

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Aktensystem ePA für alle

Version:	2.0.0 CC
Revision:	1756706
Stand:	15.10.2026
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_Aktensystem_ePAfueralle

26

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	24
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	44
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	45
3.1.8.1.4 Vereinfachte Auswahl eines Datenbestands (Fallback-Lösung)	48
3.2 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM	49
3.3 Befugnisverifikations-Modul	54

74	3.3.1 VAU-Token-Modul	55
75	3.3.2 Regeln des Befugnisverifikations-Moduls	65
76	3.4 Vertrauenswürdige Ausführungsumgebung (VAU)	85
77	3.4.1 Übergreifende VAU-Anforderungen	88
78	3.4.1.1 Schutz der Integrität der VAU	88
79	3.4.1.2 Schutz der Daten bei Verarbeitung in der VAU	89
80	3.4.1.3 Schutz der Daten bei Speicherung außerhalb der VAU.....	89
81	3.4.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM.....	90
82	3.4.1.5 Logging und Monitoring.....	90
83	3.4.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU.....	91
84	3.4.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU...91	
85	3.4.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-VAU.....	93
86	3.4.2.3 Konsistenz des Systemzustands	93
88	3.4.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU.....	94
89	3.4.4 Zusätzliche Anforderungen an eine Service-VAU	94
90	3.4.4.1 Zusätzliche Anforderungen an eine Zusatzfunktion-Service-VAU.....	97
91	3.4.4.2 Kommunikation zwischen AK-VAU und Service-VAU.....	97
92	3.4.5 Temporäres Speichern von Daten und spätere Aufnahme ins Aktenkonto	97
93	3.5 Umschlüsselung	103
94	3.6 User Session und Health Record Context.....	104
95	3.7 Consent Decision Management.....	105
96	3.7.1 Widersprüche für Funktionen der ePA	105
97	3.7.2 Einschränkung der Verwendung von Daten auf bestimmte	
98	Sekundärnutzungszwecke	108
99	3.7.3 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny	
100	Policy Medication).....	109
101	3.8 Entitlement Management.....	111
102	3.8.1 Initiale Befugnisse (static Entitlements)	117
103	3.8.2 Erstellen einer Befugnis durch Clients	119
104	3.8.2.1 Befugnisvergabe durch ein ePA-FdV.....	119
105	3.8.2.2 Befugnisvergabe durch ein Primärsystem	121
106	3.8.3 Löschen von Befugnissen	123
107	3.8.4 Befugnisausschluss (Blocked User Policy).....	124
108	3.8.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)	126
109	3.8.6 EntitlementDenyList	128
110	3.9 Legal Policy	131
111	3.10 Constraint Management.....	139
112	3.10.1 Aktenkontoweites Verbergen (General Deny Policy)	141
113	3.10.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes	
114		144
115	3.11 Device Management	144
116	3.12 Medical Services	148
117	3.12.1 XDS Document Service	148
118	3.12.1.1 Formatprüfung beim Einstellen von Dokumenten	149
119	3.12.1.2 Anforderungen zur Validierung	152
120	3.12.1.3 Namensräume.....	153
121	3.12.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von	
122	Dokumenten	154
123	3.12.1.4.1 Anforderungen an IHE ITI-Akteure.....	154

124	3.12.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen	156
125	3.12.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen ...	158
126	3.12.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen	170
127	3.12.1.5 Fehlerbehandlung in Schnittstellenoperationen	171
128	3.12.1.6 Schnittstellen im XDS Document Service	173
129	3.12.1.6.1 Schnittstelle I_Document_Management	174
130	3.12.1.6.2 Schnittstelle I_Document_Management_Insurant	177
131	3.12.1.7 Statische Metadaten	179
132	3.12.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten	181
133	3.12.1.8.1 Allgemeine Metadatenvorgaben	181
134	3.12.1.8.2 Metadaten der Dokumente und SubmissionSets	201
135	3.12.1.8.3 Metadaten für Datenkategorien	205
136	3.12.1.8.4 Automatisches Umschreiben von Daten	207
137	3.12.1.9 Strukturierte Dokumente	208
138	3.12.1.9.1 Sammlungstypen	209
139	3.12.1.9.2 Konfigurierbarkeit	211
140	3.12.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode	212
141	3.12.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die	212
142	Dokumente des Aktenkontos	212
143	3.12.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication	213
144	Service durch eine spezifische LEI auf die Dokumente des Aktenkontos	213
145	3.12.1.13 Protokollierung von Zugriffen auf den XDS Document Service	214
146	3.12.1.14 Unterstützungsleistung für das ePA-FdV	214
147	3.12.2 FHIR Data Services	215
148		
149	3.13 Audit Event Service	215
150	3.14 Information Services	215
151	3.14.1 Information Service	215
152	3.14.1.1 Informationen zu Widersprüchen (Consent Decisions)	216
153	3.14.1.2 Informationen zur Anwenderperformance (UX Performance)	216
154	3.14.2 Information Service - Account	216
155	3.14.3 EHR Information Service	217
156	3.15 Email Management	217
157	3.16 Zusätzliche Anforderungen an den Authorization Service	219
158	3.16.1 Anforderungen an den Authorization Service für die Authentisierung von	219
159	Versicherten (FdV)	219
160	3.16.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B	224
161		
162	3.16.3 Anforderungen an den Authorization Service für die Authentisierung über JWT	225
163	Bearer Token	
164	3.17 Anbindung Verzeichnisdienst FHIR-Directory	229
165	3.18 Access Gateway	229
166	3.18.1 Paketfilter	229
167	3.18.1.1 Funktion	229
168	3.18.1.2 Redundanz	230
169	3.18.1.3 Konfiguration	231

170	3.18.1.4 Adressierung.....	231
171	3.18.1.4.1 Access Gateway zum Transportnetz Internet.....	231
172	3.18.1.4.2 ePA-Aktensystem zum Zentralen Netz.....	231
173	3.18.2 Proxy für das VAU-Protokoll.....	232
174	3.18.3 Tracing in Nichtproduktivumgebungen	232
175	3.18.4 Übergreifende Festlegungen	234
176	3.19 Data Submission Service	235
177	3.19.1 Erstellung von Arbeitsnummern und Lieferpseudonymen	235
178	3.19.2 Auswahl von medizinischen Daten	236
179	3.19.3 Protokollierung des Datenexports an das FDZ	237
180	3.19.4 Pseudonymisierung von medizinischen Daten.....	237
181	3.19.5 Übermittlung der pseudonymisierten medizinischen Daten	238
182	3.20 Push Notification Management	240
183	3.20.1 Push Notification Management des ePA-Aktensystems	241
184	3.20.2 Registrierung eines ePA-FdV als Pusher.....	241
185	3.20.3 Push Notification Channels	242
186	3.20.4 Push Notification Nachrichteninhalte	244
187	3.20.5 Versenden von Push Nachrichten.....	244
188	3.21 Backendseitige Zusatzfunktionen	245
189	3.21.1 Zugriffsmodell für backendseitige Zusatzfunktionen	246
190	3.21.2 Zusatzfunktion-Manager für backendseitige Zusatzfunktionen	247
191	3.22 Schnittstellen (OpenAPI).....	251
192	3.22.1 Übersicht der Schnittstellen des Aktensystems	252
193	3.22.2 Übergreifende Festlegungen zu den Schnittstellen	261
194	4 Informationsmodelle	263
195	5 Anhang A – Verzeichnisse	264
196	5.1 Abkürzungen	264
197	5.2 Glossar	266
198	5.3 Abbildungsverzeichnis.....	266
199	5.4 Tabellenverzeichnis	266
200	5.5 Referenzierte Dokumente	268
201	5.5.1 Dokumente der gematik.....	268
202	5.5.2 Weitere Dokumente.....	272
203		

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) fest-gelegt 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.

235 1.5 Methodik

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

240
241 **<AFO-ID> - <Titel der Afo>**
242 Text / Beschreibung
243 [**<=**]

244 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [**<=**]
245 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.[<=]

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

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

300 **A_27701 -Requestkennung in HTTP Header außerhalb des VAU-Kanals**

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

305 **A_27702 -Requestkennung in HTTP Header innerhalb des VAU-Kanals**

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

310 **A_27703 -Requestkennung in der Response**

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

315 **A_27712 -Requestkennung - betriebliche Protokollierung**

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

320 **A_27443-01 -Nutzung Terminologiepaket**

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

325 Hinweise zu A_27443-*:

- 326 1. Das Terminologiepaket wird als FHIR-Package bereitgestellt und enthält z.B.
327 Vocabulary ePA und Value Set für Berechtigungskategorien. Falls ein Code in
328 einem Code System als "inactive" gekennzeichnet wird, wird der Code über eine
329 entsprechende "Property" gekennzeichnet. Der folgende Ausschnitt zeigt ein
330 Beispiel (FHIR JSON-Format):

```
331 {  
332   "code": "1",  
333   "display": "Arzt in Facharztausbildung",  
334   "property": [{  
335     "code": "status",  
336     "valueCode": "inactive"  
337   }]  
338 },
```

- 339 2. Die Registrierung von Daten und Dokumenten mit dem Code im Status
340 "deprecated" wird vom ePA-Aktensystem akzeptiert. Die Kennzeichnung erfolgt
341 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):

Nam e	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 (preferr ed) 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-Profiles 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

470 I_Information_Service_Accounts bezogenen Teillisten der anderen ePA-
471 Aktensysteme.[<=]

472 2.2 Redundanz

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

475 2.3 Datenschutz und Sicherheit

476 **A_15128 -Anbieter ePA-Aktensystem - Schutz der transportierten Daten im** 477 **ePA-Aktensystem**

478 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die Vertraulichkeit und
479 Integrität der innerhalb des ePA-Aktensystems transportierten Daten gewährleistet
480 ist.[<=]

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

483 **A_15103 -Anbieter ePA-Aktensystem - Konzept zur Verhinderung von** 484 **Profilbildung**

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

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

491 **A_25722-01 -ePA-Aktensystem - Löschen von personenbezogenen Daten von** 492 **Vertretern nach Wegfall der Notwendigkeit**

493 Das ePA-Aktensystem MUSS es ermöglichen, dass personenbezogene Daten
494 von Vertretern ohne eigene Akte in ihrem Home-AS auf Verlangen des Vertreters
495 gelöscht werden können. Der Hersteller des ePA-Aktensystems kann hierfür eine
496 herstellereigenspezifische VAU-Schnittstelle umsetzen.[<=]

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

500 **A_15104 -Anbieter ePA-Aktensystem - Ordnungsgemäße IT-Administration**

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

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

507 **A_15824 -Anbieter ePA-Aktensystem - Sichere Speicherung von Daten**

508 Unabhängig davon, ob die Daten schon verschlüsselt vorliegen, MUSS der Anbieter des
509 ePA-Aktensystems die Daten des ePA-Aktensystems bei der Speicherung
510 verschlüsseln.[<=]

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

A_24774 -Anbieter ePA-Aktensystem - Zwei-Faktor-Authentisierung von Administratoren

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

A_15107-02 -Anbieter ePA-Aktensystem - Keine unzulässige Weitergabe von Daten

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

A_15119 -Anbieter ePA-Aktensystem - Löschkonzept

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

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

[≤]

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

A_15169 -ePA-Aktensystem - Verbot von Werbe- und Usability-Tracking

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

Davon ausgenommen ist das Erfassen des standardmäßigen quantitativen Nutzerverhaltens zur Ermittlung der Standard-Aktenutzung entsprechend der Anforderung A_15154. [≤]

A_15154 -Anbieter ePA-Aktensystem - Ermittlung von Standard-Aktenutzung

Der Anbieter des ePA-Aktensystems MUSS mindestens einmal im Jahr Werte zu einer Standard-Aktenutzung von LE und Versicherten durch die Profilierung anonymer Zugriffsstatistiken auf das ePA-Aktensystem zum Zweck der Erkennung von Zugriffen gemäß A_15155 ermitteln. [≤]

A_15155 -Anbieter ePA-Aktensystem - Abweichung von Standard-Aktenutzung

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

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

A_24778 -Anbieter ePA-Aktensystem - Einsatz zertifizierter HSM

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

560 Processing Standard (FIPS) in Frage.
561 Die Prüftiefe MUSS mindestens

- 562 1. FIPS 140-2 Level 3 oder
 - 563 2. FIPS 140-3 Level 3 oder
 - 564 3. Common Criteria EAL 4+ (mit AVA_VAN.5)
- 565 entsprechen. [≤]

566 **A_15157 -Anbieter ePA-Aktensystem - Sicherer Betrieb und Nutzung eines**
567 **HSMs**

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

572 **A_15159 -Anbieter ePA-Aktensystem - Schutzmaßnahmen gegen die OWASP**
573 **Top 10 Risiken**

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

577 **A_24780-01 -Anbieter ePA-Aktensystem – Versicherte über sensible**
578 **Änderungen informieren**

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

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

585 **A_15163 -Anbieter ePA-Aktensystem - Angriffen entgegenwirken**

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

589 **A_15167 -Anbieter ePA-Aktensystem - Social Engineering Angriffen**
590 **entgegenwirken**

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

593 **A_24989 -Anbieter ePA-Aktensystem - Schutz vor Angriffen über die TI**

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

598 **A_15168 -ePA-Aktensystem - Verbot vom dynamischen Inhalt**

599 Die Komponenten des ePA-Aktensystems DÜRFEN dynamischen Inhalt von Drittanbietern
600 NICHT herunterladen und verwenden.
601 [≤]

602 **A_17080 -Verhindern von Session Hijacking**

603 Die Komponenten des ePA-Aktensystems MÜSSEN geeignete Schutzmaßnahmen gegen
604 Session-Hijacking implementieren.
605 [≤]

A_16323-01 -ePA-Aktensystem - Verbot von medizinisch irrelevantem Inhalt

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

[<=]

A_24781 -Sicherer Betrieb des Produkts nach Handbuch

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

A_18953 -Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch

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

A_19122-01 -Anbieter ePA-Aktensystem – Trennung zu anderen Mandanten

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

A_21106 -Anbieter ePA-Aktensystem – Signaturschlüssel für Protokolle

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

A_21107 -Anbieter ePA-Aktensystem – Speicherung Signaturschlüssel für Protokolle im HSM

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

[<=]

A_22409 -Anbieter ePA-Aktensystem - CA-Anbieterwechsel

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

A_19118-01 -Komponenten des Aktensystems, Schutz vor XSW-Angriffen

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

A_24783 -ePA-Aktensystem - Eingabevalidierung von Operationen

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

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

A_24992 -ePA-Aktensystem - Zugriffe durch Versicherte übers Access Gateway

Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session für einen Versicherten (NutzerID ist KVN) 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. [$\leq$]

A_25006 -ePA-Aktensystem - User Session bei Inaktivität Beenden

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

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. [$\leq$]

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. [$\leq$]

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")

[$\leq$]

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	digitalSignatur	nonRepudiation	nonRepudiation	digitalSignatur
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. [$\leq$]

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, dass 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 Validierungskonten für StoreReviews

Bei Validierungsaktenkonten, für die die Regelung gem. A_22684-* gilt [Validierungsaktenkonten im StoreReview der FdVs], MÜSSEN folgende Besonderheiten berücksichtigt werden:

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

[<=]

A_26209 -Prüfung auf Vertretungsberechtigung für Prüffidentität

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

A_24539 -Nutzung von Validierungsaktenkonten via FdV

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

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

823 2.5 Tracing in Nichtproduktivumgebungen

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

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

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

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

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

849 **A_21887-01 -Tracing, Sensorpunkt nahe vor den VAU-Instanzen** 850 **(Nichtproduktivumgebungen)**

851 Ein ePA-Aktensystem MUSS sicherstellen, dass genau in Nichtproduktivumgebungen der
852 Datenverkehr zur und von den VAU-Instanzen auf TCP-Ebene mitgeschnitten wird
853 (Sensorpunkt). Der aktuell mitgeschnittene Datenverkehr MUSS auf einen TCP-Port im
854 Access Gateway gestreamt werden (siehe A_21890-*). D. h. wenn ein Client sich zu
855 diesem TCP-Port verbindet, MUSS er die aktuell auf dem Interface durchlaufenden Daten
856 gestreamt lesen können.

857 [**<=**]

858 **A_21891-01 -Tracing, Tiger-Standalone-Proxy**

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

862 **A_22581 -Tracing, Abschaltbarkeit**

863 Ein ePA-Aktensystem MUSS den Tiger-Standalone-Proxy (und die damit verbunden
864 Sensorpunkte) gemäß A_21891-* im Rahmen der Zulassungstests auf Wunsch der
865 gematik aktivieren und insbesondere deaktivieren können. [**<=**]

866 *Hinweis: Die Aktivier- bzw. Deaktivierbarkeit nach A_22581-* kann dabei auch teilweise*
867 *mit organisatorische Maßnahmen umgesetzt werden, d. h. es ist hier **kein***
868 *vollautomatisierter Mechanismus notwendig, der im Millisekunden-Bereich umschalten*
869 *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

954 Anwendungsfälle (sogenannte UX-Usecases) dazu verpflichtet, eigene Messungen
 955 durchzuführen und diese Messwerte an eine definierte Schnittstelle im Aktensystem zu
 956 übermitteln. Das Aktensystem verarbeitet diese Informationen und leitet das
 957 konsolidierte Ergebnis im Rahmen der Betriebsdatenlieferung weiter an die gematik. Auf
 958 diese Weise erhalten sowohl die gematik (im Rahmen der Gesamt-
 959 Produktverantwortung) als auch die Anbieter der Aktensysteme Informationen darüber,
 960 wie die Anwendung ePA bei den Nutzern (insb. in der LEU und bei Versicherten)
 961 hinsichtlich bestimmter Kernfunktionalitäten wahrgenommen wird.

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

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

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

975 **A_24570-01 -Verarbeitung von UX-Messdaten**

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

- 980 - Durchschnittswert der Messergebnisse
- 981 - Anzahl der berücksichtigten Messergebnisse
- 982 - Maximalwert
- 983 - Minimalwert[<=]

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

987

3 Funktionsmerkmale

988 3.1 Aktenkontoverwaltung

989 Ein ePA-Aktenkonto wird durch den Kostenträger eines Versicherten als Anbieter der ePA
990 für jeden Versicherten angelegt und für die Nutzung im Rahmen der gesetzlichen
991 Vorgaben zur Verfügung gestellt. Die Anlage eines Aktenkontos erfordert keine
992 Beantragung durch den Versicherten. In einem Aktenkonto ist entweder der Widerspruch
993 des Versicherten gegen die ePA hinterlegt oder eine Akte für den Versicherten. Die
994 Verwaltung eines Aktenkontos und der darin enthalten Akte oder Widerspruch durch den
995 Kostenträger erfolgt über das Account Management.

996 Die ITSG stellt im Auftrag des GKV-SV ein System bereit, das über ein Token attestiert,
997 dass ein bestimmter Kostenträger berechtigt ist eine KVNR zu verwalten und damit auch
998 die ePA für diese KVNR zu verwalten. Dieses ITSG-Token wird in der
999 Aktenkontoverwaltung genutzt, um Aktionen des Kostenträgers zu berechtigen.
1000 Festlegungen zu Inhalten, Format und Signatur des ITSG-Token sind in den "Richtlinien
1001 zum Aufbau und zur Vergabe einer Krankenversichertennummer (KVNR) und Regelungen
1002 des Krankenversichertennummernverzeichnis nach § 290 SGB V einschließlich der
1003 dazugehörigen Anlagen" [RL_KVNR], in der Anlage 4 zu finden.

1004

1005 **A_30369 -Account Management - Realisierung der Schnittstelle**

1006 **I_Account_Management**

1007 Das Account Management MUSS die Operationen der Schnittstelle

1008 I_Account_Management gemäß [I_Account_Management] umsetzen.[<=]

1009 **A_30356 -Anbieter ePA-Aktensystem - Anlage eines Aktenkontos für den**

1010 **Versicherten**

1011 Der Anbieter des ePA-Aktensystems MUSS für seine Versicherten ein Aktenkonto im ePA-
1012 Aktensystem über die Schnittstellen [I_Account_Management] anlegen und
1013 verwalten.[<=]

1014 **A_24336 -Anbieter ePA-Aktensystem - Identifizierung eines Aktenkontos**

1015 Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos die
1016 KVNR des Versicherten zur Identifikation des Aktenkontos im Aktensystem verwenden
1017 und sicherstellen, dass diese Identifikation eines Aktenkontos nicht verändert werden
1018 kann.[<=]

1019 **A_30359 -Anbieter ePA-Aktensystem - Anlage Aktenkonto erst nach Ablauf**

1020 **einer Widerspruchsfrist**

1021 Der Anbieter des ePA-Aktensystems DARF ein neues Aktenkonto NICHT anlegen, bevor
1022 die gesetzliche Widerspruchsfrist abgelaufen ist es sei denn, es liegt ihm ein Widerspruch
1023 gegen die Nutzung der ePA vor.[<=]

1024 **A_30373 -Account Management - Prüfung auf Berechtigung des Kostenträgers**

1025 Das Account Management MUSS sicherstellen, dass Operationen zum Erstellen eines
1026 Aktenkontos, Erstellen einer Akte oder hinterlegen eines Widerspruchs nur durchgeführt
1027 werden können, wenn der handelnde Kostenträger ein gültiges ITSG-Token vorweisen
1028 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,

- 1075 so werden dessen Informationen in das lokale ePA-Aktensystem verschoben, bzw., wenn
1076 das Aktenkonto schon lokal existiert, die Befugnisse für den zuständigen Kostenträger
1077 und die zuständige Ombudsstelle aktualisiert.
- 1078 Nachfolgend ist der generelle Ablauf der Anlage eines Aktenkontos mit möglicher
1079 Verschiebung von Informationen aus einem bestehenden Aktenkonto dargestellt.

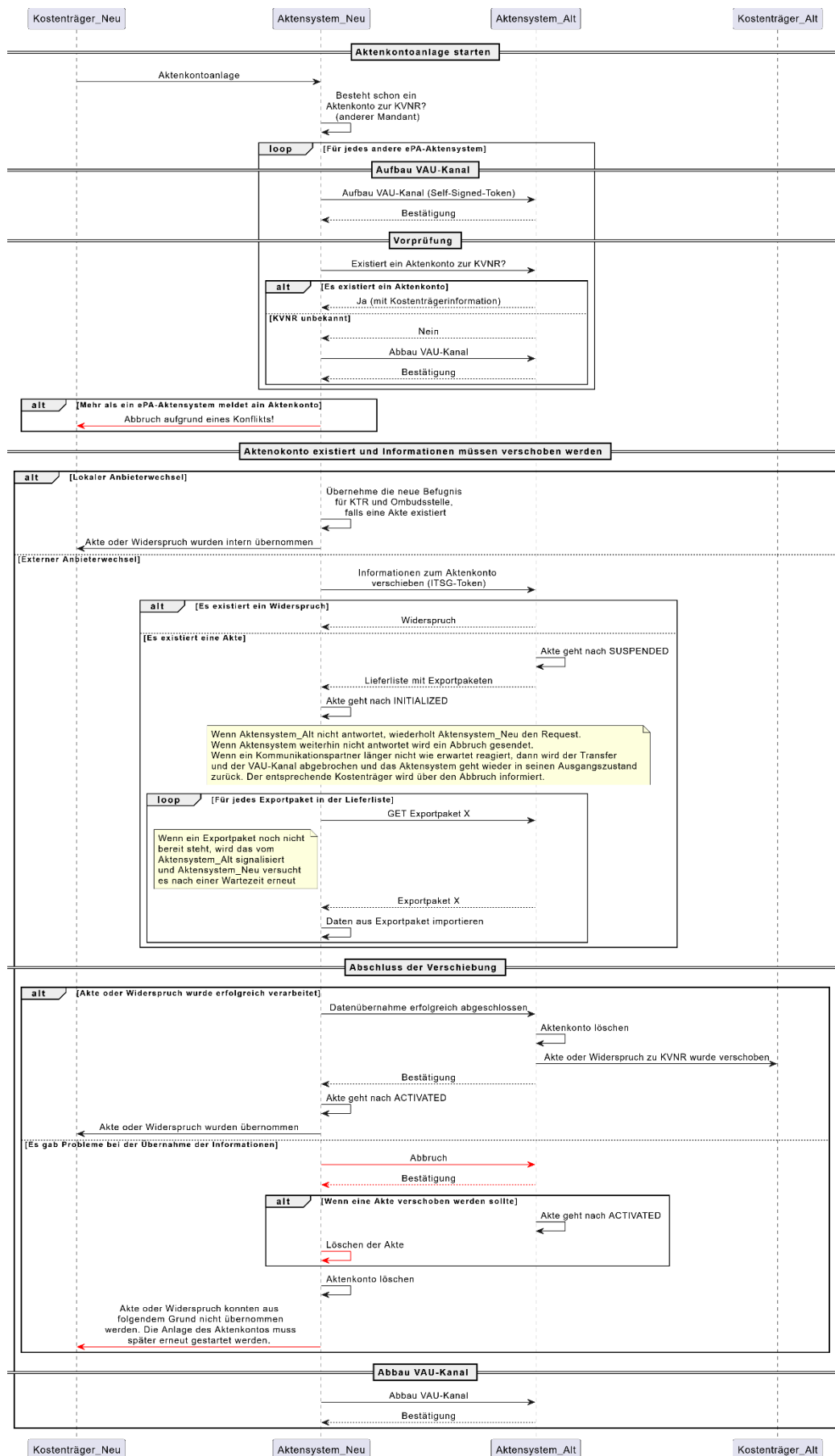


Abbildung 1 : Ablauf der Anlage eines Aktenkontos

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. [<=]

1128

1129 **3.1.3 Löschen eines Aktenkontos**

1130 Die Löschung eines Aktenkontos bei einem Anbieter und aller darin enthaltenen Daten
1131 kann z.B. in folgenden Situationen erforderlich sein:

- 1132 • nach Wechsel des Anbieters durch den Versicherten zu einem Anbieter, der die
1133 ePA seinen Versicherten nicht anbietet,
- 1134 • nachdem der Versicherte das generell das System der ePA verlassen hat, da er
1135 z.B. ins Ausland verzogen ist oder verstorben ist.

1136 Kündigt ein Versicherter das Vertragsverhältnis ohne Übernahme der Daten zu einem
1137 neuen Anbieter, löscht der Anbieter des Aktenkontos des Versicherten nach einer
1138 angemessenen Wartezeit, bzw. nach Ablauf von vorgeschriebenen Bereitstellungs- und
1139 Aufbewahrungszeiträumen, das Aktenkonto und alle darin enthaltenen Daten.

1140 Vor der Ausführung der endgültigen Löschung des Aktenkontos muss es dem
1141 Versicherten ermöglicht werden, die Protokolldaten (auch unter Einbindung der
1142 Ombudsstelle) für seinen eigenen Gebrauch außerhalb des Aktenkontos zu sichern.

1143 Bei der Löschung eines Aktenkontos muss der Anbieter die Administrationsgewalt über
1144 die entsprechende KVNR nicht über ein ITSG-Token nachweisen, da er dieses in
1145 bestimmten Anwendungsfällen (z.B. Wechsel des Versicherten zu einem Anbieter ohne
1146 ePA) nicht abrufen kann. Die Löschung erfolgt Risiko des löschenden Kostenträgers.

1147 **A_30403 -Account Management - Löschung eines Aktenkontos**

1148 Das Account Management MUSS den Auftrag zur Löschung eines Aktenkontos vom
1149 zuständigen Kostenträger unverzüglich ausführen und alle Informationen im Aktenkonto
1150 (Verwaltungsinformationen und Akte / Widerspruch) sicher löschen. [<=]

1151

1152 **3.1.4 Verschiebung der Informationen eines Aktenkontos**

1153 Wird bei der Anlage eines Aktenkontos für einen Kostenträger festgestellt, dass es zu der
1154 entsprechenden KVNR schon ein Aktenkonto bei einem anderen Kostenträger gibt, so
1155 werden die Informationen daraus zum aktuellen Kostenträger verschoben. Dabei kann es
1156 sich um eine lokale Verschiebung innerhalb eines ePA-Aktensystems handeln oder um die
1157 Verschiebung aus einem anderen ePA-Aktensystem.

1158 Das Account Management agiert im Zusammenhang mit der Verschiebung der
1159 Informationen eines Aktenkontos in zwei Rollen. Zum einen agiert das Account
1160 Management beim Anlegen eines Aktenkontos als Client der Informationen von einem
1161 anderen ePA-Aktensystem abruft. Zum anderen agiert das Account Management auf dem
1162 abgebenden ePA-Aktensystem als Server, der Informationen zum Widerspruch
1163 bereitstellt oder die Daten einer Akte in Exportpaketen zusammen- und bereitstellt.

1164

1165 Für die Verschiebung der Information eines Widerspruchs ist kein Exportpaket nötig, da
1166 diese an der Schnittstelle unmittelbar bereitgestellt wird.

1167 Der Ablauf einer Verschiebung ist wie folgt (siehe auch Abbildung "Ablauf der Anlage
1168 eines Aktenkontos"):

- 1169 1. Das lokale ePA-Aktensystem startet den Vorgang beim anderen ePA-Aktensystem

- 1170 2. Das andere ePA-Aktensystem liefert entweder einen Widerspruch oder eine Liste
1171 von Exportpaketen. Falls es ein Widerspruch ist, wird dieser übernommen und der
1172 Vorgang abgeschlossen.
- 1173 3. Falls eine Liste von Exportpaketen geliefert wurde, so wird diese nacheinander
1174 abgearbeitet indem
- 1175 a. ein Exportpaket von der Liste durch das lokale ePA-Aktensystem geholt wird
1176 b. der Inhalt des Exportpakets in die Akte des lokalen ePA-Aktensystems
1177 importiert wird
- 1178 4. Nachdem das letzte Exportpaket geholt und erfolgreich importiert wurde, wird der
1179 Vorgang abgeschlossen
- 1180 5. Die lokale Akte geht in den Status Activated und das Aktenkonto auf der
1181 abgebenden Seite wird gelöscht

1182 In dieser Spezifikation werden die Aktivitäten des Account Managements, die sich um das
1183 Erstellen von Exportpaketen und dem Import von Daten aus einem Exportpaket in einem
1184 internen virtuellen Health Record Relocation Service zusammengefasst. Dieser Service
1185 hat keine Schnittstellen außerhalb der VAU und dient nur einer fachlichen Gruppierung
1186 von Anforderungen. Nach außen hin werden diese Leistungen vom Account Management
1187 erbracht.

1188

1189 **A_30412 -Account Management - Abbruch bei Inaktivität der aufnehmenden** 1190 **Seite**

1191 Das Account Management der abgebenden Seite MUSS das Verschieben von
1192 Informationen abbrechen und wieder in den Ausgangszustand zurückkehren, wenn das
1193 Account Management der aufnehmenden Seite mehr als 60 Minuten kein neues Request
1194 schickt, obwohl die Verschiebung der Informationen noch nicht abgeschlossen ist. [<=]

1195 **A_30413 -Account Management - Abbruch bei Inaktivität der abgebenden Seite**

1196 Das Account Management der aufnehmenden Seite MUSS, wenn das Account
1197 Management der abgebenden Seite auch nach 4 Retries im Prozess der Verschiebung
1198 nicht antwortet, die Verschiebung abbrechen, den VAU-Kanal abbauen und das lokale
1199 Aktenkonto löschen. [<=]

1200 **A_30414 -Account Management - Unklare Situation bei Abschluss der** 1201 **Verschiebung**

1202 Das Account Management der aufnehmenden Seite MUSS, wenn das Account
1203 Management der abgebenden Seite den Abschluss der Verschiebung nach 4 Retries im
1204 Prozess der Verschiebung nicht bestätigt, eine mögliche lokale Akte in den Status
1205 INACCESSIBLE setzen und den zuständigen Kostenträger über das Problem beim
1206 Abschluss der Verschiebung informieren.
1207 [<=]

1208 **A_30416 -Account Management - Aktenkonto eingefroren bei unklarer Situation** 1209 **bei Abschluss der Verschiebung**

1210 Das Account Management DARF für Aktenkonten, bei denen die Verschiebung von
1211 Informationen aufgrund von Inaktivität der abgebenden Seite beim Abschluss nicht
1212 erfolgreich abgeschlossen werden konnte, NICHT eine weitere Verschiebung
1213 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. [$\leq$]

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.

[$\leq$]

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

[≤]

1274 Der Wert "ES256" (JWS-Parameters "alg") gilt auch für die Kurve "brainpoolP256r1" (also
1275 nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu
1276 erstellen."

1277

1278 **A_24821-01 -Health Record Relocation Service - Suspendierung des** 1279 **Aktenkontos**

1280 Der Health Record Relocation Service MUSS sicherstellen, dass die Akte für die Erstellung
1281 eines Exportpakets auf den Status SUSPENDED gesetzt wird. [<=]

1282 **A_24827-01 -Health Record Relocation Service - Reaktivierung des Aktenkontos**

1283 Der Health Record Relocation Service MUSS sicherstellen, dass eine Akte im Status
1284 SUSPENDED nach einem Abbruch eines Transfers von einem Anbieter zu einem anderen
1285 Anbieter aufgrund eines Fehlers (Datenübertrag ist nicht erfolgt) in den Status
1286 ACTIVATED gesetzt wird. [<=]

1287 **A_21750 -Health Record Relocation Service – Integritätsschutz Exportpaket**

1288 Der Health Record Relocation Service MUSS das erstellte Exportpaket mit einem "Digest"
1289 HTTP Response Header (<https://tools.ietf.org/html/rfc5843>) als

1290 Integritätsschutz versehen und dabei als Digest Algorithmus SHA-256 verwenden.

1291 Beispiel Digest-Header:

1292 Digest: SHA-

1293 256=MWVkmWQxYTRiMzk5MDQ0MzI3NGU5NDEyZTk5OWY1ZGFmNzgyZTJlODYzYjRjYzFh
1294 OTImNTQwYzI2M2QwM2U2MQ==

1295 [<=]

1296

1297 **3.1.4.2 Import von Exportpaketen**

1298 Beim Import eines Exportpakets werden die darin enthaltenen Daten in das lokale ePA-
1299 Aktensystem integriert. Dabei sind bestimmte Regeln einzuhalten. Die entsprechenden
1300 Vorgaben sind in diesem Kapitel dargestellt.

1301

1302 **A_14905-05 -Health Record Relocation Service – Import des Exportpakets des** 1303 **vorhergehenden Aktenkontos**

1304 Der Health Record Relocation Service MUSS das vom vorhergehenden Anbieter ePA-
1305 Aktensystem des Versicherten bezogene Exportpaket, in das neue
1306 Aktenkonto importieren und dazu:

- 1307 • den Digest gemäß A_21750-* prüfen,
- 1308 • die Befugnisse mit Regel "rr5" (siehe Tab_AS_Entitlement_Registration_Rules im
1309 Aktensystem) registrieren und
- 1310 • falls DocumentEntry.originalURI im Exportpaket vorhanden ist, wird für jedes
1311 Dokument eines SubmissionSet der Inhalt von DocumentEntry.URI durch den
1312 Inhalt von DocumentEntry.originalURI ersetzt. (Hinweis:
1313 DocumentEntry.originalURI darf nicht als eigenständiges Metadatum in die
1314 Registry übernommen werden, da es lediglich dem Transport des Originalwertes
1315 von DocumentEntry.URI aus dem alten Aktensystem dient.

1316 [<=]

1317 **A_28045-01 -Health Record Relocation Service - Übernahme von Widersprüchen**

1318 Der Health Record Relocation Service MUSS sicherstellen, dass beim Import von
1319 Widersprüchen zur Sekundärdatennutzung berücksichtigt wird, ob das Feature in der

1320 abgebenden Akte bzw. in der aufnehmenden Akte unterstützt wird. Dabei MUSS wie folgt
1321 vorgegangen werden:

- 1322 • neu unterstützt: Die Widersprüche werden unverändert übernommen.
- 1323 • neu nicht unterstützt: Die Widersprüche werden als "erteilt" gesetzt (decision =
1324 deny).

1325 Bei Veränderung der Entscheidung MUSS dem Sekundärnutzungszweck als Zeitpunkt der
1326 Änderung der feste Wert "2025-01-15T00:00:00Z" und als Akteur "system" zugeordnet
1327 werden.

1328 [$\leq$]

1329 *Hinweis:*

1330 *Die Verschiebung von einem Kostenträger, der das Feature Sekundärdatennutzung nicht*
1331 *unterstützt zu einem Kostenträger, der das Feature Sekundärdatennutzung unterstützt*
1332 *führt zu einem Opt-In für dieses Feature. D.h. für eine Sekundärdatennutzung muss ein*
1333 *Versicherter bzw. Vertreter nach der Verschiebung aktiv der Sekundärdatennutzung*
1334 *zustimmen, was durch geeignete Prozesse des Kostenträgers unterstützt wird.*

1335

1336 **A_27616 -Health Record Relocation Service - Abbruch des Imports eines** 1337 **Exportpakets**

1338 Der Health Record Relocation Service MUSS den Import eines Exportpakets vollständig
1339 abbrechen, wenn einzelne Elemente des Exportpakets aufgrund konstruktiver oder
1340 inhaltlicher Fehler nicht erfolgreich importiert werden können. Eventuell schon
1341 importierte Elemente desselben Exportpakets MÜSSEN im Falle eines Abbruchs entfernt
1342 werden.[$\leq$]

1343 *Hinweis: Das exportierende Aktensystem wird über den Abbruch durch ein `abort` an der*
1344 *Schnittstelle informiert.*

1345 *Hinweis: Eine zum Zeitpunkt des Imports eines Exportpaketes zeitlich nicht mehr gültige*
1346 *Befugnis aus dem Exportpaket ist kein Fehler im Sinne der Anforderung und führt nicht*
1347 *zu einem Abbruch. Das importierende Aktensystem kann eine solche Befugnis ignorieren.*

1348 **A_21548-02 -Health Record Relocation Service - Information der Vertreter über** 1349 **Bezeichner des neuen Abieters nach Abschluss des Anbieterwechsels**

1350 Der Health Record Relocation Service MUSS sicherstellen, dass alle Vertreter nach
1351 erfolgreichem Import aller Exportpakete und somit Abschluss der Verschiebung der Akte
1352 über Anbieterwechsel und den Bezeichner des neuen Anbieters des Versicherten
1353 informiert werden, so dass sie in der Lage sind, die erforderliche initiale Anmeldung
1354 durchzuführen und informiert sind, welche Art von personenbezogenen Daten vom
1355 Vertreter im Rahmen der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden,
1356 wie der Vertreter eine Vertreterberechtigung widerrufen kann und gegenüber wem er
1357 seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann.[$\leq$]

1358 *Hinweis 1 zu A_21548-*: Für die Benachrichtigung derjenigen Vertreter, die dem*
1359 *importierenden Aktensystem nicht bekannt sind, werden die E-Mail-Adressen aus dem*
1360 *Exportpaket genommen. Für die Benachrichtigung der Vertreter, die dem importierenden*
1361 *Aktensystem bekannt sind, wird die im importierenden Aktensystem hinterlegte E-Mail-*
1362 *Adresse des Vertreters verwendet.*

1363 *Hinweis 2 zu A_21548-*: Der Bezeichner des neuen Anbieters muss dem Wert*
1364 *entsprechen der durch die Operation `getProviderList` geliefert wird.*

1365 **A_26257 -Health Record Relocation Service - Löschen der im Exportpaket** 1366 **enthaltenen E-Mail-Adressen der Vertreter**

1367 Der Health Record Relocation Service MUSS sicherstellen, dass die im Exportpaket
1368 enthaltenen E-Mail-Adressen von Vertretern ausschließlich zur Information der Vertreter

1369 gemäß A_21548-* genutzt werden und nach Abschluss des Anbieterwechsels im
1370 importierenden Aktensystem gelöscht werden, d.h. nicht im importierenden Aktensystem
1371 gespeichert werden.[<=]

1372 **A_24788 -Health Record Relocation Service - Löschen des Exportpakets nach**
1373 **Umzug des Aktenkontos**

1374 Das Aktensystem MUSS sicherstellen, dass ein vorhandenes Exportpaket nach einem
1375 erfolgreichen Transfer eines Aktenkontos eines Versicherten von einem Anbieter zu
1376 einem anderen Anbieter gelöscht wird.[<=]

1377

1378 **3.1.5 Anlage einer Akte bei Rücknahme eines Widerspruchs gegen**
1379 **die ePA**

1380 Besteht für einen Versicherten ein Aktenkonto mit einem Widerspruch und wird dieser
1381 Widerspruch zurückgenommen, so muss der zuständige Kostenträger für diesen
1382 Versicherten eine Akte im Aktenkonto anlegen.

1383 Dafür stellt der Kostenträger die selbst-signierten Befugnisse für sich und die
1384 Ombudsstelle bereit, der Widerspruch wird im Aktenkonto gelöscht und die Akte wird
1385 initialisiert. Nach erfolgreicher Initialisierung geht der Status der Akte nach Activated
1386 über und die Akte ist in der Versorgung nutzbar.

1387 **A_30390 -Account Management - Anlage einer Akte in einem bestehenden**
1388 **Aktenkonto**

1389 Das Account Management MUSS bei der Anlage einer Akte in einem Aktenkonto den
1390 bestehenden Widerspruch löschen, die Befugnisse für den zuständigen Kostenträger und
1391 die Ombudsstelle übernehmen, die Akte initialisieren und nachfolgend die Akte in den
1392 Status ACTIVATED setzen.[<=]

1393 **3.1.6 Lebenszyklus und Zustände einer Akte**

1394 Eine Akte durchläuft in seinem Lebenszyklus diverse Zustände. Einige dieser Zustände
1395 sind für rein administrative Vorgänge vorgesehen (Initialisierung, Umzug des
1396 Aktenkontos zu einem anderen Anbieter), andere für die Nutzung der Akte im
1397 Versorgungsprozess. Diese Nutzung für Versorgungsprozesse ist dabei auf den Zustand
1398 "Activated" eingeschränkt.

1399 Eine Übersicht der unterschiedlichen Status und der Bedingungen für den
1400 Statusübergang sind in der folgenden Tabelle dargestellt.

1401 **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	Widerspruch gegen die Nutzung der ePA	UNKNOWN

Zustand	Erläuterung	zulässige Transitionen	Folgezustand
	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.	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	Die Anlässe für diesen Zustand sind entfallen (z.B. Datenmigration wurde erfolgreich durchgeführt)	ACTIVATED

Zustand	Erläuterung	zulässige Transitionen	Folgezustand
	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.	Widerspruch gegen die Nutzung der ePA	UNKNOWN
		Der Status konnte nicht auf ACTIVATED gewechselt werden, da eine weitere aktivierte Akte gefunden wurde.	INACCESSIBLE

1402 **A_28686 -Prüfung vor Wechsel in den Status ACTIVATED**

1403 Das ePA-Aktensystem MUSS unmittelbar vor dem Wechsel in den Status ACTIVATED
 1404 prüfen, ob bei einem anderen ePA-Aktensystem für die verwendete KVNR schon ein
 1405 Aktenkonto im Status ACTIVATED vorliegt und im Fall des Fundes eines solchen
 1406 Aktenkontos den Statuswechsel abbrechen, den Status INACCESSIBLE mit der Ursache
 1407 "fehlgeschlagener Statuswechsel ACTIVATED" setzen und die Situation durch den
 1408 Anbieter oder Betreiber des ePA-Aktensystems auflösen lassen. [<=]

1409 **A_24369-02 -ePA-Aktensystem - Initialisierung einer Akte**

1410 Das ePA-Aktensystems MUSS die Initialisierung der Bestandteile

- 1411 • Consent Decision Management (initiale Entscheidungen)
- 1412 • Constraint Management (Policies)
- 1413 • Entitlement Management (initiale Befugnisse und Befugnisausschlüsse)
- 1414 • Information Service (initiale Entscheidungen "Versorgungsprozess")
- 1415 • XDS Document Service (statische Aktenkontoinhalte)
- 1416 • Device Management
- 1417 • Authorization Service
- 1418 • Audit Event Service
- 1419 • Medication Service
- 1420 • MHD Service
- 1421 • Patient Service
- 1422 • EHR Information Service

1423 vor der Aktivierung einer Akte durchführen. Die genannten Bestandteile MÜSSEN nach
 1424 der Aktivierung der Akte sofort nutzbar sein. [<=]

1425 **3.1.7 Akte ist zeitweise nicht nutzbar**

1426 Während der aktiven Nutzung einer Akte kann es zu Problemen kommen, bei der die
 1427 Nutzung temporär nicht möglich ist und Maßnahmen ergriffen werden müssen, um eine
 1428 Akte zu reparieren oder wieder nutzbar zu machen. In diesem Fall setzt das Aktensystem
 1429 die Akte in den Aktenstatus INACCESSIBLE und weist im betrieblichen Log auf das
 1430 Problem und seine Ursache hin. Zusätzlich wird die Ursache für den Statuswechsel
 1431 gespeichert. Es ist auch möglich, dass im Aktenstatus INACCESSIBLE weitere Ursachen
 1432 ergänzt werden, die für eine Beibehaltung des Aktenstatus sorgen. Der Anbieter oder
 1433 Betreiber kann nun Maßnahmen ergreifen, um die Ursachen zu adressieren. Adressierte

1434 Ursachen werden gelöscht. Nachdem alle Ursachen gelöscht wurden, wird die Akte
1435 wieder in den Aktenstatus ACTIVATED gesetzt. Damit wird ermöglicht, dass die
1436 ergriffenen Maßnahmen bei der nächsten Nutzung der Akte auf die Daten des
1437 Aktenkontos wirken können.

1438 *HINWEIS: Der Aktenstatus wird nicht aufgrund temporärer betrieblicher Probleme (z.B.*
1439 *Datenbank nicht erreichbar) gewechselt sondern nur, wenn explizite Maßnahmen für*
1440 *diese spezifische Akte ergriffen werden müssen, die einige Zeit in Anspruch nehmen.*
1441 *Temporäre betrieblich Probleme werden über die entsprechenden Fehlercodes ggü. dem*
1442 *Client signalisiert, welche dann zu einem erneuten Versuch zu einem späteren Zeitpunkt*
1443 *führen.*

1444 *HINWEIS: Sollte in der Spezifikation im Zusammenhang mit dem STATUS INACCESSIBLE*
1445 *eine konkrete Ursache benannt sein, dann ist dies immer als eine semantische Ursache*
1446 *zu verstehen und muss nicht über den genannten Wortlaut im Produkt repräsentiert*
1447 *werden.*

1448 **A_28493-01 -ePA-Aktensystem – Verwaltung der Deaktivierung einer Akte** 1449 **durch Aktensystem**

1450 Das ePA-Aktensystem KANN eine Akte in den Aktenstatus *INACCESSIBLE* versetzen bzw.
1451 für eine Akte im Zustand *INACCESSIBLE* weitere Ursachen für den Verbleib im Aktenstatus
1452 *INACCESSIBLE* ergänzen oder Ursachen, die durch das Aktensystem behoben sind
1453 löschen. Die Ursache des Statuswechsel wird in der Akte gespeichert.

1454 [$\leq$]

1455 **A_28494-01 -ePA-Aktensystem – Verwaltung der Deaktivierung einer Akte** 1456 **durch Anbieter**

1457 Der Anbieter des ePA-Aktensystems KANN eine Akte in den Aktenstatus *INACCESSIBLE*
1458 versetzen bzw. für eine Akte im Zustand *INACCESSIBLE* weitere Ursachen für den Verbleib
1459 im Aktenstatus *INACCESSIBLE* ergänzen oder Ursachen die behoben sind löschen.

1460 [$\leq$]

1461 **A_28495-01 -ePA-Aktensystem – Reaktivierung einer Akte**

1462 Das ePA-Aktensystem MUSS bei einer Akte im Aktenstatus *INACCESSIBLE*, bei dem keine
1463 Ursache mehr für den Aktenstatus vorliegt, in den Aktenstatus ACTIVATED wechseln.

1464 [$\leq$]

1465 **A_28496-01 -ePA-Aktensystem – Optionale Schnittstelle zur Aktualisierung**

1466 Das ePA-Aktensystem KANN eine Schnittstelle für Kostenträger anbieten, über die der
1467 zuständige Kostenträger eine Akte zur Verarbeitung in die VAU laden kann, damit das
1468 ePA-Aktensystem Daten der Akte korrigieren kann.

1469 [$\leq$]

1470 **A_28497-01 -ePA-Aktensystem – Abgrenzung der optionalen Schnittstelle zur** 1471 **Aktualisierung**

1472 Das ePA Aktensystem MUSS sicherstellen, dass die optionale Schnittstelle gemäß
1473 A_28496-*

- 1474 • ausschließlich durch Kostenträger nutzbar ist,
- 1475 • keine fachlichen Eingangs- oder Ausgangsparameter besitzt,
- 1476 • ausschließlich technische Operationen zur Korrektur oder Aktualisierung einer
1477 Akte auslösen kann.

1478 [$\leq$]

1479 *HINWEIS: Die Schnittstelle dient zum Öffnen einer Akte zu einem vom Kostenträger*
1480 *wählbaren Zeitpunkt, um im Aktensystem implementierte technische Operationen zur*
1481 *Korrektur oder Aktualisierung einer Akte automatisch auszuführen, deren Ausführung*

1482 eine geöffnete Akte benötigen. Die technischen Operationen sind durch das Aktensystem
 1483 festgelegt, d.h. der Kostenträger hat keine Möglichkeit die Operationen über die optionale
 1484 Schnittstelle selbst zu steuern oder zu beeinflussen.

1485

1486 3.1.8 Aktenzusammenführung (Health Record Merge)

1487 Die Zusammenführung von zwei Akten desselben Versicherten aus verschiedenen
 1488 Aktenkonten erfolgt genauso, wie die Verschiebung einer Akte. Sie unterscheiden sich
 1489 nur darin, dass die Akte im Aktenkonto der abgebenden Seite einen anderen Status
 1490 haben muss und der Health Record Relocation Service auf der aufnehmenden Seite die
 1491 Daten aus den zwei beteiligten Akten gemäß festgelegter Regeln zusammenführen muss.

1492

1493 **A_28412-01 -Health Record Relocation Service - Regeln für eine** 1494 **Zusammenführung**

1495 Der Health Record Relocation Service des neuen (importierenden) Aktensystems MUSS
 1496 bei der Zusammenführung zweier Akten für Objekte `obj_export` im zu importierenden
 1497 Exportpaket die folgenden Regeln umsetzen:

1498

Daten im Exportpaket	Regel für die Zusammenführung
XDS Document Service <code>obj_export</code> = Replace- Kette bestehend aus 1...n Dokumenten ($n \geq 1$) <code>obj_export[1]</code> bezeichnet das aktuellste Dokument der Kette	<u>Bemerkung</u> ; ein Dokument <code>obj</code> ist im Aktensystem <i>vorhanden</i> , falls es ein Dokument <code>obj</code> ' im Aktensystem mit selber entryUUID, uniqueID oder selbem Hash-Wert gibt. wenn im importierenden AS kein Dokument von <code>obj_export</code> vorhanden ist, dann ergänze <code>obj_export</code> wenn im importierenden AS mindestens ein Dokument von <code>obj_export</code> vorhanden ist und das aktuellste Dokument <code>obj_export[1]</code> ist nicht vorhanden, dann ergänze <code>obj_export[1]</code> und verwurfe den Rest der Kette <code>obj_export[2..n]</code> , sonst verwurfe <code>obj_export</code>
XDS Document Service <code>obj_export</code> = Unique- Dokument (z.B. NFD, DPE)	wenn im importierenden AS das Unique-Dokument <code>obj_export</code> nicht vorhanden ist, dann ergänze <code>obj_export</code> sonst verwurfe <code>obj_export</code>

Daten im Exportpaket	Regel für die Zusammenführung
XDS Document Service obj_export = dynamischer Folder	<u>Bemerkung</u>; ein Folderobj ist im Aktensystem <i>vorhanden</i>, falls es einen Folderobj ' 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. uniqueId von obj_export bereits im importierenden AS existieren. wenn im importierenden AS der Folderobj_export vorhanden ist und SubmissionSet.submissionTime von obj_export älter als das SubmissionSet.submissionTime des vorhandenen Folders ist, dann übernimmt SubmissionSet.submissionTime von obj_export für den vorhandenen Folder sonst verwirfe 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	<i>Es erfolgt keine Zusammenführung durch das Aktensystem.</i>
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 verwirfe obj_export

Daten im Exportpaket	Regel für die Zusammenführung
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_export
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 inobj_export identifizierte 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 inobj_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 entity.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	<i>Es erfolgt keine Zusammenführung durch das Aktensystem.</i>

1499 [**<=**]

1500

1501 **A_28414 -ePA-Aktensystem – Information des Versicherten über**

1502 **Zusammenführung durch Anbieter**

1503 Der Anbieter des ePA-Aktensystems MUSS den Versicherten über eine anstehende
 1504 Zusammenführung seiner Akte informieren, sofern durch die Zusammenführung ein
 1505 Zustand der Akte entstehen könnte, den der Versicherte überprüfen sollte.[**<=**]

1506 Hinweis zu A_28414-*: In der Kommunikation mit den Versicherten kann der Anbieter
 1507 eine eigene Sprachregelung wählen, es muss gegenüber dem Versicherten nicht von
 1508 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

1553 Medication Service lediglich in einer der Akten vorgenommen wurden. Falls diese
1554 Änderungen nicht in der weiterzuführenden Akte enthalten sind, erfolgt die einfache
1555 Übertragung der Ressourcen des Medication Service in diese Akte.

1556 Dieser Fall liegt vor, wenn der Datenbestand (des Medication Service) der einen Akte
1557 schon vollständig im Datenbestand der anderen Akte vorhanden ist. Der Datenbestand
1558 mit der größeren Anzahl Ressourcen ist dann der weiterzuführende. Für den Vergleich
1559 sind alle Versionen aller Ressourcen des Datenbestands zu berücksichtigen.

1560 Die Bewertung der Datenbestände bezüglich Änderung und Abweichung kann dabei auf
1561 ein zeitliches Intervall eingegrenzt werden, wenn ein Zeitpunkt der Separation
1562 (Relocation) der beiden Akten existiert und bekannt ist und vor diesem Zeitpunkt die
1563 Datenbestände der beiden Akten identisch sind.

1564 **A_30421 -Health Record Relocation Service - Auswahl des Datenbestands des**
1565 **Medication Service für die weitere Nutzung bei nicht verteilten Ressourcen**

1566 Wenn Ressourcen des Medication Service einer Akte bei einer
1567 anstehenden Zusammenführung von Ressourcen des Medication Service vollständig im
1568 Datenbestand der anderen Akte enthalten sind, dann MUSS der Health Record Relocation
1569 Service den Datenbestand der enthaltenden Akte vollständig im Medication Service der
1570 weiterzuführenden Akte verfügbar machen.[<=]

1571

1572 *3.1.8.1.3 Zusammenführung verteilter Ressourcen*

1573 Sind eML-Ressourcen zusammenzuführen, dann werden bisher nicht vorhandene
1574 Ressourcen und Versionen von Ressourcen in die weiterzuführende Akte übertragen. Der
1575 Übertrag von Unikat-Ressourcen entfällt, wenn bereits eine inhaltsgleiche Ressource in
1576 der weiterzuführenden Akte existiert. In diesem Fall werden Referenzen in übertragenen
1577 Ressourcen angepasst, wenn sie auf diese Unikate referenzieren.

1578 **A_30422 -Health Record Relocation Service -Zusammenführung von Ressourcen**
1579 **und Ressourcenversionen des Medication Service**

1580 Der Health Record Relocation Service MUSS bei einer Zusammenführung von Ressourcen
1581 des Medication Service die Ressourcen der Profile `EPAMedication`,
1582 `EPAMedicationStatement`, `EPAMedicationRequest`, `EPAMedicationDispense` und
1583 `EPAActivityProvenance` (Änderungseintrag eML), inklusive aller Inhalte und mit allen
1584 Versionen in die weiterführende Akte übertragen, wenn diese dort nicht vorhanden sind
1585 oder weniger Versionen aufweisen.[<=]

1586 **A_30423 -Health Record Relocation Service -Zusammenführung von Unikat-**
1587 **Ressourcen des Medication Service**

1588 Der Health Record Relocation Service MUSS bei einer Zusammenführung von Ressourcen
1589 des Medication Service die Ressourcen der Profile `PractitionerDirectory`,
1590 `OrganizationDirectory` und `PractitionerRole` der eML in die weiterzuführende Akte
1591 übertragen, wenn es dort keine dieser Unikat-Ressourcen mit gleichem Inhalt gibt.
1592 Der Health Record Relocation Service MUSS die Übertragung dieser Ressourcen
1593 unterlassen, wenn es in der weiterzuführenden Akte bereits Ressourcen mit gleichem
1594 Inhalt gibt. Referenzen auf die nicht übertragenen Unikat-Ressourcen in den
1595 übertragenen weiteren Ressourcen des Medication Service MÜSSEN in Referenzen auf
1596 die im Bestand vorhandenen Ressourcen geändert werden.

1597 Zwei Ressourcen des Profils `PractitionerDirectory` oder `OrganizationDirectory` sind
1598 gleichen Inhalts, wenn die enthaltene Telematik-ID übereinstimmt.

1599 Zwei Ressourcen des Profils `PractitionerRole` sind gleichen Inhalts, wenn in den
1600 referenzierten Ressourcen `PractitionerDirectory` und `OrganizationDirectory` jeweils
1601 die Telematik-ID übereinstimmt.[<=]

1602 *Hinweis: Die Anpassung einer Referenz auf eine schon vorhandene Unikat-Ressource*
1603 *erfordert keine neuen Versionen von Ressourcen und keine Anlage einer*
1604 *EPAActivityProvenance.*

1605

1606 Wenn durch die Zusammenführung von eML-Ressourcen eine Anpassung von im Bestand
1607 vorhandenen eMP-Ressourcen erforderlich würde (Erstellen von Verknüpfungen eML-
1608 eMP) oder in beiden Akten eMP-Ressourcen angelegt oder verändert wurden (simultanes
1609 Kuratieren des eMP), dann wird der eMP, bzw. werden die eMP-Ressourcen, in der
1610 weiterzuführenden Akte entfernt und keine eMP-Ressourcen in diese Akte übertragen.

1611 **A_30424 -Health Record Relocation Service - Löschen des eMP bei**
1612 **Zusammenführung von Ressourcen**

1613 Der Health Record Relocation Service MUSS bei einer Zusammenführung von Ressourcen
1614 des Medication Service die Ressourcen des eMP (`EMPMedication`,
1615 `EMPMedicationRequest`, `EMPChronologyProvenance`, `TIOrganization` und
1616 `EPAActivityProvenance` (Änderungseintrag eMP) in der weiterzuführenden Akte löschen,
1617 wenn:

- 1618 • in beiden Akten eMP-Einträge erstellt oder geändert wurden, oder
- 1619 • in der weiterzuführenden Akte nach einer Zusammenführung von eML-Einträgen
1620 zur Erstellung eines konsistenten Datenbestands Änderungen an existierenden
1621 eMP-Ressourcen erforderlich werden.

1622 [`<=`]

1623 **A_30425 -Health Record Relocation Service - Löschen von eML-eMP**
1624 **Verknüpfungen**

1625 Der Health Record Relocation Service MUSS bei einer Zusammenführung von Ressourcen
1626 des Medication Service alle eML-eMP-Verknüpfungen aus den eML-Ressourcen der
1627 weiterzuführenden Akte löschen, wenn eMP-Ressourcen dieser Akte entfernt wurden.

1628 Der Health Record Relocation Service MUSS alle Extensions der Indikation
1629 "`LINKING_NOT_SUCCEFULL`" aus den `EPAMedicationStatements` entfernen.

1630 Für jede Änderung an Ressourcen des Profils `EPAMedicationStatement` MUSS eine
1631 Ressource `EPAActivityProvenance` mit ausführendem Dienst 'MEDICATIONSVC' erzeugt
1632 werden.[`<=`]

1633 *Hinweis: Eine eML-eMP-Verknüpfung wird vollständig entfernt, der Inhalt von `basedOn`*
1634 *der Ressourcen `EPAMedicationStatement` und `EPAMedicationRequest` wird dazu*
1635 *gelöscht.*

1636 *Hinweis: Diese Änderungen sind durch die Zusammenführung der Ressourcen bedingte*
1637 *Korrekturen und stellen keine Änderung eines eML-Eintrags dar. Eine gesonderte*
1638 *Protokollierung ist nicht erforderlich.*

1639

1640 Durch die Zusammenführung können Daten des eMP verloren gehen. Dieses können
1641 sowohl eMP-Einträge aus dem Bestand der weiterzuführenden Akte, als auch aus der
1642 anderen Akte sein. Zur Information und weiteren Verwendung durch den Versicherten
1643 wird daher jeweils ein aktueller Medikationsplan der Akten in gerendeter Form im
1644 Format PDF/A als Dokument in der Akte des Versicherten abgelegt.

1645 Durch die Zusammenführung wird die eML in der weiterzuführenden Akte um Einträge
1646 erweitert. Zur Information und weiteren Verwendung durch den Versicherten wird daher
1647 jeweils eine aktuelle Medikationsliste der Akten in gerendeter Form im Format PDF/A als
1648 Dokument in der Akte des Versicherten abgelegt. Diese Dokumente geben den Zustand
1649 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 MEDIKATIONSLISTE!"
 - eML der anderen Akte: "Übernommene Medikationsliste der Akte <Kostenträgername> 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").

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-Verknüpfungen
- 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 [≤]

1736 *Hinweis: Ein gemäß der Beschreibung in Kapitel 3.2.3.1.2 "Sonderfall exklusive Nutzung*
1737 *einer der beiden Akten" festgestellter Zeitpunkt der Separation kann auch hier zur*
1738 *Einschränkung der relevanten Ressourcenmenge angewendet werden.*

1739

1740 Durch die vereinfachte Auswahl geht der Datenbestand einer Akte verloren. Zur
1741 Information und weiteren Verwendung durch den Versicherten wird daher jeweils eine
1742 aktuelle Medikationsliste und ein aktueller Medikationsplan in gerendeter Form im
1743 Format PDF/A als Dokument in der Akte des Versicherten abgelegt. Diese Dokumente
1744 geben den Zustand des nicht weitergeführten Datenbestandes wieder. Für den
1745 weiterzuführenden Datenbestand entfällt die Erstellung dieser Dokumente.

1746 **A_30430 -Health Record Relocation Service - Archivierung der Daten des**
1747 **Medication Service als Dokument bei vereinfachter Auswahl (Fallback-Lösung)**

1748 Der Health Record Relocation Service MUSS jeweils ein Dokument für den nicht
1749 weiterzuführenden Datenbestand im Format PDF/A für den letzten Zustand des eMP und
1750 der eML des Medication Service erstellen und in der weiterzuführenden Akte des
1751 Versicherten ablegen und die Ablage der Dokumente protokollieren. Die Dokumente
1752 MÜSSEN den Vorgaben für Dokumente im Format PDF/A bei Abruf über die Render API
1753 "Medikationsplan abrufen (eMP)", bzw. "Medikationsliste abrufen (eML)", entsprechen. Der
1754 Abruf der Dokumente MUSS nicht protokolliert werden.
1755 Für die Dokumente gilt:

- 1756 • Ablage im Ordner "patient" des XDS Document Service
- 1757 • DocumentEntry.title =
- 1758 • eMP: "Gelöschte Medikationsplanung aus Aktenzusammenführung - KEIN
- 1759 GÜLTIGER MEDIKATIONSPLAN!"
- 1760 • eML: "Gelöschte Medikationsliste aus Aktenzusammenführung - KEINE
- 1761 GÜLTIGE MEDIKATIONSLISTE!"
- 1762 • mimetype = "application/pdf"
- 1763 • formatCode = "urn:ihe:iti:xds:2017:mimeTypeSufficient"

1764 [**<=**]

1765 *Hinweis: Die Ablage der Dokumente ist gemäß der Vorgaben aus IG-EPA89078Y44-* zu*
1766 *protokollieren.*

1767 *Hinweis: Dokumente müssen nicht erstellt werden, wenn diese keine Einträge enthalten*
1768 *("empty list").*

1769

1770

1771

1772 **3.2 Sichere Speicherung sensibler Schlüssel und Informationen im**
1773 **VAU-HSM**

1774 Im Folgenden wird beschrieben, welche Informationen in einem HSM (als VAU-HSM
1775 bezeichnet) zu speichern sind.

1776 Verständnishinweis: Die HMAC-Schlüssel (symmetrische Schlüssel) für die Prüfung der
1777 VSDM+-Prüfnachweise [gemSpec_SST_FD_VSDM] werden von den VSDM-Betreibern

1778 erzeugt und für die ePA-VAUs der ePA-Betreiber verschlüsselt exportiert. Die Schlüssel
1779 sowie die Export-/Import-Vorgänge (Mehr-Augen-Prinzip) sind die gleichen wie sie auch
1780 für die E-Rezept-VAU verwendet werden.

1781 **A_24611-10 -ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und**
1782 **Informationen für VAU-Betrieb**

1783 Das ePA-Aktensystem MUSS sicherstellen, dass folgende, für den Betrieb der VAU
1784 notwendigen Schlüssel und Informationen in einem HSM (als VAU-HSM bezeichnet)
1785 gespeichert werden:

- 1786 • privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
1787 (u.a. genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- 1788 • ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- 1789 • ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- 1790 • privater Schlüssel der Verschlüsselungsidentität der VAU
- 1791 • privater Schlüssel der Signaturidentität der VAU
- 1792 • Paare (kid, C.ZD.SIG) für die Zertifikate C.ZD.SIG mit professionOID `oid_popp-`
1793 `token` für die aktuelle Token-Signatur-Identität des PoPP-Services und ggf. die
1794 vorherige Token-Signatur-Identität des PoPP-Services. Der Wert kid für ein
1795 Zertifikat C.ZD.SIG ergibt sich aus dem JWK-Set, welches der PoPP-Service
1796 veröffentlicht.
- 1797 • Masterkeys für die Ableitung der versichertenindividuellen
1798 Datenpersistierungsschlüssel
- 1799 • Masterkeys für die Ableitung der versichertenindividuellen
1800 Befugnispersistierungsschlüssel
- 1801 • symmetrische Schlüssel für die HMAC-Prüfung der VSDM-Prüfziffern (jeweils einen
1802 pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als
1803 gemeinsames Geheimnis bezeichnet werden.
- 1804 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- 1805 • Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für
1806 die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf.
1807 für Service-VAUs)
- 1808 • Paare (sn, Root-Zertifikat) für das aktuelle und das vorherige (sofern nicht
1809 kompromittiert) Root-Zertifikat (Vertrauensanker) für die Prüfung der Signatur
1810 von ITSG-Token. Der Identifier sn bezeichnet die Seriennummer des Root-
1811 Zertifikats,
- 1812 • Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

1813 **[<=]**

1814 Hinweis:

1815 Es gelten die Anforderungen aus [gemSpec_Krypt#3.20 VSDM-Prüfziffer Version 2] für
1816 ein ePA-Aktensystem in der Rolle "Prüfziffer Version 2 prüfendes System". Aus den ins
1817 HSM importierten gemeinsamen Geheimnissen erfolgt im HSM eine Schlüsselableitung
1818 (A_27299-*) der für die Entschlüsselung der Prüfziffer Version 2 benötigten AES/GCM-
1819 Schlüssel.

1820 Hinweis: Das ITSG-Trust Center veröffentlicht die Root-Zertifikate für die Prüfung von
1821 Signaturen der ITSG-Token unter: [https://www.itsg.de/produkte/trust-](https://www.itsg.de/produkte/trust-center/oeffentliche-zertifikate-und-verzeichnisse/)
1822 [center/oeffentliche-zertifikate-und-verzeichnisse/](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. [$\leq$]

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. [$\leq$]

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).

[$\leq$]

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 Vorgängertzertifikat. 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 Zertifikat 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. [$\leq$]

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. [$\leq$]

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.

[$\leq$]

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

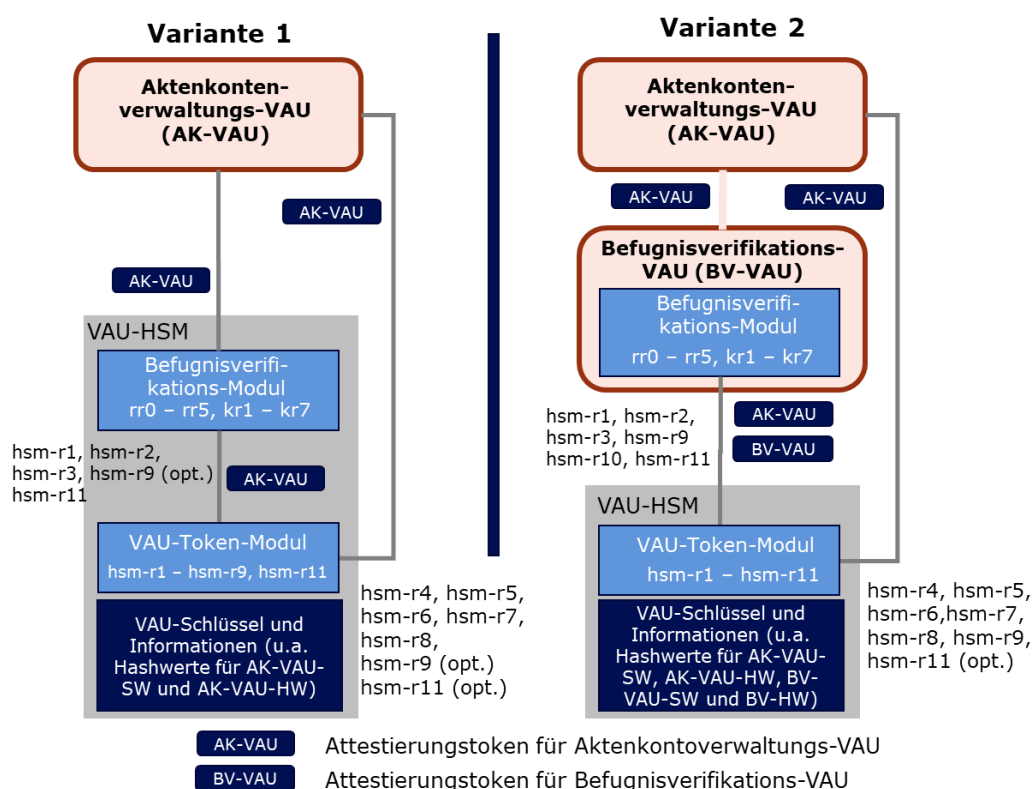


Abbildung 2: Alternativen zur Ausführung des Befugnisverifikations-Moduls

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. [<=]

- 1979 **A_24574 -ePA-Aktensystem - Befugnisverifikations-Modul im HSM oder**
 1980 **Befugnisverifikations-VAU**
 1981 Das ePA-Aktensystem MUSS sicherstellen, dass ein Befugnisverifikations-Modul
 1982 ausschließlich in einem VAU-HSM oder in einer Befugnisverifikations-VAU ausgeführt
 1983 wird. [<=]
- 1984 **A_25050 -ePA-Aktensystem - 1:1-Beziehung zwischen Befugnisverifikations-**
 1985 **VAU und Aktenkontoverwaltungs-VAU**
 1986 Das ePA-Aktensystem MUSS sicherstellen, dass eine 1:1-Beziehung zwischen einer
 1987 Instanz einer Befugnisverifikations-VAU und einer Instanz einer Aktenkontoverwaltungs-
 1988 VAU gibt. [<=]
- 1989 **3.3.1 VAU-Token-Modul**
- 1990 Dieser Abschnitt enthält die Regeln zum Zugriff auf die Schlüssel im VAU-HSM. Diese
 1991 werden von einem Befugnisverifikations-Modul genutzt.
- 1992 **A_24712-01 -ePA-Aktensystem - VAU-Token-Modul nur durch**
 1993 **Befugnisverifikations-Modul oder Aktenkontoverwaltungs-VAU aufrufbar**
 1994 Das ePA-Aktensystem MUSS sicherstellen, dass die Regeln hsm-r1 bis hsm-r3 des VAU-
 1995 Token-Moduls ausschließlich von einem Befugnisverifikations-Modul und die Regeln hsm-
 1996 r4 bis hsm-r7 ausschließlich von einer Aktenkontoverwaltungs-VAU aufgerufen
 1997 werden. [<=]
- 1998 **A_25282-07 -ePA-Aktensystem - Regeln des VAU-Token-Moduls**
 1999 Das VAU-Token-Modul MUSS die in Tabelle *Tab_AS_VAU_Token_Modul_Rules-07*
 2000 definierten Regeln umsetzen. [<=]
 2001

2002

Tabelle 4: Tab_AS_VAU_Token_Modul_Rules-07 -Prüfregeln VAU Token

Regel	Beschreibung
hsm-r1	<i>Diese Regel dient zur Sicherung von Befugnissen und HSM-ID-Token mittels CMAC.</i> 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.

Regel	Beschreibung
hsm-r2	<i>Diese Regel dient zur Ableitung der versichertenindividuellen Persistierungsschlüssel</i> 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.

Regel	Beschreibung
hsm-r3	<i>Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfziffern der Version 1 oder der Entschlüsselung der VSDM-Prüfziffern der Version 2</i> 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.

Regel	Beschreibung
hsm-r4	<i>Diese Regel dient zur Nutzung der privaten Schlüssel der AUT-Identitäten der VAU</i> 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 Signatur des 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.

Regel	Beschreibung
hsm-r5	<i>Diese Regel dient zur Nutzung des privaten Schlüssels der ENC-Identität der VAU</i> 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 Signatur des 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	<i>Diese Regel dient zur Nutzung des privaten Schlüssels der Signaturidentität der VAU</i> 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 Signatur des 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 privaten Schlüssel der Signaturidentität der VAU signiert.

Regel	Beschreibung
hsm-r7	<weggefallen>

Regel	Beschreibung
hsm-r8	<i>Diese Regel dient zum Ableiten von symmetrischen Schlüsseln für die Ver- bzw. Entschlüsselung von Daten</i> Sie dient bspw. dazu, sogenannte Submissions für die Datenausleitung an das Forschungsdatenzentrum Gesundheit (FDZ) nach § 363 Absatz 1 SGB V außerhalb der VAU im Aktensystem zwischenspeichern, bis das Forschungsdatenzentrum diese Submissions abholt. Die Submissions sind dann über die über diese Regel abgeleiteten symmetrischen Schlüssel außerhalb der VAU kryptographisch gesichert. 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.

Regel	Beschreibung
hsm-r9 (opt.)	<i>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.</i> 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 <i>kid</i> gespeichert ist Falls die Prüfungen 1) - 4) erfolgreich waren, wird (kid, C.ZD.SIG) zurückgeliefert.

hsm-r10 (opt.)	<i>Diese Regel dient in Regel kr6 zum Ableiten der Schlüssel <code>dataStorageKey</code> und <code>userSessionKey</code>. Die Regel <code>hsm-r10</code> 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.</i> 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 <code>dvector</code> • optional: Eingabezeitpunkt <code>EZ</code> als Unix-Zeit (natürliche Zahl) Ausgangsdaten: • <code>dataStorageKey</code> • <code>userSessionKey</code> • Ableitungszeitpunkt <code>AZ</code>(Unix-Zeit) • Label des genutzten Datenpersistierungs-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 <code>EZ</code> in den Eingangsdaten enthalten und <code>current_time</code> der aktuelle Zeitpunkt im VAU-HSM in Unix-Zeit ist, prüfen, ob $current\_time - (2*24*60*60) \leq EZ \leq current\_time$ 4. prüfen, ob das Label des Masterkeys zu einem Datenpersistierungs-Masterkey gehört Falls alle Prüfungen erfolgreich waren, werden <code>dataStorageKey</code> und <code>userSessionKey</code> wie folgt abgeleitet: <u><code>dataStorageKey</code></u>:Ableitung eines AES-Schlüssels [FIPS-197] <code>dataStorageKey</code> 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 <code>dvector</code> + <code>AZ</code>, wobei <code>AZ=EZ</code>, falls ein Eingabezeitpunkt in den Eingangsdaten enthalten ist, und ansonsten <code>AZ = current_time</code>, d.h. der aktuelle Zeitpunkt im VAU-HSM in Unix-Zeit, <u><code>userSessionKey</code></u>: Ableitung eines AES-Schlüssels [FIPS-197] <code>userSessionKey</code> mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren auf Basis des in den Eingangsdaten angegebenen
----------------	---

Regel	Beschreibung
	Datenpersistierungs-Masterkeys und dem Ableitungsvektor "usk:" + Akten-ID + <i>dataStorageKey</i>. Ausgangsdaten sind der abgeleitete Schlüssel <i>dataStorageKey</i>, <i>userSessionKey</i>, der genutzte Ableitungszeitpunkt AZ in Unix-Zeit und das Label des für die Ableitung genutzten Datenpersisierungs-Masterkeys.
hsm-r11	<i>Diese Regel dient zum Auslesen eines Root-Zertifikats, welches zur Prüfung der Signatur von ITSG-Token genutzt wird.</i> 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 Prüfungen 1) - 3) erfolgreich waren, wird (sn, Root-Zertifikat) mit dem Root-Zertifikat zur Prüfung von Signaturen von ITSG-Token mit der Zertifikatsseriennummer <i>sn</i> zurückgeliefert.

2003

2004 **A_24667 -ePA-Aktensystem -VAU-HSM - Prüfen des VAU-Attestierungstokens**
 2005 Das VAU-HSM MUSS bei der Prüfung eines VAU-Attestierungstokens sicherstellen, dass
 2006 dieses zeitlich gültig ist und Replay-Attacken abwehren. [<=]

2007 **A_26303 -ePA-Aktensystem - Abgeleitete Verschlüsselungsschlüssel sind**
 2008 **ausschließlich einer VAU zugänglich**

2009 Das ePA-Aktensystem MUSS sicherstellen, dass ein mit Regel hsm-r8 abgeleiteter
 2010 Schlüssel ausschließlich einer VAU zugänglich ist und ausschließlich mittels AES/GCM
 2011 analog [gemSpec_Krypt#GS-A_4389] verwendet wird. [<=]

2012 3.3.2 Regeln des Befugnisverifikations-Moduls

2013 Die folgende Tabelle zeigt die Regeln des Befugnisverifikations-Moduls im Überblick.

2014 **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.	<i>Tab_AS_Entitlement_Registration_Rules</i>
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.	<i>Tab_AS_Entitlement_Registration_Rules</i>
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 Signaturdienst signiert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
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.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr4	Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der Anlage eines Aktenkontos im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr5	Mit dieser Regel werden die Befugnisse bei einem betreiberübergreifenden Anbieterwechsel im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
kr1	Diese Regel wird für die Anmeldung des Aktenkontoinhabers genutzt.	<i>Tab_AS_SDS-Key_Rules</i>
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.	<i>Tab_AS_SDS-Key_Rules</i>

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
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.	<i>Tab_AS_SDS-Key_Rules</i>
kr4	Diese Regel wird für die Anmeldung des E-Rezept-Fachdienstes verwendet.	<i>Tab_AS_SDS-Key_Rules</i>
kr5	<weggefallen>	
kr6	Diese Regel wird für das Einfrieren und Auftauen von Daten genutzt.	<i>Tab_AS_SDS-Key_Rules</i>
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.	<i>Tab_AS_SDS-Key_Rules</i>

2015

2016 **A_24573-07 -ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls**
 2017 Das Befugnisverifikations-Modul MUSS die in den
 2018 Tabellen *Tab_AS_Entitlement_Registration_Rules-07* und *Tab_AS_SDS-Key_Rules-07*
 2019 definierten Regeln umsetzen.[<=]

2020
2021**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	<i>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.</i> 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-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> 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 <code>hsm-r1</code> 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 <code>oid_idpd_sek</code> 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 <code>oid_versicherter</code> 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 ($iat - 15s \leq \text{aktuelle Zeit} \leq exp + 15s$) 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:
-----	---

Regel	Beschreibung
	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	<i>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 Signatordienst signiert.</i> 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 <code>oid_idpd_sek</code> 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 <code>hsm-r1</code> 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 <code>oid_idpd_sek</code> 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 <code>oid_versicherter</code> 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
-----	---

Regel	Beschreibung
	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 ($i_{at} - 15s \leq \text{aktuelle Zeit} \leq e_{exp} + 15s$) 3. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis3 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 Leistungserbringenumgebung 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: <u>Szenario VSDM-Prüfziffer in Version 2:</u> Falls <code>enforce_popp_only = true</code>, 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 HSM**bis 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 ($\text{PoPP-Token.iat} - 30s \leq \text{aktuelle Zeit} < \text{PoPP-Token.iat} + 2 \text{ Tage} + 15s$, 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 $\text{PoPP-Token.iat} + \text{maxEntitlementValidity}$, 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

Regel	Beschreibung
	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	<i>Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der Anlage eines Aktenkontos im Aktensystem registriert.</i> 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 <code>oid_kostentraeger</code> bzw. <code>oid_ombudsstelle</code> 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 <code>hsm-r1</code> 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.

Regel	Beschreibung
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: - Prüfen der Befugnis1 - prüfen der Signatur gemäß A_25042-* (C.FD.SIG) - prüfen, ob im Signaturzertifikat C.FD.SIG der professionOIDoid_epa_vauist - prüfen, dass das Signaturzertifikat C.FD.SIG nicht auf das importierende Aktensystem ausgestellt ist. - Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 mit den Inhalten aus Befugnis1 erstellt. - Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 - Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. - Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

2022

2023

2024

2025

2026

A_24690-01 -ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen des ID-Tokens

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

2027

2028

2029

- das ID-Token muss gemäß A_25042-* valide signiert sein durch einen sektoralen Identity Provider oder den IDP-Dienst (professionOID ist oid_idpd_sek oder oid_idpd),

2030

- das ID-Token muss zeitlich gültig sein (Felder: iat, exp),

2031

- das ID-Token muss im Feld aud das ePA-Aktensystem eingetragen haben.

2032

[<=]

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.

2049
2050**Tabelle 7: Tab_AS_SDS-Key_Rules Key Rules-07 - Regeln zur Ableitung der versichertenindividuellen Persistierungsschlüssel**

Regel	Beschreibung
kr1	<i>Diese Regel wird für die Anmeldung des Aktenkontoinhabers genutzt.</i> 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 <code>oid_idpd_sek</code> ist oder prüfen des HSM-ID-Tokens b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel <code>hsm-r1</code> 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 <code>oid_idpd_sek</code> ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel <code>hsm-r2</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVN-R aus dem ID-Token und den Labeln der zu verwendenden Befugnispersistierungs- und Datenpersistierungs-Masterkeys zur Ableitung von Befugnis- und Datenpersistierungsschlüssel aufgerufen. 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.

Regel	Beschreibung
kr2	<i>Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssel genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.</i> 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 Befugnispersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.

kr3	<i>Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.</i> 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-Token bzw. 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.
-----	--

Regel	Beschreibung
	4. Das Befugnisverifikations-Modul liefert den abgeleiteten Datenpersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.
kr4	<i>Diese Regel wird für die Anmeldung des E-Rezept-Fachdienstes verwendet.</i> 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 <code>oid_erp-vau</code> ist 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 <code>hsm-r1</code> 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 <code>oid_erp-vau</code> ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel <code>hsm-r2</code> 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 <i>dataStorageKey</i> • symmetrischer Schlüssel <i>userSessionKey</i> • Ableitungszeitpunkt AZ(Unix-Zeit) • Label des genutzten Datenpersistierungs-Masterkeys Prüfschritte: Falls das Befugnisverifikationsmodul im VAU-HSM und nicht in einer Befugnisverifikations-VAU umgesetzt wird 1. prüfen der Signatur des VAU-Attestierungstokens und dass es ein Attestierungstoken einer AK-VAU ist (herstellerspezifisch) 2. ist ein Eingabezeitpunkt EZ in den Eingangsdaten enthalten und <i>current_time</i> der aktuelle Zeitpunkt im VAU-HSM in Unix-Zeit, prüfe, ob $current\_time - (2*24*60*60) \leq EZ \leq current\_time$. Falls alle Prüfungen erfolgreich waren: <u>Variante: Befugnisverifikationsmodul wird im VAU-HSM umgesetzt</u> 1. Ableitung eines AES-Schlüssels [FIPS-197] <i>dataStorageKey</i> 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 = <i>current_time</i>, d.h. der aktuelle Zeitpunkt im VAU-HSM in Unix-Zeit, 2. Ableitung eines AES-Schlüssels [FIPS-197] <i>userSessionKey</i> 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 + <i>dataStorageKey</i>. <u>Variante: Befugnisverifikationsmodul wird in einer Befugnisverifikations-VAU umgesetzt</u>
---------------	--

Regel	Beschreibung
	1. Ableitung der Schlüssel <i>dataStorageKey</i> und <i>userSessionKey</i> 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 <i>dataStorageKey</i>, <i>userSessionKey</i>, der genutzte Ableitungszeitpunkt AZ in Unix-Zeit und das Label des für die Ableitung genutzten Datenpersisierungs-Masterkeys.

Regel	Beschreibung
kr7	<i>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.</i> 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 <i>hsm-r11</i> 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 <i>hsm-r11</i> 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 <i>hsm-r2</i> 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.

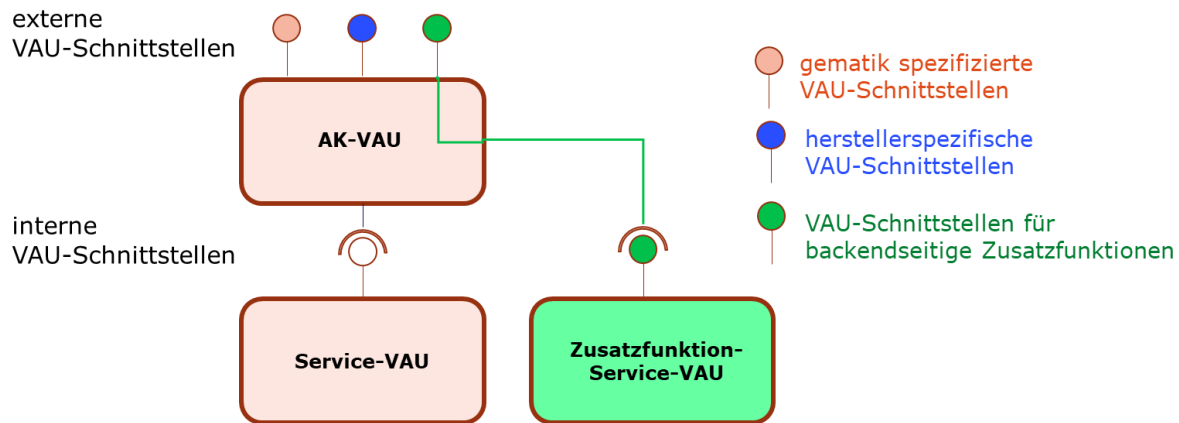


Abbildung 3 - Typen von VAU-Schnittstellen

Externe VAU-Schnittstellen sind VAU-Schnittstellen, die von Client-Systemen aufgerufen werden können, die sich außerhalb einer VAU-Instanz des ePA-Aktensystems befinden. Aus Sicht der VAU-Instanzen 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-Schnittstellen sind 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,

- 2125 • dem Produktgutachter dafür eine aktuelle und ausreichend detaillierte Liste
2126 sämtlicher Schnittstellen zur Verfügung gestellt werden

2127 [**<=**]

2128 Hinweis zu A_28805-*: Im Produktgutachten sind die VAU-Schnittstellen durch den
2129 Produktgutachter so zu dokumentieren, dass deren Zweck und die verarbeiteten Daten
2130 daraus hervorgehen. Dies bezieht sich sowohl auf Aktenkontoverwaltungs- als auch
2131 Service-VAUs.

2132 **A_28888 -ePA-Aktensystem - Herstellerspezifische VAU-Schnittstellen**
2133 **ausschließlich für den Betreiber oder Kostenträger**

2134 Der Hersteller des ePA-Aktensystems MUSS technisch sicherstellen, dass
2135 herstellerepezifische VAU-Schnittstellen ausschließlich für den Betreiber des ePA-
2136 Aktensystems oder für Kostenträger nutzbar sind. [**<=**]

2137 **A_28916 -ePA-Aktensystem - Eigene VAU-Instanz für Betreiberzugriffe**

2138 Das ePA-Aktensystem MUSS sicherstellen, dass ein Betreiber ausschließlich über
2139 herstellerepezifische VAU- Schnittstellen auf eine VAU-Instanz zugreifen kann, in der
2140 keine unverschlüsselten Daten nach A_25716-* verarbeitet werden. Dies bedeutet, dass
2141 Betreiber für administrative Funktionen eine eigene VAU-Instanz nutzen müssen. [**<=**]

2142 **A_28807 -ePA-Aktensystem - Aktensystem-Schnittstellen gewährleisten**
2143 **technischen Ausschluss des Betreibers**

2144 Das ePA-Aktensystem MUSS technisch ausschließen, dass dem Betreiber des ePA-
2145 Aktensystems über eine Schnittstelle des ePA-Aktensystems (VAU- oder Nicht-VAU-
2146 Schnittstelle) Daten offenbart werden oder der Betreiber auf entschlüsselte Daten
2147 zugreifen kann, die durch die VAU zu schützen sind, sofern dies nicht durch andere
2148 gematik-Anforderungen erlaubt wird. [**<=**]

2149 **A_28855 -ePA-Aktensystem - Zulässigkeit von Aktensystem-Schnittstellen für**
2150 **Kostenträger**

2151 Falls das ePA-Aktensystem dem Kostenträger eine Schnittstelle (VAU- oder Nicht-VAU-
2152 Schnittstelle) anbietet, MUSS das ePA-Aktensystem technisch ausschließen, dass dem
2153 Kostenträger über diese Schnittstelle Daten offenbart werden oder der Kostenträger
2154 Daten entschlüsseln kann, die durch die VAU zu schützen sind, sofern dies nicht durch
2155 andere gematik-Anforderungen erlaubt wird. [**<=**]

2156 Hinweis zu A_28807-* und A_28855-*: Die durch die VAU zu schützenden Daten sind
2157 alle Daten der in der VAU laufenden Services nach A_25716-*. Die Anforderungen des
2158 Abschnitts "Logging und Monitoring" sind ein Beispiel für gematik-Anforderungen, die
2159 dem Betreiber des ePA-Aktensystems in gewissem Rahmen erlauben, durch die VAU zu
2160 schützende Daten zu protokollieren. Ein weiteres Beispiel ist die Schnittstelle des
2161 Betreibers zum Auftauen von Daten gemäß Abschnitt 3.5.5.

2162 **A_28856 -ePA-Aktensystem - Aktensystem-Schnittstelle für Kostenträger zu**
2163 **administrativen Zwecken**

2164 Das ePA-Aktensystem KANN dem Kostenträger eine (VAU-)Schnittstelle anbieten, über
2165 die der Kostenträger administrative Informationen zu den vom Kostenträger
2166 verantworteten Akten erhalten kann, z.B. aktenübergreifende Statistiken zur
2167 Aktennutzung oder das letzte Nutzungsdatum einer Akte. [**<=**]

2168 In den folgenden Abschnitten werden zunächst die Anforderungen an eine VAU
2169 beschrieben, die sowohl von einer Aktenkontoverwaltungs-VAU als auch
2170 einer Befugnisverifikations-VAU zu erfüllen sind. Die speziellen Anforderungen an eine
2171 Aktenkontoverwaltungs-VAU bzw. an eine Befugnisverifikations-VAU folgen darauf in
2172 separaten Abschnitten.

2173 3.4.1 Übergreifende VAU-Anforderungen

2174 3.4.1.1 Schutz der Integrität der VAU

2175 Die folgenden Anforderungen stellen die Integrität der VAU sicher.

2176 **A_24613 -ePA-Aktensystem - Bildung Hashwertrepräsentation des VAU-Images**

2177 Der Hersteller des VAU-Images MUSS für seine zugelassenen VAU-Images
2178 Hashwertrepräsentationen bilden. Diese MÜSSEN signiert und die signierten
2179 Hashwertrepräsentationen an die gematik übermitteln. Dabei SOLLEN bezüglich der
2180 kryptographischen Vorgaben zur Signatur die Vorgaben aus [gemSpec_Krypt]
2181 eingehalten werden. [≤]

2182 Erläuterung zu A_24613-*:

2183 Bei Intel-SGX sind die durch die Intel-Hardware erzeugten Signaturen RSA-3072-Bit-
2184 Signaturen, bei denen der öffentliche Exponent 3 ist. Dies entspricht nicht den Vorgaben
2185 in [gemSpec_Krypt] für allgemeine RSA-Signaturen (also nicht im SGX-Kontext). Deshalb
2186 steht in A_24613-* diesbezüglich nur eine SOLL-Formulierung. Im Kontext SGX ist der
2187 öffentliche RSA-Exponent 3 zulässig.

2188 **A_24642 -ePA-Aktensystem - Ausschluss von Manipulationen an der Hardware der VAU**

2189 Die VAU MUSS die Integrität der eingesetzten Hardware schützen und damit
2190 insbesondere Manipulationen an der Hardware durch den Betreiber des ePA-
2191 Aktensystems ausschließen. [≤]

2193 **A_24616 -ePA-Aktensystem - Attestierung des VAU-Images und der VAU-Hardware beim Start**

2194 Das ePA-Aktensystem MUSS beim Start einer VAU das genutzte VAU-Image sowie die
2195 VAU-Hardware, auf der die VAU ausgeführt werden soll, kryptographisch attestieren und
2196 ein signiertes VAU-Attestierungstoken erzeugen, welches vom VAU-HSM geprüft werden
2197 kann. [≤]

2199 **A_24684 -ePA-Aktensystem - Hardwarebasierter Vertrauensanker für Attestierung der VAU**

2200 Das ePA-Aktensystem MUSS sicherstellen, dass der kryptographische Vertrauensanker
2201 für die Attestierung des VAU-Images und der VAU-Hardware in einem hardwarebasierten
2202 sicheren Schlüsselspeicher gesichert ist. [≤]

2204 **A_24617 -ePA-Aktensystem - Betreiberunabhängiger Vertrauensanker für Attestierung der VAU**

2205 Das ePA-Aktensystem MUSS sicherstellen, dass der kryptographische Vertrauensanker
2206 für die Attestierung des VAU-Images und der VAU-Hardware nicht in der Hoheit des
2207 Betreibers des Aktensystems liegt. [≤]

2209 *Hinweis zu A_24617: Mit der Anforderung soll die Bedrohung abgewehrt werden, dass*
2210 *sich einzelne Innentäter beim Betreiber des ePA-Aktensystems eigene VAU-Software oder*
2211 *VAU-Hardware mit Schwachstellen erstellen und sich für diese einen falschen Hashwert*
2212 *attestieren, der dem VAU-HSM bekannt ist.*

2213 **A_24620 -ePA-Aktensystem - Attestierung durch Systeme außerhalb der VAU zur Laufzeit**

2214 Das ePA-Aktensystem MUSS technisch ermöglichen, dass Änderungen an der VAU-
2215 Software und der VAU-Hardware während der Laufzeit durch Systeme außerhalb der VAU
2216 automatisiert geprüft werden können. [≤]

2218 *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. [$\leq$]

A_24638 -ePA-Aktensystem - Schutz der Daten vor physischem Zugang zu Systemen der VAU

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

A_24651 -ePA-Aktensystem - Betreiber ergreift Maßnahmen gegen physische Angriffe auf die VAU

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

A_24641 -ePA-Aktensystem - Löschen aller Daten beim Beenden einer VAU-Instanz

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

A_25244 -ePA-Aktensystem - x-insurantId nicht außerhalb des VAU-Kanals

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

3.4.1.3 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. [$\leq$]

Hinweise zu A_26314:

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

A_26322 -ePA-Aktensystem - Unterschiedliche Schlüssel für die Verschlüsselung von außerhalb der VAU gespeicherten Daten bei unterschiedlichen Verarbeitungszwecken

Falls Daten außerhalb der VAU im System des Aktensystembetreibers gespeichert werden, MUSS das ePA-Aktensystem sicherstellen, dass für die Verschlüsselung von

2267 Daten, die zu unterschiedlichen Zwecken verarbeitet werden, unterschiedliche
2268 Verschlüsselungsschlüssel genutzt werden. [≤]

2269 Hinweis zu A_26322: Verarbeitungszwecke für Daten sind beispielsweise die
2270 Verarbeitung von Daten zum Zwecke der Sekundärnutzung (sieheData Submission
2271 Service) oder die Verarbeitung von Daten für die Nutzerverwaltung im Aktensystem
2272 (insbesondere Geräteinformationen und E-Mail-Adressen).

2273 **3.4.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM**

2274 **A_24653 -ePA-Aktensystem - Sichere Verbindung zwischen VAU und VAU-HSM**
2275 Das ePA-Aktensystem MUSS technisch sicherstellen, dass zwischen einer VAU und einem
2276 VAU-HSM eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die
2277 vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des
2278 Betreibers des Aktensystems schützen. [≤]

2279 **3.4.1.5 Logging und Monitoring**

2280 Hinweis: Die Anforderungen dieses Abschnitts könnten sich noch ändern, falls sich bei
2281 der Umsetzung des ePA-Aktensystems herausstellt, dass weitere Protokollierungen auf
2282 Seiten des Betreibers notwendig werden.

2283 **A_24910 -ePA-Aktensystem - Erlaubte Zwecke der Betreiberprotokolle**
2284 Der Betreiber des Aktensystems MUSS sicherstellen, dass die durch die VAU für den
2285 Betrieb erstellten Protokolle des Betreibers ausschließlich zum Zwecke der Fehleranalyse
2286 und -behebung anlassbezogen sowie zum Zwecke des Security Monitorings verwendet
2287 werden. [≤]

2288 **A_24649 -ePA-Aktensystem - Datenschutzkonformes Logging und Monitoring der VAU**

2289 Die VAU MUSS die für den Betrieb des ePA-Aktensystems erforderlichen Logging- und
2290 Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit
2291 technischen Mitteln ausgeschlossen ist, dass dem Betreiber des ePA-Aktensystems
2292 vertrauliche oder zur unautorisierten Profilbildung geeignete Daten zur Kenntnis
2293 gelangen. [≤]

2295 **A_24695 -ePA-Aktensystem - Keine medizinische Informationen in VAU-Protokollen des Betreibers**

2296 Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten
2297 Protokollen des Betreibers keine personenbezogenen medizinischen Informationen
2298 enthalten sind (u. a. medizinische Daten von Versicherten oder Informationen, aus denen
2299 sich ableiten lässt, bei welchen Leistungserbringerinstitutionen ein Versicherter in
2300 Behandlung ist).
2301 [≤]
2302

2303 **A_24909 -ePA-Aktensystem - Nicht KVNR und Telematik-ID gemeinsam protokollieren**

2304 Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten
2305 Protokollen des Betreibers höchstens die KVNR oder höchstens die Telematik-ID
2306 enthalten ist, aber nicht eine Kombination aus KVNR und Telematik-ID und keine solche
2307 Verbindung über mehrere Protokolle hergestellt werden kann. [≤]
2308

2309 **A_24719 -ePA-Aktensystem - Kein kryptographisches Schlüsselmaterial in VAU-Protokollen des Betreibers**

2310 Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten
2311 Protokollen des Betreibers kein kryptographisches Schlüsselmaterial enthalten ist. [≤]
2312

A_24911 -Löschfristen Protokolle

Das ePA-Aktensystem MUSS sicherstellen, dass die

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

[<=]

A_26316 -Anbieter ePA-Aktensystem - Schutz der Protokolle des Betreibers

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

gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik

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

A_27333 -ePA-Aktensystem - Geheimer Schlüssel für Pseudonymisierung der gematik-Logdaten nur in VAU

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

A_27336 -ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung im 4-Augen-Prinzip

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

A_27334 -ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung der gematik-Logdaten im 4-Augen-Prinzip

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

A_27335 -ePA-Aktensystem - Wechsel des Schlüssels für Pseudonymisierung der gematik-Logdaten

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

3.4.2 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.*

2403 **A_25231 -ePA-Aktensystem - Schließen des Health Record Context beim**
2404 **Beenden einer User Session**

2405 Die VAU MUSS sicherstellen, dass beim Beenden einer User Session alle mit dieser User
2406 Session verknüpften Health Record Context beendet werden, wenn der jeweilige Health
2407 Record Context nicht mit mindestens einer weiteren User Session verknüpft ist. [<=]

2408 **A_25051 -ePA-Aktensystem - VAU-Kanal endet immer in einer**
2409 **Aktenkontoverwaltungs-VAU**

2410 Die VAU MUSS sicherstellen, dass ein VAU-Kanal von einem Client der ePA (ePA-Client
2411 oder ePA-FdV) ausschließlich in einer Aktenkontoverwaltungs-VAU endet. [<=]

2412 Hinweis: Der VAU-Kanal darf z.B. nicht in einer Befugnisverifikations-VAU enden.

2413 **3.4.2.2 Schutz der Daten bei Speicherung außerhalb der**
2414 **Aktenkontoverwaltungs-VAU**

2415 Die folgenden Anforderungen gewährleisten den Schutz der beim Betreiber des ePA-
2416 Aktensystems persistierten Daten von Aktenkonten. Die Verschlüsselung der Daten eines
2417 Versicherten erfolgt mit seinem versichertenindividuellen Daten- und
2418 Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel sind
2419 in [gemSpec_Krypt#3.15.2] festgelegt.

2420 **A_24643 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**
2421 **gespeicherten Daten mit dem Datenpersistierungsschlüssel**

2422 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten

- 2423 1. Daten des FHIR-Data Service
2424 2. Daten des XDS Document Service
2425 3. Daten des Audit Event Service (Protokolle für den Versicherten zum Zwecke der
2426 Datenschutzkontrolle)
2427 4. Daten des Constraint Managements (Policies zu verborgenen Daten)
2428 5. Daten des Consent Managements (Widersprüche des Versicherten)

2429 vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb
2430 des Health Record Context mit dem zum Health Record gehörenden
2431 versichertenindividuellen Datenpersistierungsschlüssel verschlüsselt werden.
2432 [<=]

2433 **A_24644 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**
2434 **gespeicherten Befugnissen mit dem Befugnispersistierungsschlüssel**

2435 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten
2436 Daten des Entitlement Managements, d. h. Befugnisse und Befugnisverbote, vor der
2437 Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health
2438 Record Context mit dem zum Health Record gehörenden versichertenindividuellen
2439 Befugnispersistierungsschlüssel verschlüsselt werden. [<=]

2440 **3.4.2.3 Konsistenz des Systemzustands**

2441 **A_24650 -ePA-Aktensystem - Konsistenter Systemzustand eines Health Record**
2442 **Context**

2443 Die VAU MUSS sicherstellen, dass ein konsistenter Zustand eines Health Record Context
2444 auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw.
2445 wiederhergestellt werden kann. [<=]

2446 **A_24696 -ePA-Aktensystem - Konsistenz bei parallelen Zugriffen**
2447 Die VAU MUSS auch bei parallelen Zugriffen auf dasselbe Aktenkonto durch mehrere
2448 Nutzer immer einen konsistenten Zustand des Aktenkontos gewährleisten.[<=]

2449 **3.4.3 Zusätzliche Anforderungen an eine Befugnisverifikations-** 2450 **VAU**

2451 Eine Befugnisverifikations-VAU ist eine spezielle VAU, in der ausschließlich das
2452 Befugnisverifikations-Modul ausgeführt wird.

2453 **A_24646 -ePA-Aktensystem - Befugnisverifikations-VAU verarbeitet** 2454 **ausschließlich ein Befugnisverifikations-Modul**

2455 Das ePA-Aktensystem MUSS sicherstellen, dass in einer Befugnisverifikations-VAU
2456 ausschließlich ein Befugnisverifikations-Modul ausgeführt wird.[<=]

2457 **A_24647 -ePA-Aktensystem - Befugnisverifikations-VAU speichert keine Daten**

2458 Eine Befugnisverifikations-VAU DARF die Daten, die sie im Rahmen der Regeln des
2459 Befugnisverifikations-Moduls verarbeitet, NICHT außerhalb der Befugnisverifikations-VAU
2460 speichern.[<=]

2461 Eine Befugnisverifikations-VAU darf insbesondere die vom VAU-HSM abgeleiteten
2462 versichertenindividuellen Persistierungsschlüssel nicht speichern.

2463 **A_24648 -ePA-Aktensystem - Befugnisverifikations-VAU löscht Daten nach** 2464 **Regelbearbeitung**

2465 Eine Befugnisverifikations-VAU MUSS sämtliche Daten, die sie im Rahmen eines
2466 Regelaufrufs des Befugnisverifikations-Moduls verarbeitet, sofort nach Abarbeitung der
2467 Regel sicher aus der Befugnisverifikations-VAU löschen bzw. einen Zugriff auf diese
2468 Daten technisch ausschließen.[<=]

2469 **A_24671 -ePA-Aktensystem - Sichere Verbindung zwischen VAU-Instanzen**

2470 Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer VAU-Instanz einer
2471 Befugnisverifikations-VAU und einer VAU-Instanz einer Aktenkontoverwaltungs-VAU eine
2472 beidseitig authentifizierte und vertrauliche Verbindung besteht. Die vertrauliche
2473 Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des
2474 Aktensystems schützen.[<=]

2475 **A_24856 -ePA-Aktensystem - Private Authentisierungsschlüssel für sichere** 2476 **Verbindung zwischen VAU-Instanzen**

2477 Das ePA-Aktensystem MUSS sicherstellen, dass sich die VAU-Instanzen bei einer
2478 Verbindung zwischen einer VAU-Instanz einer Befugnisverifikations-VAU und einer VAU-
2479 Instanz einer Aktenkontoverwaltungs-VAU mit privaten Schlüsseln authentisieren, die
2480 ausschließlich über die jeweilige VAU-Instanz nutzbar sind.[<=]

2481 **3.4.4 Zusätzliche Anforderungen an eine Service-VAU**

2482 Spezielle Funktionen der "ePA für alle" können in eigenen, von den
2483 Aktenkontoverwaltungs-VAUs (AK-VAU) getrennten, VAUs ausgelagert und ausgeführt
2484 werden. Diese VAUs werden als **Service-VAUs** bezeichnet. Es kann Service-VAUs für
2485 unterschiedliche Funktionen geben, so dass es dementsprechend unterschiedliche **Typen**
2486 **von Service-VAUs** geben kann.

2487 Service-VAU-Instanzen können durch den Betreiber des Aktensystems gestartet und in
2488 einem Pool verwaltet werden. AK-VAU-Instanzen können bei Bedarf auf Service-VAU-
2489 Instanzen zugreifen, wenn sie den Service nutzen möchten (in Abbildung 2 mit Service A

- 2490 dargestellt), Ein Kommunikationsaufbau von Service-VAU-Instanzen zu AK-VAU-
- 2491 Instanzen ist nicht möglich.
- 2492 Eine Service-VAU-Instanz kann von mehreren AK-VAU-Instanzen gleichzeitig genutzt
- 2493 werden (die Service-VAU-Instanz zu AK-VAU-Instanz-Beziehung ist eine n:m-Beziehung).

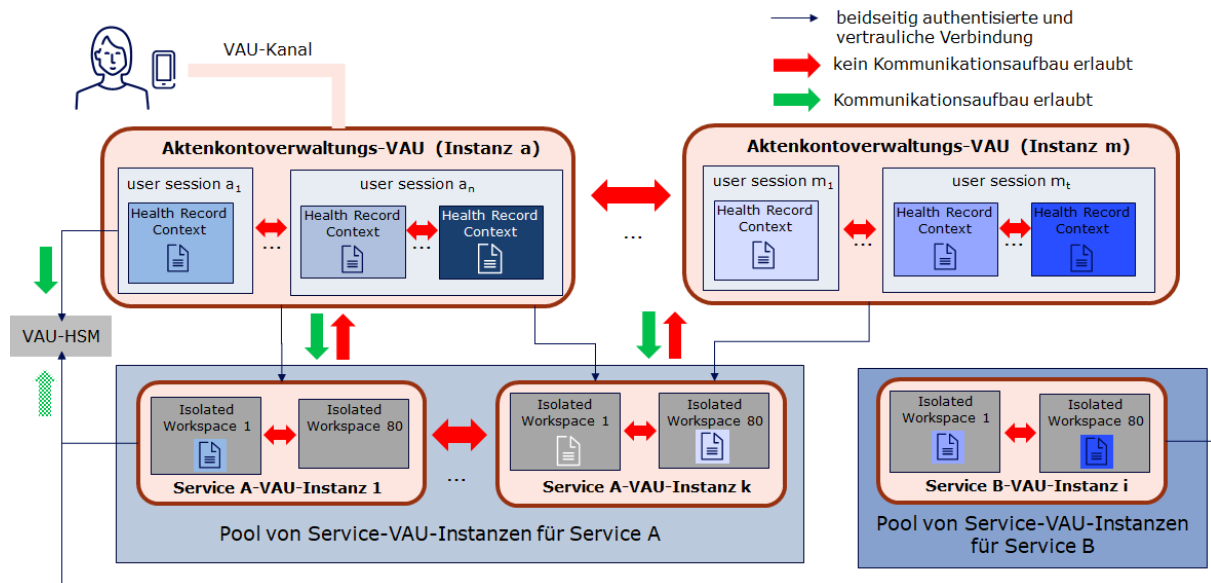


Abbildung 4: Überblick Service-VAUs

- 2494
- 2495
- 2496 Innerhalb einer Service-VAU-Instanz erfolgt die Verarbeitung unterschiedlicher Service-
- 2497 Requests in voneinander getrennten **Isolated Workspaces**. Isolated Workspaces in
- 2498 Service-VAUs werden analog zu den Health Record Contexts in Aktenkontoverwaltungs-
- 2499 VAUs geschützt.
- 2500 **A_26112 -ePA-Aktensystem - Maximale Isolated Workspaces in einer Service-**
- 2501 **VAU-Instanz**
- 2502 Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Isolated Workspaces
- 2503 gleichzeitig in einer Service-VAU-Instanz laufen können.[<=]
- 2504 **A_26113-01 -ePA-Aktensystem - Isolation zwischen Isolated Workspaces**
- 2505 **innerhalb einer Service-VAU-Instanz**
- 2506 Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb
- 2507 einer Service-VAU-Instanz zwischen Isolated Workspaces keine Informationsflüsse
- 2508 auftreten können.
- 2509 [<=]
- 2510 **A_27537 -ePA-Aktensystem – Kein gemeinsamer Speicher von Isolated**
- 2511 **Workspaces innerhalb einer Service-VAU-Instanz**
- 2512 Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb
- 2513 einer Service-VAU-Instanz von einem Isolated Workspace nicht auf den Speicher anderer
- 2514 Isolated Workspaces zugegriffen werden kann.[<=]
- 2515 **A_26114 -ePA-Aktensystem - Isolation zwischen unterschiedlichen Service-**
- 2516 **VAU-Instanzen**
- 2517 Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der
- 2518 unabhängig vom Separationsmechanismus in A_26113-* ist, ausschließen, dass sich
- 2519 Verarbeitungen in einer Service-VAU-Instanz schadhaft auf die Verarbeitungen einer
- 2520 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. [$\leq$]

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. [$\leq$]

A_30474 -ePA-Aktensystem - ZF-Service-VAU - Maximale Lebensdauer

Das ePA-Aktensystem MUSS sicherstellen, dass die Instanzen einer Zusatzfunktion-Service-VAU nach maximal 26 Stunden beendet werden. [$\leq$]

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. [$\leq$]

3.4.4.2 Kommunikation zwischen AK-VAU und Service-VAU

A_26126 -ePA-Aktensystem - Gesicherte und authentifizierte Verbindung zwischen AK-VAU- und Service-VAU-Instanzen

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

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. [$\leq$]

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. [$\leq$]

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

2612 können. Eingefrorene Daten dürfen nur in das Aktenkonto aufgenommen werden, wenn
2613 dies keine Protokollierung für den Versicherten erfordert.

2614 Ein Beispiel ist die Erstellung eines Indexes für die Volltextsuche als Ergebnis des
2615 Einstellens eines neuen Dokuments durch einen Nutzer. Die Erstellung des Indexes
2616 erfolgt in einer Service-VAU und der erstellte Index wird von der Service-VAU
2617 zwischengespeichert abgelegt ("eingefroren"). Eine Aktenkontoverwaltungs-VAU pflegt
2618 den abgelegten Index dann zu einem späteren Zeitpunkt in die Akte ein. Das
2619 Aktualisieren des Indexes erfordert keine Protokollierung für den Versicherten. Für ihn
2620 wurde das Einstellen des Dokuments protokolliert, die Aktualisierung des Indexes ist eine
2621 technische Folge dieses Zugriffs.

2622 Temporäres Zwischenspeichern ("Einfrieren") von Daten

2623 Die folgende Abbildung beschreibt das Einfrieren von Daten durch eine AK-VAU. Ein
2624 Nutzer hat ein Aktenkonto geöffnet, um z.B. ein neues Dokument einzustellen. Der
2625 Health Record Context für das Konto ist gestartet und enthält den
2626 versichertenindividuellen Datenpersistierungsschlüssel des Kontos. Die AK VAU friert die
2627 zwischenzuspeichernden Daten und den versichertenindividuellen
2628 Datenpersistierungsschlüssel des Kontos mit Hilfe der VAU-HSM-Regel *kr6* ein.

2629 Damit die im Aktensystem gespeicherten verschlüsselten Daten einem Konto zugeordnet
2630 werden können, der Betreiber des ePA-Aktensystems daraus jedoch keine Profile über
2631 Versicherte erstellen kann, werden die Chiffre nicht der KVNR des Kontos, sondern
2632 einem Akten-Pseudonym zugeordnet, welches ausschließlich innerhalb der VAU aufgelöst
2633 werden kann. Die AK-VAU erzeugt das Akten-Pseudonym.

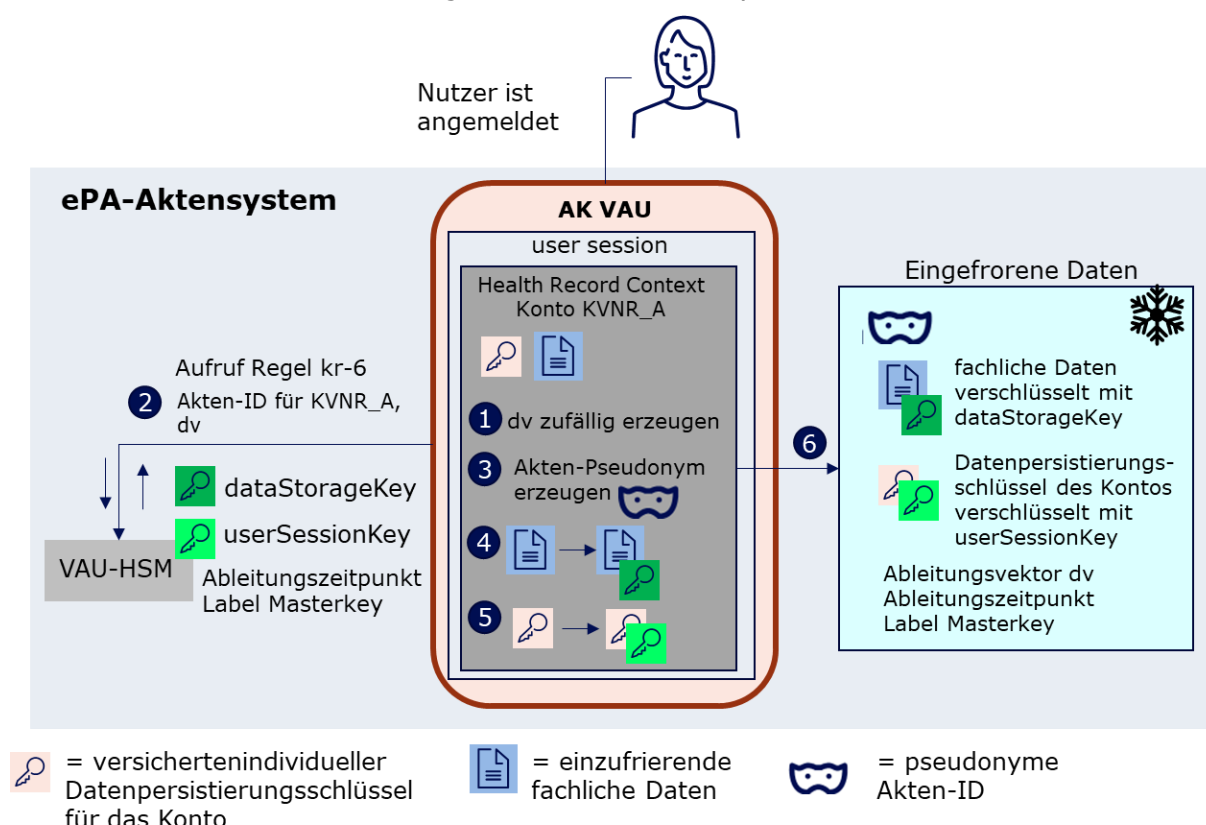


Abbildung 5: Einfrieren von Daten durch eine AK-VAU

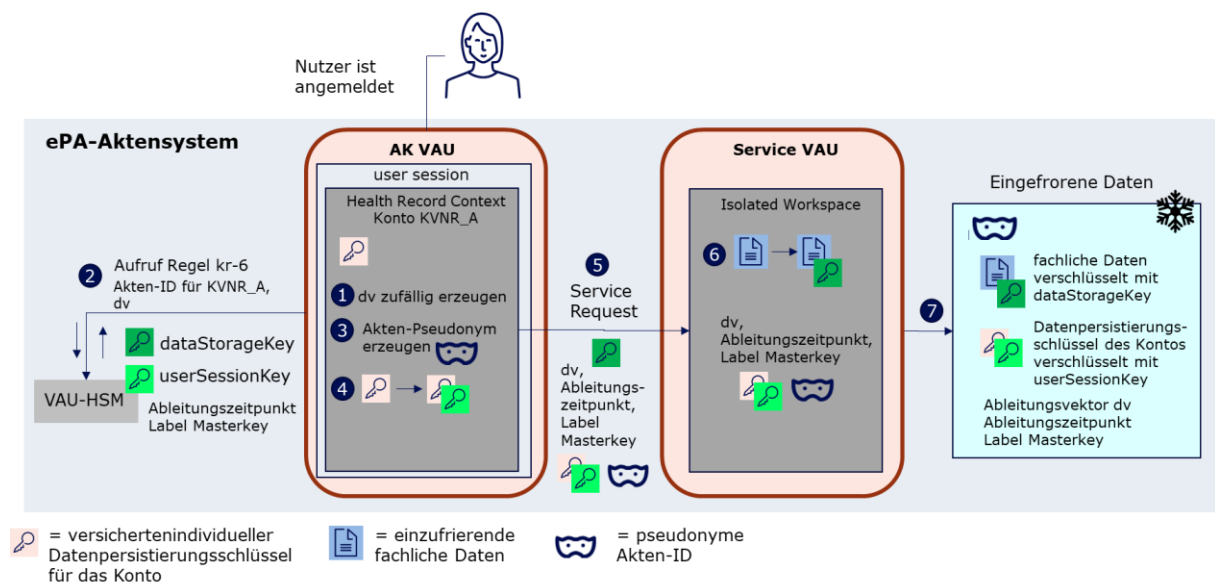
A_28767 -ePA-Aktensystem - Einfrieren von Daten durch eine AK-VAU

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 Datenpersistierungsschlüssel mit dem *userSessionKey* mittels AES/GCM verschlüsseln,
 6. die Chiffre 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 Datenpersistierungsschlüssel 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 Datenpersistierungsschlüssel 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 Datenpersistierungsschlüssel 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 übermittelten *dataStorageKey* 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 Chiffre 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,

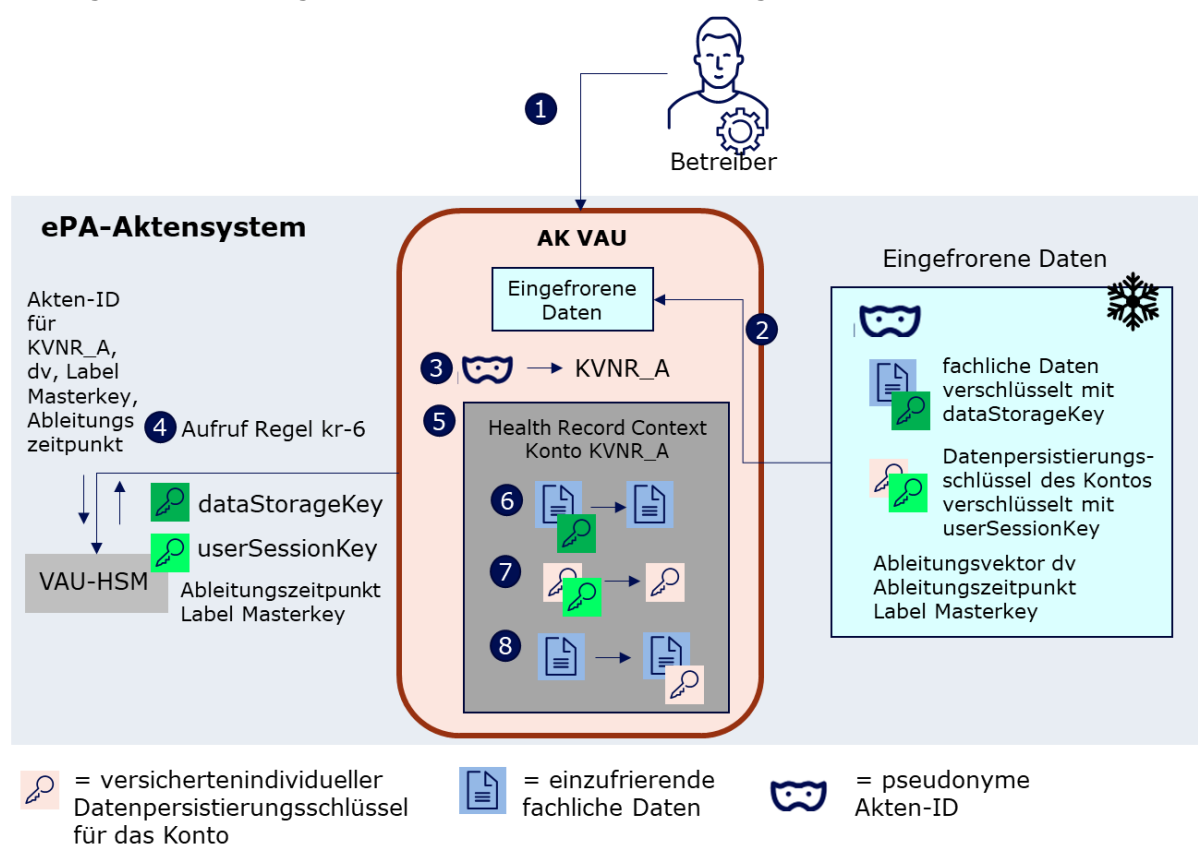
- 2709 • den mit dem *userSessionKey* verschlüsselten versichertenindividuellen
2710 Datenpersistierungsschlüssel.

2711 [$\leq$]

2712 Auftauen von Daten

2713 Die Aufnahme der temporär gespeicherten ("eingefrorenen") Daten in ein Aktenkonto
2714 erfolgt durch eine Aktenkontoverwaltungs-VAU. Service-VAUs dürfen keine Daten in
2715 Aktenkonten speichern (vgl. A_26119-*). Die hierfür benötigte AK-VAU-Instanz kann
2716 vom Betreiber des Aktensystems gestartet werden, d.h. die Aufnahme der eingefrorenen
2717 Daten in ein Aktenkonto ist unabhängig davon, wann Nutzer auf Aktenkonten zugreifen.
2718 Für die Schnittstelle, über die der Betreiber das Auftauen startet, sind die Anforderungen
2719 aus A_28805-* und A_28807-* zu berücksichtigen.

2720 Die folgende Abbildung beschreibt das Auftauen von eingefrorenen Daten.



2721

2722

Abbildung 7: Auftauen von eingefrorenen Daten

2723

1. Der Betreiber startet eine AK-VAU-Instanz.

2724

2. Die gestartete AK-VAU-Instanz lädt die im Aktensystem gespeicherten eingefrorenen Daten (Chiffre inkl. Metainformationen) in die AK-VAU-Instanz.

2725

2726

3. In der AK-VAU-Instanz wird das Akten-Pseudonym zu der Akten-ID (z.B. zur KVN_R) aufgelöst.

2727

2728

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.

2729

2730

2731

2732

5. Ein Health Record Context für die Akte zur Akten-ID wird in der AK-VAU geöffnet.

2733 6. Im Health Record Context werden die verschlüsselten fachlichen Daten mit dem
2734 *dataStorageKey* entschlüsselt.

2735 7. Im Health Record Context wird der verschlüsselte versichertenindividuelle
2736 Datenpersistierungsschlüssel mit dem *userSessionKey* entschlüsselt.

2737 8. Mit dem versichertenindividuellen Datenpersistierungsschlüssel werden die
2738 zwischengespeicherten Daten verschlüsselt und in der Akte gespeichert.

2739 **A_28770 -ePA-Aktensystem - Keine Protokollierungserfordernis der Aufnahme**
2740 **von gespeicherten Daten ins Aktenkonto**

2741 Der Hersteller des ePA-Aktensystems MUSS sicherstellen, dass eine
2742 Aktenkontoverwaltungs-VAU temporär gespeicherte (eingefrorene) Daten in ein
2743 Aktenkonto nur dann aufnimmt, wenn die dafür notwendigen Zugriffe nicht für den
2744 Versicherten protokolliert werden müssen. [$\leq$]

2745 Bis eingefrorene Daten von einer AK VAU aufgetaut und in das Aktenkonto eingebracht
2746 werden, könnten weitere Zugriffe auf das Aktenkonto erfolgen., die ggf. ebenfalls dazu
2747 führen, dass Daten für das Konto eingefroren werden. Ein Beispiel ist das Einfrieren eines
2748 neu erstellen Indexes für die Volltextsuche aufgrund eines eingestellten Dokuments. Hier
2749 könnten Nutzer neue Dokumente einstellen, nachdem ein Index eingefroren wurde aber
2750 bevor dieser eingepflegt wurde. Die AK-VAU muss dann beim Auftauen die verschiedenen
2751 Indexe zusammenführen, um einen konsistenten Aktenzustand zu erreichen.

2752 **A_28804 -ePA-Aktensystem - Kein inkonsistenter Aktenzustand durch das**
2753 **Einbringen eingefrorener Daten**

2754 Das ePA-Aktensystems MUSS sicherstellen, dass durch das Einbringen eingefrorener
2755 Daten kein inkonsistenter Aktenzustand entsteht. [$\leq$]

2756 Das Löschen der zwischengespeicherten Chiffre erfolgt nach Aufnahme der Daten in
2757 das Aktenkonto.

2758 **A_28771 -ePA-Aktensystem - Löschen nach Aufnahme von gespeicherten Daten**
2759 **ins Aktenkonto**

2760 Das ePA-Aktensystem MUSS sicherstellen, dass nach erfolgreicher Übernahme der
2761 temporär gespeicherten (eingefrorenen) Daten

- 2762 • der Health Record Context in der AK-VAU sofort geschlossen wird,
2763 • der *dataStorageKey* und der *userSessionKey* sofort gelöscht werden,
2764 • die Chiffre mitsamt aller Metainformationen sofort im ePA-Aktensystem gelöscht
2765 werden.

2766 [$\leq$]

2767 **A_28772 -ePA-Aktensystem - Schnellstmögliche Aufnahme eingefrorener**
2768 **Ergebnisdaten**

2769 Der Hersteller des ePA-Aktensystems MUSS sicherstellen, dass das ePA-Aktensystem
2770 eingefrorene Daten, die direkt in die Akte eingepflegt werden können, schnellstmöglich in
2771 die Akte einpflegt. [$\leq$]

2772 Hinweis zu A_28772-*: Ein Beispiel für Daten, die unter die Anforderung A_28772-*
2773 fallen, ist der eingefrorene Index als Ergebnis einer langlaufenden Indexierung bei der
2774 Volltextsuche. Der Index kann direkt in die Akte eingepflegt werden und benötigt keine
2775 weiteren Verarbeitungen. Wird hingegen der Auftrag der Indexierung eingefroren, um die
2776 Indexierung später auszuführen, fallen diese "Auftragsdaten" nicht unter die A_28772-*.

2777 **3.5 Umschlüsselung**

2778 Das Kerckhoffs'sche Prinzip von 1883 ist ein Grundpfeiler der Kryptographie. Es besagt u.
2779 a. dass die Sicherheit von kryptographischen Verfahren alleinig von der Geheimhaltung
2780 der Schlüssel abhängen darf, und dass Schlüssel leicht auswechselbar sein müssen. Damit
2781 kryptographische Schlüssel in der Praxis ihre Sicherheitseigenschaft behalten können
2782 müssen sie einen Lebenszyklus besitzen (vgl. bspw. [NIST-SP-800-57P1]), der den
2783 regelmäßigen Austausch (Wechsel) der Schlüssel vorsieht und umsetzt. Aus diesem
2784 Grunde werden die Masterkeys für Akten Daten und die Masterkeys für Befugnisse
2785 regelmäßig erneuert (vgl. A_15745-* und A_20519-* (beide aus [gemSpec_Krypt])). Bei
2786 dieser Erneuerung muss eine Umschlüsselung durchgeführt werden:

- 2787 • Schlüssel_alt_KVNR = Ableitung (MK_alt, KVNR),
- 2788 • Schlüssel_neu_KVNR = Ableitung (MK_neu, KVNR),
- 2789 • Umschlüsselung pro Akte: Schlüssel_alt_KVNR -> Schlüssel_neu_KVNR.

2790 Es liegt in der Verantwortung des Anbieters des ePA-Aktensystems, d.h. des
2791 Kostenträgers, eine Umschlüsselung für die Aktenkonten seiner Versicherten
2792 entsprechend der zeitlichen Vorgabe der Anforderung A_20519-* auszulösen. Den
2793 genauen Zeitpunkt der Umschlüsselung innerhalb des Zeitrahmens kann der
2794 Kostenträger zusammen mit dem Betreiber des ePA-Aktensystems abstimmen, um die
2795 Belastung des Aktensystems durch die Umschlüsselungsprozesse geeignet zu steuern.

2796 **A_28773 -Anbieter ePA-Aktensystem - Auslösen der Umschlüsselung durch**
2797 **Kostenträger**

2798 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass für die Aktenkonten aller
2799 Versicherten des Anbieters in dem durch A_20519-* vorgegebenen Zeitrahmen
2800 eine Umschlüsselung ausgelöst wird.[<=]

2801 **A_28774 -ePA-Aktensystem - Schnittstelle zum Auslösen der Umschlüsselung**

2802 Das ePA-Aktensystem MUSS dem Kostenträger eine Schnittstelle anbieten, über die der
2803 Kostenträger eine Umschlüsselung für die Konten des Kostenträgers auslösen kann.[<=]

2804 **A_28775 -ePA-Aktensystem - Auslösen der Umschlüsselung nur für Versicherte**
2805 **des Kostenträgers**

2806 Das ePA-Aktensystem MUSS sicherstellen, dass ein Kostenträger eine Umschlüsselung
2807 ausschließlich für die Konten von Versicherten auslösen kann, die beim Kostenträger
2808 versichert sind.[<=]

2809 **A_28776 -ePA-Aktensystem - Aktenstatus INACCESSIBLE während der**
2810 **Umschlüsselung**

2811 Löst der Kostenträger über die vom Aktensystem bereitgestellte Schnittstelle die
2812 Umschlüsselung für ein Aktenkonto aus, MUSS das ePA-Aktensystem den Aktenstatus
2813 des Aktenkontos auf INACCESSIBLE mit Ursache Umschlüsselung setzen bzw. für ein
2814 Aktenkonto im Zustand INACCESSIBLE die Umschlüsselung als weitere Ursache für den
2815 Verbleib im Aktenstatus INACCESSIBLE ergänzen.[<=]

2816 **A_28777 -ePA-Aktensystem - Rücksetzen des Aktenstatus nach Beendigung der**
2817 **Umschlüsselung**

2818 Nachdem die Umschlüsselung für ein Aktenkonto vom ePA-Aktensystem erfolgreich
2819 durchgeführt wurde, MUSS das ePA-Aktensystem die Ursache der Umschlüsselung aus
2820 den Ursachen des Status INACCESSIBLE entfernen. [<=]

2821 **A_28806 -ePA-Aktensystem - Keine Umschlüsselung wenn Konto von Nutzern**
2822 **genutzt wird**

2823 Das ePA-Aktensystem MUSS sicherstellen, dass während ein Konto umgeschlüsselt wird,
2824 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 Chifftrat erkennbar ist mithilfe welches Masterkeys die Chifftrate 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 Chifftrate mehr im ePA-Aktensystem existieren, die auf Basis des Masterkeys verschlüsselt wurden. Hierzu gehören auch die Chifftrate 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

2872 am längsten nicht genutzte Health Record Context geschlossen, um einen neuen Health
2873 Record Context öffnen zu können.

2874 3.7 Consent Decision Management

2875 Das Consent Decision Management des Aktensystems verwaltet die Entscheidungen eines
2876 Versicherten oder eines Vertreters für oder gegen die Nutzung von definiert
2877 widerspruchsfähigen Funktionen gemäß gesetzlicher Vorgaben.

2878 Außerdem werden im Consent Decision Management die Einschränkungen der
2879 Verwendung von Daten auf bestimmte Sekundärnutzungszwecke durch das
2880 Forschungsdatenzentrum Gesundheit verwaltet (siehe 3.7.2- Einschränkung der
2881 Verwendung von Daten auf bestimmte Sekundärnutzungszwecke).

2882 Der Widerspruch gegen die grundsätzliche Nutzung der ePA wird nicht im Consent
2883 Decision Management berücksichtigt. Die Existenz eines Aktenkontos für einen
2884 Versicherten impliziert, dass kein Widerspruch gegen die Nutzung der ePA erteilt wurde.
2885 Der Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger
2886 wird ebenfalls nicht hier verwaltet (siehe zu beiden Widersprüchen auch 3.1.1-
2887 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte).

2888 3.7.1 Widersprüche für Funktionen der ePA

2889 Die vorgehaltenen Entscheidungen zu einer Funktion umfassen dabei den Zustand "kein
2890 Widerspruch erklärt" ("permit") oder "Widerspruch erklärt" ("deny") und den Kontext
2891 einer Funktion. Der Kontext ordnet dabei die einzelnen widerspruchsfähigen Funktionen
2892 einem für die Umsetzung des Widerspruchs betroffenen Nutzerkreis zu und wird bei den
2893 zugreifenden Schnittstellen zur Filterung der Ausgabe verwendet.

2894 Initial, also bei der Erstellung eines neuen Aktenkontos oder bei Übernahme eines
2895 existierenden ePA 2.x Aktenkontos, ist für keine widerspruchsfähige Funktion ein
2896 Widerspruch gegen die Nutzung erklärt. Ein Versicherter oder ein Vertreter kann im
2897 Verlauf der Nutzung des Aktenkontos aktiv der Verwendung von widerspruchsfähigen
2898 Funktionen widersprechen oder einen erteilten Widerspruch zurücknehmen.

2899 Die aktuell erteilten Widersprüche können durch einen Versicherten oder einen Vertreter
2900 jederzeit über ein ePA-FdV eingesehen und geändert werden. Versicherte und Vertreter,
2901 die ein ePA-FdV nicht nutzen möchten, können eine Auskunft über die aktuell erteilten
2902 Widersprüche über die Ombudsstelle erhalten und dort auch Änderungen an den
2903 Entscheidungen im Aktenkonto veranlassen. Die Ansicht oder Änderung der
2904 Widersprüche erfolgt im Aktenkonto stets gesichert innerhalb der VAU, die aktuellen
2905 Entscheidungen zu den widerspruchsfähigen Funktionen der ePA sind
2906 versichertenindividuell mit dem SecureDataStorageKey verschlüsselt abgelegt.

2907 Die Information über relevante erteilte oder nicht erteilte Widersprüche können Clients
2908 auf einfache Weise (ohne Authentisierung oder Etablierung eines VAU-Kanals) im Vorfeld
2909 einer Operation über den Information Service abfragen (siehe auch 3.14- Information
2910 Services).

2911 Das Consent Decision Management des Aktenkontos spiegelt ("cached") die
2912 Entscheidungen zu den Widersprüchen für die schnelle Abfrage über den Information
2913 Service in einen Bereich, der ohne den Aufbau eines VAU-Kanals und Verwendung des
2914 versichertenindividuellen SecureDataStorageKey nutzbar ist.

Das Aktenkonto unterstützt die Durchsetzung eines erteilten Widerspruchs überall dort, wo Aktivitäten dediziert als Teil einer widerspruchsfähigen Funktion zugeordnet werden können. Beispielsweise wird das Einstellen neuer Verordnungs- und Dispensierdaten in die Ordner der Kategorie "medication" immer verhindert, wenn der Teilnahme am digital gestützten Medikationsprozess widersprochen wurde. Die konkreten Auswirkungen eines Widerspruchs sind in den jeweiligen Kapiteln zur Handhabung von Dokumenten und Daten des Aktenkontos dargestellt (siehe 3.12.1- 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. **[<=]**

2947 *Hinweis zu A_25300*: Die Änderung der Entscheidung zur Nutzung der "führenden"*
2948 *Funktion hat automatisch eine Entscheidung zur Nutzung der "abhängigen" Funktion zur*
2949 *Folge. Dieses gilt nur für die aufgeführten Entscheidungsänderungen. Alle weiteren, nicht*
2950 *aufgeführten, Änderungen zu Entscheidungen haben keine "abhängige" Auswirkung auf*
2951 *weitere Entscheidungen zu Funktionen. Beispiel: Wird die Entscheidung für 'medication'*
2952 *von 'permit' auf 'deny' gesetzt, so hat dieses keine weiteren Änderungen an*
2953 *Entscheidungen zur Folge.*

2954 **A_23766-01 -Consent Decision Management - Initialisierung der**
2955 **Widerspruchsinformation zur Nutzung von Funktionen der ePA**

2956 Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen
2957 bezüglich der Nutzung von Funktionen der elektronischen Patientenakte bei Erstellung
2958 eines neuen Aktenkontos für alle Funktionen, gegen die der Versicherte nicht
2959 widersprochen hat mit der Entscheidung "kein Widerspruch erklärt" ("permit")
2960 initialisieren sowie alle Funktionen, gegen die der Versicherte widersprochen hat, mit
2961 "deny" initialisieren.

2962 Der Entscheidung MUSS als Zeitpunkt der Initialisierung der feste Wert "2025-01-
2963 15T00:00:00Z" und als Akteur "system" zugeordnet werden.

2964 [$\leq$]

2965 **A_28043 -Consent Decision Management - Initialisierung der**
2966 **Widerspruchsinformation zur Sekundärdatennutzung (PKV)**

2967 Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen
2968 bezüglich der Sekundärdatennutzung bei Erstellung eines neuen Aktenkontos mit "deny"
2969 initialisieren, wenn die Akte durch einen Kostenträger verantwortet wird, für den
2970 gesetzlich keine Sekundärdatennutzung vorgesehen ist. [$\leq$]

2971 **A_24343 -Consent Decision Management - Speichern der Inhalte**

2972 Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen
2973 bezüglich der Nutzung von Funktionen der elektronischen Patientenakte unter
2974 Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen. [$\leq$]

2975 **A_23712 -Consent Decision Management - Übertrag der**
2976 **Widerspruchsinformation zur Nutzung von Funktionen der ePA für den**
2977 **Informationsdienst**

2978 Das Consent Decision Management MUSS die aktuellen Entscheidungen
2979 zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen
2980 Patientenakte der Funktionsklassen

2981

- Versorgungsprozess ("healthCareProcess")

2982 sofort im Anschluss an eine Änderung der Entscheidung im Consent Decision
2983 Management für die Abfrage durch den Information Service des Aktensystems ohne
2984 Nutzung der VAU und des SecureAdminStorageKeys verfügbar machen.

2985 [$\leq$]

2986 **A_24040 -Consent Decision Management - Periodischer Übertrag der**
2987 **Widerspruchsinformation zur Nutzung von Funktionen der ePA für den**
2988 **Informationsdienst**

2989 Das Consent Decision Management MUSS die aktuellen Entscheidungen
2990 zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen
2991 Patientenakte der Funktionsklassen

2992

- Versorgungsprozess ("healthCareProcess")

2993 bei jedem Start der VAU (des VAU-Kanals) für die Abfrage durch den Information Service
2994 des Aktensystems ohne Nutzung der VAU und des SecureAdminStorageKeys verfügbar
2995 machen, unabhängig von einer Änderung der Entscheidungen zu den
2996 Widersprüchen. [$\leq$]

2997 Clients der Ombudsstelle und aus der Umgebung des Versicherten nutzen das Consent
2998 Decision Management über die Operationen der Schnittstelle
2999 I_Consent_Decision_Management. Clients aus der Umgebung der LEI und der E-Rezept-
3000 Fachdienst nutzen für die schnelle Abfrage die Operation der
3001 SchnittstelleI_Information_Service.

3002 **A_23824 -Aktensystem - Realisierung der Schnittstelle**

3003 **I_Consent_Decision_Management**

3004 Das ePA-Aktensystem MUSS die Operationen der Schnittstelle
3005 I_Consent_Decision_Managementgemäß [I_Consent_Decision_Management]
3006 umsetzen.[<=]

3007 **A_23919 -Consent Decision Management - unveränderte Übernahme der** 3008 **Widerspruchsentscheidung**

3009 Das Consent Decision Management MUSS die über Operationen der Schnittstellen des
3010 Consent Managements übermittelten Entscheidungen (consent decisions) zu
3011 widerspruchsfähigen Funktionen der ePA in das Aktenkonto übernehmen. Die
3012 Entscheidungen zu den in den Operationen nicht adressierten widerspruchsfähigen
3013 Funktionen MÜSSEN im Aktenkonto unverändert bleiben.[<=]

3014 **A_24844 -Consent Decision Management - Information über Änderungen der** 3015 **Widerspruchsinformation**

3016 Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung
3017 einer Widerspruchsinformation, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail
3018 darüber informieren, dass Widerspruchsinformationen geändert wurden, wann die
3019 Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im
3020 Protokoll zu finden sind.[<=]

3021 **3.7.2 Einschränkung der Verwendung von Daten auf bestimmte** 3022 **Sekundärnutzungszwecke**

3023 Wenn kein Widerspruch gegen die Sekundärdatennutzung durch das FDZ für das
3024 Aktenkonto erteilt wurde, kann durch den Versicherten oder einen Vertreter über das ePA
3025 FdV, bzw. durch die Ombudsstelle, die Verwendung der Daten auf die in § 303e Absatz 2
3026 SGB V aufgeführten Sekundärnutzungszwecke im FDZ eingeschränkt werden.

3027 Der initiale Zustand nach Aktivierung eines Aktenkontos ist für jeden
3028 Sekundärnutzungszweck "kein Widerspruch erteilt".

3029 Eine Änderung der Widersprüche zu Verwendungszwecken führt dazu, dass diese
3030 Informationen an das Forschungsdatenzentrum Gesundheit übermittelt werden. Die
3031 Widersprüche des Versicherten in die Sekundärnutzungszwecke sind dort bindend für die
3032 Verarbeitung der übermitteltenpseudonymisierten medizinischen Daten, siehe auch 3.19-
3033 Data_Submission_Service .

3034 **A_26286-01 -Consent Decision Management - Initialisierung der** 3035 **Sekundärnutzungszwecke**

3036 Das Consent Decision Management MUSS jeden in § 303e Absatz 2 SGB V aufgeführten
3037 Sekundärnutzungszweck der elektronischen Patientenakte bei Erstellung eines neuen
3038 Aktenkontos mit der Entscheidung "kein Widerspruch erklärt" ("permit") initialisieren.
3039 Der Entscheidung MUSS als Zeitpunkt der Initialisierung der feste Wert "2025-01-
3040 15T00:00:00Z" und als Akteur "system" zugeordnet werden.[<=]

3041 **A_28044-01 -Consent Decision Management - Initialisierung der** 3042 **Sekundärnutzungszwecke (PKV)**

3043 Das Consent Decision Management MUSS jeden in § 303e Absatz 2 SGB V aufgeführten
3044 Sekundärnutzungszweck der elektronischen Patientenakte bei Erstellung eines neuen

3045 Aktenkontos mit "deny" initialisieren, wenn die Akte durch einen Kostenträger
3046 verantwortlich wird, für den gesetzlich keine Sekundärdatennutzung vorgesehen ist.
3047 Der Entscheidung MUSS als Zeitpunkt der Initialisierung der feste Wert "2025-01-
3048 15T00:00:00Z" und als Akteur "system" zugeordnet werden. [<=]

3049 **A_26287 -Consent Decision Management - Speichern der Entscheidungen zu**
3050 **Sekundärnutzungszwecken**

3051 Das Consent Decision Management MUSS die Entscheidungen
3052 zu Sekundärnutzungszwecken der elektronischen Patientenakte unter Verwendung des
3053 SecureDataStorageKeys gesichert im Aktenkonto ablegen. [<=]

3054 **A_26288 -Consent Decision Management - Übertragen der Entscheidungen zu**
3055 **Sekundärnutzungszwecken an das FDZ**

3056 Das Consent Decision Management MUSS die Entscheidungen
3057 zu Sekundärnutzungszwecken sofort im Anschluss an eine Änderung der Entscheidung im
3058 Consent Decision Management in das Paket zur Übermittlung von pseudonymisierten
3059 medizinischen Daten zu Sekundärnutzungszwecken an das FDZ aufnehmen. [<=]

3060 **A_26291 -Consent Decision Management - unveränderte Übernahme der**
3061 **Widerspruchsentscheidung zu Sekundärnutzungszwecken**

3062 Das Consent Decision Management MUSS die über Operationen der Schnittstellen des
3063 Consent Managements [I_Consent_Decision_Management] übermittelten Entscheidungen
3064 zu Sekundärnutzungszwecken in das Aktenkonto übernehmen. [<=]

3065 **A_26292 -Consent Decision Management - Information über Änderungen der**
3066 **Entscheidungen zu Sekundärnutzungszwecken**

3067 Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung der
3068 Entscheidungen zu Sekundärnutzungszwecken, sofern eine E-Mail-Adresse vorliegt, mit
3069 einer E-Mail darüber informieren, dass Entscheidungen zu Sekundärnutzungszwecken
3070 geändert wurden, wann die Änderung erfolgte und darauf hinweisen, dass nähere
3071 Informationen zur Änderung im Protokoll zu finden sind. [<=]

3072 **A_26294 -Consent Decision Management – Weiterleitung von Widersprüchen**
3073 **gegen Sekundärnutzungszwecken an das FDZ**

3074 Das Consent Decision Management MUSS die Information über einen erklärten
3075 Widerspruch gegen Sekundärnutzungszwecke über den Data Submission Service an das
3076 FDZ weiterleiten. [<=]

3077 **A_26310 -Consent Decision Management – Rücknahme des Widerspruchs gegen**
3078 **die Sekundärdatennutzung durch das FDZ**

3079 Falls ein Widerspruch gegen die Sekundärdatennutzung durch das FDZ zurückgenommen
3080 wird MUSS das Consent Decision Management die Entscheidungen
3081 zu Sekundärnutzungszwecken über den Data Submission Service an das FDZ
3082 weiterleiten. [<=]

3083 **A_26293 -Consent Decision Management – Weiterleitung von Widersprüchen**
3084 **gegen die Sekundärdatennutzung durch das FDZ**

3085 Das Consent Decision Management MUSS die Information über einen erklärten
3086 Widerspruch gegen die Sekundärdatennutzung durch das FDZ über den Data Submission
3087 Service an das FDZ weiterleiten. [<=]

3088 **3.7.3 Einschränkung des Medication Service für bestimmte LEI**
3089 **(User Specific Deny Policy Medication)**

3090 Ein Versicherter bzw. Vertreter kann den Zugriff auf den Medication Service für
3091 bestimmte LEI innerhalb seines Aktenkontos einschränken und diese Einschränkung auch
3092 wieder zurücknehmen. Durch das Setzen einer LEI auf eine User Specific Deny Policy

3093 Medication wird jeder Zugriff dieser LEI auf den Medication Service und auf die
 3094 Dokumente der Kategorie "emp" des Document Service für das Aktenkonto mit einem
 3095 Fehler abgebrochen. Durch das Entfernen einer LEI von der User Specific Deny Policy
 3096 Medication kann diese LEI Operationen des Medication Service (falls kein Widerspruch
 3097 gegen "medication" vorliegt) wieder nutzen und auf die Dokumente der Kategorie "emp"
 3098 des Document Service zugreifen.
 3099 Die User Specific Deny Policy Medication wird durch das Aktensystem für die in A_26406-
 3100 * aufgeführten Nutzergruppen angewendet und durchgesetzt.

3101 Der initiale Zustand nach Aktivierung eines Aktenkontos ist eine leere Liste.

3102 **A_26400 -Consent Decision Management - Initialisierung der User Specific Deny** 3103 **Policy Medication**

3104 Das Consent Decision Management MUSS für ein Aktenkonto eine User Specific Deny
 3105 Policy Medication ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge
 3106 der Policy über die Schnittstelle `I_Consent_Decision_Management` gemäß
 3107 `[I_Consent_Decision_Management]` ermöglichen. [`<=`]

3108 **A_26401 -Consent Decision Management - Speichern der Inhalte der User** 3109 **Specific Deny Policy Medication**

3110 Das Consent Decision Management MUSS Einträge aus der User Specific Deny Policy
 3111 Medication unter Verwendung des `SecureDataStorageKeys` gesichert im Aktenkonto
 3112 ablegen. [`<=`]

3113 **A_26403 -Consent Decision Management - Information über Änderungen der** 3114 **User Specific Deny Policy Medication**

3115 Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung der
 3116 Entscheidungen zu der User Specific Deny Policy Medication , sofern eine E-Mail-Adresse
 3117 vorliegt, mit einer E-Mail darüber informieren, welche Änderungen der User Specific Deny
 3118 Policy Medication vorgenommen wurden, wann die Änderung erfolgte und darauf
 3119 hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind. [`<=`]

3120 **A_26406-01 -Consent Decision Management - Policy für berechnigte** 3121 **Nutzergruppen und Nutzer**

3122 Das Consent Decision Management MUSS die Konfiguration der User Specific Deny Policy
 3123 Medication auf die folgenden Nutzergruppen einschränken:
 3124

3125 **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

Nutzergruppe [professionOID] der User Specific Deny Policy Medication
oid_institution-geburtshilfe
oid_praxis-physiotherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin
oid_praxis-ergotherapeut
oid_praxis-logopaede
oid_praxis-podologe
oid_praxis-ernaehrungstherapeut

3126
3127
3128

【<=】

3129 3.8 Entitlement Management

3130 Befugnisse (Entitlements) werden individuell für jeden Nutzer des Aktenkontos erstellt
3131 (Versicherter, Vertreter, Leistungserbringerinstitutionen, Kostenträger, Ombudsstelle und
3132 Fachdienste). Eine erteilte Befugnis ist notwendige Voraussetzung für die Nutzung des
3133 Aktenkontos und zum internen Bezug des Datenpersistierungsschlüssels
3134 (SecureDataStorageKey) für den Zugriff auf die Dokumenten- und Datenverwaltung.

3135 Eine Befugnis enthält folgende Informationen:

3136 **A_23734-01 -Entitlement Management - Definition einer Befugnis**

3137 Das Entitlement Management MUSS für eine individuelle Befugnis die folgenden Daten
3138 nutzen und verwalten:

3139 **Tabelle 10: Inhalt einer Befugnis**

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

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

3140 [<=]

3141 *Hinweis: Ein Nutzer ist der Adressat, für den die Befugnis ausgestellt wird. Der Ersteller*
 3142 *ist der Nutzer, welcher die Befugnisausstellung veranlasst hat. Die Bezeichner in () sind*
 3143 *die Bezeichner in den Schnittstellenbeschreibungen.*

3144 *Hinweis (*): A_23734 definiert eine "vollständige" Befugnis, welche auch Daten enthält,*
 3145 *die für eine Prüfung einer gültigen Befugnis im Kontext einer Schnittstellenoperation*
 3146 *nicht notwendig sind. Für diesen Zweck wird nur der (HSM-) signierte Anteil als Ergebnis*
 3147 *einer Befugnisverifikation verwendet (signiertes Element = ja). Eine gespeicherte*
 3148 *Befugnis enthält jedoch alle Elemente für eine qualifizierte Verwaltung der Befugnisse*
 3149 *durch einen Versicherten oder Vertreter.*

3150 *Hinweis: Befugnisse können durch das Aktensystem selbst (initiale Befugnisse), durch*
 3151 *den Versicherten oder einen befugten Vertreter unter Verwendung eines ePA-FdV oder*
 3152 *durch eine Leistungserbringerinstitution in einer Behandlungssituation erstellt werden.*

3153 Eine Befugnis kann nur für Nutzer und Nutzergruppen mit bestimmter Rolle erteilt
 3154 werden. Nutzergruppen mit abweichenden Rollen können nicht befugt werden und
 3155 erhalten keinen Zugriff auf das Aktenkonto.

3156 Erfolgt die Befugniserteilung durch eine Leistungserbringerinstitution in einer
 3157 Behandlungssituation, wird eine vorgegebene Gültigkeitsdauer der Rolle des Befugten
 3158 entsprechend durch das Entitlement Management vergeben. Ein Versicherter oder ein
 3159 befugter Vertreter kann den Gültigkeitszeitraum frei wählen (ausgenommen
 3160 Vertreterbefugnisse).

3161 **A_23941-01 -Entitlement Management - Erteilung von Befugnissen für** 3162 **berechtigte Nutzergruppen und Nutzer**

3163 Das Entitlement Management MUSS die Erteilung von Befugnissen in der jeweiligen
 3164 Umgebung auf die folgenden Nutzergruppen und Nutzer einschränken:

3165 **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

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_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

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_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 das Entitlement Management mit dem SecureAdminStorageKey verschlüsselt und im Aktenkonto gesichert abgelegt.

Einzelne Nutzer können durch den Versicherten, einen befugten Vertreter oder die Ombudsstelle explizit von der Befugnisvergabe ausgeschlossen sein (siehe 3.8.4: Befugnisauusschluss (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:

3200 **Tabelle 12: Befugnisse EU-Zugriff für berechnigte Nutzergruppen und Nutzer**

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

3201 Hinweis:

3202 'x' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung befugt
3203 werden3204 '-' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung nicht
3205 befugt werden3206
3207 LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-
3208 Prüfungsnachweis (Prüfziffer),
3209 FdV = Versicherter oder Vertreter,
3210 AS = Aktensystem (systemseitig erteilte Befugnisse)[<=]3211 **A_24371 -Entitlement Management - Verschlüsselung der Befugnisse**3212 Das Entitlement Management MUSS Befugnisse mit dem versichertenindividuellen
3213 SecureAdminStorageKey verschlüsseln und im Aktenkonto persistieren.[<=]3214 **A_24372 -Entitlement Management - Keine persistente Ablage
3215 unverschlüsselter Befugnisse**3216 Das Entitlement Management MUSS sicherstellen, dass Befugnisse ausschließlich
3217 verschlüsselt unter Verwendung des versichertenindividuellen SecureAdminStorageKey
3218 im Aktenkonto gespeichert werden.[<=]3219 **A_24687 -Entitlement Management - Keine Speicherung oder Verwendung nicht
3220 verifizierter Befugnisse**3221 Das Entitlement Management MUSS sicherstellen, dass ausschließlich Befugnisse
3222 persistiert oder für eine Befugnisprüfung verwendet werden, die erfolgreich durch das
3223 HSM unter Verwendung der adäquaten Regeln 'rr1 - rr4' gemäß A_24573*
3224 befugnisverifiziert sind.[<=]3225 **A_23842 -Entitlement Management - Eindeutigkeit der Befugnisse im
3226 Befugniskontext**3227 Das Entitlement Management MUSS sicherstellen, dass im Befugniskontext keine zwei
3228 oder mehr Befugnisse existieren, die als Identifier des befugten Nutzers die gleiche
3229 Identifikation (actorId) aufweisen.[<=]3230 **A_24785 -Entitlement Management - VSDM-Prüfungsnachweis kann höchstens
3231 einmal genutzt werden**3232 Das Entitlement Management MUSS sicherstellen, dass ein VSDM-Prüfungsnachweis
3233 (Prüfziffer) höchstens einmal zur Registrierung einer Befugnis genutzt werden kann.[<=]

3234 **A_27671 -Entitlement Management - PoPP-Token kann höchstens einmal**
 3235 **genutzt werden**

3236 Das Entitlement Management MUSS sicherstellen, dass ein PoPP-Token höchstens einmal
 3237 zur Registrierung einer Befugnis genutzt werden kann. [$\leq$]

3238 **A_27681 -Entitlement Management - Konfigurationsvariable enforce_popp_only**

3239 Das Entitlement Management MUSS eine Konfigurationsvariable `enforce_popp_only`
 3240 besitzen, die initial auf `false` gesetzt ist. [$\leq$]

3241 ePA-Clients nutzen zur Befugnisvergabe die Operationen der
 3242 Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`.
 3243 Die initialen Befugnisse des Aktenkontos werden auf organisatorischem Weg direkt im
 3244 Aktenkonto erstellt.

3245 **A_24506 -Entitlement Management- Realisierung der Schnittstelle**
 3246 **I_Entitlement_Management**

3247 Das Entitlement Management MUSS die Operationen der Schnittstelle
 3248 `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` umsetzen. [$\leq$]

3249 **A_26168 -Entitlement Management (EU)- Realisierung der Schnittstelle**
 3250 **I_Entitlement_Management_EU**

3251 Das Entitlement Management MUSS die Operationen der Schnittstelle
 3252 `I_Entitlement_Management_EU` gemäß `[I_Entitlement_Management_EU]`
 3253 umsetzen. [$\leq$]

3254 **3.8.1 Initiale Befugnisse (static Entitlements)**

3255 Einige grundsätzlich notwendige Befugnisse sind zum Zeitpunkt der Aktivierung eines
 3256 Aktenkontos verfügbar.

3257 Zu diesen initialen Befugnissen gehören die Befugnisse für den Versicherten, den E-
 3258 Rezept-Fachdienst, den Kostenträger und die Ombudsstelle. Diese Befugnisse müssen in
 3259 der Phase der Initialisierung eines Aktenkontos durch das Aktensystem erstellt werden.

3260 Diese Befugnisse sind dauerhaft gültig und unveränderbar und können nicht gelöscht
 3261 werden.

3262 **A_24145 -Entitlement Management – Implizite initiale (statische) Befugnisse**

3263 Das Entitlement Management MUSS sicherstellen, dass der Versicherte (KVNR des
 3264 Akteninhabers, `oid_versicherter`), und der E-Rezept-Fachdienst (registrierte Telematik-
 3265 ID, `oid_erp-vau`) dauerhaft den versichertenindividuellen `SecureDataStorageKey`
 3266 beziehen können und Zugriff auf die Dokumenten- und Datenverwaltung erhalten. Die
 3267 Befugnisse MÜSSEN den Vorgaben der folgenden Tabelle entsprechen:
 3268

Element	Versicherter	E-Rezept-Fachdienst
Identifizier des befugten Nutzers (<code>actorId</code>)	KVNR des Versicherten (Aktenkontoinhaber)	Telematik-ID der E-Rezept vertrauenswürdigen Ausführungsumgebung
Name des befugten Nutzers (<code>displayName</code>)	Name des Versicherten	Name/ Bezeichnung des E-Rezept-Fachdienstes oder "Fachdienst E-Rezept"

Element	Versicherter	E-Rezept-Fachdienst
Rolle des Nutzers (oid)	oid_versicherter	oid_erp-vau
Ende der Gültigkeit (validTo)	9999-12-31	9999-12-31

3269 [$\leq$]3270 **A_24374 -Entitlement Management – Signierte initiale (statische) Befugnisse**

3271 Das Entitlement Management MUSS sicherstellen, dass für den Kostenträger und die
 3272 Ombudsstelle gültige Befugnisse mit unbegrenzter Gültigkeitsdauer zum Zeitpunkt der
 3273 Aktivierung des Aktenkontos gemäß der Vorgaben der folgenden Tabelle vorliegen:

3274

Element	Kostenträger	Ombudsstelle
Identifiziert des Aktenkontos (insurantid)	KVNR des Versicherten	KVNR des Versicherten
Identifiziert 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

3275 [$\leq$]3276 **A_24688-01 -Entitlement Management – Befugnisverifikation signierter initialer Befugnisse**

3277 Das Entitlement Management MUSS sicherstellen, dass die initialen, signierten
 3278 Befugnisse des Kostenträgers und der Ombudsstelle spätestens beim ersten Zugriff auf
 3279 das Aktenkonto durch das HSM unter Verwendung der Regel 'rr4' gemäß A_24573*
 3280 befugnisverifiziert sind. [$\leq$]

3282 **A_24533 -Entitlement Management - Keine Änderung statischer Befugnisse**

3283 Das Entitlement Management MUSS sicherstellen, dass die dauerhaften Befugnisse des
 3284 Versicherten, des E-Rezept-Fachdiensts, des Kostenträgers und der Ombudsstelle nicht
 3285 verändert oder gelöscht werden können. [$\leq$]

3286 **A_24784 -Entitlement Management - Höchstens eine Befugnis für KTR und Ombudsstelle pro Aktenkonto**

3287 Das Entitlement Management MUSS sicherstellen, dass in einem Aktenkonto höchstens
 3288 eine Befugnis für einen Kostenträger und höchstens eine Befugnis für eine Ombudsstelle
 3289 hinterlegt ist. [$\leq$]

3290

3291 **A_24955 -Entitlement Management - Befugnis für KTR und Ombudsstelle nur** 3292 **bei Anlage und betreiberinterner Anbieterwechsel**

3293 Das Entitlement Management MUSS sicherstellen, dass eine signierte Befugnis des
 3294 Kostenträgers und eine signierte Befugnis der Ombudsstelle ausschließlich bei einer
 3295 Anlage eines Aktenkontos (Initialisierung) oder bei einem betreiberinternen
 3296 Anbieterwechsel in die Befugnisse des Aktenkontos aufgenommen werden.
 3297 [$\leq$]

3298 **3.8.2 Erstellen einer Befugnis durch Clients**

3299 Die Anforderung zur Vergabe einer neuen Befugnis erfolgt durch die Clients der ePA. Bei
 3300 einer Befugnisvergabe aus der Umgebung der Leistungserbringer ist dieses das
 3301 Primärsystem (PS), aus der Umgebung des Versicherten ist es das ePA-FdV.

3302 Clients verwenden zur Befugnisvergabe signierte JSON Web Token (JWS). Das Token
 3303 wird zur Verifikation an das HSM übergeben. Als Ergebnis der HSM Verarbeitung liegt
 3304 eine bestätigte, CMAC gesicherte Befugnis mit den Elementen `actorId` (Identifiziert des zu
 3305 befugnenden Nutzers), `kvnr` (AktenkontoId) und `validTo` (Gültigkeitszeitraum) für die
 3306 spätere Befugnisprüfung vor. Das HSM Ergebnis wird mit den weiteren Daten gemäß
 3307 A_23734* (`oid`, `displayName`, `issued`-*) ergänzt und gemäß A_24371* mit dem
 3308 SecureAdminStorageKey gesichert im Aktenkonto abgelegt.

3309 **3.8.2.1 Befugnisvergabe durch ein ePA-FdV**

3310 Ein ePA-FdV muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

3311 **A_24587-01 -Entitlement Management - Befugnis durch ein ePA-FdV**

3312 Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ePA-
 3313 FdV über die Schnittstelle `I_Entitlement_Management` durch Verwendung eines gültig
 3314 signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:
 3315

3316 **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

Befugnis	Claim Name	Claim	Beispiel
	"actorId"	Identifizier (Telematik-id oder KVN-R)	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

3317 [$\leq$]

3318 Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve
 3319 "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext
 3320 der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur
 3321 und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

3322 *Hinweis zu A_24587*: Im Falle der Befugnisvergabe für einen NCPeH (EU-Zugriff, "oid"*
 3323 *== "oid_ncpeh") wird durch das Aktensystem sichergestellt, dass die vorgeschriebene*
 3324 *Gültigkeitsdauer für derartige Befugnisse angewendet wird. Dieses erfolgt durch die*
 3325 *Befugnisverifikation gemäß Regel "rr1" im HSM. Die Angabe eines Gültigkeitsendes im*
 3326 *"validTo"-Element des JWT wird daher für diesen Fall ignoriert, das Element selbst muss*
 3327 *jedoch vorhanden sein.*

3328 **A_24689 -Entitlement Management - Befugnisverifikation einer Befugnis durch** 3329 **ein ePA-FdV**

3330 Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein
 3331 ePA-FdV unter Verwendung der Regeln 'rr1' (Befugnisvergabe durch den Versicherten)
 3332 bzw. 'rr2' (Befugnisvergabe durch einen Vertreter) des HSM eine Befugnisverifikation
 3333 durchführen.[$\leq$]

3334 **A_24535 -Entitlement Management - Befugnisse für Vertreter**

3335 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (actorId
 3336 = KVN-R) ausschließlich durch den Versicherten erstellt oder gelöscht werden
 3337 können.[$\leq$]

3338 **A_26698 -Entitlement Management - maximale Anzahl Befugnisse für Vertreter**

3339 Das Entitlement Management MUSS sicherstellen, dass maximal fünf gültige Befugnisse
 3340 für Vertreter gleichzeitig in einem Aktenkonto vorhanden sind.[$\leq$]

3341 **A_24536 -Entitlement Management - Gültigkeitsdauer der Befugnisse für** 3342 **Vertreter**

3343 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (actorId
 3344 = KVN-R) ausschließlich mit einer unbegrenzten Gültigkeit erstellt werden.[$\leq$]

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 Befugniserstellung

Das Entitlement Management MUSS im Anschluss an die erfolgreiche, neue Befugniserstellung für einen Vertreter eine E-Mail an die E-Mail-Adresse des Vertreters senden, die diesen über die Befugniserstellung für das Aktenkonto des Versicherten geeignet informiert. In der Nachricht MUSS der Name des Versicherten enthalten sein und welche Art von personenbezogenen Daten vom Vertreter im Rahmen der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine Vertreterberechtigung widerrufen kann und gegenüber wem er seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann. [`<=`]

Hinweis: Unter Art der personenbezogenen Daten ist z.B. „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:

3393 **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.

3394 **[<=]**

3395 *Hinweis: Die Parameter "iat" und "exp" sind optional und werden durch das Entitlement*
 3396 *Management nicht ausgewertet.*

3397 Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve
 3398 "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext
 3399 der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur
 3400 und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

3401 **A_27321-01 -Entitlement Management – Abgleich hcv bei Erstellen einer** 3402 **Befugnis über VSDM-Prüfziffer in Version 2**

3403 Falls vom Primärsystem in `setEntitlementPs` eine Befugnis (signiertes JWT) mit einer
 3404 Prüfziffer in Version 2 übergeben wird und das Ergebnis des Aufrufs der Regel rr3 eine
 3405 interne Datenstruktur der VSDM-Prüfziffer zurückliefert, MUSS das Entitlement
 3406 Management sicherstellen, dass der Wert im Attribut "hcv" des JWT mit dem Wert von
 3407 hcv aus der VSDM-Prüfziffer übereinstimmt und ansonsten die
 3408 `OperationsetEntitlementPs` abbrechen.**[<=]**

3409 **A_27289 -Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche** 3410 **der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer**

3411 Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer
 3412 Stunde maximal fünfmal eine Befugnis (signiertes JWT) über `setEntitlementPs`
 3413 übermitteln kann, bei der die mitgelieferte KVNR in `x-insurantId` von der KVNR
 3414 abweicht, die in der Prüfziffer der übermittelten Befugnis (signiertes JWT) enthalten ist,
 3415 andernfalls für den Nutzer für diesen Zeitraum die Operation `setEntitlementPs`
 3416 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. [$\leq$]

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. [$\leq$]

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. [$\leq$]

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 Befugniscontext des Aktenkontos vollständig löschen. [$\leq$]

Das explizite Löschen von Befugnissen innerhalb ihres Gültigkeitszeitraums kann ausschließlich durch den Versicherten oder einen Vertreter mittels eines ePA-FdV erfolgen. Es können alle erteilten Befugnisse gelöscht werden, ausgenommen die initialen Befugnisse gemäß 3.8.1- 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` zu löschenden Befugnis entspricht. [$\leq$]

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. [$\leq$]

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

professionOID / Nutzergruppe
oid_praxis-physiotherapeut
oid_praxis-ergotherapeut
oid_praxis-logopaede
oid_praxis-podologe
oid_praxis-ernaehrungstherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin

3490 **[<=]**

3491 Ein Eintrag der Blocked User Policy enthält Angaben gemäß der folgenden Tabelle:
3492 (Beispiel)

3493 **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

3494 **A_25135 -Entitlement Management - Initialisierung der Blocked User Policy**

3495 Das Entitlement Management MUSS für ein Aktenkonto eine Blocked User Policy ohne
3496 initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policies über die
3497 Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`
3498 ermöglichen. **[<=]**

3499 **A_24514 -Entitlement Management - Keine Befugnis für von einer Befugnis
3500 ausgeschlossene Nutzer**

3501 Das Entitlement Management MUSS sicherstellen, dass für keinen durch einen Eintrag
3502 der Blocked User Policy referenzierten Nutzer eine Befugnis existiert oder erstellt werden
3503 kann. **[<=]**

3504 **A_24515 -Entitlement Management- Verschlüsselung der Einträge der Blocked
3505 User Policy**

3506 Das Entitlement Management MUSS Einträge der Blocked User Policy mit dem
3507 Befugnispersistierungsschlüssel (`SecureAdminStorageKey`) verschlüsseln und im
3508 Aktenkonto persistieren. **[<=]**

3509 Die Konfiguration der Blocked User Policy erfolgt über die Schnittstelle
3510 `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` durch ein ePA-FdV
3511 bzw. durch die Ombudsstelle.

3512 **A_24965 -Entitlement Management - Information über Änderungen der Blocked** 3513 **User Policy**

3514 Das Entitlement Management MUSS den Aktenkontoinhaber bei einer Änderung der
3515 Blocked User Policy, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber
3516 informieren, dass ein Befugnisausschluss geändert wurde, wann die Änderung erfolgte
3517 und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden
3518 sind.[<=]

3519 **3.8.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)**

3520 Die Erstellung von Befugnissen durch Primärsysteme der Leistungserbringerinstitutionen
3521 wird durch das Aktensystem mengenmäßig über einen Zeitraum begrenzt. Diese
3522 Maßnahme verhindert den massenhaften Zugriff auf Aktenkonten durch Fehlbedienung
3523 seitens eines Primärsystems oder durch unzulässige Nutzung der Aktensysteme.

3524 Die maximal zulässige Befugnismenge ist dabei so bemessen, dass die intendierte
3525 Nutzung der ePA durch Leistungserbringerinstitutionen im Versorgungsalltag nicht
3526 eingeschränkt wird. Diese maximale Befugnismenge ist pro Nutzerrolle separat
3527 festgelegt.

3528 Jedes Aktensystem führt dazu aktensystemweit Zähler für erteilte Befugnisse aus der
3529 Umgebung der Leistungserbringer pro Telematik-ID. Die Erfassung erfolgt somit pro
3530 Leistungserbringerinstitution separat. Die Zuordnung erfolgt zur Telematik-ID der
3531 befugnisstellenden Nutzer (nicht des zu befugnenden Nutzers). Die Befugnisvergabe aus
3532 der Umgebung des Versicherten mittels ePA-FdV wird nicht erfasst und geht nicht in die
3533 Zählerstände ein.

3534 Das Entitlement Management wertet diese Menge der erfassten Befugnisvergaben im Falle
3535 einer weiteren Befugnisvergabe durch ein Primärsystem aus der Umgebung der LEI aus
3536 und verhindert die Befugniserstellung bei Erreichen der maximal zulässigen
3537 Befugnismenge.

3538 Die zulässige Befugnisrate limitiert dabei einerseits die Menge der innerhalb einer Stunde
3539 erstellbaren Befugnisse, als auch die Menge der insgesamt monatlich erstellbaren. Die
3540 Zählung erfolgt aktensystemweit pro Aktensystem eines Herstellers und unabhängig vom
3541 adressierten Aktenkonto und berücksichtigt nur erfolgreiche Befugnisvergaben. Der
3542 Zeitraum pro Stunde, bzw. pro Monat, bezieht sich dabei auf den Zeitraum der aktuellen
3543 Stunde, bzw. des aktuellen Monats.

3544 **A_27311 -Entitlement Management – RateLimit-oid-List**

3545 Das Entitlement Management MUSS eine *RateLimit-oid-List* führen, in der pro oid

- 3546 • der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden
3547 Befugnisse innerhalb einer Stunde,
- 3548 • der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden
3549 Befugnisse innerhalb eines Monats und
- 3550 • der Zeitpunkt der letzten Änderung der Werte

3551 gespeichert werden.[<=]

3552 Initial ist die RateLimit-oid-List mit folgenden Werten zu belegen:

3553 **A_27290-01 -Entitlement Management – RateLimit-oid-List: Maximale Anzahl**
 3554 **von Befugnissen für LEI pro Stunde**

3555 Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass eine LEI
 3556 mit der Rolle

- 3557 • oid_praxis_arzt maximal 200 Befugnisse
- 3558 • oid_krankenhaus maximal 1.000 Befugnisse
- 3559 • oid_institution-vorsorge-reha maximal 1.000 Befugnisse
- 3560 • oid_zahnarztpraxis maximal 200 Befugnisse
- 3561 • oid_öffentliche_apotheke maximal 200 Befugnisse
- 3562 • oid_praxis_psychotherapeut maximal 100 Befugnisse
- 3563 • oid_institution-pflege maximal 100 Befugnisse
- 3564 • oid_institution-geburtshilfe maximal 100 Befugnisse
- 3565 • oid_praxis-physiotherapeut maximal 100 Befugnisse
- 3566 • oid_praxis-ergotherapeut maximal 100 Befugnisse
- 3567 • oid_praxis-logopaede maximal 100 Befugnisse
- 3568 • oid_praxis-podologe maximal 100 Befugnisse
- 3569 • oid_praxis-ernaehrungstherapeut maximal 100 Befugnisse
- 3570 • oid_institution-oegd maximal 100 Befugnisse
- 3571 • oid_institution-arbeitsmedizin maximal 100 Befugnisse

3572 innerhalb einer Stunde durch das Primärsystem im Aktensystem registrieren kann.
 3573 [$\leq$]

3574 **A_27291-01 -Entitlement Management – RateLimit-oid-List: Maximale Anzahl**
 3575 **von Befugnissen für LEI pro Monat**

3576 Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass

- 3577 • oid_praxis_arzt maximal 10.000 Befugnisse
- 3578 • oid_krankenhaus maximal 200.000 Befugnisse
- 3579 • oid_institution-vorsorge-reha maximal 200.000 Befugnisse
- 3580 • oid_zahnarztpraxis maximal 10.000 Befugnisse
- 3581 • oid_öffentliche_apotheke maximal 25.000 Befugnisse
- 3582 • oid_praxis_psychotherapeut maximal 10000 Befugnisse
- 3583 • oid_institution-pflege maximal 10000 Befugnisse
- 3584 • oid_institution-geburtshilfe maximal 10000 Befugnisse
- 3585 • oid_praxis-physiotherapeut maximal 10000 Befugnisse
- 3586 • oid_praxis-ergotherapeut maximal 10000 Befugnisse
- 3587 • oid_praxis-logopaede maximal 10000 Befugnisse
- 3588 • oid_praxis-podologe maximal 10000 Befugnisse
- 3589 • oid_praxis-ernaehrungstherapeut maximal 10000 Befugnisse
- 3590 • oid_institution-oegd maximal 10000 Befugnisse

3591 • oid_institution-arbeitsmedizin maximal 10000 Befugnisse
3592 innerhalb eines Monats durch das Primärsystem im Aktensystem registrieren kann.
3593 [`<=`]
3594 Hinweis zu A_27290-* und A_27291-*: Die Stunde bzw. der Tag müssen sich nicht auf
3595 die aktuelle Stunde bzw. Kalendertag beziehen, sondern können auch je
3596 Leistungserbringerinstitution auf Requestzeitpunkte bezogen werden. Dann gilt für einen
3597 Monat 30 Tage.

3598 **A_27318 -ePA-Aktensystem - RateLimit-oid-List: Maßnahmen zum Schutz der**
3599 **Konfiguration**

3600 Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen
3601 umsetzen, die eine unautorisierte Änderung der *RateLimit-oid-List* verhindern.[`<=`]

3602 **A_27312 -ePA-Aktensystem - RateLimit-oid-List: Konfiguration durch Betreiber**

3603 Der Betreiber des ePA-Aktensystem MUSS sicherstellen, dass die Werte für die Anzahl
3604 der maximalen Befugnisse in der *RateLimit-oid-List* durch den Betreiber des ePA-
3605 Aktensystems ausschließlich im Vier-Augen-Prinzip konfigurierbar sind.[`<=`]

3606 Stellen LEI Befugnisse mittels der Operation *setEntitlementsPs* über das Primärsystem
3607 in das ePA-Aktensystem ein, wird für diese LEI geprüft, ob diese bereits das zulässige
3608 Limit erreicht hat. Nur falls dies nicht der Fall ist, kann die Befugnis eingestellt werden.
3609 Hierzu erfasst das ePA-Aktensystem außerhalb der VAU wann ein Nutzer mit welcher
3610 Rolle eine Befugnis registriert hat. Für den Nutzer wird außerhalb der VAU ein
3611 Nutzerpseudonym geführt.

3612 **A_27313-01 -Entitlement Management - Prüfen der RateLimit-oid-List beim**
3613 **Einstellen von Befugnissen**

3614 Das Entitlement Management MUSS bei Aufruf der Operation *setEntitlementsPs* oder
3615 *setEntitlementPsV2* prüfen, ob für das zur LEI gehörende Nutzerpseudonym und die oid
3616 der LEI bereits das in der *RateLimit-oid-List* vorgegebene maximale Limit pro Stunde
3617 oder Monat erreicht wurde. Falls ein Limit erreicht wurde, wird die Operation
3618 *setEntitlementsPs*, bzw. *setEntitlementPsV2*, mit einem Fehler abgebrochen. Falls
3619 kein Limit erreicht wurde, ist die Registrierung für das zur LEI gehörende
3620 Nutzerpseudonym zu vermerken.[`<=`]

3621 **A_27310 -ePA-Aktensystem - Erfassung der Nutzer zur Prüfung RateLimit-oid-**
3622 **List**

3623 Das ePA-Aktensystem MUSS sicherstellen dass bei der Erfassung der Nutzerdaten
3624 außerhalb der VAU zur Prüfung der *RateLimit-oid-List* eine Profilierung über die Nutzer
3625 nicht möglich ist und zu diesem Zweck aus der TelematikId eines Nutzers ein
3626 Nutzerpseudonym abgeleitet wird, gemäß gemSpec_Krypt#7.5 Routing auf VAU-
3627 Instanzen.
3628 [`<=`]

3629 **3.8.6 EntitlementDenyList**

3630 Ein Primärsystem einer Leistungserbringerinstitution (LEI) kann eine Befugnis für ein
3631 Aktenkonto eines Versicherten in einer Behandlungssituation ("Stecken" der eGK, VSDM-
3632 Prüfungsnachweis) eigenständig erstellen, wenn der Versicherte der Nutzung der ePA
3633 nicht widersprochen hat, für die konkrete Leistungserbringerinstitution im Aktenkonto
3634 kein Befugnisausschluss (3.8.4- Befugnisausschluss (Blocked User Policy)) vorliegt und
3635 die Leistungserbringerinstitution einer grundsätzlich befugbaren Nutzergruppe angehört
3636 (3.8- Entitlement Management).

3637 Die bestimmte LEI deren Telematik-ID auf einer sogenannten EntitlementDenyList
3638 stehen, wird diese Funktionalität durch das Aktensystem unterbunden, in der Weise dass
3639 eine Befugnisvergabe durch das Aktensystem unterbunden wird.

3640 Die Befugnisvergabe durch den Versicherten oder einen Vertreter mittel ePA-FdV ist
3641 durch die EntitlementDenyList nicht eingeschränkt. Über ein ePA-FdV können auch LEI
3642 befugt werden, die einen Eintrag in der EntitlementDenyList haben.

3643 Die EntitlementDenyList wird durch das Aktensystem bei jedem Aufruf einer Operation
3644 zur Befugnisvergabe durch ein Primärsystem ausgewertet. Diese Operation wird mit
3645 einem Fehler beendet, wenn die zu befugende LEI Bestandteil der Liste ist. Eventuell
3646 vorhandene Befugnisse dieser LEI, etwa aus einer Befugnisvergabe mittels ePA-FdV,
3647 verbleiben im Fehlerfall der Operation unverändert.

3648 Die EntitlementDenyList wird für alle Aktenkonten eines Aktensystems einheitlich
3649 verwaltet. Die Verwaltung erfolgt außerhalb der VAU, die Liste muss aber für Operationen
3650 der Befugnisvergabe innerhalb der VAU zugänglich sein.

3651 **A_27730 -ePA-Aktensystem - EntitlementDenyList außerhalb der VAU**
3652 Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen
3653 umsetzen, die eine unautorisierte Änderung der EntitlementDenyList verhindern. [<=]

3654 **A_27731 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren**
3655 Das ePA-Aktensystem MUSS sicherstellen, dass falls eine LEI (Telematik-ID) aus der
3656 EntitlementDenyList entfernt wird, in der VAU nach spätestens 24 Stunden die
3657 EntitlementDenyList aktualisiert wird. [<=]

3658 **A_27732 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren -**
3659 **Ausschluss einer LEI**
3660 Falls eine LEI der EntitlementDenyList hinzugefügt wird, MUSS der Betreiber des ePA-
3661 Aktensystems sicherstellen, dass die EntitlementDenyList in der VAU unverzüglich
3662 aktualisiert wird. [<=]

3663 Hinweise zu A_27732-*:

- 3664 • Die gematik übermittelt die komplette aktuelle EntitlementDenyList an den
3665 Anbieter des ePA-Aktensystems.
- 3666 • Die gematik übermittelt die aufgrund von Sicherheitsgründen aktualisierte
3667 EntitlementDenyList über die etablierten Incident-Prozesse.

3668 **A_27714 -Entitlement Management - setEntitlementPs in Abhängigkeit von**
3669 **EntitlementDenyList**
3670 Falls der Nutzer auf der EntitlementDenyList enthalten ist, MUSS das Entitlement
3671 Management die Operation `setEntitlementPs` ohne Erzeugung einer Befugnis mit dem
3672 HTTP-Statuscode 409requestMismatch abbrechen.
3673 [<=]

3674 Technische Details zur Aktualisierung der EntitlementDenyList im Aktensystem:

3675 Die gematik liefert regelmäßige Aktualisierungen der EntitlementDenyList an die
3676 Betreiber der ePA-Aktensysteme. Die gematik möchte automatisiert überwachen können,
3677 ob in den ePA-Aktensystemen jeweils die aktuelle Version der EntitlementDenylist
3678 geladen ist. In den ePA-Aktensystemen gibt es jeweils ein Enforcement-Point an dem die
3679 EntitlementDenyList technisch durchgesetzt wird. Mindestens bei Aktualisierung der
3680 EntitlementDenyList im ePA-Aktensystem soll solch ein Enforcement-Point Auskunft über
3681 eine BDE-Meldung darüber geben welche EntitlementDenyList ihm aktuell vorliegt. Dabei
3682 soll eine hohe Aussagekraft der Information erreicht werden, deshalb wird ein Hashwert
3683 über die TelematikIDs der aktuellen EntitlementDenyList erzeugt und dieser Hashwert
3684 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": "peelnuX5TxSce3Qsawdqs+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

3737 verwenden ist.

3738 [$\leq$]

3739 Beispiele für A_27281-*:

3740 1)

3741 Wäre separator="AAA" und TelematikIDs=["1", "2", "3"], dann wären die
3742 dtbh="1AAA2AAA3". Der Base64-kodierte Hashwert wäre
3743 dann NFtIcjtAGzo8tL5goB6QMXpHkNCjDSFK5oTzILjXu8k=

3744 2)

3745 Mit den Daten aus dem oben aufgeführten Beispiel für A_27780-* würde ein
3746 Aktensystem pee1nuX5TxSce3QSawdqs+Pf0L6UMCr80uM3VYtVJdU= berechnen.

3747 **A_27782 -EntitlementDenyList: Hashwertberechnung der Telematik-ID-Einträge** 3748 **im Aktensystem**

3749 Ein ePA-Aktensystem MUSS sicherstellen, dass bei Aktualisierung der
3750 EntitlementDenyList-Daten am Enforcement-Point der EntitlementDenyList wie in
3751 A_22467-* definiert, eine Meldung an die BDE erzeugt und übermittelt wird. Dabei MUSS
3752 es den dabei zu übermittelnden Hashwert wie in A_27781 definiert berechnen. (vgl. auch
3753 Hinweise zu A_22782-*)

3754 [$\leq$]

3755 Hinweise zu A_27782-*:

3756 Zum besseren Verständnis, falls der Enforcement-Point die VAU-Instanz ist, so muss
3757 beim initialen Starten der VAU-Instanz die EntitlementDenyList in die VAU-Instanz
3758 geladen werden. Diese gilt als Aktualisierung der EntitlementDenyList-Daten in der VAU-
3759 Instanz. Somit gilt dort A_27782-*.

3760 **3.9 Legal Policy**

3761 Die Legal Policy enthält die gesetzlich verbindlichen Regelungen der Zugriffsrechte bzgl.
3762 der Berufsgruppen und Datenkategorien gemäß § 341 Absatz 2 SGB V.

3763 Für die Datenkategorien sind die grundsätzlichen Zugriffsrechte der Zugriffsoperationen
3764 (CRUD - create, read, update, delete) vorgegeben. Diese Zugriffsrechte wirken
3765 ausnahmslos für jeden befugten Nutzer.

3766 Beispiele sind:

- 3767 • Apotheker haben keinen Zugriff auf die zahnärztliche Dokumentation in der
3768 Datenkategorie "dental".
- 3769 • Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen
3770 noch löschen.

3771 Die Legal Policy wird durch das Aktensystem durchgesetzt und ist jederzeit vorhanden.
3772 Die Konfiguration kann durch Clients oder Bestandteile des Aktensystems nicht verändert
3773 werden.

3774 **A_19303-26 -Legal Policy – gesetzlich vorgegebene Zugriffsrechte**

3775 Das ePA-Aktensystem MUSS alle in der folgenden Tabelle aufgeführten Regeln der Legal
3776 Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

3777 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

Kategorie	Nutzergruppe										
eau	CRU D	-	-	-	-	R	-	-	-	-	RD
rehab	CRU D	-	-	-	-	-	-	-	-	-	RD
transcripts	CRU D	-	-	-	-	-	-	-	-	-	RD
other	CRU D	-	-	-	-	R	-	-	-	-	RD
Medical Services (FHIR Data Services)	Zugriffsrecht										
medication	CRU D	CRU D	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	-

3778

3779

Nutzergruppen:

3780

3781

- Med = Arztpraxis, Zahnarztpraxis, Krankenhaus, Psychotherapeut, Vorsorge- und Rehabilitation, Öffentlicher Gesundheitsdienst

3782

3783

- (oid_praxis_arzt,, oid_krankenhaus, oid_institution-vorsorge-reha, oid_zahnarztpraxis, oid_praxis_psychotherapeutoid_institution-oegd)

3784

- Apo = Öffentliche Apotheke

- 3785 • (oid_öffentliche_apotheke)
- 3786 • Pflege = Gesundheits-, Kranken- und Altenpflege
- 3787 • (oid_institution-pflege)
- 3788 • GH = Geburtshilfe
- 3789 • (oid_institution-geburtshilfe)
- 3790 • HME = Heilmittelerbringer
- 3791 • (oid_praxis-physiotherapeut, oid_praxis-ergotherapeut, oid_praxis-logopaede,
- 3792 oid_praxis-podologe, oid_praxis-ernaehrungstherapeut)
- 3793 • AM = Arbeitsmedizin
- 3794 • (oid_institution-arbeitsmedizin)
- 3795 • KTR = Kostenträger
- 3796 • (oid_kostentraeger)
- 3797 • OM = Ombudsstelle
- 3798 • (oid_ombudsstelle)
- 3799 • DiGA = Digitale Gesundheitsanwendung
- 3800 • (oid_diga)
- 3801 • eRP = E-Rezept vertrauenswürdige Ausführungsumgebung
- 3802 • (oid_erp-vau)
- 3803 • Ver = Versicherter / Vertreter
- 3804 • (oid_versicherter)

3805 **Legende:**

- 3806 • CRUD = create, read, update, delete; update: Aktualisierung eines Dokuments
- 3807 • "-" = keine Zugriffsrechte;
- 3808 • "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den
- 3809 Dienst (Service) definiert)
- 3810 • "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- 3811 • "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung
- 3812 in einer zukünftigen Version der ePA vorgesehen.

3813 **Hinweise:**

- 3814 • (*) Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann der
- 3815 Versicherte bzw. sein Vertreter oder eine Leistungserbringerinstitution gemäß der
- 3816 zuvor genannten Liste definierter professionOIDs sein. Sofern ein
- 3817 Versicherter/Vertreter der Einsteller der Elternnotiz ist, darf er abweichend von
- 3818 den oben aufgeführten Zugriffsunterbindungsregeln in die Datenkategorie mit
- 3819 dem technischen Identifier 'child' schreiben.
- 3820 • (**) Ein Versicherter bzw. sein Vertreter sowie die Ombudsstelle kann, durch
- 3821 Setzen eines Widerspruchs gegen das Einstellen von Verwaltungsdaten und
- 3822 Dispensierinformation durch den E-Rezept-Fachdienst (erp-submission), das
- 3823 Löschen der im FHIR data service medication gespeicherten Daten erzwingen.

3824 **[<=]**

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

Das ePA-Aktensystem MUSS zusätzlich zu den Regeln aus A_19303-* alle in der folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

Tabelle 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	-

Kategorie	Nutzergruppe
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

3831

3832 Nutzergruppen:

3833 • NCPeH = NCPeH-Fachdienst (oid_ncpeh)

3834 Legende:

3835 • CRUD = create, read, update, delete; update: Aktualisierung eines Dokuments

3836 • "-" = keine Zugriffsrechte;

3837 • "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den
3838 Dienst (Service) definiert)

3839 • "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt

3840 • "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung
3841 in einer zukünftigen Version der ePA vorgesehen.3842 [**<=**]3843 Die folgende Tabelle erläutert die Kategorien und Services aus A_19303-* und A_26166-
3844 *:

3845 **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

Technischer Identifier	Beschreibung
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), siehe ePA Medication Service [gemIG_ePA_Medication]
demographics (patient)	Bereitstellung demographischer Daten des Versicherten für Medical Services, siehe ePA Patient Service, in [gemIG_ePA_Basic]
audit	Protokolle von Zugriffen aller Nutzer auf die Akte des Versicherten, siehe ePA Audit Event Service in [gemIG_ePA_Basic]
Basic Services	Account Management
Consent Decisions	Management der Entscheidungen zu widerspruchsfähigen Funktionen der ePA

Technischer Identifier	Beschreibung
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

3846

3847 **A_21211-01 -Legal Policy - Änderungen der Legal Policy nicht erlauben**

3848 Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass
 3849 Änderungen der Konfiguration der Legal Policy gemäß A_19303-* ausgeschlossen
 3850 sind. [<=]

3851 **A_24548 -Legal Policy - Durchsetzung der Zugriffsrechte der Legal Policy**

3852 Das ePA-Aktensystem MUSS sicherstellen, dass Operationen auf Daten und Operationen
 3853 der Dienste eines Aktenkontos abgebrochen und mit einer Fehlermeldung beendet
 3854 werden, wenn diese Operation durch die Vorgaben der Legal Policy gemäß A_19303-* für
 3855 die Nutzergruppe des Aufrufers der Operation nicht zulässig ist. [<=]

3856 **3.10 Constraint Management**

3857 Das Constraint Management des Aktenkontos stellt sicher, dass nur Zugriffe auf Daten in
 3858 Ordnern der Document Services über die Vorgaben der Legal Policy hinaus zugelassen
 3859 werden, welche nicht vom Versicherten oder einem Vertreter unterbunden (verborgen)
 3860 wurden.

3861 Die Umsetzung dieser Beschränkungen erfolgt anhand der **General Deny Policy** für
 3862 jeden befugten Nutzer der betroffenen Nutzergruppen des Aktenkontos.

3863 Die General Deny Policy adressiert Nutzergruppen (professionOID) und Metadaten
 3864 der Daten. Es können einzelne Dokumente, Kategorien oder Ordner verborgen werden.
 3865 Bei jedem Zugriff auf Daten in Ordnern wird diese Policy bezüglich der Rolle eines
 3866 Nutzers und der betroffenen Dokumente ausgewertet und durchgesetzt.

3867 Die folgende Anforderung zeigt eine Übersicht der Nutzergruppen, für welche Dokumente
 3868 durch Einträge in der General Deny Policy vor einem Zugriff verborgen werden können.

3869 **A_24306-02 -Constraint Management - Policy für berechnigte Nutzergruppen und Nutzer**

3870 Das Constraint Management MUSS die Konfiguration der General Deny Policy auf die
 3871 folgenden Nutzergruppen einschränken:
 3872
 3873

Nutzergruppe [professionOID] der General Deny Policy
--

oid_praxis_arzt

Nutzergruppe [professionOID] der General Deny Policy
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

3874
3875
3876

[<=]

3877
3878
3879
3880
3881
3882

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.

[<=]

3883
3884

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

3885
3886
3887

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

3888
3889
3890

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

- 3891 widerspruchsfähige Funktion "medication" der ePA verhindert (siehe 3.7. Consent
3892 Decision Management).
- 3893 Die Operationen der Schnittstelle des Constraint Managements erlauben die
3894 Konfiguration der General Deny Policy durch den Versicherten oder einen befugten
3895 Vertreter.
- 3896 **A_24395 -Constraint Management - Realisierung der Schnittstelle**
3897 **I_Constraint_Management_Insurant**
3898 Das Constraint Management MUSS die Operationen der Schnittstelle
3899 I_Constraint_Management_Insurant gemäß [I_Constraint_Management_Insurant]
3900 umsetzen.[<=]
- 3901 **A_30184 -Constraint Management - Realisierung der Schnittstelle**
3902 **I_Constraint_Management**
3903 Das Constraint Management MUSS die Operationen der Schnittstelle
3904 I_Constraint_Management gemäß [I_Constraint_Management] umsetzen.[<=]
3905
- 3906 Für die Policy gelten folgende Vorgaben.
- 3907 **A_24393-02 -Constraint Management - Initialisierung der General Deny Policy**
3908 Das Constraint Management MUSS für ein Aktenkonto eine General Deny Policy ohne
3909 initiale Einträge bereitstellen.[<=]
- 3910 **A_24462-01 -Constraint Management - Konfiguration der General Deny Policy**
3911 **anpassen nach Löschen von Ordnern**
3912 Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn
3913 diese einen Ordner referenzieren und dieser Ordner aus dem Aktenkonto gelöscht
3914 wird.[<=]
- 3915 **A_24461-01 -Constraint Management - Konfiguration der General Deny Policy**
3916 **anpassen nach Löschen von Dokumenten**
3917 Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn
3918 diese ein spezifisches Dokument referenzieren und dieses Dokument aus dem
3919 Aktenkonto gelöscht wird.[<=]
- 3920 **A_24516-01 -Constraint Management - Speichern der Inhalte der General Deny**
3921 **Policy**
3922 Das Constraint Management MUSS Einträge aus der General Deny Policy unter
3923 Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.[<=]
- 3924 **3.10.1 Aktenkontoweites Verbergen (General Deny Policy)**
- 3925 Die General Deny Policy wird durch das Aktensystem für die in A_24306-* unter "General
3926 Deny Policy" aufgeführten Nutzergruppen angewendet und durchgesetzt. Einträge der
3927 General Deny Policy gelten dabei immer für alle aufgeführten Nutzergruppen gemeinsam.
- 3928 Die Konfiguration der General Deny Policy erfolgt durch den Versicherten oder einen
3929 befugten Vertreter mittels ePA-FdV. Einträge können hinzugefügt oder entfernt werden.
3930 Zum Zeitpunkt der Erstellung des Aktenkontos enthält die General Deny Policy keine
3931 Einträge.
- 3932 Ein Eintrag in der General Deny Policy referenziert entweder ein bestimmtes Dokument,
3933 einen dynamischen Ordner oder eine Datenkategorie. Die Menge der Einträge ist nicht
3934 limitiert.
- 3935 Jeder Eintrag der General Deny Policy verbirgt die betroffenen Daten und verhindert
3936 deren Nutzung durch Nutzergruppen gemäß A_24306-*. Enthält ein Eintrag der Policy

3937 einen dynamischen Ordner oder eine Kategorie, so werden alle in diesem Ordner bzw.
 3938 Kategorie enthaltenen Daten verborgen und von der Nutzung ausgeschlossen. Ein
 3939 dynamischer Ordner selbst wird ebenfalls verborgen und von der Nutzung
 3940 ausgeschlossen, eine Kategorie selbst wird nicht verborgen. Verborgene Daten schränken
 3941 die Anwendung der Datenoperationen ein, die konkreten Auswirkungen sind bei den
 3942 jeweiligen Operationen definiert.

3943 Beim kategorienbasierten Verbergen von dynamischen Ordnern kann ein einzelner
 3944 Ordner oder die Datenkategorie an sich verborgen werden. In letzterem Fall werden alle
 3945 assoziierten Ordner verborgen.

3946 Bei Kategorien und Ordnern, die zusammengesetzte MIOs oder strukturierte Dokumente
 3947 enthalten (MIOs oder strukturierte Dokumente, deren Inhalt über mehrere Dokumente
 3948 mit Zusammenhang verteilt ist - "Passdokumente") ist das Verbergen einzelner
 3949 Dokumente des MIOs nicht sinnvoll und daher nicht zulässig. In diesen Fällen erfolgt das
 3950 Verbergen der Daten durch das Verbergen der Kategorie bzw. des dynamischen Ordners.
 3951 Diese Einschränkung betrifft die Sammlungstypen "mixed" und "uniform".

3952 Für das erfolgreiche Verbergen von Daten durch Einträge der General Deny Policy muss
 3953 das adressierte Dokument, der Ordner oder die Kategorie im Aktensystem vorhanden
 3954 sein. Wird im Verlauf von Operationen ein Dokument oder ein Ordner gelöscht, so
 3955 werden auch die referenzierenden Policy-Einträge automatisch entfernt (siehe A_24461-*
 3956 und A_24662-*).

3957 Ein Eintrag der General Deny Policy enthält Angaben gemäß der folgenden Tabelle:

3958 **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"
[choice]	rootDocumentId	documentEntry.referenceIdList, Item "rootDocumentUniqueId"	Identifiziert das zu verbergende XDS Dokuments
	masterIdentifizier	DocumentReference.masterIdentifizier.value	Identifiziert das zu verbergende MHD Dokuments

Element		Inhalt	Erläuterung
	folderUUID	folder.entryUUID	Identifiziert des zu verbergenden dynamischen Ordners
	categoryId	categoryId	technischer Identifizierer der zu verbergenden Kategorie

3959

3960 Beispiel:

3961 **Tabelle 20: Verbergen eines Medical Service**

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

3962

3963 Das Verbergen eines einzelnen Dokuments zielt immer auf das Verbergen aller in der
3964 Replace-Kette enthaltenen Dokumente ab.

3965 Die rootDocumentId in XDS verweist auf einen Identifizierer, der die gesamte Replace-Kette
3966 identifiziert. Der masterIdentifizierer in MHD hingegen verweist auf ein konkretes
3967 DocumentReference und damit implizit auf ein konkretes Dokument. Um sicherzustellen,
3968 dass in MHD das Dokument in seiner Gesamtheit (Replace-Kette) verborgen wird, muss
3969 die Replace-Kette eines Dokuments vollständig, d.h. die dazugehörige Liste von
3970 masterIdentifizierern, in die General Deny Policy aufgenommen werden. D.h. wird über die
3971 Schnittstelle `I_Constraint_Management` gemäß `[I_Constraint_Management]` der
3972 Parameter masterIdentifizierer auf die General Deny Policy gesetzt, dann muss das
3973 Constraint Management alle dazugehörigen masterIdentifizierer der Replace-Kette ermitteln
3974 und in die General Deny Policy aufnehmen.

3975 **A_30367 -Constraint Management - General Deny Policy bei MHD für Replace-** 3976 **Kette verarbeiten**

3977 Falls ein Dokument mittels masterIdentifizierer neu verborgen oder sichtbar gemacht wird,
3978 dann MUSS das Constraint Management zu diesem masterIdentifizierer die vollständige
3979 Replace-Kette des Dokuments ermitteln und in der General Deny Policy mit
3980 denyType="document" für jedes Dokument der Replace-Kette den zugehörigen
3981 masterIdentifizierer zum Verbergen aufnehmen bzw. zum Sichtbar machen entfernen. [`<=`]

3982 Der MHD Service übernimmt im weiteren Verlauf die Aktualisierung der General Deny
3983 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 in 3.12.1.10- 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 deviceIdentifizierer 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:

- deviceIdentifizierer
- deviceToken
- createdAt (Zeitpunkt der Erzeugung des deviceTokens)

- 4077 • lastUse
- 4078 • status
- 4079 • displayName
- 4080 • Geräteregistrierungscode,
- 4081 • Fehlerzähler.
- 4082 [$\leq$]
- 4083 Hinweis zu A_25271-*: Für die verschlüsselte Speicherung der Geräteinformationen sind
- 4084 die Anforderungen aus Abschnitt 3.5.1.3 zu berücksichtigen.
- 4085 **A_25272 -Device Management - Pseudonyme Speicherung der**
- 4086 **Geräteinformationen**
- 4087 Das Device Management MUSS sicherstellen, dass die Zuordnung der außerhalb der VAU
- 4088 persistierten verschlüsselten Geräteinformationen zum Nutzer eindeutig ist und durch ein
- 4089 Pseudonym erfolgt. [$\leq$]
- 4090 Hinweis: Aus A_25272 folgt, dass die Zuordnung der Speicherung der verschlüsselten
- 4091 Geräteinformationen nicht über die KVN-R des Nutzers erfolgen darf.
- 4092 **A_25273 -Device Management - Gültigkeitsdauer des Geräteregistrierungscodes**
- 4093 Das Device Management MUSS sicherstellen, dass der bei der Geräteregistrierung
- 4094 erzeugte Geräteregistrierungscode maximal 6 Stunden nach Erzeugung der DeviceID
- 4095 (createdAt) für die Verifikation eines Gerätes genutzt werden kann. [$\leq$]
- 4096 **A_25274 -Device Management - Löschen nach Gültigkeitsdauer des**
- 4097 **Geräteregistrierungscodes**
- 4098 Das Device Management MUSS sicherstellen, dass die Geräteinformationen für eine nicht
- 4099 bestätigte Geräteregistrierung nach Ende der Gültigkeitsdauer des
- 4100 Geräteregistrierungscodes gelöscht werden. [$\leq$]
- 4101 **A_25275 -Device Management - Versenden des Geräteregistrierungscodes per**
- 4102 **E-Mail**
- 4103 Das Device Management MUSS bei der Geräteregistrierung für den Nutzer, für den das
- 4104 Gerät registriert werden soll, alle im Aktensystem hinterlegten E-Mail-Adressen ermitteln
- 4105 und an alle ermittelten E-Mail-Adressen eine E-Mail in einer für den Nutzer verständlichen
- 4106 Form mit folgenden Informationen versenden:
- 4107 • Zweck der E-Mail,
- 4108 • Geräteregistrierungscode,
- 4109 • Gültigkeitsdauer des Geräteregistrierungscodes.
- 4110 [$\leq$]
- 4111 **A_25276 -Device Management - Bestätigung mittels Geräteregistrierungscodes**
- 4112 Das Device Management MUSS für einen übergebenen Geräteregistrierungscode und eine
- 4113 übergebene DeviceID (deviceIdentifier und deviceToken) prüfen, ob der vom Device
- 4114 Management bei der Geräteregistrierung erzeugte Geräteregistrierungscode für das
- 4115 angegebene Gerät (deviceIdentifier, deviceToken) mit dem übergebenen
- 4116 Geräteregistrierungscode übereinstimmt sowie der Geräteregistrierungscode zeitlich
- 4117 gültig ist und
- 4118 1. bei Gleichheit und
- 4119 a. zeitlicher Gültigkeit
- 4120 • den Status für die Geräteregistrierung wechseln, so dass die erfolgreiche
- 4121 Bestätigung des Geräts aus dem Status hervorgeht,

- 4122 • den Geräteregistrierungscode und den Fehlerzähler aus den
- 4123 Geräteinformationen löschen und
- 4124 • den Zeitpunkt der erfolgreichen Bestätigung in lastUsed erfassen,
- 4125 b. zeitlicher Ungültigkeit
- 4126 • alle Geräteinformationen zu diesem deviceIdentifier löschen,
- 4127 2. bei Ungleichheit den Fehlerzähler der Geräteinformation um eins erhöhen und
- 4128 • falls der Fehlerzähler größer oder gleich fünf ist,
- 4129 • alle Geräteinformationen zu diesem Gerät löschen.

4130 [`<=`]

4131 **A_25277 -Device Management - Sperrung bei vermehrter Anzahl von**
 4132 **abgebrochenen Geräteregistrierungen**

4133 Falls für einen Nutzer innerhalb von 8 Stunden drei Geräteregistrierungen abgebrochen
 4134 werden mussten, MUSS das Device Management sicherstellen, dass dieser Nutzer für 8
 4135 Stunden ab dem Zeitpunkt der dritten abgebrochenen Geräteregistrierung keine Geräte
 4136 mehr registrieren darf. [`<=`]

4137 **A_28157 -Device Management - Limitierung der Anzahl unbestätigter**
 4138 **Geräteregistrierungen**

4139 Das Device Management MUSS die Anzahl der gleichzeitig unbestätigten
 4140 Geräteregistrierungen eines Nutzers auf die maximale Anzahl 5 begrenzen. [`<=`]

4141 **A_25291 -ePA-Aktensystem - Health Record Context nur mit verifizierten Gerät**

4142 Das ePA-Aktensystem MUSS sicherstellen, dass ein Versicherter (auch wenn er als
 4143 Vertreter agiert) einen Health Record Context ausschließlich mit einem verifizierten Gerät
 4144 öffnen kann, außer für den Fall, dass sich der Versicherte am ePA-FdV des Vertreters
 4145 anmeldet (d.h. `x-authorize-representative=True` bei der
 4146 `OperationI_Authorization_Service::sendAuthorizationRequestFdV`). [`<=`]

4147 Eine Geräteregistrierung im Home-AS kann in einem anderen Aktensystem nachgenutzt
 4148 werden. Hierzu kann ein ePA-FdV mittels `getDeviceAttestation` eine Device Attestation
 4149 vom Home-AS abrufen, welche beim anderen Aktensystem genutzt werden kann.

4150 **A_26157 -Device Management - Device Attestation kann nur mit verifiziertem**
 4151 **Gerät abgerufen werden**

4152 Das Device Management MUSS sicherstellen, dass die Operation `getDeviceAttestation`
 4153 ausschließlich nach erfolgreicher Authentifizierung des Nutzers und mit einem auf den
 4154 Nutzer registrierten und verifizierten Gerät erfolgt.
 4155 [`<=`]

4156 **A_26156 -Device Management - Inhalte der Device Attestation**

4157 Das Device Management MUSS sicherstellen, dass eine von einem ePA-FdV über die
 4158 Operation `getDeviceAttestation` abgerufene Device Attestation folgende Inhalte
 4159 enthält:

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

Attribut	Inhalt
exp	Verfalldatum, = "iat" + 2 Stunden

4160 [$\leq$]

4161 **A_26158 -Device Management - Signatur der Device Attestation**

4162 Das Device Management MUSS sicherstellen, dass die über `getDeviceAttestation`
 4163 abgerufene Device Attestation mit dem privaten Schlüssel der Signaturidentität der VAU
 4164 des Home-AS signiert wird. [$\leq$]

4165 **A_28648 -ePA-Aktensystem - optionale Umsetzung von Snippet Management**

4166 Das ePA-Aktensystem KANN auf die Realisierung der Operationen des Snippet
 4167 Management gemäß `[I_Device_Management_Insurant]` verzichten. [$\leq$]

4168 **3.12 Medical Services**

4169 **A_25830-05 -XDS Document Service - Reihenfolge der Auswertung Legal Policy,**
 4170 **Deny Policy und Constraints**

4171 Der XDS Document Service MUSS bei der Nutzung von Operationen des XDS Document
 4172 Service die Prüfung der zugriffsverhindernden Eigenschaften in der Reihenfolge

- 4173 1. die statisch prüfbaren Beschränkungen des Aufrufenden bezüglich seiner Rolle,
- 4174 2. die Existenz oder Einschränkungen aus dem Status des Aktenkontos,
- 4175 3. die Befugnis des Aufrufenden,
- 4176 4. die weiteren Beschränkungen der Legal Policy,
- 4177 5. die Einträge der General Deny Policy.

4178 anwenden. [$\leq$]

4179 *Hinweis: Statisch prüfbare Beschränkungen sind Eigenschaften, die vor einer Öffnung der*
 4180 *Akte bewertet werden können.*

4181 *Hinweis: Beispielsweise kann eine Operation nicht erfolgreich ausgeführt werden, wenn*
 4182 *diese den Vorgaben der Legal Policy und gleichzeitig einem Eintrag der General Deny*
 4183 *Policy widerspricht. Die Fehlermeldung zum Abbruch der Operation resultiert dann aus*
 4184 *der Prüfung der Legal Policy, da die Bedingungen dieser gemäß der definierten*
 4185 *Reihenfolge vor den Bedingungen der General Deny Policy geprüft werden müssen.*

4186 **3.12.1 XDS Document Service**

4187 Die gesetzlichen Vorgaben schränken den Zugriff Dritter auf Dokumente
 4188 über berufsgruppenspezifische Vorgaben gemäß § 341 Absatz 2 SGB V ein. Dazu
 4189 verwendet der XDS Document Service festgelegte Datenkategorien, welche mit
 4190 spezifischen Zugriffsrechten der grundlegenden Zugriffsoperationen (CRUD - create,
 4191 read, update, delete) wirken.

4192 Jedes eingestellte Dokument wird vom XDS Document Service mit einer automatischen
 4193 Zuordnung zu einem statischen Ordner, welcher die Datenkategorie repräsentiert,
 4194 erweitert. Diese statischen Ordner sind initial bei jedem Aktenkonto eines Versicherten
 4195 existent. Die serverseitige Zuordnung in diese Ordner erfolgt anhand der XDS-Metadaten
 4196 in Kombination mit der Nutzergruppe des Einstellers.
 4197 Das bedeutet weiterhin, dass das Anlegen von statischen Ordnern durch ePA-Clients nicht

4198 erlaubt ist, um eine zweifelsfreie Anwendung der Zugriffsregeln auf Grundlage der
4199 Datenkategorien zu gewährleisten.

4200 Eine Ausnahme bilden bestimmte medizinische Informationsobjekte (MIOs), die eine
4201 weitere Gruppierung innerhalb der zugeordneten Datenkategorie erfordern. Ein Beispiel
4202 dafür ist der Mutterpass. Die Dokumente eines Mutterpasses müssen für die konkrete
4203 Schwangerschaft innerhalb der Kategorie separiert werden. Für die betroffenen
4204 Kategorien wird daher kein statischer Ordner vorbereitet, sondern der separierende,
4205 dynamische Ordner muss zeitgleich mit einer Dokumentenregistrierung durch den ePA-
4206 Client angelegt werden,

4207 ePA-Clients, die Dokumente für MIOs einstellen, können die dem MIO zugeordnete
4208 Kategorie und die Art des Ordners (statisch, dynamisch) aus den Metadatenvorgaben für
4209 MIOs gemäß [Implementation-Guidelines] entnehmen.

4210 Die Durchsetzung der Zugriffskontrolle auf die Kategorien, Ordner und Dokumente
4211 gemäß der gesetzlichen Vorgaben und ggf. weiterer Beschränkungen durch den
4212 Versicherten oder einen Vertreter erfolgt durch das Constraint Management (siehe 3.10.-
4213 Constraint Management).

4214 **3.12.1.1 Formatprüfung beim Einstellen von Dokumenten**

4215 **A_25233 -XDS Document Service - erlaubte Formate für PDF-Dokumente**

4216 Der XDS Document Service MUSS sicherstellen, dass ausschließlich die folgenden PDF/A-
4217 Formate unterstützt werden:

- 4218 • PDF/A-1a
- 4219 • PDF/A-1b
- 4220 • PDF/A-2a
- 4221 • PDF/A-2u
- 4222 • PDF/A-2b

4223 [<=]

4224 **A_24864-05 -XDS Document Service - Prüfen auf zulässiges Format beim** 4225 **Einstellen von Dokumenten**

4226 Der XDS Document Service MUSS beim Einstellen eines Dokumentes prüfen, dass das
4227 Dokument eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und den
4228 in Klammern angegebenen Dateiendungen (DocumentEntry.URI) besitzt

- 4229 • application/pdf nur PDF/A gemäß A_25233 (pdf)
- 4230 • application/hl7-v3 (xml)
- 4231 • application/pkcs7-mime (p7s oder p7)
- 4232 • application/fhir+xml (xml)
- 4233 • application/fhir+json (json)

4234 sowie der tatsächliche Inhalt des Dokuments konform mit dem behaupteten MIME-Type
4235 ist. Falls die Prüfung nicht erfolgreich ist, muss das Einstellen des Dokumentes abgelehnt
4236 werden.[<=]

4237 *Hinweise zu A_24864-*:*

- 4238 • *Dokumente im PDF-Format werden vom XDS Document Service abgelehnt, da sie*
4239 *ausführbaren Code enthalten können. Daher müssen die Clients, falls sie*
4240 *Dokumente im PDF-Format einstellen wollen, diese zunächst in ein PDF/A*
4241 *konvertieren.*

- 4242 • *p7s ist die Default-Dateiendung für Dokumente des mimetypes application/pkcs7-*
4243 *mime in der ePA und für Dokumente dieses mimetypes gemäß*
4244 *[gemSpec_IG_ePA] und für automatisierte Anpassungen von filename extensions*
4245 *bei Dokumentenupload (A_23447-*, A_24451-*) zu berücksichtigen.*

4246 **A_25009-04 -XDS Document Service - Prüfen auf zulässiges Format beim**
4247 **Einstellen von Dokumenten durch Versicherte**

4248 Der XDS Document Service MUSS sicherstellen, dass Versicherte ausschließlich
4249 Dokumente eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und
4250 den in Klammern angegebenen Dateiendungen (DocumentEntry.URI) einstellen können:

- 4251 • application/pdf nur PDF/A gemäß A_25233* (pdf)

4252 [**<=**]

4253 **A_28620-01 -XDS Document Service - Mindestanforderungen an die**
4254 **Dokumentenformatprüfung**

4255 Die gemäß A_24864-* und A_25009-* geforderte Prüfung des zulässigen
4256 Dokumentenformats muss mindestens

- 4257 • bei allen Formaten eine Prüfung auf Magic Bytes (soweit technisch möglich),
4258 • bei XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es bei
4259 XML-Dokumenten kein valides UTF8 ist, prüfen auf "restriktives" ISO-8859-15.
4260 Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09, 0x0a und 0x0d),
4261 1, 8, 9 sowie 0x7f verboten sind.",
4262 • bei XML-, und JSON-Dokumenten eine Prüfung der XML- bzw. JSON-Validität mit
4263 Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet
4264 sind,
4265 • auf den signierten Inhalt eines PKCS7-Dokuments sind die Regeln ebenfalls
4266 anzuwenden

4267 umfassen.

4268 Eine alleinige Prüfung auf Basis der Magic Bytes ist für kein Format ausreichend. Werden
4269 keine zusätzlichen Prüfmaßnahmen durchgeführt, dürfen die Dokumente nicht in die Akte
4270 eingestellt werden können.

4271 Für XML-Dokumente muss eine Schema-Validierung ausschließlich auf Basis bekannter,
4272 intern vorliegender XML Schema-Definitionen durchgeführt werden. Gegen nicht intern
4273 vorliegende XML Schema-Definitionen wird nicht validiert. Die Schema-Validierung kann
4274 innerhalb des Health Record Contexts ohne zusätzliche Isolation erfolgen. [**<=**]

4275 **A_29876 -XDS Document Service - PKCS7 für signierte XML- oder JSON-**
4276 **Dokumente**

4277 Der XDS Document Service MUSS sicherstellen, dass der signierte Inhalt eines PKCS7-
4278 Dokuments ausschließlich ein XML- oder JSON-Dokument ist. [**<=**]

4279 **A_24867 -XDS Document Service - Isolation der Formatprüfung**

4280 Der XDS Document Service MUSS die Prüfung des Dateiformats (siehe A_24864-*) beim
4281 Einstellen eines Dokuments so technisch isolieren, dass kein Schaden für Aktenkonten
4282 oder das ePA-Aktensystem selbst entsteht.

4283 [**<=**]

4284 *Hinweise zu A_24867-*:*

4285 *Hier kann z.B. eine Art Sandboxing oder eine separate VAU-Instanz verwendet werden,*
4286 *um die Isolation umzusetzen.*

4287 *Der in A_24636-* geforderte technische Separationsmechanismus zur Isolation von*
4288 *Health Record Contexten innerhalb einer VAU-Instanz kann ebenfalls zur Isolation der*
4289 *Formatprüfung in A_24867-* genutzt werden.*

4290 *Findet eine Dokumentenformatprüfung innerhalb eines Health Record Context statt, wird*
4291 *durch den Isolationsmechanismus aus A_24636-* verhindert, dass sich die*
4292 *Dokumentenformatprüfung schadhaft auf andere Health Record Contexte auswirkt. Es*
4293 *verbleibt dann zur Umsetzung der A_24867-* noch zu gewährleisten, dass sich die*
4294 *Dokumentenformatprüfung nicht schadhaft auf den Health Record Context auswirkt, in*
4295 *dem die Dokumentenformatprüfung erfolgt.*

4296 *Wenn Dokumentenprüfungen innerhalb eines Health Record Contexts ohne Isolation*
4297 *erfolgen, muss sichergestellt werden, dass sich diese Prüfungen nicht schadhaft auf den*
4298 *Health Record Context (oder andere) auswirken können. Dies ist vom Produktgutachter*
4299 *zu prüfen und im Produktgutachten zu dokumentieren.*

4300 *Ein Ausschluss einer schadhaften Auswirkung auf den Health Record Context ist bei*
4301 *folgenden Prüfungen des Dokumentenformats denkbar, so dass diese innerhalb des*
4302 *Health Record Contexts ohne zusätzliche Isolationsmaßnahmen durchgeführt werden*
4303 *können und kein Verstoß gegen die Anforderung A_24867-* vorliegt:*

- 4304 • *Prüfung der Magic Bytes des Dokuments (wo technisch möglich)*
- 4305 • *bei XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es bei*
4306 *XML-Dokumenten kein valides UTF8 ist, eine Prüfung auf "restriktives" ISO-8859-*
4307 *15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09,*
4308 *0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind."*
- 4309 • *bei XML- und JSON-Dokumenten: Parsen der Dokumente auf valides XML bzw.*
4310 *JSON mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert*
4311 *und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu*
4312 *bestätigen.*
- 4313 • *bei pkcs7-Dokumenten: Parsen der Dokumente mit Parsern, die entsprechend den*
4314 *Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser*
4315 *ist durch den Produktgutachter zu bestätigen.*

4316 *Der Produktgutachter muss bei der Umsetzung der oben genannten Prüfungen*
4317 *bestätigen, dass der Ausschluss einer schadhaften Auswirkung auf den Health Record*
4318 *Context (oder andere) durch die Umsetzung im Produkt tatsächlich gegeben ist.*

4319

4320 **A_28663 -XDS Document Service – Keine PDF/A-Formatprüfung bei Import im**

4321 **Rahmen eines Aktenumzugs**

4322 *Der XDS Document Service MUSS die Prüfung des Dateiformats (siehe A_24864-*) beim*
4323 *Importieren eines PDF/A-Dokuments im Rahmen eines Aktenumzugs (Health Record*
4324 *Relocation) abschalten.*

4325 **[<=]**

4326 *Die komplexe Validierung von PDF/A-Dokumenten in den Aktensystemen verschiedener*
4327 *Hersteller kann zu unterschiedlichen Ergebnissen führen (valide vs. nicht valide). Da*
4328 *jedoch die Validität im exportierenden Aktensystem und damit eine gewisse*
4329 *Formatqualität des Dokuments bereits nachgewiesen wurde, wird aus Gründen der*
4330 *Vollständigkeit der importierten Dokumente im importierenden System auf die Prüfung*
4331 *verzichtet.*

4332 **A_25285 -XDS Document Service - Sicheres Löschen von Dokumenten mit**
4333 **unzulässigem Format**

4334 Falls der XDS Document Service bei der Prüfung des Dateiformats (siehe A_24864-*)
4335 beim Einstellen eines Dokuments ein unzulässiges Format erkennt, MUSS der XDS
4336 Document Service das Dokument sicher löschen.

4337 [$\leq$]

4338 **A_24943 -XDS Document Service - Formatprüfung exponiert keine Daten aus**
4339 **der VAU heraus**

4340 Der XDS Document Service MUSS sicherstellen, dass bei der Formatprüfung (siehe
4341 A_24864-*) keine innerhalb der VAU verarbeiteten Daten die VAU verlassen. [$\leq$]

4342 **3.12.1.2 Anforderungen zur Validierung**

4343 **A_15035 -XDS Document Service – Verwendung von SOAP Message Security 1.1**

4344 Der XDS Document Service MUSS die Sicherheitsanforderungen aus SOAP Message
4345 Security 1.1 [WSS] für die Verarbeitung von SOAP 1.2-Nachrichten umsetzen. [$\leq$]

4346 **A_15034 -XDS Document Service – Unterstützung von Profilen der Web**
4347 **Services Interoperability Organization (WS-I)**

4348 Der XDS Document Service MUSS das WS-I Basic Profile V2.0 [WSIBP], das WS-I Basic
4349 Security Profile Version V1.1 [WSIBSP] sowie das WS-I Attachment Profile V1.0 [WSIAP]
4350 für die Kommunikation über Web Services berücksichtigen. [$\leq$]

4351 **A_15186 -XDS Document Service – Prüfung der Kombination von WS-**
4352 **Addressing Action und SOAP Body**

4353 Der XDS Document Service MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-
4354 Eingangsnachrichten dahingehend prüfen, ob die angegebene WS-Addressing Action zum
4355 SOAP Body passt. Ist diese Kombination nicht passend, MUSS der XDS Document Service
4356 die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und die
4357 Verarbeitung der Nachricht abbrechen. [$\leq$]

4358 **A_15585 -XDS Document Service – Gleichheit von SOAP Action und WS-**
4359 **Addressing Action**

4360 Der XDS Document Service MUSS SOAP 1.2-Eingangsnachrichten mit einem HTTP-
4361 Statuscode 400 gemäß [RFC7231] quittieren und die Verarbeitung der Nachricht
4362 abbrechen, falls die Werte aus SOAP Action (HTTP Header) und des `Action`-Elements
4363 [WSA] des SOAP Headers nicht übereinstimmen. [$\leq$]

4364 **A_14465-01 -XDS Document Service – XML Schema-Validierung für SOAP-**
4365 **Eingangsnachrichten**

4366 Der XDS Document Service MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-
4367 Eingangsnachrichten einer XML Schema-Validierung auf Basis ausschließlich intern
4368 vorliegender XML Schema-Definitionen unterziehen und gemäß [SOAP] verarbeiten. Sind
4369 Nachrichten nicht wohlgeformt oder ungültig, MUSS der XDS Document Service die
4370 Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren. [$\leq$]

4371 **A_14809 -XDS Document Service – Keine Verwendung des**
4372 **"xsi:schemaLocation"-Attributs**

4373 Der XDS Document Service MUSS SOAP 1.2-Eingangsnachrichten mit einem HTTP-
4374 Statuscode 400 gemäß [RFC7231] quittieren, falls ein `xsi:schemaLocation`-Attribut
4375 gemäß [XMLSchema#2.6.3] enthalten ist. [$\leq$]

4376 **A_14811-01 -XDS Document Service – Ablehnung von SOAP 1.2-Nachrichten**
4377 **ohne UTF-8 Kodierung**

4378 Der XDS Document Service MUSS SOAP 1.2-Nachrichten dahingehend prüfen, dass diese
4379 der Zeichenkodierung UTF-8 entsprechen, und andernfalls die Operation einem
4380 geeigneten HTTP-Statuscode gemäß [RFC7231] ablehnen. [$\leq$]

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 `deroid 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-Dokument 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

Präfix	Namensraum
xdsb	urn:ihe:iti:xds-b:2007
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

4408 **3.12.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und** 4409 **Abruf von Dokumenten**

4410 *3.12.1.4.1 Anforderungen an IHE ITI-Akteure*

4411 In diesem Abschnitt werden Anforderungen und Einschränkungen an relevante IHE ITI-
4412 Akteure und -Transaktionen des XDS Document Service gestellt, um die geforderte IHE
4413 ITI-Semantik zum ePA-Aktensystem zu bewahren. Werden IHE ITI-Akteure mit weiteren
4414 Sub-Akteuren gruppiert, so werden die Anforderungen der Sub-Akteure zum gruppierten
4415 Akteur übernommen. Eine Übersicht und Herleitung der IHE ITI-Akteure ist 3.12.1.4.2-
4416 Überblick über gruppierte IHE ITI-Akteure und Optionen zu entnehmen.

4417 *Hinweis: Alle spezifizierten Anforderungen der IHE ITI-Akteure definieren das zu*
4418 *implementierende Verhalten an den Außenschnittstellen *I_Document_Management* sowie*
4419 **I_Document_Management_Insurant*.*

4420 **A_17826-01 -XDS Document Service – Außenverhalten der IHE ITI-** 4421 **Implementierung**

4422 Der XDS Document Service DARF NICHT vom Verhalten der definierten
4423 Außenschnittstellen *I_Document_Management*, sowie *I_Document_Management_Insurant*
4424 aus Abschnitt 3.12.1.6 abweichen. Dies schließt über die Anforderungslage
4425 hinausgehende Implementierungen von IHE ITI-Akteuren und Optionen innerhalb
4426 des XDS Document Service mit ein, sodass zusätzlich implementierte IHE-
4427 Funktionalitäten keine Auswirkungen an den definierten Außenschnittstellen aufweisen
4428 dürfen. [$\leq$]

4429 **A_13806 -XDS Document Service – Implementierung des IHE ITI-Akteurs XDS** 4430 **Document Registry**

4431 Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Registry"
4432 gemäß [IHE-ITI-TF1] implementieren. [$\leq$]

4433 **A_14727 -XDS Document Service – Implementierung des IHE ITI-Akteurs XDS** 4434 **Document Repository**

4435 Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Repository"
4436 gemäß [IHE-ITI-TF1] implementieren. [$\leq$]

4437 Die § 309-konforme Protokollierung von Zugriffen erfolgt mit Mechanismen außerhalb
4438 des IHE ITI-TF. Eine technische Protokollierung via ATNA kann gemäß der Anforderung
4439 A_17826 dennoch erfolgen.

- 4440 **A_13809 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
4441 **ATNA Audit Record Repository**
4442 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "ATNA Audit Record
4443 Repository" gemäß [IHE-ITI-TF1] implementieren.[<=]
- 4444 Die Mechanismen der IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure
4445 Application" zur Node Authentication werden über das Konzept "Vertrauenswürdige
4446 Ausführungsumgebung" (siehe 3.4- Vertrauenswürdige Ausführungsumgebung (VAU)
4447 umgesetzt, sodass die Nutzung des Integrationsprofils ATNA diesbzgl. eingeschränkt
4448 wird.
- 4449 **A_17166 -XDS Document Service – Keine Implementierung der IHE ITI-Akteure**
4450 **ATNA Secure Node sowie ATNA Secure Application für Node Authentication**
4451 Der XDS Document Service DARF zur Node Authentication die IHE ITI-Akteure "ATNA
4452 Secure Node" sowie "ATNA Secure Application" gemäß [IHE-ITI-TF1] NICHT
4453 implementieren.[<=]
- 4454 Der Zeitdienst der Telematikinfrastruktur unterstützt das Network Time Protocol in
4455 Version 4. Das IHE ITI-TF verlangt hingegen, das Zeitsynchronisierungsprotokoll in
4456 Version 3.
- 4457 **A_14654 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
4458 **CT Time Client**
4459 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "CT Time Client"
4460 gemäß [IHE-ITI-TF1] implementieren.[<=]
- 4461 **A_14665 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
4462 **XDS Document Source**
4463 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDSDocument Source"
4464 gemäß [IHE-ITI-TF1] implementieren.[<=]
- 4465 **A_14667 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
4466 **XDS Integrated Document Source/Repository**
4467 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Integrated Document
4468 Source/Repository" gemäß [IHE-ITI-TF1] implementieren.[<=]
- 4469 **A_14668 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
4470 **XDS Document Consumer**
4471 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Consumer"
4472 gemäß [IHE-ITI-TF1] implementieren.[<=]
- 4473 **A_14666 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
4474 **XDS Patient Identity Source**
4475 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Patient Identity
4476 Source" gemäß [IHE-ITI-TF1] implementieren.
4477 [<=]
- 4478 **A_14669 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
4479 **XDS On-Demand Document Source**
4480 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS On-Demand Document
4481 Source" gemäß [IHE-ITI-TF1] implementieren.[<=]
- 4482 **A_14950 -XDS Document Service – Keine Angabe einer Fehlerlokalisierung im**
4483 **RegistryError-Element**
4484 Der XDS Document Service DARF NICHT das location-Attribut im rs:RegistryError-
4485 Element in der IHE ITI-Ausgangsnachricht verwenden, sofern ein Fehler bei der
4486 Verarbeitung einer IHE ITI-Eingangsnachricht auftritt. Diese Einschränkung gilt nur für
4487 Error Stack Traces bzw. der Offenbarung von Programmierdetails.[<=]

- 4488 3.12.1.4.1.1 Gruppierungen mit anderen IHE ITI-Akteuren
- 4489 3.12.1.4.1.2 Optionen des IHE ITI-Akteurs
- 4490 **A_14637 -XDS Document Service – XDS Document Registry ohne**
- 4491 **"Asynchronous Web Services Exchange"-Option**
- 4492 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
- 4493 "Asynchronous Web Services Exchange" unterstützen.[<=]
- 4494 **A_14638 -XDS Document Service – XDS Document Registry mit "Reference ID"-**
- 4495 **Option**
- 4496 Der XDS Document Service als XDS-Akteur "Document Registry" MUSS die
- 4497 Option "Reference ID" unterstützen.[<=]
- 4498 **A_14639 -XDS Document Service – XDS Document Registry ohne "Patient**
- 4499 **Identity Feed"-Option**
- 4500 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
- 4501 "Patient Identity Feed" unterstützen.
- 4502 [<=]
- 4503 **A_14640 -XDS Document Service – XDS Document Registry ohne "Patient**
- 4504 **Identity Feed HL7v3"-Option**
- 4505 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
- 4506 "Patient Identity Feed HL7v3" unterstützen.[<=]
- 4507 **A_14641 -XDS Document Service – XDS Document Registry ohne "On-Demand**
- 4508 **Documents"-Option**
- 4509 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
- 4510 "On-Demand Documents" unterstützen.[<=]
- 4511 3.12.1.4.1.3 Optionen des IHE ITI-Akteurs
- 4512 **A_14636 -XDS Document Service – XDS Document Repository ohne**
- 4513 **"Asynchronous Web Services Exchange"-Option**
- 4514 Der XDS Document Service als XDS-Akteur "Document Repository" DARF NICHT die
- 4515 Option "Asynchronous Web Services Exchange" unterstützen.[<=]
- 4516 3.12.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen
- 4517 Die folgende Tabelle fasst die oben definierten Anforderungen zu Gruppierungen und
- 4518 Optionen zusammen. Dabei wird die folgende Notation für Optionalitäten (Opt.)
- 4519 verwendet:
- 4520 **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.

4521

4522
4523

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

IHE ITI-Akteur	Opt.			Umzusetzende Option des IHE ITI-Akteurs	Opt.
		Gruppierung mit anderem IHE ITI-Akteur	Opt.		
ATNA Audit Record Repository	X				
CT Time Client	X				
XDS Document Consumer	X				
XDS Document Registry	R			Asynchronous Web Services Exchange	X
				On-Demand Documents	X
				Patient Identity Feed	X
				Patient Identity Feed HL7v3	X
				Reference ID	R
	ATNA Secure Node oder Secure Application für Node Authentication		X		
XDS Document Repository	R			Asynchronous Web Services Exchange	X
		ATNA Secure Node oder Secure Application für Node Authentication		X	
XDS Document Source	X				

IHE ITI-Akteur	Opt.			Umzusetzende Option des IHE ITI-Akteurs	Opt.
		Gruppierung mit anderem IHE ITI-Akteur	Opt.		
XDS Integrated Document Source / Repository	X				
XDS On-Demand Document Source	X				
XDS Patient Identity Source	X				

4524

4525 3.12.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen

4526 **A_17832 -XDS Document Service – Unterstützung MTOM/XOP**

4527 Der XDS Document Service MUSS gemäß den Anforderungen von [IHE-ITI-
 4528 TF2#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM]
 4529 verwenden.[<=]

4530 **A_24524 -XDS Document Service - Migration, Upload: Normalisieren des URI**

4531 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten
 4532 den `DocumentEntry.URI` normalisieren. Dies gilt für `FileURI`, z.
 4533 B. "[file:///C:/path/to/file.html#anchor](#)" oder "`/C/path/to/file.html#anchor`". Die URI MUSS
 4534 auf den reinen Dateinamen mit Extension (d. h. ohne Pfadangaben) reduziert werden, z.
 4535 B. "`file.html`". Nach der Normalisierung MUSS eine Validierung der Extension
 4536 gemäß A_23447-* erfolgen.[<=]

4537 **A_23447-01 -XDS Document Service - DocumentEntry.URI extension entspricht mimetype**

4538 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten
 4539 das Metadatum `DocumentEntry.URI` daraufhin prüfen, ob `DocumentEntry.URI` eine
 4540 filename extension aufweist, die nicht dem `DocumentEntry.mimetype` entspricht. Zuvor
 4541 muss die URI mittels A_24524-* normalisiert worden sein. Danach MUSS der XDS
 4542 Document Service sicherstellen, dass in `Document.URI` die filename extension dem
 4543 `DocumentEntry.mimeType` entspricht. Im Falle einer Abweichung MUSS an die
 4544 ursprüngliche `DocumentEntry.URI` die filename extension gemäß A_24864-*, bzw.
 4545 A_25009-*, angehängt werden, die dem `mimeType` entspricht. Die Groß-
 4546 /Kleinschreibung der filename extension ist bei der Prüfung nicht relevant.[<=]

4548 **A_24451-03 -XDS Document Service - Automatisches initiales Erzeugen einer versionsübergreifenden ID für Dokumente**

4549 Der XDS Document Service MUSS beim initialen Einstellen eines Dokumentes die
 4550 `DocumentEntry.uniqueId` als Eintrag einer `ReferenceID` in die `ReferenceIDList` in
 4551

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 zurückgegebenenXDSRegistryMetadataError-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
 einemXDSRepositoryMetadataError quittieren, sofern die Metadaten nicht konform zu
 den Nutzungsvorgaben sind. Es MUSS im codeContext-Attribut
 des zurückgegebenenrs: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>"

[<=]

4602 Hinweis:
4603 `uniqueId` kann auch auf ein `SubmissionSet` zeigen. In diesem Fall entsprechen die
4604 Metadatenattribute des `SubmissionSet` nicht den Nutzungsvorgaben.

4605 Beispiel:
4606 `codeContext =`
4607 `"uniqueId='2.25.269167723254896828623';metadata='authorPerson';metadata='au`
4608 `thorRole';errorText='Cannot register document: Metadata do not match`
4609 `A_14760'"`

4610 **A_28662-02 -XDS Document Service – Kein Code System mit Präfix "urn:oid"**

4611 Der XDS Document Service MUSS `DocumentEntries`, `SubmissionSets`, `Associations` und
4612 `Folders` ablehnen, wenn mindestens einer der verwendeten Codes einen Code System-
4613 Wert in den Metadaten enthält, der mit "urn:oid:" beginnt, und die entsprechende
4614 Operation mit dem Fehler `XDSRegistryMetadataError` abbrechen. Es MUSS im
4615 `codeContext`-Attribut des zurückgegebenen `XDSRegistryMetadataError`-Elements der
4616 Text `"uniqueId='2.25.269167723254896828623';errorText='Cannot accept`
4617 `metadata: Code system must not contain urn:oid prefix'"` zurückgegeben werden,
4618 wobei `<uniqueId>` dem `uniqueId`-Wert des entsprechenden Objekts (bspw.
4619 `DocumentEntry.uniqueId`) entsprechen muss.

4620 [`<=`]

4621 **A_28841 -XDS Document Service – Persistierung neuer Metadaten mit** 4622 **"preferred" Identifier und ggf. Version**

4623 Der XDS Document Service MUSS beim Persistieren von `DocumentEntries`,
4624 `SubmissionSets`, `Associations` und `Folders` etwaige Codes in den Metadaten derart
4625 abspeichern, dass das entsprechende Code System immer mit dem Haupt-
4626 Identifier ("preferred" Name in `[gemIG_TI_Terminology]`) persistiert wird, auch wenn
4627 der Einstellende einen alternativen Identifier verwendet hat.
4628 Wenn das Code System gemäß `[gemIG_TI_Terminology]` eine Version führt, muss diese
4629 ebenfalls persistiert werden.

4630 [`<=`]

4631 Ziel ist es eine möglichst konsistente und gleichförmige Datenbasis im Aktensystem zu
4632 pflegen.

4633 **A_28842-01 -XDS Document Service – Einstellen von Code Systeme ohne** 4634 **Versionsangabe**

4635 Der XDS Document Service MUSS beim Einstellen von `DocumentEntry`-Metadaten, die
4636 Codes enthalten, jeden Code, der mit einem Code System mit URL-basiertem Identifier
4637 aber ohne Versionsangabe geschickt wird, wie folgt behandeln:

4638 1. Die aktuellste Version des Code System gemäß `[gemIG_TI_Terminology]`, bzw.
4639 wenn dort nicht existent ggf. die aktuellste "deprecated"-Version gemäß
4640 `A_28834*`, wird ergänzt.

4641 2. Prüfung, ob der Code in der derart konstruierten Version des Code System
4642 existiert.

4643 Wenn der Code in der so konstruierten Version des Code Systems existiert, MUSS der
4644 XDS Document Service das Einstellen wie gewohnt fortsetzen, als wenn der Client den
4645 Code unter Angabe der neuesten Code System-Version gesendet hätte.

4646
4647 Andernfalls MUSS der XDS Document Service die Anfrage ggf. mit demselben Fehler
4648 ablehnen, der auch beim Einstellen mit einem anderen nicht existierenden Codes
4649 zurückgegeben würde.

4650 [`<=`]

4651 Diese Regelung erlaubt es, insbesondere KDL 2024-Codes bis auf weiteres in ePA 3.1.3
4652 unter Angabe der Code System URL aber ohne Angabe der dazugehörigen Version
4653 einzustellen wie es in ePA 3.0.5 möglich war. Dies soll (insbesondere nicht auf 3.1.3
4654 migrierten) Clients den Übergang von 3.0.5 nach 3.1.3 erleichtern.

4655 A_28841* gilt auch hier nach wie vor, das heißt ggf. wird der Code mit Haupt-URL +
4656 Version persistiert.

4657 Code Systeme, die über eine OID eingestellt werden, sind implizit (über die OID)
4658 versioniert und sind deshalb nicht für A_28842* relevant.

4659 **A_23123 -XDS Document Service – APND-Assoziation mit existierenden**
4660 **Dokument oder Dokument aus SubmissionSet**

4661 Der XDS Document Service MUSS bei APND-Assoziationen sowohl Verknüpfungen auf ein
4662 existierendes Dokument im Status "Approved" als auch auf ein Dokument aus dem
4663 übergebenen SubmissionSet ermöglichen. [`<=`]

4664 **A_23124-01 -XDS Document Service – Addendum nur mit einem Dokument**
4665 **verknüpfen**

4666 Der XDS Document Service DARF ein Addendum NICHT mit mehr als einem Dokument
4667 verknüpfen.

4668 Ist die Bedingung nicht erfüllt, MUSS der XDS Document Service das Registrieren und
4669 Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-
4670 Fehlercode `XDSRegistryMetadataError` quittieren. Es MUSS im `codeContext`-Attribut
4671 des zurückgegebenen `rs:RegistryError`-Elements `"errorText='Cannot create`
4672 `association: Only one addendum is allowed'"` angegeben werden. [`<=`]

4673 **A_23125 -XDS Document Service – Kein automatisches "Deprecated" des**
4674 **Addendums**

4675 Der XDS Document Service DARF abweichend von [IHE-ITI-TF3#4.2.2.2.3] einem
4676 Addendum NICHT den `availabilityStatus = Deprecated` zuweisen, wenn das verknüpfte
4677 Dokument den `availabilityStatus Deprecated` erhält. [`<=`]

4678 **A_24521 -XDS Document Service - Erzeugen von Prüfsummen für Dokumente**

4679 Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes
4680 Dokument seine kryptographische Prüfsumme berechnen und `inDocumentEntry.hash`
4681 hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die
4682 Dokumentengröße `inDocumentEntry.size` berechnet und gesetzt werden. [`<=`]

4683 **A_24988-03 -XDS Document Service - Dublettenprüfung für Dokumente**

4684 Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes
4685 Dokument den hash-Wert vergleichen mit allen bereits in dieser Akte existierenden hash-
4686 Werten der Dokumente und bei einer Übereinstimmung das Einstellen mit dem
4687 Fehlercode `XSDuplicateDocument` ablehnen, sofern nicht der Parameter
4688 `"EnableDocumentReuse=true"` (siehe A_27700*) verwendet wird.

4689 Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements der
4690 Text `"errorText='Cannot register document: Duplicate already exists'"` die Liste
4691 der UUIDs (`DocumentEntry.entryUUID`), der in der Akte identifizierten Dokumente, wie
4692 folgt angegeben werden:

4694 `"entryUUID=<entryUUID von document_1>;entryUUID=<entryUUID von`
4695 `document_2>;...;entryUUID=<entryUUID von document_n>"`
4696 `<=`
4697 [`<=`]

4698 Der Fehler `XSDuplicateDocument` ist für das einstellende Client-System einfach
4699 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

- 4748 • mit dem Fehler `XDSRegistryMetadataError` und im `codeContext`-Attribut
4749 des zurückgegebenen `rs:RegistryError`-Elements den Text `"errorText='Cannot`
4750 `register document: Duplicate does not match category of existing`
4751 `document'"` antworten, wenn die Kategorie des neuen Dokuments abweicht,
- 4752 • mit dem Fehler `XDSInvalidRequest` und im `codeContext`-Attribut
4753 des zurückgegebenen `rs:RegistryError`-Elements den Text
4754 `"errorText='Cannot register document: EnableDocumentReuse only allows`
4755 `value true to indicate duplicate'"` antworten, wenn der Parameter
4756 `"EnableDocumentReuse"` mit einem anderen Wert als `"true"` verwendet wird,
- 4757 • ansonsten mit dem üblichen Fehler antworten, der auch sonst beim Einstellen der
4758 Anfrage (d.h. ohne `EnableDocumentReuse`) zurückgegeben würde.

4759 [`<=`]

4760 Hintergrund ist, dass die Information, dass es sich um eine Dublette handelt, für das
4761 einstellende System hilfreicher und spezifischer ist als ein Metadatenfehler, dass bspw.
4762 die angelieferte `uniqueId` "falsch" ist.

4763 **A_24990 -XDS Document Service - Dublettenprüfung für dynamische Ordner**

4764 Der XDS Document Service MUSS beim Anlegen dynamischer Folder prüfen, ob ein
4765 Ordner bereits existiert, der gemäß vom Titel her identisch ist mit demjenigen, den der
4766 Client einzustellen versucht. Im Falle eines identischen Titels MUSS der Einstellversuch
4767 mit dem Fehlercode `XSDuplicateFolder` abgelehnt werden.[`<=`]

4768 **A_30511 -XDS Document Service – Dublettenprüfung gegen Dokumente des MHD Service**

4769 Der XDS Document Service MUSS die Dublettenprüfung gemäß A_24988-* beim
4770 Einstellen von Dokumenten auch gegen die Dokumente der Akte durchführen, die nicht
4771 über den XDS Document Service eingestellt wurden (über den MHD Service eingestellte
4772 oder vom MHD Service erzeugte Dokumente). Für diese Dokumente MUSS der XDS
4773 Document Service den Hash-Wert mit SHA-256 über deren Dokumentinhalt bilden (vgl.
4774 A_24521), um ihn mit dem einzustellenden Dokument zu vergleichen.
4775 Stimmt der Hash-Wert ausschließlich mit Dokumenten überein, die nicht über den XDS
4776 Document Service eingestellt wurden, MUSS der XDS Document Service die Anfrage auch
4777 bei Verwendung des Parameters `EnableDocumentReuse=true` (A_27700-*) mit dem
4778 Fehlercode `XSDuplicateDocument` gemäß A_24988-* ablehnen.

4779 [`<=`]

4781 **A_30512 -XDS Document Service – Eindeutigkeit der `uniqueId` gegenüber Dokumenten des MHD Service**

4782 Der XDS Document Service MUSS beim Einstellen von Dokumenten prüfen, ob die
4783 `DocumentEntry.uniqueId` bereits von einem Dokument der Akte verwendet wird, das
4784 nicht über den XDS Document Service eingestellt wurde
4785 (`DocumentReference.masterIdentifier.value` gemäß [gemIG_ePA_MHD]). Ist das der
4786 Fall und weicht der Hash-Wert ab, MUSS der XDS Document Service das Einstellen mit
4787 dem Fehlercode `XDSNonIdenticalHash` ablehnen.

4788 [`<=`]

4790 Hinweis: Der MHD Service prüft beim Einstellen bereits gegen Dubletten im XDS
4791 Document Service. Erst mit diesen Anforderungen gilt die Dublettenprüfung in beide
4792 Richtungen. Der MHD Service legt für seine Dokumente den Hash mit SHA-1 ab. Für den
4793 Vergleich braucht der XDS Document Service deshalb einen eigenen SHA-256-Wert
4794 dieser Dokumente.

4795

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 25 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 Fehler `XDSRegistryMetadataError` 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>"
```

Einzigste 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'"` angeben, 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 Samlungsdokumententypen

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_versichertereingestellt` 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`) nicht durch eine Nutzergruppe der Rolle `oid_versichertereingestellt` 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

- 4920 • mit dem Ergebnis von GetDocuments übereinstimmen, falls dieses sich im
- 4921 Zustand approved befindet;
- 4922 • andernfalls über Associations ermittelt werden. Dabei wird jeweils ausgehend von
- 4923 der übergebenen DocumentEntry.EntryUUID oder DocumentEntry.UniqueId über
- 4924 die Replace- Associations dasjenige DocumentEntry Objekt ermittelt, das sich im
- 4925 Zustand approved befindet.

4926 Das wsa:Action-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery"

4927 besitzen.

4928 [`<=`]

4929 **A_24762 -XDS Document Service – Suchanfragen über das Metadatenattribut**

4930 **DocumentEntry.title**

4931 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "FindDocumentsByTitle"

4932 mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben

4933 Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-

4934 ITI-TF2#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter

4935 \$XDSDocumentEntryTitle unterstützen, sodass eine Suchergebnismenge über das

4936 Attribut XDSDocumentEntry.title eingeschränkt werden kann. Weiterhin MUSS dieselbe

4937 Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den

4938 Parameter \$XDSDocumentEntryAuthorPerson. Das wsa:Action-Element MUSS den Wert

4939 "urn:ihe:iti:2007:RegistryStoredQuery" besitzen.[`<=`]

4940 **A_25183-02 -XDS Document Service – Suchanfragen über das**

4941 **Metadatenattribut DocumentEntry.comments**

4942 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp

4943 "FindDocumentsByComment" mit der Query-ID "urn:uuid:2609dda5-2b97-44d5-a795-

4944 3e999c24ca99" und denselben Parameternutzungsvorgaben der Registry Stored Query

4945 "FindDocuments" gemäß [IHE-ITI-TF2#3.18.4.1.2.3.7.1] sowie die weiteren

4946 verpflichtenden Suchparameter \$XDSDocumentEntryComments und

4947 \$XDSDocumentEntryComment (deprecated) unterstützen, sodass eine Suchergebnismenge

4948 über das Attribut DocumentEntry.comments eingeschränkt werden kann. Weiterhin MUSS

4949 dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen

4950 über den Parameter \$XDSDocumentEntryAuthorPerson. Es muss mindestens einer der

4951 beiden Suchparameter in diesem Anfragetyp enthalten sein, anderenfalls MUSS der XDS

4952 Document Service mit dem Fehlercode XDSStoredQueryMissingParam antworten. Bei

4953 gleichzeitiger Übermittlung beider Suchparameter DARF NUR der Suchparameter

4954 \$XDSDocumentEntryComments für die Suchanfrage verarbeitet werden. wsa:Action-

4955 Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery" besitzen.[`<=`]

4956 **A_24763 -XDS Document Service – Suche über Author Institution bei Registry**

4957 **Stored Query**

4958 Der XDS Document Service MUSS für den Anfragetyp "FindDocumentsByTitle" den

4959 weiteren optionalen Parameter \$XDSDocumentEntryAuthorInstitution verarbeiten

4960 können, sodass eine Suchergebnismenge über den authorInstitution-Slot der

4961 XDSDocumentEntry.author-Classification (Wertemenge des authorInstitution-Sub-

4962 Attributs) eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels

4963 Platzhalter implementiert sein, wie für Suchanfragen über den Parameter

4964 \$XDSDocumentEntryAuthorPerson.[`<=`]

4965 **A_24764-01 -XDS Document Service – Rückgabe unscharfer Suchergebnisse für**

4966 **Registry Stored Query**

4967 Der XDS Document Service MUSS bei der Ermittlung der Ergebnisse einer Registry

4968 Stored Query bei Auswertung der folgenden Queries und deren Suchparametern beim

4969 Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d. h. bezogen auf das

4970 jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht
4971 abweichende Ergebnisse zurück liefern können:

- 4972 • Query "FindDocuments" und Query "FindDocumentsByTitle" und Query
4973 "FindDocumentsByComment"
- 4974 • \$XDSDocumentEntryTitle
- 4975 • \$XDSDocumentEntryAuthorInstitution
- 4976 • \$XDSDocumentEntryAuthorPerson
- 4977 • \$XDSDocumentEntryComments
- 4978 • \$XDSDocumentEntryComment (deprecated)
- 4979 • Query "FindSubmissionSets"
- 4980 • \$XDSSubmissionSetAuthorPerson

4981 Dabei MUSS der XDS Document Service mindestens unscharfe Ergebnisse bezüglich
4982 Groß-/Kleinschreibung unterstützen, also Groß-/Kleinschreibung für die angegebenen
4983 Parameter der ausgewählten Query-Typen ignorieren.
4984 [**<=**]

4985 Das zur Ermittlung weiterer unscharfer Ergebnisse vom XDS Document Service
4986 einzusetzende Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu
4987 liefern, die ihm möglicherweise sonst wegen beispielsweise falscher Schreibweise eines
4988 Namens (z. B. "Meyer" vs. "Maier") vorenthalten worden wäre. Dabei sind Verfahren wie
4989 die Kölner Phonetik aber auch andere Mechanismen denkbar.

4990 **A_28668 -Unscharfe Suche über Metadatenattribute mit Code System Version**

4991 Der XDS Document Service MUSS bei Belegung des
4992 Suchparameters\$XDSDocumentEntryEventCodeList in einer Registry Stored Query [ITI-
4993 18] die Suche sowohl mit als auch ohne Angabe einer angestellten Code System Version
4994 per Pipe-Symbol (|) durchführen. Ist keine Code System Version angegeben, MUSS der
4995 XDS Document Service DocumentEntry-Einträge finden, welche mit einer beliebigen
4996 Version gespeichert wurden.[**<=**]

4997 **A_28844 -XDS Document Service – Suche nach Code System mit Haupt- 4998 Identifier und Version**

4999 Der XDS Document Service MUSS bei Belegung eines Suchparameters mit einem Code in
5000 einer Registry Stored Query [ITI-18] die Suche wie folgt durchführen:

5001 Bei Code Systemen MUSS der XDS Document Service zur Ermittlung von Treffern in der
5002 Datenbasis auch Ergebnisse finden, bei denen der entsprechende Code mit einem
5003 äquivalenten Identifier für das jeweilige Code System gespeichert ist. Dies betrifft Coding
5004 Systems gemäß [gemIG_TI_Terminology] oder die als "deprecated" gelisteten Code
5005 Systems gemäß A_28834, sofern an der jeweiligen Stelle mehr als ein Identifier für das
5006 angefragte Code System festgelegt ist.

5007 Wenn der XDS Document Service später für diese Suche einen DocumentEntry
5008 zurückgeliefert, MUSS statt des vom Client gelieferten Code-System-Werts stattdessen
5009 der Haupt-Identifier inklusive Versionsangabe zurückgeliefert werden.

5010 [**<=**]

5011 Damit werden bei der Suche die verschiedenen Identifier eines Code Systems als
5012 äquivalent behandelt; das heißt, der Client darf einen beliebigen Namen für ein Code
5013 System verwenden und der XDS Document Service muss auch dann einen Treffer
5014 generieren, wenn der entsprechende Code mit einem anderen Identifier für dasselbe
5015 Code System in der Datenbasis gespeichert wird.

- 5016 Unabhängig von der Anfrage gibt der XDS Document Service also dem Client das Code
5017 System immer mit Haupt-Identifizier zurück.
- 5018 3.12.1.4.3.3 Remove Metadata [ITI-62]
5019 **A_14908-02 -XDS Document Service – Ablauflogik für Remove Metadata**
5020 Der XDS Document Service MUSS die Umsetzung der Operation RemoveMetadata gemäß
5021 der definierten Ablauflogik in [IHE-ITI-RMD#3.62.4.1.2 und 3.62.4.1.3]
5022 implementieren. [≤]
- 5023 **A_20701 -XDS Document Service – Unwiderrufliches Löschen bei Remove**
5024 **Metadata**
5025 Der XDS Document Service MUSS sicherstellen, dass einmal gelöschte Dokumente und
5026 Metadatenobjekte nicht wiederhergestellt werden können. [≤]
- 5027 **A_21715 -XDS Document Service – Kein Löschen von "replaced"-Dokumenten**
5028 **im Status "Deprecated"**
5029 Der XDS Document Service MUSS sicherstellen, dass keine Löschanfrage eines ePA-Client
5030 auf Dokumenten mit dem availabilityStatus = Deprecated ausgeführt werden darf. [≤]
- 5031 **A_21714-04 -XDS Document Service – Löschen von strukturierten Dokumenten**
5032 **durch ein ePA-FdV**
5033 Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein
5034 ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete
5035 Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert
5036 aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie
5037 zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die
5038 Nachricht mit demXDSRegistryError-Fehlercode zurückgegeben werden.Es MUSS im
5039 codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert
5040 "errorText='Cannot delete folder: Use only entryUUID of folder'" belegt
5041 werden. [≤]
- 5042 **A_21817-04 -XDS Document Service – Löschen von strukturierten Dokumenten**
5043 **durch ein Primärsystem**
5044 Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein
5045 Primärsystem ablehnen, wenn zugehörige Submission Sets, Associations oder
5046 zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners
5047 impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets,
5048 Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben
5049 vor, MUSS die Nachricht mitXDSRegistryError-Fehlercode zurückgegeben werden. Es
5050 MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert
5051 "errorText='Cannot delete folder: Use only entryUUID of folder'" belegt
5052 werden. [≤]
- 5053 Beispiel:
5054 errorCode = XDSRegistryError
5055 codeContext = "entryUUID='2.25.514739840497321348259';errorText='Cannot
5056 delete folder: Use only entryUUID of folder'"
- 5057 **A_24663-01 -XDS Document Service – Bereinigung der General Deny Policy**
5058 Der XDS Document Service MUSS als Folge von erfolgreichen Löschanfragen alle Einträge
5059 der General Deny Policy entfernen, welche die betroffenen Dokumente oder dynamischen
5060 Ordner referenzieren. [≤]
- 5061 **A_24765 -XDS Document Service – Kein Löschen von statischen Ordnern und**
5062 **Associations**
5063 Der XDS Document Service MUSS sicherstellen, dass eine Löschanfrage keine statischen
5064 Ordner und Assoziationen löschen darf. Dies gilt nicht für dynamische Ordner. Der XDS

5065 Document Service MUSS bei Löschung eines Dokumentes die Assoziation zum Folder
5066 löschen. [≤]

5067 Dynamische Ordner sind beispielsweise Mutterpass (folderCode = pregnancy_childbirth)
5068 oder DiGA (folderCode = diga).

5069 **A_20579-03 -XDS Document Service – Löschen von Ordnern**

5070 Der XDS Document Service MUSS Requests, die darauf abzielen, einen statischen Folder
5071 direkt zu löschen, ablehnen und mit dem Fehler `XDSRegistryMetadataError` und im
5072 `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements den Text
5073 "errorText='Cannot delete folder: Invalid category'" antworten. [≤]

5074 3.12.1.4.3.4 RetrieveDocumentSet [ITI-43]

5075 **A_14914 -XDS Document Service – Ablauflogik für Retrieve Document Set**

5076 Der XDS Document Service MUSS die Umsetzung der Operation RetrieveDocumentSet
5077 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2#3.43.4.1.2 und 3.43.4.1.3] und
5078 [IHE-ITI-TF2#3.43.4.2.2 und 3.43.4.2.3] implementieren. [≤]

5079 **A_16201 -XDS Document Service – Prüfung der zurückgegebenen Paketgröße**

5080 Der XDS Document Service MUSS anhand der übergebenen DocumentUniqueIDs die
5081 Gesamtgröße ermitteln und bei Überschreitung von 250 MByte die Verarbeitung ablehnen
5082 und die Nachricht mit einem `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-
5083 TF3#4.2.4] quittieren. [≤]

5084 3.12.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen

5085 **A_24508-01 -XDS Document Service – Prüfung der Policies bei Suchanfrage**

5086 Der XDS Document Service MUSS bei einer Suchanfrage für einen angemeldeten Nutzer
5087 die Suchergebnismenge entsprechend der Legal Policy und der General Deny Policy
5088 filtern, d. h. die Suchergebnismenge enthält ausschließlich XDS-Metadaten, die für einen
5089 angemeldeten Nutzer nicht diesen Policies widersprechen. [≤]

5090 **A_24509-01 -XDS Document Service - Prüfung der Legal Policy außer**
5091 **Suchanfragen**

5092 Der XDS Document Service MUSS die Ausführung einer Operation mit dem Fehlercode
5093 `LegalPolicyViolation` beenden, wenn für den angemeldeten Nutzer die Regeln der Legal
5094 Policy nicht erfüllt sind und es sich nicht um eine Suchanfrage handelt.
5095 Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements der
5096 Fehlertext "errorText='Legal Policy violation'" angegeben werden. [≤]

5097 **A_24510-02 -XDS Document Service – Prüfung Herunterladen eines**
5098 **verborgenen oder nicht vorhandenen Dokuments**

5099 Der XDS Document Service MUSS die Ausführung der Retrieve-Operation mit dem
5100 Fehlercode `XDSDocumentUniqueIdError` beenden, wenn das assoziierte Dokument nicht
5101 vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny Policy
5102 nicht erfüllt sind. [≤]

5103 **A_24511-01 -XDS Document Service – Prüfung Löschen eines verborgenen**
5104 **Dokuments oder dynamischen Ordners**

5105 Der XDS Document Service MUSS die Ausführung der Remove-Operation mit dem
5106 Fehlercode `XDSDocumentUniqueIdError` beenden, wenn für den angemeldeten Nutzer die
5107 Regeln der General Deny Policy nicht erfüllt sind.
5108 [≤]

5109 **A_24512-02 -XDS Document Service – Prüfung Schreiben eines Dokuments in**
5110 **einen nicht vorhandenen oder verborgenen dynamischen Ordner**

5111 Der XDS Document Service MUSS die Ausführung der Provide-Operation mit dem
5112 Fehlercode `UnresolvedReferenceException` beenden, wenn der Ordner nicht existiert oder

5113 für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.
5114 [`<=`]

5115 **A_28858 -XDS Document Service – Prüfung Schreiben eines Dokuments in**
5116 **einen verborgenen statischen Ordner**

5117 Der XDS Document Service MUSS die Ausführung der Provide-Operation mit dem
5118 Fehlercode `XDSFolderAccessDenied` beenden, wenn der Ordner für den angemeldeten
5119 Nutzer die Regeln der General Deny Policy nicht erfüllt sind.
5120 [`<=`]

5121 **3.12.1.5 Fehlerbehandlung in Schnittstellenoperationen**

5122 **A_22516-02 -XDS Document Service - Alternative Verwendung von**
5123 **XDSRegistryMetadataError anstelle von XDSRepositoryMetadataError**

5124 Der XDS Document Service KANN alternativ zum Fehler "XDSRepositoryMetadataError"
5125 den Fehler "XDSRegistryMetadataError" verwenden. [`<=`]

5126 **A_23148-01 -XDS Document Service – Festlegung zu http-Statuscode bei IHE-**
5127 **Responses**

5128 Der XDS Document Service MUSS für den Fall, dass eine IHE-Response in der HTTP-
5129 Response enthalten ist, den http-Statuscode 200 zurückgeben. Das gilt auch, wenn die
5130 IHE-Response einen IHE-Fehler überträgt. [`<=`]

5131 **A_26324-04 -XDS Document Service - Aktenkonto im Umzug oder im**
5132 **Wartungsmodus**

5133 Falls sich ein Aktenkonto im Zustand `SUSPENDED` oder im Status `INACCESSIBLE` befindet
5134 MUSS der XDS Document Service die Verarbeitung ablehnen und mit
5135 einem `StatusMismatch`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren und im
5136 `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements den passenden
5137 Fehlertext mit "errorText=<Fehlertext>" angeben:

5138 **Tabelle 25 : Fehlertexte zu StatusMismatch-Fehlercode**

Aktenkontostatus	Wert für <Fehlertext> in codeContext
<code>SUSPENDED</code>	'Health Record Relocation in progress'
<code>INACCESSIBLE</code>	'Health Record is inaccessible'

5139 `<=`[`<=`]

5140 **A_26325-01 -XDS Document Service - Aktenkonto unbekannt oder im Zustand**
5141 **INITIALIZED**

5142 Falls sich ein Aktenkonto im Zustand `UNKNOWN` oder `INITIALIZED` befindet MUSS der
5143 XDS Document Service die Verarbeitung ablehnen und mit einem `NoHealthRecord`-
5144 Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. `<=`[`<=`]

5145 **A_25683-01 -XDS Document Service - Prüfung auf Befugnis**

5146 Falls keine gültige Befugnis für den aufrufenden Nutzer vorliegt MUSS der XDS Document
5147 Service die Verarbeitung ablehnen und mit einem `NotEntitled`-Fehlercode gemäß [IHE-
5148 ITI-TF3#4.2.4] quittieren. [`<=`]

5149 **A_26459 -XDS Document Service - keine Authentisierung des Nutzers**

5150 Falls keine erfolgreiche Authentifizierung des Nutzers vorliegt MUSS der XDS Document
5151 Service die Verarbeitung ablehnen und mit einem `InvalidAuth`-Fehlercode gemäß [IHE-ITI-
5152 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 abubrechen. 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 ersten Fehler abubrechen. 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>'".[<=]

5202 Beispiel:
5203 `codeContext = "uniqueId='2.25.269167723254896828623'"`

5204 Hinweis:
5205 Der Fehler, dass die Telematik-ID nicht zur Session passt (A_24497*), erfolgt ohne
5206 Angabe der uniqueId.

5207 **A_28655 -XDS Document Service – Formatvorgaben für CodeContext**

5208 Der XDS Document Service MUSS Key-Value Paare in codeContext nach folgenden
5209 Regeln behandeln:

- 5210 • Key-Value Paare sind mit `<key>=<value>` gekennzeichnet,
- 5211 • Die Reihenfolge der Key-Value Paare ist nicht vorgegeben,
- 5212 • Trennung von Key-Value Paaren erfolgt mit `;`,
- 5213 • `<key>` wird normativ vorgegeben und kann gegebenenfalls mehrfach auftreten,
- 5214 • ein identisches Key-Value Paar kann in einem codeContext nur einmal auftreten,
5215 Für `<value>` gilt:
 - 5216 • value wird immer durch Hochkommata ("") umschlossen, z.B.:
5217 `errorText='RootDocumentUniqueId must not be changed'`
 - 5218 • Escape von einfachen Anführungszeichen (') erfolgt mit `"\"`,
 - 5219 • Escape von Backslash (\\) erfolgt mit `"\"`,
 - 5220 • Maximale Anzahl von Zeichen: 1000 (Single Quotes als Beginn und
5221 Endezeichen zählen mit),
 - 5222 • White spaces sind außerhalb von `<value>` nicht erlaubt.

5223 [`<=`]

5224 **A_28656 -XDS Document Service – Format für Fehlerdetail**

5225 Der XDS Document Service KANN bei einem IHE-Fehler weitere Informationen zur
5226 Fehleranalyse imcodeContext des Fehlers als `<key>=<value>`-Paar
5227 einfügen, ausschließlich mit:

- 5228 • `errorDetail='<Details zum Fehler>'`
- 5229 • `<Details zum Fehler>='<weiterführende Informationen zum Fehler>'`
5230 In der Produktivumgebung gilt: Es dürfen keine personenbezogenen Daten,
5231 medizinische Daten, Error Stack Traces oder die Offenbarung von
5232 Programmierdetails enthalten sein.

5233 [`<=`]

5234 Beispiel:

5235 `ErrorCode =InvalidDocumentContent`
5236 `codeContext =`
5237 `"uniqueId='2.25.269167723254896828623';errorDetail='Fehlerhafter`
5238 `Aufrufparameter [PDF service encountered an unacceptable document format`
5239 `for validatePDF'"`

5240 **3.12.1.6 Schnittstellen im XDS Document Service**

5241 In diesem Abschnitt wird die Außenschnittstelle des XDS Document Service festgelegt.
5242 Einzelne Umsetzungsanforderungen suggerieren eine vermischte Verarbeitung von
5243 Funktionalitäten, welche bei IHE ITI originär getrennt von einer Document Registry und
5244 einem Document Repository (bzw. den Responding Gateways) durchgeführt werden. Da

5245 die Außenschnittstelle des XDS Document Service nicht zwischen Document Registry und
 5246 Document Repository unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit
 5247 differenzierten Pfaden, siehe A_26814-*, werden sonst bei IHE ITI explizite Operationen
 5248 zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne Umsetzung
 5249 angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-Nachricht
 5250 kann an IHE ITI-konforme Akteure ausgerichtet werden.

5251 3.12.1.6.1 Schnittstelle I_Document_Management

5252 Weitere Vorgaben zu den Operationen befinden sich in 3.12.1.4.3- Vorgaben zu IHE ITI-
 5253 Transaktionen bei mehreren Schnittstellen .

5254 **A_14152-03 -XDS Document Service – Implementierung der Schnittstelle** 5255 **I_Document_Management**

5256 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-
 5257 Service-Schnittstelle für den Zugriff von ePA-Clients, die über das zentrale Netz zugreifen
 5258 implementieren.

5259 **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]	

Schnittstelle	I_Document_Management
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

5260 **[<=]**

5261 Durch die Legal Policy ist geregelt, welche Clients (professionOID) letztendlich zugreifen
5262 dürfen.

5263 3.12.1.6.1.1 Operation I_Document_Management::ProvideAndRegisterDocumentSet-b
5264 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
5265 Transaktion "ProvideAndRegisterDocumentSet-b" [ITI-41] sind [IHE-ITI-TF2] sowie
5266 Appendix V aus [IHE-ITI-TF2] zu entnehmen.

5267 Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner
5268 gesammelt. Das Anlegen eines DiGA-Ordners erfolgt durch den XDS Document Service
5269 unter der Voraussetzung, dass es eine gültige Befugnis für die DiGA gibt. Der DiGA-
5270 Ordner wird vom XDS Document Service mit der Telematik-ID der DiGA verknüpft.
5271 Die Zuordnung von DiGA-Dokumenten beim Schreiben erfolgt implizit über die
5272 TelematikID aus dem IDToken des Nutzers. Da ein DiGA-Ordner im Titel immer den
5273 Namen der DiGA enthält kann ein Client (z.B. LEI) darüber die relevante DiGA auswählen
5274 und auf die Dokumente der DiGA, sofern eine Befugnis für den Nutzer vorliegt, lesend
5275 zugreifen.

5276 Ein Update eines bestehenden Dokuments mit der bekannten DocumentEntry.entryUUID
5277 kann durch einen DiGA-Client erfolgen. Hierzu ist es erforderlich, dass ein DiGA-Client
5278 die DocumentEntry.entryUUID persistiert und keine symbolischen IDs gemäß [IHE-ITI-
5279 TF2#3.42.4.1.3.7] verwendet.

5280 **A_21512-04 -XDS Document Service – dynamisches Anlegen von DiGA-Ordern**

5281 Falls eine gültige Befugnis für eine konkrete DiGA vorliegt, MUSS der XDS Document
5282 Service beim erstmaligen Einstellen eines Dokumentes für diese DiGA in die Akte des
5283 Versicherten (Operation I_Document_Management::ProvideAndRegisterDocumentSet-
5284 b()) sicherstellen, dass genau ein Ordner für den Versicherten mit den folgenden
5285 Eigenschaften angelegt ist:

- 5286 • DiGA-Ordner der Kategorie diga gemäß A_19388 (Belegung Folder.codeList) unter
5287 Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A_14760
5288 (Belegung der restlichen Metadatenfelder).
- 5289 • Folder.title wird entsprechend des Attributs "organizationName" aus dem IDToken
5290 der zugreifenden DiGA belegt.
- 5291 • Folder.comment wird belegt mit "urn:gematik:diga:<Telematik-ID>", wobei die
5292 Telematik-ID dem Attribut "idNummer" des ID-Token entspricht.
- 5293 • Folder.EntryUUID wird mit einer aus der TelematikID abgeleiteten UUID belegt.

5294 Die folder.EntryUUID MUSS wie folgend dargestellt aus der TelematikID der DiGA erzeugt
5295 werden:

- 5296 • Algorithmus: Name-Based UUID gemäß [RFC4122#4.3], Version 3 (MD5)
- 5297 • Namensraum-UUID: "e2310a38-0b62-415e-8b44-994dc8312965"
- 5298 • Name: "<TelematikId>"

5299 Eine konkrete DiGA wird identifiziert durch die TelematikID und ist als DiGA durch die
5300 professionOID gekennzeichnet.

5301 [`<=`]

5302 **A_22994-01 -XDS Document Service - automatische Folder-Zuordnung für DiGA**

5303 Der XDS Document Service MUSS beim Einstellen eines DiGA-Dokumentes in die Akte
5304 des Versicherten (Operation

5305 `I_Document_Management::ProvideAndRegisterDocumentSet-b()` sicherstellen, dass das
5306 DiGA-Dokument in den durch die TelematikID referenzierten DiGA-Ordner abgelegt wird.
5307 Die TelematikID des zu adressierenden Ordners entspricht dem Attribut "idNummer" des
5308 ID-Token . [`<=`]

5309 **A_21713-03 -XDS Document Service – Kein Einstellen von Ordnern**

5310 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und
5311 Dokument(en) über die

5312 Schnittstelle `I_Document_Management::ProvideAndRegisterDocumentSet-b` ablehnen

5313 und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der

5314 Eingangsnachricht ein oder mehrere neu anzulegende Folder enthalten sind. Ausnahme:

5315 Folder der Kategorie `pregnancy_childbirth` in `Folder.codeList`. [`<=`]

5316 **A_24497-01 -XDS Document Service - Verwendung der korrekten Telematik-ID 5317 beim Einstellen**

5318 Der XDS Document Service MUSS die Telematik-ID aus dem ID-Token der aktuellen User

5319 Session abgleichen mit der Telematik-ID aus `SubmissionSet.authorInstitution` und

5320 das Abweichen der Telematik-Ids mit einem `XDSRepositoryMetadataError`-Fehlercode

5321 quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError-`

5322 Elements den Text `"errorText='Telematik-ID does not match'"` angeben. [`<=`]

5323 **A_24456-01 -XDS Document Service - Durchsetzung von Uniqueness beim 5324 Einstellen von Notfalldaten**

5325 Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien

5326 "emergency" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein

5327 einzelnes NFD- und ein einzelnes DPE-Dokument im Status "approved" gibt. Der Versuch,

5328 innerhalb dieses Ordners ein zweites NFD- oder DPE-Dokument einzustellen, MUSS mit

5329 dem `IHE-ErrorInvalidDocumentContent` abgebrochen werden. Es MUSS im

5330 `codeContext`-Attribut des zurückgegebenen `InvalidDocumentContent`-Elements der Text

5331 `"errorText='Cannot register document: Medical information object has to be`

5332 `unique'"` zurückgegeben werden. [`<=`]

5333 **3.12.1.6.1.2 Operation `I_Document_Management::RegistryStoredQuery`**

5334 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-

5335 Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2] sowie Appendix V

5336 aus [IHE-ITI-TF2] zu entnehmen.

5337 **3.12.1.6.1.3 Operation `I_Document_Management::RemoveMetadata`**

5338 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-

5339 Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-

5340 ITI-TF2] zu entnehmen.

5341 3.12.1.6.1.4 Operation I_Document_Management::RetrieveDocumentSet
 5342 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 5343 Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2], sowie Appendix V
 5344 aus [IHE-ITI-TF2] zu entnehmen.

5345

5346 3.12.1.6.2 Schnittstelle I_Document_Management_Insurant

5347 Weitere Vorgaben zu den Operationen befinden sich in 3.12.1.4.3- Vorgaben zu IHE ITI-
 5348 Transaktionen bei mehreren Schnittstellen .

5349 **A_14478-03 -XDS Document Service – Implementierung der Schnittstelle**

5350 **I_Document_Management_Insurant**

5351 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-
 5352 Service-Schnittstelle für den Zugriff des ePA-FdV implementieren .

5353 **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	[XSDDocumentService]	

Schnittstelle	I_Document_Management_Insurant
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

5354

5355 [$\leq$]5356 **A_26460 -XDS Document Service - Zugriff über**5357 **I_Document_Management_Insurant mit nicht registriertem Gerät**

5358 Falls Operationen von I_Document_Management_Insurant ohne registriertes Gerät
 5359 aufgerufen werden MUSS der XDS Document Service die Verarbeitung ablehnen und mit
 5360 einemUnregisteredDevice-Fehlercode quittieren.[$\leq$]

5361 3.12.1.6.2.1 Operation

5362 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b

5363 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 5364 Transaktion "Provide And Register Document Set-b" [ITI-41] sind [IHE-ITI-TF2] sowie
 5365 Appendix V aus [IHE-ITI-TF2] zu entnehmen.

5366 **A_21481-04 -XDS Document Service – Kein Einstellen von Ordern und**
 5367 **Associations**

5368 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und
 5369 Dokument(en) über die Schnittstelle

5370 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b() ablehnen und
 5371 mit einem XDSRegistryMetadataError-Fehlercode quittieren, wenn in der
 5372 Eingangsnachricht ein oder mehrere neu anzulegende Folder oder andere als die
 5373 folgenden Assoziationen

5374

- SS-DE

5375

- SS-HM

5376

- FD-DE

5377

- RPLC

5378

- APND

5379 enthalten sind.[$\leq$]

5380 Das Referenzieren bestehender Ordner ist davon nicht berührt, wie dies z. B. beim

5381 Einstellen von Dokumenten in Sammlungen der Fall ist (z. B. Einstellen eines Dokuments
 5382 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 MUSS nach der erfolgreichen Anlage der Akte des Versicherten die Kategorienordner unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A_14760* (Belegung der restlichen Metadatenfelder) für den Versicherten gemäß der folgenden Tabelle anlegen. Alle statischen Kategorienordner werden mit jeweils einem Ordner pro Kategorie angelegt. Alle statischen Ordner sind nach dem Anlegen initial leer.

Das Anlegen von Submission Sets und zugehöriger Associations zu den statischen Ordnern ist nicht vorgegeben. Das XDS-Informationsmodell MUSS allerdings hinsichtlich der Folder-DocumentEntry- sowie SubmissionSet-HasMember-Associations bei einer Verarbeitung durch die Document Consumer (z. B. Querying) erfüllt werden.

Tabelle 28: Festlegung Folder.entryUUID zu statischen Ordnern

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
reports	b878db05-49e4-4f74-a329-b3bcdd8082c4
emp	7c1054ea-a4df-4a1b-8e10-209f6d8812ee
emergency	a7bb6be7-d756-46dd-90d4-4020ed55b777
eab	2ed345b1-35a3-49e1-a4af-d71ca4f23e57

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
dental	af547321-b8e8-4e1d-b9af-51bb4a990bda
child	2c898452-4667-40e3-9d3e-c09d7385b527
vaccination	9c3edaf3-a978-46fe-8e6e-021ff4aca60b
patient	d236c9a2-ab01-4902-a00a-1e1dff439fe7
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d
health_risk_analysis	840a59c7-61d4-4caa-80a7-1857af2f166f
care	2d62bf9e-062a-4aa7-9951-9f33bbc665b5
eau	aa7d10d6-204a-47aa-be73-44bdc77512f
other	605a9f3c-bfe8-4830-a3e3-25a4ec6612cb
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31
rehab	173f4204-fb93-4a1a-a1f6-316703b79539
transcripts	6A8E383D-8705-4B0E-A140-39A5F144501D

5415

5416 [**<=**]

5417 *Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner vom Typ*
 5418 *"pregnancy_childbirth" und verwenden als Folder.title ein Kennzeichen der*
 5419 *Schwangerschaft.*

5420 **A_20216-04 -XDS Document Service – Unveränderlichkeit von statischen** 5421 **Akteninhalten**

5422 Der XDS Document Service DARF die Metadaten eines statischen Aktenobjekts gemäß
 5423 A_24491 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen.
 5424 Dabei gelten folgende Ausnahmen:

- Folder.lastUpdateTime - Folder.lastUpdateTime wird automatisch vom XDS Document Service aktualisiert, sobald Dokumente in den Ordner eingestellt (siehe auch [IHE-ITI-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

- 5471 • I_Document_Management::ProvideAndRegisterDocumentSet-b sowie
- 5472 • I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b

5473 registriert werden.

5474

5475 Für den Produkttyp DiGA gelten die gleichen Vorgaben wie für die Primärsysteme sofern

5476 unter Nutzungsvorgaben keine abweichenden Bedingungen definiert werden.

5477 **Tabelle 29: Nutzungsvorgaben für Metadatenattribute XDS**

Metadaten- attribut XDS.b		Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
		P S	K T R	D S	F d V			
Metadaten für DocumentEntry								
author		1. .n	1. .1	0. .0	0. .n	Person oder System, welche(s) das Dokument erstellt hat	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.1] genügen. Das Primärsystem MUSS mindestens das Subattribut authorPerson oder authorInstitution inhaltlich belegen.	
authorPerson		0. .1	0. .1	0. .0	0. .1	Name des Autors	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 3.12.1.8.2- <u>Metadaten der Dokumente und SubmissionSets</u> genügen.	X
authorInstitution		0. .n	0. .n	0. .0	0. .n	Institution, die dem Autor zugeordnet ist	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 3.12.1.8.2- <u>Metadaten der Dokumente und SubmissionSets (A_21209)</u> genügen.	X
authorRole		0. .n	0. .n	0. .0	0. .n	Rolle des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS 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 EPAXDSAauthorSpecialtyVS aus [gemIG_TI_Terminology] entsprechen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorTeleco mmunication	0. .n	0. .0	0. .0	0. .n	Telekommunikati onsdaten des Autors	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.1.4.5] genügen.	X
availabilityStatu s	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: <u>Strukturierte Dokumente</u> genügen. 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.	X
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.4] genügen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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 ProvideAndRegisterDocuments et-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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
eventCodeList	0. .n	0. .0	0. .0	0. .n	Ereignisse, die zur Erstellung des Dokuments geführt haben.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.8] genügen und Codes des Value Set EPAXDSEventCodeVS aus [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.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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 Abschnitt 3.12.1.9-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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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 EPAXDSLLanguageCodeVS 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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierungsattribut, dass das Metadatenelement DocumentEntry nicht den vollständigen Satz an Metadaten enthält.		
contentType	1. .1	1. .1	0. .0	1. .1	MIME-Type des Dokuments	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 Abschnitt 3.12.1.9-Strukturierte Dokumente genügen. <u>Anmerkung:</u> In Klammern sind die Extensions angegeben, die beim entsprechenden MIME-Type in DocumentEntry.URI für das URI-scheme "file," zu verwenden sind.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
objectType	1. .1	1. .1	0. .0	1. .1	Typ des Dokuments	Der Wert MUSS immer "urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1" betragen. Dieser Wert steht für stabile Dokumente im IHE ITI XDS.b-Profil [IHE-ITI-TF3#4.2.5.2].	
patientId	1. .1	1. .1	0. .0	1. .1	Systemweit eindeutige Kennung des Patienten	Der Wert MUSS den Inhalts- und Formatvorgaben aus A_14974* genügen. Außerdem MUSS der Wert der Identität des Akteninhabers entsprechen und MUSS vom XDS Document Service dahingehend bei Registrierung der Metadaten geprüft werden.	
practiceSettingCode	1. .1	0. .0	0. .0	1. .1	Art der Fachrichtung der erstellenden Einrichtung, in der das dokumentierte Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSPracticeSettingCodeVS aus [gemIG_TI_Terminology] entsprechen. Die DiGA MUSS practiceSettingCode mit dem Wert "PAT" belegen.	X
referenceIdList	0. .n	0. .1	1. .1	0. .n	Liste von IDs, mit denen das Dokument assoziiert wird.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.28] genügen. Wenn KTR-Clients einen Wert übertragen, muss es sich um die rootDocumentId 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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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. .1	0. .0	0. .0	0. .0	Kennung des Patienten im Quellsystem	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.22] genügen.	
sourcePatientInfo	0. .n	0. .0	0. .0	0. .0	Demographische Daten zum Patienten im Quellsystem	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.23] genügen.	
title	1. .1	1. .1	1. .1	1. .1	Titel des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.24] genügen. Ein leeres Feld <code>DocumentEntry.title=""</code> bzw. ausschließlich mit nicht druckbaren Zeichen befüllt ist nicht erlaubt.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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 Abschnitt 3.12.1.9- 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- attribut XDS.b		Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
		P S	K T R	D S	F d V			
Metadaten für 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 <u>3.12.1.8.2- Metadaten der Dokumente und SubmissionSets</u> genügen. ePA-FdV: Das ePA-Aktensystem MUSS die KVNR mit den Inhalten der User Session auf Übereinstimmung prüfen. Eine Gleichheit liegt vor, wenn die KVNR aus der XCN-Struktur des Autors nach den Vorgaben von A_14762-* mit dem entsprechenden Wert aus der User Session übereinstimmt. Ist authorPerson nicht gesetzt, MUSS das ePA Aktensystem das Metadatenattribut authorPerson für Versicherte entsprechend der Vorgaben aus A_14762-* unter Verwendung der entsprechenden Informationen aus der User Session (KVNR, family_name und given_name) setzen. Das ePA Aktensystem KANN in einer übergebenen authorPerson den Nachnamen und Vornamen mit Informationen aus der User Session überschreiben. PS/DiGAs können hier im Bedarfsfall Einträge für Software-Komponente bzw. Gerät als Autor entsprechend A_14762-* vornehmen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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 <u>3.12.1.8.2- Metadaten der Dokumente und SubmissionSets (A_21209*)</u> 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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorRole	1. .n	1. .n	0. .0	1. .1	Rolle der einstellenden Per son oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS 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.	
authorSpecial ty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung der einstellenden Per son oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorSpecialtyVS aus [gemIG_TI_Terminology] entsprechen.	
authorTeleco mmunication	0. .n	0. .0	0. .0	0. .n	Telekommunikati onsdaten der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.1.4.5] genügen.	
availabilityStatu s	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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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 zusammengestell t 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							
availabilityStatu s	1. .1	n/ a	0. .0	n/ a	Status des Ordnern ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approved" entsprechen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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.						

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
patientId	1. .1	n/ a	0. .0	n/ a	Patienten ID, zu der der Ordner gehört.	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
title	1. .1	n/ a	0. .0	n/ a	Titel des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.8] genügen.	
uniqueId	1. .1	n/ a	0. .0	n/ a	Eindeutige, aktenweite Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.9] genügen.	
Metadaten für statische Folder							
availabilityStatus	n/ a	n/ a	1. .1	n/ a	Status des Ordners ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approved" entsprechen.	
codeList	n/ a	n/ a	1. .1	n/ a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI- TF3#4.2.3.4.2] 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	Freitextkomment ar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE- ITI-TF3#4.2.3.4.3] entsprechen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
uniqueId	n/ a	n/ a	1. .1	n/ a	Eindeutige, aktenweite Kennung des Ordnerns	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.9] genügen.	

5478
5479

Tabelle 30: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language Codes

Language / Country Code Kombination	Language / Country Code Kombination
bg-BG(bulgarisch, Bulgarien)	it-IT(italienisch, Italien) it-CH (italienisch, Schweiz)
cs-CZ(tschechisch, Tschechien)	lt-LT(litauisch, Litauen)
da-DK(dänisch, Dänemark)	lb-LU(luxemburgisch, Luxemburg)
de-AT(deutsch, Österreich) de-DE (deutsch, Deutschland) de-CH (deutsch, Schweiz) de-LI (deutsch, Liechtenstein) de-LU (deutsch, Luxemburg)	lv-LV(lettisch, Lettland)
el-GR(griechisch, Griechenland)	mt-MT(maltesisch, Malta)
en-GB(englisch, Vereinigtes Königreich)	nl-NL(niederländisch, Niederlande) nl-BE (niederländisch, Belgien)
es-ES(spanisch, Spanien)	no-NO(norwegisch, Norwegen)
et-EE(estnisch, Estland)	pl-PL(polnisch, Polen)
fi-FI(finisch, Finnland)	pt-PT(portugiesisch, Portugal)
fr-FR(französisch, Frankreich) fr-CH (französisch, Schweiz) fr-LU (französisch, Luxemburg) fr-BE (französisch, Belgien)	rm-CH(rätoromanisch, Schweiz)
ga-IE(irisches, Irland)	ro-RO(rumänisch, Rumänien)
hr-HR(kroatisch, Kroatien)	sk-SK(slowakisch, Slowakei)

Language / Country Code Kombination	Language / Country Code Kombination
hu-HU(ungarisch, Ungarn)	sl-SI(slowenisch, Slowenien)
is-IS(isländisch, Island)	sv-SE(schwedisch, Schweden)

5480 [**<=**]

5481 3.12.1.8.2 Metadaten der Dokumente und SubmissionSets

5482 **A_23369-04 -XDS Document Service – Verpflichtender Dokumententitel in**
 5483 **DocumentEntry.title**

5484 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
 5485 Dokumenten `DocumentEntry.title` befüllen. Der Titel des Dokumentes soll eine
 5486 fachliche Beschreibung des Dokumentes enthalten. Bei `DocumentEntry.title` MÜSSEN
 5487 führende und endende Leerzeichen entfernt werden. In `DocumentEntry.title` DARF NICHT
 5488 leer sein (`!= ""`) (insbesondere auch nicht nach etwaigen Entfernen von Leerzeichen
 5489 vorne und hinten). In `Document.title` DÜRFEN keine nicht-druckbaren Zeichen enthalten
 5490 sein.

5491 Andernfalls MUSS der XDS Document Service die Operation mit dem
 5492 Fehler `XDSRegistryMetadataError` ablehnen und im `codeContext`-Attribut
 5493 des zurückgegebenen `rs:RegistryError-Elements` mit: `"errorText='Invalid
 5494 metadata';metadata='title'"` antworten.

5495 [**<=**]

5496 **A_25188-02 -XDS Document Service - Input Sanitization**

5497 Der XDS Document Service MUSS sicherstellen, dass bei Anlage von Metadaten:

- 5498 1. führende (leading) und endende (trailing) Whitespace von den Attributen
 5499 automatisch entfernt werden.
- 5500 2. die notwendigen Attribute nichtleer sind (insbeondere auch noch Whitespace-
 5501 Entfernung aus 1.). und
- 5502 3. Die Attribute nur druckbare Zeichen enthalten.
- 5503 a. Ausnahme: Der XDS Document Service MUSS im Metadatum
 5504 `DocumentEntry.comment` die ASCII-Zeichen CR (`\r`, `0x0D`) und LF (`\n`, `0x0A`)
 5505 ignorieren und nicht als Fehler behandeln (sie werden für Zeilenumbrüche
 5506 benötigt).

5507 [**<=**]

5508 **A_14762-08 -XDS Document Service – Nutzungsvorgabe für authorPerson als**
 5509 **Teil von DocumentEntry.author und SubmissionSet.author**

5510 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
 5511 Dokumenten an `authorPerson` unterhalb von `DocumentEntry.author` und
 5512 `SubmissionSet.author` neben [IHE-ITI-TF3#4.2.3.1.4.2] auch die folgenden
 5513 Vorgaben beachten.

5514 **Bei Leistungserbringer als Autor:**
 5515

- 5516 1. Lebenslange Identifikationsnummer eines Arztes (Lebenslange Arztnummer -
 5517 LANR 9 Stellen) oder im Falle eines Zahnarztes die Zentrale Zahnarzt Nummer
 5518 (ZANR)- sofern die ZANR bekannt ist

- 5519 2. "^"
- 5520 3. Nachname
- 5521 4. "^"
- 5522 5. Vorname
- 5523 6. "^"
- 5524 7. Weiterer Vorname
- 5525 8. "^"
- 5526 9. Namenszusatz
- 5527 10. "^"
- 5528 11. Titel
- 5529 12. "^^^&" - sofern LANR oder ZANR angegeben, ansonsten "^^^"
- 5530 13. "1.2.276.0.76.4.16" - sofern LANR angegeben oder "1.2.276.0.76.4.296", falls
- 5531 ZANR angegeben
- 5532 14. "&ISO" - sofern LANR oder ZANR angegeben

5533 Beispiele:
 5534 165746304^Weber^Thilo^^^Dr.^^^&1.2.276.0.76.4.16&ISO
 5535 ^Zahnschmerz^Eberhard^^^Dr.^^^

5537 **Bei Versichertem als Autor:**

- 5538 1. Der unveränderbare Teil der KVNR (10 Stellen)
- 5539 2. "^"
- 5540 3. Nachname
- 5541 4. "^"
- 5542 5. Vorname
- 5543 6. "^"
- 5544 7. Weiterer Vorname
- 5545 8. "^"
- 5546 9. Namenszusatz
- 5547 10. "^"
- 5548 11. Titel
- 5549 12. "^^^&"
- 5550 13. "1.2.276.0.76.4.8"
- 5551 14. "&ISO"

5552 Beispiel: G995030566^Gundlach^Monika^^^^^^&1.2.276.0.76.4.8&ISO
 5553 Sowohl beim LE als auch beim Versicherten müssen Vorname und Nachname belegt
 5554 werden.

5556 **Software-Komponente bzw. Gerät als Autor**

5557 Beim (automatisierten) Einstellen von Dokumenten MUSS der max. 256-Zeichen lange

5558 Name der Software-Komponente bzw. des Geräts als Nachname und ggf. als Vorname(n)
5559 eingetragen werden.

5560 Beispiel: ^PHR-Gerät-XY^PHR-Software-XY

5561 Im Falle einer DiGA MUSS das Feld Autor folgendermaßen aufgebaut sein:

- 5562 1. Telematik-ID der DiGA
- 5563 2. "^"
- 5564 3. Name der DiGA (Name der Verordnungseinheit)
- 5565 4. "^"
- 5566 5. Name des DiGA-Herstellers
- 5567 6. "^"
- 5568 7. optionale Ergänzung der Bezeichnung der SW
- 5569 8. "^"
- 5570 9. optionale Ergänzung der Bezeichnung der SW
- 5571 10. "^"
- 5572 11. optionale Ergänzung der Bezeichnung der SW
- 5573 12. "^^^&"
- 5574 13. <OID für DiGAs, wie in professionOID>
- 5575 14. "&ISO"

5576 Für alle drei Arten von Autoren (Versicherter, LE, Gerät) MUSS jeweils Vorname und
5577 Nachname angegeben sein.

5579 Falls die Vorgaben nicht erfüllt werden, MUSS der XDS Document Service die Operation
5580 mit dem Fehler `XDSRegistryMetadataError` ablehnen und im `codeContext`-Attribut
5581 des zurückgegebenen `rs:RegistryError-Elements` antworten mit: `"errorText='Invalid
5582 metadata';metadata='authorPerson'"` antworten.

5583 [`<=`]

5584 **A_14763-04 -XDS Document Service - Nutzungsvorgabe für** 5585 **SubmissionSet.authorInstitution**

5586 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
5587 Dokumenten bei `SubmissionSet.authorInstitution` neben [IHE-ITI-TF3#4.2.3.1.4.1]
5588 auch die folgenden Vorgaben beachten.

- 5589 1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
- 5590 2. "^^^^^&"
- 5591 3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine
5592 Telematik-ID)
- 5593 4. "&ISO^^^^"
- 5594 5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

5595 Beispiele:

- 5596 • Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-
5597 e518
- 5598 • gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^8-
5599 34923902a

5600 [**<=**]

5601 Hinweis: Wenn das einstellende Client-System gar keinen Wert einstellen darf oder muss
 5602 für das `authorInstitution`-Feld, dann sind auch die entsprechenden Formatvorgaben
 5603 hinfällig. Das trifft in diesem Fall auf das ePA FdV zu, welches das Feld
 5604 `SubmissionSet.authorInstitution` gar nicht befüllen darf (siehe A_14760-*).

5605 **A_21511-01 -Nutzungsvorgabe `SubmissionSet.authorInstitution` für DiGAs**

5606 Der XDS Document Service MUSS sicherstellen, dass DiGAs beim Upload von
 5607 Dokumenten, die folgenden Nutzungsvorgaben für das Metadatenattribut
 5608 `DocumentEntry.authorInstitution` sowie `SubmissionSet.authorInstitution` berücksichtigen.
 5609 Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.1.4.1] genügen und ist inhaltlich
 5610 nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen.

- 5611 1. Name des Anbieters der DiGA
- 5612 2. "^^^^^&"
- 5613 3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine
 5614 Telematik-ID)
- 5615 4. "&ISO^^^^"
- 5616 5. Telematik-ID der DiGA

5617 [**<=**]

5618 **A_21209-03 -XDS Document Service - Nutzungsvorgabe für**
 5619 **`DocumentEntry.authorInstitution`**

5620 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
 5621 Dokumenten bei `DocumentEntry.authorInstitution` neben [IHE-ITI-
 5622 TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

- 5623 1. Name der Leistungserbringereinstitution oder Name des Kostenträgers
- 5624 2. "^^^^^&"
- 5625 3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine
 5626 Telematik-ID)
- 5627 4. "&ISO^^^^"
- 5628 5. Telematik-ID der Leistungserbringereinstitution oder des Kostenträgers

5629 Die Komponenten 2.-5. sind nur anzugeben, wenn die Telematik ID (5.) der
 5630 Autoreninstitution bekannt ist oder ad-hoc ermittelt werden kann, bspw. über den
 5631 Verzeichnisdienst der TI-Plattform (VZD). Ansonsten wird ausschließlich der Name
 5632 gesetzt.

5633 Beispiele:

- 5634 • Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^1-
 5635 2c47sd-e518
- 5636 • gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^8-
 5637 34923902a
- 5638 • Arztpraxis Dr. Wiebke Werner

5639 [**<=**]

5640 **A_22408-02 -XDS Document Service - `DocumentEntry.authorInstitution` ohne**
 5641 **Telematik-ID**

5642 Der XDS Document Service MUSS Nachrichten zum Registrieren von Dokumenten bei
 5643 fehlender Telematik-ID in `DocumentEntry.authorInstitution` akzeptieren und

5644 daraufhin alle Zeichen hinter dem Namen der authorInstitution abschneiden und
5645 verwerfen.[<=]

5646 **A_14974-03 -XDS Document Service - Nutzungsvorgabe für**
5647 **DocumentEntry.patientId und SubmissionSet.patientId**

5648 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
5649 Dokumenten die folgenden Nutzungsvorgaben für DocumentEntry.patientId und
5650 SubmissionSet.patientId berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-
5651 TF3#4.2.3.2.16] bzw. [IHE-ITI-TF3#4.2.3.3.8] genügen und ist inhaltlich nach der
5652 folgenden Vorschrift zusammenzufügen bzw. zu belegen:

- 5653 1. Der unveränderbare Teil der KVN-R des Akteninhabers (10 Stellen)
5654 2. "^^^&"
5655 3. "1.2.276.0.76.4.8" (OID zur Kennzeichnung einer unveränderbaren KVN-R)
5656 4. "&ISO"

5657 Beispiel: G995030566^^^&1.2.276.0.76.4.8&ISO[<=]

5658 **A_27759-01 -XDS Document Service - Verarbeitung von Code System Version**
5659 **beim Metadatenattribut DocumentEntry.eventCodeList**

5660 Der XDS Document Service MUSS ausschließlich beim Metadatenattribut
5661 DocumentEntry.eventCodeList die Metadaten vom Typ Coded Attribute im Slot
5662 "codingScheme" bei Angabe einer System URL oder Canonical URL eine per Pipe-Symbol
5663 (|) angehängte Version akzeptieren und für eine Terminologievalidierung verwenden.
5664 Anderenfalls MUSS der XDS Document Service die Registrierung des Dokuments mit
5665 einem XDSRepositoryMetadataError-Fehlercode quittieren. Die Prüfung des Codes ohne
5666 Versionsangabe erfolgt gegen das aktuell registrierte und gültige Code System: Ist der
5667 Code vorhanden, MUSS der XDS Document Service diese Version anhängen.[<=]

5668 Beispiel: **Fehler! Linkreferenz ungültig.**

5669

5670 *3.12.1.8.3 Metadaten für Datenkategorien*

5671 **A_19388-23 -Nutzungsvorgaben für die Verwendung von Datenkategorien**

5672 Der XDS Document Service MUSS beim Einstellen eines Dokuments die folgende
5673 Zuordnung zu einer Datenkategorie (d. h. Assoziierung mit einem bestimmten Folder)
5674 vornehmen. Dabei haben Auswertungs- und Zuordnungsregeln, die sich aus A_14761-*
5675 und damit verbunden aus [gemSpec_IG_ePA] ableiten, immer den Vorrang gegenüber
5676 anderen Auswertungsregeln. Ferner MUSS der XDS Document Service sicherstellen, dass
5677 bei einer Aktualisierung eines Dokuments derselbe Ordner des zu ersetzenden
5678 Dokuments zugeordnet wird.

5679

5680 Für eine eindeutige Zuordnung zu einer Datenkategorie MUSS die Auswertung der
5681 Metadatenvorgaben in der Reihenfolge der folgend dargestellten Einsortierungskriterien
5682 erfolgen:

5683 **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_analysis	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 Neugeborenenenscreening)
eab	classCode = BRI
care	PracticeSettingCode = PFL*
rehab	practiceSettingCode =REHA
dental	practiceSettingCode =MZKH*
emergency	eventCodeList = • ED110102 (KDL-Code Notfalldatenmanagement (NFDMM)) • 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

Datenkategorie/Technischer Identifier/Foldercode	Einsortierkriterium (anzuwenden auf DocumentEntry, wenn nicht anders angegeben. Oder-Verknüpfungen, wenn nicht "und" angegeben)
other	Alle Dokumente, die in keine andere Kategorien eingeordnet werden können

5684 *Falls Basiskonzepte angegeben werden, dann gelten automatisch alle Subkonzepte, z.B.
 5685 gilt für die Kategorie "care" die Einsortierregel bei PracticeSettingCode = PFL wie auch für
 5686 die Sub-Konzepte ALT (Altenpflege) und KIN (Kinderpflege).[<=]

5687 3.12.1.8.4 Automatisches Umschreiben von Daten

5688 Dieser Abschnitt enthält Vorgaben für Datenanpassungen, die für bestehende Daten im
 5689 XDS Document Service vorgenommen werden müssen (z. B. wenn sie durch Änderungen
 5690 im Rahmen einer neuen Version des XDS Document Service notwendig werden).

5691 **A_27482-02 -XDS Document Service – Metadatenkorrektur bei vorhandenen** 5692 **elektronischen Arztbriefen**

5693 Der XDS Document Service MUSS die Metadaten (DocumentEntry) von bestehenden
 5694 Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief)
 5695 gemäß [gemSpec_IG_ePA] derartig anpassen, dass DocumentEntry.eventCodeList
 5696 zusätzlich um den KDL-Code (code: ED110104, codeSystem: **Fehler! Linkreferenz**
 5697 **ungültig.**, displayName: eArztbrief) erweitert wird, wenn dieser nicht bereits vorhanden
 5698 ist. Dabei muss [version] mit der aktuellen Version (z.B. 2025) gemäß
 5699 [gemIG_TI_Terminology] ersetzt werden.[<=]

5700 **A_28661 -XDS Document Service – Korrektur Code System-Werte bei** 5701 **vorhandenen Dokumenten**

5702 Der XDS Document Service MUSS in den Metadaten (DocumentEntry) von bestehenden
 5703 Dokumenten diejenigen Code System-Werte, die mit dem Präfix "urn:oid:" beginnen,
 5704 derartig anpassen, dass das Präfix gelöscht wird.
 5705 [<=]

5706 Beispiel: Der ursprüngliche Wert "urn:oid:1.2.276.0.76.5.511" wird nach der Anpassung
 5707 dann als "1.2.276.0.76.5.511" gespeichert.

5708 **A_28887-01 -XDS Document Service – Korrektur einer DocumentEntry.uniqueId**

5709 Der XDS Document Service MUSS einmalig nach Öffnen des Aktenkontos jede
 5710 DocumentEntry.uniqueId, die nicht dem erlaubten Format gemäß A_14760-* entspricht,
 5711 neu vergeben. Dazu MUSS der XDS Document Service eine neue UUID generieren (in
 5712 Kleinbuchstaben, mit vorangestelltem Präfix "urn:uuid:") und die rootDocumentUniqueId
 5713 in der DocumentEntry.referenceIdList aktualisieren.Falls eine rootDocumentUniqueId in
 5714 einer General Deny Policy vorhanden ist, MUSS diese mit der neu generierten UUID
 5715 aktualisiert werden.[<=]

5716 Hinweis: Ein Beispiel für das neu zu generierende UUID-Format lautet
 5717 "urn:uuid:ce1607ec-2a37-41a4-b441-dcde48d0bed2".

5718 **A_28833 -XDS Document Service – Migration von Code Systemen auf Haupt-URL**

5719 Der XDS Document Service MUSS die Metadaten von bestehenden DocumentEntries,
 5720 SubmissionSets, Folders und Associations wie folgt anpassen, sofern das entsprechende
 5721 Metadatum Codes enthält:

- 5722 • Der XDS Document Service MUSS für jeden Code prüfen, ob für das gegebene
 5723 Code System gemäß [gemIG_TI_Terminology] unter den "Naming Systems"
 5724 alternative Namen definiert sind und das bestehende Code System durch

- denjenigen Namen ("Identifizier") 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.

5745 [$\leq$]

5746 In der Regel bedeutet dies, dass Code Systems, die bisher als OID oder unter Angabe
5747 einer Alternativ-URL abgespeichert wurden, stattdessen mit Haupt-Identifizier + Version
5748 des Code Systems gespeichert werden, um einen konsistenten Datenbestand zu
5749 erreichen.

5750 Wenn der "preferred" Identifizier in den Bestandsdaten bereits vergeben ist, ist keine
5751 Änderungen am Code System vorzunehmen.

5752 Für XDS wird die Versionsangabe eines Code-System-Werts (bei URL-basierte Werte)
5753 über ein "|" -Symbol angehängt, siehe A_27759*.

5754 Die Version ist nur in Fällen hinzuzufügen, in denen das entsprechende Code System
5755 gemäß [gemIG_TI_Terminology] eine Version führt.

5756 **A_28924-01 -XDS Document Service – Korrektur Code System bei XDW** 5757 **Workflow Codes in DocumentEntry.eventCodeList und** 5758 **DocumentEntry.formatCode**

5759 Der XDS Document Service MUSS einmalig nach dem Öffnen des Aktenkontos
5760 sicherstellen, dass die etwaig vergebenen Codes "urn:ihe:iti:xdw:2011:eventCode:open"
5761 und "urn:ihe:iti:xdw:2011:eventCode:closed" in der DocumentEntry.eventCodeList aller
5762 Dokumentmetadaten dem Code System "[http://www.ihe-](http://www.ihe-d.de/fhir/CodeSystem/WorkflowEvents)
5763 [d.de/fhir/CodeSystem/WorkflowEvents](http://www.ihe-d.de/fhir/CodeSystem/WorkflowEvents)" zugeordnet werden. Wurden sie ferner
5764 fälschlicherweise als formatCode verwendet, MUSS der XDS Document Service sie mit
5765 der zuvor genannten, korrekten Code System URL als eventCode speichern. Als Ersatz-
5766 Code ist "urn:ihe:iti:xds:2017:mimeTypeSufficient" zu verwenden. [$\leq$]

5767 **3.12.1.9 Strukturierte Dokumente**

5768 Die elektronische Patientenakte unterstützt unterschiedliche sogenannte "strukturierte
5769 Dokumente", deren Aufbau über Implementation Guides genau vorgegeben ist. Der
5770 Umfang der unterstützten strukturierten Dokumente wird durch den Umfang der
5771 veröffentlichten Implementation Guides festgelegt (3.12.1.9.2- Konfigurierbarkeit). Für

5772 alle strukturierten Dokumente gelten spezifische Metadatenvorgaben, um sie eindeutig zu
5773 identifizieren und gezielt verarbeiten zu können.

5774 **A_14761-08 -Nutzungsvorgaben für die Verwendung von IHE ITI XDS-**
5775 **Metadaten bei strukturierten Dokumenten**

5776 Der XDS Document Service MUSS die Nutzungsvorgaben für strukturierte Dokumente
5777 unter [gemSpec_IG_ePA] berücksichtigen. Dabei ist das Format des Dokuments, welches
5778 über einen Code des Metadatenattributs `formatCode` ausgedrückt wird, führend. Das
5779 bedeutet, bei Registrierung eines strukturierten Dokuments mit einem `formatCode`
5780 MÜSSEN die weiteren Metadatenattribute `classCode`, `typeCode`, `mimeType` sowie
5781 `eventCodeList` entsprechend belegt werden. Der XDS Document Service MUSS eine
5782 solche Registrierung diesbzgl. prüfen und im Fehlerfall analog zu A_14938-*
5783 antworten.[<=]

5784 *3.12.1.9.1 Sammlungstypen*

5785 Je nach Art ihrer Zusammensetzung und ihrer Handhabung existieren unterschiedliche
5786 Typen strukturierter Dokumente, sogenannte medizinische Informationsobjekte. Ein
5787 medizinisches Informationsobjekt (MIO) ist eine **Sammlung** von Informationen zu
5788 medizinischen, strukturellen oder administrativen Sachverhalten, die in sich geschlossen
5789 oder entsprechend verschachtelt vorliegt. Zudem ist ein MIO eine klar definierte Vorgabe,
5790 wie diese Informationssammlung in der elektronischen Patientenakte gespeichert wird,
5791 damit semantische und syntaktische Interoperabilität gewährleistet werden. Die
5792 Festlegung dieser Vorgaben ist gemäß SGB V Aufgabe der KBV. Beispiele für
5793 medizinische Informationsobjekte sind der Impfpass, das Kinderuntersuchungsheft, der
5794 Mutterpass, das zahnärztliche Bonusheft, oder DiGA. MIOs werden über Sammlungen
5795 und Sammlungstypen umgesetzt.

5796 Einige strukturierte Dokumente sind für sich genommen vollständig und schlüssig. Sie
5797 sind ohne Zuhilfenahme weiterer Dokumente in der ePA für einen Benutzer sinnvoll zu
5798 verwenden. Andere Typen strukturierter Dokumente müssen hingegen fast immer in
5799 Kombination betrachtet werden, z. B. Impfpassdokumente. Bei letzteren spiegelt jedes
5800 Impfpassdokument ein oder mehrere Impfungen wieder. Ein Impfpass, wie er in der
5801 analogen Welt geläufig und als logisches Konstrukt sinnvoll ist, besteht immer aus der
5802 gemeinsamen Betrachtung aller Impfpassdokumente und somit aller vorhandenen
5803 Impfeinträge. Die Kombination ein oder mehrerer strukturierter Dokumente ergeben eine
5804 Sammlung.

5805 Eine Sammlungsinstanz (z. B. der Mutterpass der ersten Schwangerschaft der Patientin
5806 Martha Mustermann) ist eine konkrete Ausprägung der Information, die zwischen den
5807 beteiligten Akteuren ausgetauscht wird. Nicht jede Sammlung besteht zwangsläufig aus
5808 Dokumenten desselben Formats: Ein Kinderuntersuchungsheft beispielsweise besteht aus
5809 Dokumenten mit drei verschiedenen strukturierten Dokumenttypen. Zentral für alle
5810 Sammlungstypen ist immer mindestens ein strukturiertes Dokument mit einem
5811 festgelegten Dokumentenformat. Für eine technische Umsetzung sind die
5812 Sammlungstypen "mixed" und "uniform" zu unterscheiden, die technisch unterschiedlich
5813 umgesetzt werden und zum Teil unterschiedliche Operationen erlauben.

5814 Der Sammlungstyp "mixed" fasst semantisch zusammengehörige, strukturierte
5815 Dokumente unterschiedlicher Struktur mittels Ordner zu einer Sammlung zusammen. Der
5816 Sammlungstyp "uniform" fasst semantisch zusammengehörige, strukturierte Dokumente
5817 gleicher Struktur zusammen.
5818 Sammlungen, die mehr als eine Sammlungsinstanz haben, z.B. Mutterpass, werden über
5819 dynamische Ordner abgebildet. Dies stellt sicher, dass zukünftige Versionen dieser
5820 strukturierten Dokumente/Pässe oder DiGA verlässlich verarbeitet werden können.
5821 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.

5860 *Hinweis: Die zeitliche Gültigkeit ergibt sich aus den Attributen "validFrom" und (optional)*
5861 *"clientReadOnlyFromDate" der Vorgaben in [gemSpec_IG_ePA].*

5862 3.12.1.9.2 Konfigurierbarkeit

5863 **A_17546-02 -Konfigurierbarkeit von strukturierten Dokumenten**

5864 Der XDS Document Service MUSS die Liste strukturierter Dokumente konfigurierbar
5865 machen, indem dieser die Unterstützung strukturierter Dokumente unter Angabe
5866 folgender Eigenschaften ermöglicht:

- 5867 • Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA]
5868 konfigurativ hinzufügen bzw. entfernen,
- 5869 • Sammlungen zu TAB_EPA_Sammlungstypen
5870 gemäß [gemSpec_IG_ePA] konfigurativ hinzufügen bzw. entfernen.

5871 [**<=**]

5872 Das Entfernen der Unterstützung von strukturierten Dokumenten oder
5873 Sammlungen bedeutet, dass diese zu einem früheren Zeitpunkt in das Aktensystem
5874 geschrieben werden konnten, aber durch Erreichen von "clientReadOnlyFromDate" nicht
5875 mehr geschrieben werden dürfen. Das Schreiben umfasst das Aktualisieren oder neu
5876 Anlegen. Das Lesen ist weiterhin erlaubt.

5877 **A_17551-01 -Prüfanforderungen zur Konfigurierbarkeit von Value Sets**

5878 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die zu konfigurierenden
5879 Value Sets des XDS Document Service gemäß der Anforderung A_17546-* den
5880 folgenden Prüfkriterien unterliegen, bevor bestehende, im XDS Document Service
5881 verarbeitete Value Sets verändert werden:

- 5882 • Es DÜRFEN KEINE Codes der Value Sets gelöscht werden, lediglich das Hinzufügen
5883 von Codes zu existierenden Value Sets ist aus Kompatibilitätsgründen erlaubt.
- 5884 • Neue Codes MÜSSEN den Formatvorgaben gemäß Tabelle 4.2.3.1.7-2 in [IHE-ITI-
5885 TF3#4.2.3.1.7] entsprechen und gegenüber einer internen Referenzliste validiert
5886 werden. Dies schließt auch Prüfungen zur Zeichenkodierung, der Datentypen als
5887 auch zu den Längenbeschränkungen ein.

5888 [**<=**]

5889 **A_21212-01 -Restriktionen zur Konfigurierbarkeit von Metadaten für** 5890 **strukturierte Dokumente und Sammlungen**

5891 Der XDS Document Service MUSS durch technische Maßnahmen sicherstellen, dass
5892 Änderungen an den in den Implementierungsvorgaben in [gemSpec_IG_ePA]
5893 spezifizierten Codes ausgeschlossen sind. [**<=**]

5894 **A_21214-03 -Konfiguration strukturierter Dokumente im Rahmen der** 5895 **Veröffentlichung durch die gematik**

5896 Der Anbieter des ePA-Aktensystems MUSS durch organisatorische Maßnahmen
5897 sicherstellen, dass die Konfiguration im Aktensystem zur Unterstützung strukturierter
5898 Dokumente aus [gemSpec_IG_ePA] ausschließlich im Rahmen der Veröffentlichung der
5899 Implementation Guides durch die gematik erfolgt. [**<=**]

5900 Bei Einführung neuer strukturierter Dokumente werden die beschriebenen
5901 Konfigurationsmöglichkeiten so verwendet, dass eine Erweiterung der Spezifikation und
5902 daraus resultierend eine Änderung des ePA-Aktensystems mit erneuter Zulassung nicht
5903 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.

widerspruchsfähige Funktion	Auswirkung bei erteiltem Widerspruch
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst ("erp-submission")	Alle vorhandenen Dokumente des Ordners "emp" (elektronischer Medikationsplan) werden gelöscht.

5937 *Hinweis zum Medikationsprozess: Dadurch wird verhindert, dass Leistungserbringer im*
 5938 *Versorgungsprozess veraltete oder unvollständige Daten verwenden.*

5939 **A_23860 -XDS Document Service - Löschen der Dokumente des**
 5940 **Medikationsprozesses**

5941 Der XDS Document Service des Aktensystems MUSS alle Dokumente aus dem Ordner
 5942 elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code =
 5943 "eMP") löschen, wenn der Status der widerspruchsfähigen Funktion "Einstellen von
 5944 Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst" (Id ==
 5945 "erp-submission") auf "Widerspruch erklärt" ("deny") geändert wird. [`<=`]

5946 **A_23895-02 -XDS Document Service - Keine Operationen mit Dokumenten des**
 5947 **Medikationsprozesses bei Widerspruch**

5948 Falls ein Widerspruch zur widerspruchsfähigen Funktion "Teilnahme am
 5949 Medikationsprozess" (Id ="medication" und status ="deny") vorliegt, MUSS der XDS
 5950 Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von
 5951 Dokumenten des Ordners elektronischer Medikationsplan (codeSystem =
 5952 "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für alle Nutzer, ausgenommen der
 5953 Versicherte oder befugte Vertreter (oid_versicherter), ablehnen und die Operation mit
 5954 dem Fehlercode ConsentDecisionViolation abrechnen.
 5955 [`<=`]

5956 **A_25151-01 -XDS Document Service – Prüfung der Widersprüche bei**
 5957 **Suchanfrage**

5958 Der XDS Document Service MUSS bei einer Suchanfrage die Suchergebnismenge für alle
 5959 Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid_versicherter), filtern
 5960 und sicherstellen, dass diese keinerlei XDS-Metadaten von Dokumenten des Ordners
 5961 elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code =
 5962 "eMP") enthält, wenn ein Widerspruch gegen die widerspruchsfähige Funktion "Teilnahme
 5963 am digital gestützten Medikationsprozess" (Id ="medication" und status ="deny")
 5964 vorliegt.
 5965 [`<=`]

5966 **3.12.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des**
 5967 **Medication Service durch eine spezifische LEI auf die Dokumente des**
 5968 **Aktenkontos**

5969 Wird ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische
 5970 LEI erklärt, verhindert der XDS Document Service, dass auf die Dokumente der Kategorie
 5971 "emp" zugegriffen werden kann.

5972 **A_26429 -XDS Document Service - Keine Operationen mit Dokumenten des**
 5973 **Medikationsprozesses bei Widerspruch gegen die Nutzung des Medication**
 5974 **Service durch eine spezifische LEI**

5975 Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische
 5976 LEI vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und
 5977 Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan
 5978 (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für diese LEI, ablehnen und

5979 die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.
5980 [`<=`]

5981 **A_26430 -XDS Document Service – Prüfung des Widerspruchs gegen die**
5982 **Nutzung des Medication Service durch eine spezifische LEI bei Suchanfrage**
5983 Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische
5984 LEI vorliegt, MUSS der XDS Document Service bei einer Suchanfrage die
5985 Suchergebnismenge für diese LEI filtern und sicherstellen, dass die
5986 Suchergebnismenge keinerlei XDS-Metadaten von Dokumenten des Ordners
5987 elektronischer Medikationsplan (`codeSystem = "urn:oid:1.2.276.0.76.5.512"; code =`
5988 `"eMP"`) enthält.
5989 [`<=`]

5990 **3.12.1.13 Protokollierung von Zugriffen auf den XDS Document Service**
5991 Anforderungen an den XDS Document Service sind in [gemIG_ePA_Basic] spezifiziert.

5992 **3.12.1.14 Unterstützungsleistung für das ePA-FdV**

5993 Der XDS Document Service akzeptiert aus Sicherheitsgründen nur bestimmte
5994 Dokumentenformate. Das schränkt auch das Format PDF auf bestimmte PDF/A-Varianten
5995 ein (siehe auch A_25233*). Daher müssen PDF-Dokumente des Versicherten unter
5996 Umständen vor dem Einstellen in die ePA konvertiert werden.
5997 Um das ePA-FdV dabei zu entlasten und Komplexität aus dem ePA-FdV zu nehmen, wird
5998 eine Funktion angeboten, durch die ein PDF in ein PDF/A konvertiert werden kann. Das
5999 ePA-FdV muss aber berücksichtigen, dass die Konvertierung ggf. technisch nicht
6000 durchgeführt werden kann oder das Ergebnis der Konvertierung durch ein geändertes
6001 Layout ggf. nicht verwendbar ist.

6002 **A_25456 -XDS Document Service - Keine negativen Auswirkungen auf**
6003 **Folgekonvertierungen von PDF zu PDF/A**

6004 Der XDS Document Service MUSS sicherstellen, dass eine Konvertierung eines PDF-
6005 Dokuments sich nicht schädlich auf folgende Konvertierungen auswirken kann. [`<=`]

6006 Hinweis zu A_25456*: Die Anforderung soll erreichen, dass ein potentiell über ein PDF-
6007 Dokument eingebrachter Schadcode nach der Konvertierung gelöscht wird, z.B. durch
6008 Zurücksetzen der Sandbox oder der VAU-Instanz

6009 **A_25455 -XDS Document Service - Isolation der Konvertierung von PDF zu**
6010 **PDF/A**

6011 Der XDS Document Service MUSS die Verarbeitung von PDF-Dokumenten, die im
6012 Rahmen der Konvertierung in ein PDF/A durchgeführt wird, in einer separaten VAU-
6013 Instanz durchführen, die ausschließlich eine Verbindung zu einem ePA-FdV besitzen
6014 darf. [`<=`]

6015 **A_25454 -XDS Document Service - Realisierung der Schnittstelle**
6016 **I_Tool_Convert_PDF_Insurant**

6017 Der XDS Document Service MUSS die Operationen der Schnittstelle
6018 I_Tool_Convert_PDF_Insurant gemäß [I_Tool_Convert_PDF_Insurant] umsetzen [`<=`]

6019 **A_26129 -ePA-Aktensystem - Rahmenbedingungen bei Nutzung einer Service-**
6020 **VAU für PDF-Konvertierung**

6021 Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV
6022 für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU
6023 verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die vom ePA-
6024 FdV übermittelten PDF-Dokumente in der Aktenkontoverwaltungs-VAU ausschließlich
6025 weitergeleitet aber ansonsten nicht verarbeitet werden. Gleiches gilt für die von der
6026 Service-VAU an das ePA-FdV übermittelten konvertierten PDF/A-Dokumente. [`<=`]

6027 **A_26130 -ePA-Aktensystem - maximale Lebensdauer einer Service-VAU für**
6028 **PDF-Konvertierung**

6029 Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV
6030 für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU
6031 verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die Lebensdauer
6032 einer solchen Service-VAU-Instanz maximal 12 Stunden beträgt.[<=]

6033 **A_26131 -ePA-Aktensystem - Keine Speicherung von in der Service-VAU für**
6034 **PDF-Konvertierung verarbeiteten Daten**

6035 Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV
6036 für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU
6037 verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass weder die vom
6038 ePA-FdV übermittelten und zu konvertierenden PDF-Dokumente noch die daraus
6039 konvertierten PDF/A-Dokumente von der "PDF-VAU" im ePA-Aktensystem gespeichert
6040 werden.[<=]

6041 **A_26121 -ePA-Aktensystem - Keine Verarbeitung von Geräteinformationen**

6042 Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV
6043 für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU
6044 verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass keine
6045 Geräteinformationen (Device Management) von Nutzern verarbeitet werden.[<=]

6046 **3.12.2 FHIR Data Services**

6047 Anforderungen für FHIR Data Services werden nicht hier aufgelistet, sondern befinden
6048 sich in dafür gepflegten FHIR Implementation Guides (IG), auf die auch im
6049 entsprechenden Produkttypdeckbrief verwiesen wird.

6050

6051 **3.13 Audit Event Service**

6052 Ereignisse und Zugriffe auf die ePA eines Versicherten werden im ePA Aktensystem durch
6053 den Audit Event Service protokolliert. Anforderungen an den Audit Event Service sind
6054 in [gemIG_ePA_Basic] spezifiziert.

6055 **3.14 Information Services**

6056 **3.14.1 Information Service**

6057 Der Information Service ist ohne die Nutzung eines VAU-Kanals nutzbar. Die über den
6058 Information Service genutzten Daten sind ausschließlich persistierte Daten des
6059 Aktenkontos, die weder mit dem SecureAdminStorageKey noch mit dem
6060 SecureDataStorageKey gesichert sind.

6061 Der Zugang erfolgt durch Nutzung der Schnittstelle `I_Information_Service`.

6062 **A_24344 -Information Service - Realisierung der Schnittstelle**
6063 **`I_Information_Service`**

6064 Der Information Service MUSS die Operationen der Schnittstelle `I_Information_Service`
6065 gemäß [`I_Information_Service`] umsetzen.[<=]

6066 **A_24345 -Information Service - Kein Zugriff auf verschlüsselte Daten des**
6067 **Aktenkontos**

6068 Der Information Service DARF NICHT auf Daten zugreifen, die nicht explizit für die
6069 Verwendung durch den Informationsdienst bereitgestellt wurden. Dazu gehören
6070 insbesondere alle Daten des Aktenkontos, die mit den versichertenindividuellen
6071 Schlüsseln zur Daten- oder Befugnispersistierung (SecureDataStorageKey oder
6072 SecureAdminStorageKey) gesichert sind.[<=]

6073 **3.14.1.1 Informationen zu Widersprüchen (Consent Decisions)**

6074 Die Widersprüche eines Versicherten gegen die Nutzung von Funktionen der
6075 elektronischen Patientenakte werden durch das Consent Decision Management gesichert
6076 administriert. Änderungen an den Widersprüchen erfolgen dort.

6077 Der Information Service bietet für die Nutzergruppen der ePA eine einfache
6078 Abfragemöglichkeit der aktuell erteilten oder nicht erteilten Widersprüche auch ohne die
6079 Nutzung des Consent Decision Managements an. Liegt ein Widerspruch gegen die
6080 Nutzung einer Funktion vor, kann auf die Ausführung der zur Nutzung dieser Funktion
6081 notwendigen Aktionen mit der ePA eines Versicherten durch den Client verzichtet
6082 werden.

6083 Für diese vereinfachte Abfragemöglichkeit der aktuellen Widersprüche verwendet der
6084 Information Service den durch das Consent Decision Management persistent
6085 übertragenen Zustand der Widersprüche ("Cache" des Zustands der Widersprüche).
6086 Berücksichtigt wird dabei die Widerspruchsinformation, für die eine vereinfachte Abfrage
6087 vorgesehen ist (Widersprüche der Klasse "Versorgungsprozess").

6088 **3.14.1.2 Informationen zur Anwenderperformance (UX Performance)**

6089 Der Information Service stellt für die Umgebung der Leistungserbringer die Operation zur
6090 Sammlung der Messwerte zu den Anwendungsfällen der Nutzererfahrung zur Verfügung.
6091 Die Weiterverarbeitung der gesammelten Daten ist in 2.8- Performance aus
6092 Anwendersicht definiert und vorgegeben.

6093 **3.14.2 Information Service - Account**

6094 Die Operationen der Information Service - Account werden für den Umzug eines
6095 existierenden Aktenkontos zu einem neuen Anbieter verwendet. Die Nutzung der
6096 Operationen erfolgt exklusiv durch die Aktensystembetreiber.

6097 Die Verwendung der einzelnen Operationen erfolgt im Verbund mit den Operationen der
6098 Schnittstelle I_Account_Management für die Umsetzung der Anwendungsfälle eines
6099 automatischen Aktenkontoumzugs und sind in 3.1- Aktenkontoverwaltung erläutert.

6100 **A_24424 -Information Service Account - Realisierung der Schnittstelle**
6101 **I_Information_Service_Accounts**

6102 Der Information Service MUSS die Operationen der Schnittstelle
6103 I_Information_Service_Accounts gemäß [I_Information_Service_Accounts]
6104 umsetzen.[<=]

6105 **A_24665 -Information Service Account - Nutzung beidseitig authentisiertes TLS**

6106 Der Information Service MUSS sicherstellen, dass die Operationen der Schnittstelle
6107 I_Information_Service_Accounts ausschließlich unter Verwendung einer beidseitig
6108 authentisierten TLS-Verbindung zwischen den beteiligten Aktensystemen genutzt werden
6109 und die Operationen ansonsten abgebrochen und mit einer Fehlermeldung gemäß
6110 Vorgaben in [I_Information_Service_Accounts] beantwortet werden.[<=]

6111 **A_25054-01 -Information Service Account - Gegenseitige Authentisierung**
6112 **Aktensysteme**

6113 Der Information Service Account MUSS für die beidseitige Authentisierung die technische
6114 Rolle `oid_epa_mgmt` und die folgenden Zertifikatsprofile verwenden:

- 6115 • C.FD.TLS-S als Anbieter des Service (Server),
- 6116 • C.FD.TLS-C als Nutzer des Service (Client)

6117 [`<=`]

6118 **A_25053 -Information Service Account - Prüfung der TLS-Zertifikate**

6119 Der Information Service Account MUSS bei der Authentifizierung eines jeweils anderen
6120 Aktensystems die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC_PKI_018
6121 durchführen. Zur Prüfung des TLS-Zertifikats C.FD.TLS-S sind dabei die
6122 Parameter `PolicyList=oid_fd_tls_s`, `IntendedKeyUsage=digitalSignature`,
6123 `intendedExtendedKeyUsage=id-kp-serverAuth`, `OCSP-Graceperiod=60` Minuten, `Offline-`
6124 `Modus=nein` zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD.TLS-C sind dabei die
6125 Parameter `PolicyList=oid_fd_tls_c`, `IntendedKeyUsage=digitalSignature`,
6126 `intendedExtendedKeyUsage=id-kp-clientAuth`, `OCSP-Graceperiod=60` Minuten, `Offline-`
6127 `Modus=nein` zu verwenden.

6128 [`<=`]

6129 **3.14.3 EHR Information Service**

6130 Der EHR Information Service erbringt eine analoge Leistung zum Information Service,
6131 aber innerhalb der VAU. Über einen bestehenden VAU-Kanal können Informationen zur
6132 Existenz einer Akte oder den Widersprüchen zu Versorgungsprozessen abgerufen
6133 werden, ohne eine separate Verbindung zum Information Service aufzubauen.

6134 Der Zugang erfolgt durch Nutzung der Schnittstelle `I_Ehr_Information_Service`.

6135 **A_30119 -EHR Information Service - Realisierung der Schnittstelle**
6136 **I_Ehr_Information_Service**

6137 Der EHR Information Service MUSS die Operationen der Schnittstelle
6138 `I_Ehr_Information_Service` gemäß [`I_Ehr_Information_Service`] umsetzen.[`<=`]

6139 **3.15 Email Management**

6140 Das Email Management ermöglicht einem FdV-Nutzer die Verwaltung seiner E-Mail-
6141 Adresse und einem Kostenträger die Verwaltung von E-Mail-Adressen von Versicherten,
6142 die bei diesem Kostenträger versichert sind.

6143 Die Schnittstelle zum Verwalten der E-Mail-Adressen durch den Kostenträger dient dem
6144 ausschließlichen Zweck des Einstellens, Lesens und der Änderung von E-Mail-Adressen
6145 auf Verlangen des Versicherten. Dies ermöglicht dem Kostenträger, seinen Versicherten
6146 die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte auf Berichtigung und
6147 Auskunft bzgl. der im Aktensystem verarbeiteten E-Mail-Adresse zu gewährleisten.

6148 Für einen Versicherten kann nur genau eine E-Mail Adresse hinterlegt werden.

6149 **A_25435 -Email Management - Realisierung der Schnittstelle**
6150 **I_Email_Management**

6151 Das Email Management MUSS die Operationen der Schnittstelle `I_Email_Management`
6152 gemäß [`I_Email_Management`] umsetzen.[`<=`]

6153 **A_25438 -Email Management - Beschränkung der Schnittstellenoperationen auf**
6154 **E-Mail-Adressen des FdV-Nutzers**

6155 Das Email Management MUSS die Operationen der Schnittstelle `I_Email_Management`
6156 gemäß `[I_Email_Management]` auf die E-Mail-Adresse des aufrufenden Nutzers
6157 einschränken, sofern der Nutzer ein FdV-Nutzer ist. [`<=`]

6158 **A_26161 -Email Management - Nutzen von Email Management auch bei**
6159 **Widerpruch**

6160 Das Email Management MUSS sicherstellen, dass das Email Management auch von
6161 Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben. [`<=`]

6162 **A_26162 -Email Management - Versicherte nutzen Email Management**
6163 **ausschließlich im Home-AS**

6164 Das Email Management des ePA-Aktensystems MUSS sicherstellen, dass das Email
6165 Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-
6166 Aktensystem das Home-AS ist. [`<=`]

6167 Hinweis: Für das Email Management ist auch Anforderung A_26154* umzusetzen.

6168 **A_25439 -Email Management - Kostenträger kann ausschließlich E-Mail-**
6169 **Adressen der eigenen Versicherten verwalten**

6170 Das Email Management MUSS sicherstellen, dass ein Kostenträger mittels der
6171 Operationen der Schnittstelle `I_Email_Management` gemäß `[I_Email_Management]`
6172 ausschließlich E-Mail-Adressen von Versicherten verwalten kann, die beim Kostenträger
6173 versichert sind. [`<=`]

6174 **A_25440-01 -Email Management - Benachrichtigung bei Änderung der E-Mail-**
6175 **Adresse**

6176 Falls eine E-Mail-Adresse a) ersetzt oder b) ergänzt wird, MUSS das Device Management
6177 bei a) eine E-Mail an die alte und die neue E-Mail-Adresse senden und bei b) eine E-Mail
6178 an die neue E-Mail-Adresse senden, in der bei a) über die Ersetzung bzw. bei b) die
6179 Ergänzung einer E-Mail-Adresse informiert wird. In der E-Mail MUSS darüber informiert
6180 werden, wann und ob der FdV-Nutzer selbst oder der Kostenträger die E-Mail ersetzt
6181 bzw. ergänzt hat. [`<=`]

6182 **A_25441 -Email Management - Information bzgl. der Ergänzung bei E-Mail-**
6183 **Adressen**

6184 Das Email Management MUSS sicherstellen, dass der FdV-Nutzer für eine im Email
6185 Management hinterlegte E-Mail-Adresse erkennen kann, wann und von wem diese E-
6186 Mail-Adresse ergänzt wurde. [`<=`]

6187 **A_25968-01 -Email Management - Maximale Anzahl E-Mail-Adressen**

6188 Das Email Management MUSS sicherstellen, dass für einen Nutzer maximal eine E-Mail-
6189 Adresse hinterlegt werden kann. [`<=`]

6190 **A_26163 -Email Management - Keine Persistierung einer im Rahmen der**
6191 **Vertreterereinrichtung übergebenen E-Mail-Adresse**

6192 Das Email Management MUSS sicherstellen, dass eine im Rahmen des Anwendungsfalls
6193 der Vertreterereinrichtung vom Nutzer übermittelte E-Mail-Adresse nicht persistiert und
6194 spätestens bei Beendigung der User Session gelöscht wird. [`<=`]

6195 **A_26164 -Email Management - Keine Geräteregistrierung mit der im Rahmen**
6196 **der Vertreterereinrichtung übergebenen E-Mail-Adresse**

6197 Das Email Management MUSS sicherstellen, dass keine E-Mail-Adressen zur Übermittlung
6198 eines Geräteregistrierungscodes genutzt werden, die dem ePA-Aktensystem im Rahmen
6199 des Anwendungsfalls der Vertreterereinrichtung übermittelt wurden. [`<=`]

6200 Hinweis zu A_26163 und A_26164: Die im Rahmen des Anwendungsfalls der
6201 Vertretereinrichtung übermittelte E-Mail-Adresse wird ausschließlich zur Information des
6202 Vertreters über die Einrichtung der Vertretung genutzt (vgl. A_24755-*).

6203 3.16 Zusätzliche Anforderungen an den Authorization Service

6204 Der ePA Authorization Service wird sowohl für die Authentisierung der Versicherten über
6205 das FdV als auch für die Authentisierung von Leistungserbringern und Kostenträgern über
6206 deren Primärsystem benötigt. Ebenso muss die Zugriffsautorisierung für andere
6207 Fachdienste wie z.B. E-Rezept geprüft werden. Die Festlegungen für den Authorization
6208 Server finden sich in [gemSpec_IDP_FD]. Dieser Abschnitt des vorliegenden Dokuments
6209 enthält spezifische Anforderungen, die vom Authorization Service des Aktensystems
6210 zusätzlich umzusetzen sind.

6211 A_24923 -Authorization Service - I_Authorization_Service

6212 Der Authorization Service MUSS die Operationen der
6213 Schnittstelle `I_Authorization_Service` implementieren gemäß
6214 `[I_Authorization_Service].[<=]`

6215 A_25283 -Authorization Service - Konvertieren von ID-Token

6216 Der Authorization Service MUSS sicherstellen, dass für ein nach erfolgreicher
6217 Authentifizierung des Nutzers vorliegendes ID-Token mittels Regel *rr0* gemäß
6218 *Tab_AS_Entitlement_Registration_Rules* ein HSM-ID-Token erstellt wird, bevor das ID-
6219 Token zeitlich ungültig ist. `[<=]`

6220 3.16.1 Anforderungen an den Authorization Service für die 6221 Authentisierung von Versicherten (FdV)

6222 Im Rahmen der Authentisierung des Versicherten erfolgt die Prüfung der
6223 Geräteregistrierung (Verifikation) direkt. Das Gerät muss dafür die Geräteparameter
6224 eines zuvor ausgeführten und bestätigten Registrierungsprozesses verwenden

6225 Bisher nicht registrierte Geräte, bzw. Geräteparameter einer bisher nicht bestätigten
6226 Geräteregistrierung, können unter Verwendung des Device Management registriert, bzw.
6227 bestätigt werden (siehe Kapitel 3.11- Device Management).

6228

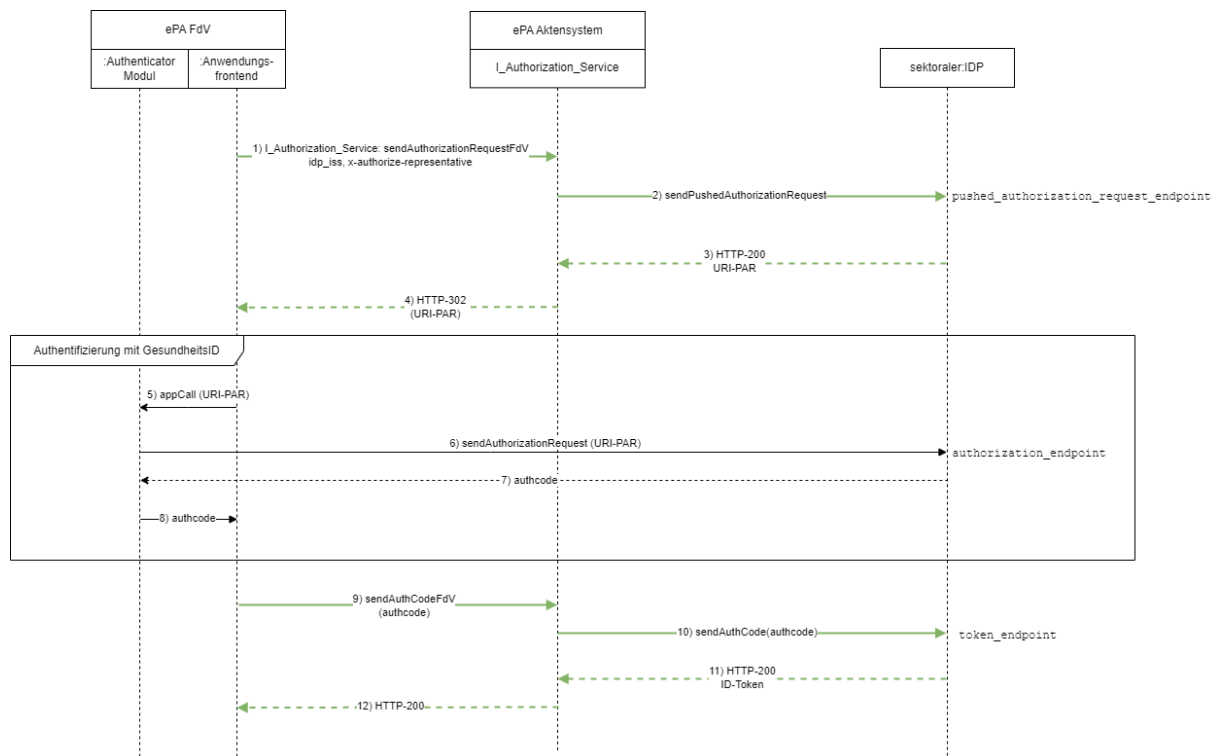


Abbildung 8: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP

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) an durch den vom ePA-FdV übergebenen Parameter idp-iss adressierten sektoralen IDP gemäß [gemSpec_IDP_FD#AF_10117] mit folgenden Parametern aufrufen:

Parameter	Wert	Anmerkung
scope	"openid urn:telematik:display_name urn:telematik:versicherter urn:telematik:family_name urn:telematik:given_name"	Notwendige Scopes für den Zugriff für die Autorisierung von Nutzern am ePA-Aktensystem
acr_values	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung

Parameter	Wert	Anmerkung
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 Authorization Service bekannt geben.

6236 [**<=**]

6237 Hinweis 1: An die redirect_uri im Pushed Authorization Request sendet der sektorale IDP
6238 den ausgestellten Authorization Code (siehe [gemSpec_IDP_Sek])

6239 Hinweis 2: Der Redirectaufruf, der vom Authenticator Modul an die redirect_uri
6240 ausgeführt wird, wird vom ePA-FdV über Plattformmechanismen (deeplink/universallink)
6241 gefangen und stellt selbst einen POST-Request an den Endpunkt des Authorization
6242 Service.

6243 **A_26584 -Authorization Service - Liste der redirect_uris im Entity Statement**

6244 Der Authorization Service MUSS in seinem Entity Statement im claim redirect_uris
6245 die redirect_uris aller Mandanten auflisten, welche bei der Registrierung an einem
6246 beliebigen ePA Authorization Service eine eigene redirect_uri angegeben haben. Über
6247 Änderungen des claim redirect_uris MUSS der Anbieter des Federation Master vor
6248 produktiver Verwendung informiert werden[**<=**]

6249 Hinweis: Im Registrierungsprozess eines Mandanten mit eigener redirect_uri muss
6250 sichergestellt sein,

- 6251 • dass alle Anbieter von ePA Authorization Servern (ePA Aktensystem Anbieter)
6252 entsprechend informiert sind und das Entity Statement anpassen
- 6253 • dem Hersteller des Federation Master über ein ITSM Change bekannt gemacht
6254 wird, dass sich die Entity Statements aller ePA Authorization Server ändern

6255 **A_27145 -Synchronisation "redirect_URI" mit Marktteilnehmer - E-Mail-Adresse**

6256 Der Anbieter ePA-Aktensystem MUSS der gematik eine E-Mail-Adresse mitteilen, über
6257 welche er die eigenverantwortliche Registrierung (von redirect-URIs im Entity-
6258 Statement) durchführt und über die der Anbieter bei Änderungen erreichbar ist.

6259
6260 Hinweis: Diese E-Mail-Adressen werden durch das Provider Management der gematik
6261 anschließend unter den relevanten Anbietern verteilt bzw. können dort erfragt werden.
6262 Die Änderung der E-Mail-Adressen ist ebenfalls zu kommunizieren.

6263
6264 Hintergrund: Für Stellvertretung via ePA-FdV ist eine Synchronisierung der redirect_URIs
6265 notwendig.[**<=**]

6266 **A_27186 -Synchronisation "redirect_URI" mit Marktteilnehmer - Information**
6267 Der Anbieter ePA-Aktensystem MUSS bei Änderungen der redirect URIs im eigenen
6268 Entity Statement allen anderen Marktteilnehmern des gleichen Fachdiensttyps diese
6269 Änderung innerhalb 24 Stunden mitteilen.[<=]

6270 **A_27187 -Synchronisation "redirect_URI" mit Marktteilnehmer - Aktualisierung**
6271 Der Anbieter ePA-Aktensystem MUSS nach dem Empfang der Mitteilungen über
6272 Änderungen der Redirect URIs in einem externen Entity Statement diese Änderung
6273 binnen 24 Stunden in den Redirect URIs des eigenen Entity Statement synchronisieren.
6274
6275 Hinweis: Diese Änderung erfordert anschließend keine Information nach A_27186.[<=]

6276 **A_24878-01 -Authorization Service - Authentifizierung eines Versicherten am**
6277 **ePA-FdV des Vertreters**
6278 Falls der Eingangsparameter x-authorize-representative=True der Operation
6279 I_Authorization_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der
6280 Authorization Service im PAR als Parameter amr mit den Werten
6281 urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer
6282 nur über eGK+PIN authentisieren darf.[<=]

6283 **A_26189-01 -Authorization Service - Authentifizierung eines Versicherten im**
6284 **Gastmodus mit eGK und PIN**
6285 Falls der Eingangsparameter x-authorize-egk=True der Operation
6286 I_Authorization_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der
6287 Authorization Service im PAR als Parameter amr mit den Werten
6288 urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer
6289 nur über eGK+PIN authentisieren darf.[<=]

6290 **A_24937-01 -Authorization Service - Einschränkung bei Authentifizierung eines**
6291 **Versicherten am ePA-FdV des Vertreters**
6292 Der Authorization Service MUSS sicherstellen, dass ein mit x-authorize-
6293 representative=True authentisierter Nutzer ausschließlich Zugriff auf das Entitlement
6294 Management erhält.[<=]

6295 **A_26159 -Authorization Service - Prüfen der Device Attestation**
6296 Der Authorization Service MUSS sicherstellen, dass von einem anderen ePA-Aktensystem
6297 signierte Device Attestations ausschließlich akzeptiert werden, wenn

- 6298 • die Device Attestation gemäß A_25042-* valide von einer Signaturidentität der
6299 VAU eines anderen ePA-Aktensystems signiert wurde,
- 6300 • die KVNR in der Device Attestation mit der KVNR im ID-Token des angemeldeten
6301 Nutzers übereinstimmt,
- 6302 • die Device Attestation zeitlich gültig ist.

6303 [<=]

6304 **A_26160 -Authorization Service - Keine Persistierung der Device Attestation**
6305 Der Authorization Service MUSS sicherstellen, dass die von einem anderen ePA-
6306 Aktensystem signierte Device Attestation und deren Inhalte spätestens bei Beendigung
6307 der User Session gelöscht und nicht persistiert werden.[<=]

6308 **A_25310-01 -Authorization Service - Einschränkung bei Authentifizierung mit**
6309 **einem unregistrierten Gerät**
6310 Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wird und der Nutzer
6311 nicht mit x-authorize-representative=True authentisiert wurde, MUSS der
6312 Authorization Service sicherstellen, dass der Nutzer ausschließlich Zugriff auf das Device
6313 Management erhält.[<=]

6314 Hinweis:
6315 Ein vollständiger Zugriff eines authentisierten Nutzers auf alle Dienste des Aktensystems
6316 kann nur mit einem Gerät erfolgen, dessen Geräteregistrierung bei der Authentifizierung
6317 des Nutzers erfolgreich verifiziert wurde.
6318 Ein Nachweis einer Geräteregistrierung ist entweder DeviceID (deviceIdentifier und
6319 deviceToken), die für den Nutzer im Aktensystem bekannt sind oder die vom Client
6320 übergebene Device Attestation (deviceAttestation), die zuvor am Device Management des
6321 Home Aktensystems durch den Client abgerufen wurde.

6322 **A_24804-01 -Authorization Service - Prüfung auf registriertes Gerät**

6323 Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des
6324 Vertreters handelt und im Operationsaufruf
6325 I_Authorization_Service::sendAuthCodeFdV eine DeviceID (deviceIdentifier und
6326 deviceToken) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung
6327 eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer
6328 registriert und bestätigt ist und übereinstimmt. [<=]

6329 **A_24914-03 -Authorization Service - Prüfung auf registriertes Gerät - kein
6330 registriertes Gerät**

6331 Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wurde, MUSS
6332 der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung
6333 abbrechen und die User Session beenden. [<=]

6334

6335 **A_24915-01 -Authorization Service - Prüfung auf registriertes Gerät -
6336 registriertes Gerät nicht bestätigt**

6337 Falls als Nachweis einer Geräteregistrierung eine DeviceID (deviceIdentifier und
6338 deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status ==
6339 'pending'), MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer
6340 Fehlermeldung abbrechen und die User Session beenden. [<=]

6341

6342 **A_28658 -Authorization Service - Prüfung des LOA Levels**

6343 Der ePA-Authorization Service MUSS ein vom sektoralen IDP erhaltenes ID-Token dahin
6344 gehend prüfen, ob

- 6345
- 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.

6349 In allen anderen Fällen MUSS der Zugang zur ePA verwehrt werden. [<=]

6350 Hinweis:

6351 Die Information, ob die Nutzereinwilligung zur Absenkung des Vertrauensniveau (nach
6352 A_23103) vorliegt, kann der Authorization Service aus dem übermittelten ID-Token
6353 extrahieren.

6354 IDPs, welche die ID-Token Version 2 liefern ,tragen die Information im claim
6355 "urn:telematik:auth:consent". Dort muss der Wert "loa-substantial" enthalten sein
6356 (gemSpec_IDP_FD - A_27593).

6357 IDPs, welche die ID-Token Version 1 liefern, tragen die Information im claim "amr". Dort
6358 muss der Wert "urn:telematik:auth:mEW" enthalten sein. (gemSpec_IDP_FD - A_23202-
6359 02).

6360

3.16.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B

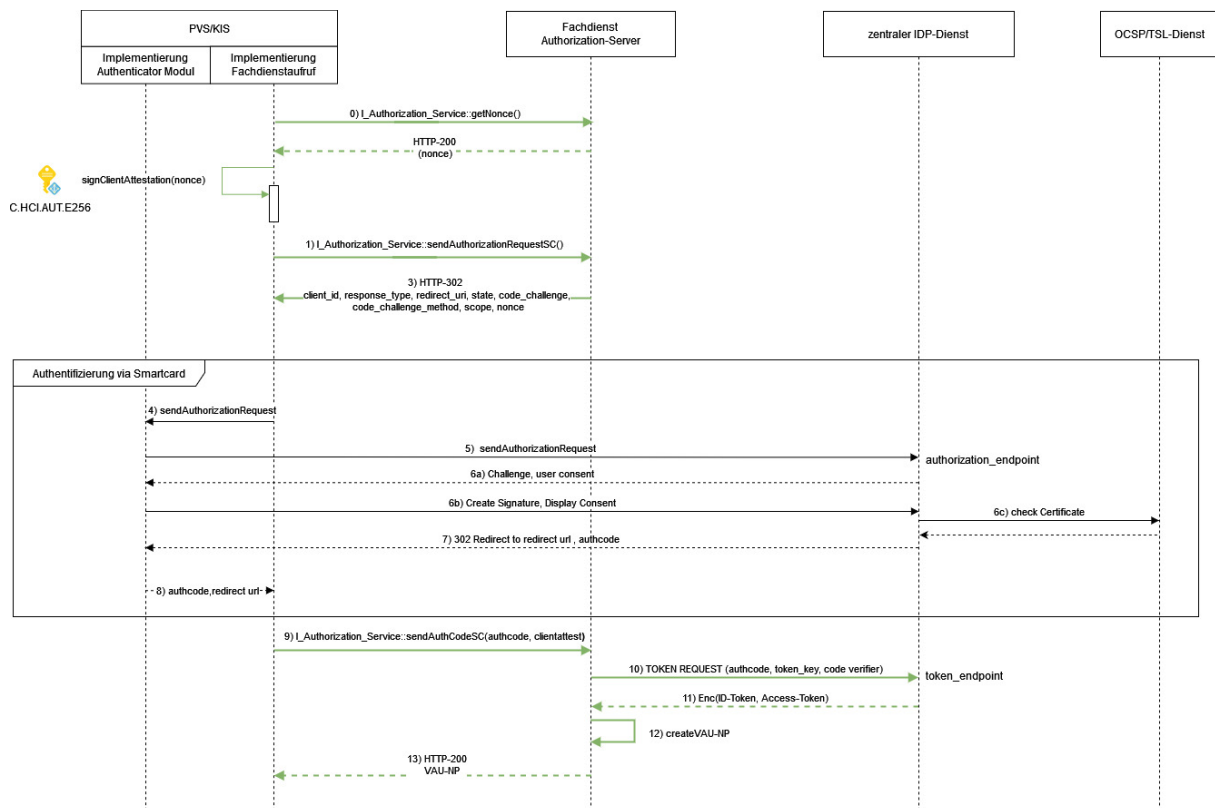


Abbildung 9: Ablauf der Authentifizierung einer LEI über den Smartcard IDP

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 Attestierung mindestens die folgenden Inhalte aufweist.

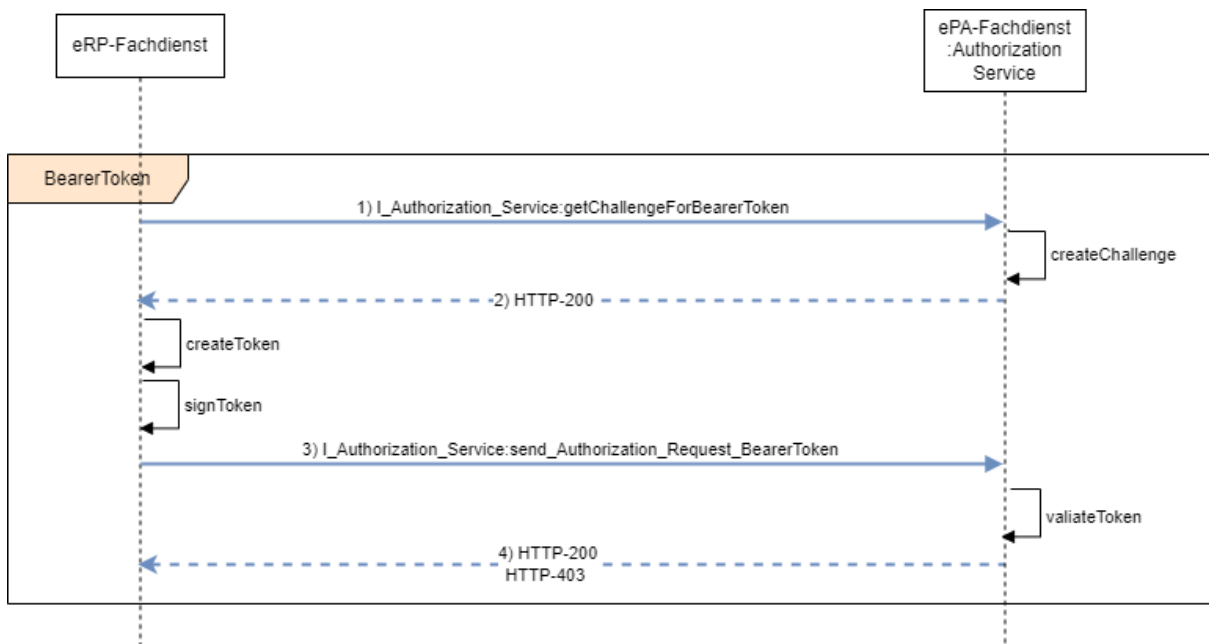
6384 **Tabelle 34 : Inhalte des übermittelten JWT der Client Attestierung**

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256" oder "PS256"	
	"x5c"	Signaturzertifikat C.HCI.AUT	
Payload			
	"nonce"	Nonce aus einer <code>getNonce</code> Operation	siehe [I_Authorization_Service]

6385 [**<=**]

6386 Für das Signaturzertifikat zu "x5c" (AUT-Zertifikat der SMC-B) gilt: Basiert der
 6387 öffentlichen Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert "ES256"
 6388 (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-256. Die
 6389 Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

6390 3.16.3 Anforderungen an den Authorization Service für die 6391 Authentisierung über JWT Bearer Token



6392

6393 **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			

Part	Claim Name	Claim	Anmerkung
	"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 Forschungsdatenzentrums	

6413 [**<=**]

6414 Die Signaturzertifikate zu "x5c" (AUT-Zertifikate) kommen aus der Komponenten-PKI der
 6415 TI. Basiert der öffentlichen Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert
 6416 "ES256" (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-
 6417 256. Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

6418

6419 **A_30391 -Authorization Service: JWT Bearer-Token eines Kostenträgers**

6420 Der Authorization Service MUSS sicherstellen, dass die Authentifizierung eines
 6421 Kostenträgers über die Schnittstelle `I_Authorization_Service` durch Verwendung eines
 6422 gültig signierten JWT Bearer Token mit den dargestellten Mindestinhalten erfolgt und die
 6423 Prüfung des Tokens gemäß A_30396-* erfolgreich ist.

6424 **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			

Part	Claim Name	Claim	Anmerkung
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"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.commonName aus dem Signaturzertifikat C.HCI.AUT entsprechen

[<=]

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. [<=]

6449 3.17 Anbindung Verzeichnisdienst FHIR-Directory

6450 **A_25176 -ePA-Aktensystem - Anbindung Verzeichnisdienst FHIR-Directory**

6451 Das ePA-Aktensystem MUSS bei der Suche des Versicherten nach Einträgen
6452 im Verzeichnisdienst FHIR-Directory und bei der initialen Anlage einer Akte den
6453 Anwendungsfall "AF_10219* - Versicherter sucht Einträge im FHIR-Directory" gemäß
6454 [gemSpec_VZD_FHIR_Directory] als Fachdienst unterstützen und dabei für die Client
6455 Anfrage von search-access_token die Operation getFHIRVZDtoken gemäß
6456 [I_Authorization_Service.yaml] bereitstellen. [$\leq$]

6457 3.18 Access Gateway

6458 Das Access Gateway ermöglicht den Versicherten bzw. deren berechtigten Vertretern den
6459 Zugang zum zugehörigen Aktensystem über das Internet. Auf der einen Seite dient es
6460 der Abschottung des ePA-Aktensystems in Richtung Internet, auf der anderen Seite
6461 regelt es den kontrollierten Zugriff der Versicherten auf das Aktensystem mit seinen
6462 funktionalen Komponenten.

6463 3.18.1 Paketfilter

6464 3.18.1.1 Funktion

6465 Der Paketfilter stellt die Anbindung des ePA-Aktensystems an das Internet her und
6466 gewährleistet die Abschottung des ePA-Aktensystems in Richtung Internet.

6467 **A_14017 -Access Gateway, Sicherung zum Transportnetz Internet durch Paketfilter**

6468 Das ePA-Aktensystem MUSS zum Transportnetz Internet durch einen Paketfilter (ACL)
6469 gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der
6470 Paketfilter der Komponente Access Gateway MUSS frei konfigurierbar sein auf der
6471 Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse,
6472 IP-Protokoll sowie Quell- und Zielport. [$\leq$]

6474 **A_14018 -Access Gateway, Platzierung des Paketfilters Internet**

6475 Der Paketfilter der Komponente Access Gateway, zum Schutz in Richtung Transportnetz
6476 Internet, DARF NICHT auf den anderen, zum Access Gateway gehörenden, physischen
6477 Komponenten implementiert werden. [$\leq$]

6478 **A_14019-03 -Access Gateway, Richtlinien für den Paketfilter zum Internet**

6479 Der Paketfilter der Komponente Access Gateway MUSS die Weiterleitung von IP-Paketen
6480 an der Schnittstelle zum Internet auf die folgenden Protokolle beschränken:

- 6481 1. HTTPS,
- 6482 2. OCSP-Zugriffe für das OCSP-Stapling (vgl. Hinweis nach A_14019-*), ggf.
6483 notwendige DNS Anfragen (und Antworten), und
- 6484 3. OCSP-Zugriffe auf OCSP-Responder der TI-PKI im Internet.

6485 Ein Verbindungsaufbau aus dem ePA-Aktensystem über das Access Gateway in Richtung
6486 Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 und
6487 3. [$\leq$]

6488 *Hinweis zu A_14019-*: Der Aktensystem-Anbieter muss für seine HTTPS-Schnittstelle ein*
6489 *TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-*

6490 Zertifikate also über einen aktuellen Webbrowser prüfbar ist, vgl. A_14776). Für dieses
6491 TLS-Zertifikat fragt das Access Gateway (die HTTPS-Schnittstelle ist Teil davon)
6492 regelmäßig für das OCSP-Stapling (vgl. [gemSpec_Krypt#A_24913-*) den OCSP-
6493 Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält
6494 das Access Gateway eine OCSP-Response. Diese wird nach A_19126 geprüft und
6495 anschließend von der HTTPS-Schnittstelle verwendet (vgl.
6496 <https://tools.ietf.org/html/rfc6066#section-8> und bspw.
6497 http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling).

6498 Um dies zu ermöglichen, muss der Paketfilter entsprechende stateful-Firewall-Regeln
6499 gemäß A_14019-* und A_19126-* definieren.

6500 **A_19126-02 -Access Gateway, OCSP-Status für das OCSP-Stapling**

6501 Der Paketfilter der Komponente Access Gateway MUSS bezüglich des OCSP-Stapling
6502 (vgl.A_24913-*) folgende Vorgaben umsetzen:

- 6503 1. Für das vom Aktensystem-Anbieter erworbene TLS-Zertifikat (vgl. Hinweis zu
6504 A_14019-01) MUSS die Komponente initial die IP-Adresse (ggf. die IP-Adressen)
6505 des entsprechenden OCSP-Responders ermitteln.
- 6506 2. Diese IP-Adresse(n) MÜSSEN gemäß A_14019-01 per stateful-Firewalling
6507 Verbindungen von der HTTPS-Schnittstelle an den OCSP-Responder erlaubt
6508 werden.
- 6509 3. Gemäß OCSP-Stapling (<https://tools.ietf.org/html/rfc6066#section-8>) MUSS die
6510 Komponente regelmäßig eine OCSP-Response vom entsprechenden OCSP-
6511 Responder beziehen (Die Regelmäßigkeit wird vom zertifikatsausgebenden TSP
6512 und der Gültigkeitsdauer dessen OCSP-Responses bestimmt).
- 6513 4. Die OCSP-Responses MÜSSEN von der Komponente geprüft werden
6514 (Signaturprüfung, CertID in der OCSP-Response passt zum angefragten
6515 Zertifikat). Falls eine der Prüfung ein nicht-positives Ergebnis liefert, so MUSS die
6516 erhaltene OCSP-Response verworfen werden.
- 6517 5. Sollte die letzte in der Komponente vorhandene OCSP-Response zeitlich nicht
6518 mehr gültig sein (bspw. der OCSP-Responder im Internet war länger nicht
6519 erreichbar), so MUSS diese OCSP-Response verworfen werden und ein von einem
6520 Klienten (ePA FdV) initiiertes TLS-Verbindungsaufbau der HTTPS-Schnittstelle
6521 ohne OCSP-Stapling durchgeführt werden.

6522 [$\leq$]

6523 **A_14776 -Access Gateway, Richtlinien zum TLS-Verbindungsaufbau**

6524 Die Komponente Access Gateway MUSS sich beim TLS-Verbindungsaufbau gegenüber
6525 dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB
6526 Forum] authentisieren. Das Zertifikat MUSS an die Schnittstelle der Proxy-Komponente
6527 gebunden werden.[$\leq$]

6528 **3.18.1.2 Redundanz**

6529 Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf#3.18.1.3]. Die
6530 Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Access
6531 Gateways.

6532 Die Auswahl der Access Gateways wird durch das ePA-Frontend des Versicherten aus
6533 einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des Access
6534 Gateways kann der Anbieter des ePA-Aktensystems durch die Konfiguration und
6535 Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn

6536 jeder Versicherte mit existierendem Konto beim Anbieter des ePA-Aktensystems oder
6537 dessen berechtigter Vertreter die Möglichkeit zum Verbindungsaufbau hat.

6538 Eine hardwaretechnische Hochverfügbarkeit der einzelnen Access Gateways ist über
6539 grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht
6540 dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische
6541 Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern
6542 einzusetzen, so dass jedes einzelne Access Gateway im Ergebnis eine höhere
6543 Verfügbarkeit oder Leistungsfähigkeit besitzt.

6544 **A_14026 -Access Gateway, Redundanz der Paketfilter im Access Gateway**

6545 Die Komponente Access Gateway MUSS sicherstellen, dass bei Ausfall eines von
6546 mehreren Paketfiltern die verbleibenden Paketfilter in dem-selben Standort den
6547 Datenverkehr aller Mandanten des ausgefallenen Paketfilters zusätzlich übernehmen
6548 können.[<=]

6549 **3.18.1.3 Konfiguration**

6550 **A_14030 -Access Gateway, Verhalten des Access Gateways bei Vollauslastung**

6551 Die Komponente Access Gateway MUSS den Paketfilter Internet so konfigurieren, dass
6552 bei Vollauslastung der Systemressourcen im ePA-Aktensystem keine weiteren
6553 Verbindungen angenommen werden.[<=]

6554 Durch die Zurückweisung von Verbindungen wird sichergestellt, dass das ePA-Frontend
6555 des Versicherten einen Verbindungsaufbau mit einem anderen Access Gateway des
6556 jeweiligen ePA-Aktensystems versucht, bei dem die erforderlichen Ressourcen zur
6557 Verfügung stehen.

6558 **3.18.1.4 Adressierung**

6559 *3.18.1.4.1 Access Gateway zum Transportnetz Internet*

6560 **A_14031 -Access Gateway, IPv4-Adressierung der Internetschnittstellen des**
6561 **Access Gateways**

6562 Der Anbieter des ePA-Aktensystems MUSS jedem Access Gateway genau eine öffentliche
6563 IPv4-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum
6564 Internet konfiguriert werden. Die öffentlichen IP-Adressen des Access Gateways MÜSSEN
6565 vom Anbieter des ePA-Aktensystems zur Verfügung gestellt werden.[<=]

6566 **A_14032 -Access Gateway, IPv6-Adressierung der Internetschnittstellen des**
6567 **Access Gateways**

6568 Der Anbieter des ePA-Aktensystems SOLL jedem Access Gateway eine IPv6-Adresse
6569 zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert
6570 werden. Die öffentliche IPv6-Adresse MUSS vom Anbieter des Access Gateways zur
6571 Verfügung gestellt werden.[<=]

6572 *3.18.1.4.2 ePA-Aktensystem zum Zentralen Netz*

6573 Die Adressen des ePA-Aktensystems am Übergang zur TI werden vom Anbieter des
6574 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. [$\leq$]

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: [].

6623 2. Sollte es keinen optionalen DoS-Schutzmechanismus gemäß A_22582-* geben, so
 6624 fallen die DoS-* Attribute in der o. g. Datenstruktur weg (sind nicht existent).

6625 3. Wenn es einen FQDN gibt, bei dem jede erfolgreiche Namensauflösung dieser
 6626 FQDN auf eine korrekte IP-Adresse verweist, dann KANN das "ipaddr"-Key-Value-
 6627 Paar durch ein Key-Value-Paar
 6628 "fqdn": "FQDN-der-nach-Namensauflösung-die-korrekte-IP-Adresse-
 6629 ergibt"
 6630 ersetzt werden. Das "ipaddr"-Feld fällt, dann also weg. (vgl. Hinweis 2 unter
 6631 A_21890-*).

6632 4. Die einzelnen Felder des Arrays sind associative array (oder auch maps oder
 6633 dictionaries genannt). Diese KÖNNEN neben "name" und "port" beliebige vom AS
 6634 definierbare, weitere key-value-Paare enthalten. Der Eintrag "port" gibt an, an
 6635 welchem öffentlich erreichbaren TCP-Port des Access Gateway die Sensordaten
 6636 des entsprechenden Sensors abrufbar sind (gestreamt werden).

6637 [**<=**]

6638 *Hinweise zu A_21890-*:*

6639 *(1) Die semistatische JSON-Datei, welche ein Client unter dem Pfad „/tracingpoints“*
 6640 *erhalten kann, ist eine einfache Form von Service-Discovery. Damit kann ein Client*
 6641 *(Fehlersuchende(r)) erfahren, welche Tracing-Quellen es aktuell im AS gibt i. S. v.*
 6642 *welche Tracing-Quellen ein Client zur Fehlersuche aktuell verwenden kann.*

6643 *(2) Es gibt Konstellationen bei denen ein FQDN auf mehrere verschiedene IP-Adresse*
 6644 *aufgelöst wird. Beispielweise als einfache Form des Load-Balancings gibt der DNS-Server*
 6645 *per Round-Robin aus einer Liste von IP-Adresse bei jeder Anfrage eine in der Liste als*
 6646 *nächstes stehende IP-Adresse als Antwort und iteriert kontinuierlich über die Liste. Wenn*
 6647 *jede erfolgreiche Antwort des DNS-Servers auf eine FQDN eine IP-Adresse als Ergebnis*
 6648 *liefert, die im Sinne von A_21890-* eine korrekte IP-Adresse ist (wo also Sensor-Daten*
 6649 *auch abrufbar sind), so kann in der Datenstruktur von A_21890-* "fqdn" anstatt "ipaddr"*
 6650 *aufgeführt werden.*

6651 **A_22582 -Tracing in Nichtproduktivumgebungen, DoS-Schutz**

6652 Die Komponente Access Gateway KANN Sicherheitsmechanismen bereitstellen und
 6653 aktivieren, die es genau in Nichtproduktiv-umgebungen ermöglichen, temporär,
 6654 automatisiert und nur nach erfolgreicher Authentifizierung die TCP-Ports für das
 6655 Streaming der Sensorpunkte für Clients nach A_21890-* freizuschalten. [**<=**]

6656 *Hinweis zu A_22582-*: In den Nichtproduktivumgebungen darf es keine Echtdaten*
 6657 *geben. Es dürfen sich dort nur Daten befinden, deren Schutzbedarf bezüglich*
 6658 *Vertraulichkeit niedrig ist. Der optionale Schutzmechanismus nach A_22582-* braucht*
 6659 *nur einen einfachen DoS-Schutz leisten gegen einen Angreifer mit niedrigen*
 6660 *Angriffspotential. Der Anbieter ist, sofern er einen solchen Mechanismus einsetzen*
 6661 *möchte, frei, dafür den Mechanismus selbst zu wählen. Er wählt dann bei "DoS-*
 6662 *protection-type" (vgl. A_21890-*) einen selbstdefinierten (möglichst sprechenden)*
 6663 *Namen.*

6664 Beispiele für Umsetzungsmöglichkeiten:

- 6665 1. Es gibt im Access Gateway eine geheime URL (bspw.
 6666 /tracing/964b059de83d20581f43dd1b867d740c). Ein Client kennt das Geheimnis
 6667 und ruft diese URL auf. Daraufhin wird im Access Gateway für die IP-Adresse des
 6668 Clients die Tracing-Quelle im Access Gateway frei geschaltet (TCP-Port 8000, ...).
- 6669 2. Die gematik stellt eine Beispielimplementierung zur Verfügung. Dort gibt es einen
 6670 UDP-Server (Access Gateway) und einen UDP-Client (Fehlersuchende), die beide
 6671 ein gemeinsames HMAC-Geheimnis teilen. Wenn der Client die aktuelle Zeit und

6672 dessen IP-Adresse per HMAC authentisiert dem UDP-Server sendet, so schaltet
6673 der UDP-Server nach erfolgreicher Prüfung des HMACs den entsprechenden TCP-
6674 Port für die authentifizierte IP-Adresse des Clients frei.

6675 3. Auf dem Access Gateway läuft ein SSH-Daemon. Der öffentliche
6676 Authentisierungsschlüssel eines Clients ist dort als gültiger Nutzer konfiguriert
6677 (Login-Shell: /bin/false). Die Tracing-Quellen im Access Gateway sind so
6678 konfiguriert, dass sie nur mittels authentisierten SSH-Port-Forwarding
6679 (<https://www.ssh.com/academy/ssh/tunneling/example>) erreichbar sind.

6680 3.18.4 Übergreifende Festlegungen

6681 **A_14249 -Komponente Access Gateway - Separierung der Schnittstellen für** 6682 **verschiedene Umgebungen**

6683 Die Komponente Access Gateway MUSS die Bereitstellung von Schnittstellen für die
6684 Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen
6685 Umgebungen der TI (RU/TU, PU) sicherstellen und voneinander separieren. [<=]

6686 **A_14034 -Access Gateway, Übergang des ePA-Aktensystems zur TI**

6687 Die Komponente Access Gateway MUSS sicherstellen, dass der Zugriff auf Dienste der TI
6688 ausschließlich über einen Sicheren Zentralen Zugangspunkt (SZZP) erfolgt. [<=]

6689 **A_14036 -Access Gateway, Synchronisierung der Komponenten mit den** 6690 **Stratum-1-NTP-Servern der TI**

6691 Die Komponente Access Gateway MUSS alle Komponenten seines Access Gateways mit
6692 den Stratum-1-NTP-Servern der TI synchronisieren. [<=]

6693 **A_13879 -Access Gateway, Serverseitige Authentisierung**

6694 Die Komponente Access Gateway MUSS sich gegenüber dem ePA-Frontend des
6695 Versicherten beim Aufbau der TLS-Session durch sein ExtendedValidation-
6696 Zertifikat authentisieren. Die Beschaffung des Zertifikats erfolgt durch den Anbieter über
6697 eine öffentliche CA. [<=]

6698 **A_14033 -Access Gateway, TLS Verschlüsselung**

6699 Die Komponente Access Gateway MUSS sicherstellen, dass jede Kommunikation mit dem
6700 ePA-Frontend des Versicherten TLS verschlüsselt erfolgt. [<=]

6701 Die Verwendung der SoapAction ermöglicht einer Reverse-Proxy-Komponente innerhalb
6702 des Access Gateways, die Nachrichten zu verarbeiten, ohne die http-Payload zu
6703 untersuchen.

6704 **A_13876 -Access Gateway, Kein direkter Zugriff auf Dienste der zentralen TI-** 6705 **Plattform**

6706 Die Komponente Access Gateway MUSS einen direkten Zugriff aus dem Internet auf
6707 Dienste der zentralen TI-Plattform verhindern. [<=]

6708 **A_14016 -Access Gateway , Schutz vor Angriffen aus dem Internet**

6709 Die Komponente Access Gateway MUSS für alle vom Internet erreichbaren Schnittstellen
6710 Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere
6711 Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS
6712 Lösungen verhindert werden. [<=]

6713 **A_15196 -Access Gateway, Schutz vor volumetrischen DoS-Angriffen**

6714 Die Komponente Access Gateway MUSS bei Beauftragung eines qualifizierten
6715 Dienstleisters zum Schutz vor volumetrischen DoS-Angriffen Kriterien des BSI zur
6716 Auswahl qualifizierter Dienstleister umsetzen. [<=]

6717 Als Maßnahme gegen volumetrische Denial-of-Service-Angriffe wird die Verwendung von
6718 DNS- oder BGP-Routing-Diensten empfohlen. Hinweise des BSI:

6719 [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos_node.html)
6720 [und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos_node.html).

6721 3.19 Data Submission Service

6722 Die Daten der elektronischen Patientenakten sollen nach § 363 Absatz 1 SGB V für die in
6723 § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszwecke zugänglich gemacht und
6724 hierfür in pseudonymisierter Form automatisiert von den ePA-Aktensystemen an das
6725 Forschungsdatenzentrum Gesundheit (FDZ) nach § 303d SGB V übermittelt werden,
6726 sofern Versicherte dem nicht widersprochen haben.

6727 Neben dem FDZ und den ePA-Aktensystemen ist die Vertrauensstelle (VST) nach § 303c
6728 SGB V im Prozess involviert. Deren Aufgabe ist es, die von den ePA-Aktensystemen
6729 erhaltenen Lieferpseudonyme in periodenübergreifende Pseudonyme umzuwandeln und
6730 diese an das FDZ zu übermitteln.

6731 Der Data Submission Service im Aktensystem übernimmt in der Übermittlung der
6732 pseudonymisierten medizinischen Daten folgende Aufgaben:

- 6733 • Erstellung der Lieferpseudonyme (auf Basis der KVN-R) und der Arbeitsnummern
- 6734 • Registrierung der Arbeitsnummer mit dem zugehörigen Lieferpseudonym bei der
6735 Vertrauensstelle
- 6736 • Pseudonymisierung der medizinischen Daten
- 6737 • Verknüpfung der pseudonymisierten medizinischen Daten mit der Arbeitsnummer
- 6738 • Übermittlung der pseudonymisierten medizinischen Daten und der zugehörigen
6739 Arbeitsnummern an das Forschungsdatenzentrum Gesundheit

6740 Die Übermittlung der Daten erfolgt blockweise. D.h. es wird ein Paket von
6741 pseudonymisierten medizinischen Daten mit zugehörigen Arbeitsnummern aus
6742 verschiedenen Aktenkonten zusammengestellt (Datenpaket FDZ) und alle für dieses
6743 Paket benötigten Arbeitsnummern und Lieferpseudonyme mit einem Mal bei der VST
6744 registriert (Datenpaket VST). Die Datenpakete haben eine anbieterübergreifend
6745 eindeutige SubmissionID und die SubmissionID zusammengehöriger Datenpakete VST
6746 und FDZ ist identisch.

6747 Für die Übermittlung wird zwischen Aktensystem und VST, sowie Aktensystem und FDZ
6748 jeweils ein beidseitig authentisierter VAU-Kanal aufgebaut, auf dem sich die Dienste VST
6749 und FDZ mit einer Identität ID.FD.AUT mit ihren entsprechenden Rollen authentisieren.

6750 Der Versicherte kann mit Hilfe seines ePA-FdVs oder über die Ombudsstelle des
6751 Kostenträgers der Übermittlung seiner pseudonymisierten medizinischen Daten an das
6752 FDZ widersprechen oder die möglichen Sekundärnutzungszwecke seiner übermittelten
6753 pseudonymisierten medizinischen Daten im FDZ einschränken. Dies erfolgt über das
6754 Consent Decision Management im Aktensystem.

6755 3.19.1 Erstellung von Arbeitsnummern und Lieferpseudonymen

6756 Der Data Submission Service erzeugt eindeutige Arbeitsnummern und Lieferpseudonyme,
6757 um die pseudonymisierten medizinischen Daten in der Übermittlung an das FDZ eindeutig
6758 zuordnen zu können.

6759 A_26211 -Data Submission Service - Erstellung des Lieferpseudonyms

6760 Der Data Submission Service MUSS das Lieferpseudonym des Versicherten gemäß
6761 [I_VST] unter Verwendung der KVN-R des Versicherten erstellen.[<=]

6762 **A_26409 -Data Submission Service - keine Erstellung von LP für**
6763 **Validierungsaktenkonten**

6764 Der Data Submission Service DARF KEINE Lieferpseudonyme für KVNRn
6765 von Validierungsaktenkonten erstellen.[<=]

6766 **A_26212 -Data Submission Service - Erstellung der Arbeitsnummer**

6767 Der Data Submission Service MUSS für die Arbeitsnummer einen Zufallswert mit einer
6768 Mindestentropie von 120 Bit erzeugen und die Kodierung aus [I_VST] verwenden.[<=]

6769 **A_26410 -Data Submission Service - keine Erstellung von AN für**
6770 **Validierungsaktenkonten**

6771 Der Data Submission Service DARF KEINE Arbeitsnummern für Daten
6772 aus Validierungsaktenkonten erstellen.[<=]

6773 **A_26255 -Data Submission Service - Verwendungsdauer von**
6774 **Lieferpseudonymen und Arbeitsnummern**

6775 Der Data Submission Service MUSS für jedes in einem Datenpaket FDZ übermittelte
6776 pseudonymisierte medizinische Datum zu einer KVNR eine neue Arbeitsnummer und ein
6777 neues Lieferpseudonym generieren.[<=]

6778 **A_26256 -Data Submission Service - Registrierung von Arbeitsnummern**

6779 Der Data Submission Service MUSS jede Arbeitsnummer zusammen mit dem
6780 zugehörigen Lieferpseudonym in das entsprechende Datenpaket VST aufnehmen und an
6781 die Vertrauensstelle übermitteln.[<=]

6782 **3.19.2 Auswahl von medizinischen Daten**

6783 Der Data Submission Service muss bestimmte neue und geänderte FHIR-Ressourcen an
6784 den FDZ übertragen. Dies betrifft im ersten Schritt die Medikationsdaten aus der E-
6785 Medikationsliste und wird subsequent weiter ausgebaut.

6786 Der Medication Service, als Quelle der Medikationsdaten zur Übertragung an den FDZ,
6787 erlaubt flexible, datenbasierte Operationen auf einzelnen FHIR-Ressourcen. Dies erfordert
6788 entsprechende Implementierung um effizient und zuverlässig die neuen und geänderten
6789 Ressourcen identifizieren können um daraus die Auswahl für die zu übertragende FHIR-
6790 Ressourcen treffen zu können.

6791 **A_26296 -Data Submission Service - Übertragung neuer und geänderter FHIR-**
6792 **Ressourcen**

6793 Der Data Submission Service MUSS neue und geänderte FHIR-Ressourcen identifizieren
6794 können und daraus die Auswahl für die Übermittlung der Daten an FDZ treffen
6795 können.[<=]

6796 **A_26297 -Data Submission Service - Einschränkung der FHIR-Ressourcen nach**
6797 **Änderungsdatum**

6798 Der Data Submission Service MUSS den Zeitpunkt der letzten Übermittlung
6799 (lastSubmissionTimestamp) merken und in nachfolgenden Übermittlungen nur die
6800 Ressourcen, die sich seit diesem Zeitpunkt geändert haben, berücksichtigen. Hierfür ist
6801 das FHIR-Element meta.lastUpdated in der jeweiligen FHIR-Ressource zu
6802 verwenden.[<=]

6803 *Hinweis: Ressourcen, die im Rahmen eines Anbieterwechsels in ein Aktenkonto*
6804 *übernommen werden, sind nicht erneut zu übermitteln.*

6805 **A_26298 -Data Submission Service - FHIR-Ressourcen zur Übermittlung an FDZ**

6806 Der Data Submission Service MUSS die FHIR-Ressourcen gemäß der Tabelle "Auswahl
6807 der zu übertragenden FHIR-Ressourcen" an FDZ übertragen, dabei sind die Filter-
6808 Bedingungen (Spalte 'Filter Expression') und zu inkludierende referenzierte Ressourcen

zu berücksichtigen (Spalte 'Include' sowie Tabelle "Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen").[<=]

6811

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

6813

Tabelle 39: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen

Ressourcentyp/Profil	Anmerkung
Medication \${epa-medication}/epa-medication	Referenziert durch MedicationRequest, MedicationDispense

6815

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. [<=]

- 6875 **A_26215 -Data Submission Service - Übermittlung Datenpaket VST**
6876 Der Data Submission Service MUSS das Datenpaket VST gemäß [I_VST] an die
6877 Vertrauensstelle übermitteln.[<=]
- 6878 **A_26407 -Data Submission Service - keine Übermittlung von Daten aus**
6879 **Validierungsaktenkonten**
6880 Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem.
6881 Kapitel 2.4) an das Forschungsdatenzentrum übermitteln.[<=]
- 6882 **A_26216 -Data Submission Service - Realisierung der Schnittstelle**
6883 **I_Data_Submission_Service**
6884 Der Data Submission Service MUSS die Operationen der Schnittstelle
6885 I_Data_Submission_Service gemäß [I_Data_Submission_Service] umsetzen.[<=]
- 6886 **A_26217 -Data Submission Service - Verbindung zur Vertrauensstelle**
6887 Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des
6888 Datenpakets VST ausschließlich über einen VAU-Kanal erfolgt in dem sich die
6889 Vertrauensstelle über ein Zertifikat C.FD.AUT mit professionOID gleich oid_epa_vst
6890 authentisiert hat.[<=]
- 6891 **A_26218 -Data Submission Service - Verbindung zum Forschungsdatenzentrum**
6892 **Gesundheit**
6893 Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des
6894 Datenpakets FDZ ausschließlich über einen VAU-Kanal erfolgt in dem sich das
6895 Forschungsdatenzentrum Gesundheit über ein Zertifikat C.FD.AUT mit professionOID
6896 gleich oid_epa_fdz authentisiert hat.[<=]
- 6897 **A_26299 -Data Submission Service - Wechsel des Verschlüsselungsschlüssels**
6898 **für Datenpakete**
6899 Falls die Datenpakete VST und FDZ außerhalb der VAU im System des
6900 Aktensystembetreibers gespeichert werden, MUSS der Data Submission Service
6901 sicherstellen, dass ein Schlüssel für die Verschlüsselung der Datenpakete VST bzw. FDZ
6902 maximal 4 Wochen genutzt werden kann und danach ein neuer
6903 Verschlüsselungsschlüssel mittels der Regel hsm-r8 mit Hilfe eines geänderten
6904 Ableitungsvektors abgeleitet wird.[<=]
- 6905 **A_26312 -Data Submission Service - Timeout in der Übermittlung**
6906 Der Data Submission Service MUSS die Übermittlung der Pakete VST und FDZ erneut
6907 starten, wenn das Datenpaket FDZ nicht innerhalb von 30 Minuten nach erfolgreicher
6908 Übermittlung des Datenpakets VST abgerufen wird.[<=]
- 6909 **A_26313 -Data Submission Service - Konfiguration der Intervalle und**
6910 **maximalen Größe eines Datenpakets**
6911 Der Data Submission Service MUSS folgende Parameter konfigurierbar gestalten:
6912
 - das Intervall in dem Datenpakete VST und FDZ übermittelt werden
 - eine maximale Größe eines Datenpakets FDZ bei deren Erreichen die Datenpakete
6914 übermittelt werden
6915 [<=]
- 6916 **A_26244-01 -Data Submission Service - Löschen von Datenpaketen nach**
6917 **Übermittlung**
6918 Der Data Submission Service MUSS nach erfolgreicher Übermittlung des Datenpakets
6919 FDZ an das Forschungsdatenzentrum Gesundheit das übermittelte Datenpaket FDZ und
6920 das zugehörige Datenpaket VST nach Ablauf eine Wartefrist von 15 Minuten lokal
6921 löschen.[<=]

6922 *Hinweis: Das ePA-Aktensystem kann von einer erfolgreichen Übermittlung im Sinne der*
6923 *Anforderung ausgehen, wenn die letzten Daten des Datenpakets FDZ gesendet wurden.*
6924 *Die Wartefrist soll es dem Forschungsdatenzentrum ermöglichen eine erfolglose*
6925 *Übermittlung erneut anzustoßen.*

6926 **A_26245-01 -Data Submission Service - Löschen von Datenpaketen bei Nicht-**
6927 **Übermittlung**

6928 Der Data Submission Service MUSS das Datenpaket FDZ und das zugehörige Datenpaket
6929 VST lokal löschen, wenn das Datenpaket FDZ länger als 72 Stunden nicht an das
6930 Forschungsdatenzentrum Gesundheit übermittelt werden konnte. Die enthaltenen
6931 Widersprüche gegen die Übermittlung von Daten zur Sekundärnutzung durch das FDZ
6932 und zu Sekundärnutzungszwecken MÜSSEN in die aktuell in Erstellung befindlichen
6933 Datenpakete VST und FDZ übernommen werden.[<=]

6934 *Hinweis: Wenn Widersprüche in ein neues Datenpaket übernommen werden, muss für*
6935 *jeden der Widersprüche eine neue Arbeitsnummer (AN) und ein Lieferpseudonym (LP)*
6936 *erstellt werden, da die bisherigen AN und LP im Kontext des zu löschenden Paketes*
6937 *stehen.*

6938 **A_26246 -Data Submission Service - Aufnahme von Widersprüchen**

6939 Der Data Submission Service MUSS Widersprüche gegen die Freigabe von Daten zur
6940 Sekundärnutzung durch das FDZ oder Änderungen zu Sekundärnutzungszwecken, aus
6941 dem Consent Decision Management, in die aktuell in Erstellung befindlichen Datenpakete
6942 VST und FDZ übernehmen. Es MUSS sichergestellt werden, dass in einem Datenpaket
6943 FDZ für eine KVNR immer nur die zuletzt erklärten Widersprüche gegen die Übermittlung
6944 von Daten zur Sekundärnutzung durch das FDZ bzw. zu Sekundärnutzungszwecken
6945 enthalten sind.[<=]

6946 *Hinweis: Sollte während der Erstellung eines Datenpakets FDZ mehrfach die*
6947 *Widersprüche für eine KVNR geändert werden, wird immer nur der letzte Stand*
6948 *übermittelt.*

6949 **A_26307 -Data Submission Service - Durchsetzung von Widersprüchen**

6950 Falls für ein Aktenkonto ein Widerspruch gegen die Übermittlung an das FDZ eingestellt
6951 wird, MUSS der Data Submission Service sicherstellen, dass in allen zukünftig zu
6952 übermittelnden Datenpaketen VST und FDZ außer den Daten für den Widerspruch keine
6953 Daten für dieses Aktenkonto enthalten sind.
6954 [<=]

6955 *Hinweis zu A_26307: Zum Zeitpunkt des Eingangs des Widerspruchs im Aktensystems*
6956 *bereits in der Übermittlung befindliche Datenpakete sind von der Anforderung*
6957 *ausgeschlossen. Betroffen sind jedoch auch die aktuell in Erstellung befindlichen*
6958 *Datenpakete VST und FDZ, bei denen die Übermittlung an die VST bzw. das FDZ noch*
6959 *nicht begonnen hat.*

6960 **3.20 Push Notification Management**

6961 Nutzer von Anwendungen für Versicherte (ePA-FdV) können mittels Push Notifications
6962 direkt über Ereignisse in bestimmten Fachdiensten der TI oder des Kostenträgers auf
6963 ihren Endgeräten informiert werden. Diese Notifications erreichen einen Nutzer auch
6964 außerhalb aktiver Anmeldungen in diesen Fachdiensten. Die Ereignisse von Interesse zur
6965 Benachrichtigung des Nutzers sind dabei individuell abonnierbar.

6966 Der Versand einer Push Notification erfolgt stets durch die einzelnen Fachdienste für
6967 Ereignisse ihrer Domäne. Die Übertragung in das Endgerät des Nutzers unter Einbindung
6968 der plattformspezifischen, externen Push-Dienste und betreiberspezifischen Push-

6969 Gateways wird für alle beteiligten Fachdienste gemeinsam durch ein Push Notification
6970 System realisiert. Dieses anwendungsübergreifende System und seine Komponenten für
6971 Push Notifications im Gesundheitswesen sind in [gemF_PushNotification] und
6972 [PushNotificationConcept] detailliert beschrieben.

6973 Dort sind auch die normativen Vorgaben für unterstützende Anwendungen und
6974 Fachdienste in Bezug auf Registrierung von Applikationen und Ereignissen für Push
6975 Nachrichten, Schnittstellen, sicherheitstechnische Anforderungen und notwendige
6976 Artefakte für einen interoperablen Betrieb formuliert.

6977 **3.20.1 Push Notification Management des ePA-Aktensystems**

6978 Das Push Notification Management des ePA-Aktensystems ist als ein spezifischer
6979 Fachdienst in dieses übergreifende System eingebunden und bedient die in
6980 [gemF_PushNotification] geforderten und in [PushNotificationConcept] beschriebenen
6981 Schnittstellen und Verfahren.

6982 Push Notifications der ePA können ausschließlich durch Versicherte für Ereignisse ihres
6983 eigenen Aktenkontos genutzt werden. Der Erhalt von Benachrichtigungen aus dem
6984 Aktenkonto eines vertretenen Versicherten wird nicht unterstützt.

6985 Der Nutzung des Push Notification Managements der ePA kann nicht widersprochen
6986 werden. Dieser Dienst gehört nicht zu den widerspruchsfähigen Funktionen der ePA.
6987 Versicherte, die keine Benachrichtigungen der ePA erhalten möchten, können die
6988 Benachrichtigungen durch Abwahl der Benachrichtigungskanäle oder auch generell durch
6989 den Verzicht des ePA-FdV auf eine Registrierung für Push Notifications unterbinden.

6990 Schnittstellen, die das Push Notification Management der ePA zur Nutzung durch Clients
6991 (ePA-FdV) anbietet, sind um ePA-spezifische Verfahren und Anforderungen ergänzt und
6992 als OpenApi gemäß [I_Push_Notification_Management] verfügbar.

6993 **A_27637 -Push Notification Management - Realisierung der Schnittstelle** 6994 **I_Push_Notification_Management**

6995 Das Push Notification Management MUSS die Operationen der Schnittstelle
6996 I_Push_Notification_Management gemäß [I_Push_Notification_Management]
6997 umsetzen.[<=]

6998 **3.20.2 Registrierung eines ePA-FdV als Pusher**

6999 (siehe auch: [gemF_PushNotification]#Kapitel "Pusher registrieren")

7000 Ein Versicherter kann registrierte Geräte (im Sinne des Device Managements gemäß 3.11.1-
7001 Device Management) zur Nutzung seiner aktivierten elektronischen Patientenakte auch
7002 für den Erhalt von Push Nachrichten nutzen, sofern das übergreifende Push Notification
7003 System die technologische Infrastruktur für Benachrichtigungen an den Geräte-, bzw.
7004 Betriebssystemtyp des Versichertengeräts unterstützt. Dazu kann die ePA-FdV-
7005 Anwendung jedes dieser Geräte als ePA-FdV Instanz, bzw. 'Pusher', im eigenen
7006 Aktenkonto des Versicherten registriert werden.

7007 Die ePA-FdV Instanz Registrierung eines Gerätes als Pusher erfolgt immer durch und für
7008 das auf diesem Gerät installierte ePA-FdV und unter Nutzung der Schnittstelle
7009 [I_Push_Notification_Management]. Über diese Schnittstelle werden existierende
7010 Registrierungen auch aktualisiert und wieder entfernt.

7011 Die Daten der Registrierungen, inklusive des kryptographischen Materials der
7012 Schlüsselableitungen und der Auswahl der Benachrichtigungskanäle, sind Bestandteil des
7013 Aktenkontos und werden dort gespeichert. Pro registriertem Gerät kann jeweils nur eine

7014 ePA-FdV Instanz im Aktenkonto hinterlegt sein und eine Registrierung gilt immer nur für
7015 genau eine bestimmte ePA-FdV Instanz. Eine ePA-FdV Instanz Registrierung ist daher
7016 fest an eine Device Registration gebunden.

7017 **A_27638 -Push Notification Management- Speicherung der Daten**

7018 Das Push Notification Management MUSS alle Daten des Dienstes für einen Versicherten
7019 im SecureDataStorage des Aktenkontos des Versicherten speichern.[<=]

7020 **A_27640 -Push Notification Management - automatisches Löschen der**
7021 **Registrierung einer ePA-FdV Instanz**

7022 Das Push Notification Management MUSS sicherstellen, dass eine existierende
7023 Registrierung einer ePA-FdV Instanz und die dazugehörigen Daten vollständig und
7024 automatisch gelöscht werden, wenn die Device Registration des assoziierten Geräts im
7025 Device Management des Aktensystems gelöscht wird.[<=]

7026 **A_27639 -Push Notification Management - eindeutiger pushKey**

7027 Das Push Notification Management MUSS sicherstellen, dass der `pushKey` einer
7028 Registrierung einer ePA-FdV Instanz eindeutig ist und es keine zwei oder mehr
7029 Registrierungen mit gleichem `pushKey` gibt.[<=]

7030 Bei jedem Versand einer Push Nachricht an das Push Gateway kann dieses in den
7031 Rückgabewerten der Push Operation einen Eintrag oder eine Liste veralteter, bzw.
7032 ungültiger `pushKeys` melden. Eine weitere Nutzung solcher Registrierungen, bzw.
7033 `pushKeys`, soll unterbleiben. Die assoziierten Registrierungen von ePA-FdV-Instanzen
7034 werden daher aus dem Aktenkonto entfernt.

7035 **A_27682 -Push Notification Management - Entfernen ungültiger pushKeys**

7036 Das Push Notification Management MUSS Registrierungen von ePA-FdV-Instanzen
7037 löschen, wenn `pushKeys` dieser Registrierungen durch das Push Gateway als ungültig
7038 gemeldet werden.[<=]

7039 *Hinweis: Es werden nur Registrierungen aus dem versendenden Aktenkonto entfernt.*
7040 *Ebventuelle Rückmeldungen des Push Gateways zu `pushKeys`, die nicht oder nicht mehr*
7041 *mit dem versendenden Aktenkonto verbunden sind, werden ignoriert.*

7042 **3.20.3 Push Notification Channels**

7043 (siehe auch: [gemF_PushNotification]#Kapitel "Channel/ Trigger Konfiguration")

7044 Das ePA-Aktensystem bietet eine Auswahl an Channels zu Ereignissen, über deren
7045 Aktivität ein Versicherter durch Push-Benachrichtigungen informiert werden kann. Der
7046 jeweilige Nachrichteninhalt beschreibt dabei in Kurzform das auslösende Ereignis.

7047 Die Grundeinstellung für den Versand von Push-Benachrichtigungen an neu erstellten
7048 Registrierungen für ePA-FdV-Instanzen lautet für jeden Channel zunächst 'not_set'. Das
7049 bedeutet, der Channel wurde bisher nicht konfiguriert und es werden keine
7050 Benachrichtigung für diesen Kanal versendet.

7051 Ein Versicherter kann diese Grundeinstellung individuell für jede seiner ePA-FdV-
7052 Instanzen jederzeit ändern und die Benachrichtigung pro Channel aktivieren ('enabled' -
7053 Benachrichtigungen für diesen Kanal), bzw. auch wieder deaktivieren.

7054 Die Verwaltung der individuellen Channelkonfiguration des ePA-Aktenkontos für eine
7055 registrierte ePA-FdV-Instanz erfolgt über die Schnittstelle
7056 [I_Push_Notification_Management].

7057 **A_27641-02 -Push Notification Management - Push Notification Channels**

7058 Das Push Notification Management MUSS ausschließlich für die folgenden Ereignisse Push
7059 Nachrichten erstellen können, wenn das Ereignis durch einen Nutzer der definierten

7060 Nutzergruppe ausgelöst wird und die damit verbundene Operation erfolgreich (nicht
7061 durch einen Fehler abgebrochen) ist.

7062

7063 **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

7064 **[<=]**

7065 Hinweis 1 zu A_27641*:

7066 Da technische Dokumente gemäß A_23144* ausschließlich der Nutzung durch das ePA
7067 FdV dienen und für Nutzer nicht sichtbar sind, werden für technische Dokumente keine
7068 Push Notification versendet.

7069 Hinweis 2 zu A_27641*:

7070 Die Ereignisse zum Einstellen und Aktualisieren von Dokumenten sind nicht
7071 eingeschränkt auf den XDS Document Service, sondern werden in allen Services wirksam
7072 in denen Dokumente in das ePA-Aktensystem eingestellt werden.

7073 3.20.4 Push Notification Nachrichteninhalte

7074 (siehe auch: [gemF_PushNotification]#Kapitel "Operation Notify")

7075 Für jedes ausgelöste Ereignis eines Push Channels wird eine Push Notification erstellt. Die
7076 Nachrichtendaten für ein Ereignis werden strukturiert gemäß Schema angeordnet und
7077 nach den Vorgaben in [gemF_PushNotification#A_27610-*] auf konstante Länge
7078 aufgefüllt.

7079 **A_27645 -Push Notification Management - Push Notification Datenstruktur**

7080 Das Push Notification Management MUSS die Nachrichtendaten einer Push Nachricht für
7081 den Versand gemäß [Schema_PushNotifications] strukturieren.[<=]

7082 Es gibt eine maximal erlaubte Größe für Nachrichteninhalte, die durch das Push
7083 Notification System [gemF_PushNotification] vorgegeben wird. Es muss sichergestellt
7084 werden, dass erzeugte Nachrichteninhalte diese Größe nicht übersteigen.

7085 **A_27673 -Push Notification Management - Verkürzung der Nachrichteninhalte**

7086 Falls der erzeugte Nachrichtinhalt die maximal erlaubte Größe für Nachrichteninhalte
7087 übersteigt MUSS das Push Notification Management die Elemente `actor`, `title`, `who`,
7088 `folderTitle` so verkürzen, dass die maximal erlaubte Größe für Nachrichteninhalte
7089 gerade nicht überschritten wird.[<=]

7090 *Hinweis: Es müssen nicht alle aufgeführten Elemente gleichzeitig verkürzt werden.*

7091 **A_27674 -Push Notification Management - Art der Verkürzung**

7092 Falls Elemente einer Nachricht verkürzt werden, dann sollen diese so verkürzt werden,
7093 dass:

- 7094 • am Ende der Zeichenkette Zeichen entfernt werden
- 7095 • die Verkürzung mit "..." angezeigt wird.

7096 [<=]

7097 *Hinweis: Es kann sinnvoll sein, nur das längste kürzbare Element zu kürzen. Es wird*
7098 *empfohlen eine Mindestlänge von 50 Bytes nicht zu unterschreiten.*

7099 3.20.5 Versenden von Push Nachrichten

7100 (siehe auch: [gemF_PushNotification]#Kapitel "Operation Notify" und [PushNotificationConcept]#Concept:
7101 "Verschlüsselung des Benachrichtigungsinhalts")

7102 Eine erstellte Push Nachricht wird an jede ePA-FdV-Instanz mit einer Registrierung im
7103 Aktenkonto gesendet, wenn für diese der assoziierte Kanal abonniert wurde
7104 (Konfiguration `channelId == enabled`).

7105 Die längenkorrigierte Nachricht wird jeweils mit dem für den aktuellen Monat gültigen
7106 Schlüssel `AES/CGM-Schlüssel-Jahr-Monat` der Registrierung für jede adressierte ePA-
7107 FdV-Instanz verschlüsselt. Das Verschlüsselungsergebnis ist der Inhalt von `ciphertext`
7108 der `notification` für den Versand ([I_Push_Gateway]).

7109 **A_27651 -Push Notification Management - verpflichtende Verschlüsselung der** 7110 **Nachrichteninhalte**

7111 Das Push Notification Management MUSS sicherstellen, dass ausschließlich verschlüsselte
7112 Nachrichteninhalte als Push Nachricht versendet werden.[<=]

7113 Jedes einer Push Nachricht zugrundeliegenden Ereignis erzeugt auch einen
7114 Protokolleintrag im Audit Event Service. Die Menge der korrespondierenden
7115 Protokolleinträge ergibt dadurch im Aktenkonto ein Archiv der Push Ereignisse. Damit
7116 Clients ein Push Ereignis zu einem späteren Zeitpunkt, also nachdem die Push Nachricht
7117 im Client selbst schon gelöscht ist, restaurieren können, wird jeder Push Nachricht auch
7118 der Identifier des Protokolleintrags angehängt.

7119 **A_27644 -Push Notification Management - Referenz auf Protokolleintrag**

7120 Das Push Notification Management MUSS den eindeutigen Identifier `Resource.id` des zu
7121 einem Push Notification Ereignis gehörenden Protokolleintrags (AuditEvent) des
7122 Aktenkontos im Feld `notification/identifizier` einer Push Notification angeben.[<=]

7123 Hinweis:

7124 Gemäß A_24925 können Zugriffe gleicher Art im XDS Document Service mit mehreren
7125 Entity Strukturen unter einem AuditEvent gebündelt werden. Es gibt dann einen Audit
7126 Event Identifier, auch wenn beispielsweise drei Dokumente in die Akte eingestellt
7127 wurden. Im Feld `notification/identifizier` einer Push Notification wird dann mehrmals
7128 der gleiche Identifier eingetragen.

7129 **A_28218 -Push Notification Management - verpflichtende Stapelverarbeitung**

7130 Das Push Notification Management MUSS beim Senden von Push Notifications mehrere
7131 Push Notifications, die an denselben Endpunkt eines Push Gateways geschickt werden,
7132 gemeinsam in einer Stapelverarbeitung bearbeiten.[<=]

7133 **3.21 Backendseitige Zusatzfunktionen**

7134 Backendseitige Zusatzfunktionen sind Funktionen, die vom Hersteller des ePA-
7135 Aktensystems im ePA-Aktensystem integriert werden können und mit denen
7136 Kostenträger ihren Versicherten Mehrwerte anbieten können, die über den gesetzlich
7137 vorgegebenen Funktionsumfang der ePA hinausgehen. Backendseitige Zusatzfunktionen
7138 können hierfür Daten aus Akten der Versicherten nutzen.

7139 Backendseitige Zusatzfunktionen sind ein Angebot der Kostenträger für ihre Versicherten,
7140 welches die Versicherten freiwillig nutzen können. Mit ihrem ePA-FdV können sie
7141 jederzeit in eine backendseitige Zusatzfunktion, die durch ihren Kostenträger angeboten
7142 wird, einwilligen oder eine erteilte Einwilligung widerrufen.

7143 Die gematik spezifiziert die backendseitigen Zusatzfunktionen nicht, legt jedoch in
7144 diesem Abschnitt die Rahmenbedingungen fest, um backendseitige Zusatzfunktionen im
7145 ePA-Aktensystem integrieren zu können.

7146 Im Folgenden werden mit

7147 • **ePA-Daten** diejenigen Daten und Dokumente der Akte eines Versicherten
7148 bezeichnet, die durch die gesetzlichen Funktionen der ePA eingestellt und
7149 verarbeitet werden,

7150 • **ZF-Daten** diejenigen Daten und Dokumente bezeichnet, die durch eine
7151 backendseitige Zusatzfunktion erzeugt und verarbeitet werden.

7152 **A_30445 -Backendseitige Zusatzfunktionen - Angebot ausschließlich durch**
7153 **Anbieter des Aktensystems (Kostenträger)**

7154 Der Betreiber des ePA-Aktensystems MUSS gewährleisten, dass backendseitige
7155 Zusatzfunktionen im ePA-Aktensystem ausschließlich durch einen Anbieter des ePA-
7156 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 backendseitigen 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.

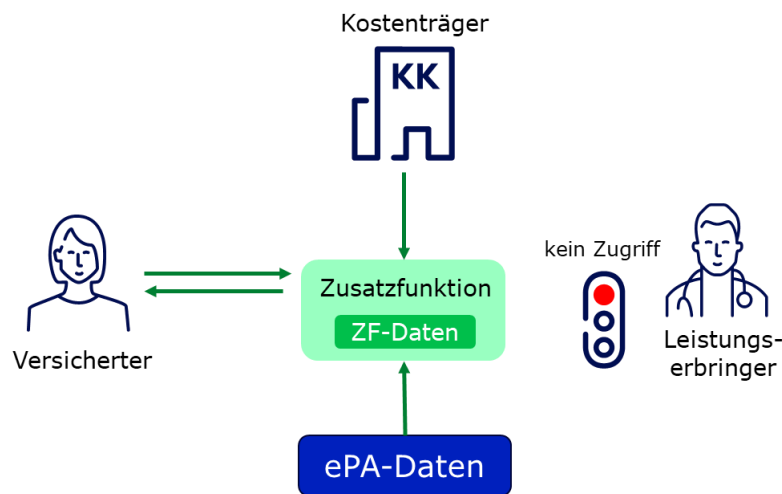


Abbildung 11 - Zugriffsmodell für backendseitige Zusatzfunktionen (Pfeile zeigen zulässigen Datenfluss)

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.

Leistungserbringer 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 konfiguratив 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 Zusatzfunktionsspezifischen **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**).

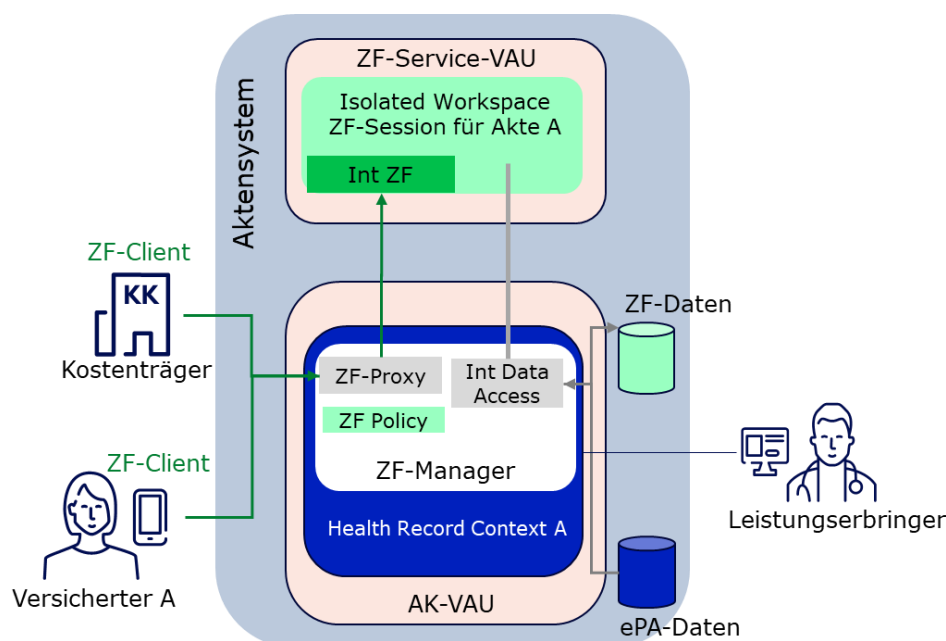


Abbildung 12 - Zusatzfunktion-Manager

ZF-Proxy und *Int Data Access* sind feste Bestandteile des Zusatzfunktion-Managers und unabhängig von einer speziellen Zusatzfunktion. Eine *ZF-Policy* ist spezifisch für eine Zusatzfunktion und wird dem Zusatzfunktion-Manager konfiguratativ 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. [$\leq$]

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. [$\leq$]

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. [$\leq$]

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. [$\leq$]

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

7255 Anforderung umfasst alle ZF-Daten, die die backendseitige Zusatzfunktion verarbeitet,
7256 insbesondere auch ggf. mit ePA-Daten des Versicherten trainierte Machine-Learning-
7257 Modelle.

7258 **A_30453 -Backendseitige Zusatzfunktionen - Schreib- und Löschzugriff**
7259 **ausschließlich für Versicherte oder Kostenträger**

7260 Der Zusatzfunktion-Manager MUSS sicherstellen, dass ausschließlich Nutzer in der Rolle
7261 "Versicherter" oder "Kostenträger" Daten an eine backendseitige
7262 Zusatzfunktion übermitteln oder ZF-Daten ändern bzw. löschen können. [<=]

7263 **A_30454 -Backendseitige Zusatzfunktionen - Schreibzugriff für Kostenträger**
7264 **ausschließlich für selbst angebotene ZF**

7265 Der Zusatzfunktion-Manager MUSS sicherstellen, dass Kostenträger ausschließlich auf
7266 Zusatzfunktionen zugreifen können, die der Kostenträger selbst anbietet. [<=]

7267

7268 **2. Starten und Beenden von Zusatzfunktionen**

7269 Eine Zusatzfunktion, in die der Versicherte eingewilligt hat, kann im Aktensystem
7270 ausgeführt werden, wenn die Akte des Versicherten im Aktensystem durch einen
7271 befugten Nutzer geöffnet wurde (z.B. durch den Aktenkontoinhaber, einen Vertreter,
7272 seinen Kostenträger oder einen befugten Leistungserbringer).

7273 Eine Zusatzfunktion kann direkt nach dem Öffnen der Akte gestartet werden oder aber
7274 auch erst aufgrund gewisser Ereignisse in der Akte (z.B. nach dem Einstellen von
7275 bestimmten Dokumenten bzw. Daten). Für jede Zusatzfunktion wird in einer zugehörigen
7276 ZF-Policy beschrieben, wann die Zusatzfunktion durch den ZF-Manager zu starten ist.

7277 **A_30455 -Backendseitige Zusatzfunktionen - ZF-Policies für Zusatzfunktionen**

7278 Der Hersteller des ePA-Aktensystems MUSS gewährleisten, dass für eine backendseitige
7279 Zusatzfunktion in einer ZF-Policy festgelegt werden kann, bei welchen Ereignissen in der
7280 Akte der ZF-Manager die Zusatzfunktion starten soll, insbesondere

- 7281 • beim Start des Health Record Contexts und/oder
- 7282 • beim Einstellen, Löschen oder Ändern von bestimmten Kategorien von ePA-Daten
7283 (z.B. das Einstellen von Impfeinträgen oder das Einstellen neuer
7284 Medikationsdaten) und/oder
- 7285 • beim Aufruf einer Operation der Zusatzfunktion durch einen Client.

7286 [<=]

7287 **A_30456 -Backendseitige Zusatzfunktionen - ZF-Policy enthält Namen der**
7288 **Zusatzfunktion**

7289 Der Hersteller des ePA-Aktensystems MUSS gewährleisten, dass in der ZF-Policy für eine
7290 backendseitige Zusatzfunktion ein für Versicherte verständlicher Zusatzfunktionsname
7291 definiert ist. [<=]

7292 Hinweis zu A_30456-*: Der Zusatzfunktionsname in der ZF-Policy wird für die
7293 Protokolleinträge verwendet, die beim lesenden Zugriff der backendseitigen
7294 Zusatzfunktion auf die ePA-Daten vom ZF-Manager erzeugt wird.

7295 **A_30457 -Backendseitige Zusatzfunktionen - Konfiguration von ZF-Policies im**
7296 **ZF-Manager**

7297 Das ePA-Aktensystem MUSS es ermöglichen, ZF-Policies für Zusatzfunktionen
7298 konfiguratativ 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 Zusatzfunktionen, 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 persistiert werden. [<=]

A_30465 -Backendseitige Zusatzfunktionen - Chiffre 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 Chiffre 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 Zusatzfunktionen

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.

7383 **3.22.1 Übersicht der Schnittstellen des Aktensystems**

7384 **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.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
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	

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
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.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
getAccessCode	Diese Operation erlaubt dem FdV den Abruf des Zugriffscode 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 ein 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

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
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

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
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

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
sendAuthorizationRequestBearerToken	Diese Operation initiiert die Authentifizierung über Bearer Token
sendAuthCodeSC	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
sendAuthCodeFdV	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
logoutFdV	Diese Operation beendet aktiv die Sitzung
I_Medication_Service_eML_Render	
renderEMLAsHTML	Diese Operation gibt die Medikationsliste im html-Format zurück.
renderEMLAsPDF	Diese Operation gibt die Medikationsliste im PDF/A-Format zurück.
I_Medication_Service_FHIR	
REST-Schnittstelle zum Abruf der Medikationsdaten im FHIR-Format	
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]	

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
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 Konfiguration der Push Notification Channels für einen Pusher aus
updateChannelsOfPusher	Diese Operation aktualisiert die Auswahl der Push Notification Channels für einen Pusher
getChannels	Diese Operation gibt die möglichen Push Notification Channels der ePA aus
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.

7385

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

7386 Die Schnittstellen (REST) und Operationen sind funktional in den Beschreibungen der
 7387 jeweiligen Schnittstelle beschrieben. Darüber hinaus gelten die folgenden übergreifenden
 7388 Anforderungen.

7389 3.22.2 Übergreifende Festlegungen zu den Schnittstellen

7390 **A_23918 -Schnittstellen (OpenApi) - Prüfung der Befugnis**

7391 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
 7392 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
 7393 eine vorhandene und gültige Befugnis (entitlement) für den Nutzer der Operation fordern
 7394 und diese nicht vorliegt. [**<=**]

7395 *Hinweis: A_23918 deckt auch die Fehlersituationen "kein VAU-Kanal" und "keine User*
 7396 *Session" ab, da diese eine Vorbedingung für den Nachweis einer gültigen Befugnis sind.*

7397 **A_24365 -Schnittstellen (OpenApi) - Prüfung des Aktenkontos**

7398 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
 7399 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
 7400 die Existenz des adressierten Aktenkontos fordern und diese nicht für den
 7401 Operationsaufruf verwendet wird. [**<=**]

7402 *Hinweis A_24365 deckt auch die Fehlersituation "kein Health Record Context" ab, da*
 7403 *dieses nur infolge eines nicht vorhandenen Aktenkontos auftritt.*

7404 **A_24538 -Schnittstellen (OpenApi) - Prüfung des Aktenkontostatus**

7405 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
 7406 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
 7407 einen vorgegebenen Status des Aktenkontos fordern und dieser nicht vorhanden ist. [$\leq$]

7408 **A_24366 -Schnittstellen (OpenApi) - Prüfung der Rolle**

7409 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
 7410 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
 7411 die Zulässigkeit der Operation auf bestimmte Rollen (professionOID) einschränken und
 7412 der Nutzer der Operation diese nicht nachweist. [$\leq$]

7413 **A_24367 -Schnittstellen(OpenApi) - Prüfung des Identifiers**

7414 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
 7415 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
 7416 die Zulässigkeit der Operation auf bestimmte Identifier (KVNR oder Telematik-ID)
 7417 einschränken und der Nutzer der Operation diese nicht nachweist. [$\leq$]

7418 **A_24580 -Schnittstellen (OpenApi) - Protokollierung der Operationen**

7419 Das ePA-Aktensystem MUSS nach der Ausführung der Operationen der REST-
 7420 Schnittstellen eine Protokolleintrag erstellen, wenn die Protokollierung in den
 7421 Nachbedingungen (Postconditions) der Operationen gefordert ist (log-entry). [$\leq$]

4 Informationsmodelle

7422

7423 Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten
7424 wird nicht benötigt.

7425

5 Anhang A – Verzeichnisse

7426

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

Kürzel	Erläuterung
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

7427 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]).

7428 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung
7429 gestellt.

7430 5.3 Abbildungsverzeichnis

7431	Abbildung 1 : Ablauf der Anlage eines Aktenkontos.....	30
7432	Abbildung 2: Alternativen zur Ausführung des Befugnisverifikations-Moduls.....	54
7433	Abbildung 3 - Typen von VAU-Schnittstellen	86
7434	Abbildung 4: Überblick Service-VAUs	95
7435	Abbildung 5: Einfrieren von Daten durch eine AK-VAU.....	98
7436	Abbildung 6: Einfrieren von Daten durch eine Service-VAU	99
7437	Abbildung 7: Auftauen von eingefrorenen Daten.....	101
7438	Abbildung 8: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP ..	220
7439	Abbildung 9: Ablauf der Authentifizierung einer LEI über den Smartcard IDP	224
7440	Abbildung 10: Ablauf der Authentisierung über JWT Bearer Token am Beispiel eRP-FD	225
7441	Abbildung 11 - Zugriffsmodel für backendseitige Zusatzfunktionen (Pfeile zeigen	
7442	zulässigen Datenfluss)	247
7443	Abbildung 12 - Zusatzfunktion-Manager	248
7444		

7445 5.4 Tabellenverzeichnis

7446	Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat	18
7447	Tabelle 2 : Inhalte des JWT der Befugnisse im Exportpaket.....	34
7448	Tabelle 3: Zustandswechsel im Lebenszyklus einer Akte	37
7449	Tabelle 4: Tab_AS_VAU_Token_Modul_Rules-07 -Prüfregeln VAU Token	56
7450	Tabelle 5: Überblick über die Regeln des Befugnisverifikations-Moduls	66
7451	Tabelle 6: Tab_AS_Entitlement_Registration_Rules-07 - Regeln zur Registrierung von	
7452	Befugnissen	68

7453	Tabelle 7: Tab_AS_SDS-Key_Rules Key Rules-07 - Regeln zur Ableitung der	
7454	versichertenindividuellen Persistierungsschlüssel	78
7455	Tabelle 8: Widerspruchsfähige Funktionen der elektronischen Patientenakte	106
7456	Tabelle 9: Nutzergruppen der User Specific Deny Policy Medication.....	110
7457	Tabelle 10: Inhalt einer Befugnis	111
7458	Tabelle 11: Befugnisse für berechnigte Nutzergruppen und Nutzer	113
7459	Tabelle 12: Befugnisse EU-Zugriff für berechnigte Nutzergruppen und Nutzer	116
7460	Tabelle 13 : JWT zur Befugnisvergabe mit den Mindest-Inhalten.....	119
7461	Tabelle 14 : JWT zur Befugnisvergabe mit Mindest-Inhalten.....	122
7462	Tabelle 15: Inhalt eines Blocked User Policy Eintrags	125
7463	Tabelle 16: Legal Policy	132
7464	Tabelle 17: Legal Policy - EU-Zugriff	135
7465	Tabelle 18: Beschreibung der Kategorien und Services.....	137
7466	Tabelle 19: Inhalt eines General Deny Policy Eintrags	142
7467	Tabelle 20: Verbergen eines Medical Service.....	143
7468	Tabelle 21: Kennzeichnung von Optionalitäten	156
7469	Tabelle 22: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den	
7470	Außerschnittstellen des XDS Document Service	157
7471	Tabelle 23 : Liste mit Dokumententypen, die ersetzt werden können	165
7472	Tabelle 24 : Liste mit Ordnern, in denen Dokumente ersetzt werden dürfen.....	165
7473	Tabelle 25 : Fehlertexte zu StatusMismatch-Fehlercode.....	171
7474	Tabelle 26: Schnittstelle I_Document_Management	174
7475	Tabelle 27: Schnittstelle I_Document_Management_Insurant	177
7476	Tabelle 28: Festlegung Folder.entryUUIDzu statischen Ordnern	179
7477	Tabelle 29: Nutzungsvorgaben für Metadatenattribute XDS	182
7478	Tabelle 30: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language	
7479	Codes	200
7480	Tabelle 31: Einsortierung_Datenkategorien.....	206
7481	Tabelle 32: TAB_EPA_Sammlungstypen	210
7482	Tabelle 33: Auswirkungen bei Widerspruch gegen eine Funktion der ePA	212
7483	Tabelle 34 : Inhalte des übermittelten JWT der Client Attestierung	225
7484	Tabelle 35 : JWT Bearer Token mit den Mindest-Inhalten	226
7485	Tabelle 36 : JWT Bearer Token FDZ mit den Mindest-Inhalten.....	226
7486	Tabelle 37 : JWT Bearer Token eines Kostenträgers mit den Mindestinhalten	227
7487	Tabelle 38: Auswahl der zu übertragenden FHIR-Ressourcen	237
7488	Tabelle 39: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen	237
7489	Tabelle 40: Ereignisse und deren Push Nachrichten.....	243

7490	Tabelle 41: Übersicht der Schnittstellen des Aktensystems	252
7491		

7492 5.5 Referenzierte Dokumente

7493 5.5.1 Dokumente der gematik

7494 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
7495 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

[Quelle]	Herausgeber: Titel
[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

[Quelle]	Herausgeber: Titel
[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_Convert_PDF_Insurant]	gematik: I_Tool_Convert_PDF_Insurant Schnittstelle für die PDF Formatkonvertierung siehe [ePA_XDS_Document] Path: src/openapi/I_Tool_Convert_PDF_Insurant.yaml
[XDSDocumentService]	gematik: XDSDocumentService.wsdl IHE-Schnittstelle des XDSDocumentService siehe [ePA_XDS_Document] Path: src/schema
[Exportpaket]	gematik: HealthRecordExportPackage.adoc Aktenkontoverwaltung - Exportpaket für Daten der Akte siehe [ePA_Basic] Path: src/docs/HealthRecordExportPackage.adoc

[Quelle]	Herausgeber: Titel
[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/

[Quelle]	Herausgeber: Titel
[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

7496 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

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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 Internet: 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/

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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/

7497