die Prüfung von Signaturen der ITSG-Token unter: https://www.itsg.de/produkte/trust-center/oeffentliche-zertifikate-und-verzeichnisse/.

A_26109 -ePA-Aktensystem - Unterschiedliche private Authentisierungsschlüssel für AK-, Befugnisverifikations- und Service-VAU
Das ePA-Aktensystem MUSS sicherstellen, dass für die Authentisierungsidentitäten für Aktenkontoverwaltungs-VAUs, Befugnisverifikations-VAUs und Service-VAUs unterschiedliche private Schlüssel verwendet werden.**[<=]**

A_26110 -ePA-Aktensystem - Unterschiedliche private Authentisierungsschlüssel für unterschiedliche Service-VAUs
Das ePA-Aktensystem MUSS sicherstellen, dass für unterschiedliche Typen von Service-VAUs unterschiedliche private Schlüssel für die Authentisierung genutzt werden.**[<=]**

Hinweis zu A_26110: Ein Typ einer Service-VAU könnte beispielsweise eine PDF-Konvertierungs-Service-VAU oder eine Pseudonymisierungs-Service-VAU für Daten zur Sekundärnutzung sein. Alle Instanzen einer PDF-Konvertierungs-Service-VAU nutzen denselben privaten Authentisierungsschlüssel. Die Instanzen der Pseudonymisierungs-Service-VAU dürfen den Authentisierungsschlüssel der PDF-Konvertierungs-Service-VAU jedoch nicht verwenden.

A_24612-08 -ePA-Aktensystem - Erzwingen von 4-Augen-Prinzip für Einbringen und Verwalten von Informationen ins VAU-HSM
Das ePA-Aktensystem MUSS technisch erzwingen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip in das VAU-HSM eingebracht und verwaltet werden können:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Paare (kid, C.ZD.SIG) für die Zertifikate C.ZD.SIG mit professionOID `oid_popp-token` für die aktuelle Token-Signatur-Identität des PoPP-Services und ggf. die vorherige Token-Signatur-Identität des PoPP-Services. Der Wert kid für ein Zertifikat C.ZD.SIG ergibt sich aus dem JWK-Set, welches der PoPP-Service veröffentlicht.
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Paare (sn, Root-Zertifikat) für das aktuelle und das vorherige (sofern nicht kompromittiert) Root-Zertifikat (Vertrauensanker) für die Prüfung der Signatur von ITSG-Token. Der Identifier sn bezeichnet die Seriennummer des Root-Zertifikat,
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

A_24614-09 -ePA-Aktensystem - Einbringung von Informationen ins VAU-HSM im 4-Augen-Prinzip mit der gematik
Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip ins VAU-HSM eingebracht und im VAU-HSM verwaltet werden, bei dem eine von der gematik benannte Person beteiligt ist:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Paare (kid, C.ZD.SIG) für die Zertifikate C.ZD.SIG mit professionOID `oid_popp-token` für die aktuelle Token-Signatur-Identität des PoPP-Services und ggf. die

vorherige Token-Signatur-Identität des PoPP-Services. Der Wert kid für ein Zertifikat C.ZD.SIG ergibt sich aus dem JWK-Set, welches der PoPP-Service veröffentlicht.

- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Paare (sn, Root-Zertifikat) für das aktuelle und das vorherige (sofern nicht kompromittiert) Root-Zertifikat (Vertrauensanker) für die Prüfung der Signatur von ITSG-Token. Der Identifier sn bezeichnet die Seriennummer des Root-Zertifikat,
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

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

Die von der gematik benannte Person prüft, dass die Zertifikate für die Token-Signatur-Identität des PoPP-Services gültig sind und die geforderten Inhalte enthält (Zertifikatsprofil oid_zd_sig (OID 1.2.276.0.76.4.287, "C.ZD.SIG"), technische Rolle oid_popp-token (OID 1.2.276.0.76.4.320)).

Um einen unterbrechungsfreien Betrieb des ePA-Aktensystems bei Wechsel des Zertifikats der Token-Signatur-Identität des PoPP-Services zu gewährleisten, sind im VAU-HSM im Normalfall zwei Zertifikate für die Token-Signatur-Identität des PoPP-Services hinterlegt, nämlich das aktuelle und das Vorgängerzertifikat. Wechselt der PoPP-Service das Zertifikat aufgrund einer Kompromittierung, muss das kompromittierte Zertifikat aus dem VAU-HSM gelöscht werden. In diesem Fall ist dann nur ein Zertifkat für den PoPP-Service im VAU-HSM gespeichert.

A_29007 -ePA-Aktensystem - Unverzügliches Löschen eines kompromittierten PoPP-Service-Zertifikats aus dem VAU-HSM
Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass ein kompromittiertes Zertifikat C.ZD.SIG mit professionOID `oid_popp-token` für die Token-Signatur-Identität des PoPP-Services unverzüglich aus dem VAU-HSM entfernt wird.**[<=]**

Analog ist ein kompromittiertes Root-Zertifikat für die Prüfung der Signaturen von ITSG-Token unverzüglich aus dem VAU-HSM zu entfernen.

A_30432 -ePA-Aktensystem - Unverzügliches Löschen eines kompromittierten ITSG-Root-Zertifikats aus dem VAU-HSM
Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass ein kompromittiertes Root-Zertifikat für die Prüfung der Signatur von ITSG-Token unverzüglich aus dem VAU-HSM entfernt wird.**[<=]**

A_24618-09 -ePA-Aktensystem - Zugriff auf Schlüssel und Informationen im VAU-HSM
Das ePA-Aktensystem MUSS sicherstellen, dass auf die folgenden, für den Betrieb der VAU notwendigen und im VAU-HSM gespeicherten Schlüssel und Informationen ausschließlich über attestierte VAU-Instanzen zugegriffen werden kann:

- privater Schlüssel der Authentisierungsidentität der VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz

- privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU ausschließlich durch eine Befugnisverifikations-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität eines Service-VAU-Typs ausschließlich durch eine Service-VAU-Instanz dieses Service-VAU-Typs
- privater Schlüssel der Verschlüsselungsidentität der VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Signaturidentität der VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Paare (kid, C.ZD.SIG) für die Zertifikate C.ZD.SIG mit professionOID `oid_popp-token` für die aktuelle Token-Signatur-Identität des PoPP-Services und ggf. die vorherige Token-Signatur-Identität des PoPP-Services. Der Wert kid für ein Zertifikat C.ZD.SIG ergibt sich aus dem JWK-Set, welches der PoPP-Service veröffentlicht.
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüsselausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüsselausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden,ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz.

[<=]

3.3 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-Modul). Das VAU-HSM speichert in Variante 2 neben den Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der Aktenkontoverwaltung zusätzlich auch die Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der Befugnisverifikations-VAU. Ein Zugriff auf das HSM ist dann nur mit einem validen Attestierungstoken für die Aktenkontoverwaltung-VAU und die Befugnisverifikations-VAU möglich.

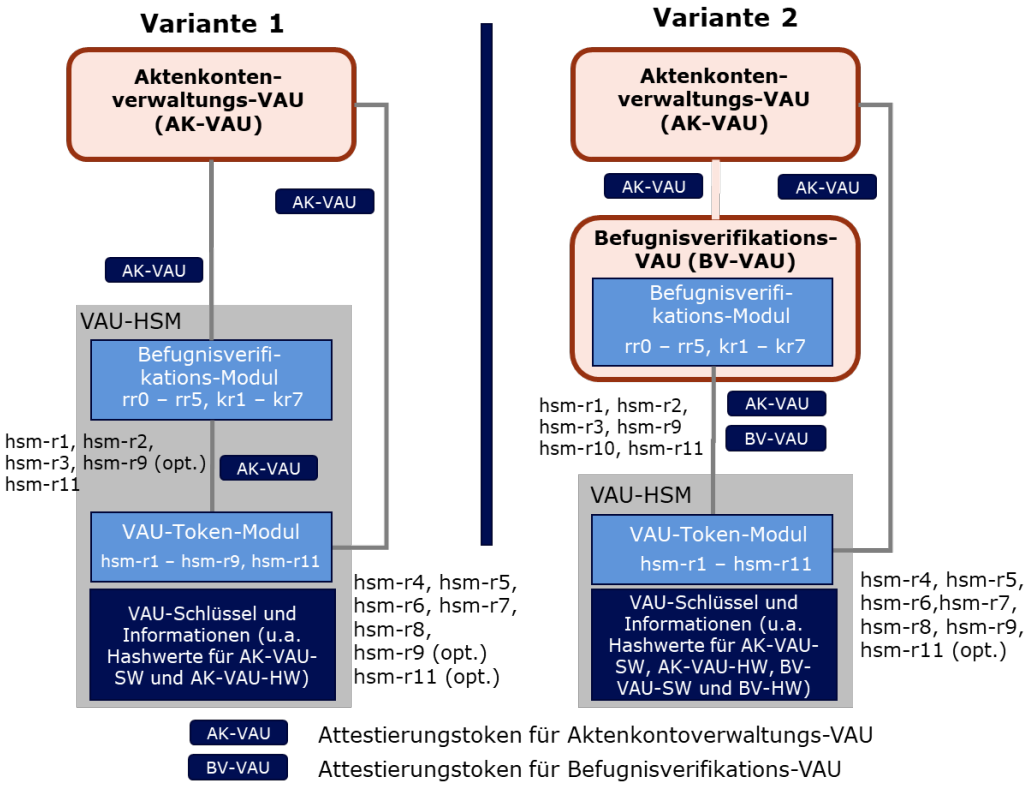


Abbildung 2: Alternativen zur Ausführung des Befugnisverifikations-Moduls

A_25281 -ePA-Aktensystem - VAU-Token-Modul ausschließlich im HSM
Das ePA-Aktensystem MUSS sicherstellen, dass ein VAU-Token-Modul ausschließlich in einem VAU-HSM ausgeführt wird.**[<=]**

A_24574 -ePA-Aktensystem - Befugnisverifikations-Modul im HSM oder Befugnisverifikations-VAU
Das ePA-Aktensystem MUSS sicherstellen, dass ein Befugnisverifikations-Modul ausschließlich in einem VAU-HSM oder in einer Befugnisverifikations-VAU ausgeführt wird. **[<=]**

A_25050 -ePA-Aktensystem - 1:1-Beziehung zwischen Befugnisverifikations-VAU und Aktenkontoverwaltungs-VAU
Das ePA-Aktensystem MUSS sicherstellen, dass eine 1:1-Beziehung zwischen einer Instanz einer Befugnisverifikations-VAU und einer Instanz einer Aktenkontoverwaltungs-VAU gibt.**[<=]**

3.3.1 VAU-Token-Modul

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

A_24712-01 -ePA-Aktensystem - VAU-Token-Modul nur durch Befugnisverifikations-Modul oder Aktenkontoverwaltungs-VAU aufrufbar
Das ePA-Aktensystem MUSS sicherstellen, dass die Regeln hsm-r1 bis hsm-r3 des VAU-Token-Moduls ausschließlich von einem Befugnisverifikations-Modul und die Regeln hsm-r4 bis hsm-r7 ausschließlich von einer Aktenkontoverwaltungs-VAU aufgerufen werden. **[<=]**

A_25282-07 -ePA-Aktensystem - Regeln des VAU-Token-Moduls

Das VAU-Token-Modul MUSS die in Tabelle*Tab_AS_VAU_Token_Modul_Rules-07* definierten Regeln umsetzen.**[<=]**

Tabelle 4: Tab_AS_VAU_Token_Modul_Rules-07 -Prüfregeln VAU Token

Regel	Beschreibung
hsm-r1	*Diese Regel dient zur Sicherung von Befugnissen und HSM-ID-Token mittels CMAC.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (optional) • Daten **Ausgangsdaten**: • Daten 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, werden die übergebenen Daten mittels CMAC gesichert.
hsm-r2	*Diese Regel dient zur Ableitung der versichertenindividuellen Persistierungsschlüssel* **Eingangsdaten**: • KVNR • gewünschte Persistierungsschlüssel [Label für Datenpersistierungs-Masterkey und/oder Label für Befugnispersistierungs-Masterkey] • 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 von den durch die Label identifizierten Masterkeys abgeleitet.

hsm-r3	*Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfziffern der Version 1 oder der Entschlüsselung der VSDM-Prüfziffern der Version 2*
	Eingangsdaten:
	• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU
	• VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)
	• Szenario VSDM-Prüfziffer Version 1
	  • Daten
	  • Bezeichner des HMAC-Schlüssels
	• Szenario VSDM-Prüfziffer Version 2
	  • VSDM-Prüfziffer in Version 2
	Ausgangsdaten:
	• Szenario VSDM-Prüfziffer Version 1: HMAC der Daten mit dem symmetrischen Schlüssel, der zum übergebenen Bezeichner des HMAC-Schlüssels gehört
	• Szenario VSDM-Prüfziffer Version 2: innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) bei erfolgreicher Entschlüsselung
	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. (opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind
	Szenario VSDM-Prüfziffer Version 1: Falls die Prüfungen 1) - 3) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.
	
	Szenario VSDM-Prüfziffer Version 2: Falls die Prüfungen 1) - 3) erfolgreich waren, wird die VSDM-Prüfziffer gemäß den Prüfschritten 4. und 5. aus A_27279-* geprüft und entschlüsselt. Bei erfolgreicher Entschlüsselung der VSDM-Prüfziffer wird die innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) zurückgeliefert, ansonsten ein Fehler.

hsm-r4	*Diese Regel dient zur Nutzung der privaten Schlüssel der AUT-Identitäten der VAU* **Eingangsdaten**: • Challenge • [VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU| VAU-Attestierungstoken einer Befugnisverifikations-VAU|

	VAU-Attestierungstoken eines Service-VAU-Typs]
	Ausgangsdaten:
	• Challenge signiert mit privatem Schlüssel der AUT-Identität
	  • der Aktenkontoverwaltungs-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU übergeben wurde,
	  • der Befugnisverifikations-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Befugnisverifikations-VAU übergeben wurde,
	  • des Service-VAU-Typs, falls in den Eingangsdaten ein VAU-Attestierungstoken des Service-VAU-Typs übergeben wurde.
	Prüfschritte
	1. prüfen der Signaturdes VAU-Attestierungstokens (herstellerspezifisch)
	2. prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und zum VAU-Typ passt.
	Falls die Prüfungen in 1) bis 2) erfolgreich waren, wird die übergebene Challenge mit dem privaten Schlüssel der zum VAU-Attestierungstoken gehörenden AUT-Identität signiert.

hsm-r5	*Diese Regel dient zur Nutzung des privaten Schlüssels der ENC-Identität der VAU* **Eingangsdaten**: • verschlüsselte Daten oder asymmetrische Teil des Chiffrats (Hybridverschlüsselung, siehe Hinweis weiter unten) • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU **Ausgangsdaten**: • entschlüsselte Daten oder Shared-Secret aus der Decapsulation-Funktion (Hybridverschlüsselung) Hinweis zum Thema Hybridverschlüsselung: Die Regel hsm-r5 wird u. a. beim Aktenumzug verwendet, wo große Exportpakete (vgl. Abschnitt "3.2.3 Aktenkontozusammenführung") entschlüsselt werden müssen. Das verwendete Verschlüsselungsverfahren ist ECIES, eine Hybrid-Verschlüsselung mit einem asymmetrischen und einem symmetrischen Anteil. Der private Schlüssel der ENC-Identität wird nur für den asymmetrischen Teil notwendig. Der asymmetrische Teil muss im HSM durchgeführt werden. Der symmetrische Teil kann innerhalb der VAU (also außerhalb des VAU-HSMs) ausgeführt werden. **Prüfschritte** 1. prüfen der Signaturdes VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind. Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen verschlüsselten Daten mit dem privaten Schlüssel der ENC-Identität der VAU entschlüsselt.
hsm-r6	*Diese Regel dient zur Nutzung des privaten Schlüssels der Signaturidentität der VAU* **Eingangsdaten**:

	• zu signierende Daten oder der Hashwert der zu signierenden Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU **Ausgangsdaten**: • signierte Daten inkl. Signatur oder nur Signatur (für den Fall, dass bei den Eingangsdaten nur ein Hashwert übergeben wurde) **Prüfschritte** 1. prüfen der Signaturdes VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen Daten mit dem privatem Schlüssel der Signaturidentität der VAU signiert.
hsm-r7	*<weggefallen>*
hsm-r8	*Diese Regel dient zum Ableiten von symmetrischen Schlüsseln für die Ver- bzw. Entschlüsselung von Daten* Sie dient bspw. dazu, sogenannte Submissions für die Datenausleitung an das Forschungsdatenzentrum Gesundheit (FDZ) nach § 363 Absatz 1 SGB V außerhalb der VAU im Aktensystem zwischenzuspeichern, bis das Forschungsdatenzentrum diese Submissions abholt. Die Submissions sind dann über die über diese Regel abgeleiteten symmetrischen Schlüssel außerhalb der VAU kryptographisch gesichert. **Eingangsdaten:** • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder einer Service-VAU • Ableitungsvektor dv • Label für Masterkey (opt.) **Ausgangsdaten:** • symmetrischer Schlüssel symKey • Label für Befugnis-Masterkey **Prüfschritte:** 1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und es sich um die Attestierung einer Aktenkontoverwaltungs-VAU oder Service-VAU handelt 3. falls ein Label für einen Masterkey In den Eingangsdaten enthalten ist, prüfen, ob das Label zu einem Befugnis-Masterkey gehört Falls alle Prüfungen erfolgreich waren, wird symKey wie folgt abgeleitet: Fall: Eingangsdaten enthalten ein Label mkey_label für einen Befugnis-Masterkey: Ableitung eines AES-Schlüssels [FIPS-197] symKey mit 256 Bit Schlüssellänge

	nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren auf Basis des Befugnis-Masterkeys mit Label mkey_label und dem Ableitungsvektor "eds: "+ dv. Ausgangsdaten sind der abgeleitete Schlüssel symKey und das Label mkey_label. (Verständnishinweis: eds steht für "External Data Storage". Das HSM erzwingt bei dieser Regel, dass das Präfix "eds: " (also 5 Byte) dem vom Aufrufer übergebenen Ableitungsvektor (dv) vorangestellt wird.) Fall: Eingangsdaten enthalten kein Label für einen Befugnis-Masterkey: Ableitung eines AES-Schlüssels [FIPS-197] symKey mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#Abschnitt 2.4] zulässigen Verfahren auf Basis des aktuellen Befugnis-Masterkeys und dem Ableitungsvektor "eds: " + dv. Ausgangsdaten sind der abgeleitete Schlüssel symKey und das Label des aktuellen Befugnis-Masterkeys.
hsm-r9 (opt.)	*Diese Regel dient zum Auslesen eines Signatur-Zertifikats des PoPP-Services. Falls Hersteller das Befugnisverifikations-Modul im VAU-HSM umsetzen, kann auf die Regel hsm-r9 verzichtet werden.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (falls der Regelaufruf aus einer Befugnisverifikations-VAU heraus erfolgt) • kid **Ausgangsdaten**: • (kid, C.ZD.SIG) mit Signaturzertifikat C.ZD.SIG des PoPP-Services **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 4. prüfen, ob im VAU-HSM ein Paar (kid, C.ZD.SIG) für den in den Eingangsdaten übergebenen Wert*kid* gespeichert ist Falls die Prüfungen 1) - 4) erfolgreich waren, wird (kid, C.ZD.SIG) zurückgeliefert.
hsm-r10 (opt.)	*Diese Regel dient in Regel kr6 zum Ableiten der Schlüssel dataStorageKey und userSessionKey. Die Regel hsm-r10 muss nur umgesetzt werden, falls das Aktensystem die Funktion des Einfrierens und Auftauens von Daten umsetzt und das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU umgesetzt wird.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU • Akten-ID

	• Label Datenpersistierungs-Masterkey, der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren) • Ableitungsvektor dvector • optional: Eingabezeitpunkt EZ als Unix-Zeit (natürliche Zahl) **Ausgangsdaten**: • dataStorageKey • userSessionKey • Ableitungszeitpunkt AZ(Unix-Zeit) • Label des genutzten Datenpersisitierungs-Masterkeys **Prüfschritte**: 1. prüfen der Signaturender VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die in den VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und es sich bei dem einen Token um die Attestierung einer Aktenkontoverwaltungs-VAU und dem anderen Token um ein Befugnisverifikations-VAU handelt 3. falls ein Eingabezeitpunkt EZ in den Eingangsdaten enthalten und *current_time* der aktuelle Zeitpunkt im VAU-HSM in Unix-Zeit ist, prüfen, ob *current_time - (2*24*60*60) <= EZ <= current_time* 4. prüfen, ob das Label des Masterkeys zu einem Datenpersistierungs-Masterkey gehört Falls alle Prüfungen erfolgreich waren, werden dataStorageKey und userSessionKey wie folgt abgeleitet: dataStorageKey:Ableitung eines AES-Schlüssels [FIPS-197] dataStorageKey mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren auf Basis des in den Eingangsdaten angegebenen Datenpersistierungs-Masterkeys und dem Ableitungsvektor dvector + AZ, wobei AZ=EZ, falls ein Eingabezeitpunkt in den Eingangsdaten enthalten ist, und ansonsten AZ = current_time, d.h. der aktuelle Zeitpunkt im VAU-HSM in Unix-Zeit, userSessionKey: Ableitung eines AES-Schlüssels [FIPS-197] *userSessionKey* mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren auf Basis des in den Eingangsdaten angegebenen Datenpersistierungs-Masterkeys und dem Ableitungsvektor "usk:"+ Akten-ID + *dataStorageKey*. Ausgangsdaten sind der abgeleitete Schlüssel *dataStorageKey, userSessionKey*, der genutzte Ableitungszeitpunkt AZ in Unix-Zeit und das Label des für die Ableitung genutzten Datenpersisierungs-Masterkeys.
hsm-r11	*Diese Regel dient zum Auslesen eines Root-Zertifikats, welches zur Prüfung der Signatur von ITSG-Token genutzt wird.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU

	• VAU-Attestierungstoken einer Befugnisverifikations-VAU (optional) • sn **Ausgangsdaten**: • (sn, Root-Zertifikat) **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 Prüfungen1) - 3) erfolgreich waren, wird (sn, Root-Zertifikat) mit dem Root-Zertifikat zur Prüfung von Signaturen von ITSG-Token mit der Zertifikatsseriennummer *sn* zurückgeliefert.

A_24667 -ePA-Aktensystem -VAU-HSM - Prüfen des VAU-Attestierungstokens
Das VAU-HSM MUSS bei der Prüfung eines VAU-Attestierungstokens sicherstellen, dass dieses zeitlich gültig ist und Replay-Attacken abwehren.**[<=]**

A_26303 -ePA-Aktensystem - Abgeleitete Verschlüsslungsschlüssel sind ausschließlich einer VAU zugänglich
Das ePA-Aktensystem MUSS sicherstellen, dass ein mit Regel hsm-r8 abgeleiteter Schlüssel ausschließlich einer VAU zugänglich ist und ausschließlich mittels AES/GCM analog [gemSpec_Krypt#GS-A_4389] verwendet wird.**[<=]**

3.3.2 Regeln des Befugnisverifikations-Moduls

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

Tabelle 5: Überblick über die Regeln des Befugnisverifikations-Moduls

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
rr0	Mit dieser Regel werden **ID-Token** im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.	*Tab_AS_Entitlement_Registration_Rules*
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 Befugnisse sind vom Vertreter mittels	*Tab_AS_Entitlement_Registration_Rules*

	Signaturdienst signiert.	
rr3	Mit dieser Regel werden **Befugnisse** im Aktensystem registriert, die sich durch das **Stecken der eGK in einer Leistungserbringerumgebung** oder aufgrund eines **PoPP-Tokens** 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*
kr5	<weggefallen>	
kr6	Diese Regel wird für das **Einfrieren** und **Auftauen** von Daten genutzt.	*Tab_AS_SDS-Key_Rules*
kr7	Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels und des versichertenindividuellen Befugnispersistierungsschlüssels durch	*Tab_AS_SDS-Key_Rules*

	einen **Kostenträger** verwendet, der mittels ITSG-Tokens seine Zuständigkeit für das Aktenkonto nachweist.	

A_24573-07 -ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls
Das Befugnisverifikations-Modul MUSS die in den Tabellen*Tab_AS_Entitlement_Registration_Rules-07* und *Tab_AS_SDS-Key_Rules-07* definierten Regeln umsetzen.**[<=]**

Tabelle 6: Tab_AS_Entitlement_Registration_Rules-07 - Regeln zur Registrierung von Befugnissen

Regel	Beschreibung
rr0	Mit dieser Regel werden **ID-Token** im Aktensystem registriert und zu einem HSM-ID-Token konvertiert. **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token mit NutzerID=x signiert durch einen sektoralen Identity Provider, den IDP-Dienst oder den E-Rezept-Fachdienst **Ausgangsdaten**: • HSM-ID-Token mit NutzerID=x gesichert mittels CMAC **Prüfschritte**: 1. prüfen des ID-Tokens gemäß A_24690-* (C.FD.SIG) bei Token eines IDPs bzw. gemäß A_24658-* bei Token des E-Rezept-Fachdiensts (C.FD.AUT). 2. Falls die Prüfung in 1) erfolgreich war, a. erstellt das Befugnisverifikations-Modul ein HSM-ID-Token mit der NutzerID=x, einer Gültigkeitsdauer von 24 Stunden und der professionOID aus dem Signaturzertifikat (`oid_idpd_sek`,`oid_idpd` oder `oid_erp-vau`). b. ruft das Befugnisverifikations-Modul die VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und dem HSM-ID-Token auf. i. 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 das mittels CMAC gesicherte HSM-ID-Token als Ergebnis des Regelaufrufs zurück.
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 oder HSM-ID-Token gesichert mit CMAC • 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-Tokensgemäß A_24690-* (Zertifikatsprofil C.FD.SIG) a. prüfen, ob die professionOID im Signaturzertifikat `oid_idpd_sek` ist b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt oder prüfen des HSM-ID-Tokens c. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. d. prüfen, ob die professionOID im HSM-ID-Token `oid_idpd_sek` ist e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt. 2. prüfen der Befugnis1 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-* zeitlich gültig ist (`iat` - 15s <= aktuelle Zeit <`exp` + 15s) 3. Falls die Prüfungen in 1) bis 2) erfolgreich waren, erstellt das Befugnisverifikations-Modul die Befugnis2. Die Inhalte werden aus Befugnis1 übernommen mit folgender Ausnahme: Für eine Befugnis1 mit oid = oid_ncpeh wird die Gültigkeit validTo in Befugnis2 auf aktuelle Zeit + 1 Stunde gesetzt. 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
- ID-Token oder HSM-ID-Token gesichert mit CMAC
- Befugnis1 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) signiert vom Vertreter
- Befugnis2 = (KVNR Aktenkonto, KVNR Vertreter) gesichert mittels CMAC

Ausgangsdaten:

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

Prüfschritte:

1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG)
   a. prüfen, ob die professionOID im Signaturzertifikat `oid_idpd_sek` ist
   b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt

      oder prüfen des HSM-ID-Tokens
   c. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens
      i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
   d. prüfen, ob die professionOID im HSM-ID-Token `oid_idpd_sek` ist
   e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt.
2. prüfen der Befugnis1 und Befugnis2
   a. prüfen der Signatur von Befugnis1 gemäß A_25042-* (Zertifikatsprofil C.CH.SIG)
   b. prüfen, ob die professionOID im Signaturzertifikat `oid_versicherter` ist
   c. prüfen des CMAC von Befugnis2
   d. prüfen, dass die Telematik-ID in Befugnis 1 keine KVNR ist (Vertreter dürfen keine weiteren Vertreter befugen)
   e. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der „KVNR Vertreter“ in der Befugnis2 übereinstimmt
   f. prüfen, ob die „KVNR Aktenkonto“ in Befugnis 1 mit der „KVNR Aktenkonto“ in Befugnis2 übereinstimmt
   g. prüfen, dass das JWT gemäß A_24587-* zeitlich gültig ist (`iat` - 15s <= aktuelle Zeit <`exp` + 15s)
3. Falls die Prüfungen in 1) erfolgreich waren, wird die Befungnis3 vom

	Befugnisverifikations-Modul erstellt. Die Inhalte werden aus Befugnis1 übernommen. 4. 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. 5. 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 oder aufgrund eines PoPP-Tokens ergeben. **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VSDM-Prüfziffer in Version 2 signiert mit AUT-Identität der SMC-B **oder** signiertes PoPP-Token **Ausgangsdaten**: • Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC • falls VSDM-Prüfziffer in Version 2, zusätzlich die innere Struktur der Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) **Prüfschritte**: Szenario VSDM-Prüfziffer in Version 2: Falls `enforce_popp_only = true`, dann FAIL, ansonsten führe die folgenden Prüfschritte durch: 1. prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A_25042-* (C.HCI.AUT) 2. Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert. 3. Aufruf von VAU-HSM Regel hsm-r3 mit der dekodierten VSDM-Prüfziffer a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. prüfen der inneren Struktur nach Prüfschritt 6 gemäß A_27279-* (d.h. eGK ist nicht gesperrt) 5. prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer (prüfziffer.iat) nicht länger als 20 Minuten zurückliegt (prüfziffer.iat - 30s <= aktuelle Zeit < prüfziffer.iat + 20 Minuten +15s, Hinweis in der Prüfziffer gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben) 6. prüfen des prüfziffer.hcv nach Prüfschritt 8 gemäß A_27279-* bzgl. des hcv im JWT 7. Falls die Prüfungen in 1) bis 6) erfolgreich waren, und die VAU-HSM Regel hsm-r3 den Klartext der inneren Struktur der Prüfziffer zurückgeliefert hat, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten

erstellt:

- Aktenkonto: KVNR, die als Ergebnis der VAU-HSM Regel hsm-r3 zurückgeliefert wird
- Telematik-ID: die Telematik-ID aus der SMC-B-Signatur
- Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur.

8. 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.
9. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis sowie die entschlüsselte innere Struktur der Prüfziffer im Klartext gemäß A_27278-* als Ergebnis des Regelaufrufs zurück.

Szenario PoPP-Token:

1. prüfen des PoPP-Tokens via TI-PKI gemäß Abschnitt "PoPP-Token Prüfung" in [gemSpec_PoPP_Service], wobei im HSMbis auf den OCSP-Sperrstatus keine Prüfung des Signaturzertifikats des PoPP-Tokens erfolgt, da das Signaturzertifikat kontrolliert im 4-Augenprinzip in das HSM eingebracht wird. Für die PoPP-Token Prüfung muss ein in das HSM eingebrachtes TI-PKI-Signaturzertifikat genutzt werden. Da das in das HSM eingebrachte TI-PKI-Signaturzertifikat genutzt wird, ist auch kein Bezug und keine Verarbeitung von Entity Statements im HSM erforderlich. Der Claim`iss` im PoPP-Token muss nicht geprüft werden. Das benötigte Signaturzertifikat des PoPP-Service kann bei Bedarf mittels Regel hsm-r9 und dem kid-Wert aus dem PoPP-Token-header vom VAU-HSM abgerufen werden. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird der Regel hsm-r9 zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU übergeben.
2. prüfen, dass der Ausstellungszeitpunkt des PoPP-Tokens (PoPP-Token.iat) nicht länger als 2 Tage zurückliegt (PoPP-Token.iat - 30s <= aktuelle Zeit < PoPP-Token.iat + 2 Tage+15s, Hinweis: im PoPP-Token gibt es kein exp, deshalb wird im Vergleich explizit 2 Tage + 15 Sekunden angegeben).
3. prüfen, dass PoPP-Token.proofMethod keine Prüfmethode `ehc-provider-*` ist.
4. Falls die Prüfungen in 1) bis 3) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:
   - Aktenkonto: KVNR aus PoPP-Token.patientId
   - Telematik-ID: Telematik-ID aus PoPP-Token.actorID
   - Gültigkeitszeitraum: das Ende der Gültigkeit (validTo) ergibt sich aus`PoPP-Token.iat + maxEntitlementValidity`, wobei `maxEntitlementValidity` die in A_23941-* festgelegte Standard-Befugnisdauer für die Rolle in PoPP-Token.actorProfessionOid in Sekunden ist.
5. 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. 6. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis 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 professionOID`oid_epa_vauist` c. prüfen, dass das SignaturzertifikatC.FD.SIG nicht auf das importierende Aktensystem ausgestellt 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_24690-01 -ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen des ID-Tokens
Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung eines ID-Tokens durchführen:

- dasID-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 Feldauddas ePA-Aktensystem eingetragen haben.

[<=]

A_24691 -ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen von übers ePA-FdV erstellten Befugnissen
Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung einer von einem Versicherten bzw. Vertreter über das ePA-FdV eingestellten signierten Befugnis durchführen:

- die Befugnis muss gemäß A_25042-* valide signiert sein durch einen Versicherten bzw. Vertreter (C.CH.SIG, professionOID istoid_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 7: Tab_AS_SDS-Key_Rules Key Rules-07 - 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 oder HSM-ID-Token gesichert mit CMAC • Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren). • Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren). **Ausgangsdaten**: • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys • versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys **Regelverhalten**: 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) a. prüfen, ob die professionOID im Signaturzertifikat `oid_idpd_sek` ist oder prüfen des HSM-ID-Tokens b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. c. prüfen, ob die professionOID im HSM-ID-Token `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, der KVNR aus dem ID-Token und den Labeln der zu verwendenden Befugnispersistierungs- und Datenpersistierungs-Masterkeys 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) • Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll **Ausgangsdaten**: • versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys **Prüfschritte**: 1. Aufruf der VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR und dem Label des Befugnispersistierungs-Masterkeys zur Ableitung des Befugnispersistierungsschlüssels 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 oder HSM-ID-Token gesichert mit CMAC • Befugnis = (KVNR Aktenkonto, BefugtenID (TID|KVNR), Gültigkeitszeitraum (opt.)) mit CMAC gesichert **Ausgangsdaten**: • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys **Prüfschritte**: 1. prüfen des ID-Tokens a. gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) oder prüfen des HSM-ID-Tokens b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.

	2. Prüfen der Befugnis a. prüfen des CMAC der Befugnis mittels VAU-HSM Regel hsm-r1 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 bzw. im HSM-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, der KVNR aus dem ID-Tokenbzw. im HSM-ID-Token und dem Label für den Datenpersistierungs-Masterkey 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 oder HSM-ID-Token gesichert mit CMAC • KVNR (Aktenkonten-ID) • Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll **Ausgangsdaten**: • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys **Prüfschritte**: 1. Prüfen des ID-Tokens a. prüfen der Signaturgemäß A_25042-* (C.FD.AUT) b. prüfen, ob die professionOID im Zertifikat C.FD.AUT gleich `oid_erp-vauist` c. prüfen des ID-Tokens gemäß A_24658-* oder prüfen des HSM-ID-Tokens d. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.

	e. prüfen, ob die professionOID im HSM-ID-Token `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, der KVNR aus dem ID-Token bzw. dem HSM-ID-Token und dem Label für den Datenpersistierungs-Masterkey 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. 3. Das Befugnisverifikations-Modul liefert den abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.
kr5	*<weggefallen>*
kr6 (opt.)	Diese Regel wird für das temporäre**Einfrieren** und **Auftauen** von Daten genutzt. Hinweis: Die Regel kr6 muss nicht umgesetzt werden, falls das Aktensystem die Funktion des Einfrierens und Auftauens von Daten nicht umsetzt. **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Akten-ID: eindeutige ID des Aktenkontos (z.B. KVNR oder aktenspezifisches Pseudonym) • Ableitungsvektor dv • Label Datenpersistierungs-Masterkey, der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren) • optional: Eingabezeitpunkt EZ als Unix-Zeit (natürliche Zahl) **Ausgangsdaten**: • symmetrischer Schlüssel *dataStorageKey* • symmetrischer Schlüssel *userSessionKey* • Ableitungszeitpunkt AZ(Unix-Zeit) • Label des genutzten Datenpersisitierungs-Masterkeys **Prüfschritte**: Falls das Befugnisverifikationsmodul im VAU-HSM und nicht in einer Befugnisverifikations-VAU umgesetzt wird 1. prüfen der Signatur des VAU-Attestierungstokens und das es ein Attestierungstoken einer AK-VAU ist (herstellerspezifisch) 2. ist ein Eingabezeitpunkt EZ in den Eingangsdaten enthalten und *current_time* der aktuelle Zeitpunkt im VAU-HSM in Unix-Zeit, prüfe, ob *current_time - (2*24*60*60) <= EZ <= current_time*. Falls alle Prüfungen erfolgreich waren: <u>Variante: Befugnisverifikationsmodul wird im VAU-HSM umgesetzt</u> 1. Ableitung eines AES-Schlüssels [FIPS-197] *dataStorageKey* mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren

	auf Basis des in den Eingangsdaten angegebenen Datenpersistierungs-Masterkeys und dem Ableitungsvektor "dsk: " + Akten-ID+ dv + AZ, wobei AZ=EZ, falls ein Eingabezeitpunkt in den Eingangsdaten enthalten ist, und ansonsten AZ =*current_time*, d.h. der aktuelle Zeitpunkt im VAU-HSM in Unix-Zeit, 2. Ableitung eines AES-Schlüssels [FIPS-197] *userSessionKey* mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren auf Basis des in den Eingangsdaten angegebenen Datenpersistierungs-Masterkeys und dem Ableitungsvektor "usk:"+ Akten-ID +*dataStorageKey*. Variante: Befugnisverifikationsmodul wird in einer Befugnisverifikations-VAU umgesetzt 1. Ableitung der Schlüssel *dataStorageKey* und *userSessionKey* durch Aufruf der HSM-Regel hsm-r10 mit den folgenden Aufrufparametern: a. hsm-r10 Eingangsparameter "Akten-ID": Akten-ID aus den Eingangsdaten b. hsm-r10 Eingangsparameter "Label desDatenpersisitierungs-Masterkeys": Label des Datenpersisitierungs-Masterkeys aus den Eingangsdaten, c. hsm-r10 Eingangsparameter "dvector": "dsk: " + Akten-ID+ dv d. hsm-r10 Eingangsparameter "Eingabezeitpunkt": Eingabezeitpunkt EZaus Eingangsdaten, falls vorhanden Ausgangsdaten sind der abgeleitete Schlüssel *dataStorageKey, userSessionKey*, der genutzte Ableitungszeitpunkt AZ in Unix-Zeit und das Label des für die Ableitung genutzten Datenpersisierungs-Masterkeys.
kr7	*Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels und des versichertenindividuellen Befugnispersistierungsschlüssels durch einen* ***Kostenträger*** *verwendet, der mittels****ITSG-Tokens*** *seine Zuständigkeit für das Aktenkonto nachweist.* **Eingangsdaten**: • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • signiertes ITSG-Token • self-signed ID-Token des Kostenträgers • Label Datenpersistierungs-Masterkey, der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren). • Label Befugnispersistierungs-Masterkey, der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren). **Ausgangsdaten**: • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys • versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys **Prüfschritte**: 1. prüfen des ITSG-Tokens gemäß A_30433-*, wobei mit *hsm-r11* das für die

	Prüfung der Signatur benötigte ITSG-Root-Zertifikat ausgelesen wird, a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird der Regel hsm-r11 zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU übergeben. 2. prüfen des self-signed ID-Tokens des Kostenträgers gemäß A_30396-*, 3. prüfen, dass der „commonName”-Wert im ITSG-Token gleich dem „cn“-Wert im self-signed ID-Token des Kostenträgers ist 4. bilden des SHA-256 Hashwertes des ITSG-Tokens und prüfen, dass der gebildete Hashwert des ITSG-Tokens gleich dem „hash-itsg“-Wert im self-signed ID-Token des Kostenträgers ist. Falls die Prüfungen in 1) – 4) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung (und ggf. dem VAU-Attestierungstoken für die Befugnisverifikations-VAU) und der KVNR aus dem Claim „sub“ des ITSG-Tokens aufgerufen. Das Befugnisverifikations-Modul liefert die abgeleiteten Daten- und Befugnispersistierungsschlüssel als Ergebnis des Regelaufrufs sowie die Label der verwendeten Masterkeys zurück

A_30433 -ePA-Aktensystem - Prüfung eines ITSG-Tokens
Das ePA-Aktensystem MUSS sicherstellen, dass eine Prüfung eines signierten ITSG-Tokens nur dann erfolgreich ist, wenn

- dass im Header aufgeführte "signierende" Zertifikat gültig ist, inkl. OCSP-Prüfung (vgl. OCSP-Response-Caching nach [gemSpec_PKI#A_23225]),
- die Signatur valide ist,
- die "iat"-Zeit nicht älter als 15 Minuten ist,
- der "aud"-Wert gleich „ePA“ ist.

[<=]

3.4 Vertrauenswürdige Ausführungsumgebung (VAU)

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

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

A_25716-03 -ePA-Aktensystem - Services ausschließlich in der VAU
Das ePA-Aktensystem MUSS sicherstellen, dass die folgenden Services ausschließlich innerhalb einer VAU ausgeführt werden können und ein Zugriff auf die Schnittstellen ausschließlich über einen VAU-Kanal erfolgen kann:

- Consent Decision Management Service

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

[<=]

Typen von VAU-Schnittstellen

Die folgende Abbildung zeigt die unterschiedlichen Typen von VAU-Schnittstellen.

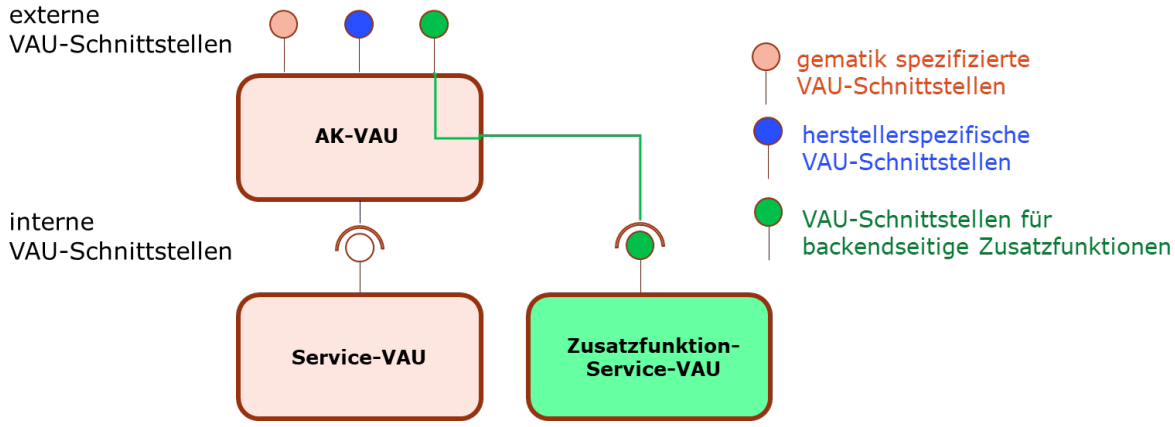


Abbildung 3 - Typen von VAU-Schnittstellen

Externe VAU-Schnittstellensind VAU-Schnittstellen, die von Client-Systemen aufgerufen werden können, die sich außerhalb einer VAU-Instanz des ePA-Aktensystems befinden. Aus Sicht der VAU-Isntanzen des ePA-Aktensystems sind diese Clients extern. Externe Schnittstellen werden insbesondere von Client-Systemen der gesetzlich festgelegten Nutzer (z.B. Versicherte, Leistungserbringer, Kostenträger) der ePA aufgerufen. Es kann jedoch auch externe VAU-Schnittstellen geben, die von Client-Systemen des Betreibers der ePA-Aktensystems zum Betrieb des Aktensystems genutzt werden.

Bei externen VAU-Schnittstellen werden unterschieden:

- **gematik-spezifizierte VAU-Schnittstellen**sind VAU-Schnittstellen, die von der gematik durch die Spezifikation vorgegeben sind,
- **herstellerspezifische VAU-Schnittstellen**sind VAU-Schnittstellen, die ein Hersteller des ePA-Aktensystems von sich aus entwickelt und für den Betrieb des ePA-Aktensystems für den Betreiber oder den Anbieter des ePA-Aktensystems notwendig sind. Die gematik gibt herstellerspezifische VAU-Schnittstellen nicht durch die Spezifikation vor.

- **VAU-Schnittstellen backendseitiger Zusatzfunktionen**werden durch den ZF-Manager über den ZF-Proxy für Client-Systeme nach außen exponiert. Die Schnittstellen einer backendseitigen Zusatzfunktion werden ebenfalls nicht durch die gematik vorgegeben.

Interne VAU-Schnittstellensind VAU-Schnittstellen, die ausschließlich von VAU-Instanzen innerhalb des ePA-Aktensystems aufgerufen werden können. Client-Systeme außerhalb einer VAU-Instanz haben technisch keinen Zugriff auf interne VAU-Schnittstellen. Ausschließlich Service-VAU-Instanzen können interne VAU-Schnittstellen besitzen.

A_28805-01 -ePA-Aktensystem - Begutachtung aller herstellerspezifischen VAU-Schnittstellen
Der Hersteller eines ePA-Aktensystems MUSS sicherstellen, dass

- alle externen herstellerspezifischen und internen VAU-Schnittstellen vom Produktgutachter im Produktgutachten dokumentiert werden. Dies beinhaltet insbesondere auch herstellerspezifische VAU-Schnittstellen, die z.B. zum Anlegen oder Löschen einer Akte oder sonstiger administrativer Funktionen implementiert wurden.
- alle externen herstellerspezifischen VAU-Schnittstellen begutachtet werden,
- dem Produktgutachter dafür eine aktuelle und ausreichend detaillierte Liste sämtlicher Schnittstellen zur Verfügung gestellt werden

[<=]

Hinweis zu A_28805-*: Im Produktgutachten sind die VAU-Schnittstellen durch den Produktgutachter so zu dokumentieren, dass deren Zweck und die verarbeiteten Daten daraus hervorgehen. Dies bezieht sich sowohl auf Aktenkontoverwaltungs- als auch Service-VAUs.

A_28888 -ePA-Aktensystem - Herstellerspezifische VAU-Schnittstellen ausschließlich für den Betreiber oder Kostenträger
Der Hersteller des ePA-Aktensystems MUSS technisch sicherstellen, dass herstellerspezifische VAU-Schnittstellen ausschließlich für den Betreiber des ePA-Aktensystems oder für Kostenträger nutzbar sind.**[<=]**

A_28916 -ePA-Aktensystem - Eigene VAU-Instanz für Betreiberzugriffe
Das ePA-Aktensystem MUSS sicherstellen, dass ein Betreiber ausschließlich über herstellerspezifische VAU- Schnittstellen auf eine VAU-Instanz zugreifen kann, in der keine unverschlüsselten Daten nach A_25716-* verarbeitet werden. Dies bedeutet, dass Betreiber für administrative Funktionen eine eigene VAU-Instanz nutzen müssen.**[<=]**

A_28807 -ePA-Aktensystem - Aktensystem-Schnittstellen gewährleisten technischen Ausschluss des Betreibers
Das ePA-Aktensystem MUSS technisch ausschließen, dass dem Betreiber des ePA-Aktensystems über eine Schnittstelle des ePA-Aktensystems (VAU- oder Nicht-VAU-Schnittstelle) Daten offenbart werden oder der Betreiber auf entschlüsselte Daten zugreifen kann, die durch die VAU zu schützen sind, sofern dies nicht durch andere gematik-Anforderungen erlaubt wird.**[<=]**

A_28855 -ePA-Aktensystem - Zulässigkeit von Aktensystem-Schnittstellen für Kostenträger
Falls das ePA-Aktensystem dem Kostenträger eine Schnittstelle (VAU- oder Nicht-VAU-Schnittstelle) anbietet, MUSS das ePA-Aktensystem technisch ausschließen, dass dem Kostenträger über diese Schnittstelle Daten offenbart werden oder der Kostenträger Daten entschlüsseln kann, die durch die VAU zu schützen sind, sofern dies nicht durch andere gematik-Anforderungen erlaubt wird.**[<=]**

Hinweis zu A_28807-* und A_28855-*: Die durch die VAU zu schützenden Daten sind alle Daten der in der VAU laufenden Services nach A_25716-*. Die Anforderungen des

Abschnitts "Logging und Monitoring" sind ein Beispiel für gematik-Anforderungen, die dem Betreiber des ePA-Aktensystems in gewissem Rahmen erlauben, durch die VAU zu schützende Daten zu protokollieren.Ein weiteres Beispiel ist die Schnittstelle des Betreibers zum Auftauen von Daten gemäß Abschnitt 3.5.5.

A_28856 -ePA-Aktensystem - Aktensystem-Schnittstelle für Kostenträger zu administrativen Zwecken
Das ePA-Aktensystem KANN dem Kostenträger eine (VAU-)Schnittstelle anbieten, über die der Kostenträger administrative Informationen zu den vom Kostenträger verantworteten Akten erhalten kann, z.B. aktenübergreifende Statistiken zur Aktennutzung oder das letzte Nutzungsdatum einer Akte.**[<=]**

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.

3.4.1 Übergreifende VAU-Anforderungen

3.4.1.1 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.

3.4.1.2 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.**[<=]**

A_25244 -ePA-Aktensystem - x-insurantId nicht außerhalb des VAU-Kanals
Das ePA-Aktensystem MUSS sicherstellen, dass das HTTP Header-Element mit dem Namen "x-insurantId"nicht außerhalb des VAU-Kanals gesendet wird.**[<=]**

3.4.1.3 Schutz der Daten bei Speicherung außerhalb der VAU

A_26314 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Daten
Das ePA-Aktensystem MUSS sicherstellen, dass eine VAU-Daten, die im System des Aktensystembetreibers gespeichert werden sollen und für die keine spezifischen Anforderungen zum Schutz der gespeicherten Daten existieren, ausschließlich verschlüsselt gespeichert werden und der verwendete Verschlüsselungsschlüssel mittels der Regel hsm-r8 vom VAU-HSM abgeleitet wird.**[<=]**

Hinweise zu A_26314:

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

A_26322 -ePA-Aktensystem - Unterschiedliche Schlüssel für die Verschlüsselung von außerhalb der VAU gespeicherten Daten bei unterschiedlichen Verarbeitungszwecken
Falls Daten außerhalb der VAU im System des Aktensystembetreibers gespeichert werden, MUSS das ePA-Aktensystem sicherstellen, dass für die Verschlüsselung von Daten, die zu unterschiedlichen Zwecken verarbeitet werden, unterschiedliche Verschlüsselungsschlüssel genutzt werden.**[<=]**

Hinweis zu A_26322: Verarbeitungszwecke für Daten sind beispielsweise die Verarbeitung von Daten zum Zwecke der Sekundärnutzung (sieheData Submission Service) oder die Verarbeitung von Daten für die Nutzerverwaltung im Aktensystem (insbesondere Geräteinformationen und E-Mail-Adressen).

3.4.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM

A_24653 -ePA-Aktensystem - Sichere Verbindung zwischen VAU und VAU-HSM
Das ePA-Aktensystem MUSS technisch sicherstellen, dass zwischen einer VAU und einem VAU-HSM eine beidseitig authentisierte und vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen.**[<=]**

3.4.1.5 Logging und Monitoring

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

A_24910 -ePA-Aktensystem - Erlaubte Zwecke der Betreiberprotokolle
Der Betreiber des Aktensystems MUSS sicherstellen, dass die durch die VAU für den Betrieb erstellten Protokolle des Betreibers ausschließlich zum Zwecke der Fehleranalyse und -behebung anlassbezogen sowie zum Zwecke des Security Monitorings verwendet werden.**[<=]**

A_24649 -ePA-Aktensystem - Datenschutzkonformes Logging und Monitoring der VAU
Die VAU MUSS die für den Betrieb des ePA-Aktensystems erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dem Betreiber des ePA-Aktensystems vertrauliche oder zur unautorisierten Profilbildung geeignete Daten zur Kenntnis gelangen. **[<=]**

A_24695 -ePA-Aktensystem - Keine medizinische Informationen in VAU-Protokollen des Betreibers
Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten Protokollen des Betreibers keine personenbezogenen medizinischen Informationen enthalten sind (u. a. medizinische Daten von Versicherten oder Informationen, aus denen sich ableiten lässt, bei welchen Leistungserbringerinstitutionen ein Versicherter in Behandlung ist).
[<=]

A_24909 -ePA-Aktensystem - Nicht KVNR und Telematik-ID gemeinsam protokollieren
Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten Protokollen des Betreibers höchstens die KVNR oder höchstens die Telematik-ID enthalten ist, aber nicht eine Kombination aus KVNR und Telematik-ID und keine solche Verbindung über mehrere Protokolle hergestellt werden kann.**[<=]**

A_24719 -ePA-Aktensystem - Kein kryptographisches Schlüsselmaterial in VAU-Protokollen des Betreibers
Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten Protokollen des Betreibers kein kryptographisches Schlüsselmaterial enthalten ist.**[<=]**

A_24911 -Löschfristen Protokolle
Das ePA-Aktensystem MUSS sicherstellen, dass die

- zum Zwecke der Fehleranalyse erhobenen Protokolle nach Behebung des Fehlers unverzüglich gelöscht werden,
- zum Zwecke des Security Monitorings erhobenen Protokolle nach 3 Monaten gelöscht werden.

[<=]

A_26316 -Anbieter ePA-Aktensystem - Schutz der Protokolle des Betreibers
Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die durch die VAU für den Betrieb erstellten Protokolle des Betreibers durch technische und organistorische Maßnahmen vor einer missbräuchlichen Nutzung geschützt werden.**[<=]**

gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik

Hinweis zu A_27336-*: Der geheime Schlüssel für die Pseudonymisierung muss nicht im VAU-HSM gespeichert werden.

A_27333 -ePA-Aktensystem - Geheimer Schlüssel für Pseudonymisierung der gematik-Logdaten nur in VAU
Das ePA-Aktensystem MUSS sicherstellen, dass der für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigte geheime Schlüssel `key_pn_log` im Klartext ausschließlich innerhalb einer VAU-Instanz verarbeitet wird.**[<=]**

A_27336 -ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung im 4-Augen-Prinzip
Das ePA-Aktensystem MUSS sicherstellen, dass der für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigte geheime Schlüssel `key_pn_log` ausschließlich im 4-Augen-Prinzip ins ePA-Aktensystem eingebracht werden kann.**[<=]**

A_27334 -ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung der gematik-Logdaten im 4-Augen-Prinzip
Der Betreiber des ePA-Aktensystems MUSS den für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigten geheimen Schlüssel `key_pn_log` ausschließlich im 4-Augen-Prinzip mit der gematik ins ePA-Aktensystem einbringen.**[<=]**

A_27335 -ePA-Aktensystem - Wechsel des Schlüssels für Pseudonymisierung der gematik-Logdaten
Der Betreiber des ePA-Aktensystems MUSS den für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigten geheimen Schlüssel `key_pn_log` spätestens nach 1 Jahr wechseln.**[<=]**

3.4.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU

3.4.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU

A_24636-01 -ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen innerhalb einer VAU-Instanz
Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb einer VAU-Instanz zwischen Health Record Contexten bzw. User Sessions keine Informationsflüsse auftreten können.**[<=]**

A_27534 -ePA-Aktensystem – Kein gemeinsamer Speicher von Datenverarbeitungsprozessen innerhalb einer VAU-Instanz
Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb einer VAU-Instanz von einem Health Record Context bzw. einer User Sessions nicht auf den Speicher anderer Health Record Contexte bzw. User Sessions zugegriffen werden kann.**[<=]**

Hinweis zu A_24636-* und A_27534-*: Die in den Anforderungen geforderten technischen Maßnahmen beziehen sich ausschließlich auf den Regelfall der Datenverarbeitung ("Gutfall").

A_27535-01 -ePA-Aktensystem – Maximale Lebensdauer von VAU-Instanzen
Das ePA-Aktensystem MUSS sicherstellen, dass VAU-Instanzen einer Aktenkontoverwaltungs-VAU nach maximal 26 Stunden beendet werden.**[<=]**

A_24885 -ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen unterschiedlicher VAU-Instanzen
Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der unabhängig vom Separationsmechanismus in A_24636-* ist, ausschließen, dass sich Verarbeitungen in einer VAU-Instanz schadhaft auf die Verarbeitungen einer anderen VAU-Instanz auswirken können.
[<=]

A_24637 -ePA-Aktensystem - Maximale Health Record Context in einer VAU-Instanz
Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Health Record Context gleichzeitig in einer VAU-Instanz laufen können.
[<=]

A_25028 -ePA-Aktensystem - Keine Kommunikation zwischen Aktenkontoverwaltungs-VAUs
Das ePA-Aktensystem MUSS sicherstellen, dass es keine direkte Kommunikation zwischen VAU-Instanzen von Aktenkontoverwaltungs-VAUs gibt.**[<=]**

A_26111 -ePA-Aktensystem - Keine Kommunikation zwischen Health Record Contexts
Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer Aktenkontoverwaltungs-VAU-Instanz keine Kommunikation zwischen Health Record Contexts gibt.**[<=]**

A_24639 -ePA-Aktensystem - Löschen aller Daten beim Beenden eines Health Record Context
Die VAU MUSS sicherstellen, dass beim Beenden eines Health Record Context sämtliche Daten dieses Health Record Context aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. **[<=]**

A_24640 -ePA-Aktensystem - Löschen aller Daten beim Beenden einer User Session

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

Hinweis zu A_24639-, A_24640-* und A_24648-*: Eine zeitliche Verzögerung des Löschens ist tolerabel, sofern ein sofortiges Löschen aufgrund der Architektur des Aktensystemherstellers aus Performanzgründen nicht sinnvoll ist. In diesem Fall ist ein geeigneter Kompromiss zwischen dem Löschzeitpunkt und der Performanz zu wählen.*

A_25231 -ePA-Aktensystem - Schließen des Health Record Context beim Beenden einer User Session
Die VAU MUSS sicherstellen, dass beim Beenden einer User Session alle mit dieser User Session verknüpften Health Record Context beendet werden, wenn der jeweilige Health Record Context nicht mit mindestens einer weiteren User Session verknüpft ist.**[<=]**

A_25051 -ePA-Aktensystem - VAU-Kanal endet immer in einer Aktenkontoverwaltungs-VAU
Die VAU MUSS sicherstellen, dass ein VAU-Kanal von einem Client der ePA (ePA-Client oder ePA-FdV) ausschließlich in einer Aktenkontoverwaltungs-VAU endet.**[<=]**

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

3.4.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-VAU

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

A_24643 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Daten mit dem Datenpersistierungsschlüssel
Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten

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

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

A_24644 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Befugnissen mit dem Befugnispersistierungsschlüssel
Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten Daten des Entitlement Managements, d. h. Befugnisse und Befugnisverbote, vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health Record Context mit dem zum Health Record gehörenden versichertenindividuellen Befugnispersistierungsschlüssel verschlüsselt werden.**[<=]**

3.4.2.3 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.**[<=]**

3.4.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU

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

A_24646 -ePA-Aktensystem - Befugnisverifikations-VAU verarbeitet ausschließlich ein Befugnisverifikations-Modul
Das ePA-Aktensystem MUSS sicherstellen, dass in einer Befugnisverifikations-VAU ausschließlich ein Befugnisverifikations-Modul ausgeführt wird.**[<=]**

A_24647 -ePA-Aktensystem - Befugnisverifikations-VAU speichert keine Daten
Eine Befugnisverifikations-VAU DARF die Daten, die sie im Rahmen der Regeln des Befugnisverifikations-Moduls verarbeitet, NICHT außerhalb der Befugnisverifikations-VAU speichern.**[<=]**

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

A_24648 -ePA-Aktensystem - Befugnisverifikations-VAU löscht Daten nach Regelbearbeitung
Eine Befugnisverifikations-VAU MUSS sämtliche Daten, die sie im Rahmen eines Regelaufrufs des Befugnisverifikations-Moduls verarbeitet, sofort nach Abarbeitung der Regel sicher aus der Befugnisverifikations-VAU löschen bzw. einen Zugriff auf diese Daten technisch ausschließen.**[<=]**

A_24671 -ePA-Aktensystem - Sichere Verbindung zwischen VAU-Instanzen
Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer VAU-Instanz einer Befugnisverifikations-VAU und einer VAU-Instanz einer Aktenkontoverwaltungs-VAU eine beidseitig 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.**[<=]**

3.4.4 Zusätzliche Anforderungen an eine Service-VAU

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

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

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

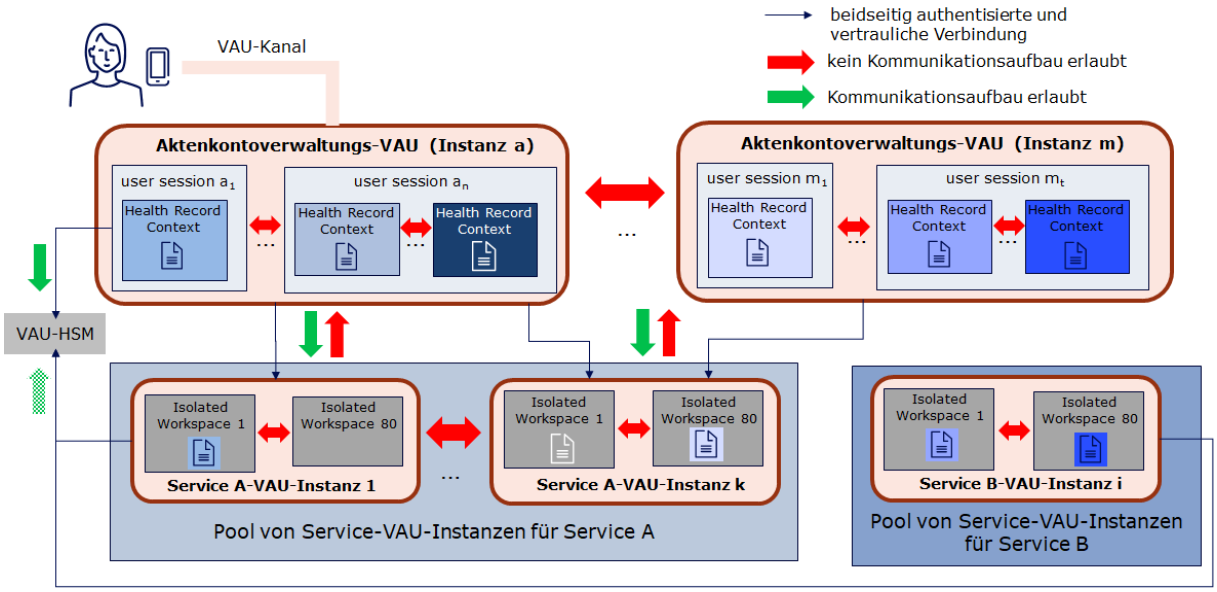


Abbildung 4: Überblick Service-VAUs

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

A_26112 -ePA-Aktensystem - Maximale Isolated Workspaces in einer Service-VAU-Instanz
Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Isolated Workspaces gleichzeitig in einer Service-VAU-Instanz laufen können.**[<=]**

A_26113-01 -ePA-Aktensystem - Isolation zwischen Isolated Workspaces innerhalb einer Service-VAU-Instanz
Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb einer Service-VAU-Instanz zwischen Isolated Workspaces keine Informationsflüsse auftreten können.
[<=]

A_27537 -ePA-Aktensystem – Kein gemeinsamer Speicher von Isolated Workspaces innerhalb einer Service-VAU-Instanz
Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb einer Service-VAU-Instanz von einem Isolated Workspace nicht auf den Speicher anderer Isolated Workspaces zugegriffen werden kann.**[<=]**

A_26114 -ePA-Aktensystem - Isolation zwischen unterschiedlichen Service-VAU-Instanzen
Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der unabhängig vom Separationsmechanismus in A_26113-* ist, ausschließen, dass sich Verarbeitungen in einer Service-VAU-Instanz schadhaft auf die Verarbeitungen einer anderen Service-VAU-Instanz auswirken können.**[<=]**

A_26115 -ePA-Aktensystem - Isolated Workspace verarbeitet maximal einen Request einer AK-VAU
Nachdem ein Isolated-Workspace einen (1) Service-Request einer Aktenkontoverwaltungs-VAU-Instanz verarbeitet hat, MUSS das ePA-Aktensystem sicherstellen, dass alle Daten des Isolated-Workspaces sicher gelöscht werden, um den Isolated-Workspace für nachfolgende Service-Requests wieder neu zu initialisieren.**[<=]**

A_26116 -ePA-Aktensystem - In einem Isolated Workspace sind zu einem Zeitpunkt nur Daten eines Versicherten
Das ePA-Aktensystem MUSS sicherstellen, dass in einem Isolated Workspace zu einem Zeitpunkt ausschließlich Daten eines Versicherten verarbeitet werden können, sofern die Auswahl der zu verarbeitenden Daten durch die Logik im ePA-Aktensystem bestimmt wird.**[<=]**

Hinweis zu A_26116-*: Falls Nutzer die Daten für die Service-VAU auswählen, ohne dass das ePA-Aktensystem auf diese Daten Einfluss hat (z.B. Nutzer wählt zu konvertierende PDF-Dokumente im ePA-FdV aus) kann es dazu kommen, dass zu einem Zeitpunkt auch Daten mehrerer Versicherter in einem Isolated Workspace verarbeitet werden.

A_26117 -ePA-Aktensystem - Keine Kommunikation zwischen Isolated Workspaces
Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer Service-VAU-Instanz keine Kommunikation zwischen Isolated Workspaces gibt.**[<=]**

A_26118 -ePA-Aktensystem - Keine Kommunikation zwischen Service-VAU
Das ePA-Aktensystem MUSS sicherstellen, dass es keine Kommunikation zwischen Instanzen von Service-VAUs gibt.**[<=]**

A_26119 -ePA-Aktensystem - Service-VAUs speichern keine Daten in Aktenkonten
Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine Daten in einem Aktenkonto eines Versicherten persistieren.**[<=]**

A_26120 -ePA-Aktensystem - Service-VAUs verarbeiten keine Identitätstoken
Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine Identitätstoken von Nutzern verarbeiten.**[<=]**

A_26123 -ePA-Aktensystem - Service-VAU-Instanzen haben maximale Lebensdauer
Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen nach einer definierten Lebensdauer (abhängig von der Funktionalität der Services) keine neuen Service-Requests mehr annehmen können und, nachdem die laufenden Requests abgearbeitet wurden, beendet und neu gestartet werden.**[<=]**

A_26124 -ePA-Aktensystem - Information über neuen Service-VAU-Typ
Der Hersteller des ePA-Aktensystems MUSS die gematik über die Absicht der Einführung eines neuen Service-VAU-Typs informieren und ggf. für diesen neuen Service-VAU-Typ zu erfüllende Rahmenbedingungen abstimmen.**[<=]**

Hinweis zu A_26124-*: Hierzu gehört z.B. auch die Festlegung der maximalen Lebensdauer für den neuen Service-VAU-Typ (siehe A_26123-*).

A_26125 -ePA-Aktensystem - Starten ausschließlich attestierter Service-VAUs
Das ePA-Aktensystem MUSS sicherstellen, dass ausschließlich attestierte Service-VAU-Instanzen gestartet werden können.**[<=]**

3.4.4.1 Zusätzliche Anforderungen an eine Zusatzfunktion-Service-VAU

Zusatzfunktion-Service-VAUs sind eine Ausprägung von Service-VAUs zur isolierten Ausführung von backendseitigen Zusatzfunktionen.

A_30472 -ePA-Aktensystem - ZF-Service-VAU - Zusatzfunktion-Service-VAUs ausschließlich für Zusatzfunktionen
Das ePA-Aktensystem MUSS sicherstellen, dass in Zusatzfunktion-Service-VAUs ausschließlich backendseitige Zusatzfunktionen ausgeführt werden.**[<=]**

A_30473 -ePA-Aktensystem - ZF-Service-VAU - Isolated Workspace für eine ZF
Das ePA-Aktensystem MUSS sicherstellen, dass in einem Isolated-Workspace einer Zusatzfunktion-Service-VAU nicht mehrere Zusatzfunktionen ausgeführt werden.**[<=]**

A_30474 -ePA-Aktensystem - ZF-Service-VAU - Maximale Labensdauer
Das ePA-Aktensystem MUSS sicherstellen. dass die Instanzen einer Zusatzfunktion-Service-VAU nach maximal 26 Stunden beendet werden.**[<=]**

Zusatzfunktion-Service-VAUs besitzen die Eigenschaften einer Service-VAU. Es gibt allerdings folgende Abweichung: Ein Isolated Workspace in einer ZF-Service-VAU kann abweichend von A_26115-* mehr als einen Request einer AK-VAU verarbeiten.

A_30475 -ePA-Aktensystem - ZF-Service-VAU - Isolated Workspace verarbeitet mehrere Requests einer AK-VAU
Das ePA-Aktensystem MUSS sicherstellen, dass ein Isolated-Workspace in einer Zusatzfunktion-Service-VAU mehr als einen Request des ZF-Managers einer AK-VAU zu einer Akte verarbeiten kann, ohne dass der Isolated Workspace gelöscht wird.**[<=]**

3.4.4.2 Kommunikation zwischen AK-VAU und Service-VAU

A_26126 -ePA-Aktensystem - Gesicherte und authentisierte Verbindung zwischen AK-VAU- und Service-VAU-Instanzen
Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer Aktenkontoverwaltungs-VAU-Instanz und einer Service-VAU-Instanz eine beidseitig authentisierte und vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen.**[<=]**

A_26127 -ePA-Aktensystem - Kein Kommunikationsaufbau von Service-VAU-Instanzen zu AK-VAU-Instanzen
Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine Kommunikation zu einer AK-VAU-Instanz aufbauen kann.**[<=]**

A_26128-01 -ePA-Aktensystem - Kein Aufruf von Schnittstellen von AK-VAU-Instanzen durch Service-VAU-Instanzen
Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine Schnittstellen/Services aufrufen kann, die in einer AK-VAU-Instanz ausgeführt werden, sofern es sich nicht um eine Zusatzfunktion-Service-VAU-Instanz handelt, die den ZF-Manager aufruft.**[<=]**

3.4.5 Temporäres Speichern von Daten und spätere Aufnahme ins Aktenkonto

Eine VAU-Instanz (AK-VAU oder Service-VAU) kann Daten von Versicherten zwischenspeichern ("einfrieren"), damit diese zu einem späteren Zeitpunkt von einer Aktenkontoverwaltungs-VAU in das Aktenkonto des Versicherten aufgenommen werden können. Dies ist insbesondere für Ergebnisse von Service-VAUs vorgesehen, für deren Erstellung die Service-VAU länger benötigt und somit die Ergebnisse nicht mehr direkt an die User Session der aufrufenden Aktenkontoverwaltungs-VAU zurückgegeben werden können. Eingefrorene Daten dürfen nur in das Aktenkonto aufgenommen werden, wenn dies keine Protokollierung für den Versicherten erfordert.

Ein Beispiel ist die Erstellung eines Indexes für die Volltextsuche als Ergebnis des Einstellens eines neuen Dokuments durch einen Nutzer. Die Erstellung des Indexes erfolgt in einer Service-VAU und der erstellte Index wird von der Service-VAU

zwischengespeichert abgelegt ("eingefroren"). Eine Aktenkontoverwaltungs-VAU pflegt den abgelegten Index dann zu einem späteren Zeitpunkt in die Akte ein. Das Aktualisieren des Indexes erfordert keine Protokollierung für den Versicherten. Für ihn wurde das Einstellen des Dokuments protokolliert, die Aktualisierung des Indexes ist eine technische Folge dieses Zugriffs.

Temporäres Zwischenspeichern ("Einfrieren") von Daten

Die folgende Abbildung beschreibt das Einfrieren von Daten durch eine AK-VAU. Ein Nutzer hat ein Aktenkonto geöffnet, um z.B. ein neues Dokument einzustellen. Der Health Record Context für das Konto ist gestartet und enthält den versichertenindividuellen Datenpersistierungsschlüssel des Kontos. Die AK VAU friert die zwischenzuspeichernden Daten und den versichertenindividuellen Datenpersistierungsschlüssel des Kontos mit Hilfe der VAU-HSM-Regel *kr6* ein.

Damit die im Aktensystem gespeicherten verschlüsselten Daten einem Konto zugeordnet werden können, der Betreiber des ePA-Aktensystems daraus jedoch keine Profile über Versicherte erstellen kann, werden die Chiffrate nicht der KVNR des Kontos, sondern einem Akten-Pseudonym zugeordnet, welches ausschließlich innerhalb der VAU aufgelöst werden kann. Die AK-VAU erzeugt das Akten-Pseudonym.

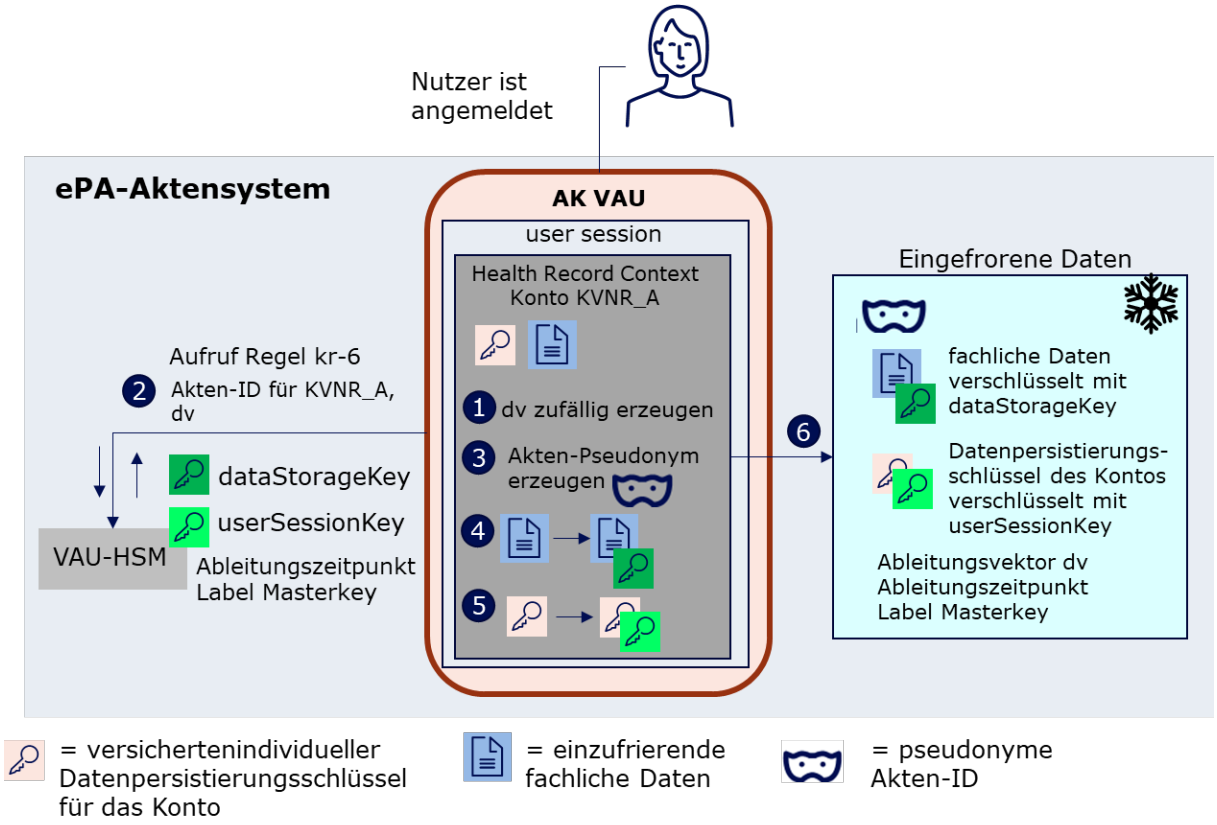


Abbildung 5: Einfrieren von Daten durch eine AK-VAU

A_28767 -ePA-Aktensystem - Einfrieren von Daten durch eine AK-VAU
Falls eine Aktenkontoverwaltungs-VAU Daten *data_kvnr* eines Aktenkontos KVNR temporär speichern ("einfrieren") möchte, MUSS die Aktenkontoverwaltungs-VAU

1. einen zufälligen Ableitungsvektor *dv* mit 120 Bit Entropie erzeugen,
2. mittels VAU-HSM-Regel *kr6*, dem erzeugten Ableitungsvektor *dv* aus 1., einer eindeutigen Akten-ID für die KVNR des Aktenkontos (die KVNR selbst oder ein aktenspezifisches Pseudonym) und dem aktuellen Datenpersistierungs-Masterkey die Schlüssel *dataStorageKey* und *userSessionKey* ableiten (Hinweis: Es darf in der Regel

kr6 kein Eingabezeitpunkt übergeben werden, da für die Ableitung der Schlüssel der aktuelle Zeitpunkt im VAU-HSM genutzt werden muss),

3. ein Akten-Pseudonym erzeugen

und

4. die Daten *data_kvnr* mit dem *dataStorageKey* mittels AES/GCM verschlüsseln,
5. den im Health Record Context des Kontos KVNR vorliegenden versichertenindividuellen Datenpersisitierungsschlüssel mit dem *userSessionKey* mittels AES/GCM verschlüsseln,
6. die Chiffrate mit folgenden Metainformationen speichern (die Metainformationen dürfen die KVNR nicht enthalten):
   a. Akten-Pseudonym
   b. Ableitungsvektor dv aus 1,
   c. Label des genutzten Masterkeys (Ergebnis der Regel *kr6*),
   d. Ableitungszeitpunkt (Ergebnis der Regel *kr6*).

[<=]

Auch eine Service-VAU kann Daten temporär speichern (vgl. folgende Abbildung). Da nur die AK-VAU die benötigten Schlüssel vom VAU-HSM abrufen kann, müssen die benötigten Informationen der Service-VAU von der AK-VAU im Service-Request übermittelt werden. Der versichertenindividuelle Datenpersisitierungsschlüssel darf nicht unverschlüsselt an eine Service-VAU übermittelt werden.

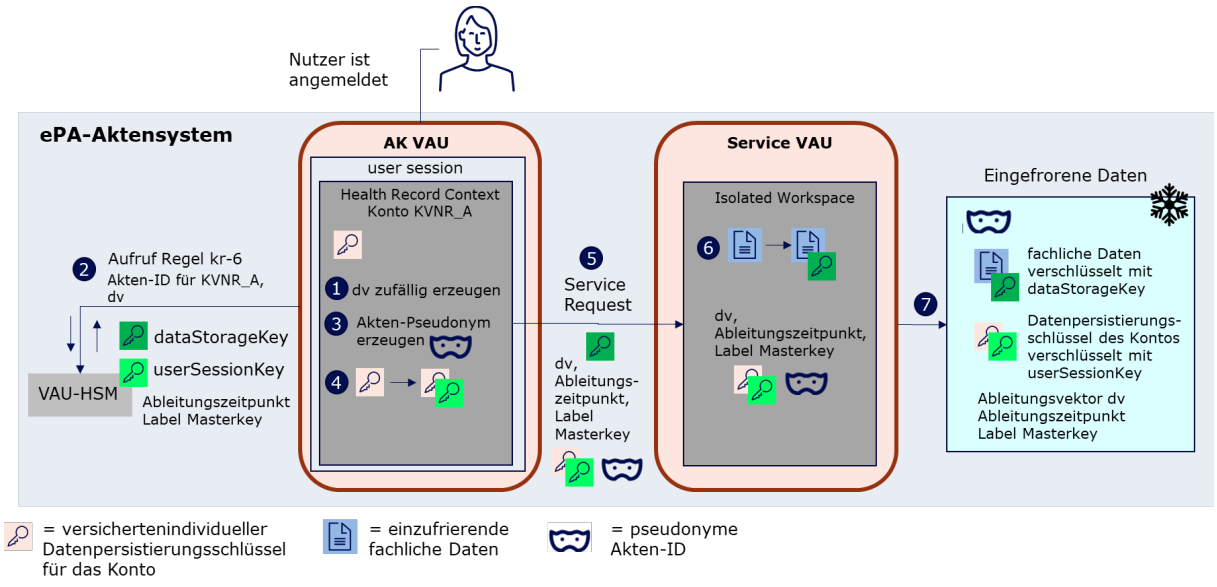


Abbildung 6: Einfrieren von Daten durch eine Service-VAU

A_28768 -ePA-Aktensystem - Einfrieren von Daten durch eine Service-VAU
Falls eine Aktenkontoverwaltungs-VAU einer Service-VAU die Speicherung von Daten bzgl. eines Aktenkontos KVNR ermöglichen will, MUSS die Aktenkontoverwaltungs-VAU

1. einen zufälligen Ableitungsvektor *dv* mit 120 Bit Entropie erzeugen,
2. mittels VAU-HSM-Regel *kr6*, dem erzeugten Ableitungsvektor dv aus 1., einer eindeutigen Akten-ID für die KVNR des Aktenkontos (die KVNR selbst oder ein aktenspezifisches Pseudonym) und dem aktuellen Datenpersistierungs-Masterkey die Schlüssel *dataStorageKey* und *userSessionKey* ableiten (Hinweis: Es wird der Regel

kr6 kein Eingabezeitpunkt übergeben, da für die Ableitung der Schlüssel der aktuelle Zeitpunkt im VAU-HSM genutzt werden muss),

3. ein Akten-Pseudonym erzeugen,
4. den im Health Record Context des Kontos KVNR vorliegenden versichertenindividuellen Datenpersisitierungsschlüssel mit dem *userSessionKey* mittels AES/GCM verschlüsseln

und der Service-VAU im Service-Request folgende Informationen übermitteln:

- *dataStorageKey aus 2*
- *Akten-Pseudonym aus 3,*
- Ableitungsvektor dv aus 1.
- Label des genutzten Masterkeys (Ergebnis der Regel *kr6*),,
- den Ableitungszeitpunkt (Ergebnis der Regel *kr6*),
- den verschlüsselten versichertenindividuellen Datenpersisitierungsschlüssel aus 4..

[<=]

Wurden der Service-VAU in einem Service-Request von der AK-VAU Informationen für die Speicherung übermittelt, kann die Service-VAU für diesen Service-Request Daten im ePA-Aktensystem temporär zwischenspeichern ("einfrieren"). Für die Verschlüsselung der Daten darf die Service-VAU ausschließlich den von der AK-VAU übermitteltendataStorageKey nutzen.

A_28769 -ePA-Aktensystem - Verschlüsselte Speicherung durch Service-VAU mit von AK-VAU übermittelten Schlüssel
Falls Daten, die im Rahmen eines durch eine AK-VAU erzeugten Service-Requests in der Service-VAU verarbeitet werden, außerhalb der Service-VAU gespeichert werden sollen, MUSS die Service-VAU sicherstellen, dass

1. die Daten mit dem von der AK-VAU im Rahmen des Service-Requests übermittelten *dataStorageKey* verschlüsselt abgespeichert werden und
2. dem Chiffrat folgende von der AK-VAU im Service-Request übermittelte Informationen angefügt werden (die Informationen dürfen die KVNR nicht enthalten):
   - das Akten-Pseudonym,
   - der für die Ableitung des *dataStorageKeys* genutzte Ableitungsvektor *dv*,
   - das Label des für die Ableitung genutzten Masterkeys,
   - Ableitungszeitpunkt,
   - den mit dem *userSessionKey* verschlüsselten versichertenindividuellen Datenpersisitierungsschlüssel.

[<=]

Auftauen von Daten

Die Aufnahme der temporär gespeicherten ("eingefrorenen") Daten in ein Aktenkonto erfolgt durch eine Aktenkontoverwaltungs-VAU. Service-VAUs dürfen keine Daten in Aktenkonten speichern (vgl. A_26119-*). Die hierfür benötigte AK-VAU-Instanz kann vom Betreiber des Aktensystems gestartet werden, d.h. die Aufnahme der eingefrorenen Daten in ein Aktenkonto ist unabhängig davon, wann Nutzer auf Aktenkonten zugreifen. Für die Schnittstelle, über die der Betreiber das Auftauen startet, sind die Anfoderungen aus A_28805-* und A_28807-* zu berücksichtigen.

Die folgende Abbildung beschreibt das Auftauen von eingefrorenen Daten.

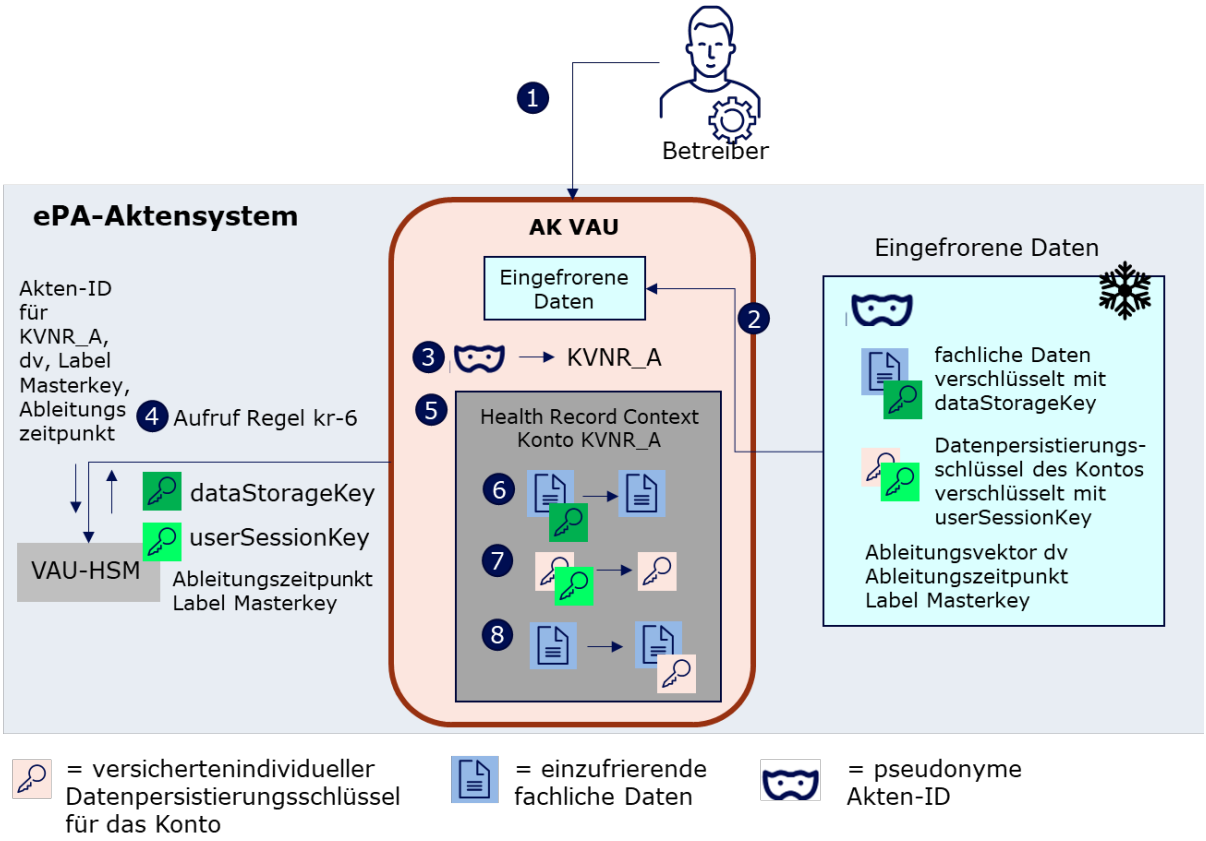


Abbildung 7: Auftauen von eingefrorenen Daten

1. Der Betreiber startet eine AK-VAU-Instanz.
2. Die gestartete AK-VAU-Instanz lädt die im Aktensystem gespeicherten eingefrorenen Daten (Chiffrate inkl. Metainformationen) in die AK-VAU-Instanz.
3. In der AK-VAU-Instanz wird das Akten-Pseudonym zu der Akten-ID (z.B. zur KVNR) aufgelöst.
4. Die AK-VAU ruft VAU-HSM-Regel *kr6* mit der Akten-ID und dem in den Metainformationen enthaltenem Ableitungsvektor *dv* , dem Label des Masterkeys und dem Ableitungszeitpunkt auf. Es werden der *dataStorageKey* und der *userSessionKey* vom VAU-HSM abgeleitet.
5. EinHealth Record Context für die Akte zur Akten-ID wird in der AK-VAU geöffnet.
6. Im Health Record Context werden die verschlüsselten fachlichen Daten mit dem *dataStorageKey* entschlüsselt.
7. Im Health Record Context wird der verschlüsselte versichertenindividuelle Datenpersistierungsschlüssel mit dem *userSessionKey* entschlüsselt.
8. Mit dem versichertenindividuellen Datenpersistierungsschlüssel werden die zwischengespeicherten Daten verschlüsselt und in der Akte gespeichert.

A_28770 -ePA-Aktensystem - Keine Protokollierungserfordernis der Aufnahme von gespeicherten Daten ins Aktenkonto
Der Hersteller des ePA-Aktensystems MUSS sicherstellen, dass eine Aktenkontoverwaltungs-VAU temporär gespeicherte (eingefrorene) Daten in ein Aktenkonto nur dann aufnimmt, wenn die dafür notwendigen Zugriffe nicht für den Versicherten protokolliert werden müssen.**[<=]**

Bis eingefrorene Daten von einer AK VAU aufgetaut und in das Aktenkonto eingebracht werden, könnten weitere Zugriffe auf das Aktenkonto erfolgen., die ggf. ebenfalls dazu führen, dass Daten für das Konto eingefroren werden. Ein Beispiel ist das Einfrieren eines neu erstellen Indexes für die Volltextsuche aufgrund eines eingestellten Dokuments. Hier könnten Nutzer neue Dokumente einstellen, nachdem ein Index eingefroren wurde aber bevor dieser eingepflegt wurde. Die AK-VAU muss dann beim Auftauen die verschiedenen Indexe zusammenführen, um einen konsistenten Aktenzustand zu erreichen.

A_28804 -ePA-Aktensystem - Kein inkonsistenter Aktenzustand durch das Einbringen eingefrorener Daten
Das ePA-Aktensystens MUSS sicherstellen, dass durch das Einbringen eingefrorener Daten kein inkonsistenter Aktenzustand entsteht.**[<=]**

Das Löschen der ziwschengespeicherten Chiffrate erfolgt nach Aufnahme der Daten in das Aktenkonto.

A_28771 -ePA-Aktensystem - Löschen nach Aufnahme von gespeicherten Daten ins Aktenkonto
Das ePA-Aktensystem MUSS sicherstellen, dass nach erfolgreicher Übernahme der temporär gespeicherten (eingefrorenen) Daten

- der Health Record Context in der AK-VAU sofort geschlossen wird,
- der *dataStorageKey* und der *userSessionKey* sofort gelöscht werden,
- die Chiffrate mitsamt aller Metainformationen sofort im ePA-Aktensystem gelöscht werden.

[<=]

A_28772 -ePA-Aktensystem - Schnellstmögliche Aufnahme eingefrorener Ergebnisdaten
Der Hersteller des ePA-Aktensystems MUSS sicherstellen, dass das ePA-Aktensystem eingefrorene Daten, die direkt in die Akte eingepflegt werden können, schnellstmöglich in die Akte einpflegt.**[<=]**

Hinweis zu A_28772-*: Ein Beispiel für Daten, die unter die Anforderung A_28772-* fallen, ist der eingefrorene Index als Ergebnis einer langlaufenden Indexierung bei der Volltextsuche. Der Index kann direkt in die Akte eingepflegt werden und benötigt keine weiteren Verarbeitungen. Wird hingegen der Auftrag der Indexierung eingefroren, um die Indexierung später auszuführen, fallen diese "Auftragsdaten" nicht unter die A_28772-*.

3.5 Umschlüsselung

Das Kerckhoffs'sche Prinzip von 1883 ist ein Grundpfeiler der Kryptographie. Es besagt u. a. dass die Sicherheit von kryptographischen Verfahren alleinig von der Geheimhaltung der Schüssel abhängen darf, und dass Schlüssel leicht auswechselbar sein müssen. Damit kryptographische Schlüssel in der Praxis ihre Sicherheitseigenschaft behalten können müssen sie einen Lebenszyklus besitzen (vgl. bspw. [NIST-SP-800-57P1]), der den regelmäßigen Austausch (Wechsel) der Schlüssel vorsieht und umsetzt. Aus diesem Grunde werden die Masterkeys für Aktendaten und die Masterkeys für Befugnisse regelmäßig erneuert (vgl. A_15745-* und A_20519-* (beide aus [gemSpec_Krypt])). Bei dieser Erneuerung muss eine Umschlüsselung durchgeführt werden:

- Schlüssel_alt_KVNR = Ableitung (MK_alt, KVNR),
- Schlüssel_neu_KVNR = Ableitung (MK_neu, KVNR),
- Umschlüsselung pro Akte: Schlüssel_alt_KVNR -> Schlüssel_neu_KVNR.

Es liegt in der Verantwortung des Anbieters des ePA-Aktensystems, d.h. des Kostenträgers, eine Umschlüsselung für die Aktenkonten seiner Versicherten entsprechend der zeitlichen Vorgabe der Anforderung A_20519-* auszulösen. Den genauen Zeitpunkt der Umschlüsselung innerhalb des Zeitrahmens kann der Kostenträger zusammen mit dem Betreiber des ePA-Aktensystems abstimmen, um die Belastung des Aktensystems durch die Umschlüsselungsprozesse geeignet zu steuern.

A_28773 -Anbieter ePA-Aktensystem - Auslösen der Umschlüsselung durch Kostenträger
Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass für die Aktenkonten aller Versicherten des Anbieters in dem durch A_20519-* vorgegebenen Zeitrahmen eine Umschlüsselung ausgelöst wird.**[<=]**

A_28774 -ePA-Aktensystem - Schnittstelle zum Auslösen der Umschlüsselung
Das ePA-Aktensystem MUSS dem Kostenträger eine Schnittstelle anbieten, über die der Kostenträger eine Umschlüsselung für die Konten des Kostenträgers auslösen kann.**[<=]**

A_28775 -ePA-Aktensystem - Auslösen der Umschlüsselung nur für Versicherte des Kostenträghers
Das ePA-Aktensystem MUSS sicherstellen, dass ein Kostenträger eine Umschlüsselung ausschließlich für die Konten von Versicherten auslösen kann, die beim Kostenträger versichert sind.**[<=]**

A_28776 -ePA-Aktensystem - Aktenstatus INACCESSIBLE während der Umschlüsselung
Löst der Kostenträger über die vom Aktensystem bereitgestellte Schnittstelle die Umschlüsselung für ein Aktenkonto aus, MUSS das ePA-Aktensystem den Aktenstatus des Aktenkontos auf INACCESSIBLE mit Ursache Umschlüsselung setzen bzw. für ein Aktenkonto im Zustand *INACCESSIBLE* die Umschlüsselung als weitere Ursache für den Verbleib im Aktenstatus *INACCESSIBLE* ergänzen.**[<=]**

A_28777 -ePA-Aktensystem - Rücksetzen des Aktenstatus nach Beendigung der Umschlüsselung
Nachdem die Umschlüsselung für ein Aktenkonto vom ePA-Aktensystem erfolgreich durchgeführt wurde, MUSS das ePA-Aktensystem die Ursache der Umschlüsselung aus den Ursachen des Status INACCESSIBLE enttfernen. **[<=]**

A_28806 -ePA-Aktensystem - Keine Umschlüsslung wenn Konto von Nutzern genutzt wird
Das ePA-Aktensystem MUSS sicherstellen, dass während ein Konto umgeschlüsselt wird, kein Nutzer dieses Konto geöffnet hat.**[<=]**

A_26199-01 -ePA-Aktensystem - Notfall-Aktivierung Umschlüsselung
Ein ePA-Aktensystem MUSS sicherstellen, dass das ePA-Aktensystem es einem ePA-Betreiber ermöglicht eine Erneuerung der betreiberspezifischen Schlüssel zu starten/aktivieren. Es MUSS also dem ePA-Betreiber möglich sein neben der regelmäßigen Erneuerung der betreiberspezifischen Schlüssel (A_20519-*) eine Erneuerung zu initiieren.
[<=]

Nach A_20519-* muss es jährlich eine Schlüsselerneuerung geben. Mit 26199-* kann ein ePA-Betreiber im Notfall sozusagen den Zyklus "beschleunigen" -- ein neues Intervall sofort einleiten/erzeugen.

A_28778 -Anbieter ePA-Aktensystem - Auslösen der Umschlüsselung durch Kostenträger
Der Anbieter des ePA-Aktensystems MUSS bei einer unplanmäßigen Erneuerung der betreiberspezifischen Schlüssel gemäß A_26199-* eine Umschlüsselung der Konten der Versicherten des Kostenträgers innerhalb von 1 Woche auslösen.**[<=]**

A_26223-01 -ePA-Aktensystem - Metadaten von ePA-spezifischen Chiffraten

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

A_28791 -Anbieter ePA-Aktensystem - Löschen von Masterkeys für Daten- bzw. Befugnispersistierungsschlüssel aus dem VAU-HSM
Der Anbieter des ePA-Aktensystems MUSS einen Masterkey für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel bzw. einen Masterkey für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel aus dem VAU-HSM löschen, falls keine Chiffrate mehr im ePA-Aktensystem existieren, die auf Basis des Masterkeys verschlüsselt wurden. Hierzu gehören auch die Chiffrate in Backups.
[<=]

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.

Außerdem werden im Consent Decision Management die Einschränkungen der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke durch das Forschungsdatenzentrum Gesundheit verwaltet (siehe3.7.2- Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke).

Der Widerspruch gegen die grundsätzliche Nutzung der ePA wird nicht im Consent Decision Management berücksichtigt. Die Existenz eines Aktenkontos für einen Versicherten impliziert, dass kein Widerspruch gegen die Nutzung der ePA erteilt wurde. Der Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger

wird ebenfalls nicht hier verwaltet (siehe zu beiden Widersprüchen auch3.1.1- Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte).

3.7.1 Widersprüche für Funktionen der ePA

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

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

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

Die Information über relevante erteilte oder nicht erteilte Widersprüche können Clients auf einfache Weise (ohne Authentisierung oder Etablierung eines VAU-Kanals) im Vorfeld einer Operation über den Information Service abfragen (siehe auch 3.14- Information Services).

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

Das Aktenkonto unterstützt die Durchsetzung eines erteilten Widerspruchs überall dort, wo Aktivitäten dediziert als Teil einer widerspruchsfähigen Funktion zugeordnet werden können. Beispielsweise wird das Einstellen neuer Verordnungs- und Dispensierdaten in die Ordner der Kategorie "medication" immer verhindert, wenn der Teilnahme am digital gestützten Medikationsprozess widersprochen wurde. Die konkreten Auswirkungen eines Widerspruchs sind in den jeweiligen Kapiteln zur Handhabung von Dokumenten und Daten des Aktenkontos dargestellt (siehe3.12.1- XDS Document Service und 3.12.2- FHIR Data Services) .

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

A_23874-01 -Consent Decision Management - Definition der widerspruchsfähigen Funktionen der ePA
Das Consent Decision Management MUSS die Attribute zu widerspruchsfähigen Funktionen der ePA gemäß der folgenden Tabelle verwenden.

Tabelle 8: Widerspruchsfähige Funktionen der elektronischen Patientenakte

Funktion (name)	Funktionsklasse (consent class)	Id der Funktion (id)	Entscheidung (consent decision)

Teilnahme am digital gestützten Medikationsprozess	Versorgungsprozess ("healthCareProcess")	"medication"	"deny"/"permit"
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst	Versorgungsprozess ("healthCareProcess")	"erp-submission"	"deny"/"permit"
Sekundärdatennutzung durch das Forschungsdatenzentrum Gesundheit	Sekundärdatennutzung ("secondaryDataUsage")	"data-submission"	"deny"/"permit"

[<=]

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

Hinweis: Die Verwaltung der Widersprüche gegen die Nutzung des Aktenkontos durch eine spezifische Leistungserbringerinstitution erfolgt über die Befugnisverwaltung (siehe 3.8.4- Befugnisausschluss (Blocked User Policy)).

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

A_25300 -Consent Decision Management - Untereinander abhängige Entscheidungen zu Widersprüchen
Das Consent Decision Management MUSS durch interne Maßnahmen sicherstellen, dass bei Erteilung eines Widerspruchs gegen die Nutzung der Funktion der elektronischen Patientenakte 'erp-submission' ('deny') auch der Widerspruch gegen die Nutzung der Funktion 'medication' gesetzt wird ('deny') und dass bei der Rücknahme ('permit') des Widerspruchs gegen die Nutzung der Funktion 'medication' auch der Widerspruch gegen die Nutzung der Funktion 'erp-submission' zurückgenommen wird.**[<=]**

Hinweis zu A_25300: Die Änderung der Entscheidung zur Nutzung der "führenden" Funktion hat automatisch eine Entscheidung zur Nutzung der "abhängigen" Funktion zur Folge. Dieses gilt nur für die aufgeführten Entscheidungsänderungen. Alle weiteren, nicht aufgeführten, Änderungen zu Entscheidungen haben keine "abhängige" Auswirkung auf weitere Entscheidungen zu Funktionen. Beispiel: Wird die Entscheidung für 'medication'' von 'permit' auf 'deny' gesetzt, so hat dieses keine weiteren Änderungen an Entscheidungen zur Folge.*

A_23766-01 -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 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.
Der Entscheidung MUSS als Zeitpunkt der Initialisierung der feste Wert "2025-01-15T00:00:00Z" und als Akteur "system" zugeordnet werden.
[<=]

A_28043 -Consent Decision Management - Initialisierung der Widerspruchsinformation zur Sekundärdatennutzung (PKV)
Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen bezüglich der Sekundärdatennutzung bei Erstellung eines neuen Aktenkontos mit "deny"

initialisieren, wenn die Akte durch einen Kostenträger verantwortet wird, für den gesetzlich keine Sekundärdatennutzung vorgesehen ist.**[<=]**

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 SchnittstelleI_Information_Service.

A_23824 -Aktensystem - Realisierung der Schnittstelle I_Consent_Decision_Management
Das ePA-Aktensystem MUSS die Operationen der Schnittstelle `I_Consent_Decision_Management`gemäß [I_Consent_Decision_Management] umsetzen.
[<=]

A_23919 -Consent Decision Management - unveränderte Übernahme der Widerspruchsentscheidung
Das Consent Decision Management MUSS die über Operationen der Schnittstellen des Consent Managements übermittelten Entscheidungen (consent decisions) zu widerspruchsfähigen Funktionen der ePA in das Aktenkonto übernehmen. Die Entscheidungen zu den in den Operationen nicht adressierten widerspruchsfähigen Funktionen MÜSSEN im Aktenkonto unverändert bleiben.**[<=]**

A_24844 -Consent Decision Management - Information über Änderungen der Widerspruchsinformation
Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung einer Widerspruchsinformation, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber informieren, dass Widerspruchsinformationen geändert wurden, wann die

Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind.**[<=]**

3.7.2 Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke

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

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

Eine Änderung der Widersprüche zu Verwendungszwecken führt dazu, dass diese Informationen an das Forschungsdatenzentrum Gesundheit übermittelt werden. Die Widersprüche des Versicherten in die Sekundärnutzungszwecke sind dort bindend für die Verarbeitung der übermitteltenpseudonymisierten medizinischen Daten, siehe auch 3.19-Data Submission Service .

A_26286-01 -Consent Decision Management - Initialisierung der Sekundärnutzungszwecke
Das Consent Decision Management MUSS jeden in § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszweck der elektronischen Patientenakte bei Erstellung eines neuen Aktenkontos mit der Entscheidung "kein Widerspruch erklärt" ("permit") initialisieren. Der Entscheidung MUSS als Zeitpunkt der Initialisierung der feste Wert "2025-01-15T00:00:00Z" und als Akteur "system" zugeordnet werden.**[<=]**

A_28044-01 -Consent Decision Management - Initialisierung der Sekundärnutzungszwecke (PKV)
Das Consent Decision Management MUSS jeden in § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszweck der elektronischen Patientenakte bei Erstellung eines neuen Aktenkontos mit "deny" initialisieren,wenn die Akte durch einen Kostenträger verantwortet wird, für den gesetzlich keine Sekundärdatennutzung vorgesehen ist. Der Entscheidung MUSS als Zeitpunkt der Initialisierung der feste Wert "2025-01-15T00:00:00Z" und als Akteur "system" zugeordnet werden.**[<=]**

A_26287 -Consent Decision Management - Speichern der Entscheidungen zu Sekundärnutzungszwecken
Das Consent Decision Management MUSS die Entscheidungen zu Sekundärnutzungszwecken der elektronischen Patientenakte unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.**[<=]**

A_26288 -Consent Decision Management - Übertragen der Entscheidungen zu Sekundärnutzungszwecken an das FDZ
Das Consent Decision Management MUSS die Entscheidungen zu Sekundärnutzungszwecken sofort im Anschluss an eine Änderung der Entscheidung im Consent Decision Management in das Paket zur Übermittlung von pseudonymisierten medizinischen Daten zu Sekundärnutzungszwecken an das FDZ aufnehmen.**[<=]**

A_26291 -Consent Decision Management - unveränderte Übernahme der Widerspruchsentscheidung zu Sekundärnutzungszwecken
Das Consent Decision Management MUSS die über Operationen der Schnittstellen des Consent Managements [I_Consent_Decision_Management] übermittelten Entscheidungen zuSekundärnutzungszwecken in das Aktenkonto übernehmen.**[<=]**

A_26292 -Consent Decision Management - Information über Änderungen der Entscheidungen zu Sekundärnutzungszwecken

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

A_26294 -Consent Decision Management – Weiterleitung von Widersprüchen gegen Sekundärnutzungszwecken an das FDZ
Das Consent Decision Management MUSS die Information über einen erklärten Widerspruch gegen Sekundärnutzungszwecke über den Data Submission Service an das FDZ weiterleiten.**[<=]**

A_26310 -Consent Decision Management – Rücknahme des Widerspruchs gegen die Sekundärdatennutzung durch das FDZ
Falls ein Widerspruch gegen die Sekundärdatennutzung durch das FDZ zurückgenommen wird MUSS das Consent Decision Management die Entscheidungen zu Sekundärnutzungszwecken über den Data Submission Service an das FDZ weiterleiten. **[<=]**

A_26293 -Consent Decision Management – Weiterleitung von Widersprüchen gegen die Sekundärdatennutzung durch das FDZ
Das Consent Decision Management MUSS die Information über einen erklärten Widerspruch gegen die Sekundärdatennutzung durch das FDZ über den Data Submission Service an das FDZ weiterleiten.**[<=]**

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

Ein Versicherter bzw. Vertreter kann den Zugriff auf den Medication Service für bestimmte LEI innerhalb seines Aktenkontos einschränken und diese Einschränkung auch wieder zurücknehmen. Durch das Setzen einer LEI auf eine User Specific Deny Policy Medication wird jeder Zugriff dieser LEI auf den Medication Service und auf die Dokumente der Kategorie "emp" des Document Service für das Aktenkonto mit einem Fehler abgebrochen. Durch das Entfernen einer LEI von der User Specific Deny Policy Medication kann diese LEI Operationen des Medication Service (falls kein Widerspruch gegen "medication" vorliegt) wieder nutzen und auf die Dokumente der Kategorie "emp" des Document Service zugreifen.
Die User Specific Deny Policy Medication wird durch das Aktensystem für die in A_26406-* aufgeführten Nutzergruppen angewendet und durchgesetzt.

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

A_26400 -Consent Decision Management - Initialisierung der User Specific Deny Policy Medication
Das Consent Decision Management MUSS für ein Aktenkonto eine User Specific Deny Policy Medication ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policy über die Schnittstelle `I_Consent_Decision_Management` gemäß [I_Consent_Decision_Management] ermöglichen.**[<=]**

A_26401 -Consent Decision Management - Speichern der Inhalte der User Specific Deny Policy Medication
Das Consent Decision Management MUSS Einträge aus der User Specific Deny Policy Medication unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.**[<=]**

A_26403 -Consent Decision Management - Information über Änderungen der User Specific Deny Policy Medication
Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung der Entscheidungen zu der User Specific Deny Policy Medication , sofern eine E-Mail-Adresse

vorliegt, mit einer E-Mail darüber informieren, welche Änderungen der User Specific Deny Policy Medication vorgenommen wurden, wann die Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind.**[<=]**

A_26406-01 -Consent Decision Management - Policy für berechtigte Nutzergruppen und Nutzer
Das Consent Decision Management MUSS die Konfiguration der User Specific Deny Policy Medication auf die folgenden Nutzergruppen einschränken:

Tabelle 9: Nutzergruppen der User Specific Deny Policy Medication

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

[<=]

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_23734-01 -Entitlement Management - Definition einer Befugnis
Das Entitlement Management MUSS für eine individuelle Befugnis die folgenden Daten nutzen und verwalten:

Tabelle 10: 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 und Zeitpunkt (letzter Tag der Gültigkeit, d.h. eine heutige Befugnisvergabe für 3 Tage setzt für validTo das Datum von übermorgen (aktueller Tag + 2 Tage). aktueller Tag ist inklusiv zu bewerten).	Wird gemäß [RFC3339] mit Zeitzone UTC (z.B.: 2024-04-12T22:59:59Z) bzw. Zeitzonen-Offset (z.B.: 2024-04-12T23:59:59+01:00) gespeichert. Eine unbegrenzt gültige Befugnis erhält das Datum 9999-12-31T00:00:00Z. . Die Befugnisdauer der Befugnisse (Karte stecken), die durch das Aktensystem erstellt werden, werden auf das Ende des resultierenden Tages der aktuell gültigen Zeitzone in Deutschland gesetzt, z.B.: 2024-04-12T23:59:59+01:00. Wird durch den Versicherten oder einen Vertreter oder das Entitlement Management	ja

		gesetzt.	
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_23941-01 -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 11: 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_praxis-ergotherapeut	x	x	-	90	var
oid_praxis-logopaede	x	x	-	90	var
oid_praxis-podologe	x	x	-	90	var
oid_praxis-ernaehrungstherapeut	x	x	-	90	var
oid_institution-oegd	x	x	-	3	var
oid_institution-arbeitsmedizin	x	x	-	3	var
oid_kostentraeger	-	-	x (statisch)	-	-
oid_ombudsstelle	-	-	x (statisch)	-	-
oid_erp-vau (E-Rezept vertrauenswürdige Ausführungsumgebung)	-	-	x (statisch)	-	-
oid_versicherter (Versicherter)	-	-	x (statisch)	-	-
oid_versicherter (Vertreter)	-	x	-	-	dauerhaft
oid_diga	-	x	-	-	dauerhaft

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

LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-Prüfungsnachweis (Prüfziffer),
FdV = Versicherter oder Vertreter,
KTR = Kostenträger
AS = Aktensystem (systemseitig erteilte Befugnisse)
Tage = Gültigkeit in Tagen: angegebener Wert ist einschließlich aktuellem Datum, z. B. 90 Tage bedeutet aktuelles Datum + 89 Tage.
dauerhaft = Befugnis unbegrenzt gültig (Enddatum = 9999-12-31)
statisch = Gültigkeit analog 'dauerhaft', Befugnis ist implizit vorhanden.
var = Gültigkeitsdauer von 1 Tag bis dauerhaft in jeweils ganzen Tagen**[<=]**

Befugnisse werden durch dasEntitlement Management mit dem SecureAdminStorageKey verschlüsselt und im Aktenkonto gesichert abgelegt.

Einzelne Nutzer können durch den Versicherten, einen befugten Vertreter oder die Ombudsstelle explizit von der Befugnisvergabe ausgeschlossen sein (siehe 3.8.4-Befugnisausschluss (Blocked User Policy)). Eine Befugniserstellung ist dann weder für Leistungserbringerinstitutionen in einer Behandlungssituation, noch durch den Versicherten oder einen Vertreter möglich.

Die Befugnisse für den Versicherten und den E-Rezept-Fachdienst werden dabei nicht persistiert. Diese Befugnisse werden als implizit vorhanden und gültig angenommen.

Eine Besonderheit stellt hierbei eine Befugnis EU-Zugriff dar. Es gibt zu einem Zeitpunkt für ein Aktenkonto maximal eine Befugnis EU-Zugriff. Die Dauer dieser Befugnis wird durch das Aktensystem festgelegt und beträgt 1 Stunde. Das Ende der Gültigkeit (validTo) wird ermittelt vom Ausstellungszeitpunkt + 1 Stunde.

A_26167 -Entitlement Management (EU) - Erteilung der Befugnis EU-Zugriff
Das Entitlement Management MUSS die Erteilung einer Befugnis EU-Zugriff in der jeweiligen Umgebung zusätzlich zu A_23941-* auf die folgenden Nutzergruppen und Nutzer einschränken:

Tabelle 12: Befugnisse EU-Zugriff für berechtigte Nutzergruppen und Nutzer

professionOID / Nutzergruppe und Nutzer	**Umgebung**			**Standard-Befugnisdauer**	**Befugnisdauer FdV**
	LEI	FdV	AS	durch das Entitlement Management bei Erteilung der Befugnis aus der Umgebung LEI	bei Erteilung der Befugnis aus der Umgebung FdV
oid_ncpeh	-	x	-	-	1 Stunde; wird durchgesetzt durch das Aktensystem

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

LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-Prüfungsnachweis (Prüfziffer),
FdV = Versicherter oder Vertreter,
AS = Aktensystem (systemseitig erteilte Befugnisse)**[<=]**

A_24371 -Entitlement Management - Verschlüsselung der Befugnisse
Das Entitlement Management MUSS Befugnisse mit dem versichertenindividuellen SecureAdminStorageKey verschlüsseln und im Aktenkonto persistieren.**[<=]**

A_24372 -Entitlement Management - Keine persistente Ablage unverschlüsselter Befugnisse
Das Entitlement Management MUSS sicherstellen, dass Befugnisse ausschließlich verschlüsselt unter Verwendung des versichertenindividuellen SecureAdminStorageKey im Aktenkonto gespeichert werden.**[<=]**

A_24687 -Entitlement Management - Keine Speicherung oder Verwendung nicht verifizierter Befugnisse
Das Entitlement Management MUSS sicherstellen, dass ausschließlich Befugnisse persistiert oder für eine Befugnisprüfung verwendet werden, die erfolgreich durch das HSM unter Verwendung der adäquaten Regeln 'rr1 - rr4' gemäß A_24573* befugnisverifiziert sind.**[<=]**

A_23842 -Entitlement Management - Eindeutigkeit der Befugnisse im Befugniskontext
Das Entitlement Management MUSS sicherstellen, dass im Befugniskontext keine zwei oder mehr Befugnisse existieren, die als Identifier des befugten Nutzers die gleiche Identifikation (`actorId`) aufweisen.**[<=]**

A_24785 -Entitlement Management - VSDM-Prüfungsnachweis kann höchstens einmal genutzt werden
Das Entitlement Management MUSS sicherstellen, dass ein VSDM-Prüfungsnachweis (Prüfziffer) höchstens einmal zur Registrierung einer Befugnis genutzt werden kann.**[<=]**

A_27671 -Entitlement Management - PoPP-Token kann höchstens einmal genutzt werden
Das Entitlement Management MUSS sicherstellen, dass ein PoPP-Token höchstens einmal zur Registrierung einer Befugnis genutzt werden kann.**[<=]**

A_27681 -Entitlement Management - Konfigurationsvariable enforce_popp_only
Das Entitlement Management MUSS eine Konfigurationsvariable `enforce_popp_only` besitzen, die initial auf `false` gesetzt ist.**[<=]**

ePA-Clients nutzen zur Befugnisvergabe die Operationen der SchnittstelleI_Entitlement_Management gemäß [I_Entitlement_Management].
Die initialen Befugnisse des Aktenkontos werden auf organisatorischem Weg direkt im Aktenkonto erstellt.

A_24506 -Entitlement Management- Realisierung der Schnittstelle I_Entitlement_Management
Das Entitlement Management MUSS die Operationen der Schnittstelle `I_Entitlement_Management` gemäß [I_Entitlement_Management] umsetzen.**[<=]**

A_26168 -Entitlement Management (EU)- Realisierung der Schnittstelle I_Entitlement_Management_EU

Das Entitlement Management MUSS die Operationen der Schnittstelle `I_Entitlement_Management_EU` gemäß [I_Entitlement_Management_EU] umsetzen.**[<=]**

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_24688-01 -Entitlement Management – Befugnisverifikation signierter initialer Befugnisse
Das Entitlement Management MUSS sicherstellen, dass die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle spätestens beim ersten Zugriff auf das Aktenkonto durch das HSM unter Verwendung der Regel 'rr4' gemäß A_24573* befugnisverifiziert sind.**[<=]**

A_24533 -Entitlement Management - Keine Änderung statischer Befugnisse
Das Entitlement Management MUSS sicherstellen, dass die dauerhaften Befugnisse des Versicherten, des E-Rezept-Fachdiensts, des Kostenträgers und der Ombudsstelle nicht verändert oder gelöscht werden können.**[<=]**

A_24784 -Entitlement Management - Höchstens eine Befugnis für KTR und Ombudsstelle pro Aktenkonto
Das Entitlement Management MUSS sicherstellen, dass in einem Aktenkonto höchstens eine Befugnis für einen Kostenträger und höchstens eine Befugnis für eine Ombudsstelle hinterlegt ist.**[<=]**

A_24955 -Entitlement Management - Befugnis für KTR und Ombudsstelle nur bei Anlage und betreiberinterner Anbieterwechsel
Das Entitlement Management MUSS sicherstellen, dass eine signierte Befugnis des Kostenträgers und eine signierte Befugnis der Ombudsstelle ausschließlich bei einer Anlage eines Aktenkontos (Initialisierung) oder bei einem betreiberinternen Anbieterwechsel in die Befugnisse des Aktenkontos aufgenommen werden.
[<=]

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` (AktenkontoId) und `validTo` (Gültigkeitszeitraum) für die spätere Befugnisprüfung vor. Das HSM Ergebnis wird mit den weiteren Daten gemäß A_23734* (`oid`, `displayName`, `issued`-*) ergänzt und gemäß A_24371* mit dem SecureAdminStorageKey gesichert im Aktenkonto abgelegt.

3.8.2.1 Befugnisvergabe durch ein ePA-FdV

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

A_24587-01 -Entitlement Management - Befugnis durch ein ePA-FdV
Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ePA-FdV über die Schnittstelle `I_Entitlement_Management` durch Verwendung eines gültig signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:

Tabelle 13 : JWT zur Befugnisvergabe mit den Mindest-Inhalten

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, (Bei unbegrenzter Gültigkeit ist 9999-12-31T00:00:00Z zu verwenden.)	gemäß [RFC3339], z.B. 2025-06-30T21:59:59Z oder 2025-06-30T23:59:59+02:00

[<=]

Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

Hinweis zu A_24587: Im Falle der Befugnisvergabe für einen NCPeH (EU-Zugriff, "oid" == "oid_ncpeh") wird durch das Aktensystem sichergestellt, dass die vorgeschriebene Gültigkeitsdauer für derartige Befugnisse angewendet wird. Dieses erfolgt durch die Befugnisverifikation gemäß Regel "rr1" im HSM. Die Angabe eines Gültigkeitsendes im "validTo"-Element des JWT wird daher für diesen Fall ignoriert, das Element selbst muss jedoch vorhanden sein.*

A_24689 -Entitlement Management - Befugnisverifikation einer Befugnis durch ein ePA-FdV
Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein ePA-FdV unter Verwendung der Regeln 'rr1' (Befugnisvergabe durch den Versicherten) bzw. 'rr2' (Befugnisvergabe durch einen Vertreter) des HSM eine Befugnisverifikation durchführen.**[<=]**

A_24535 -Entitlement Management - Befugnisse für Vertreter
Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId` = KVNR) ausschließlich durch den Versicherten erstellt oder gelöscht werden können. **[<=]**

A_26698 -Entitlement Management - maximale Anzahl Befugnisse für Vertreter
Das Entitlement Management MUSS sicherstellen, dass maximal fünf gültige Befugnisse für Vertreter gleichzeit in einem Aktenkonto vorhanden sind.**[<=]**

A_24536 -Entitlement Management - Gültigkeitsdauer der Befugnisse für Vertreter
Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId` = KVNR) ausschließlich mit einer unbegrenzten Gültigkeit erstellt werden.**[<=]**

A_24754 -Entitlement Management - E-Mail-Adresse des Vertreters
Das Entitlement Management MUSS sicherstellen, dass bei Befugnissen für Vertreter (`actorId` = KVNR) eine E-Mail-Adresse des Vertreters für dessen Benachrichtigung angegeben wird.**[<=]**

Die in A_24754 angegebene E-Mail-Adresse wird ausschließlich zur Benachrichtigung des Vertreters über die eingestellte Befugnis verwendet (vgl. A_24755-*), jedoch nicht für die Geräteregistrierung. Um eine Vertretung wahrnehmen zu können und hierfür Geräte zu registrieren, muss der Vertreter in seinem Home-AS eine E-Mail-Adresse hinterlegt haben.

A_24755-01 -Entitlement Management - Benachrichtigung des Vertreters bei 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 MUSS der Name des Versicherten enthalten sein und welche Art von personenbezogenen Daten vom Vertreter im Rahmen der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine Vertreterberechtigung widerrufen kann und gegenüber wem er seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann.**[<=]**

Hinweis: Unter Art der personenbezogenen Daten ist z.B. „Krankenversichertennummer, Name und E-Mail-Adresse“ gemeint, aber nicht die tatsächliche KVNR des Vertreters, der tatsächliche Name oder die tatsächliche E-Mail-Adresse.

https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/#A_24755-01

A_28175 -Entitlement Management - Benachrichtigung des Versicherten bei Befugniserstellung
Das Entitlement Management MUSS im Anschluss an die erfolgreiche, neue Befugniserstellung für einen Vertreter eine E-Mail an die E-Mail-Adresse des Versicherten

senden, sofern eine E-Mail-Adresse für den Versicherten im Aktensystem hinterlegt ist, die den Versicherten über die Befugniserstellung informiert.**[<=]**

3.8.2.2 Befugnisvergabe durch ein Primärsystem

A_27288-01 -Entitlement Management – Abgleich der KVNR bei Erstellen einer Befugnis
Das Entitlement Management MUSS sicherstellen, dass für die in `setEntitlementPs` bzw. `setEntitlementsPsV2` vom Primärsystem in `x-insurantid` übergebene KVNR folgendes gilt: die KVNR in `x-insurantid` stimmt mit der KVNR überein, die in der CMAC-gesicherten Befugnis enthalten ist, die als Ergebnis des Aufrufs der Regel rr3 mit der vom Primärsystem erhaltenen Befugnis (signiertes JWT) bzw. dem erhaltenen PoPP-Token vom HSM zurückgegeben wird.
[<=]

Ein Primärsystem muss für die Befugnisvergabe mittels VSDM-Prüfziffer ein JWS gemäß folgender Vorgabe erstellen.

A_24590-03 -Entitlement Management - Befugnis durch ein Primärsystem
Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ein Primärsystem über die Operation `I_Entitlement_Management::setEntitlementPs` durch die Verwendung eines gültig signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:

Tabelle 14 : JWT zur Befugnisvergabe mit Mindest-Inhalten

Befugnis	Claim Name	Claim
Protected Header		
	`"typ"`	"JWT"
	`"alg"`	"ES256" oder "PS256"
	`"x5c"`	Signaturzertifikat C.HCI.AUT
Payload		
	`"iat"`	Zeitstempel Ausgabezeitpunkt
	`"exp"`	Verfalldatum, = "iat" + 20 min
	`"auditEvidence"`	VSDM-Prüfziffer aus dem VSDM-Prüfungsnachweis, base64-kodiert.
	`"hcv"`	Hash check value, der als Ergebnis der Operation ReadVSD gemäß A_27352-* berechnet wird. Der berechnete hcv-Wert MUSS base64 kodiert werden.

[<=]

Hinweis: Die Parameter "iat" und "exp" sind optional und werden durch das Entitlement Management nicht ausgewertet.

Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

A_27321-01 -Entitlement Management – Abgleich hcv bei Erstellen einer Befugnis über VSDM-Prüfziffer in Version 2
Falls vom Primärsystem in `setEntitlementPs` eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2 übergeben wird und das Ergebnis des Aufrufs der Regel rr3 eine interne Datenstruktur der VSDM-Prüfziffer zurückliefert, MUSS das Entitlement Management sicherstellen, dass der Wert im Attribut "hcv" des JWT mit dem Wert von hcv aus der VSDM-Prüfziffer übereinstimmt und ansonsten die Operation`setEntitlementPs` abbrechen.**[<=]**

A_27289 -Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer
Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer Stunde maximal fünfmal eine Befugnis (signiertes JWT) über `setEntitlementPs` übermitteln kann, bei der die mitgelieferte KVNR in `x-insurantId` von der KVNR abweicht, die in der Prüfziffer der übermittelten Befugnis (signiertes JWT) enthalten ist, andernfalls für den Nutzer für diesen Zeitraum die Operation `setEntitlementPs` abbrechen.**[<=]**

A_27322 -Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche der VSD-Update-Zeit bei Erstellen einer Befugnis über VSDM-Prüfziffer in Version 2
Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer Stunde maximal fünfmal eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2 über `setEntitlementPs` übermitteln kann, bei der die Operation `setEntitlementPs` gemäß A_27321-* abbricht.**[<=]**

A_27679 -Entitlement Management - Telematik-ID im PoPP-Token ist gleich der Telematik-ID des angemeldeten Nutzers
Das Entitlement Management MUSS bei der Befugnisvergabe durch ein Primärsystem unter Verwendung eines PoPP-Tokens sicherstellen, dass die Telematik-ID in PoPP-Token.actorID gleich der Telematik-ID des Nutzers der User Session ist.**[<=]**

A_24537 -Entitlement Management - Standardgültigkeitsdauer für Befugnisse
Das Entitlement Management MUSS sicherstellen, dass neue Befugnisse, die unter Verwendung der Schnittstelle `I_Entitlement_Management` gemäß [I_Entitlement_Management] erstellt werden, eine vorgegebene, rollenspezifische Befugnisdauer gemäß A_23941-* erhalten.**[<=]**

3.8.3 Löschen von Befugnissen

Erteilte Befugnisse werden grundsätzlich nach Erreichen des Endzeitpunkts ihrer Gültigkeit durch das Aktensystem gelöscht.

A_24504 -Entitlement Management - Löschen ungültiger Befugnisse
Das Entitlement Management MUSS vorhandene Befugnisse, deren Enddatum der Gültigkeit überschritten ist, unverzüglich aus dem Befugniskontext des Aktenkontos vollständig löschen.**[<=]**

Das explizite Löschen von Befugnissen innerhalb ihres Gültigkeitszeitraums kann ausschließlich durch den Versicherten oder einen Vertreter mittels eines ePA-FdV erfolgen. Es können alle erteilten Befugnisse gelöscht werden, ausgenommen die initialen Befugnisse gemäß3.8.1- Initiale Befugnisse (static Entitlements) .

Für das Löschen von Befugnissen durch einen Vertreter gilt darüber hinaus folgende Einschränkung:

A_25246 -Entitlement Management - Löschen von Befugnissen durch einen Vertreter
Das Entitlement Management MUSS sicherstellen, dass eine erteilte Befugnis für einen Vertreter (`actorId`der Befugnis == KVNR) durch einen Vertreter nur dann gelöscht werden kann, wenn die KVNR des löschenden Vertreters der KVNR der `actorId`der zu löschenden Befugnis entspricht.**[<=]**

Hinweis: Ein Vertreter darf nur seine eigene Befugnis löschen, nicht aber die Befugnis weiterer Vertreter.

A_25269 -Entitlement Management - Benachrichtigung des Versicherten bei Löschen einer Vertreterbefugnis durch Vertreter
Falls ein Vertreter seine eigene Vertreterbefugnis löscht MUSS das Entitlement Management für den Fall, dass für den Versicherten mindestens eine E-Mail-Adresse hinterlegt ist, den Versicherten über das Löschen der Vertreterbefugnis an alle seine hinterlegten E-Mail-Adressen informieren.**[<=]**

3.8.4 Befugnisausschluss (Blocked User Policy)

Das Entitlement Management erlaubt die Verwaltung von Widersprüchen des Versicherten oder eines Vertreters gegen die Nutzung des Aktenkontos durch spezifische 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_24463-01 -Entitlement Management - zulässige Rollen für den Widerspruch gegen die Nutzung durch eine Leistungserbringerinstitution
Das Entitlement Management MUSS den Widerspruch gegen die Nutzung durch eine Leistungserbringerinstitution ausschließlich für Nutzer der folgenden Nutzergruppen zulassen:

professionOID / Nutzergruppe

oid_praxis_arzt
oid_krankenhaus
oid_institution-vorsorge-reha
oid_zahnarztpraxis
oid_öffentliche_apotheke
oid_praxis_psychotherapeut
oid_institution-pflege
oid_institution-geburtshilfe
oid_praxis-physiotherapeut
oid_praxis-ergotherapeut
oid_praxis-logopaede
oid_praxis-podologe
oid_praxis-ernaehrungstherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin

[<=]

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

Tabelle 15: Inhalt eines Blocked User Policy Eintrags

Element	Inhalt	Beispiel
`actorId`	Telematik-Id	2-883110000099999
`oid`	professionOID	1.2.276.0.76.4.5
`displayName`	Name der Leistungserbringerinstitution	Zahnarztpraxis Dr. Beispiel
`at`	Zeitpunkt des Widerspruchs (wird durch das Entitlement Management gesetzt)	2025-01-01T12:00:00Z

A_25135 -Entitlement Management - Initialisierung der Blocked User Policy
Das Entitlement Management MUSS für ein Aktenkonto eine Blocked User Policy ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policies über die

SchnittstelleI_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.**[<=]**

3.8.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)

Die Erstellung von Befugnissen durch Primärsysteme der Leistungserbringerinstitutionen wird durch das Aktensystem mengenmäßig über einen Zeitraum begrenzt. Diese Maßnahme verhindert den massenhaften Zugriff auf Aktenkonten durch Fehlbedienung seitens eines Primärsystems oder durch unzulässige Nutzung der Aktensysteme.

Die maximal zulässige Befugnismenge ist dabei so bemessen, dass die intendierte Nutzung der ePA durch Leistungserbringerinstitutionen im Versorgungsalltag nicht eingeschränkt wird. Diese maximale Befugnismenge ist pro Nutzerrolle separat festgelegt.

Jedes Aktensystem führt dazu aktensystemweit Zähler für erteilte Befugnisse aus der Umgebung der Leistungserbringer pro Telematik-ID. Die Erfassung erfolgt somit pro Leistungserbringerinstitution separat. Die Zuordnung erfolgt zur Telematik-ID der befugniserstellenden Nutzer (nicht des zu befugenden Nutzers). Die Befugnisvergabe aus der Umgebung des Versicherten mittels ePA-FdV wird nicht erfasst und geht nicht in die Zählerstände ein.

Das Entitlement Mangement wertet diese Menge der erfassten Befugnisvergaben im Falle einer weiteren Befugnisvergabe durch ein Primärsystem aus der Umgebung der LEI aus und verhindert die Befugniserstellung bei Erreichen der maximal zulässigen Befugnismenge.

Die zulässige Befugnisrate limitiert dabei einerseits die Menge der innerhalb einer Stunde erstellbaren Befugnisse, als auch die Menge der insgesamt monatlich erstellbaren. Die Zählung erfolgt aktensystemweit pro Aktensystem eines Herstellers und unabhängig vom adressierten Aktenkonto und berücksichtigt nur erfolgreiche Befugnisvergaben. Der Zeitraum pro Stunde, bzw. pro Monat, bezieht sich dabei auf den Zeitraum der aktuellen Stunde, bzw. des aktuellen Monats.

A_27311 -Entitlement Management – RateLimit-oid-List
Das Entitlement Management MUSS eine *RateLimit-oid-List* führen, in der pro oid

- der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden Befugnisse innerhalb einer Stunde,
- der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden Befugnisse innerhalb eines Monats und
- der Zeitpunkt der letzten Änderung der Werte

gespeichert werden.**[<=]**

Initial ist die RateLimit-oid-List mit folgenden Werten zu belegen:

A_27290-01 -Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Stunde
Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass eine LEI mit der Rolle

- oid_praxis_arzt maximal 200 Befugnisse
- oid_krankenhaus maximal 1.000 Befugnisse
- oid_institution-vorsorge-reha maximal 1.000 Befugnisse
- oid_zahnarztpraxis maximal 200 Befugnisse
- oid_öffentliche_apotheke maximal 200 Befugnisse
- oid_praxis_psychotherapeut maximal 100 Befugnisse
- oid_institution-pflege maximal 100 Befugnisse
- oid_institution-geburtshilfe maximal 100 Befugnisse
- oid_praxis-physiotherapeut maximal 100 Befugnisse
- oid_praxis-ergotherapeut maximal 100 Befugnisse
- oid_praxis-logopaede maximal 100 Befugnisse
- oid_praxis-podologe maximal 100 Befugnisse
- oid_praxis-ernaehrungstherapeut maximal 100 Befugnisse
- oid_institution-oegd maximal 100 Befugnisse
- oid_institution-arbeitsmedizin maximal 100 Befugnisse

innerhalb einer Stunde durch das Primärsystem im Aktensystem registrieren kann.
[<=]

A_27291-01 -Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Monat
Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass

- oid_praxis_arzt maximal 10.000 Befugnisse
- oid_krankenhaus maximal 200.000 Befugnisse
- oid_institution-vorsorge-reha maximal 200.000 Befugnisse
- oid_zahnarztpraxis maximal 10.000 Befugnisse
- oid_öffentliche_apotheke maximal 25.000 Befugnisse
- oid_praxis_psychotherapeut maximal 10000 Befugnisse
- oid_institution-pflege maximal 10000 Befugnisse
- oid_institution-geburtshilfe maximal 10000 Befugnisse
- oid_praxis-physiotherapeut maximal 10000 Befugnisse

- oid_praxis-ergotherapeut maximal 10000 Befugnisse
- oid_praxis-logopaede maximal 10000 Befugnisse
- oid_praxis-podologe maximal 10000 Befugnisse
- oid_praxis-ernaehrungstherapeut maximal 10000 Befugnisse
- oid_institution-oegd maximal 10000 Befugnisse
- oid_institution-arbeitsmedizin maximal 10000 Befugnisse

innerhalb eines Monats durch das Primärsystem im Aktensystem registrieren kann.
[<=]

Hinweis zu A_27290-* und A_27291-*: Die Stunde bzw. der Tag müssen sich nicht auf die aktuelle Stunde bzw. Kalendertag beziehen, sondern können auch je Leistungserbringerinstitution auf Requestzeitpunkte bezogen werden. Dann gilt für einen Monat 30 Tage.

A_27318 -ePA-Aktensystem - RatelLimit-oid-List: Maßnahmen zum Schutz der Konfiguration
Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen umsetzen, die eine unautorisierte Änderung der *RateLimit-oid-List* verhindern.**[<=]**

A_27312 -ePA-Aktensystem - RatelLimit-oid-List: Konfiguration durch Betreiber
Der Betreiber des ePA-Aktensystem MUSS sicherstellen, dass die Werte für die Anzahl der maximalen Befugnisse in der RateLimit-oid-List durch den Betreiber des ePA-Aktensystems außschließlich im Vier-Augen-Prinzip konfigurierbar sind.**[<=]**

Stellen LEI Befugnisse mittels der Operation `setEntitlementsPs` über das Primärsystem in das ePA-Aktensystem ein, wird für diese LEI geprüft, ob diese bereits das zulässige Limit erreicht hat. Nur falls dies nicht der Fall ist, kann die Befugnis eingestellt werden. Hierzu erfasst das ePA-Aktensystem außerhalb der VAU wann ein Nutzer mit welcher Rolle eine Befugnis registriert hat. Für den Nutzer wird außerhalb der VAU ein Nutzerpseudonym geführt.

A_27313-01 -Entitlement Management - Prüfen der RateLimit-oid-List beim Einstellen von Befugnissen
Das Entitlement Management MUSS bei Aufruf der Operation `setEntitlementsPs` oder `setEntitlementPsV2` prüfen, ob für das zur LEI gehörende Nutzerpseudonym und die oid der LEI bereits das in der RateLimit-oid-List vorgegebene maximale Limit pro Stunde oder Monat erreicht wurde. Falls ein Limit erreicht wurde, wird die Operation `setEntitlementsPs`, bzw. `setEntitlementPsV2`, mit einem Fehler abgebrochen. Falls kein Limit erreicht wurde, ist die Registrierung für das zur LEI gehörende Nutzerpseudonym zu vermerken.**[<=]**

A_27310 -ePA-Aktensystem - Erfassung der Nutzer zur Prüfung RateLimit-oid-List
Das ePA-Aktensystem MUSS sicherstellen dass bei der Erfassung der Nutzerdaten außerhalb der VAU zur Prüfung der *RateLimit-oid-List* eine Profilierung über die Nutzer nicht möglich ist und zu diesem Zweck aus der TelematikId eines Nutzers ein Nutzerpseudonym abgeleitet wird, gemäß gemSpec_Krypt#7.5 Routing auf VAU-Instanzen.
[<=]

3.8.6 EntitlementDenyList

Ein Primärsystem einer Leistungserbringerinstitution (LEI) kann eine Befugnis für ein Aktenkonto eines Versicherten in einer Behandlungssituation ("Stecken" der eGK, VSDM-Prüfungsnachweis) eigenständig erstellen, wenn der Versicherte der Nutzung der ePA

nicht widersprochen hat, für die konkrete Leistungserbringerinstitution im Aktenkonto kein Befugnisausschluss (3.8.4- Befugnisausschluss (Blocked User Policy)) vorliegt und die Leistungserbringerinstitution einer grundsätzlich befugbaren Nutzergruppe angehört (3.8- Entitlement Management).

Die bestimmte LEI deren Telematik-ID auf einer sogenannten EntitlementDenyList stehen, wird diese Funktionalität durch das Aktensystem unterbunden, in der Weise dass eine Befugnisvergabe durch das Aktensystem unterbunden wird.

Die Befugnisvergabe durch den Versicherten oder einen Vertreter mittel ePA-FdV ist durch die EntitlementDenyList nicht eingeschränkt. Über ein ePA-FdV können auch LEI befugt werden, die einen Eintrag in der EntitlementDenyList haben.

Die EntitlementDenyList wird durch das Aktensystem bei jedem Aufruf einer Operation zur Befugnisvergabe durch ein Primärsystem ausgewertet. Diese Operation wird mit einem Fehler beendet, wenn die zu befugende LEI Bestandteil der Liste ist. Eventuell vorhandene Befugnisse dieser LEI, etwa aus einer Befugnisvergabe mittels ePA-FdV, verbleiben im Fehlerfall der Operation unverändert.

Die EntitlementDenyList wird für alle Aktenkonten eines Aktensystems einheitlich verwaltet. Die Verwaltung erfolgt außerhalb der VAU, die Liste muss aber für Operationen der Befugnisvergabe innerhalb der VAU zugänglich sein.

A_27730 -ePA-Aktensystem - EntitlementDenyList außerhalb der VAU
Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen umsetzen, die eine unautorisierte Änderung der EntitlementDenyList verhindern.**[<=]**

A_27731 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren
Das ePA-Aktensystem MUSS sicherstellen, dass falls eine LEI (Telematik-ID) aus der EntitlementDenyList entfernt wird, in der VAU nach spätestens 24 Stunden die EntitlementDenyList aktualisiert wird.**[<=]**

A_27732 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren - Ausschluss einer LEI
Falls eine LEI der EntitlementDenyList hinzugefügt wird, MUSS der Betreiber des ePA-Aktensystems sicherstellen, dass die EntitlementDenyList in der VAU unverzüglich aktualisiert wird.**[<=]**

Hinweise zu A_27732-*:

- Die gematik übermittelt die komplette aktuelle EntitlementDenyList an den Anbieter des ePA-Aktensystems.
- Die gematik übermittelt die aufgrund von Sicherheitsgründen aktualisierte EntitlementDenyList über die etablierten Incident-Prozesse.

A_27714 -Entitlement Management - setEntitlementPs in Abhängigkeit von EntitlementDenyList
Falls der Nutzer auf der EntitlementDenyList enthalten ist, MUSS das Entitlement Management die Operation `setEntitlementPs` ohne Erzeugung einer Befugnis mit dem HTTP-Statuscode 409requestMismatch abbrechen.
[<=]

Technische Details zur Aktualisierung der EntitlementDenyList im Aktensystem:

Die gematik liefert regelmäßige Aktualisierungen der EntitlementDenyList an die Betreiber der ePA-Aktensysteme. Die gematik möchte automatisiert überwachen können, ob in den ePA-Aktensystemen jeweils die aktuelle Version der EntitlementDenylist geladen ist. In den ePA-Aktensystemen gibt es jeweils ein Enforcement-Point an dem die EntitlementDenyList technisch durchgesetzt wird. Mindestens bei Aktualisierung der EntitlementDenyList im ePA-Aktensystem soll solch ein Enforcement-Point Auskunft über eine BDE-Meldung darüber geben welche EntitlementDenyList ihm aktuell vorliegt. Dabei soll eine hohe Aussagekraft der Information erreicht werden, deshalb wird ein Hashwert

über die TelematikIDs der aktuellen EntitlementDenyList erzeugt und dieser Hashwert wird über die BDE-Daten an die gematik (Betriebsüberwachung) übermittelt.

A_27780 -Übertragungsformat der EntitlementDenyList (gematik->ePA-Aktensystem).
Das ePA-Aktensystem MUSS sicherstellen, dass es eine EntitlementDenyList im JSON-Format von der gematik in folgender Art entgegen nehmen / auswerten kann.

```
{
  "type": "EntitlementDenyList",
  "version": <natürliche Zahl>,
  "iat": <Unix-Zeit als natürliche Zahl>,
  "separator": "<Trennsequenz>",
  "TelematikIDs": [
      "<TID_1>", ... "<TID_2>"
  ],
  "TruncatedHash": "Base64-kodierter 24-Byte-gekürzter-SHA256-Hashwert"
}
```

Die Attribute "version", "iat" dienen nur der Information, i. S. v. müssen von Aktensystem nicht notwendiger Weise technisch ausgewertet werden.

Ein ePA-Aktensystem KANN den TruncatedHash analog A_27781-* berechnen (es werden nur die ersten 192 Bit / 24 Byte verwendet) und für aktensysteminterne Zwecke verwendet.

Die Telematik-IDs im Array "TelematikIDs" (bspw. "1-1.12345678") sind in alphabetisch aufsteigender Ordnung sortiert (werden also schon durch die gematik sortiert geliefert). Die JSON-Datei ist wie üblich UTF-8 kodiert.**[<=]**

Beispiel für eine EntitlementDenyList gemäß A_27780-*:

```
{
  "type": "EntitlementDenyList",
  "version": 6,
  "iat": 1749563839,
  "separator": "+++",
  "TelematikIDs": [
      "1-1.1234567890",
      "1-123456789",
      "1-12345678901234",
      "1-22345678901234",
      "3-06.2.1234567890.10.123",
      "3-07.2.1234567890.123",
      "3-14.2.1234567890.123"
  ],
  "TruncatedHash": "pee1nuX5TxSce3QSawdqs+Pf0L6UMCr8"
}
```

A_27781 -Hashwertberechnung der Telematik-ID-Einträge in einer EntitlementDenyList
Eine ePA-Aktensystem MUSS bei der Berechnung des Hashwertes für die BDE-Datenlieferung gemäß A_22469-*:

1. die Einträge in Array "TelematikIDs" alphabetisch aufsteigend sortieren,
2. die Einträge jeweils mit dem Inhalt von "separator" als Verbindungselement zu einer einzigen lange Bytefolge konkatenieren,
3. von dieser langen Bytefolge den SHA-256-Hashwert berechnen.

Der berechnete Hashwert MUSS Base64 kodiert werden. Das Ergebnis ist dann der Hashwert der für die BDE-Datenlieferung gemäß A_22469-* und A_27782-* zu verwenden ist.
[<=]

Beispiele für A_27281-*:

1)

Wäre separator="AAA" und TelematikIDs=["1", "2", "3"], dann wären die dtbh="1AAA2AAA3". Der Base64-kodierte Hashwert wäre dann NFtIcjtAGzo8tL5goB6QMXpHkNCjDSFK5oTzILjXu8k=

2)

Mit den Daten aus dem oben aufgeführten Beispiel für A_27780-* würde ein Aktensystem pee1nuX5TxSce3QSawdqs+Pf0L6UMCr80uM3VYtVJdU= berechnen.

A_27782 -EntitlementDenyList: Hashwertberechnung der Telematik-ID-Einträge im Aktensystem
Ein ePA-Aktensystem MUSS sicherstellen, dass bei Aktualisierung der EntitlementDenyList-Daten am Enforcement-Point der EntitlementDenyList wie in A_22467-* definiert, eine Meldung an die BDE erzeugt und übermittelt wird. Dabei MUSS es den dabei zu übermittelnden Hashwert wie in A_27781 definiert berechnen. (vgl. auch Hinweise zu A_22782-*)
[<=]

Hinweise zu A_27782-*:

Zum besseren Verständnis, falls der Enforcement-Point die VAU-Instanz ist, so muss beim initialen Starten der VAU-Instanz die EntitlementDenyList in die VAU-Instanz geladen werden. Diese gilt als Aktualisierung der EntitlementDenyList-Daten in der VAU-Instanz. Somit gilt dort A_27782-*.

3.9 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 die zahnärztliche Dokumentation in der Datenkategorie "`dental`".
- Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen noch löschen.

Die Legal Policy wird durch das Aktensystem durchgesetzt und ist jederzeit vorhanden. Die Konfiguration kann durch Clients oder Bestandteile des Aktensystems nicht verändert werden.

A_19303-26 -Legal Policy – gesetzlich vorgegebene Zugriffsrechte
Das ePA-Aktensystem MUSS alle in der folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

Tabelle 16: Legal Policy

Kategorie	Nutzergruppe

Technischer Identifier	**Med**	**Apo**	**Pflege**	**GH**	**HME**	**AM**	**KTR**	**OM**	**DiGA**	**eRP**	**Ver**
Medical Services (Document Service)	**Zugriffsrecht gemäß § 352 SGB V**										
reports	CRUD	R	R	R	CRUD	R	-	-	-	-	RD
emp	R	R	R	R	R	R	-	-	-	-	RD
emergency	CRUD	R	R	R	R	R	-	-	-	-	RD
eab	CRUD	R	R	R	R	R	-	-	-	-	RD
dental	CRUD	-	R	-	-	R	-	-	-	-	RD
childsrecord	RD	R	R	RD	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	C	-	-	-	CRUD
receipt	-	-	-	-	-	-	CU	-	-	-	RD
health_risk_analysis	-	-	-	-	-	-	C	-	-	-	RD
diga	R	R	R	R	R	R	-	-	CU	-	RD
care	CRUD	R	CRUD	R	R	R	-	-	-	-	RD
eau	CRUD	-	-	-	-	R	-	-	-	-	RD

rehab	CRUD	-	-	-	-	-	-	-	-	-	RD
transcripts	CRUD	-	-	-	-	-	-	-	-	-	RD
other	CRUD	-	-	-	-	R	-	-	-	-	RD
Medical Services (FHIR Data Services)	**Zugriffsrecht**										
medication	CRUD	CRUD	R	R	R	R	-	D(**)	-	CU	RD(**)
demographics (Patient)	R	-	-	-	-	-	CU	-	-	-	R
Basic Services	**Zugriffsrecht**										
Audit	-	-	-	-	-	-	-	R	-	-	R
Consent Decisions	-	-	-	-	-	-	-	x	-	-	x
Constraints	-	-	-	-	-	-	-	-	-	-	x
Devices	-	-	-	-	-	-	-	-	-	-	x
Entitlements	x	x	x	x	x	x	-	-	-	-	x
Entitlements.Blocked User	-	-	-	-	-	-	-	x	-	-	x
Information	x	x	x	x	x	x	x	x	x	x	-

Nutzergruppen:

- Med = Arztpraxis, Zahnarztpraxis, Krankenhaus, Psychotherapeut, Vorsorge- und Rehabilitation, Öffentlicher Gesundheitsdienst
  - (oid_praxis_arzt,, oid_krankenhaus, oid_institution-vorsorge-reha, oid_zahnarztpraxis, oid_praxis_psychotherapeutoid_institution-oegd)
- Apo = Öffentliche Apotheke
  - (oid_öffentliche_apotheke)
- Pflege = Gesundheits-, Kranken- und Altenpflege
  - (oid_institution-pflege)
- GH = Geburtshilfe
  - (oid_institution-geburtshilfe)

- HME = Heilmittelerbringer
  - (oid_praxis-physiotherapeut, oid_praxis-ergotherapeut, oid_praxis-logopaede, oid_praxis-podologe, oid_praxis-ernaehrungstherapeut)
- AM = Arbeitsmedizin
  - (oid_institution-arbeitsmedizin)
- KTR = Kostenträger
  - (oid_kostentraeger)
- OM = Ombudsstelle
  - (oid_ombudsstelle)
- DiGA = Digitale Gesundheitsanwendung
  - (oid_diga)
- eRP = E-Rezept vertrauenswürdige Ausführungsumgebung
  - (oid_erp-vau)
- Ver = Versicherter / Vertreter
  - (oid_versicherter)

Legende:

- CRUD = create, read, update, delete; update: Aktualisierung eines Dokuments
- "-" = keine Zugriffsrechte;
- "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den Dienst (Service) definiert)
- "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung in einer zukünftigen Version der ePA vorgesehen.

Hinweise:

- (*) Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann der Versicherte bzw. sein Vertreter oder eine Leistungserbringerinstitution gemäß der zuvor genannten Liste definierter professionOIDs sein. Sofern ein Versicherter/Vertreter der Einsteller der Elternnotiz ist, darf er abweichend von den oben aufgeführten Zugriffsunterbindungsregeln in die Datenkategorie mit dem technischen Identifier 'child' schreiben.
- (**) Ein Versicherter bzw. sein Vertreter sowie die Ombudsstelle kann, durch Setzen eines Widerspruchs gegen das Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst (`erp-submission`), das Löschen der im FHIR data service `medication` gespeicherten Daten erzwingen.

[<=]

A_26166-04 -Legal Policy (EU) – EU-Zugriff: gesetzlich vorgegebene Zugriffsrechte

Das ePA-Aktensystem MUSS zusätzlich zu den Regeln ausA_19303-* alle in der folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

Tabelle 17: Legal Policy - EU-Zugriff

Kategorie	Nutzergruppe

Technischer Identifier	**NCPeH**
Medical Services (Document Service)	**Zugriffsrecht gemäß § 352 SGB V**
reports	-
emp	-
emergency	R - ePA EU Patient Summary
eab	-
dental	-
child	-
childsrecord	-
pregnancy_childbirth	-
vaccination	-
patient	-
receipt	-
health_risk_analysis	-
diga	-
care	-
eau	-
rehab	-
transcripts	-
other	-
Medical Services (FHIR Data Service)	**Zugriffsrecht**
medication	-
demographics (Patient)	R
audit	-

Basic Services	Zugriffsrecht
Consent Decisions	-
Constraints	-
Devices	-
Entitlements	-
Entitlements.Blocked User	-
Information	x

Nutzergruppen:

- NCPeH = NCPeH-Fachdienst (oid_ncpeh)

Legende:

- CRUD = create, read, update, delete; update: Aktualisierung eines Dokuments
- "-" = keine Zugriffsrechte;
- "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den Dienst (Service) definiert)
- "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung in einer zukünftigen Version der ePA vorgesehen.

[<=]

Die folgende Tabelle erläutert die Kategorien und Services aus A_19303-* und A_26166-*:

Tabelle 18: Beschreibung der Kategorien und Services

Technischer Identifier	Beschreibung
Medical Services	**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 aus der zahnärztlichen Dokumentation
child	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
childsrecord	Archiv aus ePA 2.x: Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
pregnancy_childbirth	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass) sowie Daten, die sich aus der Versorgung der Versicherten mit Hebammenhilfe ergeben
vaccination	Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation)
patient	Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden
receipt	Bei Kostenträgern gespeicherte Daten über die in Anspruch genommenen Leistungen des Versicherten
health_risk_analysis	Ergebnisse datengestützter Auswertungen der Krankenkassen zu individuellen Gesundheitsrisiken gemäß SGB V § 25b.
diga	Daten des Versicherten aus digitalen Gesundheitsanwendungen des Versicherten nach § 33a.
care	Daten zur pflegerischen Versorgung des Versicherten nach den §§ 24g, 37, 37b, 37c, 39a und 39c und der Haus- oder Heimpflege nach § 44 des Siebten Buches und nach dem Elften Buch
eau	Daten nach § 73 Absatz 2 Satz 1 Nummer 9 ausgestellte Bescheinigung über eine Arbeitsunfähigkeit
rehab	Daten der Heilbehandlung und Rehabilitation nach § 27 Absatz 1 des Siebten Buches
transcripts	Elektronische Abschriften von der Patientenakte eines Primärsystems gemäß §630g Abs. 2 BGB

other	Sonstige von Leistungserbringern für Versicherten bereitgestellte Daten, insbesondere Daten, die sich aus der Teilnahme des Versicherten an strukturierten Behandlungsprogrammen bei chronischen Krankheiten gemäß § 137f ergeben
Medical Services	**FHIR Data Services**
medication	Verordnungs-, Dispensier- und Medikationsdaten in einer elektronischen Medikationsliste (eML) und einem elektronischen Medikationsplan (eMP), sieheePA Medication Service [gemIG_ePA_Medication]
demographics (patient)	Bereitstellung demographischer Daten des Versicherten für Medical Services, sieheePA Patient Service, in [gemIG_ePA_Basic]
audit	Protokolle von Zugriffen aller Nutzer auf die Akte des Versicherten, sieheePA Audit Event Service in [gemIG_ePA_Basic]
Basic Services	**Account Management**
Consent Decisions	Management der Entscheidungen zu widerspruchsfähigen Funktonen der ePA
Constraints	Management der Konfiguration der General Deny Policy
Entitlements	Management der Befugnisse für Nutzer und Nutzergruppen
Audit Events	Abruf der Protokolleinträge eines Aktenkontos
Information	Informationen für nicht befugte Nutzer
Devices	Management der registrierten Geräte eines Nutzers

A_21211-01 -Legal Policy - Änderungen der Legal Policy nicht erlauben
Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass Änderungen der Konfiguration der Legal Policy gemäß A_19303-* ausgeschlossen sind. **[<=]**

A_24548 -Legal Policy - Durchsetzung der Zugriffsrechte der Legal Policy
Das ePA-Aktensystem MUSS sicherstellen, dass Operationen auf Daten und Operationen der Dienste eines Aktenkontos abgebrochen und mit einer Fehlermeldung beendet werden, wenn diese Operation durch die Vorgaben der Legal Policy gemäß A_19303-* für die Nutzergruppe des Aufrufers der Operation nicht zulässig ist.**[<=]**

3.10 Constraint Management

Das Constraint Management des Aktenkontos stellt sicher, dass nur Zugriffe auf Daten in Ordnern der Document Services über die Vorgaben der Legal Policy hinaus zugelassen werden, welche nicht vom Versicherten oder einem Vertreter unterbunden (verborgen) wurden.

Die Umsetzung dieser Beschränkungen erfolgt anhand der **General Deny Policy** für jeden befugten Nutzer der betroffenen Nutzergruppen des Aktenkontos.

Die General Deny Policy adressiert Nutzergruppen (professionOID) und Metadaten der Daten. Es können einzelne Dokumente, Kategorien oder Ordner verborgen werden. Bei jedem Zugriff auf Daten in Ordnern wird diese Policy bezüglich der Rolle eines Nutzers und der betroffenen Dokumente ausgewertet und durchgesetzt.

Die folgende Anforderung zeigt eine Übersicht der Nutzergruppen, für welche Dokumente durch Einträge in der General Deny Policy vor einem Zugriff verborgen werden können.

A_24306-02 -Constraint Management - Policy für berechtigte Nutzergruppen und Nutzer
Das Constraint Management MUSS die Konfiguration der General Deny Policy auf die folgenden Nutzergruppen einschränken:

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

[<=]

A_24390-02 -Constraint Management- Anwendung der General Deny Policy
Das Constraint Management MUSS bei jedem Zugriff auf Daten durch einen Document Service durch befugte Nutzer oder Nutzergruppen die General Deny Policy anwenden und den Zugriff verhindern, wenn ein Dokument oder dessen assoziierter Ordner oder dessen assoziierte Datenkategorie in der Policy konfiguriert ist.
[<=]

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

Datendienste (Medication Service) können nicht auf Daten- oder 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 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 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_30184 -Constraint Management - Realisierung der Schnittstelle I_Constraint_Management
Das Constraint Management MUSS die Operationen der Schnittstelle `I_Constraint_Management` gemäß [I_Constraint_Management] umsetzen.**[<=]**

Für die Policy gelten folgende Vorgaben.

A_24393-02 -Constraint Management - Initialisierung der General Deny Policy
Das Constraint Management MUSS für ein Aktenkonto eine General Deny Policy ohne initiale Einträge bereitstellen.**[<=]**

A_24462-01 -Constraint Management - Konfiguration der General Deny Policy anpassen nach Löschen von Ordnern
Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn diese einen Ordner referenzieren und dieser Ordner aus dem Aktenkonto gelöscht wird.
[<=]

A_24461-01 -Constraint Management - Konfiguration der General Deny Policy anpassen nach Löschen von Dokumenten
Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn diese ein spezifisches Dokument referenzieren und dieses Dokument aus dem Aktenkonto gelöscht wird.**[<=]**

A_24516-01 -Constraint Management - Speichern der Inhalte der General Deny Policy
Das Constraint Management MUSS Einträge aus der General Deny Policy unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.**[<=]**

3.10.1 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 dynamischen Ordner oder eine Datenkategorie. Die Menge der Einträge ist nicht limitiert.

Jeder Eintrag der General Deny Policy verbirgt die betroffenen Daten und verhindert deren Nutzung durch Nutzergruppen gemäß A_24306-*. Enthält ein Eintrag der Policy einen dynamischen Ordner oder eine Kategorie, so werden alle in diesem Ordner bzw. Kategorie enthaltenen Daten verborgen und von der Nutzung ausgeschlossen. Ein dynamischer Ordner selbst wird ebenfalls verborgen und von der Nutzung ausgeschlossen, eine Kategorie selbst wird nicht verborgen. Verborgene Daten schränken die Anwendung der Datenoperationen ein, die konkreten Auswirkungen sind bei den jeweiligen Operationen definiert.

Beim kategorienbasierten Verbergen von dynamischen Ordnern kann ein einzelner Ordner oder die Datenkategorie an sich verborgen werden. In letzterem Fall werden alle assoziierten Ordner verborgen.

Bei Kategorien und Ordnern, die zusammengesetzte MIOs oder strukturierte Dokumente enthalten (MIOs oder strukturierte Dokumente, deren Inhalt über mehrere Dokumente mit Zusammenhang verteilt ist - "Passdokumente") ist das Verbergen einzelner 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 Dokument, der Ordner oder die Kategorie im Aktensystem vorhanden sein. Wird im Verlauf von Operationen ein 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 19: Inhalt eines General Deny Policy Eintrags

Element		Inhalt	Erläuterung
denyType		"document" oder "folder" oder "category"	Art des zu verbergenden Inhalts,
parameter:			eine technische Referenz passend zu "denyType"
	rootDocumentId	documentEntry.referenceIdList, Item "rootDocumentUniqueId"	Identifier des zu

[choice]			verbergenden XDS Dokuments
	masterIdentifier	DocumentReference.masterIdentifier.value	Identifier des zu verbergenden MHD Dokuments
	folderUUID	folder.entryUUID	Identifier des zu verbergenden dynamischen Ordners
	categoryId	categoryId	technischer Identifier der zu verbergenden Kategorie

Beispiel:

Tabelle 20: Verbergen eines Medical Service

General Deny Policy - Verbergen der Datenkategorie "dental" (Daten aus der zahnärztlichen Dokumentation)		
denyType		"category"
parameters:		
	categoryId	"dental"

Das Verbergen eines einzelnen Dokuments zielt immer auf das Verbergen aller in der Replace-Kette enthaltenen Dokumente ab.

Die rootDocumentId in XDS verweist auf einen Identifier, der die gesamte Replace-Kette identifiziert. Der masterIdentifier in MHD hingegen verweist auf ein konkretes DocumentReference und damit implizit auf ein konkretes Dokument. Um sicherzustellen, dass in MHD das Dokument in seiner Gesamtheit (Replace-Kette) verborgen wird, muss die Replace-Kette eines Dokuments vollständig, d.h. die dazugehörige Liste von masterIdentifier, in die General Deny Policy aufgenommen werden. D.h. wird über die Schnittstelle `I_Constraint_Management` gemäß [I_Constraint_Management] der Parameter masterIdentifier auf die General Deny Policy gesetzt, dann muss das Constraint Management alle dazugehörigen masterIdentifier der Replace-Kette ermitteln und in die General Deny Policy aufnehmen.

A_30367 -Constraint Management - General Deny Policy bei MHD für Replace-Kette verarbeiten
Falls ein Dokument mittels masterIdentifier neu verborgen oder sichtbar gemacht wird, dann MUSS das Constraint Management zu diesem masterIdentifier die vollständige

Replace-Kette des Dokuments ermitteln und in der General Deny Policy mit denyType="document" für jedes Dokument der Replace-Kette den zugehörigen masterIdentifier zum Verbergen aufnehmen bzw. zum Sichtbar machen entfernen.**[<=]**

Der MHD Service übernimmt im weiteren Verlauf die Aktualisierung der General Deny Policy.

3.10.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes

Das Verbergen über den confidentialityCode ist im Kontext der Operationen des XDS Document Service definiert und in3.12.1.10- Verbergen von Dokumenten durch Verwendung des confidentialityCode beschrieben.

3.11 Device Management

Die Geräteverwaltung ermöglicht ePA-FdVs die Registrierung und Verwaltung der vom Nutzer verwendeten Geräte. Das Device Management stellt das API zum ePA-FdV für die Geräteverwaltung bereit und ist nur in einer VAU/authentisierten User Session erreichbar.

Im Folgenden wird als **Home-AS** eines Versicherten das ePA-Aktensystem desjenigen Betreibers bezeichnet, der vom Kostenträger des Versicherten beauftragt wurde. Falls der Versicherte der Anlage eines Aktenkontos nicht widersprochen hat, wird sein Aktenkonto im Home-AS verwaltet. Im Falle von Vertretern kann es vorkommen, dass das Home-AS des zu vertretenden Versicherten nicht das Home-AS des Vertreters ist.

Die E-Mail-Adressen und die Geräte eines Versicherten werden ausschließlich im Home-AS des Versicherten verwaltet. Für Vertreter, deren Home-AS nicht das Home-AS des Versicherten ist, können im Home-AS des Versicherten die im Home-AS des Vertreters registrierten Geräte nachgenutzt werden. Das ePA-Aktensystem bietet dem ePA-FdV eine Schnittstelle, über die die durch das Home-AS signierte Geräteinformationen abgerufen werden können.

Bei erstmaliger Nutzung des Gerätes initiiert das ePA-FdV die Geräteregistrierung und erhält dadurch eine DeviceID (bestehend aus deviceIdentifier und deviceToken), welche bei folgenden Verwendungen des ePA-FdV zur Identifizierung des Geräts verwendet wird. Eine neue Geräteregistrierung muss durch den Nutzer bestätigt werden. Der Zugriff auf ein Aktenkonto kann nur mit einem Gerät mit bestätigter Geräteregistrierung erfolgen.

Das Device Management ermittelt dazu die für den Nutzer im ePA-Aktensystem hinterlegte E-Mail-Adresse und versendet bei der Geräteregistrierung eine E-Mail an den Nutzer mit einem generierten Geräteregistrierungscode (confirmationCode). Der Nutzer sendet den Geräteregistrierungscode unter Verwendung des ePA-FdV zurück an das Device Management und bestätigt dadurch die Registrierung des neuen Geräts. Das Gerät kann nach der Bestätigung uneingeschränkt mit einem Aktenkonto genutzt werden.

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

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

A_26153 -Device Management - Nutzen von Device Management auch bei Widerspruch gegen Aktenkonto
Das Device Management MUSS sicherstellen, dass das Device Management auch von Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben.**[<=]**

A_26154-01 -ePA-Aktensystem - Ausschließlich Nutzen von Email Management und Device Management bei Widerspruch
Das ePA-Aktensystem MUSS sicherstellen, dass Versicherte, die einem Aktenkonto widersprochen haben, für sich selbst ausschließlich das Email Management und das Device Management nutzen können.**[<=]**

A_26155 -Device Management - Versicherte nutzen Device Management ausschließlich im Home-AS
Das Device Management des ePA-Aktensystems MUSS sicherstellen, dass das Device Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-Aktensystem das Home-AS ist.**[<=]**

A_24979 -Device Management - Sicheres Löschen von Geräten
Das Device Management MUSS beim Entfernen eines Gerätes sicherstellen, dass das Gerät gelöscht ist und dass das Gerät nicht mehr als verifiziertes Gerät genutzt werden kann.**[<=]**

A_17947-03 -Device Management - Gültigkeitszeitraum und Löschung der Devicekennung
Das Device Management MUSS jede generierte und zu einem Nutzer gespeicherte Geräteregistrierung nach 2 Jahren löschen und darf Nutzeranfragen mit dieser Device-Kennung nach diesem Zeitpunkt nicht mehr akzeptieren.
[<=]

Hinweis zu A_17947-*: Der Hersteller des ePA-FdVs kann die Nutzerführung seines ePA-FdVs so gestalten, dass der Versicherte auf ein baldiges Auslaufen der Registrierung hingewiesen wird und automatisch eine neue Registrierung vom ePA-FdV am Aktensystem ausgelöst wird.

A_14595-02 -Device Management - Pflegeprozess Geräteverwaltung
Das Device Management MUSS die interne Liste aller bekannten Geräte derart pflegen, dass ein Gerät nach spätestens 1 Jahr nach der letzten Nutzung des Gerätes automatisch aus der Liste der registrierten Geräte gelöscht wird.**[<=]**

Hinweis zu A_14595-*: Der Abruf einer Device Attestation durch ein registriertes Gerät gilt ebenfalls als eine Nutzung dieses Geräts.

A_25270 -Device Management - Erzeugung von Geräteinformationen und Geräteregistrierungscode bei der Geräteregistrierung
Das Device Management MUSS bei der Geräteregistrierung für das zu registrierende Gerät eines Nutzers

- einen deviceIdentifier als aktensystemweit eindeutigen Gerätebezeichner (uuid),
- ein deviceToken als eine Zufallszahl als String mit 64 Zeichen mit einer Mindestentropie von 120 Bit gemäß [gemSpec_Krypt#GS-A_4367] und
- eine zufällige sechsstellige natürliche Zahl als Geräteregistrierungscode

erzeugen.**[<=]**

A_25271-01 -Device Management - Speicherung der Geräteinformationen
Das Device Management MUSS bei einer Geräteregistrierung eines Geräts eines Nutzers folgende Inhalte für den Nutzer verschlüsselt persistieren:

- decviceIdentifier
- deviceToken

- createdAt (Zeitpunkt der Erzeugung des deviceTokens)
- lastUse
- status
- displayName
- Geräteregistrierungscode,
- Fehlerzähler.

[<=]

Hinweis zu A_25271-*: Für die verschlüsselte Speicherung der Geräteinformationen sind die Anforderungen aus Abschnitt 3.5.1.3 zu berücksichtigen.

A_25272 -Device Management - Pseudonyme Speicherung der Geräteinformationen
Das Device Management MUSS sicherstellen, dass die Zuordnung der außerhalb der VAU persistierten verschlüsselten Geräteinformationen zum Nutzer eindeutig ist und durch ein Pseudonym erfolgt.**[<=]**

Hinweis: Aus A_25272 folgt, dass die Zuordnung der Speicherung der verschlüsselten Geräteinformationen nicht über die KVNR des Nutzers erfolgen darf.

A_25273 -Device Management - Gültigkeitsdauer des Geräteregistrierungscodes
Das Device Management MUSS sicherstellen, dass der bei der Geräteregistrierung erzeugte Geräteregistrierungsscode maximal 6 Stunden nach Erzeugung der DeviceID (createdAt) für die Verifikation eines Gerätes genutzt werden kann.**[<=]**

A_25274 -Device Management - Löschen nach Gültigkeitsdauer des Geräteregistrierungscodes
Das Device Management MUSS sicherstellen, dass die Geräteinformationen für eine nicht bestätigte Geräteregistrierung nach Ende der Gültigkeitsdauer des Geräteregistrierungscodes gelöscht werden.**[<=]**

A_25275 -Device Management - Versenden des Geräteregistrierungscodes per E-Mail
Das Device Management MUSS bei der Geräteregistrierung für den Nutzer, für den das Gerät registriert werden soll, alle im Aktensystem hinterlegten E-Mail-Adressen ermitteln und an alle ermittelten E-Mail-Adressen eine E-Mail in einer für den Nutzer verständlichen Form mit folgenden Informationen versenden:

- Zweck der E-Mail,
- Geräteregistrierungsscode,
- Gültigkeitsdauer des Geräteregistrierungscodes.

[<=]

A_25276 -Device Management - Bestätigung mittels Geräteregistrierungscodes
Das Device Management MUSS für einen übergebenen Geräteregistrierungscode und eine übergebene DeviceID (deviceIdentifier und deviceToken) prüfen, ob der vom Device Management bei der Geräteregistrierung erzeugte Geräteregistrierungscode für das angegebene Gerät (deviceIdentifier, deviceToken) mit dem übergebenen Geräteregistrierungscode übereinstimmt sowie der Geräteregistrierungscode zeitlich gültig ist und

1. bei Gleichheit und
    a. zeitlicher Gültigkeit

- den Status für die Geräteregistrierung wechseln, so das die erfolgreiche Bestätigung des Geräts aus dem Status hervorgeht,
- den Geräteregistrierungscode und den Fehlerzähler aus den Geräteinformationen löschen und
- den Zeitpunkt der erfolgreichen Bestätigung in lastUsed erfassen,

b. zeitlicher Ungültigkeit

- alle Geräteinformationen zu diesem deviceIdentifier löschen,

2. bei Ungleichheit den Fehlerzählerder Geräteinformation um eins erhöhen und

- falls der Fehlerzähler größer oder gleich fünf ist,
  - alle Geräteinformationen zu diesem Gerät löschen.

[<=]

A_25277 -Device Management - Sperrung bei vermehrter Anzahl von abgebrochenen Geräteregistrierungen
Falls für einen Nutzer innerhalb von 8 Stunden drei Geräteregistrierungen abgebrochen werden mussten, MUSS das Device Management sicherstellen, dass dieser Nutzer für 8 Stunden ab dem Zeitpunkt der dritten abgebrochenen Geräteregistrierung keine Geräte mehr registrieren darf.**[<=]**

A_28157 -Device Management - Limitierung der Anzahl unbestätigter Geräteregistrierungen
Das Device Management MUSS die Anzahl der gleichzeitig unbestätigten Geräteregistrierungen eines Nutzers auf die maximale Anzahl 5 begrenzen.**[<=]**

A_25291 -ePA-Aktensystem - Health Record Context nur mit verifizierten Gerät
Das ePA-Aktensystem MUSS sicherstellen, dass ein Versicherter (auch wenn er als Vertreter agiert) einen Health Record Context ausschließlich mit einem verifizierten Gerät öffnen kann, außer für den Fall, dass sich der Versicherte am ePA-FdV des Vertreters anmeldet (d.h. `x-authorize-representative=True` bei der Operation`I_Authorization_Service::sendAuthorizationRequestFdV`).**[<=]**

Eine Geräteregistrierung im Home-AS kann in einem anderen Aktensystem nachgenutzt werden. Hierzu kann ein ePA-FdV mittels `getDeviceAttestation` eine Device Attestation vom Home-AS abrufen, welche beim anderen Aktensystem genutzt werden kann.

A_26157 -Device Management - Device Attestation kann nur mit verifiziertem Gerät abgerufen werden
Das Device Management MUSS sicherstellen, dass die Operation `getDeviceAttestation` ausschließlich nach erfolgreicher Authentifizierung des Nutzers und mit einem auf den Nutzer registrierten und verifizierten Gerät erfolgt.
[<=]

A_26156 -Device Management - Inhalte der Device Attestation
Das Device Management MUSS sicherstellen, dass eine von einem ePA-FdV über die Operation `getDeviceAttestation` abgerufene Device Attestation folgende Inhalte enthält:

Attribut	Inhalt
actorId	KVNR aus dem ID-Token des angemeldeten Nutzers (bzw. der User Session)
iat	Zeitstempel Ausgabezeitpunkt

exp	Verfalldatum, = "iat" + 2 Stunden

[<=]

A_26158 -Device Management - Signatur der Device Attestation
Das Device Management MUSS sicherstellen, dass die über `getDeviceAttestation` abgerufene Device Attestation mit dem privaten Schlüssel der Signaturidentität der VAU des Home-AS signiert wird.**[<=]**

A_28648 -ePA-Aktensystem - optionale Umsetzung von Snippet Management
Das ePA-Aktensystem KANN auf die Realisierung der Operationen des Snippet Management gemäß [I_Device_Management_Insurant] verzichten.**[<=]**

3.12 Medical Services

A_25830-05 -XDS Document Service - Reihenfolge der Auswertung Legal Policy, Deny Policy und Constraints
Der XDS Document Service MUSS bei der Nutzung von Operationen des XDS Document Service die Prüfung der zugriffsverhindernden Eigenschaften in der Reihenfolge

1. die statisch prüfbaren Beschränkungen des Aufrufenden bezüglich seiner Rolle,
2. die Existenz oder Einschränkungen aus dem Status des Aktenkontos,
3. die Befugnis des Aufrufenden,
4. die weiteren Beschränkungen der Legal Policy,
5. die Einträge der General Deny Policy.

anwenden.**[<=]**

Hinweis: Statisch prüfbare Beschränkungen sind Eigenschaften, die vor einer Öffnung der Akte bewertet werden können.
Hinweis: Beispielsweise kann eine Operation nicht erfolgreich ausgeführt werden, wenn diese den Vorgaben der Legal Policy und gleichzeitig einem Eintrag der General Deny Policy widerspricht. Die Fehlermeldung zum Abbruch der Operation resultiert dann aus der Prüfung der Legal Policy, da die Bedingungen dieser gemäß der definierten Reihenfolge vor den Bedingungen der General Deny Policy geprüft werden müssen.

3.12.1 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_25233 -XDS Document Service - erlaubte Formate für PDF-Dokumente
Der XDS Document Service MUSS sicherstellen, dass ausschließlich die folgenden PDF/A-Formate unterstützt werden:

- PDF/A-1a
- PDF/A-1b
- PDF/A-2a
- PDF/A-2u
- PDF/A-2b

[<=]

A_24864-05 -XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten
Der XDS Document Service MUSS beim Einstellen eines Dokumentes prüfen, dass das Dokument eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und den in Klammern angegebenen Dateiendungen (DocumentEntry.URI) besitzt

- application/pdf nur PDF/A gemäß A_25233 (pdf)
- application/hl7-v3 (xml)
- application/pkcs7-mime (p7s oder 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.**[<=]**

Hinweise zu A_24864-:*

- *Dokumente im PDF-Format werden vom XDS Document Service abgelehnt, da sie ausführbaren Code enthalten können. Daher müssen die Clients, falls sie Dokumente im PDF-Format einstellen wollen, diese zunächst in ein PDF/A konvertieren.*
- *p7s ist die Default-Dateiendung für Dokumente des mimetypes application/pkcs7-mime in der ePA und für Dokumente dieses mimetypes gemäß [gemSpec_IG_ePA] und für automatisierte Anpassungen von filename extensions bei Dokumentenupload (A_23447-*, A_24451-*) zu berücksichtigen.*

A_25009-04 -XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten durch Versicherte

Der XDS Document Service MUSS sicherstellen, dass Versicherte ausschließlich Dokumente eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und den in Klammern angegebenen Dateiendungen (DocumentEntry.URI) einstellen können:

- application/pdf nur PDF/A gemäß A_25233* (pdf)

[<=]

A_28620-01 -XDS Document Service - Mindestanforderungen an die Dokumentenformatprüfung
Die gemäß A_24864-* und A_25009-* geforderte Prüfung des zulässigen Dokumentenformats muss mindestens

- bei allen Formaten eine Prüfung auf Magic Bytes (soweit technisch möglich),
- bei XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es bei XML-Dokumenten kein valides UTF8 ist, prüfen auf "restriktives" ISO-8859-15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09, 0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind.",
- bei XML-, und JSON-Dokumenten eine Prüfung der XML- bzw. JSON-Validität mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet sind,
- auf den signierten Inhalt eines PKCS7-Dokuments sind die Regeln ebenfalls anzuwenden

umfassen.
Eine alleinige Prüfung auf Basis der Magic Bytes ist für kein Format ausreichend. Werden keine zusätzlichen Prüfmaßnahmen durchgeführt, dürfen die Dokumente nicht in die Akte eingestellt werden können.
Für XML-Dokumente muss eine Schema-Validierung ausschließlich auf Basis bekannter, intern vorliegender XML Schema-Definitionen durchgeführt werden. Gegen nicht intern vorliegende XML Schema-Definitionen wird nicht validiert. Die Schema-Validierung kann innerhalb des Health Record Contexts ohne zusätzliche Isolation erfolgen.**[<=]**

A_29876 -XDS Document Service - PKCS7 für signierte XML- oder JSON-Dokumente
Der XDS Document Service MUSS sicherstellen, dass der signierte Inhalt eines PKCS7-Dokuments ausschließlich ein XML- oder JSON-Dokument ist.**[<=]**

A_24867 -XDS Document Service - Isolation der Formatprüfung
Der XDS Document Service MUSS die Prüfung des Dateiformats (siehe A_24864-*) beim Einstellen eines Dokuments so technisch isolieren, dass kein Schaden für Aktenkonten oder das ePA-Aktensystem selbst entsteht.
[<=]

Hinweise zu A_24867-:*

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

Der in A_24636- geforderte technische Separationsmechanismus zur Isolation von Health Record Contexten innerhalb einer VAU-Instanz kann ebenfalls zur Isolation der Formatprüfung in A_24867-* genutzt werden.*

Findet eine Dokumentenformatprüfung innerhalb eines Health Record Context statt, wird durch den Isolationsmechanismus aus A_24636- verhindert, dass sich die Dokumentenformatprüfung schadhaft auf andere Health Record Contexte auswirkt. Es verbleibt dann zur Umsetzung der A_24867-* noch zu gewährleisten, dass sich die Dokumentenformatprüfung nicht schadhaft auf den Health Record Context auswirkt, in dem die Dokumentenformatprüfung erfolgt.*

Wenn Dokumentenprüfungen innerhalb eines Health Record Contexts ohne Isolation erfolgen, muss sichergestellt werden, dass sich diese Prüfungen nicht schadhaft auf den Health Record Context (oder andere) auswirken können. Dies ist vom Produktgutachter zu prüfen und im Produktgutachten zu dokumentieren.

Ein Ausschluss einer schadhaften Auswirkung auf den Health Record Context ist bei folgenden Prüfungen des Dokumentenformats denkbar, so dass diese innerhalb des Health Record Contexts ohne zusätzliche Isolationsmaßnahmen durchgeführt werden können und kein Verstoß gegen die Anforderung A_24867- vorliegt:*

- *Prüfung der Magic Bytes des Dokuments (wo technisch möglich)*
- *bei XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es bei XML-Dokumenten kein valides UTF8 ist, eine Prüfung auf "restriktives" ISO-8859-15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09, 0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind.",*
- *bei XML- und JSON-Dokumenten: Parsen der Dokumente auf valides XML bzw. JSON mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu bestätigen.*
- *bei pkcs7-Dokumenten: Parsen der Dokumente mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu bestätigen.*

Der Produktgutachter muss bei der Umsetzung der oben genannten Prüfungen bestätigen, dass der Ausschluss einer schadhaften Auswirkung auf den Health Record Context (oder andere) durch die Umsetzung im Produkt tatsächlich gegeben ist.

A_28663 -XDS Document Service – Keine PDF/A-Formatprüfung bei Import im Rahmen eines Aktenumzugs
Der XDS Document Service MUSS die Prüfung des Dateiformats (siehe A_24864-*) beim Importieren eines PDF/A-Dokuments im Rahmen eines Aktenumzugs (Health Record Relocation) abschalten.
[<=]

Die komplexe Validierung von PDF/A-Dokumenten in den Aktensystemen verschiedener Hersteller kann zu unterschiedlichen Ergebnissen führen (valide vs. nicht valide). Da jedoch die Validität im exportierenden Aktensystem und damit eine gewisse Formatqualität des Dokuments bereits nachgewiesen wurde, wird aus Gründen der Vollständigkeit der importierten Dokumente im importierenden System auf die Prüfung verzichtet.

A_25285 -XDS Document Service - Sicheres Löschen von Dokumenten mit unzulässigem Format
Falls der XDS Document Service bei der Prüfung des Dateiformats (siehe A_24864-*) beim Einstellen eines Dokuments ein unzulässiges Format erkennt, MUSS der XDS Document Service das Dokument sicher löschen.
[<=]

A_24943 -XDS Document Service - Formatprüfung exponiert keine Daten aus der VAU heraus
Der XDS Document Service MUSS sicherstellen, dass bei der Formatprüfung (siehe A_24864-*) keine innerhalb der VAU verarbeiteten Daten die VAU verlassen.**[<=]**

3.12.1.2 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_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.

A_29877-01 -XDS Document Service - Akzeptanz von PKCS7/CMS-Dokumenten
Der XDS Document Service MUSS sicherstellen, dass das ePA-Aktensystem ausschließlich das Einstellen von PKCS7/CMS-Dokumenten akzeptiert, bei denen der äußere Content Type der`oid 1.2.840.113549.1.7.2` und der der innere Content Type der `oid 1.2.840.113549.1.7.1`entspricht.**[<=]**

A_30008-01 -XDS Document Service - Fehlermeldung beim Ablehnen von PKCS7/CMS-Dokumenten mit ungültigem Content Type
Der XDS-Document Service MUSS das Einstellen eines PKCS7/CMS-Dokuments, welches nicht die Content Type Vorgaben aus A_29877-* erfüllt, mit dem Fehler

`InvalidDocumentContent` abbrechen und im `codeContext`-Attribut des zurückgegebenen XDSRegistryMetadataError-Elements den Text "errorText='Cannot register document: document has invalid cms content type'" zurückgeben.**[<=]**

Beispiel zu A_30008-*:
ErrorCode = InvalidDocumentContent
codeContext = "uniqueId='2.25.269167723254896828623';errorText='Cannot register document: document has invalid cms content type'"

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
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 ist3.12.1.4.2- 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 § 309-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" (siehe3.4- 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.**[<=]**

3.12.1.4.1.1 Gruppierungen mit anderen IHE ITI-Akteuren

3.12.1.4.1.2 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.**[<=]**

3.12.1.4.1.3 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 21: 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 22: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen des XDS Document Service

<table>
<tr><th rowspan="2">IHE ITI-Akteur</th><th rowspan="2">Opt.</th><th colspan="2"></th><th>Umzusetzende Option des IHE ITI-Akteurs</th><th>Opt.</th></tr>
<tr><th colspan="2">Gruppierung mit anderem IHE ITI-Akteur</th><th>Opt.</th><th colspan="2"></th></tr>
<tr><td>ATNA Audit Record Repository</td><td>X</td><td colspan="4" rowspan="2"></td></tr>
<tr><td>CT Time Client</td><td>X</td></tr>
<tr><td>XDS Document Consumer</td><td>X</td><td colspan="4"></td></tr>
<tr><td rowspan="6">XDS Document Registry</td><td rowspan="6">R</td><td colspan="2" rowspan="5"></td><td>Asynchronous Web Services Exchange</td><td>X</td></tr>
<tr><td>On-Demand Documents</td><td>X</td></tr>
<tr><td>Patient Identity Feed</td><td>X</td></tr>
<tr><td>Patient Identity Feed HL7v3</td><td>X</td></tr>
<tr><td>Reference ID</td><td>R</td></tr>
<tr><td colspan="2">ATNA Secure Node oder Secure Application</td><td>X</td><td colspan="2"></td></tr>
</table>

		für Node Authentication			
XDS Document Repository	R			Asynchronous Web Services Exchange	X
		ATNA Secure Node oder Secure Application für Node Authentication	X		
XDS Document Source	X				
XDS Integrated Document Source / Repository	X				
XDS On-Demand Document Source	X				
XDS Patient Identity Source	X				

3.12.1.4.3 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-TF2#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_24451-03 -XDS Document Service - Automatisches initiales Erzeugen einer versionsübergreifenden ID für Dokumente
Der XDS Document Service MUSS beim initialen Einstellen eines Dokumentes die DocumentEntry.uniqueId als Eintrag einer ReferenceID in die ReferenceIDList in folgendem Format einstellen:
`<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2023:rootDocumentUniqueId`
Beim Upload einer neuen Version des Dokumentes DARF dieser Eintrag in der ReferenceIdList, d.h. die rootDocumentUniqueId, NICHT verändert werden. Er bleibt über alle Versionen des Dokumentes hinweg unverändert erhalten. Der Versuch eines Clients, die `rootDocumentUniqueId` 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 `"errorText='Cannot register document: RootDocumentUniqueId must not be changed'"` zurückgegeben werden.**[<=]**

A_14926-04 -XDS Document Service – Automatisiertes Löschen oder Verbergen von Dokumenten in RPLC-Ketten
Der XDS Document Service MUSS bei zu löschenden oder zu verbergenden Dokumenten und DocumentEntry-Einträgen im selben Zuge auch alle mittels urn:ihe:iti:2007:AssociationType:RPLC assoziierten DocumentEntry-Einträge und Dokumente löschen bzw. verbergen.**[<=]**

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-TF2#3.41.4.1.2 und 3.41.4.1.3] und [IHE-ITI-TF2#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).

[<=]

RPLC-Ketten können je nach Dokumententyp in ihrer Länge beschränkt sein. Ggf. ist diese Beschränkung im jeweiligen Implementation Guide des Dokumententyps in [gemSpec_IG_ePA] unter dem Schlüsselwort "maxDocumentHistory" angegeben.

A_14938-04 -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 der Text `"errorText='Cannot register document: Metadata do not match A_14760'"` und wie folgt angegeben werden, welche Metadatenattribute nicht den Nutzungsvorgaben entsprechen: `"metadata=`<Name Metadatum_1>`;metadata=`<Name

Metadatum_2>;...;metadata=<Name Metadatum_n>"
[<=]

Hinweis:
uniqueId kann auch auf ein SubmissionSet zeigen. In diesem Fall entsprechen die Metadatenattribute des SubmissionSet nicht den Nutzungsvorgaben.

Beispiel:
```
codeContext =
"uniqueId='2.25.269167723254896828623';metadata='authorPerson';metadata='au
thorRole';errorText='Cannot register document: Metadata do not match
A_14760'"
```

A_28662-02 -XDS Document Service – Kein Code System mit Präfix "urn:oid"
Der XDS Document Service MUSS DocumentEntries, SubmissionSets, Associations und Folders ablehnen, wenn mindestens einer der verwendeten Codes einen Code System-Wert in den Metadaten enthält, der mit "urn:oid:" beginnt, und die entsprechende Operation mit dem FehlerXDSRegistryMetadataError abbrechen. Es MUSS im codeContext-Attribut des zurückgegebenen XDSRegistryMetadataError-Elements der Text "uniqueId='2.25.269167723254896828623';errorText='Cannot accept metadata: Code system must not contain urn:oid prefix'" zurückgegeben werden, wobei<uniqueId> dem uniqueId-Wert des entsprechenden Objekts (bspw. DocumentEntry.uniqueId) entsprechen muss.
[<=]

A_28841 -XDS Document Service – Persistierung neuer Metadaten mit "preferred" Identifier und ggf. Version
Der XDS Document Service MUSS beim Persistieren von DocumentEntries, SubmissionSets, Associations und Folders etwaige Codes in den Metadaten derart abspeichern, dass das entsprechende Code System immer mit dem Haupt-Identifier ("preferred" Name in [gemIG_TI_Terminology]) persistiert wird, auch wenn der Einstellende einen alternativen Identifier verwendet hat.
Wenn das Code System gemäß [gemIG_TI_Terminology] eine Version führt, muss diese ebenfalls persistiert werden.
[<=]

Ziel ist es eine möglichst konsistente und gleichförmige Datenbasis im Aktensystem zu pflegen.

A_28842-01 -XDS Document Service – Einstellen von Code Systeme ohne Versionsangabe
Der XDS Document Service MUSS beim Einstellen von DocumentEntry-Metadaten, die Codes enthalten, jeden Code, der mit einem Code System mit URL-basiertem Identifier aber ohne Versionsangabe geschickt wird, wie folgt behandeln:

1. Die aktuellste Version des Code System gemäß [gemIG_TI_Terminology], bzw. wenn dort nicht existent ggf. die aktuellste "deprecated"-Version gemäß A_28834*, wird ergänzt.
2. Prüfung, ob der Code in der derart konstruierten Version des Code System existiert.

Wenn der Code in der so konstruierten Version des Code Systems existiert, MUSS der XDS Document Service das Einstellen wie gewohnt fortsetzen, als wenn der Client den Code unter Angabe der neuesten Code System-Version gesendet hätte.

Andernfalls MUSS der XDS Document Service die Anfrage ggf. mit demselben Fehler ablehnen, der auch beim Einstellen mit einem anderen nicht existierenden Codes zurückgegeben würde.
[<=]

Diese Regelung erlaubt es, inbesondere KDL 2024-Codes bis auf weiteres in ePA 3.1.3 unter Angabe der Code System URL aber ohne Angabe der dazugehörigen Version einzustellen wie es in ePA 3.0.5 möglich war. Dies soll (insbesondere nicht auf 3.1.3 migrierten) Clients den Übergang von 3.0.5 nach 3.1.3 erleichtern.

A_28841* gilt auch hier nach wie vor, das heißt ggf. wird der Code mit Haupt-URL + Version persistiert.

Code Systeme, die über eine OID eingestellt werden, sind implizit (über die OID) versioniert und sind deshalb nicht für A_28842* relevant.

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_23124-01 -XDS Document Service – Addendum nur mit einem Dokument verknüpfen
Der XDS Document Service DARF ein Addendum NICHT mit mehr als einem Dokument verknüpfen.
Ist die Bedingung nicht erfüllt, MUSS der XDS Document Service das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-FehlercodeXDSRegistryMetadataError quittieren. Es MUSS im codeContext-Attribut des zurückgegebenenrs:RegistryError-Elements "errorText='Cannot create association: Only one addendum is allowed'" angegeben werden.**[<=]**

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 inDocumentEntry.hash hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die Dokumentengröße inDocumentEntry.size berechnet und gesetzt werden.**[<=]**

A_24988-03 -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, sofern nicht der Parameter "EnableDocumentReuse=true" (siehe A_27700*) verwendet wird.

Es MUSS im codeContext-Attribut des zurückgegebenenrs:RegistryError-Elements der Text "errorText='Cannot register document: Duplicate already exists'" die Liste der UUIDs (DocumentEntry.entryUUID), der in der Akte identifizierten Dokumente, wie folgt angegeben werden:
"entryUUID=<entryUUID von document_1>;entryUUID=<entryUUID von document_2>;...;entryUUID=<entryUUID von document_n>"
<=
[<=]

Der Fehler XDSDuplicateDocument ist für das einstellende Client-System einfach verständlich und eindeutig und deshalb allen anderen Fehlermeldungen, die aufgrund von weiteren Fehlern in den Metadaten gesendet werden könnten, vorzuziehen. Ob die zugrundeliegende Hash-Prüfung ganz am Anfang bei der Prüfung des einzustellenden DocumentEntries ausgeführt wird oder erst am Ende erfolgt, ist davon unberührt.

A_27700-02 -XDS Document Service - Option zum Akzeptieren von Duplikaten
Der XDS Document Service MUSS in der Lage sein Duplikate, das heißt Dokumente, bei dem der DocumentEntry.hash eines einzustellenden Dokuments identisch ist mit einem existierenden Dokument, ohne Fehler zu akzeptieren, wenn
die Anfrage in der `<RequestSlotList>` den folgenden Parameter enthält

```
<Slotname="urn:gematik:iti:xds:EnableDocumentReuse">
<ValueList>
  <Value>true</Value>
</ValueList>
</Slot>
```

und wenn

- die Anfrage auch erfolgreich wäre, wenn die Dokumente noch nicht vorhanden wären,
- das bestehende Dokument in derselben Kategorie existiert, in die auch das neue einsortiert würde,
- das bestehende Dokumente sichtbar ist für das einstellende System.

Wird der SubmissionRequest gemäß der obigen Bedingungen akzeptiert, MUSS der XDS Document Service

- den dazugehörigen einzustellenden DocumentEntry und die Association, die ihn mit dem mitgelieferten SubmissionSet verbindet, aus dem mitgelieferten SubmissionSet entfernen,
- das SubmissionSet selbst verwerfen, sofern keine Associations, DocumentEntries oder Folders neu gespeichert werden (es also im Endeffekt "leer" wäre),
- neu mitgesendete Anhangsbeziehungen mit dem bestehenden Dokument verknüpfen (sofern durch andere Anforderungen nicht verhindert) und bestehende Anhangsbeziehungen erhalten,
- die Antwort (mit dem üblichen Status "`Success`") in der`<RegistryResponse>` um folgende `<ResponseSlotList>` ergänzen (mit einem Slot für jedes vorhandene Dokument):

  ```
  <ResponseSlotList>
  <Slotname="urn:gematik:iti:xds:ReusedDocumentMapping">
  <ValueList>
    <Value>$uniqueId_neu|$uniqueId_alt</Value>
  </ValueList>
  </Slot>
  </ResponseSlotList>
  ```

  wobei `$uniqueId_neu` die DocumentEntry.uniqueId des Dokuments aus dem SubmissionRequest ist, während `$uniqueId_alt` die DocumentEntry.uniqueId des bestehenden Dokuments darstellt.

Wird das Dokument nicht akzeptiert, MUSS der XDS Document Service

- mit dem Fehler `XDSRegistryMetadataError` und im `codeContext`-Attribut des zurückgegebenen`rs:RegistryError`-Elements den Text "`errorText='Cannot register document: Duplicate does not match category of existing document'`" antworten, wenn die Kategorie des neuen Dokuments abweicht,
- mit dem Fehler `XDSInvalidRequest` und im `codeContext`-Attribut des zurückgegebenen`rs:RegistryError-Elements den Text "errorText='Cannot register document: EnableDocumentReuse only allows value true to`

indicate duplicate'" antworten, wenn der Parameter "EnableDocumentReuse" mit einem anderen Wert als "true" verwendet wird,

- ansonsten mit dem üblichen Fehler antworten, der auch sonst beim Einstellen der Anfrage (d.h. ohneEnableDocumentReuse) zurückgegeben würde.

[<=]

Hintergrund ist, dass die Information, dass es sich um eine Dublette handelt, für das einstellende System hilfreicher und spezifischer ist als ein Metadatenfehler, dass bspw. die angelieferte uniqueId "falsch" ist.

A_24990 -XDS Document Service - Dublettenprüfung für dynamische Ordner
Der XDS Document Service MUSS beim Anlegen dynamischer Folder prüfen, ob ein Ordner bereits existiert, der gemäß vom Titel her identisch ist mit demjenigen, den der Client einzustellen versucht. Im Falle eines identischen Titels MUSS der Einstellversuch mit dem Fehlercode `XDSDuplicateFolder` abgelehnt werden.**[<=]**

A_30511 -XDS Document Service – Dublettenprüfung gegen Dokumente des MHD Service
Der XDS Document Service MUSS die Dublettenprüfung gemäß A_24988-* beim Einstellen von Dokumenten auch gegen die Dokumente der Akte durchführen, die nicht über den XDS Document Service eingestellt wurden (über den MHD Service eingestellte oder vom MHD Service erzeugte Dokumente). Für diese Dokumente MUSS der XDS Document Service den Hash-Wert mit SHA-256 über deren Dokumentinhalt bilden (vgl. A_24521), um ihn mit dem einzustellenden Dokument zu vergleichen.
Stimmt der Hash-Wert ausschließlich mit Dokumenten überein, die nicht über den XDS Document Service eingestellt wurden, MUSS der XDS Document Service die Anfrage auch bei Verwendung des Parameters `EnableDocumentReuse=true` (A_27700-*) mit dem Fehlercode `XDSDuplicateDocument` gemäß A_24988-* ablehnen.
[<=]

A_30512 -XDS Document Service – Eindeutigkeit der uniqueId gegenüber Dokumenten des MHD Service
Der XDS Document Service MUSS beim Einstellen von Dokumenten prüfen, ob die `DocumentEntry.uniqueId` bereits von einem Dokument der Akte verwendet wird, das nicht über den XDS Document Service eingestellt wurde (`DocumentReference.masterIdentifier.value` gemäß [gemIG_ePA_MHD]). Ist das der Fall und weicht der Hash-Wert ab, MUSS der XDS Document Service das Einstellen mit dem Fehlercode `XDSNonIdenticalHash` ablehnen.
[<=]

Hinweis: Der MHD Service prüft beim Einstellen bereits gegen Dubletten im XDS Document Service. Erst mit diesen Anforderungen gilt die Dublettenprüfung in beide Richtungen. Der MHD Service legt für seine Dokumente den Hash mit SHA-1 ab. Für den Vergleich braucht der XDS Document Service deshalb einen eigenen SHA-256-Wert dieser Dokumente.

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 Transportcodierung. Größere Dokumente können nicht hochgeladen werden.

A_23098-03 -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 `"errorText='Cannot register document: Version of submitted structured document is not supported'"` zurückgegeben werden.**[<=]**

Beispiel:
codeContext = `"uniqueId='2.25.269167723254896828623';errorText='Cannot register document: Version of submitted structured document is not supported'"`

A_21610-04 -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 und andernfalls mit dem FehlerXDSRegistryMetadataError antworten. Im `codeContext`-Attribut des zurückgegebenen`rs:RegistryError`-Elements MUSS in dem Fall der Text`"errorText='Cannot create folder: Invalid category'"` enthalten sein.**[<=]**

A_24797-05 -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.Es MUSS im `codeContext`-Attribut des zurückgegebenen rs:RegistryError-Elements wie folgt angegeben werden, welche Metadatenattribute nicht den Nutzungsvorgaben entsprechen:
`"errorText='Cannot register document: Change of metadata not allowed';metadata=`<Name Metadatum_1>`;metadata=`<Name Metadatum_2>`;...;metadata=`<Name Metadatum_n>"
Einzige Ausnahmen sind:

- Metadatenattribute creationTime, entryUUID sowie uniqueId und confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491).
- Das Metadatenattribut DocumentEntry.referenceIdList DARF ohne die rootDocumentUniqueId gesendet werden; in dem Fall wird die rootDocumentUniqueId automatisch vom XDS Document Service gesetzt (Wert identisch zu dem des ersetzten Dokuments).

[<=]

A_27760-02 -XDS Document Service - Ablehnen von RPLC-Ersetzungen bei nicht erlaubten Dokumententypen
Der XDS Document Service MUSS das Ersetzen von Dokumenten via RPLC-Associations mit dem Fehlercode `XDSReplacementForbidden` ablehnen und in `codeContext`-Attribut des zurückgegebenen`rs:RegistryError`-Elements `"errorText='Cannot replace document: formatCode not allowed'"` angegeben, wenn das zu ersetzende Dokument weder einen der folgenden DocumentEntry.formatCode-Werte besitzt,

Tabelle 23 : Liste mit Dokumententypen, die ersetzt werden können

Dokument	codeSystem	code
NFD	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:Notfalldatensatz:r3.1
DPE	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1
DiGA	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:diga:v1.1
Notizen Kinderuntersuchungsheft	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:KinderuntersuchungsheftNotizen:v1.0.1

noch in einen der folgenden Ordner einsortiert ist:

Tabelle 24 : Liste mit Ordnern, in denen Dokumente ersetzt werden dürfen

Ordner-Kategorie	Folder.entryUUID	
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d	
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31	

[<=]

Die Länge von RPLC-Ketten (d.h. die Anzahl Dokumente, die über RPLC-Assoziationen miteinander in Kette verbunden werden können), kann über [gemSpec_IG_ePA] für ausgewählte strukturierte Dokumente weiter eingeschränkt werden.

A_27764 -XDS Document Service - Keine Anhangsbeziehungen mit Sammlungsdokumententypen
Der XDS Document Service MUSS das Etablieren von Anhangsbeziehungen zu allen Dokumententypen, die in Sammlungen (mixed oder uniform) organisiert werden, unterbinden und mit dem Fehler `XDSAttachmentForbidden` ablehnen.
[<=]

A_27763-01 -XDS Document Service - Keine Anhangsbeziehungen mit RPLC-fähigen Dokumententypen
Der XDS Document Service MUSS das Etablieren von Anhangsbeziehungen zu allen Dokumententypen, die in RPLC-Ketten verwendet werden dürfen (siehe A_27760) oder die bereits aufgrund der Migration von Altdaten in RPLC-Beziehungen stehen, unterbinden und mit dem Fehler `XDSAttachmentForbidden` ablehnen.
[<=]

Seit ePA 3.1.2 ist das Ersetzen von Dokumenten via RPLC-Associations nur noch für die oben aufgeführten Dokumententypen bzw. -kategorien erlaubt. Der Versuch, andere Dokumententypen zu ersetzen, führt zu einem Fehler. Es kann Altdaten geben, die diese Regel noch missachten. Neue Ersetzung für diese Altdaten werden jedoch gleichermaßen fehlschlagen; d.h. neue Ersetzungen sind nur noch für die oben angegebenen Dokumententypen erlaubt.

Die Notizen zum Kinderuntersuchungsheft können in zwei Versionen in der Akte vorliegen: Die alte Version 1.0.0 kann nicht mehr neu eingestellt werden, sondern nur die

Version 1.0.1. Altdokumente in Version 1.0.0 können nicht ersetzt werden durch Dokumente in der Version 1.0.1, da A_27760* dies verbietet. Stattdessen muss an dieser Stelle das alte Dokument in der Version 1.0.0 gelöscht und das neue in Version 1.0.1 neu eingestellt werden.

A_24531-05 -Constraint Management - Verbergen von Dokumenten durch confidentialityCode
Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491)durch eine Nutzergruppe der Rolle`oid_versicherter`eingestellt wird, nicht Bestandteil einer Sammlung der Ausprägung "mixed" oder "uniform" ist,und kein Dokument der Kategorie "emp" ist, dann MUSS der XDS Document Service sicherstellen, dass das Dokument durch einen Eintrag in der General Deny Policy verborgen wird. Es MUSS ein Eintrag mit denyType = "document" für die General Deny Policy erzeugt werden.**[<=]**

A_25856-03 -XDS Document Service - Fehlerhaftes Verbergen von Dokumenten durch confidentialityCode
Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) nichtdurch eine Nutzergruppe der Rolle`oid_versicherter`eingestellt wird, oder Bestandteil einer Sammlung der Ausprägung "mixed" oder "uniform" ist, dann MUSS der XDS Document Service die Operation abbrechen und mit einem Fehlercode ConstraintViolation beenden.**[<=]**

Das Verbergen von Dokumenten ist in Kapitel 3.12.1.10- Verbergen von Dokumenten durch Verwendung des confidentialityCode beschrieben.

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-TF2#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-TF2#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-TF2#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_25183-02 -XDS Document Service – Suchanfragen über das Metadatenattribut DocumentEntry.comments
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-TF2#3.18.4.1.2.3.7.1]sowie die weiteren verpflichtenden Suchparameter `$XDSDocumentEntryComments` und `$XDSDocumentEntryComment` (deprecated)unterstützen, sodass eine Suchergebnismenge über das Attribut `DocumentEntry.comments` eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter `$XDSDocumentEntryAuthorPerson`. Es muss mindestens einer der beiden Suchparameter in diesem Anfragetyp enthalten sein, anderenfalls MUSS der XDS Document Service mit dem Fehlercode `XDSStoredQueryMissingParam` antworten. Bei gleichzeitiger Übermittlung beider Suchparameter DARF NUR der Suchparameter `$XDSDocumentEntryComments` für die Suchanfrage verarbeitet werden.`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_24764-01 -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
  - $XDSDocumentEntryComments
  - $XDSDocumentEntryComment (deprecated)
- Query "FindSubmissionSets"
  - $XDSSubmissionSetAuthorPerson

Dabei MUSS der XDS Document Service mindestens unscharfe Ergebnisse bezüglich Groß-/Kleinschreibung unterstützen, also Groß-/Kleinschreibung für die angegebenen Parameter der ausgewählten Query-Typen ignorieren.
[<=]

Das zur Ermittlung weiterer unscharfer Ergebnisse vom XDS Document Service einzusetzende Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu liefern, die ihm möglicherweise sonst wegen beispielsweise falscher Schreibweise eines Namens (z. B. "Meyer" vs. "Maier") vorenthalten worden wäre. Dabei sind Verfahren wie die Kölner Phonetik aber auch andere Mechanismen denkbar.

A_28668 -Unscharfe Suche über Metadatenattribute mit Code System Version
Der XDS Document Service MUSS bei Belegung des Suchparameters$XDSDocumentEntryEventCodeList in einer Registry Stored Query [ITI-18] die Suche sowohl mit als auch ohne Angabe einer angestellten Code System Version per Pipe-Symbol (|) durchführen. Ist keine Code System Version angegeben, MUSS der XDS Document Service DocumentEntry-Einträge finden, welche mit einer beliebigen Version gespeichert wurden.**[<=]**

A_28844 -XDS Document Service – Suche nach Code System mit Haupt-Identifier und Version
Der XDS Document Service MUSS bei Belegung eines Suchparameters mit einem Code in einer Registry Stored Query [ITI-18] die Suche wie folgt durchführen:
Bei Code Systemen MUSS der XDS Document Service zur Ermittlung von Treffern in der Datenbasis auch Ergebnisse finden, bei denen der entsprechende Code mit einem äquivalenten Identifier für das jeweilige Code System gespeichert ist. Dies betrift Coding Systems gemäß [gemIG_TI_Terminology] oder die als "deprecated" gelisteten Code Systems gemäß A_28834, sofern an der jeweiligen Stelle mehr als ein Identifier für das angefragte Code System festgelegt ist.
Wenn der XDS Document Service später für diese Suche einen DocumentEntry zurückgeliefert, MUSS statt des vom Client gelieferten Code-System-Werts stattdessen der Haupt-Identifier inklusive Versionsangabe zurückgeliefert werden.
[<=]

Damit werden bei der Suche die verschiedenen Identifier eines Code Systems als äquivalent behandelt; das heißt, der Client darf einen beliebigen Namen für ein Code System verwenden und der XDS Document Service muss auch dann einen Treffer generieren, wenn der entsprechende Code mit einem anderen Identifier für dasselbe Code System in der Datenbasis gespeichert wird.

Unabhängig von der Anfrage gibt der XDS Document Service also dem Client das Code System immer mit Haupt-Identifier zurück.

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_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_21714-04 -XDS Document Service – Löschen von strukturierten Dokumenten durch ein ePA-FdV
Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie

zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die Nachricht mit dem`XDSRegistryError`-Fehlercode zurückgeben werden.Es MUSS im `codeContext`-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert `"errorText='Cannot delete folder: Use only entryUUID of folder'"` belegt werden.**[<=]**

A_21817-04 -XDS Document Service – Löschen von strukturierten Dokumenten durch ein Primärsystem
Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein Primärsystem ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die Nachricht mit`XDSRegistryError`-Fehlercode zurückgeben werden. Es MUSS im `codeContext`-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert `"errorText='Cannot delete folder: Use only entryUUID of folder'"` belegt werden. **[<=]**

Beispiel:
errorCode = `XDSRegistryError`
codeContext = `"entryUUID='2.25.514739840497321348259';errorText='Cannot delete folder: Use only entryUUID of folder'"`

A_24663-01 -XDS Document Service – Bereinigung der General Deny Policy
Der XDS Document Service MUSS als Folge von erfolgreichen Löschanfragen alle Einträge der General Deny Policy entfernen, welche die betroffenen Dokumente oder dynamischen Ordner referenzieren.**[<=]**

A_24765 -XDS Document Service – Kein Löschen von statischen Ordnern und Associations
Der XDS Document Service MUSS sicherstellen, dass eine Löschanfrage keine statischen Ordner und Assoziationen löschen darf. Dies gilt nicht für dynamische Ordner. Der XDS Document Service MUSS bei Löschung eines Dokumentes die Assoziation zum Folder löschen.**[<=]**

Dynamische Ordner sind beispielsweise Mutterpass (folderCode = pregnancy_childbirth) oder DiGA (folderCode = diga).

A_20579-03 -XDS Document Service – Löschen von Ordnern
Der XDS Document Service MUSS Requests, die darauf abzielen, einen statischen Folder direkt zu löschen, ablehnen und mit dem Fehler`XDSRegistryMetadataError` und im `codeContext`-Attribut des zurückgegebenen`rs:RegistryError`-Elements den Text `"errorText='Cannot delete folder: Invalid category'"` antworten. **[<=]**

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-TF2#3.43.4.1.2 und 3.43.4.1.3] und [IHE-ITI-TF2#3.43.4.2.2 und 3.43.4.2.3] implementieren.**[<=]**

A_16201 -XDS Document Service – Prüfung der zurückgegebenen Paketgröße
Der XDS Document Service MUSS anhand der übergebenen DocumentUniqueIDs die Gesamtgröße ermitteln und bei Überschreitung von 250 MByte die Verarbeitung ablehnen und die Nachricht mit einem`MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.**[<=]**

3.12.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen

A_24508-01 -XDS Document Service – Prüfung der Policies bei Suchanfrage

Der XDS Document Service MUSS bei einer Suchanfrage für einen angemeldeten Nutzer die Suchergebnismenge entsprechend der Legal Policy und der General Deny Policy filtern, d. h. die Suchergebnismenge enthält ausschließlich XDS-Metadaten, die für einen angemeldeten Nutzer nicht diesen Policies widersprechen.**[<=]**

A_24509-01 -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 der Fehlertext `"errorText='Legal Policy violation'"` angegeben werden.**[<=]**

A_24510-02 -XDS Document Service – Prüfung Herunterladen eines verborgenen oder nicht vorhandenen Dokuments
Der XDS Document Service MUSS die Ausführung der Retrieve-Operation mit dem Fehlercode XDSDocumentUniqueIdError beenden, wenn das assoziierte Dokument nicht vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.**[<=]**

A_24511-01 -XDS Document Service – Prüfung Löschen eines verborgenen Dokuments oder dynamischen Ordners
Der XDS Document Service MUSS die Ausführung der Remove-Operation mit dem Fehlercode XDSDocumentUniqueIdError beenden, wenn für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.
[<=]

A_24512-02 -XDS Document Service – Prüfung Schreiben eines Dokuments in einen nicht vorhandenen oder verborgenen dynamischen Ordner
Der XDS Document Service MUSS die Ausführung der Provide-Operation mit dem Fehlercode UnresolvedReferenceException beenden, wenn der Ordner nicht existiert oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.
[<=]

A_28858 -XDS Document Service – Prüfung Schreiben eines Dokuments in einen verborgenen statischen Ordner
Der XDS Document Service MUSS die Ausführung der Provide-Operation mit dem Fehlercode `XDSFolderAccessDenied` beenden, wenn der Ordner für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.
[<=]

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.**[<=]**

A_26324-04 -XDS Document Service - Aktenkonto im Umzug oder im Wartungsmodus
Falls sich ein Aktenkonto im Zustand SUSPENDED oder im Status INACCESSIBLE befindet MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem`StatusMismatch`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren und im

codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements den passenden Fehlertext mit "errorText=<Fehlertext>" angeben:

Tabelle 25 : Fehlertexte zu StatusMismatch-Fehlercode

Aktenkontostatus	Wert für <Fehlertext> in codeContext
SUSPENDED	'Health Record Relocation in progress'
INACCESSIBLE	'Health Record is inaccessible'

<=[<=]

A_26325-01 -XDS Document Service - Aktenkonto unbekannt oder im Zustand INITIALIZED
Falls sich ein Aktenkonto im Zustand UNKNOWN oder INITIALIZED befindet MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem NoHealthRecord-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.<=[<=]

A_25683-01 -XDS Document Service - Prüfung auf Befugnis
Falls keine gültige Befugnis für den aufrufenden Nutzer vorliegt MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem NotEntitled-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.[<=]

A_26459 -XDS Document Service - keine Authentisierung des Nutzers
Falls keine erfolgreiche Authentifizierung des Nutzers vorliegt MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem InvalAuth-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.<=[<=]

A_27541 -XDS Document Service - keine Geräteregistrierung des Nutzers
Falls der Nutzer der Versicherte oder ein Vertreter ist (oid_versicherter) und keine Geräteregistrierung des Nutzers vorliegt, MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem UnregisteredDevice-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.[<=]

A_28142-02 -XDS Document Service – Fehler Verwendung von Codes im Status inactive
Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit dem Fehler XDSInactiveCode quittieren, falls ein Metadatum Code den Status "inactive" besitzt. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Text "errorText='Cannot update metadata: Code is inactive'" angegeben werden und welche der Codes nicht mehr unterstützt werden (im Format "code^^codeSystem" bzw. ggf. mit Version gemäß A_27759 "code^^codeSystem|version"):
"code=<code_1^^codeSystem_1>;code=<code_2^^codeSystem_2>;...;code=<code_n^^codeSystem_n>"
Es gibt eine Ausnahme: Beim Ersetzen eines Dokuments in der RPLC-Kette wird ein Code im Status "inactive" akzeptiert, sofern er bereits auch an dieser Stelle im zu ersetzenden Objekt vorhanden ist. In diesem Fall MUSS der XDS Document Service den Code ohne Fehler verarbeiten können.[<=]

Allgemeine Anforderungen zu Fehlermeldungen

Aus der Fehlermeldung soll hervorgehen welches Dokument den Fehler verursacht hat. Bei einer konkreten Fehlerprüfung sollen alle Dokumente des SubmissionSet auf diesen Fehler geprüft werden, ohne nach dem ersten Auftreten des Fehlers abzubrechen. Es soll die Möglichkeit geben, dass weitere Informationen zu diesem Fehler zurückgegeben werden.

Es wird geregelt, wie im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die Informationen zum Fehler angegeben werden.

A_28657 -XDS Document Service – Fehlerprüfung für alle im Request enthaltenen Dokumente
Der XDS Document Service MUSS alle im SubmissionSet enthaltenen Dokumente in eine konkrete Fehlerprüfung einbeziehen ohne nach dem erstem Fehler abzubrechen. Die RegistryErrorList MUSS jeweils einen RegistryError für jedes zu diesem Fehler erkannte Dokument enthalten, wobei der Inhalt des RegistryError den Vorgaben für diesen Fehler entsprechen muss.**[<=]**

Hinweis:
Die Anforderung bezieht sich auf eine konkrete Fehlerprüfung. Ziel ist es nicht, alle Ergebnisse aller Fehlerprüfungen in der Response zu übermitteln.

A_28654-02 -XDS Document Service – Fehler mit uniqueId in codeContext
Falls im XDS Document Service ein IHE-Fehler auftritt, der sich auf ein SubmissionSet, DocumentEntry oder Folder zurückführen lässt, und dessen uniqueId bekannt ist und für den Fehler keine spezifischere Fehlerregelung vorgegeben ist, MUSS in codeContext die entsprechende uniqueId wie folgt enthalten sein: `"uniqueId='<DocumentEntry|SubmissionSet|Folder.uniqueId>'"`.
Kann die uniqueId nicht ermittelt bzw. darf nicht zurückgegeben werden (z.B. Dokument verborgen), dann wird stattdessen die entryUUID angegeben mit:
`"entryUUID='<DocumentEntry|SubmissionSet|Folder.entryUUID>'"`.**[<=]**

Beispiel:
codeContext = `"uniqueId='2.25.269167723254896828623'"`

Hinweis:
Der Fehler, dass die Telematik-ID nicht zur Session passt (A_24497*), erfolgt ohne Angabe der uniqueId.

A_28655 -XDS Document Service – Formatvorgaben für CodeContext
Der XDS Document Service MUSS Key-Value Paare in codeContext nach folgenden Regeln behandeln:

- Key-Value Paare sind mit <key>=<value> gekennzeichnet,
- Die Reihenfolge der Key-Value Paare ist nicht vorgegeben,
- Trennung von Key-Value Paaren erfolgt mit ‘;’ ,
- <key> wird normativ vorgegeben und kann gegebenenfalls mehrfach auftreten,
- ein identisches Key-Value Paar kann in einem codeContext nur einmal auftreten,
  Für <value> gilt:
  - value wird immer durch Hochkommata ("'") umschlossen, z.B.:
    errorText='RootDocumentUniqueId must not be changed'
  - Escape von einfachen Anführungszeichen (‘) erfolgt mit "\‘",
  - Escape von Backslash (\) erfolgt mit "\\",
  - Maximale Anzahl von Zeichen: 1000 (Single Quotes als Beginn und Endezeichen zählen mit),
  - White spaces sind außerhalb von <value> nicht erlaubt.

[<=]

A_28656 -XDS Document Service – Format für Fehlerdetail
Der XDS Document Service KANN bei einem IHE-Fehler weitere Informationen zur Fehleranalyse im`codeContext` des Fehlers als <key>=<value>-Paar einfügen, ausschließlich mit:

- `errorDetail='<Details zum Fehler>'`
- `<Details zum Fehler>='<weiterführende Informationen zum Fehler>'`
  In der Produktivumgebung gilt: Es dürfen keine personenbezogenen Daten, medizinische Daten, Error Stack Traces oder die Offenbarung von Programmierdetails enthalten sein.

[<=]

Beispiel:
ErrorCode =`InvalidDocumentContent`
codeContext =
`"uniqueId='2.25.269167723254896828623';errorDetail='Fehlerhafter Aufrufparameter [PDF service encountered an unacceptable document format for validatePDF'"`

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_26814-*, werden sonst bei IHE ITI explizite Operationen zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne Umsetzung angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-Nachricht kann an IHE ITI-konforme Akteure ausgerichtet werden.

3.12.1.6.1 Schnittstelle I_Document_Management

Weitere Vorgaben zu den Operationen befinden sich in3.12.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen .

A_14152-03 -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 26: Schnittstelle I_Document_Management

Schnittstelle	I_Document_Management	
Version	3.0.0	
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
WSDL	[XDSDocumentService]	
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-TF2] sowie Appendix V aus [IHE-ITI-TF2] zu entnehmen.

Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner gesammelt. Das Anlegen eines DiGA-Ordners erfolgt durch den XDS Document Service unter der Voraussetzung, dass es eine gültige Befugnis für die DiGA gibt. Der DiGA-Ordner wird vom XDS Document Service mit der Telematik-ID der DiGA verknüpft.
Die Zuordnung von DiGA-Dokumenten beim Schreiben erfolgt implizit über die TelematikID aus dem IDToken des Nutzers. Da ein DiGA-Ordner im Titel immer den Namen der DiGA enthält kann ein Client (z.B. LEI) darüber die relvante DiGA auswählen und auf die Dokumente der DiGA, sofern eine Befugnis für den Nutzer vorliegt, lesend zugreifen.
Ein Update eines bestehenden Dokuments mit der bekannten DocumentEntry.entryUUID kann durch einen DiGA-Client erfolgen. Hierzu ist es erforderlich, dass ein DiGA-Client die DocumentEntry.entryUUID persistiert und keine symbolischen IDs gemäß [IHE-ITI-TF2#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_24497-01 -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 `"errorText='Telematik-ID does not match'"` angeben.**[<=]**

A_24456-01 -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 `"errorText='Cannot register document: Medical information object has to be unique'"` zurückgegeben werden.**[<=]**

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-TF2] sowie Appendix V aus [IHE-ITI-TF2] 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-TF2] 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-TF2], sowie Appendix V aus [IHE-ITI-TF2] zu entnehmen.

3.12.1.6.2 Schnittstelle I_Document_Management_Insurant

Weitere Vorgaben zu den Operationen befinden sich in3.12.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen .

A_14478-03 -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 27: Schnittstelle I_Document_Management_Insurant

Schnittstelle	**I_Document_Management_Insurant**	
Version	3.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente im XDS Document Service
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Metadata	Löschen ein oder mehrerer Dokumente oder Folder
WSDL	[XDSDocumentService]	
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

[<=]

A_26460 -XDS Document Service - Zugriff über I_Document_Management_Insurant mit nicht registriertem Gerät
Falls Operationen von I_Document_Management_Insurant ohne registriertes Gerät aufgerufen werden MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem`UnregisteredDevice`-Fehlercode quittieren.**[<=]**

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-TF2] sowie Appendix V aus [IHE-ITI-TF2] zu entnehmen.

A_21481-04 -XDS Document Service – Kein Einstellen von Ordnern und Associations
Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) über die Schnittstelle I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b() ablehnen und mit einem XDSRegistryMetadataError-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder oder andere als die folgenden Assoziationen

- SS-DE
- SS-HM
- FD-DE
- RPLC
- 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_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-TF2] sowie Appendix V aus [IHE-ITI-TF2] zu entnehmen.

3.12.1.6.2.3 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-TF2] sowie Appendix V aus [IHE-ITI-TF2] zu entnehmen.

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_24491-02 -XDS Document Service – Anlegen von statischen Ordnern
Der XDS Document Service MUSSnach 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 28: Festlegung Folder.entryUUIDzu statischen Ordnern

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
reports	b878db05-49e4-4f74-a329-b3bcdd8082c4
emp	7c1054ea-a4df-4a1b-8e10-209f6d8812ee
emergency	a7bb6be7-d756-46dd-90d4-4020ed55b777
eab	2ed345b1-35a3-49e1-a4af-d71ca4f23e57
dental	af547321-b8e8-4e1d-b9af-51bb4a990bda
child	2c898452-4667-40e3-9d3e-c09d7385b527
vaccination	9c3edaf3-a978-46fe-8e6e-021ff4aca60b
patient	d236c9a2-ab01-4902-a00a-1e1dff439fe7

receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d
health_risk_analysis	840a59c7-61d4-4caa-80a7-1857af2f166f
care	2d62bf9e-062a-4aa7-9951-9f33bbc665b5
eau	aa7d10d6-204a-47aa-be73-44bdcb77512f
other	605a9f3c-bfe8-4830-a3e3-25a4ec6612cb
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31
rehab	173f4204-fb93-4a1a-a1f6-316703b79539
transcripts	6A8E383D-8705-4B0E-A140-39A5F144501D

[<=]

Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner vom Typ "pregnancy_childbirth" und verwenden als Folder.title ein Kennzeichen der Schwangerschaft.

A_20216-04 -XDS Document Service – Unveränderlichkeit von statischen Akteninhalten
Der XDS Document Service DARF die Metadaten eines statischen Aktenobjekts gemäß A_24491 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen. Dabei gelten folgende Ausnahmen:

- Folder.lastUpdateTime - Folder.lastUpdateTime wird automatisch vomXDS Document Service aktualisiert, sobald Dokumente in den Ordner eingestellt (siehe auch [IHE-ITI-TF2#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6]), daraus gelöscht oder darin aktualisiert werden.

[<=]

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_14760-31 -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 werden.

Für den Produkttyp DiGA gelten die gleichen Vorgaben wie für die Primärsysteme sofern unter Nutzungsvorgaben keine abweichenden Bedingungen definiert werden.

Tabelle 29: 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	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.1] genügen. Das Primärsystem MUSS	

					erstellt hat	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 Value Sets EPAXDSAuthorRoleVS aus [gemIG_TI_Terminology] entsprechen.	X
	authorSpecialty	0..n	0..0	0..0	0..n	Fachliche Spezialisierung des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAuthorSpecialtyVS aus [gemIG_TI_Terminology] entsprechen.	X
	authorTelecommunication	0..n	0..0	0..0	0..n	Telekommunikationsdaten des Autors	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	X
availabilityStatus		0..0	0..0	1..1	0..0	Status des Dokuments ("Approved" oder "Deprecated")	Der Wert MUSS initial "`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" entsprechen.	
classCode		1..1	1..1	0..0	1..1	Grobe Klassifizierung des Dokuments	Der Wert MUSS einem Code des Value Sets EPAXDSClassCodeVS aus [gemIG_TI_Terminology] 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.	X

						PS-KTR MUSS für Dokumente • der Kategorie receipt ausschließlich den Code "ADM" (Administratives Dokument) verwenden • und für solche der Kategorie health_risk_analysis den Code "ASM" (Assessment) verwenden.	
comments	0..1	0..1	0..0	0..1	Ergänzende Hinweise in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.4] genügen.	X
confidentialityCode	0..n	0..n	0..1	0..n	Vertraulichkeitskennzeichnung des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3# 4.2.3.2.5] genügen und einem Code des Value Sets EPAXDSConfidentialityCodeVS aus [gemIG_TI_Terminology] entsprechen. Für `ProvideAndRegisterDocumentSet-b` MUSS für das Verbergen des Dokumentes der Code • Code = "`CON`", Display Name = "`constraint`" aus dem Code System `1.2.276.0.76.5.491` (siehe auch Value Set EPAXDSConfidentialityCodeVS aus [gemIG_TI_Terminology]) 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-TF2#3.42.4.1.3.7] auflösen.	
eventCodeList	0.	0.	0.	0.	Ereignisse, die	Der Wert MUSS den	X

	.n	.0	.0	.n	zur Erstellung des Dokuments geführt haben.	Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.8] genügen und Codes des Value Set EPAXDSEventCodeVS aus [gemIG_TI_Terminology] entsprechen. Der Wert darf höchstens einen KDL-Code ("Klinische Dokumentenklassen-Liste") und höchstens einen DMP-Code ("Disease Management Programm") enthalten. Hinweis: Frühere Versionen der ePA für alle haben das Einstellen von mehreren KDL- bzw. DMP-Codes in die eventCodeList nicht unterbunden. Deshalb kann es Altdaten geben, die noch mehr als einen Code der entsprechenden Code-Systeme in der eventCodeList enthalten.	
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 Value Sets EPAXDSFormatCode aus [gemIG_TI_Terminology] entsprechen. Der Wert KANN `"urn:ihe:iti:xds:2017:mimeTypeSufficient"` (siehe [IHE-ITI-TF-3#4.2.3.2.9]) entsprechen, um anzuzeigen, dass über den MIME-Type hinaus keine genaueren Angaben zum Dokumentenformat gemacht werden können oder der MIME-Type ausreichend ist. Für Dokumente, die in den Ordner "technical" eingestellt werden, ist ausschließlich ein formatCode gemäß A_23144* zugelassen. Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt3.12.1.9-Strukturierte Dokumente genügen.	
hash	0..0	0..0	1..1	0..0	Kryptographische Prüfsumme des Dokuments	Der Wert wird vom XDS Document Service beim Einstellen des Dokuments in die	

						Akte berechnet.	
healthcareFacilityTypeCode	1..1	1..1	0..0	1..1	Art der Einrichtung, in der das dokumentierte Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSHealthcareFacilityTypeCodeVS aus [gemIG_TI_Terminology] entsprechen. Das PS-KTR MUSS healthcareFacilityTypeCode ausschließlich mit dem Wert "VER" (Versicherungsträger) belegen. Die DiGA MUSS healthcareFacilityTypeCode mit dem Wert "PAT" belegen.	X
homeCommunityId	0..1	0..1	0..0	0..1		n/a Eine optional übertragene homeCommunityId wird nicht gespeichert.	
languageCode	1..1	1..1	0..0	1..1	Sprache, in der das Dokument abgefasst ist.	Der Wert MUSS einem Code des Value Sets EPAXDSLanguageCodeVS aus [gemIG_TI_Terminology] 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. PS-KTR MUSS für Dokumente der Kategorie health_risk_analysis ausschließlich den Wert "application/pdf" gemäß A_25009-* verwenden. Als formatCode ist dann entsprechend "urn:ihe:iti:xds:2017:mimeTypeSufficient" zu verwenden Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt3.12.1.9-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 ausA_14974* genügen. Außerdem MUSS der Wert der Identität des Akteninhabers entsprechen und MUSS vom XDS Document Service dahingehend bei Registrierung der Metadaten geprüft werden.	
practiceSettingC	1.	0.	0.	1.	Art der Fachrichtung der	Der Wert MUSS einem Code des Value Sets	X

ode	.1	.0	.0	.1	erstellenden Einrichtung, in der das dokumentiere Ereignis stattgefunden hat.	EPAXDSPracticeSettingCodeVS aus [gemIG_TI_Terminology] entsprechen. Die DiGA MUSS practiceSettingCode mit dem Wert "PAT" belegen.	
referenceIdList	0..n	0..1	1..1	0..n	Liste von IDs, mit denen das Dokument assoziiert wird.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.28] genügen. Wenn KTR-Clients einen Wert übertragen, muss es sich um die rootDocumentId beim Ersetzen (RPLC) eines Dokuments handeln.	
repositoryUniqueId	0..1	0..1	1..1	0..1	Kennung des Document Repository, in welches das Dokument eingestellt wird/wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.18] genügen.	
serviceStartTime	0..1	0..1	0..0	0..1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis begonnen wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.19] genügen.	X
serviceStopTime	0..1	0..1	0..0	0..1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis beendet wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.20] genügen.	X
size	0..0	0..0	1..1	0..0	Größe des Dokuments in Bytes	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.21] genügen. Der XDS Document Service MUSS die Größe des Dokuments berechnen und in den Metadaten während des Registriervorgangs setzen (vgl. [IHE-ITI-TF2#3.41.4.1.3]).	
sourcePatientId	0.	0.	0.	0.	Kennung des	Der Wert MUSS den	

	.1	.0	.0	.0	Patienten im Quellsystem	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 Value Sets EPAXDSTypeCodeVS aus [gemIG_TI_Terminology] entsprechen. PS-KTR MUSS für Dokumente der Kategorie health_risk_analysis ausschließlich den Code "GRIS" verwenden Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Inhalts- und Formatvorgaben aus Abschnitt3.12.1.9- Strukturierte Dokumente genügen.	X
uniqueId	1..1	1..1	0..0	1..1	Eindeutige, aktenweite Kennung des Dokuments	Das Format MUSS den folgenden Formatvorgaben genügen: - Es dürfen nur die folgenden druckbaren ASCII-Zeichen verwendet werden: Zeichen Codes (hexadezimal): 0x21-0x7E - Minimal 1 Zeichen, maximal 256 Zeichen. Hinweis 1: Groß- und Kleinschreibung ist relevant.	
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	0..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. ePA-FdV: Das ePA-Aktensystem MUSS die KVNR mit den Inhalten der User Session auf Übereinstimmung prüfen. Eine Gleichheit liegt vor, wenn die KVNR aus der XCN-Struktur des Autors nach den Vorgaben von A_14762-* mit dem entsprechenden Wert aus der User Session übereinstimmt. Ist authorPerson nicht gesetzt, MUSS das ePA Aktensystem das Metadatenattribut authorPerson für Versicherte entsprechend der Vorgaben aus A_14762-* unter Verwendung der entsprechenden Informationen aus der User Session (KVNR, family_name und given_name) setzen. Das ePA Aktensystem KANN in einer übergebenen authorPerson den Nachnamen und Vornamen mit Informationen aus der User Session überschreiben. PS/DiGAs können hier im Bedarfsfall Einträge für Software-Komponente bzw. Gerät als Autor entsprechend A_14762-* vornehmen.	

	authorInstitution	0..1	0..1	0..0	0..0	Institution, welcher die einstellende Person oder das einstellende System zugeordnet ist.	Der Wert MUSS den Formatvorgaben aus Abschnitt 3.12.1.8.2- Metadaten der Dokumente und SubmissionSets (A_21209*) genügen. Das ePA-Aktensystem MUSS die Identität von TelematikID-basierten Identitäten mit den Inhalten aus authorInstitution prüfen. Eine Gleichheit liegt vor, wenn Telematik-ID aus der XCN-Struktur des Autors nach den Vorgaben von A_14763-* bzw. A_21511-* mit dem entsprechenden Wert aus der User Session übereinstimmt. Ist authorInstitution nicht gesetzt, MUSS das ePA Aktensystem das Metadatenattribut authorInstitution entsprechend der Vorgaben aus A_14763-* bzw. A_21511-* unter Verwendung der entsprechenden Informationen aus der User Session (organizationName und idNummer) setzen.	
	authorRole	1..n	1..n	0..0	1..1	Rolle der einstellenden Person oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAuthorRoleVS aus [gemIG_TI_Terminology] entsprechen. Das PS-KTR MUSS den Code "105" (Kostenträgervertreter) verwenden. Das ePA-Frontend des VersichertenMUSS den Code "102" (der Patient selbst) verwenden. Die DiGA MUSS authorRole mit dem Code "12" (dokumentierendes Gerät) verwenden. Ein PS-System, das kein PS-KTR-System ist, DARF NICHT den Code "105" (Kostenträger) oder "102" (Patient) verwenden.	
	authorSpecialty	0..n	0..0	0..0	0..n	Fachliche Spezialisierung der	Der Wert MUSS einem Code des Value Sets EPAXDSAuthorSpecialtyVS aus	

						einstellenden Person oder des einstellenden Systems	[gemIG_TI_Terminology] entsprechen.	
	authorTelecommunication	0..n	0..0	0..0	0..n	Telekommunikationsdaten der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	
availabilityStatus		0..0	0..0	1..1	0..0	Status des Submission Sets ("Approved")	Der Wert MUSS "`urn:oasis:names:tc:ebxml-regrep:StatusType:Approved`" entsprechen.	
comments		0..1	0..1	0..0	0..1	Ergänzende Hinweise zum Submission Set in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.3] genügen.	X
contentTypeCode		0..1	0..1	0..0	0..1	Klinische Aktivität, die zum Einstellen des Submission Set geführt hat.	Der Wert MUSS einem Code des Value Sets EPAXDSContentTypeCodeVS aus [gemIG_TI_Terminology] 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-TF2#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] und einem Code des Value Sets EPADataCategoryOtherVS aus [gemIG_TI_Terminology] entsprechen. 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 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-TF2#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-TF2#3.42.4.1.3.6] aktuell halten. Zudem MUSS der XDS Document Service den Wert aktualisieren, wenn ein Dokument aus dem Ordner gelöscht wurde.	
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							
availabilityStatu	n/	n/	1.	n/	Status des	Der Wert MUSS	

s	a	a	.1	a	Ordners ("Approved")	"urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
codeList	n/a	n/a	1..1	n/a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] und einem Code des Value Sets EPADataCategoryOtherVS und EPADataCategoryMedicalVS aus [gemIG_TI_Terminology] entsprechen. Der XDS Document Service MUSS codeList gemäß A_19388* setzen.	
comments	n/a	n/a	0..1	n/a	Freitextkommentar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen.	
entryUUID	n/a	n/a	1..1	n/a	Intern verwendete, aktenweit eindeutige Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2#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-TF2#3.42.4.1.3.6] aktuell halten.Zudem MUSS der XDS Document Service den Wert aktualisieren, wenn ein Dokument aus dem Ordner gelöscht oder dessen Metadaten aktualisiert wurden.	
limitedMetadata	Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden.						
patientId	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.	

5448 **Tabelle 30: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language**
5449 **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_23369-04 -XDS Document Service – Verpflichtender Dokumententitel in DocumentEntry.title
Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von 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.
Andernfalls MUSS der XDS Document Service die Operation mit dem Fehler`XDSRegistryMetadataError` ablehnen undim `codeContext`-Attribut des zurückgegebenen`rs:RegistryError`-Elements mit:`"errorText='Invalid metadata';metadata='title'"` antworten.
[<=]

A_25188-02 -XDS Document Service - Input Sanitization
Der XDS Document Service MUSS sicherstellen, dass bei Anlage 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. Ausnahme: Der XDS Document Service MUSS im Metadatum DocumentEntry.comment die ASCII-Zeichen CR (\r, 0x0D) und LF (\n, 0x0A) ignorieren und nicht als Fehler behandeln (sie werden für Zeilenumbrüche benötigt).

[<=]

A_14762-08 -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 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.
Falls die Vorgaben nicht erfüllt werden, MUSS der XDS Document Service die Operation mit dem Fehler`XDSRegistryMetadataError` ablehnen undim `codeContext`-Attribut des zurückgegebenen`rs:RegistryError`-Elements antworten mit:`"errorText='Invalid metadata';metadata='authorPerson'"` antworten.
[<=]

A_14763-04 -XDS Document Service - Nutzungsvorgabe für SubmissionSet.authorInstitution
Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten bei`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^^^^8-34923902a`

[<=]

Hinweis: Wenn das einstellende Client-System gar keinen Wert einstellen darf oder muss für das authorInstitution-Feld, dann sind auch die entsprechenden Formatvorgaben hinfällig. Das trifft in diesem Fall auf das ePA FdV zu, welches das Feld SubmissionSet.authorInstitution gar nicht befüllen darf (siehe A_14760-*).

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_21209-03 -XDS Document Service - Nutzungsvorgabe für DocumentEntry.authorInstitution
Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten bei`DocumentEntry.authorInstitution` neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

Die Komponenten 2.-5. sind nur anzugeben, wenn die Telematik ID (5.) der Autoreninstitution bekannt ist oder ad-hoc ermittelt werden kann, bspw. über den Verzeichnisdienst der TI-Plattform (VZD). Ansonsten wird ausschließlich der Name gesetzt.
Beispiele:

- `Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-e518`
- `gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^8-34923902a`
- `Arztpraxis Dr. Wiebke Werner`

[<=]

A_22408-02 -XDS Document Service - DocumentEntry.authorInstitution ohne Telematik-ID
Der XDS Document Service MUSS Nachrichten zum Registrieren von Dokumenten bei fehlender Telematik-ID in `DocumentEntry.authorInstitution` akzeptieren und daraufhin alle Zeichen hinter dem Namen der authorInstitution abschneiden und verwerfen.**[<=]**

A_14974-03 -XDS Document Service - Nutzungsvorgabe für DocumentEntry.patientId und SubmissionSet.patientId
Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten die folgenden Nutzungsvorgaben für `DocumentEntry.patientId` und `SubmissionSet.patientId` berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.2.16] bzw. [IHE-ITI-TF3#4.2.3.3.8] genügen und ist inhaltlich nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen:

1. Der unveränderbare Teil der KVNR des Akteninhabers (10 Stellen)
2. "^^^&"
3. "1.2.276.0.76.4.8" (OID zur Kennzeichnung einer unveränderbaren KVNR)

4. "&ISO"

Beispiel: G995030566^^^&1.2.276.0.76.4.8&ISO**[<=]**

A_27759-01 -XDS Document Service - Verarbeitung von Code System Version beim Metadatenattribut DocumentEntry.eventCodeList
Der XDS Document Service MUSS ausschließlich beim Metadatenattribut DocumentEntry.eventCodeList die Metadaten vom Typ Coded Attribute im Slot "codingScheme" bei Angabe einer System URL oder Canocial URL eine per Pipe-Symbol (|) angehängte Version akzeptieren und für eine Terminologievalidierung verwenden. Anderenfalls MUSS der XDS Document Service die Registrierung des Dokuments mit einem XDSRepositoryMetadataError-Fehlercode quittieren. Die Prüfung des Codes ohne Versionsangabe erfolgt gegen das aktuell registrierte und gültige Code System: Ist der Code vorhanden, MUSS der XDS Document Service diese Version anhängen.**[<=]**

Beispiel: http://dvmd.de/fhir/CodeSystem/kdl|2025

3.12.1.8.3 Metadaten für Datenkategorien

A_19388-23 -Nutzungsvorgaben für die Verwendung von Datenkategorien
Der XDS Document Service MUSS beim Einstellen eines Dokuments die folgende Zuordnung zu einer Datenkategorie (d. h. Assoziierung mit einem bestimmten Folder) vornehmen. Dabei haben Auswertungs- und Zuordnungsregeln, die sich aus A_14761-* und damit verbunden aus [gemSpec_IG_ePA] ableiten, immer den Vorrang gegenüber anderen Auswertungsregeln. Ferner MUSS der XDS Document Service sicherstellen, dass bei einer Aktualisierung eines Dokuments derselbe Ordner des zu ersetzenden Dokuments zugeordnet wird.

Für eine eindeutige Zuordnung zu einer Datenkategorie MUSS die Auswertung der Metadatenvorgaben in der Reihenfolge der folgend dargestellten Einsortierungskriterien erfolgen:

Tabelle 31: 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 und Submissionset.authorRole = 105
health_risk_analsysis	healthcareFacilityTypeCode = VER und typeCode = GRIS und DocumentEntry.authorRole= 105 und Submissionset.authorRole = 105
patient	Dokumente bei denen der Einsteller der Versicherte oder sein Vertreter ist: Submissionset.authorRole = 102 Dokumente bei denen der Einsteller der Kostenträger ist: Submissionset.authorRole = 105
pregnancy_childbirth	healthcareFacilityTypeCode = HEB eventCodeList=SD070104 (KDL-Code

	Neugeborenenscreening)
eab	classCode = BRI
care	PracticeSettingCode = PFL*
rehab	practiceSettingCode =REHA
dental	practiceSettingCode =MZKH*
emergency	eventCodeList = • ED110102 (KDL-Code Notfalldatenmanagement (NFDM)) • AU190104 (KDL-Code Notfalldatensatz) • AD020105 (KDL-Code Notfall-/Vertretungsschein)
transcripts	eventCodeList = • UB999997 (KDL-Code Gesamtdokumentation stationäre Versorgung) oder • UB999998 (KDL-Code Gesamtdokumentation ambulante Versorgung)
reports	classCode = ANF, ASM, BEF, BIL, DOK, DUR, LAB oder PLA
other	Alle Dokumente, die in keine andere Kategorien eingeordnet werden können

*Falls Basiskonzepte angegeben werden, dann gelten automatisch alle Subkonzepte, z.B. gilt für die Kategorie "care" die Einsortieregel bei PracticeSettingCode = PFL wie auch für die Sub-Konzepte ALT (Altenpflege) und KIN (Kinderpflege).**[<=]**

3.12.1.8.4 Automatisches Umschreiben von Daten

Dieser Abschnitt enthält Vorgaben für Datenanpassungen, die für bestehende Daten im XDS Document Service vorgenommen werden müssen (z. B. wenn sie durch Änderungen im Rahmen einer neuen Version des XDS Document Service notwendig werden).

A_27482-02 -XDS Document Service – Metadatenkorrektur bei vorhandenen elektronischen Arztbriefen
Der XDS Document Service MUSS die Metadaten (DocumentEntry) von bestehenden Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief) gemäß [gemSpec_IG_ePA] derartig anpassen, dass DocumentEntry.eventCodeList zusätzlich um den KDL-Code (code: ED110104, codeSystem: http://dvmd.de/fhir/CodeSystem/kdl|[version], displayName: eArztbrief) erweitert wird, wenn dieser nicht bereits vorhanden ist. Dabei muss [version] mit der aktuellen Version (z.B. 2025) gemäß [gemIG_TI_Terminology] ersetzt werden.**[<=]**

A_28661 -XDS Document Service – Korrektur Code System-Werte bei vorhandenen Dokumenten
Der XDS Document Service MUSS in den Metadaten (DocumentEntry) von bestehenden Dokumenten diejenigen Code System-Werte, die mit dem Präfix "urn:oid:" beginnen,

derart anpassen, dass das Präfix gelöscht wird.
[<=]

Beispiel: Der ursprüngliche Wert "urn:oid:1.2.276.0.76.5.511" wird nach der Anpassung dann als "1.2.276.0.76.5.511" gespeichert.

A_28887-01 -XDS Document Service – Korrektur einer DocumentEntry.uniqueId
Der XDS Document Service MUSS einmalig nach Öffnen des Aktenkontos jede DocumentEntry.uniqueId, die nicht dem erlaubten Format gemäß A_14760-* entspricht, neu vergeben. Dazu MUSS der XDS Document Service eine neue UUID generieren (in Kleinbuchstaben, mit vorangestelltem Präfix "urn:uuid:") und die rootDocumentUniqueId in der DocumentEntry.referenceIdList aktualisieren.Falls eine rootDocumentUniqueId in einer General Deny Policy vorhanden ist, MUSS diese mit der neu generierten UUID aktualisiert werden.**[<=]**

Hinweis: Ein Beispiel für das neu zu generierende UUID-Format lautet "urn:uuid:ce1607ec-2a37-41a4-b441-dcde48d0bed2".

A_28833 -XDS Document Service – Migration von Code Systemen auf Haupt-URL
Der XDS Document Service MUSS die Metadaten von bestehenden DocumentEntries, SubmissionSets, Folders und Associations wie folgt anpassen, sofern das entsprechende Metadatum Codes enthält:

- Der XDS Document Service MUSS für jeden Code prüfen, ob für das gegebene Code System gemäß [gemIG_TI_Terminology] unter den "Naming Systems" alternative Namen definiert sind und das bestehende Code System durch denjenigen Namen ("Identifier") des Code System ersetzen, der in den "Naming Systems" als "preferred" gekennzeichnet ist und die Version gemäß [gemIG_TI_Terminology] hinzufügen.
- Der XDS Document Service MUSS den folgenden Code-System-Wert "1.2.276.0.76.5.518" (ICD-10GM Version 2022) durch den Wert "http://fhir.de/CodeSystem/bfarm/icd-10-gm" ersetzen und die Version "2022" ergänzen.
- Der XDS Document Service MUSS den folgenden Code-System-Wert "1.2.276.0.76.5.519" (OPS Version 2022) durch den Wert "http://fhir.de/CodeSystem/bfarm/ops" ersetzen und die Version "2022" ergänzen.
  Der XDS Document Service MUSS den folgenden Code-System-Wert "1.2.276.0.76.5.533" (KDL Version 2022) durch den Wert "http://dvmd.de/fhir/CodeSystem/kdl" ersetzen und die Version "2022" ergänzen.
- Der XDS Document Service MUSS den folgenden Code-System-Wert "1.2.276.0.76.5.552" (KDL Version 2024) durch den Wert "http://dvmd.de/fhir/CodeSystem/kdl" ersetzen und die Version "2024" ergänzen.
- Der XDS Document Service MUSS den folgenden Code-System-Wert "http://dvmd.de/fhir/CodeSystem/kdl", sofern er ohne Version angegeben wird, um die Version "2024" ergänzen.

[<=]

In der Regel bedeutet dies, dass Code Systems, die bisher als OID oder unter Angabe einer Alternativ-URL abgespeichert wurden, stattdessen mit Haupt-Identifier + Version des Code Systems gespeichert werden, um einen konsistenten Datenbestand zu erreichen.

Wenn der "preferred" Identifier in den Bestandsdaten bereits vergeben ist, ist keine Änderungen am Code System vorzunehmen.

Für XDS wird die Versionsangabe eines Code-System-Werts (bei URL-basierte Werte) über ein "|"-Symbol angehängt, siehe A_27759*.

Die Version ist nur in Fällen hinzuzufügen, in denen das entsprechende Code System gemäß [gemIG_TI_Terminology] eine Version führt.

A_28924-01 -XDS Document Service – Korrektur Code System bei XDW Workflow Codes in DocumentEntry.eventCodeList und DocumentEntry.formatCode
Der XDS Document Service MUSS einmalig nach dem Öffnen des Aktenkontos sicherstellen, dass die etwaig vergebenen Codes "urn:ihe:iti:xdw:2011:eventCode:open" und "urn:ihe:iti:xdw:2011:eventCode:closed" in der DocumentEntry.eventCodeList aller Dokumentmetadaten dem Code System "http://www.ihe-d.de/fhir/CodeSystem/WorkflowEvents" zugeordnet werden. Wurden sie ferner fälschlicherweise als formatCode verwendet, MUSS der XDS Document Service sie mit der zuvor genannten, korrekten Code System URL als eventCode speichern. Als Ersatz-Code ist "urn:ihe:iti:xds:2017:mimeTypeSufficient" zu verwenden.
[<=]

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_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. 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"fasst semantisch zusammengehörige, strukturierte Dokumente gleicher Struktur zusammen.
Sammlungen, die mehr als eine Sammlungsinstanz haben , z.B. Mutterpass, werden über dynamische 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_20577-07 -Definition und Zuweisung von Sammlungstypen
Der XDS Document Service MUSS jeder Sammlung einen von zwei Sammlungstypen zuweisen:

Tabelle 32: TAB_EPA_Sammlungstypen

Sammlungstyp	Definition
`mixed`	Strukturierte Dokumente, die einer Sammlung des Typs "mixed" angehören, können stets ein oder mehrere Dokumente unterschiedlicher Struktur entsprechend der Art der Sammlung enthalten.
`uniform`	Strukturierte Dokumente, die einer Sammlung des Typs "uniform" angehören, können stets ein oder mehrere Dokumente gleicher Struktur 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.
Es gelten die Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA]. In den unter [gemSpec_IG_ePA] gemachten Vorgaben werden auch Sammlungstyp und Kardinalitäten für spezifische Sammlungen festgelegt. Diese Angaben sagen aus, wie viele Instanzen einer Sammlung (d. h. minimal und maximal) registriert werden können.
[<=]

A_20707-06 -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 wie folgt angegeben werden, welche Metadaten nicht korrekt angegeben wurden:
`"errorText='Cannot register document: Structured document is not permitted for dynamic folder: invalid metadata';metadata=<value_1>;metadata=<value_2>;...;metadata=<value_n>"`**[<=]**

A_20581-06 -XDS Document Service – Löschen von Dokumenten aus Sammlungen der Typen "mixed" und "uniform" durch ein ePA-FdV
Der XDS Document Service MUSS beim Löschen eines Dokuments der Sammlungstypen "mixed" und "uniform"durch das ePA-FdV sicherstellen, dass die Operation mit dem Fehler `ReferencesExistException` abgebrochen wird, wenn die Löschanfrage nicht alle Dokumente der Sammlung enthält. Es besteht folgende Ausnahme: Das Löschen einer Elternnotiz im Kinderuntersuchungsheft ist erlaubt.**[<=]**

Nur Leistungserbringern ist es erlaubt, einzelne Dokumente aus Sammlungen der Typen "mixed" und "uniform" zu löschen, um die medizinische Interpretation der gesamten Sammlungsinstanz nicht zu gefährden.

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

3.12.1.9.2 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 ePA-Aktensystems MUSS durch organisatorische Maßnahmen sicherstellen, dass die Konfiguration im Aktensystem zur Unterstützung strukturierter Dokumente aus [gemSpec_IG_ePA] ausschließlich im Rahmen der Veröffentlichung der Implementation Guides durch die gematik erfolgt.**[<=]**

Bei Einführung neuer strukturierter Dokumente werden die beschriebenen Konfigurationsmöglichkeiten so verwendet, dass eine Erweiterung der Spezifikation und daraus resultierend eine Änderung des ePA-Aktensystems mit erneuter Zulassung nicht erforderlich sind.

3.12.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode

Der Versicherte oder ein Vertreter kann vorhandene Dokumente des Aktenkontos durch die Verwendung der General Deny Policy des Constraint Managements verbergen oder sichtbar machen.

Der Versicherte oder ein Vertreter kann ein neues Dokument auch direkt beim Einstellen in das Aktenkonto verbergen. Dazu wird durch den XDS Document Service beim Einstellen bzw. Aktualisieren (Replace) eines Dokuments der DocumentEntry.confidentialityCode der Dokumentmetadaten ausgewertet. Enthält der confidentialityCode beim Einstellen bzw. Aktualisieren den Wert "CON" (constraint), wird durch das Aktensystem ein Eintrag in der General Deny Policy erzeugt und das Dokument verborgen.

Diese zusätzliche Art des direkten Verbergens ist dabei grundsätzlich nur auf Dokumententypen anwendbar, welche durch einen Versicherten oder einen Vertreter über ein ePA-FdV eingestellt werden können (keine MIOs oder strukturierten Dokumente).

Das Metadatum DocumentEntry.confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491:

1. Führt beim Einstellen und Replace eines Dokuments zum Verbergen des Dokuments, d.h. das Dokument wird auf die General Deny Policy des Aktenkontos gesetzt.
2. Wird im Aktensystem nicht persistiert sondern über dort intern über eine General Deny Policy umgesetzt.
3. Wird im ePA-FdV nicht zur Anzeige gebracht und kann dort auch nicht geändert werden.
4. Eine LEI darf DocumentEntry.confidentialityCode = "CON" nicht verwenden.

3.12.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die Dokumente des Aktenkontos

Wird ein Widerspruch gegen die Nutzung einer Funktion der ePA erklärt, verhindert der XDS Document Service, abhängig von der jeweils widersprochenen Funktion, deren weitere Nutzung.

Im Falle eines Widerspruchs gilt:

Tabelle 33: Auswirkungen bei Widerspruch gegen eine Funktion der ePA

widerspruchsfähige Funktion	Auswirkung bei erteiltem Widerspruch

Teilnahme am digital gestützten Medikationsprozess ("medication")	Das Einstellen, Verändern, Lesen oder Suchen von Dokumenten des Ordners "emp" (elektronischer Medikationsplan) wird durch den XDS Document Service abgelehnt. Ausgenommen hiervon sind der Versicherte und befugte Vertreter.
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst ("erp-submission")	Alle vorhandenen Dokumente des Ordners "emp" (elektronischer Medikationsplan) werden gelöscht.

Hinweis zum Medikationsprozess: Dadurch wird verhindert, dass Leistungserbringer im Versorgungsprozess veraltete oder unvollständige Daten verwenden.

A_23860 -XDS Document Service - Löschen der Dokumente des Medikationsprozesses
Der XDS Document Service des Aktensystems MUSS alle Dokumente aus dem Ordner elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") löschen, wenn der Status der widerspruchsfähigen Funktion "Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdiens" (Id == "erp-submission") auf "Widerspruch erklärt" ("deny") geändert wird.**[<=]**

A_23895-02 -XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch
Falls ein Widerspruch zur widerspruchsfähigen Funktion "Teilnahme am Medikationsprozess" (Id ="medication" und status ="deny") vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSytem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für alle Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid_versicherter), ablehnen und die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.
[<=]

A_25151-01 -XDS Document Service – Prüfung der Widersprüche bei Suchanfrage
Der XDS Document Service MUSS bei einer Suchanfrage die Suchergebnismenge für alle Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid_versicherter), filtern und sicherstellen, dass diese keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (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.
[<=]

3.12.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI auf die Dokumente des Aktenkontos

Wird ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI erklärt, verhindert der XDS Document Service, dass auf die Dokumente der Kategorie "emp" zugegriffen werden kann.

A_26429 -XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI
Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und

Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSytem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für diese LEI, ablehnen und die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.
[<=]

A_26430 -XDS Document Service – Prüfung des Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI bei Suchanfrage
Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service bei einer Suchanfrage die Suchergebnismenge für diese LEI filtern und sicherstellen, dass die Suchergebnismenge keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSytem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält.
[<=]

3.12.1.13 Protokollierung von Zugriffen auf den XDS Document Service

Anforderungen an den XDS Document Service sind in [gemIG_ePA_Basic] spezifiziert.

3.12.1.14 Unterstützungsleistung für das ePA-FdV

Der XDS Document Service akzeptiert aus Sicherheitsgründen nur bestimmte Dokumentenformate. Das schränkt auch das Format PDF auf bestimmte PDF/A-Varianten ein (siehe auch A_25233*). Daher müssen PDF-Dokumente des Versicherten unter Umständen vor dem Einstellen in die ePA konvertiert werden.
Um das ePA-FdV dabei zu entlasten und Komplexität aus dem ePA-FdV zu nehmen, wird eine Funktion angeboten, durch die ein PDF in ein PDF/A konvertiert werden kann. Das ePA-FdV muss aber berücksichtigen, dass die Konvertierung ggf. technisch nicht durchgeführt werden kann oder das Ergebnis der Konvertierung durch ein geändertes Layout ggf. nicht verwendbar ist.

A_25456 -XDS Document Service - Keine negativen Auswirkungen auf Folgekonvertierungen von PDF zu PDF/A
Der XDS Document Service MUSS sicherstellen, dass eine Konvertierung eines PDF-Dokuments sich nicht schädlich auf folgende Konvertierungen auswirken kann.**[<=]**

Hinweis zu A_25456*: Die Anforderung soll erreichen, dass ein potentiell über ein PDF-Dokument eingebrachter Schadcode nach der Konvertierung gelöscht wird, z.B. durch Zurücksetzen der Sandbox oder der VAU-Instanz

A_25455 -XDS Document Service - Isolation der Konvertierung von PDF zu PDF/A
Der XDS Document Service MUSS die Verarbeitung von PDF-Dokumenten, die im Rahmen der Konvertierung in ein PDF/A durchgeführt wird, in einer separaten VAU-Instanz durchführen, die ausschließlich eine Verbindung zu einem ePA-FdV besitzen darf.**[<=]**

A_25454 -XDS Document Service - Realisierung der Schnittstelle I_Tool_Convert_PDF_Insurant
Der XDS Document Service MUSS die Operationen der Schnittstelle I_Tool_Convert_PDF_Insurant gemäß [I_Tool_Convert_PDF_Insurant] umsetzen**[<=]**

A_26129 -ePA-Aktensystem - Rahmenbedingungen bei Nutzung einer Service-VAU für PDF-Konvertierung
Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die vom ePA-FdV übermittelten PDF-Dokumente in der Aktenkontoverwaltungs-VAU ausschließlich weitergeleitet aber ansonsten nicht verarbeitet werden. Gleiches gilt für die von der Service-VAU an das ePA-FdV übermittelten konvertierten PDF/A-Dokumente.**[<=]**

A_26130 -ePA-Aktensystem - maximale Lebensdauer einer Service-VAU für PDF-Konvertierung
Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die Lebensdauer einer solchen Service-VAU-Instanz maximal 12 Stunden beträgt.**[<=]**

A_26131 -ePA-Aktensystem - Keine Speicherung von in der Service-VAU für PDF-Konvertierung verarbeiteten Daten
Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass weder die vom ePA-FdV übermittelten und zu konvertierenden PDF-Dokumente noch die daraus konvertierten PDF/A-Dokumente von der "PDF-VAU" im ePA-Aktensystem gespeichert werden.**[<=]**

A_26121 -ePA-Aktensystem - Keine Verarbeitung von Geräteinformationen
Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass keine Geräteinformationen (Device Management) von Nutzern verarbeitet werden.**[<=]**

3.12.2 FHIR Data Services

Anforderungen für FHIR Data Services werden nicht hier aufgelistet, sondern befinden sich in dafür gepflegten FHIR Implementation Guides (IG), auf die auch im entsprechenden Produkttypteckbrief verwiesen wird.

3.13 Audit Event Service

Ereignisse und Zugriffe auf die ePA eines Versicherten werden im ePA Aktensystem durch den Audit Event Service protokolliert. Anforderungen an den Audit Event Service sind in [gemIG_ePA_Basic] spezifiziert.

3.14 Information Services

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 in2.8- 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_Account_Management für die Umsetzung der Anwendungsfälle eines automatischen Aktenkontoumzugs und sind in 3.1- Aktenkontoverwaltung 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_25054-01 -Information Service Account - Gegenseitige Authentisierung Aktensysteme
Der Information Service Account MUSS für die beidseitige Authentisierung die technische Rolle `oid_epa_mgmt` und die folgenden Zertifikatsprofile verwenden:

- C.FD.TLS-S als Anbieter des Service (Server),
- C.FD.TLS-C als Nutzer des Service (Client)

[<=]

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.
[<=]

3.14.3 EHR Information Service

Der EHR Information Service erbringt eine analoge Leistung zum Information Service, aber innerhalb der VAU. Über einen bestehenden VAU-Kanal können Informationen zur Existenz einer Akte oder den Widersprüchen zu Versorgungsprozessen abgerufen werden, ohne eine separate Verbindung zum Information Service aufzubauen.

Der Zugang erfolgt durch Nutzung der Schnittstelle `I_Ehr_Information_Service`.

A_30119 -EHR Information Service - Realisierung der Schnittstelle I_Ehr_Information_Service
Der EHR Information Service MUSS die Operationen der Schnittstelle `I_Ehr_Information_Service` gemäß [I_Ehr_Information_Service] umsetzen.**[<=]**

3.15 Email Management

Das Email Management ermöglicht einem FdV-Nutzer die Verwaltung seiner E-Mail-Adresse und einem Kostenträger die Verwaltung von E-Mail-Adressen von Versicherten, die bei diesem Kostenträger versichert sind.

Die Schnittstelle zum Verwalten der E-Mail-Adressen durch den Kostenträger dient dem ausschließlichen Zweck des Einstellens, Lesens und der Änderung von E-Mail-Adressen auf Verlangen des Versicherten. Dies ermöglicht dem Kostenträger, seinen Versicherten die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte auf Berichtigung und Auskunft bzgl. der im Aktensystem verarbeiteten E-Mail-Adresse zu gewährleisten.

Für einen Versicherten kann nur genau eine E-Mail Adresse hinterlegt werden.

A_25435 -Email Management - Realisierung der Schnittstelle I_Email_Management
Das Email Management MUSS die Operationen der Schnittstelle `I_Email_Management` gemäß [I_Email_Management] umsetzen.**[<=]**

A_25438 -Email Management - Beschränkung der Schnittstellenoperationen auf E-Mail-Adressen des FdV-Nutzers
Das Email Management MUSS die Operationen der Schnittstelle `I_Email_Management` gemäß [I_Email_Management] auf die E-Mail-Adresse des aufrufenden Nutzers einschränken, sofern der Nutzer ein FdV-Nutzer ist.**[<=]**

A_26161 -Email Management - Nutzen von Email Management auch bei Widerpruch
Das Email Management MUSS sicherstellen, dass das Email Management auch von Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben.**[<=]**

A_26162 -Email Management - Versicherte nutzen Email Management ausschließlich im Home-AS
Das Email Management des ePA-Aktensystems MUSS sicherstellen, dass das Email Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-Aktensystem das Home-AS ist.**[<=]**

Hinweis: Für das Email Management ist auch Anforderung A_26154* umzusetzen.

A_25439 -Email Management - Kostenträger kann ausschließlich E-Mail-Adressen der eigenen Versicherten verwalten
Das Email Management MUSS sicherstellen, dass ein Kostenträger mittels der Operationen der Schnittstelle `I_Email_Management` gemäß [I_Email_Management] ausschließlich E-Mail-Adressen von Versicherten verwalten kann, die beim Kostenträger versichert sind.**[<=]**

A_25440-01 -Email Management - Benachrichtigung bei Änderung der E-Mail-Adresse
Falls eine E-Mail-Adresse a) ersetzt oder b) ergänzt wird, MUSS das Device Management bei a) eine E-Mail an die alte und die neue E-Mail-Adresse senden und bei b) eine E-Mail an die neue E-Mail-Adresse senden, in der bei a) über die Ersetzung bzw. bei b) die Ergänzung einer E-Mail-Adresse informiert wird. In der E-Mail MUSS darüber informiert werden, wann und ob der FdV-Nutzer selbst oder der Kostenträger die E-Mail ersetzt bzw. ergänzt hat.**[<=]**

A_25441 -Email Management - Information bzgl. der Ergänzung bei E-Mail-Adressen
Das Email Management MUSS sicherstellen, dass der FdV-Nutzer für eine im Email Management hinterlegte E-Mail-Adresse erkennen kann, wann und von wem diese E-Mail-Adresse ergänzt wurde.**[<=]**

A_25968-01 -Email Management - Maximale Anzahl E-Mail-Adressen
Das Email Management MUSS sicherstellen, dass für einen Nutzer maximal eine E-Mail-Adresse hinterlegt werden kann.**[<=]**

A_26163 -Email Management - Keine Persistierung einer im Rahmen der Vertretereinrichtung übergebenen E-Mail-Adresse
Das Email Management MUSS sicherstellen, dass eine im Rahmen des Anwendungsfalls der Vertretereinrichtung vom Nutzer übermittelte E-Mail-Adresse nicht persisitiert und spätestens bei Beendigung der User Session gelöscht wird.**[<=]**

A_26164 -Email Management - Keine Geräteregistrierung mit der im Rahmen der Vertretereinrichtung übergebenen E-Mail-Adresse
Das Email Management MUSS sicherstellen, dass keine E-Mail-Adressen zur Übermittlung eines Geräteregistrierungscodes genutzt werden, die dem ePA-Aktensystem im Rahmen des Anwendungsfalls der Vertretereinrichtung übermittelt wurden.**[<=]**

Hinweis zu A_26163 und A_26164: Die im Rahmen des Anwendungsfalls der Vertretereinrichtung übermittelte E-Mail-Adresse wird ausschließlich zur Information des Vertreters über die Einrichtung der Vertretung genutzt (vgl. A_24755-*).

3.16 Zusätzliche Anforderungen an den Authorization Service

Der ePA Authorization Service wird sowohl für die Authentisierung der Versicherten über das FdV als auch für die Authentisierung von Leistungserbringern und Kostenträgern über

deren Primärsystem benötigt. Ebenso muss die Zugriffsautorisierung für andere Fachdienste wie z.B. E-Rezept geprüft werden. Die Festlegungen für den Authorization Server finden sich in [gemSpec_IDP_FD]. Dieser Abschnitt des vorliegenden Dokuments enthält spezifische Anforderungen, die vom Authorization Service des Aktensystems zusätzlich umzusetzen sind.

A_24923 -Authorization Service - I_Authorization_Service
Der Authorization Service MUSS die Operationen der SchnittstelleI_Authorization_Service implementieren gemäß [I_Authorization_Service].
[<=]

A_25283 -Authorization Service - Konvertieren von ID-Token
Der Authorization Service MUSS sicherstellen, dass für ein nach erfolgreicher Authentifizierung des Nutzers vorliegendes ID-Token mittels Regel *rr0* gemäß *Tab_AS_Entitlement_Registration_Rules* ein HSM-ID-Token erstellt wird, bevor das ID-Token zeitlich ungültig ist.**[<=]**

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

Im Rahmen der Authentisierung des Versicherten erfolgt die Prüfung der Geräteregistrierung (Verifikation) direkt. Das Gerät muss dafür die Geräteparameter eines zuvor ausgeführten und bestätigten Registrierungsprozesses verwenden

Bisher nicht registrierte Geräte, bzw. Geräteparameter einer bisher nicht bestätigten Geräteregistrierung, können unter Verwendung des Device Management registriert, bzw. bestätigt werden (siehe Kapitel3.11- Device Management).

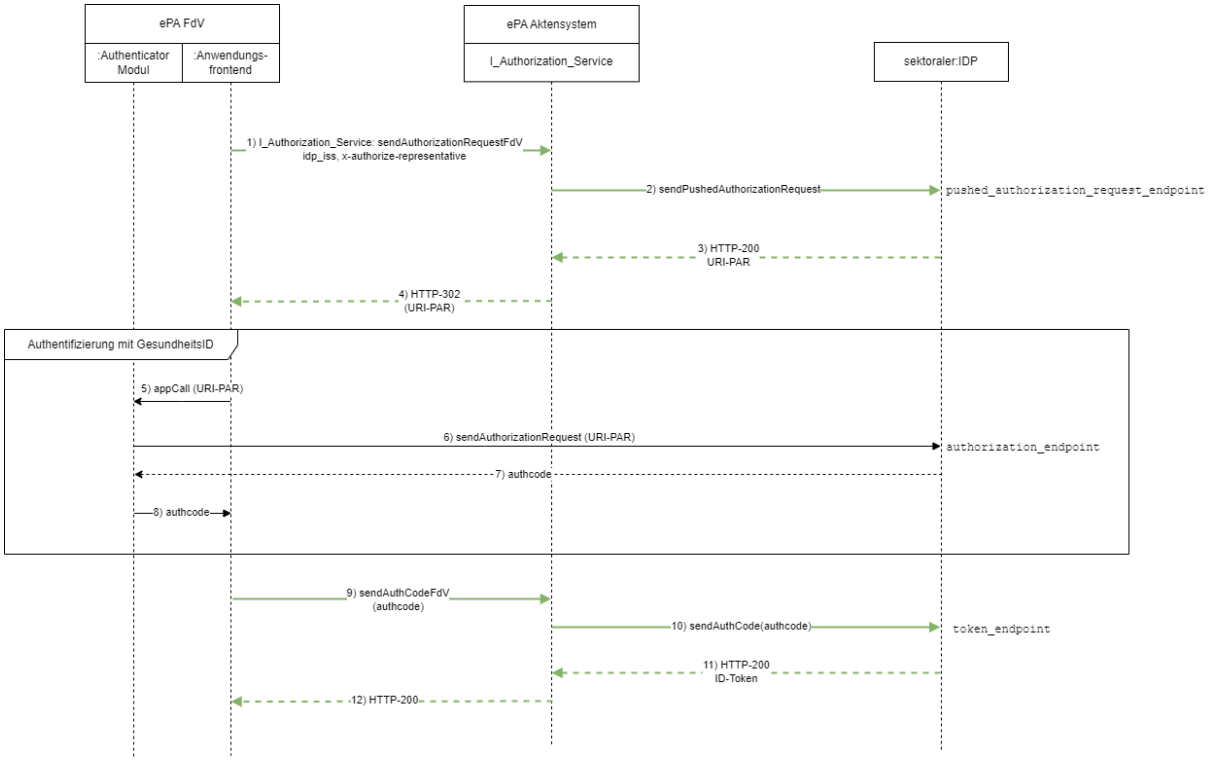


Abbildung 8: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP

A_25717-03 -Authorization Service - Pushed Authorization-Request des Authorization Service an sektorale Identity Provider

Der ePA Authorization Service MUSS den Pushed Authorization Request (PAR) am durch den vom ePA-FdV übergebenen Parameter idp-iss adressierten sektoralen IDP gemäß [gemSpec_IDP_FD#AF_10117] mit folgenden Parametern aufrufen:

Parameter	Wert	Anmerkung
`scope`	"openid urn:telematik:display_name urn:telematik:versicherter urn:telematik:family_name urn:telematik:given_name"	Notwendige Scopes für den Zugriff für die Autorisierung von Nutzern am ePA-Aktensystem
`acr_values`	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung
`redirect_uri`	Inhalt des Parameters x-redirecturi [`sendAuthorizationRequestFdV` in `I_Authorization_Service`], andernfalls eine herstellerspezifische Standard-redirect_uri.	Diese URI muss unter dem claim `redirect_uris` im Entity Statement des Authorization Service enthalten sein. Mandanten, welche eine eigene `redirect_uri` verwenden [`sendAuthorizationRequestFdV` in `I_Authorization_Service`] , müssen diese im Rahmen des Registrierungsprozesses beim Autorization Service bekannt geben.

[<=]

Hinweis 1: An die redirect_uri im Pushed Authorization Request sendet der sektorale IDP den ausgestellten Authorization Code (siehe [gemSpec_IDP_Sek])

Hinweis 2: Der Redirectaufruf, der vom Authenticator Modul an die redirect_uri ausgeführt wird, wird vom ePA-FdV über Plattformmechanismen (deeplink/universallink) gefangen und stellt selbst einen POST-Request an den Endpunkt des Authorization Service.

A_26584 -Authorization Service - Liste der redirect_uris im Entity Statement
Der Authorization Service MUSS in seinem Entity Statement im `claim redirect_uris` die `redirect_uris` aller Mandanten auflisten, welche bei der Registrierung an einem beliebigen ePA Authorization Service eine eigene redirect_uri angegeben haben. Über Änderungen des `claim redirect_uris` MUSS der Anbieter des Federation Master vor produktiver Verwendung informiert werden**[<=]**

Hinweis: Im Registrierungsprozess eines Mandanten mit eigener redirect_uri muss sichergestellt sein,

- dass alle Anbieter von ePA Authorization Servern (ePA Aktensystem Anbieter) entsprechend informiert sind und das Entity Statement anpassen
- dem Hersteller des Federation Master über ein ITSM Change bekannt gemacht wird, dass sich die Entity Statements aller ePA Authorization Server ändern

A_27145 -Synchronisation "redirect_URI" mit Marktteilnehmer - E-Mail-Adresse
Der Anbieter ePA-Aktensystem MUSS der gematik eine E-Mail-Adresse mitteilen, über welche er die eigenverantwortliche Registrierung (von redirect-URIs im Entity-Statement) durchführt und über die der Anbieter bei Änderungen erreichbar ist.

Hinweis: Diese E-Mail-Adressen werden durch das Provider Management der gematik

anschließend unter den relevanten Anbietern verteilt bzw. können dort erfragt werden. Die Änderung der E-Mail-Adressen ist ebenfalls zu kommunizieren.

Hintergrund: Für Stellvertretung via ePA-FdV ist eine Synchronisierung der redirect_URIs notwendig.**[<=]**

A_27186 -Synchronisation "redirect_URI" mit Marktteilnehmer - Information
Der Anbieter ePA-Aktensystem MUSS bei Änderungen der redirect_URIs im eigenen Entity Statement allen anderen Marktteilnehmern des gleichen Fachdiensttyps diese Änderung innerhalb 24 Stunden mitteilen.**[<=]**

A_27187 -Synchronisation "redirect_URI" mit Marktteilnehmer - Aktualisierung
Der Anbieter ePA-Aktensystem MUSS nach dem Empfang der Mitteilungen über Änderungen der Redirect URIs in einem externen Entity Statement diese Änderung binnen 24 Stunden in den Redirect URIs des eigenen Entity Statement synchronisieren.

Hinweis: Diese Änderung erfordert anschließend keine Information nach A_27186.**[<=]**

A_24878-01 -Authorization Service - Authentifizierung eines Versicherten am ePA-FdV des Vertreters
Falls der Eingangsparameter `x-authorize-representative=True` der Operation `I_Authorization_Service::sendAuthorizationRequestFdV` gesetzt ist, MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:guest:eGK` belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf.**[<=]**

A_26189-01 -Authorization Service - Authentifizierung eines Versicherten im Gastmodus mit eGK und PIN
Falls der Eingangsparameter `x-authorize-egk=True` der Operation `I_Authorization_Service::sendAuthorizationRequestFdV` gesetzt ist, MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:guest:eGK` belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf.**[<=]**

A_24937-01 -Authorization Service - Einschränkung bei Authentifizierung eines Versicherten am ePA-FdV des Vertreters
Der Authorization Service MUSS sicherstellen, dass ein mit`x-authorize-representative=True` authentisierter Nutzer ausschließlich Zugriff auf das Entitlement Management erhält.**[<=]**

A_26159 -Authorization Service - Prüfen der Device Attestation
Der Authorization Service MUSS sicherstellen, dass von einem anderen ePA-Aktensystem signierte Device Attestations ausschließlich akzeptiert werden, wenn

- die Device Attestation gemäß A_25042-* valide von einer Signaturidentität der VAU eines anderen ePA-Aktensystems signiert wurde,
- die KVNR in der Device Attestation mit der KVNR im ID-Token des angemeldeten Nutzers übereinstimmt,
- die Device Attestation zeitlich gültig ist.

[<=]

A_26160 -Authorization Service - Keine Persistierung der Device Attestation
Der Authorization Service MUSS sicherstellen, dass die von einem anderen ePA-Aktensystem signierte Device Attestation und deren Inhalte spätestens bei Beendigung der User Session gelöscht und nicht persistiert werden.**[<=]**

A_25310-01 -Authorization Service - Einschränkung bei Authentifizierung mit einem unregistrierten Gerät

Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wird und der Nutzer nicht mit `x-authorize-representative=True` authentisiert wurde, MUSS der Authorization Service sicherstellen, dass der Nutzer ausschließlich Zugriff auf das Device Management erhält.**[<=]**

Hinweis:
Ein vollständiger Zugriff eines authentisierten Nutzers auf alle Dienste des Aktensystems kann nur mit einem Gerät erfolgen, dessen Geräteregistrierung bei der Authentifizierung des Nutzers erfolgreich verifiziert wurde.
Ein Nachweis einer Geräteregistrierung ist entweder DeviceID (deviceIdentifier und deviceToken), die für den Nutzer im Aktensystem bekannt sind oder die vom Client übergebene Device Attestation (deviceAttestation), die zuvor am Device Management des Home Aktensystems durch den Client abgerufen wurde.

A_24804-01 -Authorization Service - Prüfung auf registriertes Gerät
Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des Vertreters handelt und im Operationsaufruf `I_Authorization_Service::sendAuthCodeFdV` eine DeviceID (deviceIdentifier und deviceToken) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer registriert und bestätigt ist und übereinstimmt.**[<=]**

A_24914-03 -Authorization Service - Prüfung auf registriertes Gerät - kein registriertes Gerät
Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wurde, MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung abbrechen und die User Session beenden.**[<=]**

A_24915-01 -Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht bestätigt
Falls als Nachweis einer Geräteregistrierung eine DeviceID (deviceIdentifier und deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status == 'pending'), MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung abbrechen und die User Session beenden.**[<=]**

A_28658 -Authorization Service - Prüfung des LOA Levels
Der ePA-Authorization Service MUSS ein vom sektoralen IDP erhaltenes ID-Token dahin gehend prüfen, ob

- entweder der im claim arc übermittelte Wert "gematik-ehealth-loa-high" ist,
- oder, wenn der im claim arc übermittelte Wert "gematik-ehealth-loa-substantial" ist, die Nutzereinwilligung zur Absenkung des Vertrauensniveau (nach A_23103) vorliegt.

In allen anderen Fällen MUSS der Zugang zur ePA verwehrt werden.**[<=]**

Hinweis:
Die Information, ob die Nutzereinwilligung zur Absenkung des Vertrauensniveau (nach A_23103) vorliegt, kann der Authorization Service aus dem übermittelten ID-Token extrahieren.
IDPs, welche die ID-Token Version 2 liefern ,tragen die Information im claim "urn:telematik:auth:consent". Dort muss der Wert "loa-substantial" enthalten sein (gemSpec_IDP_FD - A_27593).
IDPs, welche die ID-Token Version 1 liefern, tragen die Information im claim "amr". Dort muss der Wert "urn:telematik:auth:mEW" enthalten sein. (gemSpec_IDP_FD - A_23202-02).

3.16.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B

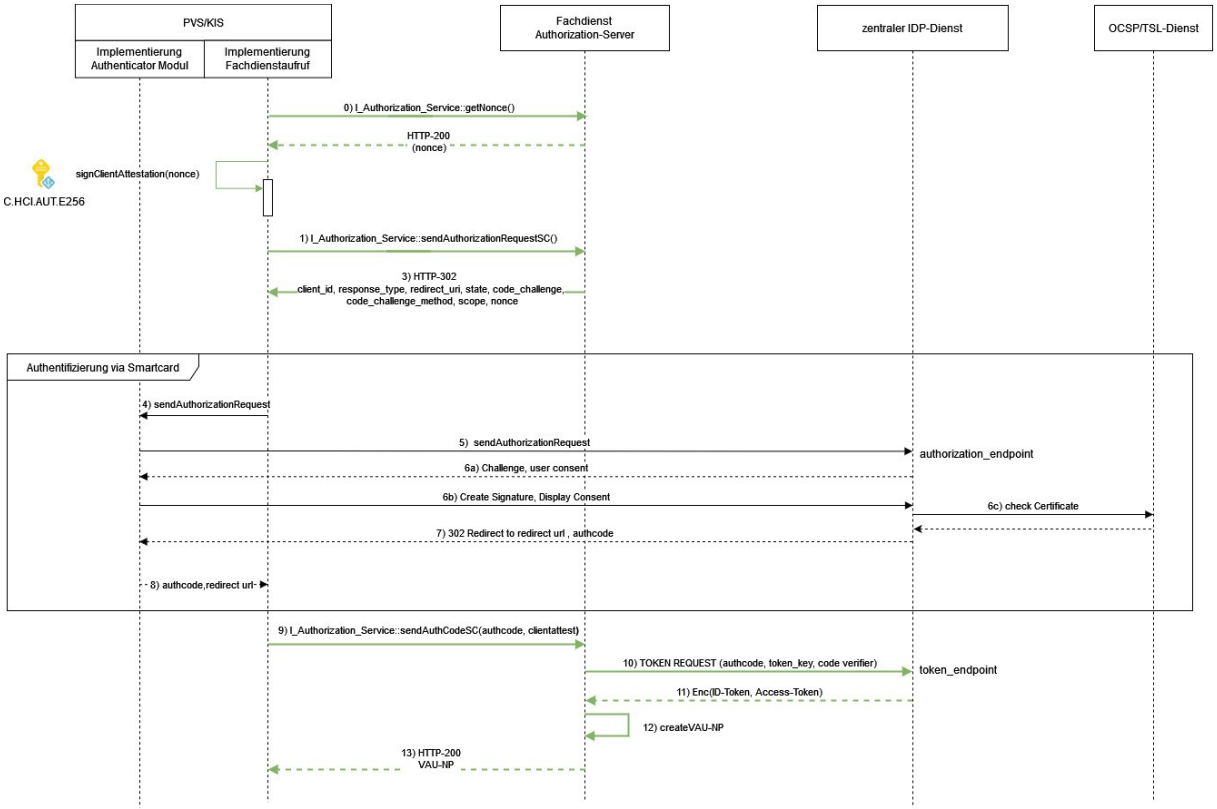


Abbildung 9: Ablauf der Authentifizierung einer LEI über den Smartcard IDP

A_24717 -Authorization Service: IDToken vom IDP-Dienst nur mit Client-Attestation nutzbar
Der Authorization Service MUSS sicherstellen, dass ein vom IDP-Dienst abgerufenes ID-Token für Nutzer "TelematikID_X" nur dann akzeptiert wird, falls im Authorization Service auch eine Client-Attestation vom Nutzer "TelematikID_X" vorliegt.**[<=]**

A_24718 -Authorization Service: Client-Attestation nur einmal nutzbar (Replay Angriffe)
Der Authorization Service MUSS sicherstellen, dass eine Client-Attestation eines Nutzers im Authorization Service mit dem ID-Token nur einmalig für die Aktivierung einer User Session verwendet wird.**[<=]**

A_25444-03 -Authorization Service - JWT Client Attestation
Der Authorization Service MUSS bei der Authentifizierung einer Leistungserbringerinstitution prüfen , dass das übermittelte JWT der Client Attesttierung mindestens die folgenden Inhalte aufweist.

Tabelle 34 : Inhalte des übermittelten JWT der Client Attestierung

Part	Claim	Claim	Anmerkung

	Name		
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256" oder "PS256"	
	"x5c"	Signaturzertifikat C.HCI.AUT	
Payload			
	"nonce"	Nonce aus einer `getNonce` Operation	siehe [I_Authorization_Service]

[<=]

Für das Signaturzertifikat zu "x5c" (AUT-Zertifikat der SMC-B) gilt: Basiert der öffentlichen Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

3.16.3 Anforderungen an den Authorization Service für die Authentisierung über JWT Bearer Token



Abbildung 10: Ablauf der Authentisierung über JWT Bearer Token am Beispiel eRP-FD

A_25165-03 -Authorization Service: JWT Bearer-Token des E-Rezept-Fachdienstes

Das Authorization Service MUSS sicherstellen, dass die Authentifizierung des E-Rezept-Fachdienstes über die Schnittstelle `I_Authorization_Service` durch Verwendung eines gültig signierten JWT Bearer Token mit den dargestellten Mindest-Inhalten und Prüfung durch Regel 'rr0' des Befugnisverifikations-Moduls erfolgt. Die Claims in 'Payload' MÜSSEN dazu die Vorgaben aus [gemSpec_Krypt], A_24658* befolgen.

Tabelle 35 : JWT Bearer Token mit den Mindest-Inhalten

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Krypt]
	"sub"	Telematik-ID des E-Rezept-Fachdienstes	

[<=]

A_29875 -Authorization Service: JWT Bearer-Token des Forschungsdatenzentrums

Der Authorization Service MUSS sicherstellen, dass die Authentifizierung des Forschungsdatenzentrums über die Schnittstelle`I_Authorization_Service` durch Verwendung eines gültig signierten JWT Bearer Token mit den dargestellten Mindest-Inhalten erfolgt. Die Claims in 'Payload' MÜSSEN dazu die Vorgaben aus [gemSpec_Krypt], A_24658* befolgen.

Tabelle 36 : JWT Bearer Token FDZ mit den Mindest-Inhalten

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	

	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674
	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Kr
	"sub"	Telematik-ID des Forschungsdatenzentrums	

[<=]

Die Signaturzertifikate zu "x5c" (AUT-Zertifikate) kommen 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.

A_30391 -Authorization Service: JWT Bearer-Token eines Kostenträgers
Der Authorization Service MUSS sicherstellen, dass die Authentifizierung eines Kostenträgers über die Schnittstelle`I_Authorization_Service` durch Verwendung eines gültig signierten JWT Bearer Token mit den dargestellten Mindestinhalten erfolgt und die Prüfung des Tokens gemäß A_30396-* erfolgreich ist.

Tabelle 37 : JWT Bearer Token eines Kostenträgers mit den Mindestinhalten

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.HCI.AUT	das "signierende" Zertifikat
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674
	"hash-itsg"	SHA-256 Hashwert des JWT ITSG-Tokens, welches an das JWT Bearer Token des Kostenträgers gebunden wird.	
	"sub"	Telematik-ID des Kostenträgers	

	"cn"	Name des Kostenträgers	muss dem Wert aus subject.commonNa aus dem Signaturzertifikat C.HCI.AUT entspre

[<=]

A_30396 -ePA-Aktensystem - Vorgaben für JWT Bearer Token eines Kostenträgers
Das ePA-Aktensystem MUSS sicherstellen, dass eine Prüfung des JWT Bearer Tokens eines Kostenträgers gemäß A_30391-* nur dann erfolgreich ist, wenn

- die Prüfung der Signatur des Tokens gemäß A_25042-* (C.HCI.AUT) erfolgreich ist,
- der "sub"-Wert im Payload mit der Telematik-ID im "signierenden" Zertifikat übereinstimmt,
- der „cn“-Wert im Payload mit dem subject.commonName im "signierenden“ Zertifikat übereinstimmt,
- der "type"-Wert im Payload gleich "ePA-Authentisierung über PKI" ist,
- die professionOID im "signierenden" Zertifikat gleich 1.2.276.0.76.4.59 [oid_kostentraeger] ist,
- die "iat"-Zeit nicht älter als 15 Minuten ist.

[<=]

A_30434 -ePA-Aktensystem - Kostenträger können mit einem self-signed ID-Token ausschließlich den Aktenkontoumzug nutzen
Das ePA-Aktensystem MUSS sicherstellen, dass ein Kostenträger, der sich über ein selbst-signiertes JWT Bearer Token gemäß A_30391-* authentisiert hat, außer den Operationen des Account Managements zum Verschieben eines Aktenkontos keine weiteren Operationen oder Schnittstellen nutzen kann.**[<=]**

3.17 Anbindung Verzeichnisdienst FHIR-Directory

A_25176 -ePA-Aktensystem - Anbindung Verzeichnisdienst FHIR-Directory
Das ePA-Aktensystem MUSS bei der Suche des Versicherten nach Einträgen imVerzeichnisdienst 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.**[<=]**

3.18 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.

3.18.1 Paketfilter

3.18.1.1 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_14019-03 -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 folgenden Protokolle beschränken:

1. HTTPS,
2. OCSP-Zugriffe für das OCSP-Stapling (vgl. Hinweis nach A_14019-*), ggf. notwendige DNS Anfragen (und Antworten), und
3. OCSP-Zugriffe auf OCSP-Responder der TI-PKI im Internet.

Ein Verbindungsaufbau aus dem ePA-Aktensystem über das Access Gateway in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 und 3.
[<=]

Hinweis zu A_14019-: Der Aktensystem-Anbieter muss für seine HTTPS-Schnittstelle ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-Zertifikate also über einen aktuellen Webbrowser prüfbar ist, vgl. A_14776). Für dieses TLS-Zertifikat fragt das Access Gateway (die HTTPS-Schnittstelle ist Teil davon) regelmäßig für das OCSP-Stapling (vgl. [gemSpec_Krypt#A_24913-*]) den OCSP-Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält das Access Gateway eine OCSP-Response. Diese wird nach A_19126 geprüft und anschließend von der HTTPS-Schnittstelle verwendet (vgl. https://tools.ietf.org/html/rfc6066#section-8 und bspw. http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling).*

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

A_19126-02 -Access Gateway, OCSP-Status für das OCSP-Stapling
Der Paketfilter der Komponente Access Gateway MUSS bezüglich des OCSP-Stapling (vgl.A_24913-*) folgende Vorgaben umsetzen:

1. Für das vom Aktensystem-Anbieter erworbene TLS-Zertifikat (vgl. Hinweis zu A_14019-01) MUSS die Komponente initial die IP-Adresse (ggf. die IP-Adressen) des entsprechenden OCSP-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.**[<=]**

3.18.1.2 Redundanz

Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf#3.18.1.3]. Die Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Access Gateways.

Die Auswahl der Access Gateways wird durch das ePA-Frontend des Versicherten aus einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des Access Gateways kann der Anbieter des ePA-Aktensystems durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn jeder Versicherte mit existierendem Konto beim Anbieter des ePA-Aktensystems oder dessen berechtigter Vertreter die Möglichkeit zum Verbindungsaufbau hat.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen Access Gateways ist über grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern einzusetzen, so dass jedes einzelne Access Gateway im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

A_14026 -Access Gateway, Redundanz der Paketfilter im Access Gateway
Die Komponente Access Gateway MUSS sicherstellen, dass bei Ausfall eines von mehreren Paketfiltern die verbleibenden Paketfilter in demselben Standort den Datenverkehr aller Mandanten des ausgefallenen Paketfilters zusätzlich übernehmen können.**[<=]**

3.18.1.3 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.

3.18.1.4 Adressierung

3.18.1.4.1 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.**[<=]**

3.18.1.4.2 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.

3.18.2 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.**[<=]**

3.18.3 Tracing in Nichtproduktivumgebungen

Für die Fehlersuche - insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase - hat es sich als notwendig erwiesen, dass ein Fehlersuchender den Klartext der Kommunikation zwischen ePA-Client und VAU-Instanz mitlesen kann. (vgl. auch 2.5- Tracing in Nichtproduktivumgebungen)

Das Access Gateway stellt Informationen über die aktuell verfügbaren Sensorpunkte im AS bereit. Weiterhin exponiert das Access Gateway die Daten der Sensorpunkte über TCP (i. S. v. nicht TLS-gesichert) bspw. über Port 8001,...,8009. Die dort von den Sensorpunkten ge-streamten Daten sind nur Testdaten, also keine Echtdaten, d. h. sie haben keinen Schutzbedarf bezüglich Vertraulichkeit. Um die exponierten Sensordaten-Punkte vor DoS-Angriffen zu schützen, erlaubt das Access Gateway im Fall der Fälle die TCP-Ports auf IP-Layer über Firewall-Regeln abzusichern.

A_21890-02 -Access Gateway, Sensorpunkt für Nichtproduktivumgebungen
Die Komponente Access Gateway MUSS genau in Nichtproduktivumgebungen:

- die Daten der Sensorpunkte des Aktensystems auf TCP-Ports (bspw. auf 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,
"ipaddr": "IPv4-oder-IPv6-Adresse",
 "DoS-protection-type" : „secret_url“
 "DoS-protection-port" : „udp/46789“
},
{"name" : "Extra Senor VAU RZ2/B1/R1",
 "port" : 8002,
"ipaddr": "IPv4-oder-IPv6-Adresse",
 "DoS-protection-type" : „ssh_tunnel“
 "DoS-protection-port" : „tcp/46790“
}, ...
]
```

Weiter MÜSSEN folgende Vorgaben für die o. g. Datenstruktur eingehalten werden.

1. Sollten keine Sensorpunkte aktuell im AS aktiviert sein (bspw. bei Lasttests) so ist das Array leer: [ ].
2. Sollte es keinen optionalen DoS-Schutzmechanismus gemäß A_22582-* geben, so fallen die DoS-* Attribute in der o. g. Datenstruktur weg (sind nicht existent).
3. Wenn es einen FQDN gibt, bei dem jede erfolgreiche Namensauflösung dieser FQDN auf eine korrekte IP-Adresse verweist, dann KANN das "ipaddr"-Key-Value-Paar durch ein Key-Value-Paar
   `"fqdn": "FQDN-der-nach-Namesauflösung-die-korrekte-IP-Adresse-ergibt"`
   ersetzt werden. Das "ipaddr"-Feld fällt, dann also weg. (vgl. Hinweis 2 unter A_21890-*).
4. 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).

[<=]

Hinweise zu A_21890-:*

(1) 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.

(2) Es gibt Konstellationen bei denen ein FQDN auf mehrere verschiedene IP-Adresse aufgelöst wird. Beispielweise als einfache Form des Load-Balancings gibt der DNS-Server per Round-Robin aus einer Liste von IP-Adresse bei jeder Anfrage eine in der Liste als nächstes stehende IP-Adresse als Antwort und iteriert kontinuierlich über die Liste. Wenn jede erfolgreiche Antwort des DNS-Servers auf eine FQDN eine IP-Adresse als Ergebnis liefert, die im Sinne von A_21890- eine korrekte IP-Adresse ist (wo also Sensor-Daten auch abrufbar sind), so kann in der Datenstruktur von A_21890-* "fqdn" anstatt "ipaddr" aufgeführt werden.*

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.

3.18.4 Übergreifende Festlegungen

A_14249 -Komponente Access Gateway - Separierung der Schnittstellen für verschiedene Umgebungen
Die Komponente Access Gateway MUSS die Bereitstellung von Schnittstellen für die Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen Umgebungen der TI (RU/TU, PU) sicherstellen und voneinander separieren.**[<=]**

A_14034 -Access Gateway, Übergang des ePA-Aktensystems zur TI
Die Komponente Access Gateway MUSS sicherstellen, dass der Zugriff auf Dienste der TI ausschließlich über einen Sicheren Zentralen Zugangspunkt (SZZP) erfolgt.**[<=]**

A_14036 -Access Gateway, Synchronisierung der Komponenten mit den Stratum-1-NTP-Servern der TI
Die Komponente Access Gateway MUSS alle Komponenten seines Access Gateways mit den Stratum-1-NTP-Servern der TI synchronisieren.**[<=]**

A_13879 -Access Gateway, Serverseitige Authentisierung
Die Komponente Access Gateway MUSS sich gegenüber dem ePA-Frontend des Versicherten beim Aufbau der TLS-Session durch sein ExtendedValidation-Zertifikat authentisieren. Die Beschaffung des Zertifikats erfolgt durch den Anbieter über eine öffentliche CA.**[<=]**

A_14033 -Access Gateway, TLS Verschlüsselung
Die Komponente Access Gateway MUSS sicherstellen, dass jede Kommunikation mit dem ePA-Frontend des Versicherten TLS verschlüsselt erfolgt.**[<=]**

Die Verwendung der SoapAction ermöglicht einer Reverse-Proxy-Komponente innerhalb des Access Gateways, die Nachrichten zu verarbeiten, ohne die http-Payload zu untersuchen.

A_13876 -Access Gateway, Kein direkter Zugriff auf Dienste der zentralen TI-Plattform
Die Komponente Access Gateway MUSS einen direkten Zugriff aus dem Internet auf Dienste der zentralen TI-Plattform verhindern.**[<=]**

A_14016 -Access Gateway , Schutz vor Angriffen aus dem Internet
Die Komponente Access Gateway MUSS für alle vom Internet erreichbaren Schnittstellen Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS Lösungen verhindert werden.**[<=]**

A_15196 -Access Gateway, Schutz vor volumetrischen DoS-Angriffen
Die Komponente Access Gateway MUSS bei Beauftragung eines qualifizierten Dienstleisters zum Schutz vor volumetrischen DoS-Angriffen Kriterien des BSI zur Auswahl qualifizierter Dienstleister umsetzen.**[<=]**

Als Maßnahme gegen volumetrische Denial-of-Service-Angriffe wird die Verwendung von DNS- oder BGP-Routing-Diensten empfohlen. Hinweise des BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/DDoS/ddos_node.html.

3.19 Data Submission Service

Die Daten der elektronischen Patientenakten sollen nach § 363 Absatz 1 SGB V für die in § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszwecke zugänglich gemacht und hierfür in pseudonymisierter Form automatisiert von den ePA-Aktensystemen an das Forschungsdatenzentrum Gesundheit (FDZ) nach § 303d SGB V übermittelt werden, sofern Versicherte dem nicht widerprochen haben.

Neben dem FDZ und den ePA-Aktensystemen ist die Vertrauensstelle (VST) nach § 303c SGB V im Prozess involviert. Deren Aufgabe ist es, die von den ePA-Aktensystemen erhaltenen Lieferpseudonyme in periodenübergreifende Pseudonyme umzuwandeln und diese an das FDZ zu übermitteln.

Der Data Submission Service im Aktensystem übernimmt in der Übermittlung der pseudonymisierten medizinischen Daten folgende Aufgaben:

- Erstellung der Lieferpseudonyme (auf Basis der KVNR) und der Arbeitsnummern
- Registrierung der Arbeitsnummer mit dem zugehörigen Lieferpseudonym bei der Vertrauensstelle
- Pseudonymisierung der medizinischen Daten
- Verknüpfung der pseudonymisierten medizinischen Daten mit der Arbeitsnummer
- Übermittlung der pseudonymisierten medizinischen Daten und der zugehörigen Arbeitsnummern an das Forschungsdatenzentrum Gesundheit

Die Übermittlung der Daten erfolgt blockweise. D.h. es wird ein Paket von pseudonymisierten medizinischen Daten mit zugehörigen Arbeitsnummern aus verschiedenen Aktenkonten zusammengestellt (Datenpaket FDZ) und alle für dieses Paket benötigten Arbeitsnummern und Lieferpseudonyme mit einem Mal bei der VST registriert (Datenpaket VST). Die Datenpakete haben eine anbieterübergreifend eindeutige SubmissionID und die SubmissionID zusammengehöriger Datenpakete VST und FDZ ist identisch.

Für die Übermittlung wird zwischen Aktensystem und VST, sowie Aktensystem und FDZ jeweils ein beidseitig authentisierter VAU-Kanal aufgebaut, auf dem sich die Dienste VST und FDZ mit einer Identität ID.FD.AUT mit ihren entsprechenden Rollen authentisieren.

Der Versicherte kann mit Hilfe seines ePA-FdVs oder über die Ombudsstelle des Kostenträgers der Übermittlung seiner pseudonymisierten medizinischen Daten an das FDZ widersprechen oder die möglichen Sekundärnutzungszwecke seiner übermittelten pseudonymisierten medizinischen Daten im FDZ einschränken. Dies erfolgt über das Consent Decision Management im Aktensystem.

3.19.1 Erstellung von Arbeitsnummern und Lieferpseudonymen

Der Data Submission Service erzeugt eindeutige Arbeitsnummern und Lieferpseudonyme, um die pseudonymisierten medizinischen Daten in der Übermittlung an das FDZ eindeutig zuordnen zu können.

A_26211 -Data Submission Service - Erstellung des Lieferpseudonyms
Der Data Submission Service MUSS das Lieferpseudonym des Versicherten gemäß [I_VST] unter Verwendung der KVNR des Versicherten erstellen.**[<=]**

A_26409 -Data Submission Service - keine Erstellung von LP für Validierungsaktenkonten
Der Data Submission Service DARF KEINE Lieferpseudonyme für KVNRn von Validierungsaktenkonten erstellen.**[<=]**

A_26212 -Data Submission Service - Erstellung der Arbeitsnummer
Der Data Submission Service MUSS für die Arbeitsnummer einen Zufallswert mit einer Mindestentropie von 120 Bit erzeugen und die Kodierung aus [I_VST] verwenden.**[<=]**

A_26410 -Data Submission Service - keine Erstellung von AN für Validierungsaktenkonten
Der Data Submission Service DARF KEINE Arbeitsnummern für Daten aus Validierungsaktenkonten erstellen.**[<=]**

A_26255 -Data Submission Service - Verwendungsdauer von Lieferpseudonymen und Arbeitsnummern
Der Data Submission Service MUSS für jedes in einem Datenpaket FDZ übermittelte pseudonymisierte medizinische Datum zu einer KVNR eine neue Arbeitsnummer und ein neues Lieferpseudonym generieren.**[<=]**

A_26256 -Data Submission Service - Registrierung von Arbeitsnummern
Der Data Submission Service MUSS jede Arbeitsnummer zusammen mit dem zugehörigen Lieferpseudonym in das entsprechende Datenpaket VST aufnehmen und an die Vertrauensstelle übermitteln.**[<=]**

3.19.2 Auswahl von medizinischen Daten

Der Data Submission Service muss bestimmte neue und geänderte FHIR-Ressourcen an den FDZ übertragen. Dies betrifft im ersten Schritt die Medikationsdaten aus der E-Medikationsliste und wird subsequent weiter ausgebaut.

Der Medication Service, als Quelle der Medikationsdaten zur Übertragung an den FDZ, erlaubt flexible, datenbasierte Operationen auf einzelnen FHIR-Ressourcen. Dies erfordert entsprechende Implementierung um effizient und zuverlässig die neuen und geänderten Ressourcen identifizieren können um daraus die Auswahl für die zu übertragende FHIR-Ressourcen treffen zu können.

A_26296 -Data Submission Service - Übertragung neuer und geänderter FHIR-Ressourcen

Der Data Submission Service MUSS neue und geänderte FHIR-Ressourcen identifizieren können und daraus die Auswahl für die Übermittlung der Daten an FDZ treffen können. **[<=]**

A_26297 -Data Submission Service - Einschränkung der FHIR-Ressourcen nach Änderungsdatum
Der Data Submission Service MUSS den Zeitpunkt der letzten Übermittlung (lastSubmissionTimestamp) merken und in nachfolgenden Übermittlungen nur die Ressourcen, die sich seit diesem Zeitpunkt geändert haben, berücksichtigen. Hierfür ist das FHIR-Element meta.lastUpdated in der jeweiligen FHIR-Ressource zu verwenden.**[<=]**

Hinweis: Ressourcen, die im Rahmen eines Anbieterwechsels in ein Aktenkonto übernommen werden, sind nicht erneut zu übermitteln.

A_26298 -Data Submission Service - FHIR-Ressourcen zur Übermittlung an FDZ
Der Data Submission Service MUSS die FHIR-Ressourcen gemäß der Tabelle "Auswahl der zu übertragenden FHIR-Ressourcen" an FDZ übertragen, dabei sind die Filter-Bedingungen (Spalte 'Filter Expression') und zu inkludierende referenzierte Ressourcen zu berücksichtigen (Spalte 'Include' sowie Tabelle "Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen").**[<=]**

Tabelle 38: Auswahl der zu übertragenden FHIR-Ressourcen

Ressourcentyp /Profil	Filter Expression	Include
MedicationRequest ${epa-medication}/epa-medication-request	`status != 'active' and identifier.where(system='https://gematik.de/fhir/epa-medication/sid/rx-prescription-process-identifier').hasValue()`	`MedicationRequest:medication`
MedicationDispense ${epa-medication}/epa-medication-response	`status != 'in-progress' and extension('https://gematik.de/fhir/epa-medication/StructureDefinition/rx-prescription-process-identifier-extension').hasValue()`	`MedicationDispense:medication`

Tabelle 39: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen

Ressourcentyp/Profil	Anmerkung
Medication ${epa-medication}/epa-medication	Referenziert durch MedicationRequest, MedicationDispense

3.19.3 Protokollierung des Datenexports an das FDZ

Ein Datenexport erfolgt immer in Verbindung mit dem Einstellen neuer oder der Änderung existierender Daten für ein Aktenkonto. Ein Datenexport nach Auswahl der Daten gemäß A_26298 wird als Bestandteil der Protokollierung des auslösenden Ereignisses protokolliert (siehe [gemIG_ePA_Medication]).

3.19.4 Pseudonymisierung von medizinischen Daten

Bevor medizinische Daten an das FDZ übermittelt werden dürfen, müssen diese pseudonymisiert werden und Daten mit direktem Personenbezug entfernt werden.

A_26300 -Data Submission Service - Pseudonymisierung von medizinischen Daten
Der Data Submission Service MUSS an das FDZ zu übermittelnde medizinische Daten gemäß der Vorgaben aus [DataPseudonymization] pseudonymisieren.**[<=]**

A_26408 -Data Submission Service - keine Pseudonymisierung von Daten aus Validierungsaktenkonten
Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem. Kapitel 2.4) pseudonymisieren.**[<=]**

A_26315 -Data Submission Service - Randomisierung der Reihenfolge des Datenpakets FDZ
Das ePA-Aktensystem MUSS sicherstellen, dass in einem Datenpaket FDZ vor der Übermittlung die Einträge nach Arbeitsnummer (AN) aufsteigend sortiert werden. Die Arbeitsnummer (32-Byte Zufallswert, A_26212-*) wird dabei als natürliche Zahl (byteorder=big) interpretiert.**[<=]**

Verständnishinweis:

Die Akten werden regelmäßig nach zu übermittelnden Daten vom ePA-Aktensystem durchsucht. Dabei kann es passiert, dass in einer Akte mehrere Daten zur Übermittlung anfallen, die nach der Pseudonymisierung in einer Reihenfolge in das Datenpaket FDZ gelangen. Deshalb kann die Reihenfolge der Einträge im Datenpaket FDZ statistisch relevante Informationen über den Zusammenhang von Einträgen geben. Durch eine Randomisierung der Reihenfolge der Einträge innerhalb des Datenpakets wird dies verhindert. Die AN werden zufällig erzeugt, eine Sortierung nach AN ist deshalb eine Randomisierung der Reihenfolge.

3.19.5 Übermittlung der pseudonymisierten medizinischen Daten

Die Übermittlung von Datenpaketen an VST und FDZ erfolgt gemäß den Vorgaben des RKI (VST) und BfArM (FDZ) und deren Schnittstellenspezifikationen.

Die Übermittlung der pseudonymisierten Daten eines Aktenkontos für Sekundärnutzungszwecke erfolgt automatisch, sofern kein Widerspruch gegen Sekundärdatennutzung vorliegt. Die Voreinstellung ist dabei "kein Widerspruch erteilt" (siehe:3.7.1- Widersprüche für Funktionen der ePA). Vor der allerersten Übermittlung solcher Daten wird dem Versicherten daher eine Frist gewährt, gegebenenfalls einen Widerspruch gegen diese Sekundärdatennutzung zu formulieren.

A_26462 -Data Submission Service - Übermittlung Datenpaket nach Ablauf der Widerspruchsfrist
Der Data Submission Service MUSS sicherstellen, dass vor der erstmaligen Übermittlung von Daten eines Aktenkontos die Widerspruchsfrist gemäß den Vorgaben des Kostenträgers abgelaufen ist.**[<=]**

Hinweis: Die erste Datenübermittlung ist die erste automatisiert mögliche Übermittlung (nach Aktivierung des Aktenkontos) und nicht die erste Datenübermittlung nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung.

Hinweis: Für eine Übermittlung nach Ablauf dieser Widerspruchsfrist oder nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung werden immer nur ab diesem Zeitpunkt neu angefallene Daten berücksichtigt, Es erfolgt keine Übermittlung von vorhandenen Daten des Aktenkontos.

A_26214 -Data Submission Service - Erstellung der SubmissionID
Der Data Submission Service MUSS für zusammengehörige Datenpakete VST und FDZ eine gemeinsame anbieterübergreifend eindeutige SubmissionID erzeugen und diese mit den Datenpaketen übertragen.**[<=]**

A_26304 -Data Submission Service - Zufällige SubmissionID
Der Data Submission Service MUSS sicherstellen, dass die SubmissionID ein zufällig gewählter 256-Bit Wert mit einer Mindestentropie von 120 Bit ist.**[<=]**

A_26215 -Data Submission Service - Übermittlung Datenpaket VST
Der Data Submission Service MUSS das Datenpaket VST gemäß [I_VST] an die Vertrauensstelle übermitteln.**[<=]**

A_26407 -Data Submission Service - keine Übermittlung von Daten aus Validierungsaktenkonten
Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem. Kapitel 2.4) an das Forschungsdatenzentrum übermitteln.**[<=]**

A_26216 -Data Submission Service - Realisierung der Schnittstelle I_Data_Submission_Service
Der Data Submission Service MUSS die Operationen der Schnittstelle I_Data_Submission_Service gemäß [I_Data_Submission_Service] umsetzen.**[<=]**

A_26217 -Data Submission Service - Verbindung zur Vertrauensstelle
Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des Datenpakets VST ausschließlich über einen VAU-Kanal erfolgt in dem sich die Vertrauensstelle über ein Zertifikat C.FD.AUT mit professionOID gleich oid_epa_vst authentisiert hat.**[<=]**

A_26218 -Data Submission Service - Verbindung zum Forschungsdatenzentrum Gesundheit
Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des Datenpakets FDZ ausschließlich über einen VAU-Kanal erfolgt in dem sich das Forschungsdatenzentrum Gesundheit über ein Zertifikat C.FD.AUT mit professionOID gleich oid_epa_fdz authentisiert hat.**[<=]**

A_26299 -Data Submission Service - Wechsel des Verschlüsselungsschlüssels für Datenpakte
Falls die Datenpakete VST und FDZ außerhalb der VAU im System des Aktensystembetreibers gespeichert werden, MUSS der Data Submission Service sicherstellen, dass ein Schlüssel für die Verschlüsselung der Datenpakete VST bzw. FDZ maximal 4 Wochen genutzt werden kann und danach ein neuer Verschlüsselungsschlüssel mittels der Regel hsm-r8 mit Hilfe eines geänderten Ableitungsvektors abgeleitet wird.**[<=]**

A_26312 -Data Submission Service - Timeout in der Übermittlung
Der Data Submission Service MUSS die Übermittlung der Pakete VST und FDZ erneut starten, wenn das Datenpaket FDZ nicht innerhalb von 30 Minuten nach erfolgreicher Übermittlung des Datenpakets VST abgerufen wird.**[<=]**

A_26313 -Data Submission Service - Konfiguration der Intervalle und maximalen Größe eines Datenpakets
Der Data Submission Service MUSS folgende Parameter konfigurierbar gestalten:

- das Intervall in dem Datenpakete VST und FDZ übermittelt werden
- eine maximale Größe eines Datenpakets FDZ bei deren Erreichen die Datenpakete übermittelt werden

[<=]

A_26244-01 -Data Submission Service - Löschen von Datenpaketen nach Übermittlung
Der Data Submission Service MUSS nach erfolgreicher Übermittlung des Datenpakets FDZ an das Forschungsdatenzentrum Gesundheit das übermittelte Datenpaket FDZ und das zugehörige Datenpaket VST nach Ablauf eine Wartefrist von 15 Minuten lokal löschen.
[<=]

Hinweis: Das ePA-Aktensystem kann von einer erfolgreichen Übermittlung im Sinne der Anforderung ausgehen, wenn die letzten Daten des Datenpakets FDZ gesendet wurden. Die Wartefrist soll es dem Forschungsdatenzentrum ermöglichen eine erfolglose Übermittlung erneut anzustoßen.

A_26245-01 -Data Submission Service - Löschen von Datenpaketen bei Nicht-Übermittlung
Der Data Submission Service MUSS das Datenpaket FDZ und das zugehörige Datenpaket VST lokal löschen, wenn das Datenpaket FDZ länger als 72 Stunden nicht an das Forschungsdatenzentrum Gesundheit übermittelt werden konnte. Die enthaltenen Widersprüche gegen die Übermittlung von Daten zur Sekundärnutzung durch das FDZ und zu Sekundärnutzungszwecken MÜSSEN in die aktuell in Erstellung befindlichen Datenpakete VST und FDZ übernommen werden.**[<=]**

Hinweis: Wenn Widersprüche in ein neues Datenpaket übernommen werden, muss für jeden der Widersprüche eine neue Arbeitsnummer (AN) und ein Lieferpseudonym (LP) erstellt werden, da die bisherigen AN und LP im Kontext des zu löschenden Paketes stehen.

A_26246 -Data Submission Service - Aufnahme von Widersprüchen
Der Data Submission Service MUSS Widersprüche gegen die Freigabe von Daten zur Sekundärnutzung durch das FDZ oder Änderungen zu Sekundärnutzungszwecken, aus dem Consent Decision Management, in die aktuell in Erstellung befindlichen Datenpakete VST und FDZ übernehmen. Es MUSS sichergestellt werden, dass in einem Datenpaket FDZ für eine KVNR immer nur die zuletzt erklärten Widersprüche gegen die Übermittlung von Daten zur Sekundärnutzung durch das FDZ bzw. zu Sekundärnutzungszwecken enthalten sind.**[<=]**

Hinweis: Sollte während der Erstellung eines Datenpakets FDZ mehrfach die Widersprüche für eine KVNR geändert werden, wird immer nur der letzte Stand übermittelt.

A_26307 -Data Submission Service - Durchsetzung von Widersprüchen
Falls für ein Aktenkonto ein Widerspruch gegen die Übermittlung an das FDZ eingestellt wird, MUSS der Data Submission Service sicherstellen, dass in allen zukünftig zu übermittelnden Datenpaketen VST und FDZ außer den Daten für den Widerspruch keine Daten für dieses Aktenkonto enthalten sind.
[<=]

*Hinweis zu A_26307: Zum Z*eitpunkt des Eingangs des Widerspruchs im Aktensystems bereits in der Übermittlung befindliche Datenpakte sind von der Anforderung ausgeschlossen. Betroffen sind jedoch auch die aktuell in Erstellung befindlichen Datenpakte VST und FDZ, bei denen die Übermittlung an die VST bzw. das FDZ noch nicht begonnen hat.

3.20 Push Notification Management

Nutzer von Anwendungen für Versicherte (ePA-FdV) können mittels Push Notifications direkt über Ereignisse in bestimmten Fachdiensten der TI oder des Kostenträgers auf ihren Endgeräten informiert werden. Diese Notifications erreichen einen Nutzer auch außerhalb aktiver Anmeldungen in diesen Fachdiensten. Die Ereignisse von Interesse zur Benachrichtigung des Nutzers sind dabei individuell abonnierbar.

Der Versand einer Push Notification erfolgt stets durch die einzelnen Fachdienste für Ereignisse ihrer Domäne. Die Übertragung in das Endgerät des Nutzers unter Einbindung der plattformspezifischen, externen Push-Dienste und betreiberspezifischen Push-Gateways wird für alle beteiligten Fachdienste gemeinsam durch ein Push Notification System realisiert. Dieses anwendungsübergreifende System und seine Komponenten für Push Notifications im Gesundheitswesen sind in [gemF_PushNotification] und [PushNotificationConcept] detailliert beschrieben.

Dort sind auch die normativen Vorgaben für unterstützende Anwendungen und Fachdienste in Bezug auf Registrierung von Applikationen und Ereignissen für Push Nachrichten, Schnittstellen, sicherheitstechnische Anforderungen und notwendige Artefakte für einen interoperablen Betrieb formuliert.

3.20.1 Push Notification Management des ePA-Aktensystems

Das Push Notification Management des ePA-Aktensystems ist als ein spezifischer Fachdienst in dieses übergreifende System eingebunden und bedient die in [gemF_PushNotification] geforderten und in [PushNotificationConcept] beschriebenen Schnittstellen und Verfahren.

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

Der Nutzung des Push Notification Managements der ePA kann nicht widersprochen werden. Dieser Dienst gehört nicht zu den widerspruchsfähigen Funktionen der ePA. Versicherte, die keine Benachrichtigungen der ePA erhalten möchten, können die Benachrichtigungen durch Abwahl der Benachrichtigungskanäle oder auch generell durch den Verzicht des ePA-FdV auf eine Registrierung für Push Notifications unterbinden.

Schnittstellen, die das Push Notification Management der ePA zur Nutzung durch Clients (ePA-FdV) anbietet, sind um ePA-spezifische Verfahren und Anforderungen ergänzt und als OpenApi gemäß [I_Push_Notification_Management] verfügbar.

A_27637 -Push Notification Management - Realisierung der Schnittstelle I_Push_Notification_Management
Das Push Notification Management MUSS die Operationen der Schnittstelle I_Push_Notification_Management gemäß [I_Push_Notification_Management] umsetzen.
[<=]

3.20.2 Registrierung eines ePA-FdV als Pusher

(siehe auch: [gemF_PushNotification]#Kapitel "Pusher registrieren")

Ein Versicherter kann registrierte Geräte (im Sinne des Device Managements gemäß3.11-Device Management) zur Nutzung seiner aktivierten elektronischen Patientenakte auch für den Erhalt von Push Nachrichten nutzen, sofern das übergreifende Push Notification System die technologische Infrastruktur für Benachrichtigungen an den Geräte-, bzw. Betriebsystemtyp des Versichertengeräts unterstützt. Dazu kann die ePA-FdV-Anwendung

jedes dieser Geräte als ePA-FdV Instanz, bzw. 'Pusher', im eigenen Aktenkonto des Versicherten registriert werden.

Die ePA-FdV Instanz Registrierung eines Gerätes als Pusher erfolgt immer durch und für das auf diesem Gerät installierte ePA-FdV und unter Nutzung der Schnittstelle [I_Push_Notification_Management]. Über diese Schnittstelle werden existierende Registrierungen auch aktualisiert und wieder entfernt.

Die Daten der Registrierungen, inklusive des kryptographischen Materials der Schlüsselableitungen und der Auswahl der Benachrichtigungskanäle, sind Bestandteil des Aktenkontos und werden dort gespeichert. Pro registriertem Gerät kann jeweils nur eine ePA-FdV Instanz im Aktenkonto hinterlegt sein und eine Registrierung gilt immer nur für genau eine bestimmte ePA-FdV Instanz. Eine ePA-FdV Instanz Registrierung ist daher fest an eine Device Registration gebunden.

A_27638 -Push Notification Management- Speicherung der Daten
Das Push Notification Management MUSS alle Daten des Dienstes für einen Versicherten im SecureDataStorage des Aktenkontos des Versicherten speichern.**[<=]**

A_27640 -Push Notification Management - automatisches Löschen der Registrierung einer ePA-FdV Instanz
Das Push Notification Management MUSS sicherstellen, dass eine existierende Registrierung einer ePA-FdV Instanz und die dazugehörigen Daten vollständig und automatisch gelöscht werden, wenn die Device Registration des assoziierten Geräts im Device Management des Aktensystems gelöscht wird.**[<=]**

A_27639 -Push Notification Management - eindeutiger pushKey
Das Push Notification Management MUSS sicherstellen, dass der pushKey einer Registrierung einer ePA-FdV Instanz eindeutig ist und es keine zwei oder mehr Registrierungen mit gleichem pushKey gibt.**[<=]**

Bei jedem Versand einer Push Nachricht an das Push Gateway kann dieses in den Rückgabewerten der Push Operation einen Eintrag oder eine Liste veralteter, bzw. ungültiger pushKeys melden. Eine weitere Nutzung solcher Registrierungen, bzw. pushKeys, soll unterbleiben. Die assoziierten Registrierungen von ePA-FdV-Instanzen werden daher aus dem Aktenkonto entfernt.

A_27682 -Push Notification Management - Entfernen ungültiger pushKeys
Das Push Notification Management MUSS Registrierungen von ePA-FdV-Instanzen löschen, wenn pushKeys dieser Registrierungen durch das Push Gateway als ungültig gemeldet werden.**[<=]**

Hinweis: Es werden nur Registrierungen aus dem versendenden Aktenkonto entfernt. Ebventuelle Rückmeldungen des Push Gateways zu pushKeys, die nicht oder nicht mehr mit dem versendenden Aktenkonto verbunden sind, werden ignoriert.

3.20.3 Push Notification Channels

(siehe auch: [gemF_PushNotification]#Kapitel "Channel/ Trigger Konfiguration")

Das ePA-Aktensystem bietet eine Auswahl an Channels zu Ereignissen, über deren Aktivität ein Versicherter durch Push-Benachrichtigungen informiert werden kann. Der jeweilige Nachrichteninhalt beschreibt dabei in Kurzform das auslösende Ereignis.

Die Grundeinstellung für den Versand von Push-Benachrichtigungen an neu erstellten Registrierungen für ePA-FdV-Instanzen lautet für jeden Channel zunächst 'not_set'. Das bedeutet, der Channel wurde bisher nicht konfiguriert und es werden keine Benachrichtigung für diesen Kanal versendet.
Ein Versicherter kann diese Grundeinstellung individuell für jede seiner ePA-FdV-

Instanzen jederzeit ändern und die Benachrichtigung pro Channel aktivieren ('enabled' - Benachrichtigungen für diesen Kanal), bzw. auch wieder deaktivieren.

Die Verwaltung der individuellen Channelkonfiguration des ePA-Aktenkontos für eine registrierte ePA-FdV-Instanz erfolgt über die Schnittstelle [I_Push_Notification_Management].

A_27641-02 -Push Notification Management - Push Notification Channels
Das Push Notification Management MUSS ausschließlich für die folgenden Ereignisse Push Nachrichten erstellen können, wenn das Ereignis durch einen Nutzer der definierten Nutzergruppe ausgelöst wird und die damit verbundene Operation erfolgreich (nicht durch einen Fehler abgebrochen) ist.

Tabelle 40: Ereignisse und deren Push Nachrichten

Ereignis	channelId	Beschreibung	Nutzergruppen
Neues Dokument eingestellt	epa.document.put	Ein Dokument wurde durch einen Nutzer neu eingestellt.	alle, außer Versicherter
Dokument aktualisiert	epa.document.update	Ein aktualisiertes Dokument wurde durch einen Nutzer eingestellt.	alle, außer Versicherter
Befugnis erstellt	epa.entitle.put	Eine Befugnis wurde durch das ePA-FdV erstellt.	nur Vertreter
Befugnis gelöscht	epa.entitle.del	Eine existierende Befugnis wurde durch das ePA-FdV gelöscht.	nur Vertreter
Befugniserstellung im Behandlungskontext	epa.entitle.ps	Eine Befugnis wurde mittels VSDM-Prüfnachweis, bzw. PoPP, erstellt.	alle, außer FdV Nutzer
Verbergen aufgehoben (Dokument)	epa.constraint.del	Ein zuvor verborgenes Dokument ist wieder sichtbar.	nur Vertreter
Verbergen aufgehoben (dynamischer Ordner)		Ein zuvor verborgener dynamischer Ordner ist wieder sichtbar.	nur Vertreter
Verbergen aufgehoben (Kategorie)		Eine zuvor verborgene Kategorie wieder sichtbar.	nur Vertreter

[<=]

Hinweis 1 zu A_27641*:
Da technische Dokumente gemäß A_23144* ausschließlich der Nutzung durch das ePA

FdV dienen und für Nutzer nicht sichtbar sind, werden für technische Dokumente keine Push Notification versendet.

Hinweis 2 zu A_27641*:

Die Ereignisse zum Einstellen und Aktualisieren von Dokumenten sind nicht eingeschränkt auf den XDS Document Service, sondern werden in allen Services wirksam in denen Dokumente in das ePA-Aktensystem eingestellt werden.

3.20.4 Push Notification Nachrichteninhalte

(siehe auch: [gemF_PushNotification]#Kapitel "Operation Notify")

Für jedes ausgelöste Ereignis eines Push Channels wird eine Push Notification erstellt. Die Nachrichtendaten für ein Ereignis werden strukturiert gemäß Schema angeordnet und nach den Vorgaben in [gemF_PushNotification#A_27610-*] auf konstante Länge aufgefüllt.

A_27645 -Push Notification Management - Push Notification Datenstruktur
Das Push Notification Management MUSS die Nachrichtendaten einer Push Nachricht für den Versand gemäß [Schema_PushNotifications] strukturieren.**[<=]**

Es gibt eine maximal erlaubte Größe für Nachrichteninhalte, die durch das Push Notification System [gemF_PushNotification] vorgegeben wird. Es muss sichergestellt werden, dass erzeugte Nachrichteninhalte diese Größe nicht übersteigen.

A_27673 -Push Notification Management - Verkürzung der Nachrichteninhalte
Falls der erzeugte Nachrichteninhalt die maximal erlaubte Größe für Nachrichteninhalte übersteigt MUSS das Push Notification Management die Elemente `actor`, `title`, `who`, `folderTitle` so verkürzen, dass die maximal erlaubte Größe für Nachrichteninhalte gerade nicht überschritten wird.**[<=]**

Hinweis: Es müssen nicht alle aufgeführten Elemente gleichzeitig verkürzt werden.

A_27674 -Push Notification Management - Art der Verkürzung
Falls Elemente einer Nachricht verkürzt werden, dann sollen diese so verkürzt werden, dass:

- am Ende der Zeichenkette Zeichen entfernt werden
- die Verkürzung mit "..." angezeigt wird.

[<=]

Hinweis: Es kann sinnvoll sein, nur das längste kürzbare Element zu kürzen. Es wird empfohlen eine Mindestlänge von 50 Bytes nicht zu unterschreiten.

3.20.5 Versenden von Push Nachrichten

(siehe auch: [gemF_PushNotification]#Kapitel "Operation Notify" und [PushNotificationConcept]#Concept: "Verschlüsselung des Benachrichtigungsinhasts")

Eine erstellte Push Nachricht wird an jede ePA-FdV-Instanz mit einer Registrierung im Aktenkonto gesendet, wenn für diese der assoziierte Kanal abonniert wurde (Konfiguration channelId == enabled).

Die längenkorrigierte Nachricht wird jeweils mit dem für den aktuellen Monat gültigen Schlüssel`AES/CGM-Schlüssel-Jahr-Monat` der Registrierung für jede adressierte ePA-FdV-Instanz verschlüsselt. Das Verschlüsselungsergebnis ist der Inhalt von`ciphertext` der `notification` für den Versand ([I_Push_Gateway]).

A_27651 -Push Notification Management - verpflichtende Verschlüsselung der Nachrichteninhalte
Das Push Notification Management MUSS sicherstellen, dass ausschließlich verschlüsselte Nachrichteninhalte als Push Nachricht versendet werden.**[<=]**

Jedes einer Push Nachricht zugrundeliegenden Ereignis erzeugt auch einen Protokolleintrag im Audit Event Service. Die Menge der korrespondierenden Protokolleinträge ergibt dadurch im Aktenkonto ein Archiv der Push Ereignisse. Damit Clients ein Push Ereignis zu einem späteren Zeitpunkt, also nachdem die Push Nachricht im Client selbst schon gelöscht ist, restaurieren können, wird jeder Push Nachricht auch der Identifier des Protokolleintrags angehängt.

A_27644 -Push Notification Management - Referenz auf Protokolleintrag
Das Push Notification Management MUSS den eindeutigen Identifier `Resource.id` des zu einem Push Notification Ereignis gehörenden Protokolleintrags (AuditEvent) des Aktenkontos im Feld `notification/identifier` einer Push Notification angeben.**[<=]**

Hinweis:
Gemäß A_24925 können Zugriffe gleicher Art im XDS Document Service mit mehreren Entity Strukturen unter einem AuditEvent gebündelt werden. Es gibt dann einen Audit Event Identifier, auch wenn beispielsweise drei Dokumente in die Akte eingestellt wurden. Im Feld `notification/identifier` einer Push Notification wird dann mehrmals der gleiche Identifier eingetragen.

A_28218 -Push Notification Management - verpflichtende Stapelverarbeitung
Das Push Notification Management MUSS beim Senden von Push Notifications mehrere Push Notifications, die an denselben Endpunkt eines Push Gateways geschickt werden, gemeinsam in einer Stapelverarbeitung bearbeiten.**[<=]**

3.21 Backendseitige Zusatzfunktionen

Backendseitige Zusatzfunktionen sind Funktionen, die vom Hersteller des ePA-Aktensystems im ePA-Aktensystem integriert werden können und mit denen Kostenträger ihren Versicherten Mehrwerte anbieten können, die über den gesetzlich vorgegebenen Funktionsumfang der ePA hinausgehen. Backendseitige Zusatzfunktionen können hierfür Daten aus Akten der Versicherten nutzen.

Backendseitige Zusatzfunktionen sind ein Angebot der Kostenträger für ihre Versicherten, welches die Versicherten freiwillig nutzen können. Mit ihrem ePA-FdV können sie jederzeit in eine backendseitige Zusatzfunktion, die durch ihren Kostenträger angeboten wird, einwilligen oder eine erteilte Einwilligung widerrufen.

Die gematik spezifiziert die backendseitigen Zusatzfunktionen nicht, legt jedoch in diesem Abschnitt die Rahmenbedingungen fest, um backendseitige Zusatzfunktionen im ePA-Aktensystem intergieren zu können.

Im Folgenden werden mit

- **ePA-Daten**diejenigen Daten und Dokumente der Akte eines Versicherten bezeichnet, die durch die gesetzlichen Funktionen der ePA eingestellt und verarbeitet werden,
- **ZF-Daten**diejenigen Daten und Dokumente bezeichnet, die durch eine backendseitige Zusatzfunktion erzeugt und verarbeitet werden.

A_30445 -Backendseitige Zusatzfunktionen - Angebot ausschließlich durch Anbieter des Aktensystems (Kostenträger)
Der Betreiber des ePA-Aktensystems MUSS gewährleisten, dass backendseitige Zusatzfunktionen im ePA-Aktensystem ausschließlich durch einen Anbieter des ePA-Aktensystems (Kostenträger) angeboten werden.**[<=]**

A_30448 -Backendseitige Zusatzfunktionen - Anbieter gewährleistet Datenschutz und Sicherheit der Zusatzfunktion
Der Anbieter eines ePA-Aktensystems, der seinen Versicherten eine backendseitige Zusatzfunktion anbietet, MUSS sicherstellen, dass die backendseitige Zusatzfunktion

- die für die Verarbeitung von personenbezogenen Daten geltenden Vorschriften zum Datenschutz einhält und
- die erforderlichen technischen und organisatorischen Maßnahmen entsprechend dem Stand der Technik umsetzt, um die Anforderungen an die Sicherheit im Hinblick auf die Schutzbedürftigkeit der in der Zusatzfunktion verarbeiteten Daten zu gewährleisten.

[<=]

A_30446 -Backendseitige Zusatzfunktionen - Information im Sicherheitsgutachten für den Betrieb des Aktensystems
Der Betreiber eines ePA-Aktensystems MUSS sicherstellen, dass im durch den Anbietertypsteckbrief des ePA-Aktensystems geforderten Sicherheitsgutachten für den Zeitraum zwischen der letzten Sicherheitsbegutachtung und der aktuellen Sicherheitsbegutachtung aufgelistet wird, welche Kostenträger beim Betreiber seit wann welche backensdseitigen Zusatzfunktionen anbieten oder bis wann angeboten haben.
[<=]

A_30447 -Backendseitige Zusatzfunktionen - Information im Produktgutachten für das Produkt ePA-Aktensystem
Der Hersteller eines ePA-Aktensystems MUSS sicherstellen, dass im Produktgutachten für das ePA-Aktensystem aufgelistet wird, welche backendseitigen Zusatzfunktionen in dem Zeitraum zwischen der letzten Sicherheitsbegutachtung und der aktuellen Sicherheitsbegutachtung zum ePA-Aktensystem hinzugefügt und entfernt wurden. In der Auflistung der backendseitigen Zusatzfunktionen ist deren Zweckbestimmung anzugeben.**[<=]**

Hinweis zu A_30446 und A_30447: Es wird keine Begutachtung der backendseitigen Zusatzfunktionen durch den Gutachter gefordert. Es soll jedoch transparent sein, welche backendseitigen Zusatzfunktionen im ePA-Aktensystem implementiert und von welchem Kostenträger genutzt werden.

3.21.1 Zugriffsmodell für backendseitige Zusatzfunktionen

Die folgende Abbildung zeigt zum einen die möglichen Zugriffsrechte der backendseitigen Zusatzfunktionen auf die ePA-Daten der Akten, zum anderen die Zugriffsrechte der Nutzer auf die ZF-Daten der Zusatzfunktionen.

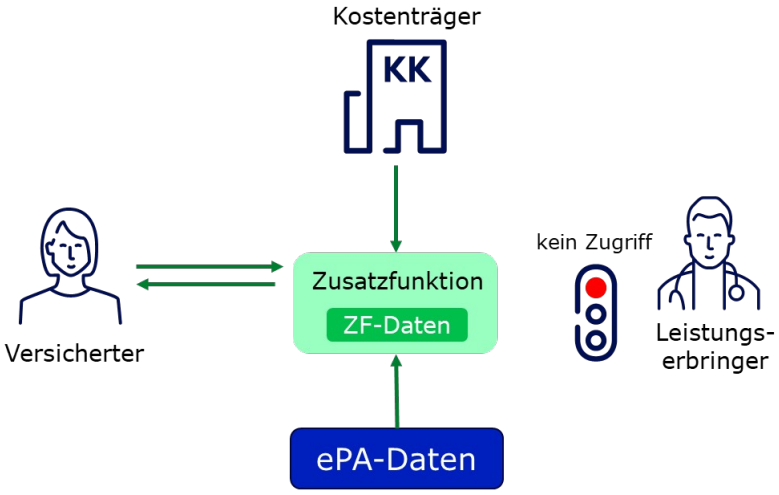


Abbildung 11 - Zugriffsmodel für backendseitige Zusatzfunktionen (Pfeile zeigen zulässigen Datenfluss)

Backendseitige Zusatzfunktionen können ausschließlich lesend auf die ePA-Daten der Akten zugreifen. Voraussetzung dafür ist eine Einwilligung des Versicherten in die Nutzung der Zusatzfunktion. Backendseitige Zusatzfunktionen können nicht in die ePA eines Versicherten schreiben oder ePA-Daten ändern bzw. löschen.

Versicherte können auf die Zusatzfunktionen und deren ZF-Daten zugreifen. Sie können abhängig von der Zusatzfunktion ZF-Daten lesen, ändern, löschen oder selbst Daten zur Verfügung stellen. Vertreter eines Versicherten können auf die Zusatzfunktionen und die ZF-Daten des Versicherten mittels ihres ePA-FdVs zugreifen, sofern das ePA-FdV des Vertreters die Nutzung der Zusatzfunktion ermöglicht.

Der Kostenträger als Anbieter einer Zusatzfunktion kann seinen Versicherten für diese Zusatzfunktion Daten zur Verfügung stellen, z.B. falls zusätzliche Daten aus dem eigenen Datenbestand für eine Zusatzfunktion nützlich sind.

Leistungserbinger und sonstige Nutzer haben keinen Zugriff auf die Zusatzfunktionen und deren ZF-Daten.

3.21.2 Zusatzfunktion-Manager für backendseitige Zusatzfunktionen

Der **Zusatzfunktion-Manager(ZF-Manager)** ermöglicht dem Hersteller die Entwicklung eines ePA-Aktensystems, in welchem backendseitige Zusatzfunktionen konfigurativ ohne Anpassung des ePA-Aktensystems hinzugefügt und entfernt werden können.

Der Zusatzfunktion-Manager (ZF-Manager)ist ein Service einer Aktenkontoverwaltungs-VAU und hat mehrere Aufgaben. Der ZF-Manager

1. setzt das Zugriffsmodell aus Abschnitt 3.21.1 durch,
2. startet und beendet Zusatzfunktionen für eine Akte basierend auf Zusatzfunktion-spezifischen**ZF-Policies** in einer **Zusatzfunktion-Service-VAU** für Zusatzfunktionen (vgl. ZF-Service-VAU in Abschnitt 3.4.4.1),
3. vermittelt die Kommunikation zwischen ZF-Client im ePA-FdV bzw. KTR-Client und der Zusatzfunktion in der ZF-Service-VAU durch einen**ZF-Proxy**,
4. bietet Zusatzfunktionen, die in einer ZF-Service-VAU laufen, eine Schnittstelle zum Zugriff auf ePA- und ZF-Daten (**Int Data Access**).

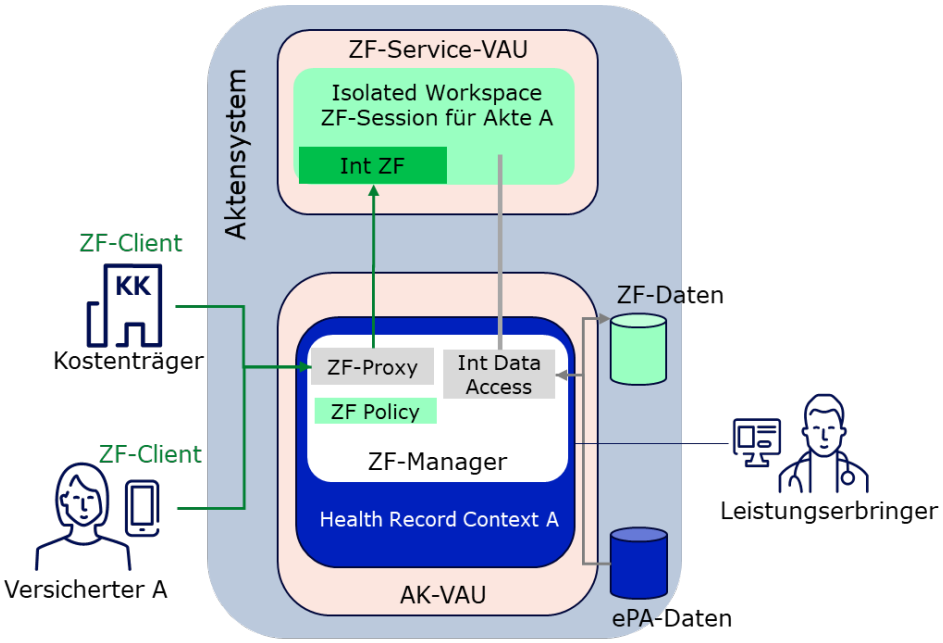


Abbildung 12 - Zusatzfunktion-Manager

*ZF-Proxy*und *Int Data Access* sind feste Bestandteile des Zusatzfuntion-Managers und unabhängig von einer speziellen Zusatzfunktion. Eine *ZF-Policy* ist spezifisch für eine Zusatzfunktion und wird dem Zusatzfunktion-Manager konfigurativ ergänzt bzw. von diesem entfernt.

A_30449 -Backendseitige Zusatzfunktionen - ZF-Manager in AK-VAU
Das ePA-Aktensystem MUSS den Zusatzfunktion-Manager in einer Aktenkontoverwaltungs-VAU umsetzen.**[<=]**

A_30450 -Backendseitige Zusatzfunktionen - Ausführung von Zusatzfunktionen ausschließlich in ZF-Service-VAUs
Das ePA-Aktensystem MUSS sicherstellen, dass backendseitige Zusatzfunktionen ausschließlich in einer Zusatzfunktion-Service-VAU ausgeführt werden.**[<=]**

Hinweis zu A_30450-*: Die Anforderungen an eine Zusatzfunktion-Service-VAU sind in Abschnitt 3.4.4.1 beschrieben.

1. Durchsetzen des Zugriffsmodells

A_30451 -Backendseitige Zusatzfunktionen - Ausschließlich Lesezugriff auf ePA-Daten
Der Zusatzfunktion-Manager MUSS sicherstellen, dass backendseitige Zusatzfunktionen ausschließlich lesend auf die ePA-Daten der Akten von Versicherten zugreifen können. **[<=]**

A_30452 -Backendseitige Zusatzfunktionen - Lesezugriff ausschließlich für Versicherte
Der Zusatzfunktion-Manager MUSS sicherstellen, dass ZF-Daten einer backendseitigen Zusatzfunktion ausschließlich an Nutzer in der Rolle "Versicherter" übermittelt werden können.**[<=]**

Hinweis zu A_30452-*: Dies impliziert insbesondere, dass weder Kostenträger noch Leistungserbringer auf ZF-Daten lesend zugreifen können. Vertreter besitzen ebenfalls die Rolle "Versicherter" und können prinzipiell auf die ZF-Daten des zu vertretenden Versicherten zugreifen, sofern das ePA-FdV des Vertreters dies ermöglicht. Die Anforderung umfasst alle ZF-Daten, die die backendseitige Zusatzfunktion verarbeitet,

insbesondere auch ggf. mit ePA-Daten des Versicherten trainierte Machine-Learning-Modelle.

A_30453 -Backendseitige Zusatzfunktionen - Schreib- und Löschzugriff ausschließlich für Versicherte oder Kostenträger
Der Zusatzfunktion-Manager MUSS sicherstellen, dass ausschließlich Nutzer in der Rolle "Versicherter" oder "Kostenträger" Daten an eine backendseitige Zusatzfunktion übermitteln oder ZF-Daten ändern bzw. löschen können.**[<=]**

A_30454 -Backendseitige Zusatzfunktionen - Schreibzugriff für Kostenträger ausschließlich für selbst angebotene ZF
Der Zusatzfunktion-Manager MUSS sicherstellen, dass Kostenträger ausschließlich auf Zusatzfunktionen zugreifen können, die der Kostenträger selbst anbietet.**[<=]**

2. Starten und Beenden von Zusatzfunktionen

Eine Zusatzfunktion, in die der Versicherte eingewilligt hat, kann im Aktensystem ausgeführt werden, wenn die Akte des Versicherten im Aktensystem durch einen befugten Nutzer geöffnet wurde (z.B. durch den Aktenkontoinhaber, einen Vertreter, seinen Kostenträger oder einen befugten Leistungserbringer).

Eine Zusatzfunktion kann direkt nach dem Öffnen der Akte gestartet werden oder aber auch erst aufgrund gewisser Ereignisse in der Akte (z.B. nach dem Einstellen von bestimmten Dokumenten bzw. Daten). Für jede Zusatzfunktion wird in einer zugehörigen ZF-Policy beschrieben, wann die Zusatzfunktion durch den ZF-Manager zu starten ist.

A_30455 -Backendseitige Zusatzfunktionen - ZF-Policies für Zusatzfunktionen
Der Hersteller des ePA-Aktensystems MUSS gewährleisten, dass für eine backendseitige Zusatzfunktion in einer ZF-Policy festgelegt werden kann, bei welchen Ereignissen in der Akte der ZF-Manager die Zusatzfunktion starten soll, insbesondere

- beim Start des Health Record Contexts und/oder
- beim Einstellen, Löschen oder Ändern von bestimmten Kategorien von ePA-Daten (z.B. das Einstellen von Impfeinträgen oder das Einstellen neuer Medikationsdaten) und/oder
- beim Aufruf einer Operation der Zusatzfunktion durch einen Client.

[<=]

A_30456 -Backendseitige Zusatzfunktionen - ZF-Policy enthält Namen der Zusatzfunktion
Der Hersteller des ePA-Aktensystems MUSS gewährleisten, dass in der ZF-Policy für eine backendseitige Zusatzfunktion ein für Versicherte verständlicher Zusatzfunktionsname definiert ist.**[<=]**

Hinweis zu A_30456-*: Der Zusatzfunktionsname in der ZF-Policy wird für die Protokolleinträge verwendet, die beim lesenden Zugriff der backendseitigen Zusatzfunktion auf die ePA-Daten vom ZF-Manager erzeugt wird.

A_30457 -Backendseitige Zusatzfunktionen - Konfiguration von ZF-Policies im ZF-Manager
Das ePA-Aktensystem MUSS es ermöglichen, ZF-Policies für Zusatzfunktionen konfigurativ am ZF-Manager zu ergänzen oder zu entfernen.**[<=]**

A_30458 -Backendseitige Zusatzfunktionen - Nur mit Einwilligung des Versicherten
Der Zusatzfunktion-Manager MUSS sicherstellen, dass eine backendseitige Zusatzfunktion nur dann für eine Akte gestartet wird und auf ePA-Daten eines Versicherten zugreifen kann, falls im Aktenkonto des Versicherten eine gültige Einwilligung für diese backendseitige Zusatzfunktion hinterlegt ist.**[<=]**

3. ZF-Proxy als Vermittler zwischen ZF-Client und backendseitiger Zusatzfunktion

Zusatzfunktionen bieten Clients zusatzfunktionsspezifische Schnittstellen für den Zugriff auf die ZF-Daten an, um bspw. die ZF-Daten einer Zusatzfunktion zu lesen. Clients bauen ausschließlich eine Verbindung zu einer AK-VAU auf. Um mit einer in einer ZF-Service-VAU laufenden Zusatzfunktion kommunizieren zu können, bietet der ZF-Manager daher eine Proxy-Funktionalität, um die Kommunikation zwischen einem Client und der Zusatzfunktion zu vermitteln.

A_30459 -Backendseitige Zusatzfunktionen - ZF-Proxy für Zusatzfunktionen im ZF-Manager
Der Zusatzfunktion-Manager MUSS einen ZF-Proxy zur Verfügung stellen, der die Kommunikation zwischen einem Client und der backendseitigen Zusatzfunktion, die in einer ZF-Service-VAU läuft, vermittelt.**[<=]**

4. Datenzugriff auf ePA-Daten und ZF-Daten

A_30460 -Backendseitige Zusatzfunktionen - Datenzugriff auf ePA-Daten und ZF-Daten ausschließlich über ZF-Manager
Das ePA-Aktensystem MUSS sicherstellen, dass backendseitige Zusatzfunktionen, die in einer ZF-Service-VAU ausgeführt werden, ausschließlich über den ZF-Manager auf ePA-Daten und ZF-Daten zugreifen können.**[<=]**

A_30461 -Backendseitige Zusatzfunktionen - ZF-Manager bietet Schnittstelle für Datenzugriff
Der Zusatzfunktion-Manager MUSS backendseitigen Zusatzfuntkionen, die in einer ZF-Service-VAU ausgeführt werden, eine Schnittstelle zum Suchen und Lesen von ePA-Daten sowie zum Suchen, Lesen, Schreiben, Ändern und Löschen von ZF-Daten bereitstellen. **[<=]**

Hinweis zu A_30461-*: Diese Schnittstelle für den Datenzugriff kann analog zur MHD-Schnittstelle realisiert werden.

A_30462 -Backendseitige Zusatzfunktionen - Protokollierung der Lesezugriffe auf ePA-Daten
Der Zusatzfunktion-Manager MUSS sicherstellen, dass Lesezugriffe einer backendseitigen Zusatzfunktion auf ePA-Daten im Audit Event Service für den Versicherten protokolliert werden, wobei als auslösender Akteur der in der ZF-Policy festgelegte Zusatzfunktionsname verwendet wird.**[<=]**

A_30463 -Backendseitige Zusatzfunktionen - Getrenntes Speichern von ePA-Daten und ZF-Daten
Der Zusatzfunktion-Manager MUSS sicherstellen, dass eine backendseitige Zusatzfunktion ihre ZF-Daten ausschließlich in einem Bereich des Aktenkontos des Versicherten speichert, der von den gespeicherten ePA-Daten getrennt ist, so dass durch eine Speicherung oder Löschung der ZF-Daten die Integrität und Verfügbarkeit der ePA-Daten nicht beeinträchtigt werden kann.**[<=]**

A_30464 -Backendseitige Zusatzfunktionen - Verschlüsselung der ZF-Daten mit SecureDataStorageKey des Versicherten
Falls ZF-Daten einer backendseitigen Zusatzfunktion im Aktensystem persistiert werden sollen, MUSS der Zusatzfunktion-Manager sicherstellen, dass die ZF-Daten mit dem SecureDataStorageKey (Datenpersistierungsschlüssel) des Versicherten verschlüsselt persisitiert werden.**[<=]**

A_30465 -Backendseitige Zusatzfunktionen - Chiffrate der ZF-Daten sind der Zusatzfunktion zuordenbar

Falls ZF-Daten einer backendseitigen Zusatzfunktion im ePA-Aktensystem persistiert werden, MUSS das ePA-Aktensystem ohne Öffnen eines Health Record Contetxts identifizieren können, zu welcher backendseitigen Zusatzfunktion die Chiffrate gehören.**[<=]**

A_30468 -Backendseitige Zusatzfunktionen - Keine Profilbildung über versichertenspezifische Nutzung von Zusatzfunktionen
Das ePA-Aktensystem MUSS sicherstellen, dass außerhalb der VAU nicht erkannt werden kann, welche Versicherten welche Zusatzfunktionen nutzen.**[<=]**

A_30469 -Backendseitige Zusatzfunktionen - Löschen der ZF-Daten bei Widerruf der Einwilligung
Das ePA-Aktensystem MUSS sicherstellen, dass alle ZF-Daten einer backendseitigen Zusatzfunktion aus der Akte eines Versicherten unverzüglich gelöscht werden, wenn der Versicherte seine Einwilligung für die backendseitige Zusatzfunktion widerruft.**[<=]**

A_30470 -Backendseitige Zusatzfunktionen - Löschen der ZF-Daten bei Widerspruch oder Löschen der ePA
Das ePA-Aktensystem MUSS sicherstellen, dass alle ZF-Daten einer backendseitigen Zusatzfunktion bei Löschung des Aktenkontos aufgrund eines Widerspruchs zur ePA oder einer Löschung des Aktenkontos aus sonstigen Gründen ebenfalls gelöscht werden.**[<=]**

A_30471 -Backendseitige Zusatzfunktionen - Löschen von ZF-Daten zu entfernten Zusatzfuntkionen
Falls eine backendseitige Zusatzfunktion aus dem ePA-Aktensystem entfernt wird, MUSS das ePA-Aktensystem sicherstellen, dass alle ZF-Daten zu dieser Zusatzfunktion aus den Aktenkonten der Versicherten gelöscht werden.**[<=]**

3.22 Schnittstellen (OpenAPI)

Hinweis: Die Vorgaben in den beschreibenden Dateien der REST-Schnittstellen (yaml) sind normativ für den Anbieter der Schnittstellen. Die Anforderungen im vorliegenden Dokument ergänzen diese Vorgaben, insbesondere, wenn diese für sicherheitstechnische Gutachten erforderlich sind.

3.22.1 Übersicht der Schnittstellen des Aktensystems

Tabelle 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 und der Ombudsstelle die Änderung des Zustand des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA für eine Funktion.
`getConsentDecisions`	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen aller Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der ePA.
`getConsentDecision`	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen eines Widerspruchs einer Funktion gegen die Nutzung von widerspruchsfähigen Funktionen.
`updateDataUsagePurposes`	Diese Operation erlaubt dem FdV und der Ombudsstelle die Änderung der Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden.
`getDataUsagePurposes`	Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht der aktuellen Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden bzw. wurden.
`getUserSpecificMedicationDenyList`	Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht, welche LEI keinen Zugriff auf den Medication Service haben.
`setUserSpecificMedicationDeny`	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI in die Liste der LEIs aufzunehmen, die keinen Zugriff auf den Medication Service haben.
`getUserSpecificMedicationDeny`	Diese Operation erlaubt dem FdV und der Ombudsstelle eine bestimmte LEI aus der Liste der LEIs anzuzeigen, die keinen Zugriff auf den Medication Service haben.

deleteUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI aus der Liste der LEIs zu entfernen, damit diese LEI wieder Zugriff auf den Medication Service haben kann.
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 aus.
setPolicyAssignment	Diese Operation fügt der General Deny Policy einen neuen Eintrag hinzu.
deletePolicyAssignment	Diese Operation löscht einen bestimmten Eintrag der General Deny Policy.
I_Constraint_Management	
Schnittstelle des Constraint Managements gemäß [I_Constraint_Management]	
getDenyPolicyAssignments	Diese Operation gibt eine Liste aller konfigurierten Einträge der General Deny Policy aus.
setPolicyAssignment	Diese Operation fügt der General Deny Policy einen neuen Eintrag hinzu.
deletePolicyAssignment	Diese Operation löscht einen bestimmten Eintrag der General Deny Policy.
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 (VSDM Prüfnachweis).
setEntitlementPsV2	Diese Operation fügt eine Befugnis für eine Leistungserbringerinstitution in einer Behandlungssituation hinzu (PoPP).

`getEntitlements`	Diese Operation erlaubt dem FdV den Abruf aller aktuellen Befugnisse.
`getEntitlement`	Diese Operation erlaubt dem FdV den Abruf einer bestimmten Befugnis.
`setEntitlement`	Diese Operation erlaubt dem FdV das Setzen einer Befugnis für einen Nutzer.
`deleteEntitlement`	Diese Operation erlaubt dem FdV den Abruf das Löschen einer existierenden Befugnis.
`getBlockedUserPolicyAssignments`	Diese Operation erlaubt dem FdV den Abruf der aktuell vorhandenen Befugnisausschlüsse.
`setBlockedUserPolicyAssignment`	Diese Operation erlaubt dem FdV den Befugnisausschluss für einen Nutzer.
`getBlockedUserPolicyAssignment`	Diese Operation erlaubt dem FdV den Abruf eines bestimmten Befugnisausschlusses.
`deleteBlockedUserPolicyAssignment`	Diese Operation erlaubt dem FdV die Aufhebung eines Befugnisausschlusses.
I_Entitlement_Management_EU	
Schnittstelle des Entitlement Management EU-Zugriff gemäß [I_Entitlement_Management_EU] zur Verwaltung Befugnis EU-Zugriff	
`setEntitlementEu`	Diese Operation erlaubt dem FdV das Setzen einer Befugnis EU-Zugriff für einen Versicherten.
`getAccessCode`	Diese Operation erlaubt dem FdV den Abruf des Zugriffscodes für die Befugnis EU-Zugriff.
Render API: PDF Audit	
Schnittstelle des Audit Event Service gemäß [gemIG_ePA_Basic] zum Abruf der Protokolldaten in lesbarer Form	
`renderAuditEventsToPDF`	Diese Operation erlaubt FdV und Ombudsstelle den Abruf der Protokolldaten als PDF.

Query API: AuditEvent	
Schnittstelle des Audit Event Service gemäß [gemIG_ePA_Basic] zum Abruf der Protokolldaten im FHIR-Format	
`listAuditEvents_AuditEventSvc`	Diese Operation ermöglicht die Suche nach AuditEvent Instanzen.
`getAuditEventById_AuditEventSvc`	Diese Operation ermöglicht das Lesen einer AuditEvent Instanz.
I_Account_Management	
Schnittstelle zur Verwaltung von Aktenkonten, Aktenkontoumzug und Aktenzusammenführung	
`getAccountState`	Diese Operation gibt Kostenträgersystemen Auskunft über den internen Status eines Aktenkontos
`createAccount`	Diese Operation erstellt eine neues Aktenkonto mit einer Akte oder einem Widerspruch
`deleteAccount`	Diese Operation löscht ein Aktenkonto
`setObjection`	Diese Operation setzt den Widerspruch für ein Aktenkonto und löscht die enthaltene Akte
`setRecord`	Diese Operation erstellt eine Akte in einem Aktenkonto und löscht den enthaltenen Widerspruch
`mergeRecord`	Diese Operation führt die Akten aus zwei Aktenkonten des Versicherten zusammen
`doesKvnrExist`	Diese Operation prüft auf Vorhandensein eines Aktenkontos zu einer Kvnr bei einem Aktensystem
`transferStartRelocation`	Diese Operation startet den Umzug eines Aktenkontos zu einem neuen Anbieter
`transferStartMerge`	Diese Operation startet die Zusammenführung von Akten
`getContent`	Diese Operation überträgt das Exportpaket für eine Aktenkontoumzug

	oder eine Aktenzusammenführung

transferComplete	Diese Operation bestätigt den erfolgreichen Abschluss eines Aktenkontoumzugs oder einer Aktenzusammenführung
transferAbort	Diese Operation bricht einen Aktenkontoumzug oder eine Aktenzusammenführung ab
I_Device_Management_Insurant	
Schnittstelle zur Geräteverwaltung aus der Umgebung des Versicherten (Device Management)	
getDevice	Diese Operation ruft eine bestimmte Geräteregistrierung ab.
getDevices	Diese Operation ruft alle Geräteregistrierungen ab.
updateDevice	Diese Operation ändert den Displayname einer Geräteregistrierung.
deleteDevice	Diese Operation löscht eine bestimmte Geräteregistrierung.
registerDevice	Diese Operation erzeugt eine neue Geräteregistrierung und neue Geräteparameter
confirmPendingDevice	Diese Operation bestätigt eine neue Geräteregistrierung mit einem Geräteregistrierungscode
getDeviceAttestation	Diese Operation ruft die Bestätigung einer Geräteregistrierung am Home-AS ab.
optional: Schnittstelle zur Verbesserung der Nutzbarkeit eines ePA FdV (Snippet Mangement)	
getSnippets	Diese Operation liefert die Liste aller für das Aktenkonto gespeicherten Artefakte.
getSnippet	Diese Operation liefert ein bestimmtes Artefakt des Aktenkontos.
putSnippet	Diese Operation speichert ein Artefakt für das Aktenkonto.
deleteSnippet	Diese Operation löscht ein bestimmtes

	Artefakt für das Aktenkonto.

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
`getFreshnessParameter`	Diese Operation erzeugt einen Frischeparameter für die Authentisierung mittels Bearer Token
`sendAuthorizationRequestBearerToken`	Diese Operation initiert 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	
I_Email_Management	

getEmailAddress	Diese Operation ruft die hinterlegte E-Mail-Adresse des Versicherten ab.
replaceEmailAddress	Diese Operation setzt oder ändert die E-Mail Adresse für einen Versicherten ab.
I_Tool_Convert_PDF_Insurant	
Schnittstelle des XDS Document Managements gemäß [I_Tool_Convert_PDF_Insurant]	
convertPDF	Diese Operation konvertiert ein PDF in ein PDF/A Format
I_Data_Submission_Service	
Schnittstelle des Data Submission Service gemäß [I_Data_Submission_Service]	
getSubmissionPackage	Diese Operation stellt dem FDZ ein Datenpaket für eine bestimmte SubmissionID bereit.
I_Push_Notification_Management_Insurant	
Schnittstelle des Push Notification Managements gemäß [I_Push_Notification_Management]	
getPushers	Diese Operation gibt alle Pusher Registrierungen eines Aktenkontos aus
updatePusher	Diese Operation setzt, aktualisiert oder löscht eine Pusher Registrierung
getChannelsOfPusher	Diese Operation gibt die aktuelle Konfiuration der Push Notification Channels für einen Pusher aus
updateChannelsOfPusher	Diese Operation aktualisiert die Auswahl der Push Notification Channels für einen Pusher
getChannels	Diese Operation gibt die möglichen Push Notification Channels der ePA aus
I_Ehr_Information_Service	
Schnittstelle des Informationsdienstes in der VAU [I_Ehr_Information_Service]	

`getConsentDecisionInformationV2`	Diese Operation liest den aktuellen Zustand der Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der Funktionsklasse "Versorgungsprozess" aus.
`setUserExperienceResultV2`	Die Operation dient der Sammlung von Client Performancedaten aus der Umgebung der Leistungserbringer.
`getRecordStatusV2`	Diese Operation fragt die Existenz eines bestimmten Aktenkontos bei einem Betreiber an.

7338

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 oder einer Aktenkontozusammenführung	
`getGeneralConsentDecision`	Diese Operation dient der Abfrage eines Widerspruchs gegen die Nutzung der ePA bei einem anderen Aktensystemanbieter.
`getProviderList`	Diese Operation gibt eine Liste von FQDNs der Versicherungen / ePA-Anbieter aus

7339 Die Schnittstellen (REST) und Operationen sind funktional in den Beschreibungen der
7340 jeweiligen Schnittstelle beschrieben. Darüber hinaus gelten die folgenden übergreifenden
7341 Anforderungen.

3.22.2 Übergreifende Festlegungen zu den Schnittstellen

A_23918 -Schnittstellen (OpenApi) - Prüfung der Befugnis
Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) eine vorhandene und gültige Befugnis (entitlement) für den Nutzer der Operation fordern und diese nicht vorliegt.**[<=]**

Hinweis: A_23918 deckt auch die Fehlersituationen "kein VAU-Kanal" und "keine User Session" ab, da diese eine Vorbedingung für den Nachweis einer gültigen Befugnis sind.

A_24365 -Schnittstellen (OpenApi) - Prüfung des Aktenkontos
Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) die Existenz des adressierten Aktenkontos fordern und diese nicht für den Operationsaufruf verwendet wird.**[<=]**

Hinweis A_24365 deckt auch die Fehlersituation "kein Health Record Context" ab, da dieses nur infolge eines nicht vorhandenen Aktenkontos auftritt.

A_24538 -Schnittstellen (OpenApi) - Prüfung des Aktenkontostatus
Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) einen vorgegebenen Status des Aktenkontos fordern und dieser nicht vorhanden ist.**[<=]**

A_24366 -Schnittstellen (OpenApi) - Prüfung der Rolle
Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) die Zulässigkeit der Operation auf bestimmte Rollen (professionOID) einschränken und der Nutzer der Operation diese nicht nachweist.**[<=]**

A_24367 -Schnittstellen(OpenApi) - Prüfung des Identifiers
Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) die Zulässigkeit der Operation auf bestimmte Identifier (KVNR oder Telematik-ID) einschränken und der Nutzer der Operation diese nicht nachweist.**[<=]**

A_24580 -Schnittstellen (OpenApi) - Protokollierung der Operationen
Das ePA-Aktensystem MUSS nach der Ausführung der Operationen der REST-Schnittstellen 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
AN	Arbeitsnummer in der Übermittlung von Daten zur Sekundärnutzung
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BGP	Border Gateway Protokoll
BPPC	Basic Patient Privacy Consents
CRUD	Create Read Update Delete
DiGA	Digitale Gesundheitsanwendung
ePA-FdV	ePA-Frontend des Versicherten
ePA-FdV AdV	ePA-Frontend des Versicherten im KTR-AdV-Terminal
FDZ	Forschungsdatenzentrum Gesundheit
HL7	Health Level Seven
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IHE ITI TF	IHE IT Infrastructure Technical Framework
JWT	JSON-Web-Token
JWS	signiertes JSON-Web-Token

KTR	Kostenträger
LP	Lieferpseudonym in der Übermittlung von Daten zur Sekundärnutzung
MIO	Medizinisches Informationsobjekt
MHD	Mobile access to Health Documents (FHIR-Service im Aktensystem u.a. für Volltextsuche)
MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
PDSG	Patientendaten-Schutz-Gesetz
PHR	Personal Health Record
SAML	Security Assertion Markup Language
TLS	Transport Layer Security
UUID	Universally Unique Identifier
VAU	Vertrauenswürdige Ausführungsumgebung
VST	Vertrauensstelle Elektronische Patientenakte für Datenausleitung an das FDZ
W3C	World Wide Web Consortium
WS-I	Web-Services Interoperability Consortium
XCA	Cross-Community Access Profile
XDS	Cross-Enterprise Document Sharing Profile
XDW	Cross-Enterprise Document Workflow Profile
XOP	XML-binary Optimized Packaging
XSPA	Cross-Enterprise Security and Privacy Authorization Profile

5.2 Glossar

Begriff	Erläuterung

Authenticator-Modul	Das Authenticator-Modul ist die Client-Komponente zum sektoralen Identity Provider. Über die das Authenticator-Modul authentifiziert sich der Versicherte gegenüber des sektoralen IDP. Das Authenticator-Modul kann in ein App (z.B. Service-App einer Krankenkasse oder ePA-FdV) integriert oder als eigenständige App implementiert werden (siehe auch [gemSpec_IDP_Sek].

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

5.3 Abbildungsverzeichnis

Abbildung 1 : Ablauf der Anlage eines Aktenkontos....30
Abbildung 2: Alternativen zur Ausführung des Befugnisverifikations-Moduls....54
Abbildung 3 - Typen von VAU-Schnittstellen....77
Abbildung 4: Überblick Service-VAUs....86
Abbildung 5: Einfrieren von Daten durch eine AK-VAU....90
Abbildung 6: Einfrieren von Daten durch eine Service-VAU....91
Abbildung 7: Auftauen von eingefrorenen Daten....93
Abbildung 8: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP....205
Abbildung 9: Ablauf der Authentifizierung einer LEI über den Smartcard IDP....209
Abbildung 10: Ablauf der Authentisierung über JWT Bearer Token am Beispiel eRP-FD..210
Abbildung 11 - Zugriffsmodel für backendseitige Zusatzfunktionen (Pfeile zeigen zulässigen Datenfluss)....231
Abbildung 12 - Zusatzfunktion-Manager....232

5.4 Tabellenverzeichnis

Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat....18
Tabelle 2 : Inhalte des JWT der Befugnisse im Exportpaket....34
Tabelle 3: Zustandswechsel im Lebenszyklus einer Akte....37
Tabelle 4: Tab_AS_VAU_Token_Modul_Rules-07 -Prüfregeln VAU Token....55
Tabelle 5: Überblick über die Regeln des Befugnisverifikations-Moduls....61
Tabelle 6: Tab_AS_Entitlement_Registration_Rules-07 - Regeln zur Registrierung von Befugnissen....63
Tabelle 7: Tab_AS_SDS-Key_Rules Key Rules-07 - Regeln zur Ableitung der versichertenindividuellen Persistierungsschlüssel....70
Tabelle 8: Widerspruchsfähige Funktionen der elektronischen Patientenakte....98
Tabelle 9: Nutzergruppen der User Specific Deny Policy Medication....102

Tabelle 10: Inhalt einer Befugnis....103
Tabelle 11: Befugnisse für berechtigte Nutzergruppen und Nutzer....105
Tabelle 12: Befugnisse EU-Zugriff für berechtigte Nutzergruppen und Nutzer....107
Tabelle 13 : JWT zur Befugnisvergabe mit den Mindest-Inhalten....110
Tabelle 14 : JWT zur Befugnisvergabe mit Mindest-Inhalten....112
Tabelle 15: Inhalt eines Blocked User Policy Eintrags....116
Tabelle 16: Legal Policy....122
Tabelle 17: Legal Policy - EU-Zugriff....125
Tabelle 18: Beschreibung der Kategorien und Services....127
Tabelle 19: Inhalt eines General Deny Policy Eintrags....132
Tabelle 20: Verbergen eines Medical Service....133
Tabelle 21: Kennzeichnung von Optionalitäten....146
Tabelle 22: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen des XDS Document Service....147
Tabelle 23 : Liste mit Dokumententypen, die ersetzt werden können....155
Tabelle 24 : Liste mit Ordnern, in denen Dokumente ersetzt werden dürfen....155
Tabelle 25 : Fehlertexte zu StatusMismatch-Fehlercode....161
Tabelle 26: Schnittstelle I_Document_Management....164
Tabelle 27: Schnittstelle I_Document_Management_Insurant....166
Tabelle 28: Festlegung Folder.entryUUIDzu statischen Ordnern....169
Tabelle 29: Nutzungsvorgaben für Metadatenattribute XDS....171
Tabelle 30: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language Codes....186
Tabelle 31: Einsortierung_Datenkategorien....191
Tabelle 32: TAB_EPA_Sammlungstypen....195
Tabelle 33: Auswirkungen bei Widerspruch gegen eine Funktion der ePA....198
Tabelle 34 : Inhalte des übermittelten JWT der Client Attestierung....209
Tabelle 35 : JWT Bearer Token mit den Mindest-Inhalten....211
Tabelle 36 : JWT Bearer Token FDZ mit den Mindest-Inhalten....211
Tabelle 37 : JWT Bearer Token eines Kostenträgers mit den Mindestinhalten....212
Tabelle 38: Auswahl der zu übertragenden FHIR-Ressourcen....221
Tabelle 39: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen....222
Tabelle 40: Ereignisse und deren Push Nachrichten....227
Tabelle 41: Übersicht der Schnittstellen des Aktensystems....236

5.5 Referenzierte Dokumente

5.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemKPT_ePAfuerAlle]	gematik: Grobkonzept der "ePA für alle"
[gemSpec_FdV_ePA]	gematik: Spezifikation ePA-Frontend des Versicherten
[gemSpec_IDP_Sek]	gematik: Spezifikation des sektoralen IDP (GesundheitsID)
[gemSpec_IDP_FD]	gematik: Spezifikation der Fachdienste der TI-Föderation
[gemSpec_IDP_Frontend]	gematik: Spezifikation der Frontendkomponenten für Fachdienste der TI-Föderation
[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform
[gemSpec_IG_ePA]	gematik: Implementation Guides für strukturierte Dokumente GitHub: siehe [ePA_XDS_Document] Path: src/implementation_guides
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory
[ePA_Basic]	gematik: GitHub Repository "ePA-Basic" https://github.com/gematik/ePA-Basic
[I_Account_Management]	gematik: I_Account_Management REST-Schnittstelle zum Management von Aktenkonten siehe [ePA_Basic] Path: src/openapi/I_Account_Management.yaml
[I_Consent_Decision_Management]	gematik: I_Consent_Decision_Management REST-Schnittstelle zum Management der Widersprüche zu Versorgungsprozessen

	siehe [ePA_Basic] Path: src/openapi/I_Consent_Decision_Management.yaml
[I_Entitlement_Management]	gematik: I_Entitlement_Management REST-Schnittstelle zur Verwaltung von Befugnissen und Befugnisausschlüssen siehe [ePA_Basic] Path: src/openapi/I_Entitlement_Management.yaml
[I_Entitlement_Management_EU]	gematik: I_Entitlement_Management_EU REST-Schnittstelle zur Verwaltung von Befugnissen EU-Zugriff siehe [ePA_Basic] Path: src/openapi/I_Entitlement_Management_EU.yaml
[I_Device_Management_Insurant]	gematik: I_Device_Management_Insurant.yaml REST-Schnittstelle zur Geräteverwaltung siehe [ePA_Basic] Path: src/openapi/I_Device_Management_Insurant.yaml
[I_Health_Record_Relocation_Service]	gematik: I_Health_Record_Relocation_Service REST-Schnittstelle zum Aktenumzug siehe [ePA_Basic] Path: src/openapi/I_Health_Record_Relocation_Service.yaml
[I_Information_Service_Accounts]	Schnittstellenspezifikation Information Service für Betreiber siehe [ePA_Basic] Path: src/openapi/I_Information_Service_Accounts.yaml
[I_Information_Service]	Schnittstellenspezifikation Information Service siehe [ePA_Basic] Path: src/openapi/I_Information_Service.yaml
[I_Ehr_Information_Service]	Schnittstellenspezifikation EHR Information Service siehe [ePA_Basic] Path: src/openapi/I_Ehr_Information_Service.yaml
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung und impliziten Geräteregistrierung siehe [ePA_Basic] Path: src/openapi/I_Authorization_Service.yaml
[I_Email_Management]	gematik: I_Email_Management REST-Schnittstelle zum Management von E-Mail-Adressen eines Versicherten siehe [ePA_Basic]

	Path: src/openapi/I_Email_Management.yaml
[ePA_XDS_Document]	gematik: GitHub Repository "ePA-xds-document" https://github.com/gematik/ePA-XDS-Document
[I_Constraint_Management_Insurant]	gematik: I_Constraint_Management_Insurant.yaml (deprecated) REST-Schnittstelle zum Verbergen und Sichtbarmachen von Dokumenten siehe [ePA_XDS_Document] Path: src/openapi/I_Constraint_Management_Insurant.yaml
[I_Constraint_Management]	gematik: I_Constraint_Management.yaml REST-Schnittstelle zum Verbergen und Sichtbarmachen von Dokumenten siehe [ePA_XDS_Document] Path: src/openapi/I_Constraint_Management.yaml
[I_Tool_Comvert_PDF_Insurant]	gematik: I_Tool_Convert_PDF_Insurant Schnittstelle für die PDF Formatkonvertierung siehe [ePA_XDS_Document] Path: src/openapi/ I_Tool_Convert_PDF_Insurant.yaml
[XDSDocumentService]	gematik: XDSDocumentService.wsdl IHE-Schnittstelle des XDSDocumentService siehe [ePA_XDS_Document] Path: src/schema
[Exportpaket]	gematik: HealthRecordExportPackage.adoc Aktenkontoverwaltung - Exportpaket für Daten der Akte siehe [ePA_Basic] Path: src/docs/HealthRecordExportPackage.adoc
[gemIG_ePA_Basic]	gematik: FHIR Implementation Guide "ePA Basisfunktionalitäten" https://gematik.de/fhir/epa/ImplementationGuide/de.gematik.epa
[gemIG_ePA_Medication]	gematik: FHIR Implementation Guide "ePA Medication Service" https://gematik.de/fhir/epa-medication/ImplementationGuide/de.gematik.epa.medication
[gemIG_ePA_MHD]	gematik: FHIR Implementation Guide "ePA MHD Service" https://gematik.de/fhir/epa-mhd/ImplementationGuide/de.gematik.epa.mhd
[gemIG_TI_Terminology]	gematik: Implementation Guide "TITerminology"

	https://gemspec.gematik.de/ig/fhir/terminology/
[DataPseudonymization]	gematik: epa-research Vorgaben zur Pseudonymisierung von Daten zur Sekundärnutzung GitHub: https://github.com/gematik/epa-research Path: docs/leitfaden_pseudonymisierung.md
[I_Data_Submission_Service]	gematik: I_Data_Submission_Service Schnittstelle für den Abruf eines Datenpaketes FDZ siehe [ePA_Basic] Path: src/openapi/ I_Data_Submission_Service.yaml
[I_Push_Notification_Management]	gematik: I_Push_Notification_Management_Insurant REST-Schnittstelle zum Management des Benachrichtigungsdienstes der ePA siehe [ePA_Basic] Path: src/openapi/I_Push_Notification_Management_Insurant.yaml
[gemF_PushNotification]	gematik: Anwendungsübergreifende Push Notification
[PushNotificationConcept]	gematik: Push Notification Concept Repository mit Artefakten und Vorgaben für anwendungsübergreifende Push Notification GitHub: https://gematik.github.io/gem-push-notifications-concept/
[I_Push_Gateway]	gematik: Push Gateway API REST-Schnittstelle des Push Gateways zum Versand von Push Nachrichten GitHub: https://gematik.github.io/gem-push-notifications-concept Tab: Push_Gateway_OpenAPI
[Schema_PushNotifications]	gematik: PushNotificationSchema Strukturvorgaben für Nachrichteninhalte des Push Notification Managements siehe [ePA_Basic] Path: src/schema/PushNotificationSchema.yaml

7449 ### 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-TF1]	IHE International (2025): 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 20.2, https://profiles.ihe.net/ITI/TF/Volume1/
[IHE-ITI-TF2]	IHE International (2025): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.2, https://profiles.ihe.net/ITI/TF/Volume2/
[IHE-ITI-TF3]	IHE International (2025): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Document Sharing Metadata and Content Profiles, Revision 20.2, https://profiles.ihe.net/ITI/TF/Volume3/
[RL_KVNR]	Richtlinien zum Aufbau und zur Vergabe einer Krankenversichertennummer (KVNR) und Regelungen des Krankenversichertennummernverzeichnis nach § 290 SGB V einschließlich der dazugehörigen Anlagen https://www.gkv-datenaustausch.de/kvnr/kvnr.jsp
[I_VST]	Vertrauensstelle ePA – Pseudonymisierungskonzept Datenausleitung ePA zu Forschungszwecken Version 2.2 (13.06.2025), Herausgeber: Robert Koch-Institut, Nordufer 20,13353 Berlin
[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
[RFC3339]	IETF (2002): Date and Time on the Internat: Timestamps, RFC 3339, https://datatracker.ietf.org/doc/html/rfc3339
[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/

7450