

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Aktensystem ePA für alle

Version: 1.5-06.0 CC
Revision: 127421399005
Stand: 27.0515.07.2025
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich Entwurf
Referenzierung: gemSpec_Aktensystem_ePAfueralle

26

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

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

Inhaltsverzeichnis

1 Einführung	8
1.1 Zielsetzung	8
1.2 Zielgruppe	8
1.3 Geltungsbereich	8
1.4 Abgrenzungen	8
1.5 Methodik	9
2 Übergreifende Festlegungen	10
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	21
2.6 Benutzerführung	22
2.7 Useragent	24
2.8 Performance aus Anwendersicht	24
3 Funktionsmerkmale	26
3.1 Aktenkonto eines Versicherten (Health Record)	26
3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte	26
3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger	26
3.1.2 Lebenszyklus und Zustände eines Aktenkontos	27
3.1.3 Anlage eines neuen Aktenkontos	28
3.1.4 Löschen eines Aktenkontos	30
3.2 Health Record Relocation Service	31
3.2.1 Ablauf eines Aktenkontoumzugs	36
3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter	36
3.2.1.2 Start Transfer eines existierenden Aktenkontos	37
3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen Anbieter	37
3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den neuen Anbieter	37
3.2.1.5 Import des Exportpakets durch den neuen Anbieter	38
3.2.1.6 Abschluss des Transfers durch beide Anbieter	38
3.2.1.7 Fehlersituationen und Handhabung	38
3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich oder derzeit nicht möglich	38
3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter	39

69	3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen	
70	Anbieter	40
71	3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter	41
72	3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM	
73	42
74	3.4 Befugnisverifikations-Modul	45
75	3.4.1 VAU-Token-Modul	46
76	3.4.2 Regeln des Befugnisverifikations-Moduls	51
77	3.5 Vertrauenswürdige Ausführungsumgebung (VAU)	64
78	3.5.1 Übergreifende VAU-Anforderungen	65
79	3.5.1.1 Schutz der Integrität der VAU	65
80	3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU	66
81	3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU	67
82	3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM	67
83	3.5.1.5 Logging und Monitoring	67
84	3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU	69
85	3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU ...	69
86	3.5.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-	
87	VAU	70
88	3.5.2.3 Konsistenz des Systemzustands	71
89	3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU	71
90	3.5.4 Zusätzliche Anforderungen an eine Service-VAU	72
91	3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU	74
92	3.6 Umschlüsselung und Überschlüsselung	74
93	3.7 User Session und Health Record Context	78
94	3.8 Consent Decision Management	79
95	3.8.1 Widersprüche für Funktionen der ePA	79
96	3.8.2 Einschränkung der Verwendung von Daten auf bestimmte	
97	Sekundärnutzungszwecke	83
98	3.8.3 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny	
99	Policy Medication)	86
100	3.9 Entitlement Management	88
101	3.9.1 Initiale Befugnisse (static Entitlements)	94
102	3.9.2 Erstellen einer Befugnis durch Clients	96
103	3.9.2.1 Befugnisvergabe durch ein ePA-FdV	96
104	3.9.2.2 Befugnisvergabe durch ein Primärsystem	98
105	3.9.3 Löschen von Befugnissen	100
106	3.9.4 Befugnisausschluss (Blocked User Policy)	101
107	3.9.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)	103
108	3.9.6 EntitlementDenyList	105
109	3.10 Legal Policy	108
110	3.11 Constraint Management	116
111	3.11.1 Aktenkontoweites Verbergen (General Deny Policy)	119
112	3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes	
113	120
114	3.12 Device Management	121
115	3.13 Medical Services	125
116	3.13.1 XDS Document Service	125

117	3.13.1.1 Formatprüfung beim Einstellen von Dokumenten	126
118	3.13.1.2 Anforderungen zur Validierung	128
119	3.13.1.3 Namensräume.....	129
120	3.13.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von	
121	Dokumenten	130
122	3.13.1.4.1 Anforderungen an IHE ITI-Akteure.....	130
123	3.13.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen	133
124	3.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen ...	135
125	3.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen	151
126	3.13.1.5 Fehlerbehandlung in Schnittstellenoperationen	152
127	3.13.1.6 Schnittstellen im XDS Document Service	153
128	3.13.1.6.1 Schnittstelle I_Document_Management.....	153
129	3.13.1.6.2 Schnittstelle I_Document_Management_Insurant	156
130	3.13.1.6.3 Schnittstelle I_Document_Management_Ncpeh	158
131	3.13.1.7 Statische Metadaten	159
132	3.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten	161
133	3.13.1.8.1 Allgemeine Metadatenvorgaben	161
134	3.13.1.8.2 Metadaten der Dokumente und SubmissionSets	177
135	3.13.1.8.3 Metadaten für Datenkategorien	181
136	3.13.1.8.4 Automatisches Umschreiben von Daten	182
137	3.13.1.9 Strukturierte Dokumente.....	183
138	3.13.1.9.1 Sammlungstypen.....	184
139	3.13.1.9.2 Konfigurierbarkeit	185
140	3.13.1.9.3 Verarbeitungsvorgaben für spezifische Dokumente	186
141	3.13.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode	
142	187
143	3.13.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die	
144	Dokumente des Aktenkontos	188
145	3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication	
146	Service durch eine spezifische LEI auf die Dokumente des Aktenkontos.....	189
147	3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service	189
148	3.13.1.14 Unterstützungsleistung für das ePA-FdV	192
149	3.13.2 FHIR Data Services.....	193
150	3.13.2.1 Patient Service.....	193
151	3.13.2.2 Medication Service.....	194
152	3.13.2.3 MHD Service	197
153	3.13.2.4 Dienstübergreifende Festlegungen	199
154	Wenn Migrationsvorgaben für den Datenbestand eines FHIR Data Services für	
155	verschiedene Versionen des Services existieren, MUSS der FHIR Data Service	
156	199
157	3.14 Audit Event Service	199
158	3.15 Information Service.....	206
159	3.15.1 Information Service	206
160	3.15.1.1 Informationen zu Widersprüchen (Consent Decisions)	206
161	3.15.1.2 Informationen zur Anwenderperformance (UX Performance)	207
162	3.15.2 Information Service - Account.....	207

163	3.16 Email Management	207
164	3.17 Zusätzliche Anforderungen an den Authorization Service.....	209
165	3.17.1 Anforderungen an den Authorization Service für die Authentisierung von	
166	Versicherten (FdV)	209
167	3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B	
168	213
169	3.17.3 Anforderungen an den Authorization Service für die Authentisierung des E-	
170	Rezept-Fachdienstes	215
171	3.18 Anbindung Verzeichnisdienst FHIR-Directory	216
172	3.19 Access Gateway	216
173	3.19.1 Paketfilter	216
174	3.19.1.1 Funktion	216
175	3.19.1.2 Redundanz	218
176	3.19.1.3 Konfiguration	218
177	3.19.1.4 Adressierung.....	218
178	3.19.1.4.1 Access Gateway zum Transportnetz Internet	218
179	3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz	219
180	3.19.2 Proxy für das VAU-Protokoll	219
181	3.19.3 Tracing in Nichtproduktivumgebungen	219
182	3.19.4 Übergreifende Festlegungen	220
183	3.20 Data Submission Service	221
184	3.20.1 Erstellung von Arbeitsnummern und Lieferpseudonymen	222
185	3.20.2 Auswahl von medizinischen Daten	223
186	3.20.3 Protokollierung des Datenexports an das FDZ	224
187	3.20.4 Pseudonymisierung von medizinischen Daten.....	224
188	3.20.5 Übermittlung der pseudonymisierten medizinischen Daten	225
189	3.21 Push Notification Management	227
190	3.21.1 Push Notification Management des ePA-Aktensystems	227
191	3.21.2 Registrierung eines ePA-FdV als Pusher.....	228
192	3.21.3 Push Notification Channels	229
193	3.21.4 Push Notification Nachrichteninhalte	230
194	3.21.5 Versenden von Push Nachrichten.....	231
195	3.21.6 Protokollierung.....	231
196	3.22 Schnittstellen (OpenAPI).....	233
197	3.22.1 Übersicht der Schnittstellen des Aktensystems	233
198	3.22.2 Übergreifende Festlegungen zu den Schnittstellen	241
199	4 Informationsmodelle	242
200	5 Anhang A – Verzeichnisse	243
201	5.1 Abkürzungen	243
202	5.2 Glossar	245
203	5.3 Abbildungsverzeichnis.....	245
204	5.4 Tabellenverzeichnis	245
205	5.5 Referenzierte Dokumente	247
206	5.5.1 Dokumente der gematik.....	247
207	5.5.2 Weitere Dokumente.....	251

208	6 Anhang B – Erläuternde Informationen	254
209	6.1 Dokumentenanhänge.....	254
210	6.2 Überblick	254
211	6.3 Ungültige Anhänge	256
212	6.3.1 Verweiszirkel und doppelte Eltern.....	257
213	6.3.2 Anhangskette zu lang	258
214		

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.

246 1.5 Methodik

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

251
252 **<AFO-ID> - <Titel der Afo>**
253 Text / Beschreibung
254 [**<=**]

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

2 Übergreifende Festlegungen

257

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

261 **A_24986 -ePA-Aktensystem - Rollentrennung ePA-Aktensystem und IDP-Dienst**

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

268 **A_25149-01 -ePA-Aktensystem - Rollentrennung ePA-Aktensystem und** 269 **sektoraler IDP**

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

276 **A_24673 -Zeitsynchronisation über Zeitdienst in der TI**

277 Das ePA-Aktensystem MUSS die Systemzeit über den Zeitdienst in der TI
278 gemäß [gemSpec_Net#6.2] synchronisieren
279 [<=]

280 **A_25612 -ePA-Aktensystem - Authentisierung gegenüber einem Client** 281 **innerhalb der TI**

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

284 **A_24676 -Useragent Information in HTTP Header außerhalb des VAU-Kanals**

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

289 **A_24677 -Useragent Information in HTTP Header innerhalb des VAU-Kanals**

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

294 Die Formatvorgaben zum Useragent sind in A_22470* definiert.

295 **A_24816-01 -Aktenkontokennung in HTTP Header innerhalb des VAU-Kanals**

296 Das ePA-Aktensystem MUSS sicherstellen, dass ePA-Clients in der Kommunikation mit
297 den Medical Services der ePA innerhalb des VAU-Kanals ein HTTP Header Element mit
298 dem Namen "x-insurantId" gesendet wird und andernfalls den Request mit HTTP-Fehler
299 400 ablehnen.[<=]

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

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

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

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

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

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

317 **A_27703 -Requestkennung in der Response**

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

322 **A_27712 -Requestkennung - betriebliche Protokollierung**

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

327 **A_27443 -Nutzung Terminologiepaket**

328 Das ePA-Aktensystem MUSS die relevanten Terminologien des Terminologiepakets
 329 gemäß [IG_TI_Terminology] verarbeiten und in der Kommunikation mit dem ePA-
 330 Aktensystem berücksichtigen. [<=]

331 Hinweis zu A_27443:

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

334 **A_27708 -ePA-Aktensystem – Festlegung zu Formatvorgabe für Datentyp** 335 **datetime gemäß RFC3339**

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

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

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

346 Beispiele für Datentyp datetime:

347 2025-04-12T15:20:50Z

348 2025-06-30T23:59:59+01:00

A_27868 -ePA-Aktensystem – fehlerhafter URL-Pfad

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

[<=]

2.1 Aktensystem- und Service-Lokalisierung

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

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

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

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

A_24592-02 -Anbieter ePA-Aktensystem -Registrierung an übergreifender ePA-Domäne

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

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

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

[<=]

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

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

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

387

388 **Beispiele der Dienstlokalisierung**389 **PU :**390 **Aktensystem A**

391 epa-as-1.prod.epa4all.de A 100.102.x1.x2

392 ggf. ... weitere IP-Adressen für epa-as-1.prod.epa4all.de (DNS-Round-Robin)

393 ...

394 epa-asisa-1.prod.epa4all.de A 100.102.x3.x4

395

396 **Aktensystem B**

397 epa-as-2.prod.epa4all.de A 100.102.x5.x6

398 epa-asisa-2.prod.epa4all.de A 100.102.x7.x8

399

400 **TU :**401 **Aktensystem 1**

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

403 ...

404

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

409 **A_14128-04 -Anbieter ePA-Aktensystem - Resource Records FQDN ePA**

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

412 [**<=**]

413 **A_22688-04 -Anbieter ePA-Aktensystem, Konfiguration Schnittstellen über**
 414 **/.well-known/**

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

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

421

```
422 {
423     "version" : "<Produkttypversion des Aktensystems im Format[0-
424 9]{1,3}\.\[0-9]{1,3}\.\[0-9]{1,3}>",
425     ....
426 }
```

426 } [**<=**]427 **A_22687 -Aktensystem, Konfiguration Schnittstellen über /.well-known/**

428 Das ePA-Aktensystem MUSS sicherstellen, dass dem Anbieter des ePA-Aktensystems die
 429 technische Möglichkeit bereitgestellt wird A_22688-* umzusetzen. [**<=**]

430 **A_26814 -ePA-Aktensystem - Schnittstellenadressierung**

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

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

435 Für Operationen, die innerhalb einer ePA-VAU aufgerufen werden, gelten die
436 Schnittstellenspezifikationen für den inneren HTTP-Request.
437 Abgrenzend hierzu wird das VAU-Protokoll und die dabei verwendeten Pfade in
438 [gemSpec_Krypt#7] definiert.

439 **A_24801 -Aktensystem, Liste von FQDN im Internet**

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

445 **2.2 Redundanz**

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

448 **2.3 Datenschutz und Sicherheit**

449 **A_15128 -Anbieter ePA-Aktensystem - Schutz der transportierten Daten im** 450 **ePA-Aktensystem**

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

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

456 **A_15103 -Anbieter ePA-Aktensystem - Konzept zur Verhinderung von** 457 **Profilbildung**

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

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

464 **A_25722 -ePA-Aktensystem - Löschen von personenbezogenen Daten von** 465 **Vertretern nach Wegfall der Notwendigkeit**

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

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

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

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

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

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

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

482 **A_24774 -Anbieter ePA-Aktensystem - Zwei-Faktor-Authentisierung von** 483 **Administratoren**

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

486 **A_15107-02 -Anbieter ePA-Aktensystem - Keine unzulässige Weitergabe von** 487 **Daten**

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

494 **A_15119 -Anbieter ePA-Aktensystem - Löschkonzept**

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

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

504 [<=]

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

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

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

510 Davon ausgenommen ist das Erfassen des standardmäßigen quantitativen
511 Nutzerverhaltens zur Ermittlung der Standard-Aktenutzung entsprechend der
512 Anforderung A_15154. [<=]

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

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

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

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

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

A_24778 -Anbieter ePA-Aktensystem - Einsatz zertifizierter HSM

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

Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3 oder
2. FIPS 140-3 Level 3 oder
3. Common Criteria EAL 4+ (mit AVA_VAN.5)

entsprechen.[<=]

A_15157 -Anbieter ePA-Aktensystem - Sicherer Betrieb und Nutzung eines HSMs

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

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

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

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

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

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

A_15163 -Anbieter ePA-Aktensystem - Angriffen entgegenwirken

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

A_15167 -Anbieter ePA-Aktensystem - Social Engineering Angriffen entgegenwirken

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

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

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

A_15168 -ePA-Aktensystem - Verbot vom dynamischen Inhalt

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

[<=]

A_17080 -Verhindern von Session Hijacking

572 Die Komponenten des ePA-Aktensystems MÜSSEN geeignete Schutzmaßnahmen gegen
573 Session-Hijacking implementieren.

574 [\leq]

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

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

580 [\leq]

581 **A_24781 -Sicherer Betrieb des Produkts nach Handbuch**

582 Der Anbieter eines ePA-Aktensystems MUSS die im Handbuch des eingesetzten ePA-
583 Aktensystems beschriebenen Voraussetzungen für den sicheren Betrieb des Produktes
584 gewährleisten.[\leq]

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

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

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

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

594 **A_21106 -Anbieter ePA-Aktensystem – Signaturschlüssel für Protokolle**

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

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

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

603 [\leq]

604 **A_22409 -Anbieter ePA-Aktensystem - CA-Anbieterwechsel**

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

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

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

613 **A_24783 -ePA-Aktensystem - Eingabevalidierung von Operationen**

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

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

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

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

623 **A_24993 -ePA-Aktensystem - Zugriffe übers Access Gateway ausschließlich für**
624 **Versicherte**

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

628 **A_25006 -ePA-Aktensystem - User Session bei Inaktivität Beenden**

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

631 **A_25022 -ePA-Aktensystem - Debug-Protokoll für Testbetrieb**

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

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

636 **A_25023 -ePA-Aktensystem - Keine Echtdaten im Testbetrieb**

637 Das ePA-Aktensystem MUSS sicherstellen, dass im Testbetrieb keine Echtdaten
638 verarbeitet werden. [<=]

639 **A_25042 -ePA-Aktensystem - Prüfung von Signaturen**

640 Das ePA-Aktensystem MUSS bei der Prüfung von Signaturen

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

644 [<=]

645 **A_25040-01 -ePA-Aktensystem - Prüfung Signaturzertifikate**

646 Das ePA-Aktensystem MUSS Signaturzertifikate gemäß [gemSpec_PKI#TUC_PKI_018]
647 mit folgenden Parametern auf Gültigkeit prüfen:

648 **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	digitalSignatu re	nonRepudiati on	nonRepudiatio n	digitalSignatu re
intendedExtendedKeyUsa ge	(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

649 Das ePA-Aktensystem MUSS sicherstellen, dass die Prüfung des Signaturzertifikats nur
650 erfolgreich ist, falls das Signaturzertifikat anhand der Zertifikatsprüfung für

651 [Zertifikatsignatur "valid" UND zeitlich gültig UND online gültig] befunden wird.
652 [=]

653 **A_27498 -Anbieter ePA-Aktensystem - Offline-Datensicherung**

654 Der Anbieter des ePA-Aktensystems MUSS Offline-Datensicherungen für die Aktenkonten
655 umsetzen.[<=]

656 **A_27497 -Anbieter ePA-Aktensystem - Rollenkonzept zum Schutz der** 657 **permanenten Verfügbarkeit von Aktenkonten**

658 Der Anbieter des ePA-Aktensystems MUSS durch ein Rollenkonzept sicherstellen, dass ein
659 einzelner Mitarbeiter die Verfügbarkeit der Akten nicht permanent zerstören kann, z.B.
660 durch endgültiges Löschen von Masterkeys oder von Chiffren der Daten der
661 Aktenkonten. Organisatorische Maßnahmen wie Dienstanweisungen sind alleine nicht
662 ausreichend, um eine Rollentrennung zu etablieren.
663 [=]

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

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

668 **A_27500 -Anbieter ePA-Aktensystem - Rollentrennung Administratoren für** 669 **Backup- und Produktionsdaten**

670 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass es eine Rollentrennung
671 zwischen Backup-Administratoren und Administratoren der Produktivumgebung
672 gibt.[<=]

673 **2.4 Validierungsaktenkonto**

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

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

695 Folgende Anwendungsfälle sollen mit den Validierungsaktenkonten adressiert werden:

- 696 • Monitoring der Aktensystemfunktionalität
- 697 • Troubleshooting bei Störungsmeldungen (über FdV oder Primärsystem)

- 698 • Validierung der Konfiguration in der LEU
- 699 • Store-Review seitens der App-Store-Betreiber (über FdV)
- 700 • Validierung der EU-Anbindung
- 701 Die mittels der Validierungskonten in der Produktivumgebung realisierten
- 702 Anwendungsfälle müssen sich möglichst auf die genannten, unbedingt jedoch auf
- 703 spezifizierte Anwendungsfälle beschränken.
- 704 **A_18168-01 -Anbieter des ePA-Aktensystem - Validierungsaktenkonto für**
- 705 **gematik**
- 706 Nach Aufforderung durch die gematik MUSS der Anbieter des ePA-Aktensystems
- 707 • für die gematik ein Validierungsaktenkonto im ePA-Aktensystem für die von der
- 708 gematik übergebene KVNR anlegen, wobei die KVNR die Festlegungen für die
- 709 Versichertennummer [gem. gemSysL_PK_eGK] erfüllen muss.
- 710 • das durch die gematik angegebene Validierungsaktenkonto löschen, sofern die
- 711 gematik dessen Anlage beantragt hatte.
- 712 [**<=**]
- 713 **A_18169-02 -Anbieter des ePA-Aktensystem - Validierungsaktenkonto für**
- 714 **eigene Zwecke**
- 715 Falls sich der Anbieter des ePA-Aktensystems ein Validierungsaktenkonto für eigene
- 716 Zwecke anlegen möchte, MUSS er sicherstellen, dass nur eine Versichertennummer aus
- 717 dem von der gematik für diesen Anbieter freigegebenen Nummernkreis [gem.
- 718 gemSysL_PK_eGK] verwendet wird.
- 719 [**<=**]
- 720 **A_22522-01 -Anbieter des ePA-Aktensystems - Validierungskonto für Dritte**
- 721 Der Anbieter des ePA-Aktensystems MUSS auf Antrag der gematik
- 722 • Validierungsaktenkonten für Dritte (z.B. DVO, PS-Hersteller) für eine vom
- 723 Antragsteller übermittelte KVNR anlegen, sofern die KVNR die Festlegungen für
- 724 die Versichertennummer [gem. gemSysL_PK_eGK] erfüllt ist.
- 725 • das durch einen Antragsteller angegebene Validierungsaktenkonto löschen, sofern
- 726 der Antragsteller dessen Anlage beantragt hatte.
- 727 [**<=**]
- 728 Hinweis zu A_22522-*: Die Einrichtung der Validierungsaktenkonten für Dritte kann
- 729 gegen Bezahlung erfolgen. Die Entscheidung *dafür obliegt dem Anbieter des ePA-*
- 730 *Aktensystems.*
- 731 Im Design der ePA für alle wird die Initialisierung und Aktivierung durch den
- 732 Kostenträger vorgenommen. Da es diese Rolle bei Validierungsaktenkonten nicht gibt,
- 733 sind für diese speziellen Aktenkonten die folgenden Besonderheiten zu berücksichtigen:
- 734 **A_26187 -Anlage von Validierungsaktenkonten**
- 735 Das ePA-Aktensystem MUSS die Anlage von Validierungsaktenkonten auch ohne KTR-
- 736 und Ombudsstellen-Befugnisse zulassen.[**<=**]
- 737 **A_26188 -Anbieter des ePA-Aktensystems -Aktivierung von**
- 738 **Validierungsaktenkonten**
- 739 Der Anbieter des ePA-Aktensystems MUSS den Status von Validierungsaktenkonten,
- 740 welche für die gematik (gem. A_18168-*) oder für Dritte (gem. A_22522-*) angelegt
- 741 wurden, nach der Anlage auf ACTIVATED setzen.[**<=**]
- 742 Falls ein Antragsteller keine Löschung eines Validierungsaktenkontos beim Anbieter des
- 743 ePA-Aktensystems beantragt, wird das Validierungsaktenkonto nach einer Lebensdauer

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

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

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

A_22684-01 -Validierungsaktenkonten im Store-Review der FdVs

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

A_22942 -Besonderheiten bei Validierungsaktenkonten für StoreReviews

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

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

[<=]

A_26209 -Prüfung auf Vertretungsberechtigung für Prüfidentität

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

A_24539 -Nutzung von Validierungsaktenkonten via FdV

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

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

2.5 Tracing in Nichtproduktivumgebungen

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

789 ein Tracing im Aktensystem für Nichtproduktivumgebungen eingeführt und wird mit ePA
790 für alle wie folgt umgesetzt:

- 791 1. Innerhalb des AS werden an die für die Fehlersuche in Nichtproduktivumgebungen
792 wichtigen Stellen Sensoren platziert. Diese Sensoren streamen die aktuell
793 transportierten Daten an bestimmte TCP-Ports am Access Gateway. Die
794 Sensorpunkte liegen im AS immer hinter der TLS-Entschlüsselung.
795 Fehlersuchende können sich zu diesen TCP-Ports am Access Gateway verbinden
796 und lesen dann im Read-Only-Modus den aktuellen Datenverkehr, der an den
797 Sensorpunkten vorbeifließt, mit.
- 798 2. ePA-Clients müssen in Nichtproduktivumgebungen beim VAU-Protokoll die
799 symmetrischen Verbindungsschlüssel offenlegen [gemSpec_Krypt#A_24477-*].

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

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

809 **A_21887-01 -Tracing, Sensorpunkt nahe vor den VAU-Instanzen** 810 **(Nichtproduktivumgebungen)**

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

817 [\leq]

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

819 Ein ePA-Aktensystem MUSS zum Mitschneiden und Streamen der Testdaten in
820 Nichtproduktivumgebungen nach A_21887-* den von der gematik bereitgestellten
821 aggregierenden Tiger-Standalone-Proxy (mindestens der Version 0.20) verwenden. [\leq]

822 **A_22581 -Tracing, Abschaltbarkeit**

823 Ein ePA-Aktensystem MUSS den Tiger-Standalone-Proxy (und die damit verbunden
824 Sensorpunkte) gemäß A_21891-* im Rahmen der Zulassungstests auf Wunsch der
825 gematik aktivieren und insbesondere deaktivieren können. [\leq]

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

830 **2.6 Benutzerführung**

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

834 **A_15842 -Anbieter ePA-Aktensystem - Ergonomie der Benutzerführung**

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

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

839 Zusätzlich zu den in diesem Kapitel aufgeführten Anforderungen zur Benutzerführung
840 sollen auch die in der ISO 9241 aufgeführten Qualitätsrichtlinien zur Sicherstellung der
841 Ergonomie interaktiver Systeme und Anforderungen aus der Verordnung zur Schaffung
842 barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz
843 (Barrierefreie-Informationstechnik-Verordnung – BITV 2.0) beachtet werden.

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

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

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

858 **BITV 2.0 - Barrierefreie Informationstechnik-Verordnung**

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

861 Insbesondere sollen deshalb neben der Übernahme der international anerkannten
862 Standards für barrierefreie Webinhalte, die Web Content Accessibility Guidelines (WCAG)
863 2.1, auch die Belange gehörloser, hör-, lern- und geistig behinderter Menschen
864 berücksichtigt werden.

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

867 Weitere Richtlinien und Empfehlungen zur digitalen Barrierefreiheit sind die EU-Richtlinie
868 2016/2102 für öffentliche Stellen und die europäische Norm EN 301 549 V2.1.2 mit dem
869 Titel "Accessibility requirements for ICT products and services".

870 **A_15846 -Anbieter ePA-Aktensystem - Schnittstellen für die Unterstützung der** 871 **barrierefreien Bedienungsmöglichkeit**

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

2.7 Useragent

A_22470-06 -Definition x-useragent

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

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

Beispiel: "CLIENTID1234567890AB/2.1.12-45"

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

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

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

2.8 Performance aus Anwendersicht

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

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

Die Übermittlung der Messdaten erfolgt im Anschluss an den erfolgreichen Abschluss des Anwendungsfalles an das gleiche Aktensystem (unter Verwendung der Schnittstelle

920 InformationService.setUserExperienceResult), bei dem auch der Anwendungsfall
921 stattgefunden hat. Hierbei ist die Schnittstelle zur Lieferung der Messdaten an der
922 Komponente "Information Service" nur für Primärsysteme normiert. Es steht dem
923 Hersteller des Aktensystems frei, die Lieferschnittstelle für Messdaten von FdVs selbst
924 oder nach dem Vorbild der PS-Schnittstelle zu implementieren.

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

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

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

- 933 - Durchschnittswert der Messergebnisse
- 934 - Anzahl der berücksichtigten Messergebnisse
- 935 - Maximalwert
- 936 - Minimalwert[<=]

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

940

3 Funktionsmerkmale

941 3.1 Aktenkonto eines Versicherten (Health Record)

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

947 3.1.1 Widerspruch des Versicherten gegen die Nutzung der 948 elektronischen Patientenakte

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

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

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

962 **A_23886 -Anbieter ePA-Aktensystem - Keine Aktenkontoanlage bei 963 Widerspruch des Versicherten**

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

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

970 **A_25181 -Anbieter ePA-Aktensystem - Aktenkontoanlage bei Zurücknahme des 971 Widerspruchs des Versicherten**

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

975 3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch 976 den Kostenträger

977 Die Regelungen zum Widerspruch oder die Rücknahme des Widerspruchs gegen das
978 Einstellen von Abrechnungsdaten des Kostenträgers in die ePA sind durch den Anbieter

979 der ePA eigenständig im Rahmen der gesetzlichen Vorgaben umzusetzen und sind nicht
980 Bestandteil dieser Spezifikation.

981 3.1.2 Lebenszyklus und Zustände eines Aktenkontos

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

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

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

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

SUSPENDED	Die Daten des Aktenkontos des Versicherten werden zu einem neuen Anbieter übertragen. Die Nutzung des Aktenkontos ist in diesem Zustand nicht möglich.	Erfolgreicher Abschluss des Umzugs Widerspruch gegen die Nutzung der ePA	Unknown
		Der Bereitstellungszeitraum des Exportpakets ist abgelaufen.	Activated

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

992 3.1.3 Anlage eines neuen Aktenkontos

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

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

999 Bei der Initialisierung wird ein neues Aktenkonto bei einem Betreiber eines ePA-
1000 Aktensystems für den Versicherten angelegt und die Dienste des Aktenkontos für die
1001 Nutzung vorbereitet. Die Identifikation eines Aktenkontos erfolgt dabei über die KVNR
1002 des Versicherten (unveränderlicher Anteil der Versichertennummer) im Aktensystem und
1003 gegenüber Clients bei Nutzung der ePA.

1004 **A_24336 -Anbieter ePA-Aktensystem - Identifizierung eines Aktenkontos**

1005 Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos die
1006 KVNR des Versicherten zur Identifikation des Aktenkontos im Aktensystem verwenden
1007 und sicherstellen, dass diese Identifikation eines Aktenkontos nicht verändert werden
1008 kann.[<=]

1009 **A_23775 -Anbieter ePA-Aktensystem - Neues Aktenkonto anlegen**

1010 Der Anbieter des ePA-Aktensystems MUSS für Versicherte jeweils ein Aktenkonto
1011 anlegen, wenn kein Widerspruch des Versicherten gegen die Nutzung der ePA vorliegt,
1012 und dabei die KVNR des Versicherten zur Identifikation eines Aktenkontos im Aktenkonto
1013 registrieren. Das initialisierte Aktenkonto MUSS den Status INITIALIZED erhalten.[<=]

1014 Wechselt der Versicherte den Anbieter, so kann ein Widerspruch des Versicherten gegen
1015 die Nutzung der ePA auch bei diesem bisherigen schon vorliegen. In diesem Fall kann die
1016 Anlage eines Aktenkontos bei einem neuen Anbieter entfallen. Andernfalls kann bei dem
1017 bisherigen Anbieter ein Aktenkonto existieren, dessen Daten im Rahmen der Anlage eines
1018 Aktenkontos beim neuen Anbieter importiert werden müssen.

1019 **A_27343 -Anbieter ePA-Aktensystem - verpflichtende Prüfung auf Widerspruch gegen die Nutzung der ePA bei einem anderen Anbieter**

1020 Der Anbieter des ePA-Aktensystems MUSS vor der Anlage eines Aktenkontos durch
1021 Verwendung der Operationen der Schnittstelle gemäß [I_Information_Service_Accounts]
1022 prüfen, ob bei einem anderen Anbieter ein Widerspruch des Versicherten gegen die
1023 Nutzung der ePA vorliegt oder ein Aktenkonto des Versicherten existiert.[<=]

1025 **A_24789 -Anbieter ePA-Aktensystem - verpflichtender Import eines existierenden Aktenkontos**

1027 Der Anbieter des ePA-Aktensystems MUSS die Inhalte eines existierenden Aktenkontos in
1028 ein neues, initialisiertes Aktenkonto vor dessen Aktivierung übernehmen. [<=]

1029 **A_24302-01 -Anbieter ePA-Aktensystem - verpflichtende Nutzung der**
1030 **Schnittstelle des Information Service Accounts**

1031 Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos einen
1032 Import der Inhalte eines existierenden Aktenkontos von einem anderen Anbieter durch
1033 Verwendung der Operationen der Schnittstelle gemäß [I_Information_Service_Accounts]
1034 veranlassen. [<=]

1035 Der weitere Import eines existierenden Aktenkontos vor dessen Aktivierung erfolgt unter
1036 Verwendung des Health Record Relocation Service (3.2- Health Record Relocation Service
1037).

1038 **A_24790-01 -Anbieter ePA-Aktensystem - keine unbegründeter Import eines**
1039 **Aktenkontos**

1040 Der Anbieter des ePA-Aktensystems DARF den Import eines existierenden Aktenkontos
1041 von einem anderen Anbieter für Zwecke abweichend der Vorgaben in A_24302-* NICHT
1042 nutzen oder veranlassen. [<=]

1043 **A_15870-02 -Anbieter ePA-Aktensystem - Abbruch bei Nichtverfügbarkeit**
1044 **anderer Anbieter**

1045 Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen,
1046 wenn die Prüfung gemäß A_27343-* mindestens bei einem anderen Anbieters eines ePA-
1047 Aktensystems eine technische Fehlermeldung liefert oder dieser nicht erreichbar ist. [<=]

1048 **A_27344 -Anbieter ePA-Aktensystem - Abbruch bei fehlgeschlagenem Import**

1049 Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen,
1050 wenn ein Import von Daten eines Aktenkontos von einem bisherigen Anbieter erforderlich
1051 ist und dieser nicht erfolgreich abgeschlossen werden kann. [<=]

1052 Hinweis zu A_23744*: Ein Import kann beispielsweise fehlschlagen, wenn
1053 schwerwiegende Fehler bei der Exportpaketerstellung oder bei der Übertragung auftreten
1054 (siehe 3.2- Health Record Relocation Service).

1055 Für die Geräteregistrierung bei Nutzung eines ePA-FdV durch den Versicherten ist eine E-
1056 Mail-Adresse des Versicherten für Bestätigung der Geräteregistrierung erforderlich. Falls
1057 vorhanden, kann diese E-Mail-Adresse bei der Anlage eines Aktenkontos im Device
1058 Management hinterlegt werden. Ansonsten muss eine E-Mail-Adresse bei der ersten
1059 Einrichtung eines ePA-FdV zur Nutzung des Aktenkontos hinterlegt werden. Eine E-Mail-
1060 Adresse muss vor der Übernahme in das Aktensystem validiert sein, beispielsweise durch
1061 Versand eines Bestätigungslink an diese E-Mail-Adresse.

1062 **A_14996-01 -Anbieter ePA-Aktensystem - Manuelle Ergänzung E-Mail-Adresse**

1063 Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten auf geeignetem Weg
1064 ermöglichen, die Registrierung einer E-Mail-Adresse für die Geräteverwaltung auch
1065 nachträglich vorzunehmen. [<=]

1066 **A_14993-02 -Anbieter ePA-Aktensystem - Mailadresse validieren**

1067 Der Anbieter des ePA-Aktensystems MUSS eine Mailadresse

- 1068 • bei der ersten Hinterlegung im Aktensystem,
- 1069 • bei einer Änderung der Mailadresse

1070 auf Gültigkeit hin validieren. [<=]

1071 **A_24369 -Anbieter ePA-Aktensystem - Initialisierung des Aktenkontos**

1072 Der Anbieter des ePA-Aktensystems MUSS die Initialisierung der Bestandteile

- 1073 • Consent Decision Management (initiale Entscheidungen)

- 1074 • Constraint Management (Policies)
- 1075 • Entitlement Management (initiale Befugnisse und Befugnisausschlüsse)
- 1076 • Information Service (initiale Entscheidungen "Versorgungsprozess")
- 1077 • XDS Document Service (statische Aktenkontoinhalte)
- 1078 • Device Management
- 1079 • Authorization Service
- 1080 • Audit Event Service
- 1081 • Medication Service

1082 vor der Aktivierung eines Aktenkontos durchführen. Die genannten Bestandteile MÜSSEN
1083 nach der Aktivierung des Aktenkontos sofort nutzbar sein. [≤]

1084 Im Zustand INITIALIZED obliegt es dem Anbieter, ein Aktenkonto mittels administrativer
1085 Eingriffe in die verschiedenen Bestandteile des Aktensystems und -kontos auf die
1086 Aktivierung vorzubereiten bzw. zu konfigurieren.

1087 **A_26005 -ePA-Aktensystem – Optionale Schnittstelle zum Einbringen von** 1088 **initialen Befugnissen**

1089 Das ePA-Aktensystem KANN eine Schnittstelle für Kostenträger anbieten, über die
1090 Kostenträger die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle
1091 ins ePA-Aktensystem einbringen können. [≤]

1092 **A_26006 -ePA-Aktensystem – Nutzen der optionalen Schnittstelle zum** 1093 **Einbringen von initialen Befugnissen ausschließlich im Status INITIALIZED**

1094 Falls das ePA-Aktensystem eine Schnittstelle für Kostenträger anbietet, über die
1095 Kostenträger die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle
1096 für ein Aktenkonto einbringen können, MUSS das ePA-Aktensystem sicherstellen, dass
1097 diese Schnittstelle ausschließlich genutzt werden kann, wenn sich das Aktenkonto im
1098 Status INITIALIZED befindet.
1099 [≤]

1100 Das Aktenkonto wird nach Abschluss der Initialisierung durch den Anbieter aktiviert und
1101 kann dann durch befugte Nutzer und Nutzergruppen verwendet werden. Eine Aktivierung
1102 erfolgt für den Rollout der ePA Version 3 im Kontext des ePA Go-Live-Termins und zu
1103 späteren, individuellen Zeitpunkten, wenn Versicherte als ePA-Nutzer neu dazu
1104 gekommen (bspw. Widerspruch wird zurückgenommen und ePA wird später angelegt
1105 oder Versicherte Person kommt erstmalig ins Gesundheitssystem im Falle eines Zuzugs
1106 oder eines Neugeborenen).

1107 **A_24335 -Anbieter ePA-Aktensystem - Neues Aktenkonto aktivieren**

1108 Der Anbieter des ePA-Aktensystems MUSS ein neues Aktenkonto nach Abschluss der
1109 Initialisierung aktivieren (Status ACTIVATED), wenn die gesetzliche Widerspruchsfrist
1110 abgelaufen ist. [≤]

1111 **3.1.4 Löschen eines Aktenkontos**

1112 Die Löschung eines Aktenkontos bei einem Anbieter und aller darin enthaltenen Daten
1113 kann in folgenden Situationen erforderlich sein:

- 1114 • Widerspruch des Versicherten gegen die Nutzung der ePA,
- 1115 • nach erfolgreichem Wechsel des Anbieters durch den Versicherten und
1116 abgeschlossener Datenübernahme aus dem bisherigen Aktenkonto,

- 1117 • nach Beendigung des Versicherungsverhältnisses des Versicherten bei seinem
1118 Kostenträger.

1119 Ein Versicherter kann nach der Anlage eines Aktenkontos der grundsätzlichen Nutzung
1120 der ePA widersprechen. Liegt dieser erklärte Widerspruch vor, werden das Aktenkonto
1121 des Versicherten und sämtliche Inhalte durch den Anbieter des Aktenkontos gelöscht.

1122 Bei einem Anbieterwechsel erfolgt die Übernahme der Daten des bisherigen Aktenkontos
1123 zu dem neuen Anbieter. Nach erfolgreichem Abschluss der Datenübernahme in das
1124 Aktenkonto des neuen Anbieters löscht der bisherige Anbieter das Aktenkonto des
1125 Versicherten und alle darin enthaltenen Daten.

1126 Kündigt ein Versicherter das Vertragsverhältnis ohne Übernahme der Daten zu einem
1127 neuen Anbieter, löscht der Anbieter des Aktenkontos des Versicherten nach einer
1128 angemessenen Wartezeit, bzw. nach Ablauf von vorgeschriebenen Bereitstellungs- und
1129 Aufbewahrungszeiträumen, das Aktenkonto und alle darin enthaltenen Daten.

1130 Vor der Ausführung der endgültigen Löschung des Aktenkontos muss es dem
1131 Versicherten ermöglicht werden, die Protokolldaten (auch unter Einbindung der
1132 Ombudsstelle) für seinen eigenen Gebrauch außerhalb des Aktenkontos zu sichern.
1133 Dieses ist nicht erforderlich, wenn das Aktenkonto in Folge eines erfolgreichen Umzugs zu
1134 einem anderen Anbieter geschlossen wird.

1135

1136 **A_25289 -Anbieter ePA-Aktensystem - Löschen des Aktenkontos durch den** 1137 **Kostenträger**

1138 Der Anbieter des ePA-Aktensystems MUSS das Aktenkonto eines Versicherten inklusive
1139 aller enthaltenen Daten löschen (sämtliche Dokumente, Schlüsselmaterial, Protokolle,
1140 Widerspruchsinformation, Befugnisse und Beschränkungen), wenn dies durch den
1141 zuständigen Kostenträger beauftragt wird.[<=]

1142 **3.2 Health Record Relocation Service**

1143 Transfer eines Aktenkontos zu einem neuen Anbieter (Aktenkontoumzug).

1144 Wechselt der Versicherte den Kostenträger bzw. den Anbieter seines Aktenkontos, so
1145 erfolgt der Umzug der Inhalte seines bestehenden Aktenkontos vom bisherigen Anbieter
1146 zu einem neuen Anbieter weitestgehend automatisiert.

1147 Seitens der Aktensysteme werden für einen Aktenkontoumzug zwei Schnittstellen
1148 angeboten: *I_Health_Record_Relocation_Service* zur Nutzung durch die Anbieter (alt und
1149 neu) für den Zugriff auf das Aktenkonto des Versicherten und
1150 *I_Information_Service_Accounts* für die Interaktion der Aktensysteme (alt und neu)
1151 untereinander. Die notwendige Kommunikation der Kassen-Backends mit ihren
1152 Aktensystemen außerhalb der VAU erfolgt dabei in Absprache der Beteiligten und ist nicht
1153 Bestandteil der genannten Schnittstellen.

1154 **A_24786 -Health Record Relocation Service - Realisierung der Schnittstelle** 1155 ***I_Health_Record_Relocation_Service***

1156 Der Health Record Relocation Service MUSS die Operationen der Schnittstelle
1157 *I_Health_Record_Relocation_Service* gemäß [*I_Health_Record_Relocation_Service*]
1158 umsetzen.[<=]

1159 *Hinweis: Zur Schnittstelle I_Information_Service_Accounts siehe 3.15.2- Information*
1160 *Service - Account).*

1161 **A_24821 -Health Record Relocation Service - Suspendierung des Aktenkontos**

1162 Der Health Record Relocation Service MUSS sicherstellen, dass das Aktenkontos für die
1163 Erstellung eines Exportpakets auf den Status SUSPENDED gesetzt wird.[<=]

1164 **A_24827 -Health Record Relocation Service - Reaktivierung des Aktenkontos**

1165 Der Health Record Relocation Service MUSS sicherstellen, dass ein Aktenkonto im Status
1166 SUSPENDED nach einem Abbruch eines Transfers von einem Anbieter zu einem anderen
1167 Anbieter aufgrund eines Fehlers (Datenübertrag ist nicht erfolgt) in den Status
1168 ACTIVATED gesetzt wird.[<=]

1169 **A_25005-03 -Health Record Relocation Service - Daten des Exportpakets**

1170 Der Health Record Relocation Service MUSS sicherstellen, dass alle Daten des
1171 Aktenkontos in das Exportpaket übernommen werden aus:

- 1172 • XDS Document Service
- 1173 • Medication Service
- 1174 • Consent Management
- 1175 • Constraint Management
- 1176 • Audit Event Service
- 1177 • Entitlement Management (außer Befugnisse für Versicherte, E-Rezept-Fachdienst,
1178 Kostenträger, Ombudsstelle und NCPeH (EU-Zugriff)).
- 1179 • E-Mail Management (die E-Mail-Adresse des Aktenkontoinhabers (falls vorhanden)
1180 sowie für alle Vertreter die E-Mail-Adressen, sofern sie die dem exportierenden
1181 Aktensystem bekannt sind).

1182 Bei FHIR Data Services MUSS der Health Record Relocation Service sicherstellen, dass
1183 die jeweilige Resource.id aller FHIR-Instanzen ebenso in das Exportpaket einfließen,
1184 sodass nach einem Import die Identitäten der FHIR-Daten stabil bleiben.
1185 [<=]

1186 *Hinweis: Die Geräteregistrierungen des Versicherten oder der Vertreter werden nicht*
1187 *exportiert. Bei einem neuen Anbieter ist für den Versicherten eine erneute*
1188 *Geräteregistrierung erforderlich.*

1189 **A_25605 -Health_Record_Relocation_Service - Erstellung des Exportpakets**

1190 Der Health Record Relocation Service MUSS sicherstellen, dass das Exportpaket gemäß
1191 der Vorgaben in [HealthRecordMigration] bezüglich der Struktur, der Formate für die
1192 enthaltenen Daten und die Verschlüsselung erfolgt.[<=]

1193 **A_25012 -Health Record Relocation Service - Signatur der Befugnisse**

1194 Der Health Record Relocation Service MUSS sicherstellen, dass die gemäß A_23734-*
1195 signierten Anteile einer Befugnis mit der Signaturidentität ID.FD.SIG (Rolle oid_epa_vau)
1196 signiert werden.[<=]

1197 *Hinweis: Der CMAC einer Befugnis wird nicht ins Export-Paket übernommen.*

1198 **A_25719 -Health Record Relocation Service - JWT der Befugnis im Exportpaket**

1199 Der Health Record Relocation Service MUSS sicherstellen, dass die Befugnisse im
1200 Exportpaket als gültig signierte JWT mit den dargestellten Inhalten abgelegt sind:
1201

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

1202 [**<=**]

1203 Der Wert "ES256" (JWS-Parameters "alg") gilt auch für die Kurve "brainpoolP256r1" (also
1204 nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu
1205 erstellen."

1206 **A_24787-01 -Health Record Relocation Service - Verschlüsselung des** 1207 **Exportpaktes**

1208 Der Health Record Relocation Service MUSS sicherstellen, dass Exportpakete
1209 ausschließlich verschlüsselt für den Download zu einem anderen Betreiber zur Verfügung
1210 stehen. Für die Verschlüsselung MUSS das kryptographische Material des ENC-Zertifikats
1211 verwendet werden, welches mittels der Regel hsm-r7 vom VAU-HSM abgerufen
1212 wurde.[**<=**]

1213 **A_24942 -Health Record Relocation Service – Prüfung Provider ENC Zertifikat**

1214 Der Health Record Relocation Service MUSS das übergebene Provider ENC-Zertifikat
1215 mittels TUC_PKI_018 (OCSP-Graceperiod=12h, PolicyList= oid_fd_enc, professionOID =
1216 oid_epa_vau) prüfen und ungültige Zertifikate mit der Fehlermeldung "
1217 CERTIFICATE_INVALID " ablehnen.[**<=**]

1218 **A_21750 -Health Record Relocation Service – Integritätsschutz Exportpaket**

1219 Der Health Record Relocation Service MUSS das erstellte Exportpaket mit einem "Digest"
1220 HTTP Response Header (<https://tools.ietf.org/html/rfc5843>) als Integritätsschutz
1221 versehen und dabei als Digest Algorithmus SHA-256verwenden.

1222 Beispiel Digest-Header:

1223 Digest: SHA-

1224 256=MWVkmWQxYTRiMzk5MDQ0MzI3NGU5NDEyZTk5OWY1ZGFmNzgyZTJlODYzYjRjYzFh

1225 OTImNTQwYzI2M2QwM2U2MQ==
1226 [`<=`]

1227 **A_15051 -Health Record Relocation Service - Authentisierung gegenüber einem** 1228 **neuen Aktenanbieter**

1229 Der Health Record Relocation Service, welcher das Exportpaket zur Verfügung stellt,
1230 MUSS sich beim Abruf des Exportpakets durch ein anderes ePA-Aktensystem mit der
1231 TLS-Identität `oid_epa_mgmt` und Zertifikatsprofil C.FD.TLS-S authentisieren.
1232 [`<=`]

1233 **A_15048 -Health Record Relocation Service - Authentifizierung des neuen** 1234 **Aktenanbieters**

1235 Der Health Record Relocation Service MUSS den Abruf des Exportpakets durch ein
1236 anderes ePA-Aktensystem ablehnen, wenn sich der abrufende Client nicht als ePA-
1237 Aktensystem in der Rolle `oid_epa_mgmt` in einem TLS-Zertifikat C.FD.TLS-C
1238 authentisiert. [`<=`]

1239 **A_17236 -Health Record Relocation Service - Prüfung der TLS-Zertifikate**

1240 Der Health Record Relocation Service MUSS bei der Authentifizierung eines anderen
1241 Aktensystems beim Abruf des Exportpakets die Prüfung der verwendeten TLS-Zertifikate
1242 entsprechend TUC_PKI_018 durchführen. Zur Prüfung des TLS-Zertifikats C.FD.TLS-S
1243 sind dabei die Parameter `PolicyList=oid_fd_tls_s`, `IntendedKeyUsage=digitalSignature`,
1244 `intendedExtendedKeyUsage=id-kp-serverAuth`, `OCSP-Graceperiod=60 Minuten`, `Offline-`
1245 `Modus=nein` zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD.TLS-C sind dabei die
1246 Parameter `PolicyList=oid_fd_tls_c`, `IntendedKeyUsage=digitalSignature`,
1247 `intendedExtendedKeyUsage=id-kp-clientAuth`, `OCSP-Graceperiod=60 Minuten`, `Offline-`
1248 `Modus=nein` zu verwenden.
1249 [`<=`]

1250 **A_15703 -Health Record Relocation Service - Verfügbarkeit Export-Paket**

1251 Der Health Record Relocation Service MUSS ein erstelltes Export-Paket für maximal
1252 sieben Kalendertage zum Abruf durch einen anderen Anbieter eines ePA-Aktensystems
1253 bereithalten. [`<=`]

1254 **A_21239 -Health Record Relocation Service – Verhalten bei Nichtabholen des** 1255 **Exportpakets**

1256 Der Health Record Relocation Service MUSS nach Ablauf des Bereithaltungszeitraums
1257 entsprechend A_15703* ein erstelltes Export-Paket löschen und den Status des
1258 Aktensystems von `SUSPENDED` auf `ACTIVATED` zurücksetzen. [`<=`]

1259 *Hinweis: siehe dazu auch 3.2.1.7.3- Nicht erfolgter Download oder fehlende*
1260 *Rückmeldung durch den neuen Anbieter*

1261 **A_14905-04 -Health Record Relocation Service – Import des Exportpakets des** 1262 **vorhergehenden Aktenkontos**

1263 Der Health Record Relocation Service MUSS das vom vorhergehenden Anbieter ePA-
1264 Aktensystem des Versicherten bezogene Exportpaket, in das neue
1265 Aktenkonto importieren und dazu:

- 1266 • das Exportpaket mittels des privaten ENC-VAU-Schlüssels des neuen
1267 Betreibers entschlüsseln,
- 1268 • den Digest gemäß A_21750-* prüfen,
- 1269 • die Befugnisse mit Regel "rr5" (siehe `Tab_AS_Entitlement_Registration_Rules` im
1270 Aktensystem) registrieren und
- 1271 • falls `DocumentEntry.originalURI` im Exportpaket vorhanden ist, wird für jedes
1272 Dokument eines `SubmissionSet` der Inhalt von `DocumentEntry.URI` durch den
1273 Inhalt von `DocumentEntry.originalURI` ersetzt. (Hinweis:

1274 DocumentEntry.originalURI darf nicht als eigenständiges Metadatum in die
1275 Registry übernommen werden, da es lediglich dem Transport des Originalwertes
1276 von DocumentEntry.URI aus dem alten Aktensystem dient.

1277 [\leq]

1278 **A_27616 -Health Record Relocation Service - Abbruch des Imports eines**
1279 **Exportpakets**

1280 Der Health Record Relocation Service MUSS den Import eines Exportpakets vollständig
1281 abbrechen, wenn einzelne Elemente des Exportpakets aufgrund konstruktiver oder
1282 inhaltlicher Fehler nicht erfolgreich importiert werden können. Eventuell schon
1283 importierte Elemente desselben Exportpakets MÜSSEN im Falle eines Abbruchs entfernt
1284 werden.[\leq]

1285 *Hinweis: Das exportierende Aktensystem kann über den Abbruch durch ein Incident*
1286 *packageCorrupt benachrichtigt werden.*

1287 *Hinweis: Eine zum Zeitpunkt des Imports eines Exportpaketes zeitlich nicht mehr gültige*
1288 *Befugnis aus dem Exportpaket ist kein Fehler im Sinne der Anforderung und führt nicht*
1289 *zu einem Abbruch. Das importierende Aktensystem kann eine solche Befugnis ignorieren.*

1290 **A_21548-02 -Health Record Relocation Service - Information der Vertreter über**
1291 **neuen FQDN nach Abschluss des Anbieterwechsels**

1292 Der Health Record Relocation Service MUSS sicherstellen, dass alle Vertreter nach
1293 erfolgreichem Import des Exportpakets und somit Abschluss des Anbieterwechsels über
1294 Anbieterwechsel und den Bezeichner des neuen Anbieters des Versicherten informiert
1295 werden, so dass sie in der Lage sind, die erforderliche initiale Anmeldung durchzuführen
1296 und informiert sind, welche Art von personenbezogenen Daten vom Vertreter im Rahmen
1297 der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter
1298 eine Vertreterberechtigung widerrufen kann und gegenüber wem er seine
1299 datenschutzrechtlichen Betroffenenrechte wahrnehmen kann.[\leq]

1300 *Hinweis 1 zu A_21548-*: Für die Benachrichtigung derjenigen Vertreter, die dem*
1301 *importierenden Aktensystem nicht bekannt sind, werden die E-Mail-Adressen aus dem*
1302 *Exportpaket genommen. Für die Benachrichtigung der Vertreter, die dem importierenden*
1303 *Aktensystem bekannt sind, wird die im importierenden Aktensystem hinterlegte E-Mail-*
1304 *Adresse des Vertreters verwendet.*

1305 *Hinweis 2 zu A_21548-*: Der Bezeichner des neuen Anbieters muss dem Wert*
1306 *entsprechen der durch die Operation getProviderList geliefert wird.*

1307 **A_26257 -Health Record Relocation Service - Löschen der im Exportpaket**
1308 **enthaltenen E-Mail-Adressen der Vertreter**

1309 Der Health Record Relocation Service MUSS sicherstellen, dass die im Exportpaket
1310 enthaltenen E-Mail-Adressen von Vertretern ausschließlich zur Information der Vertreter
1311 gemäß A_21548-* genutzt werden und nach Abschluss des Anbieterwechsels im
1312 importierenden Aktensystem gelöscht werden, d.h. nicht im importierenden Aktensystem
1313 gespeichert werden.[\leq]

1314 **A_24788 -Health Record Relocation Service - Löschen des Exportpakets nach**
1315 **Umgang des Aktenkontos**

1316 Das Aktensystem MUSS sicherstellen, dass ein vorhandenes Exportpaket nach einem
1317 erfolgreichen Transfer eines Aktenkontos eines Versicherten von einem Anbieter zu
1318 einem anderen Anbieter gelöscht wird.[\leq]

1319 **A_24982-02 -Health Record Relocation Service – Protokollierung des**
1320 **Anbieterwechsels eines Aktenkontos**

1321 Der Health Record Relocation Service des neuen (importierenden) Aktensystems MUSS
1322 nach der erfolgreichen oder einer abgebrochenen Übertragung der Inhalte eines

1323 Aktenkontos vom bisherigen Anbieter einen Protokolleintrag gemäß A_24704* erzeugen.
 1324 Dabei ist folgende Wertebelegung zu berücksichtigen:

1325 **Tabelle 3 : Health Record Relocation Service Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"object"		
AuditEvent.action	E		Übertrag von Daten eines Aktenkontos von einem anderen Anbieter
AuditEvent.agent.type	PAYOR		Umzug wurde ausgelöst vom Kostenträger.
AuditEvent.entity.name	"HealthRecordRelocation"		
AuditEvent.entity.detail	type	value[x]	
	"OriginName"	<Name des Kostenträgers>	Name des Kostenträgers, von welchem ein bestehendes Aktenkonto übernommen wird

1326 [**<=**]

1327

1328 *Hinweis: Das Aktensystem des bisherigen Anbieters muss keinen Protokolleintrag gemäß*
 1329 *A_24982* erzeugen.*

1330 **3.2.1 Ablauf eines Aktenkontoumzugs**

1331 **3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter**

1332 Der Anbieter (neu) lässt im Aktensystem (neu) ein neues Aktenkonto anlegen. Dieses
 1333 erhält den Status INITIALIZED. Hierfür gelten die Anforderungen gemäß 3.1.3- Anlage
 1334 eines neuen Aktenkontos.

1335 Falls der Versicherte schon einen Widerspruch gegen die Nutzung der ePA bei seinem
 1336 bisherigen Kostenträger erklärt hat, kann die Initialisierung eines neuen Aktenkontos ggf.
 1337 entfallen. Ein Transfer, bzw. die Erstellung eines Exportpakets, ist in diesem Fall mangels
 1338 eines existierenden Aktenkontos beim bisherigen Anbieter nicht erforderlich.

1339 Die Abfrage eines existierenden Widerspruchs des Versicherten bei einem anderen
 1340 Anbieter ePA-Aktensystem erfolgt über dessen Information Service.

Abfrage eines existierenden Widerspruchs gegen die Nutzung der ePA

I_Information_Service_Accounts (bisheriges Aktensystem)

getGeneralConsentDecision

Abfrage des ggf. schon erteilten Widerspruchs gegen die Nutzung der ePA durch den Versicherten

1341 **3.2.1.2 Start Transfer eines existierenden Aktenkontos**

1342 Hat der Versicherte bei keinem Anbieter einen Widerspruch gegen die Nutzung der ePA
1343 erklärt und existiert bei einem bisherigen Anbieter (alt) ein Aktenkonto, wird der Transfer
1344 der Daten durch das Aktensystem (neu) initiiert.

1345 Das Aktensystem (alt), bei welchem das Aktenkonto existiert, bestätigt diese Anfrage
1346 zum Transfer mit einer Vorgangs-ID.

Starten des Transfers

I_Information_Service_Accounts (bisheriges Aktensystem)

startRelocation

initiiieren der Exportpaketerstellung

1347 **3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen** 1348 **Anbieter**

1349 Das Aktensystem (alt) informiert den Anbieter (alt) über die Anfrage zum Transfer und
1350 die Vorgangsnummer. Der Anbieter (alt) öffnet das existierende Aktenkonto des
1351 Versicherten und stößt in der VAU die Erzeugung des Exportpakets an. Der Health Record
1352 Relocation Service beantwortet diese Anfrage durch Rückgabe einer URL für den späteren
1353 Download des Exportpakets durch den neuen Anbieter und startet die Erzeugung des
1354 Exportpakets. Das Aktenkonto wird vor der Paketerstellung auf den Status SUSPENDED
1355 gesetzt, um weitere Aktivitäten seitens der Nutzer zu verhindern.

Erzeugen des Exportpakets

I_Health_Record_Relocation_Service_ (bisheriger Anbieter)

startPackageCreation

Starten der Erzeugung des Exportpakets in der VAU

1356 In dieses Exportpaket werden alle Daten des Aktenkontos gemäß A_25005*
1357 übernommen. Das fertige Exportpaket wird mittels ENC-Zertifikat, welches im VAU-HSM
1358 eingebracht und gespeichert wurde, verschlüsselt und am vorbereiteten Downloadpunkt
1359 bereitgestellt.

1360 **3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den** 1361 **neuen Anbieter**

1362 Der Anbieter (alt) veranlasst nach Erhalt der Download-URL über das Aktensystem (alt)
1363 den Versand der Url an das Aktensystem (neu).

1364 Das Aktensystem (alt) prüft vor der Übermittlung der Download-URL an das Aktensystem
1365 (neu), ob das Exportpaket für den Download bereitsteht, ggf. wird auf den Abschluss der

- 1366 Paketerstellung gewartet. Ist dieses der Fall, erfolgt die Benachrichtigung des
1367 Information_Service des Aktensystem (neu) mit der Übergabe der URL

Übergabe der Download-URL für das Exportpaket

I_Information_Service_Accounts (neues Aktensystem)

putDownloadUrlForExportPackage	Übergabe der geprüften Download-URL
--------------------------------	-------------------------------------

1368 **3.2.1.5 Import des Exportpakets durch den neuen Anbieter**

- 1369 Der Information Service des Aktensystems (neu) nimmt die Download-URL entgegen und
1370 übermittelt diese an den Kostenträger (neu). Dieser öffnet den Zugang zum Aktenkonto
1371 (neu) des Versicherten und veranlasst in der VAU den Import des Exportpakets.

Import und Integration des Exportpakets

I_Health_Record_Relocation_Service (neuer Anbieter)

startPackageImport	Starten des Imports der vorhandenen Daten
--------------------	---

1372 **3.2.1.6 Abschluss des Transfers durch beide Anbieter**

- 1373 Das Aktensystem (neu) startet den Download des Exportpakets, entschlüsselt dieses und
1374 übernimmt die Daten in das initialisierte Aktenkonto des Versicherten. Nach
1375 erfolgreichem Abschluss wird (kann) das Aktenkonto (neu) in den Status ACTIVATED
1376 überführt werden.

- 1377 Unter Verwendung des Information Service wird das Aktensystem (alt) über den
1378 erfolgreichen Import und den Abschluss des Transfers informiert. Das Aktenkonto (alt)
1379 kann daraufhin, ggf. unter Einhaltung weiterer Bedingungen des Kostenträgers bzw.
1380 gesetzlicher Vorgaben, gelöscht werden (Status = UNKNOWN).

Abschluss des Transfers

I_Information_Service_Accounts (bisheriges Aktensystem)

deleteExportPackage	Beenden des Vorgangs (Löschen Exportpaket und ggf. bisheriges Aktenkonto)
---------------------	---

1381 **3.2.1.7 Fehlersituationen und Handhabung**

- 1382 Der gesamte Austausch von Informationen zwischen Aktensystemen und Anbietern kann
1383 durch die in Schritt 1 erzeugte Vorgangs-ID genau einem konkreten Relocation Vorgang
1384 zugeordnet werden. Diese Vorgangsnummer wird auch verwendet, wenn das jeweils
1385 andere Aktensystem über Fehler im Ablauf benachrichtigt werden muss (Incidents).

- 1386 *3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich oder*
1387 *derzeit nicht möglich*

- 1388 Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter
1389 (alt) das Exportpaket voraussehbar nicht importieren oder widerspricht der Versicherte

1390 nach der Initialisierung des Aktenkontos beim neuen Kostenträger der Nutzung der ePA,
 1391 so kann durch Übertragung eines Incidents an das Aktensystem (alt) dieser Sachverhalt
 1392 mitgeteilt werden, so dass der Transfervorgang abgebrochen und das Exportpaket nicht
 1393 erzeugt oder wieder gelöscht wird.

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

1394 Das Aktenkonto wird bei Anbieter (alt) wieder in den Status ACTIVATED gesetzt, um eine
 1395 weitere Nutzung zu ermöglichen.

1396 Für einen Transfer zu einem späteren Zeitpunkt muss der Anbieter (neu) den Vorgang
 1397 durch Anfrage bei den weiteren Anbietern (alt) und Übermittlung eines ENC-Zertifikats
 1398 erneut starten.

1399 3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter

1400 Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter
 1401 (alt) das Exportpaket unter Verwendung der übertragenen Download-URL nicht oder
 1402 nicht vollständig laden oder die Inhalte des Exportpaketes aufgrund fehlerhafter
 1403 Verschlüsselung oder fehlerhafter Struktur oder Inhalte nicht erfolgreich integrieren oder
 1404 der Anbieter (neu) hat keine Download-URL vom Anbieter (alt) bezogen, so kann durch
 1405 Übertragung eines Incidents an den Anbieter (alt) dieser Sachverhalt mitgeteilt werden.

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

1406 Das Aktenkonto verbleibt beim neuen Anbieter in Status INITIALIZED. Die
 1407 Incidentmeldung an den Anbieter (alt) kann durch Kommunikation der Anbieter und/oder
 1408 Betreiber untereinander zum Zweck der Problemlösung ergänzt werden.

1409 Der Anbieter (alt) meldet die Korrektur durch erneuten Versand einer Download-URL an
 1410 den Anbieter (neu) für den unterbrochenen Vorgang.

1411 Es obliegt dem Anbieter (alt), bei zeitlich aufwendigen Korrekturen das Aktenkonto
 1412 zunächst für eine weitere Nutzung wieder zu aktivieren (Status ACTIVATED) und nach
 1413 Abschluss der Korrektur wieder in den Status SUSPENDED zu überführen.

1414 Es obliegt dem Anbieter (alt) auch, bei zeitlich aufwendigen Korrekturen den Transfer
 1415 durch Senden des Incidents "relocationAborted" an den Anbieter (neu) abubrechen und
 1416 das Aktenkonto zur weiteren Nutzung wieder zu aktivieren (Status ACTIVATED). Der
 1417 Transfer muss dann durch den Anbieter (neu) erneut gestartet werden.

1418 3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter

1419 Ruft ein neuer Anbieter ein bereitgestelltes Exportpaket nicht ab oder erfolgt durch den
 1420 neuen Anbieter keine Benachrichtigung über einen erfolgreichen Abschluss des Transfers
 1421 oder einen Fehler beim Import des Exportpakets, dann kann eine Benachrichtigung an
 1422 den neuen Anbieter erfolgen.

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

1423 Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei
 1424 Anbieter (alt) auf den Status ACTIVATED gesetzt, um eine weitere Nutzung zu
 1425 ermöglichen. Exportpaket und Downloadlink können gelöscht werden. Der Transfer muss
 1426 durch den Anbieter (neu) erneut gestartet werden.

1427 3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter

1428 Ein Anbieter (alt) kann den Abbruch eines angeforderten Transfers an den Anbieter (neu)
 1429 signalisieren.

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

1430 Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei
 1431 Anbieter (alt) auf den Status ACTIVATED zurückgesetzt, wenn dieses schon den Status
 1432 SUSPENDED hat, um eine weitere Nutzung zu ermöglichen. Exportpaket und
 1433 Downloadlink können gelöscht werden. Der Transfer muss durch den Anbieter (neu)
 1434 erneut gestartet werden.

3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM

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

Verständnishinweis: Die HMAC-Schlüssel (symmetrische Schlüssel) für die Prüfung der VSDM+-Prüfnachweise [gemSpec_SST_FD_VSDM], [C_11321] werden von den VSDM-Betreibern erzeugt und für die ePA-VAUs der ePA-Betreiber verschlüsselt exportiert. Die Schlüssel und auch die Export/Import-Vorgänge (Mehr-Augen-Prinzip) sind die gleichen wie sie auch für/bei der E-Rezept-VAU verwendet werden.

A_24611-06 -ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und Informationen für VAU-Betrieb

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

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

[<=]

Hinweis:

Es gelten die Anforderungen aus [gemSpec_Krypt#3.18 VSDM-Prüfziffer Version 2] für ein ePA-Aktensystem in der Rolle "Prüfziffer Version 2 prüfendes System". Aus den ins

1478 HSM importierten gemeinsamen Geheimnissen erfolgt im HSM eine Schlüsselableitung
1479 (A_27299-*) der für die Entschlüsselung der Prüfziffer Version 2 benötigten AES/GCM-
1480 Schlüssel.

1481 **A_26109 -ePA-Aktensystem - Unterschiedliche private**

1482 **Authentisierungsschlüssel für AK-, Befugnisverifikations- und Service-VAU**

1483 Das ePA-Aktensystem MUSS sicherstellen, dass für die Authentisierungsidentitäten für
1484 Aktenkontoverwaltungs-VAUs, Befugnisverifikations-VAUs und Service-VAUs
1485 unterschiedliche private Schlüssel verwendet werden. [\leq]

1486 **A_26110 -ePA-Aktensystem - Unterschiedliche private**

1487 **Authentisierungsschlüssel für unterschiedliche Service-VAUs**

1488 Das ePA-Aktensystem MUSS sicherstellen, dass für unterschiedliche Typen von Service-
1489 VAUs unterschiedliche private Schlüssel für die Authentisierung genutzt werden. [\leq]

1490 Hinweis zu A_26110: Ein Typ einer Service-VAU könnte beispielsweise eine PDF-
1491 Konvertierungs-Service-VAU oder eine Pseudonymisierungs-Service-VAU für Daten zur
1492 Sekundärnutzung sein. Alle Instanzen einer PDF-Konvertierungs-Service-VAU nutzen
1493 denselben privaten Authentisierungsschlüssel. Die Instanzen der Pseudonymisierungs-
1494 Service-VAU dürfen den Authentisierungsschlüssel der PDF-Konvertierungs-Service-VAU
1495 jedoch nicht verwenden.

1496 **A_24612-05 -ePA-Aktensystem - Erzwingen von 4-Augen-Prinzip für Einbringen**
1497 **und Verwalten von Informationen ins VAU-HSM**

1498 Das ePA-Aktensystem MUSS technisch erzwingen, dass die folgenden, für den Betrieb der
1499 VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip in das
1500 VAU-HSM eingebracht und verwaltet werden können:

- 1501 • privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- 1502 • ggf. privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- 1503 • ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- 1504 • privater Schlüssel der Verschlüsselungsidentität der VAU
- 1505 • privater Schlüssel der Signaturidentität der VAU
- 1506 • Zertifikat C.FD.ENC mit professionOID oid_epa_vau für die
- 1507 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- 1508 • Zertifikat C.ZD.SIG mit professionOID oid_popp-token für die Token-Signatur-
- 1509 Identität des PoPP-Services
- 1510 • symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-
- 1511 Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames
- 1512 Geheimnis bezeichnet werden.
- 1513 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- 1514 • Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für
- 1515 die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf.
- 1516 für Service-VAUs)
- 1517 • Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

1518 [\leq]

1519 **A_24614-05 -ePA-Aktensystem - Einbringung von Informationen ins VAU-HSM**
1520 **im 4-Augen-Prinzip mit der gematik**

1521 Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die folgenden, für den
1522 Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-

1523 Prinzip ins VAU-HSM eingebracht und im VAU-HSM verwaltet werden, bei dem eine von
1524 der gematik benannte Person beteiligt ist:

- 1525 • privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- 1526 • ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- 1527 • ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- 1528 • privater Schlüssel der Verschlüsselungsidentität der VAU
- 1529 • privater Schlüssel der Signaturidentität der VAU
- 1530 • Zertifikat C.FD.ENC mit professionOID `oid_epa_vau` für die
- 1531 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- 1532 • Zertifikat C.ZD.SIG mit professionOID `oid_popp-token` für die Token-Signatur-
- 1533 Identität des PoPP-Services
- 1534 • symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-
- 1535 Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames
- 1536 Geheimnis bezeichnet werden.
- 1537 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- 1538 • Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für
- 1539 die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf.
- 1540 für Service-VAUs)
- 1541 • Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

1542 [**<=**]

1543 Beim Einbringen der Hashwertrepräsentation der erlaubten VAU-Software ins VAU-HSM
1544 prüft die von der gematik benannte Person, dass die Hashwertrepräsentation des VAU-
1545 Images zuvor vom Hersteller des ePA-Aktensystems an die gematik übermittelt wurde
1546 und zulässig für den Produktivbetrieb ist.

1547 Die von der gematik benannte Person prüft, dass das Zertifikat für die Token-Signatur-
1548 Identität des PoPP-Services gültig ist und die geforderten Inhalte enthält (Zertifikatsprofil
1549 `oid_zd_sig` (OID 1.2.276.0.76.4.287, "C.ZD.SIG"), technische Rolle `oid_popp-token` (OID
1550 1.2.276.0.76.4.320)).

1551 **A_24618-05 -ePA-Aktensystem - Zugriff auf Schlüssel und Informationen im** 1552 **VAU-HSM**

1553 Das ePA-Aktensystem MUSS sicherstellen, dass auf die folgenden, für den Betrieb der
1554 VAU notwendigen und im VAU-HSM gespeicherten Schlüssel und Informationen
1555 ausschließlich über attestierte VAU-Instanzen zugegriffen werden kann:

- 1556 • privater Schlüssel der Authentisierungsidentität der VAUausschließlich durch eine
1557 Aktenkontoverwaltungs-VAU-Instanz
- 1558 • privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
1559 ausschließlich durch eine Befugnisverifikations-VAU-Instanz
- 1560 • privater Schlüssel der Authentisierungsidentität eines Service-VAU-Typs
1561 ausschließlich durch eine Service-VAU-Instanz dieses Service-VAU-Typs
- 1562 • privater Schlüssel der Verschlüsselungsidentität der VAUausschließlich durch eine
1563 Aktenkontoverwaltungs-VAU-Instanz
- 1564 • privater Schlüssel der Signaturidentität der VAUausschließlich durch eine
1565 Aktenkontoverwaltungs-VAU-Instanz

- 1566 • Zertifikat C.FD.ENC mit professionOID `oid_epa_vau` für die
1567 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibersausschließlich
1568 durch eine Aktenkontoverwaltungs-VAU-Instanz
- 1569 • Zertifikat C.ZD.SIG mit professionOID `oid_popp-token` für die Token-Signatur-
1570 Identität des PoPP-Services
- 1571 • Masterkeys für die Ableitung der versichertenindividuellen
1572 Datenpersistierungsschlüsselausschließlich durch eine Aktenkontoverwaltungs-
1573 VAU-Instanz
- 1574 • Masterkeys für die Ableitung der versichertenindividuellen
1575 Befugnispersistierungsschlüsselausschließlich durch eine Aktenkontoverwaltungs-
1576 VAU-Instanz
- 1577 • Masterkeys für die Ableitung der versichertenindividuellen
1578 Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und
1579 Überschlüsselung") ausschließlich durch die Aktenkontoverwaltungs-VAU-Instanz
1580 oder durch eine dedizierte Überschlüsselungs-VAU
- 1581 • symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-
1582 Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames
1583 Geheimnis bezeichnet werden,ausschließlich durch eine Aktenkontoverwaltungs-
1584 VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz
- 1585 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten
1586 Befugnisse)ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder
1587 eine Befugnisverifikations-VAU-Instanz.

1588 [\leq]

1589 3.4 Befugnisverifikations-Modul

1590 Das Befugnisverifikations-Modul enthält die Regeln zur Befugnisregistrierung (entitlement
1591 registration rules) und die Regeln zum Abruf der versichertenindividuellen
1592 Persistierungsschlüssel (key rules).

1593 Die folgende Abbildung zeigt die zwei möglichen Architekturvarianten für die Ausführung
1594 des Befugnisverifikations-Moduls. In Variante 1 wird es direkt im VAU-HSM ausgeführt. In
1595 Variante 2 wird es in einer Befugnisverifikations-VAU ausgeführt, die zwischen einer
1596 Aktenkontoverwaltungs-VAU und einem VAU-HSM vermittelt und Prüfungen für das VAU-
1597 HSM übernimmt (z. B. prüfen der ID-Token oder registrieren neuer Befugnisse).

1598 In beiden Varianten ist ein Zugriff auf die Schlüssel im VAU-HSM nur durch integrale und
1599 attestierte VAUs möglich. Die Prüfung der VAU-Attestierungstoken verbleibt in beiden
1600 Varianten im VAU-HSM (VAU-Token-Modul). Das VAU-HSM speichert in Variante 2 neben
1601 den Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware
1602 für die VAU der Aktenkontoverwaltung zusätzlich auch die Hashwertrepräsentationen der
1603 erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der
1604 Befugnisverifikations-VAU. Ein Zugriff auf das HSM ist dann nur mit einem validen
1605 Attestierungstoken für die Aktenkontoverwaltung-VAU und die Befugnisverifikations-VAU
1606 möglich.

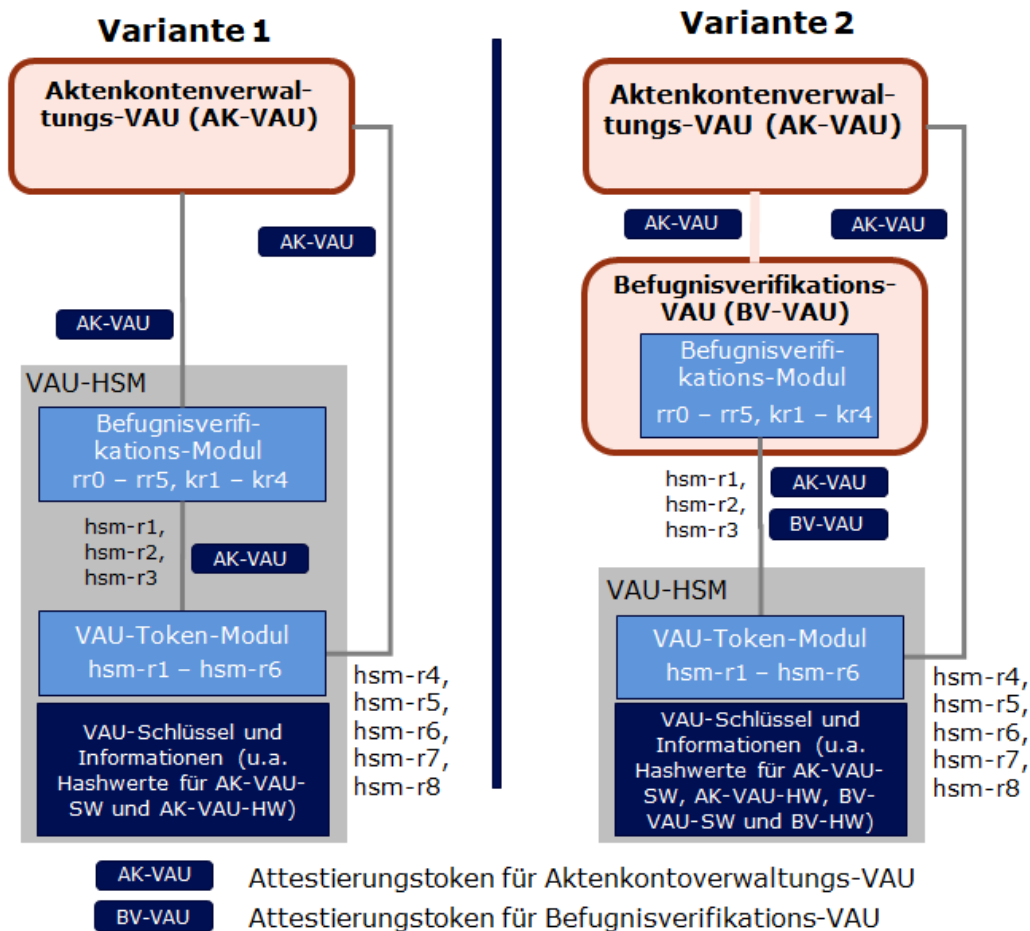


Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls

A_25281 -ePA-Aktensystem - VAU-Token-Modul ausschließlich im HSM

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

A_24574 -ePA-Aktensystem - Befugnisverifikations-Modul im HSM oder Befugnisverifikations-VAU

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

A_25050 -ePA-Aktensystem - 1:1-Beziehung zwischen Befugnisverifikations-VAU und Aktenkontoverwaltungs-VAU

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

3.4.1 VAU-Token-Modul

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

A_24712-01 -ePA-Aktensystem - VAU-Token-Modul nur durch

Befugnisverifikations-Modul oder Aktenkontoverwaltungs-VAU aufrufbar

1627 Das ePA-Aktensystem MUSS sicherstellen, dass die Regeln hsm-r1 bis hsm-r3 des VAU-
 1628 Token-Moduls ausschließlich von einem Befugnisverifikations-Modul und die Regeln hsm-
 1629 r4 bis hsm-r7 ausschließlich von einer Aktenkontoverwaltungs-VAU aufgerufen
 1630 werden.[<=]

1631 **A_25282-02 -ePA-Aktensystem - Regeln des VAU-Token-Moduls**

1632 Das VAU-Token-Modul MUSS die in Tabelle *Tab_AS_VAU-Token-Modul_Rules* definierten
 1633 Regeln umsetzen.[<=]

1634

1635 **Tabelle 4: Tab_AS_VAU-Token-Modul_Rules -Prüfregeln VAU Token**

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

	<p>Datenpersistierungsschlüssel</p> <p>Prüfschritte:</p> <ol style="list-style-type: none"> 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 <p>Falls die Prüfungen 1) - 3) erfolgreich waren, wird der angeforderte versichertenindividuelle Befugnispersistierungsschlüssel und/oder versichertenindividuelle Datenpersistierungsschlüssel für die übergebene KVNR von den durch die Label identifizierten Masterkeys abgeleitet.</p>
hsm-r3	<p><i>Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfziffern der Version 1 oder der Entschlüsselung der VSDM-Prüfziffern der Version 2</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) • Szenario VSDM-Prüfziffer Version 1 <ul style="list-style-type: none"> • Daten • Bezeichner des HMAC-Schlüssels • Szenario VSDM-Prüfziffer Version 2 <ul style="list-style-type: none"> • VSDM-Prüfziffer in Version 2 <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • 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 erfolgreichen Entschlüsselung <p>Prüfschritte:</p> <ol style="list-style-type: none"> 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 <p>Szenario VSDM-Prüfziffer Version 1: Falls die Prüfungen 1) - 3) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.</p>

	<p>Szenario VSDM-Prüfziffer Version 2: Falls die Prüfungen 1) - 3) erfolgreich waren, wird die VSDM-Prüfziffer gemäß den Prüfschritten 4. und 5. aus A_27279-* geprüft und entschlüsselt. Bei erfolgreicher Entschlüsselung der VSDM-Prüfziffer wird die innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) zurückgeliefert, ansonsten ein Fehler.</p>
hsm-r4	<p><i>Diese Regel dient zur Nutzung der privaten Schlüssel der AUT-Identitäten der VAU</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • Challenge • [VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU] VAU-Attestierungstoken einer Befugnisverifikations-VAU] VAU-Attestierungstoken eines Service-VAU-Typs] <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Challenge signiert mit privatem Schlüssel der AUT-Identität <ul style="list-style-type: none"> • 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. <p>Prüfschritte</p> <ol style="list-style-type: none"> 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. <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, wird die übergebene Challenge mit dem privatem Schlüssel der zum VAU-Attestierungstoken gehörenden AUT-Identität signiert.</p>
hsm-r5	<p><i>Diese Regel dient zur Nutzung des privaten Schlüssels der ENC-Identität der VAU</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • verschlüsselte Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • entschlüsselte Daten <p>Prüfschritte</p> <ol style="list-style-type: none"> 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. <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen verschlüsselten Daten mit dem privatem Schlüssel der ENC-Identität der VAU entschlüsselt.</p>

hsm-r6	<p><i>Diese Regel dient zur Nutzung des privaten Schlüssels der Signaturidentität der VAU</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • zu signierende Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • signierte Daten <p>Prüfschritte</p> <ol style="list-style-type: none"> 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 <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen Daten mit dem privaten Schlüssel der Signaturidentität der VAU signiert.</p>
hsm-r7	<p><i>Diese Regel dient zum Auslesen des ENC-Zertifikats des anderen Aktensystembetreibers.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Verschlüsselungszertifikat C.FD.ENC des anderen Aktensystembetreibers <p>Prüfschritte:</p> <ol style="list-style-type: none"> 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 <p>Falls die Prüfungen 1) - 2) erfolgreich waren, wird das ENC-Zertifikat des anderen Aktensystembetreibers zurückgeliefert.</p>
hsm-r8	<p>Diese Regel dient zum Ableiten von symmetrischen Schlüsseln für die Ver- bzw. Entschlüsselung von Daten</p> <p>Sie dient bspw. dazu, sogenannte Submissions für die Datenausleitung an das Forschungsdatenzentrum Gesundheit (FDZ) nach § 363 Absatz 1 SGB V außerhalb der VAU im Aktensystem zwischenspeichern, bis das Forschungsdatenzentrum diese Submissions abholt. Die Submissions sind dann über die über diese Regel abgeleiteten symmetrischen Schlüssel außerhalb der VAU kryptographisch gesichert.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder einer Service-VAU • Ableitungsvektor <i>dv</i> • Label für Masterkey (opt.) <p>Ausgangsdaten:</p>

	<ul style="list-style-type: none"> • <i>symmetrischer Schlüssel symKey</i> • <i>Label für Befugnis-Masterkey</i> <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. <i>prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</i> 2. <i>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</i> 3. <i>falls ein Label für einen Masterkey In den Eingangsdaten enthalten ist, prüfen, ob das Label zu einem Befugnis-Masterkey gehört</i> <p>Falls alle Prüfungen erfolgreich waren, wird symKey wie folgt abgeleitet:</p> <p>Fall: Eingangsdaten enthalten ein Label mkey_label für einen Befugnis-Masterkey: Ableitung eines AES-Schlüssels [FIPS-197] symKey mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren auf Basis des Befugnis-Masterkeys mit Label mkey_label und dem Ableitungsvektor "eds: "+ dv. Ausgangsdaten sind der abgeleitete Schlüssel symKey und das Label mkey_label.</p> <p>(Verständnishinweis: eds steht für "External Data Storage". Das HSM erzwingt bei dieser Regeln, dass das Präfix "eds: " (also 5 Byte) dem vom Aufrufer übergebenen Ableitungsvektor (dv) vorangestellt wird.)</p> <p>Fall: Eingangsdaten enthalten kein Label für einen Befugnis-Masterkey: Ableitung eines AES-Schlüssels [FIPS-197] symKey mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#Abschnitt 2.4] zulässigen Verfahren auf Basis des aktuellen Befugnis-Masterkeys und dem Ableitungsvektor "eds: " + dv. Ausgangsdaten sind der abgeleitete Schlüssel symKey und das Label des aktuellen Befugnis-Masterkeys.</p>
--	---

1636

1637 **A_24667 -ePA-Aktensystem -VAU-HSM - Prüfen des VAU-Attestierungstokens**
 1638 Das VAU-HSM MUSS bei der Prüfung eines VAU-Attestierungstokens sicherstellen, dass
 1639 dieses zeitlich gültig ist und Replay-Attacken abwehren. [**<=**]

1640 **A_26303 -ePA-Aktensystem - Abgeleitete Verschlüsselungsschlüssel sind**
 1641 **ausschließlich einer VAU zugänglich**

1642 Das ePA-Aktensystem MUSS sicherstellen, dass ein mit Regel hsm-r8 abgeleiteter
 1643 Schlüssel ausschließlich einer VAU zugänglich ist und ausschließlich mittels AES/GCM
 1644 analog [gemSpec_Krypt#GS-A_4389] verwendet wird. [**<=**]

1645 3.4.2 Regeln des Befugnisverifikations-Moduls

1646 Die folgende Tabelle zeigt die Regeln des Befugnisverifikations-Moduls im Überblick.

1647 **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	<i>Tab_AS_Entitlement_Registration_Rules</i>

	HSM-ID-Token konvertiert.	
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 Leistungserbringenumgebung 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>
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	<i>Tab_AS_SDS-Key_Rules</i>

	wurde.	
kr4	Diese Regel wird für die Anmeldung des E-Rezept-Fachdienstes verwendet.	<i>Tab_AS_SDS-Key_Rules</i>
kr5	Diese Regel wird für die Überschlüsselung (ggf. mit Umschlüsselung einer Überschlüsselung) verwendet.	<i>Tab_AS_SDS-Key_Rules</i>

1648

1649 **A_24573-03 -ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls**

1650 Das Befugnisverifikations-Modul MUSS die in den
 1651 Tabellen *Tab_AS_Entitlement_Registration_Rules* und *Tab_AS_SDS-Key_Rules* definierten
 1652 Regeln umsetzen. [<=]

1653 **Tabelle 6: Tab_AS_Entitlement_Registration_Rules - Regeln zur Registrierung von**
 1654 **Befugnissen**

Regel	Beschreibung
rr0	<p>Mit dieser Regel werden ID-Token im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token mit NutzerID=x signiert durch einen sektoralen Identity Provider, den IDP-Dienst oder den E-Rezept-Fachdienst <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • HSM-ID-Token mit NutzerID=x gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (C.FD.SIG) bei Token eines IDPs bzw. gemäß A_24658-* bei Token des E-Rezept-Fachdienstes (C.FD.AUT). 2. Falls die Prüfung in 1) erfolgreich war, <ol style="list-style-type: none"> a. erstellt das Befugnisverifikations-Modul ein HSM-ID-Token mit der NutzerID=x, einer Gültigkeitsdauer von 24 Stunden und der professionOID aus dem Signaturzertifikat (<code>oid_idpd_sek</code>, <code>oid_idpd</code> oder <code>oid_erp-vau</code>). b. ruft das Befugnisverifikations-Modul die VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und dem HSM-ID-Token auf. <ol style="list-style-type: none"> 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	<p>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.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Befugnis1 = (KVN- Aktenkonto, Telematik-ID oder KVN, Gültigkeitszeitraum) signiert vom Versicherten <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis2 = (KVN- Aktenkonto, Telematik-ID oder KVN, Gültigkeitszeitraum) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist b. prüfen, ob die KVN im ID-Token mit der KVN im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt oder prüfen des HSM-ID-Tokens <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> 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 KVN im HSM-ID-Token mit der KVN im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt. 2. prüfen der Befugnis1 <ol style="list-style-type: none"> 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 KVN im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der "KVN- 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: Für eine Befugnis1 mit <code>oid = oid_ncpeh</code> wird die Gültigkeit <code>validTo</code> in Befugnis2 auf <code>aktuelle Zeit + 1 Stunde</code> gesetzt.

	<p>4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis2</p> <p>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> <p>5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.</p>
rr2	<p><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 Signaturdienst signiert.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • 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 <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis3 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist 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 <ol style="list-style-type: none"> Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens <ol style="list-style-type: none"> Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt. prüfen der Befugnis1 und Befugnis2 <ol style="list-style-type: none"> prüfen der Signatur von Befugnis1 gemäß A_25042-* (Zertifikatsprofil C.CH.SIG) prüfen, ob die professionOID im Signaturzertifikat <code>oid_versicherter</code> ist

	<ul style="list-style-type: none"> c. prüfen des CMAC von Befugnis2 d. prüfen, dass die Telematik-ID in Befugnis 1 keine KVNR ist (Vertreter dürfen keine weiteren Vertreter befugen) e. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der „KVNR Vertreter“ in der Befugnis2 übereinstimmt f. prüfen, ob die „KVNR Aktenkonto“ in Befugnis 1 mit der „KVNR Aktenkonto“ in Befugnis2 übereinstimmt g. prüfen, dass das JWT gemäß A_24587-* zeitlich gültig ist ($i_{at} - 15s \leq \text{aktuelle Zeit} < e_{xp} + 15s$) <ol style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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	<p>Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das Stecken der eGK in einer Leistungserbringenumgebung oder aufgrund eines PoPP-Tokens ergeben.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VSDM-Prüfziffer in Version 2 signiert mit AUT-Identität der SMC-B oder signiertes PoPP-Token <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • 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) <p>Prüfschritte:</p> <p><u>Szenario VSDM-Prüfziffer in Version 2:</u> Falls <code>enforce_popp_only = true</code>, dann FAIL, ansonsten führe die folgenden Prüfschritte durch:</p> <ol style="list-style-type: none"> 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 <ul style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-

	<p>VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> <ol style="list-style-type: none"> prüfen der inneren Struktur nach Prüfschritt 6 gemäß A_27279-* (d.h. eGK ist nicht gesperrt) prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer (prüfziffer.iat) nicht länger als 20 Minuten zurückliegt ($\text{prüfziffer.iat} - 30s \leq \text{aktuelle Zeit} < \text{prüfziffer.iat} + 20 \text{ Minuten} + 15s$, Hinweis in der Prüfziffer gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben) prüfen des prüfziffer.hcv nach Prüfschritt 8 gemäß A_27279-* bzgl. des hcv im JWT 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: <ul style="list-style-type: none"> 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. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis <ol style="list-style-type: none"> 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 Befugnis sowie die entschlüsselte innere Struktur der Prüfziffer im Klartext gemäß A_27278-* als Ergebnis des Regelaufrufs zurück. <p><u>Szenario PoPP-Token:</u></p> <ol style="list-style-type: none"> prüfen des PoPP-Tokens via TI-PKI gemäß Abschnitt "PoPP-Token Prüfung" in [gemSpec_PoPP_Service], wobei im HSMbis auf den OCSP-Sperrstatus keine Prüfung des Signaturzertifikats des PoPP-Tokens erfolgt, da das Signaturzertifikat kontrolliert im 4-Augenprinzip in das HSM eingebracht wird. 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 <code>iss</code> im PoPP-Token muss nicht geprüft werden. prüfen, dass der Ausstellungszeitpunkt des PoPP-Tokens (PoPP-Token.iat) nicht länger als 20 Minuten zurückliegt ($\text{PoPP-Token.iat} - 30s \leq \text{aktuelle Zeit} < \text{PoPP-Token.iat} + 20 \text{ Minuten} + 15s$, Hinweis: im PoPP-Token gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben). prüfen, dass PoPP-Token.proofMethod keine Prüfmethode -* ist. Falls die Prüfungen in 1) bis 3) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:
--	---

	<ul style="list-style-type: none"> • Aktenkonto: KVNR aus PoPP-Token.patientId • Telematik-ID: Telematik-ID aus PoPP-Token.actorID • Gültigkeitszeitraum: ergibt sich aus PoPP-Token.actorProfessionOid. <ol style="list-style-type: none"> 5. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis <ol style="list-style-type: none"> 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	<p><i>Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der Anlage eines Aktenkontos im Aktensystem registriert.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Befugnis1 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) signiert mit SMC-B des Kostenträgers bzw. der Ombudsstelle <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis2 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Prüfen der Befugnis1 <ol style="list-style-type: none"> a. prüfen der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle gemäß A_25042-* (C.HCI.OSIG) b. prüfen, ob die professionOID im Signaturzertifikat oid_kostentraeger bzw. oid_ombudsstelle ist c. prüfen, ob die Telematik-ID im Signaturzertifikat C.HCI.OSIG der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle mit der Telematik-ID in der Befugnis1 übereinstimmt 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 erstellt. Die Inhalte der Befugnis2 sind: <ul style="list-style-type: none"> • Aktenkonto: die KVNR des Aktenkontos aus Befugnis1 • Telematik-ID: die Telematik-ID aus Befugnis1 3. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

rr5	<p>Mit dieser Regel werden die Befugnisse bei einem betreiberübergreifenden Anbieterwechsel im Aktensystem registriert.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Befugnis1 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) signiert vom alten Aktensystembetreiber <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis2 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Prüfen der Befugnis1 <ol style="list-style-type: none"> a. prüfen der Signatur gemäß A_25042-* (C.FD.SIG) b. prüfen, ob im Signaturzertifikat C.FD.SIG der professionOIDoid_epa_vauist c. prüfen, dass das SignaturzertifikatC.FD.SIG nicht auf das importierende Aktensystem ausgestellt ist. 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 mit den Inhalten aus Befugnis1 erstellt. 3. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 <ol style="list-style-type: none"> 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.
-----	--

1655

1656 **A_24690-01 -ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen des ID-Tokens**

1657 Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung eines ID-Tokens durchführen:

- 1660 • dasID-Token muss gemäß A_25042-* valide signiert sein durch einen sektoralen Identity Provider oder den IDP-Dienst (professionOID ist oid_idpd_sek oder oid_idpd),
- 1661
- 1662
- 1663 • das ID-Token muss zeitlich gültig sein (Felder: iat, exp),
- 1664 • das ID-Token muss im Feldauddas ePA-Aktensystem eingetragen haben.

1665 [**<=**]

1666 **A_24691 -ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen von übers ePA-FdV erstellten Befugnissen**

1668 Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung einer von
 1669 einem Versicherten bzw. Vertreter über das ePA-FdV eingestellten signierten Befugnis
 1670 durchführen:

- 1671 • die Befugnis muss gemäß A_25042-* valide signiert sein durch einen Versicherten
 1672 bzw. Vertreter (C.CH.SIG, professionOID istoid_versicherter),
- 1673 • das JWT für die Befugnis gemäß A_24587-* darf nicht abgelaufen sein (Feld:
 1674 exp),
- 1675 • das Feld insurantID des JWT muss eine KVN-R sein,
- 1676 • das Feld actorID des JWT muss eine KVN-R oder eine Telematik-ID sein,
- 1677 • das Feld validTO des JWT muss ein zeitliches Datum sein.

1678 [**<=**]

1679 Die folgenden Regeln dienen zum Abruf der versichertenindividuellen Daten- und
 1680 Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel und
 1681 die Ableitungsvorschriften sind in [gemSpec_Krypt] in Abschnitt 3.15.2 festgelegt.

1682 **Tabelle 7: Tab_AS_SDS-Key_Rules Key Rules - Regeln zur Ableitung der**
 1683 **versichertenindividuellen Persistierungsschlüssel**

Regel	Beschreibung
kr1	<p><i>Diese Regel wird für die Anmeldung des Aktenkontoinhabers genutzt.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • 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). • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys • versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys <p>Regelverhalten:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> a. prüfen, ob die professionOID im Signaturzertifikat oid_idpd_sek ist oder prüfen des HSM-ID-Tokens b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung

	<ol style="list-style-type: none"> <ol style="list-style-type: none"> 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 KVNR aus dem ID-Token und den Labeln der zu verwendenden Befugnispersistierungs- und Datenpersistierungs-Masterkeys zur Ableitung von Befugnis- und Datenpersistierungsschlüssel aufgerufen. <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert die abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.
kr2	<p><i>Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssel genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • KVNR (Aktenkonten-ID) • Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys • ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Aufruf der VAU-HSM Zugriffsregel <code>hsm-r2</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR und dem Label des Befugnispersistierungs-Masterkeys zur Ableitung des Befugnispersistierungsschlüssels <ol style="list-style-type: none"> 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	<p><i>Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.</i></p>

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
- Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll
- ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll

Ausgangsdaten:

- versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys
- ggf. versichertenindividueller Überschlüsselungsschlüssel + 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.

	4. Das Befugnisverifikations-Modul liefert den abgeleiteten Datenpersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.
kr4	<p><i>Diese Regel wird für die Anmeldung des E-Rezept-Fachdienstes verwendet.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • 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 • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys • ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Prüfen des ID-Tokens <ol style="list-style-type: none"> 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 <ol style="list-style-type: none"> d. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <ol style="list-style-type: none"> 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. <ol style="list-style-type: none"> 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	Diese Regel wird für die Überschlüsselung verwendet (ggf. mit Umschlüsselung)

einer Überschlüsselung).

Diese Regel kann von einer VAU (AK-VAU oder dedizierte Überschlüsselungs-VAU) verwendet werden um verschlüsselte Akten zu überschlüsseln (vgl. Abschnitt 3.6: Umschlüsselung und Überschlüsselung). Dabei kann es auch zu einer Umschlüsselung einer älteren Überschlüsselung kommen.

Sei <current> ein spezielles Symbol was im VAU-HSM durch das Label des jüngsten Überschlüsselungsschlüssel ersetzt wird. Ein Aufruf braucht so das tatsächliche Label nicht zu kennen. (Der Hersteller ist frei "<current>" durch ein selbstgewählten Symbolnamen zu ersetzen.)

Eingangsdaten:

- VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder ggf. einer dedizierten Überschlüsselungs-VAU
- KVNR (Aktenkonten-ID)
- Labelliste: nicht leere Liste von Label-n von Überschlüsselungs-Masterkeys (im Regelfall enthält die Liste mindestens "<current>" als Element)

Ausgangsdaten:

- Liste von Paaren:
versichertenindividueller Überschlüsselungsschlüssel (Secure Data Storage Key),
Label für verwendeten Überschlüsselungs-Masterkey

(Hinweis: Die Liste enthält mindestens ein Element -- im Fall der ersten Überschlüsselung in Intervall 2 (vgl. Abschnitt 3.6))

Ablauf:

Das VAU-HSM muss des VAU-Attestierungstoken prüfen, ob es sich um eine AK-VAU oder dedizierte Überschlüsselungs-VAU handelt. Falls nein, Abbruch.

Das VAU-HSM durchläuft die Label-Liste und führt mit dem entsprechenden Label verbundenen Überschlüsselungs-Masterkey und der KVNR eine Schlüsselableitung durch. Dabei wird im VAU-HSM das spezielle Symbol "<current>" durch das Label des jüngsten Überschlüsselungs-Masterkeys vor Abarbeitung ersetzt.

In der Ergebnisse (siehe Ausgangsdaten) ist "<current>" ebenfalls so ersetzt. Die Reihenfolge in der Eingangsliste muss in der Ausgabeliste gleich bleiben.

1684

1685 **3.5 Vertrauenswürdige Ausführungsumgebung (VAU)**

1686 Eine Vertrauenswürdige Ausführungsumgebung (VAU) gewährleistet mit technischen
1687 Maßnahmen, dass Daten serverseitig im ePA-Aktensystem im Klartext verarbeitet werden
1688 können, ohne dass einzelne Mitarbeiter des Betreibers auf diese Daten zugreifen können.

1689 Die Datenverarbeitungen der Aktenkontoverwaltung müssen in einer VAU ausgeführt
1690 werden. Diese VAU wird im folgenden als Aktenkontoverwaltungs-VAU bezeichnet. Des
1691 weiteren kann das Befugnisverifikations-Modul in einer VAU ausgeführt werden. Diese
1692 VAU wird im folgenden als Befugnisverifikations-VAU bezeichnet.

AA_25716-02 -ePA-Aktensystem - Services ausschließlich in der VAU

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

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

[<=]

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

3.5.1 Übergreifende VAU-Anforderungen**3.5.1.1 Schutz der Integrität der VAU**

Die folgenden Anforderungen stellen die Integrität der VAU sicher.

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

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

Erläuterung zu A_24613-*:

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

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

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

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

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

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

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

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

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

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

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

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

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

3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU

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

A_24621 -ePA-Aktensystem - Äußere Isolation der VAU von Datenverarbeitungsprozessen des Betreibers

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

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

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

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

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

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

1781 Das ePA-Aktensystem MUSS sicherstellen, dass beim Beenden einer VAU-Instanz
1782 sämtliche Daten dieser VAU-Instanz aus flüchtigen Speichern sicher gelöscht werden
1783 oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [≤]

1784 **A_25244 -ePA-Aktensystem - x-insurantId nicht außerhalb des VAU-Kanals**

1785 Das ePA-Aktensystem MUSS sicherstellen, dass das HTTP Header-Element mit dem
1786 Namen "x-insurantId" nicht außerhalb des VAU-Kanals gesendet wird. [≤]

1787 **3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU**

1788 **A_26314 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**
1789 **gespeicherten Daten**

1790 Das ePA-Aktensystem MUSS sicherstellen, dass eine VAU-Daten, die im System des
1791 Aktensystembetreibers gespeichert werden sollen und für die keine spezifischen
1792 Anforderungen zum Schutz der gespeicherten Daten existieren, ausschließlich
1793 verschlüsselt gespeichert werden und der verwendete Verschlüsselungsschlüssel mittels
1794 der Regel hsm-r8 vom VAU-HSM abgeleitet wird. [≤]

1795 Hinweise zu A_26314:

- 1796 • Spezifische Anforderungen zum Schutz der gespeicherten Daten gibt es z.B. für
1797 die Aktenkontoverwaltungs-VAU in Abschnitt 3.5.2.2 und die durch die VAU für
1798 den Betrieb erstellten Protokolle in Abschnitt 3.5.1.5.
- 1799 • Außerhalb der VAU verschlüsselt gespeicherte Daten der ePA3.0, die bisher nicht
1800 mit Regel hsm-r8 verschlüsselt sein konnten, sind beim Öffnen der Akte
1801 umzuschlüsseln und mit einem Schlüssel zu sichern, der mit Regel hsm-r8
1802 abgeleitet wird. Eine Umschlüsselung ohne Öffnen der Akte ist nicht erforderlich.

1803 **A_26322 -ePA-Aktensystem - Unterschiedliche Schlüssel für die**
1804 **Verschlüsselung von außerhalb der VAU gespeicherten Daten bei**
1805 **unterschiedlichen Verarbeitungszwecken**

1806 Falls Daten außerhalb der VAU im System des Aktensystembetreibers gespeichert
1807 werden, MUSS das ePA-Aktensystem sicherstellen, dass für die Verschlüsselung von
1808 Daten, die zu unterschiedlichen Zwecken verarbeitet werden, unterschiedliche
1809 Verschlüsselungsschlüssel genutzt werden. [≤]

1810 Hinweis zu A_26322: Verarbeitungszwecke für Daten sind beispielsweise die
1811 Verarbeitung von Daten zum Zwecke der Sekundärnutzung (sieheData Submission
1812 Service) oder die Verarbeitung von Daten für die Nutzerverwaltung im Aktensystem
1813 (insbesondere Geräteinformationen und E-Mail-Adressen).

1814 **3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM**

1815 **A_24653 -ePA-Aktensystem - Sichere Verbindung zwischen VAU und VAU-HSM**

1816 Das ePA-Aktensystem MUSS technisch sicherstellen, dass zwischen einer VAU und einem
1817 VAU-HSM eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die
1818 vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des
1819 Betreibers des Aktensystems schützen. [≤]

1820 **3.5.1.5 Logging und Monitoring**

1821 Hinweis: Die Anforderungen dieses Abschnitts könnten sich noch ändern, falls sich bei
1822 der Umsetzung des ePA-Aktensystems herausstellt, dass weitere Protokollierungen auf
1823 Seiten des Betreibers notwendig werden.

1824 **A_24910 -ePA-Aktensystem - Erlaubte Zwecke der Betreiberprotokolle**

1825 Der Betreiber des Aktensystems MUSS sicherstellen, dass die durch die VAU für den
1826 Betrieb erstellten Protokolle des Betreibers ausschließlich zum Zwecke der Fehleranalyse
1827 und -behebung anlassbezogen sowie zum Zwecke des Security Monitorings verwendet
1828 werden. [≤]

1829 **A_24649 -ePA-Aktensystem - Datenschutzkonformes Logging und Monitoring**
1830 **der VAU**

1831 Die VAU MUSS die für den Betrieb des ePA-Aktensystems erforderlichen Logging- und
1832 Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit
1833 technischen Mitteln ausgeschlossen ist, dass dem Betreiber des ePA-Aktensystems
1834 vertrauliche oder zur unautorisierten Profilbildung geeignete Daten zur Kenntnis
1835 gelangen. [≤]

1836 **A_24695 -ePA-Aktensystem - Keine medizinische Informationen in VAU-**
1837 **Protokollen des Betreibers**

1838 Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten
1839 Protokollen des Betreibers keine personenbezogenen medizinischen Informationen
1840 enthalten sind (u. a. medizinische Daten von Versicherten oder Informationen, aus denen
1841 sich ableiten lässt, bei welchen Leistungserbringerinstitutionen ein Versicherter in
1842 Behandlung ist).
1843 [≤]

1844 **A_24909 -ePA-Aktensystem - Nicht KVNR und Telematik-ID gemeinsam**
1845 **protokollieren**

1846 Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten
1847 Protokollen des Betreibers höchstens die KVNR oder höchstens die Telematik-ID
1848 enthalten ist, aber nicht eine Kombination aus KVNR und Telematik-ID und keine solche
1849 Verbindung über mehrere Protokolle hergestellt werden kann. [≤]

1850 **A_24719 -ePA-Aktensystem - Kein kryptographisches Schlüsselmateri al in VAU-**
1851 **Protokollen des Betreibers**

1852 Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten
1853 Protokollen des Betreibers kein kryptographisches Schlüsselmateri al enthalten ist. [≤]

1854 **A_24911 -Löschfristen Protokolle**

1855 Das ePA-Aktensystem MUSS sicherstellen, dass die

- 1856 • zum Zwecke der Fehleranalyse erhobenen Protokolle nach Behebung des Fehlers
1857 unverzüglich gelöscht werden,
- 1858 • zum Zwecke des Security Monitorings erhobenen Protokolle nach 3 Monaten
1859 gelöscht werden.

1860 [≤]

1861 **A_26316 -Anbieter ePA-Aktensystem - Schutz der Protokolle des Betreibers**

1862 Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die durch die VAU für den
1863 Betrieb erstellten Protokolle des Betreibers durch technische und organisatorische
1864 Maßnahmen vor einer missbräuchlichen Nutzung geschützt werden. [≤]

1865 **gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik**

1866 Hinweis zu A_27336-*: Der geheime Schlüssel für die Pseudonymisierung muss nicht im
1867 VAU-HSM gespeichert werden.

1868 **A_27333 -ePA-Aktensystem - Geheimer Schlüssel für Pseudonymisierung der**
1869 **gematik-Logdaten nur in VAU**

1870 Das ePA-Aktensystem MUSS sicherstellen, dass der für die Pseudonymisierung der
1871 Logdaten gemäß A_27332-* benötigte geheime Schlüssel `key_pn_log` im Klartext
1872 ausschließlich innerhalb einer VAU-Instanz verarbeitet wird. [≤]

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

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

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

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

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

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

3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU**3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU****A_24636-01 -ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen innerhalb einer VAU-Instanz**

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

A_27534 -ePA-Aktensystem – Kein gemeinsamer Speicher von Datenverarbeitungsprozessen innerhalb einer VAU-Instanz

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

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

A_27535 -ePA-Aktensystem – Maximale Lebensdauer von VAU-Instanzen

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

A_24885 -ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen unterschiedlicher VAU-Instanzen

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

A_24637 -ePA-Aktensystem - Maximale Health Record Context in einer VAU-Instanz

1918 Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Health Record Context
1919 gleichzeitig in einer VAU-Instanz laufen können.

1920 [\leq]

1921 **A_25028 -ePA-Aktensystem - Keine Kommunikation zwischen**
1922 **Aktenkontoverwaltungs-VAUs**

1923 Das ePA-Aktensystem MUSS sicherstellen, dass es keine direkte Kommunikation
1924 zwischen VAU-Instanzen von Aktenkontoverwaltungs-VAUs gibt. [\leq]

1925 **A_26111 -ePA-Aktensystem - Keine Kommunikation zwischen Health Record**
1926 **Contexts**

1927 Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer
1928 Aktenkontoverwaltungs-VAU-Instanz keine Kommunikation zwischen Health Record
1929 Contexts gibt. [\leq]

1930 **A_24639 -ePA-Aktensystem - Löschen aller Daten beim Beenden eines Health**
1931 **Record Context**

1932 Die VAU MUSS sicherstellen, dass beim Beenden eines Health Record Context sämtliche
1933 Daten dieses Health Record Context aus flüchtigen Speichern sicher gelöscht werden
1934 oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [\leq]

1935 **A_24640 -ePA-Aktensystem - Löschen aller Daten beim Beenden einer User**
1936 **Session**

1937 Die VAU MUSS sicherstellen, dass beim Beenden einer User Session sämtliche Daten
1938 dieser User Session aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf
1939 diese Daten technisch ausgeschlossen ist. [\leq]

1940 *Hinweis zu A_24639-*, A_24640-* und A_24648-*: Eine zeitliche Verzögerung des*
1941 *Löschens ist tolerabel, sofern ein sofortiges Löschen aufgrund der Architektur des*
1942 *Aktensystemherstellers aus Performanzgründen nicht sinnvoll ist. In diesem Fall ist ein*
1943 *geeigneter Kompromiss zwischen dem Löschzeitpunkt und der Performanz zu wählen.*

1944 **A_25231 -ePA-Aktensystem - Schließen des Health Record Context beim**
1945 **Beenden einer User Session**

1946 Die VAU MUSS sicherstellen, dass beim Beenden einer User Session alle mit dieser User
1947 Session verknüpften Health Record Context beendet werden, wenn der jeweilige Health
1948 Record Context nicht mit mindestens einer weiteren User Session verknüpft ist. [\leq]

1949 **A_25051 -ePA-Aktensystem - VAU-Kanal endet immer in einer**
1950 **Aktenkontoverwaltungs-VAU**

1951 Die VAU MUSS sicherstellen, dass ein VAU-Kanal von einem Client der ePA (ePA-Client
1952 oder ePA-FdV) ausschließlich in einer Aktenkontoverwaltungs-VAU endet. [\leq]

1953 Hinweis: Der VAU-Kanal darf z.B. nicht in einer Befugnisverifikations-VAU enden.

1954 **3.5.2.2 Schutz der Daten bei Speicherung außerhalb der**
1955 **Aktenkontoverwaltungs-VAU**

1956 Die folgenden Anforderungen gewährleisten den Schutz der beim Betreiber des ePA-
1957 Aktensystems persistierten Daten von Aktenkonten. Die Verschlüsselung der Daten eines
1958 Versicherten erfolgt mit seinem versichertenindividuellen Daten- und
1959 Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel sind
1960 in [gemSpec_Krypt#3.15.2] festgelegt.

1961 **A_24643 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**
1962 **gespeicherten Daten mit dem Datenpersistierungsschlüssel**

1963 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten

1964 1. Daten des FHIR-Data Service

- 1965 2. Daten des XDS Document Service
- 1966 3. Daten des Audit Event Service (Protokolle für den Versicherten zum Zwecke der
- 1967 Datenschutzkontrolle)
- 1968 4. Daten des Constraint Managements (Policies zu verborgenen Daten)
- 1969 5. Daten des Consent Managements (Widersprüche des Versicherten)
- 1970 vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb
- 1971 des Health Record Context mit dem zum Health Record gehörenden
- 1972 versichertenindividuellen Datenpersistierungsschlüssel verschlüsselt werden.
- 1973 [\leq]
- 1974 **A_24644 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**
- 1975 **gespeicherten Befugnissen mit dem Befugnispersistierungsschlüssel**
- 1976 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten
- 1977 Daten des Entitlement Managements, d. h. Befugnisse und Befugnisverbote, vor der
- 1978 Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health
- 1979 Record Context mit dem zum Health Record gehörenden versichertenindividuellen
- 1980 Befugnispersistierungsschlüssel verschlüsselt werden. [\leq]
- 1981 **3.5.2.3 Konsistenz des Systemzustands**
- 1982 **A_24650 -ePA-Aktensystem - Konsistenter Systemzustand eines Health Record**
- 1983 **Context**
- 1984 Die VAU MUSS sicherstellen, dass ein konsistenter Zustand eines Health Record Context
- 1985 auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw.
- 1986 wiederhergestellt werden kann. [\leq]
- 1987 **A_24696 -ePA-Aktensystem - Konsistenz bei parallelen Zugriffen**
- 1988 Die VAU MUSS auch bei parallelen Zugriffen auf dasselbe Aktenkonto durch mehrere
- 1989 Nutzer immer einen konsistenten Zustand des Aktenkontos gewährleisten. [\leq]
- 1990 **3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-**
- 1991 **VAU**
- 1992 Eine Befugnisverifikations-VAU ist eine spezielle VAU, in der ausschließlich das
- 1993 Befugnisverifikations-Modul ausgeführt wird.
- 1994 **A_24646 -ePA-Aktensystem - Befugnisverifikations-VAU verarbeitet**
- 1995 **ausschließlich ein Befugnisverifikations-Modul**
- 1996 Das ePA-Aktensystem MUSS sicherstellen, dass in einer Befugnisverifikations-VAU
- 1997 ausschließlich ein Befugnisverifikations-Modul ausgeführt wird. [\leq]
- 1998 **A_24647 -ePA-Aktensystem - Befugnisverifikations-VAU speichert keine Daten**
- 1999 Eine Befugnisverifikations-VAU DARF die Daten, die sie im Rahmen der Regeln des
- 2000 Befugnisverifikations-Moduls verarbeitet, NICHT außerhalb der Befugnisverifikations-VAU
- 2001 speichern. [\leq]
- 2002 Eine Befugnisverifikations-VAU darf insbesondere die vom VAU-HSM abgeleiteten
- 2003 versichertenindividuellen Persistierungsschlüssel nicht speichern.
- 2004 **A_24648 -ePA-Aktensystem - Befugnisverifikations-VAU löscht Daten nach**
- 2005 **Regelbearbeitung**
- 2006 Eine Befugnisverifikations-VAU MUSS sämtliche Daten, die sie im Rahmen eines
- 2007 Regelaufrufs des Befugnisverifikations-Moduls verarbeitet, sofort nach Abarbeitung der
- 2008 Regel sicher aus der Befugnisverifikations-VAU löschen bzw. einen Zugriff auf diese
- 2009 Daten technisch ausschließen. [\leq]

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

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

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

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

3.5.4 Zusätzliche Anforderungen an eine Service-VAU

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

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

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

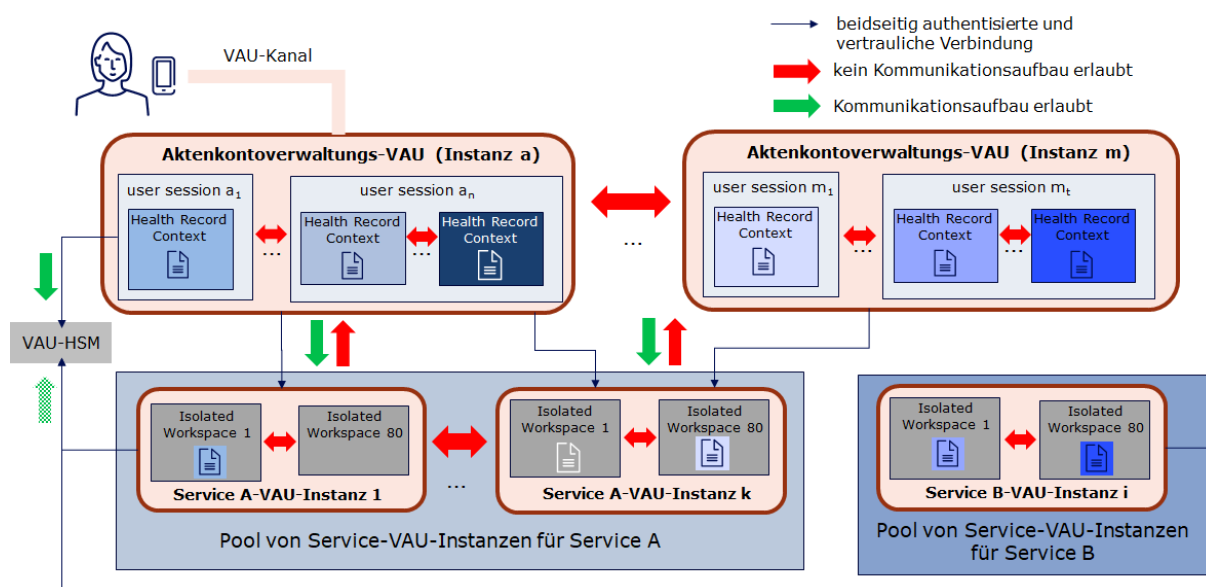


Abbildung 2 - Überblick Service-VAUs

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

2041 **A_26112 -ePA-Aktensystem - Maximale Isolated Workspaces in einer Service-**
2042 **VAU-Instanz**

2043 Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Isolated Workspaces
2044 gleichzeitig in einer Service-VAU-Instanz laufen können.[<=]

2045 **A_26113-01 -ePA-Aktensystem - Isolation zwischen Isolated Workspaces**
2046 **innerhalb einer Service-VAU-Instanz**

2047 Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb
2048 einer Service-VAU-Instanz zwischen Isolated Workspaces keine Informationsflüsse
2049 auftreten können.
2050 [<=]

2051 **A_27537 -ePA-Aktensystem – Kein gemeinsamer Speicher von Isolated**
2052 **Workspaces innerhalb einer Service-VAU-Instanz**

2053 Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb
2054 einer Service-VAU-Instanz von einem Isolated Workspace nicht auf den Speicher anderer
2055 Isolated Workspaces zugegriffen werden kann.[<=]

2056 **A_26114 -ePA-Aktensystem - Isolation zwischen unterschiedlichen Service-**
2057 **VAU-Instanzen**

2058 Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der
2059 unabhängig vom Separationsmechanismus in A_26113-* ist, ausschließen, dass sich
2060 Verarbeitungen in einer Service-VAU-Instanz schadhaft auf die Verarbeitungen einer
2061 anderen Service-VAU-Instanz auswirken können.[<=]

2062 **A_26115 -ePA-Aktensystem - Isolated Workspace verarbeitet maximal einen**
2063 **Request einer AK-VAU**

2064 Nachdem ein Isolated-Workspace einen (1) Service-Request einer
2065 Aktenkontoverwaltungs-VAU-Instanz verarbeitet hat, MUSS das ePA-Aktensystem
2066 sicherstellen, dass alle Daten des Isolated-Workspaces sicher gelöscht werden, um den
2067 Isolated-Workspace für nachfolgende Service-Requests wieder neu zu initialisieren.[<=]

2068 **A_26116 -ePA-Aktensystem - In einem Isolated Workspace sind zu einem**
2069 **Zeitpunkt nur Daten eines Versicherten**

2070 Das ePA-Aktensystem MUSS sicherstellen, dass in einem Isolated Workspace zu einem
2071 Zeitpunkt ausschließlich Daten eines Versicherten verarbeitet werden können, sofern die
2072 Auswahl der zu verarbeitenden Daten durch die Logik im ePA-Aktensystem bestimmt
2073 wird.[<=]

2074 Hinweis zu A_26116-*: Falls Nutzer die Daten für die Service-VAU auswählen, ohne dass
2075 das ePA-Aktensystem auf diese Daten Einfluss hat (z.B. Nutzer wählt zu konvertierende
2076 PDF-Dokumente im ePA-FdV aus) kann es dazu kommen, dass zu einem Zeitpunkt auch
2077 Daten mehrerer Versicherter in einem Isolated Workspace verarbeitet werden.

2078 **A_26117 -ePA-Aktensystem - Keine Kommunikation zwischen Isolated**
2079 **Workspaces**

2080 Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer Service-VAU-Instanz
2081 keine Kommunikation zwischen Isolated Workspaces gibt.[<=]

2082 **A_26118 -ePA-Aktensystem - Keine Kommunikation zwischen Service-VAU**

2083 Das ePA-Aktensystem MUSS sicherstellen, dass es keine Kommunikation zwischen
2084 Instanzen von Service-VAUs gibt.[<=]

2085 **A_26119 -ePA-Aktensystem - Service-VAUs speichern keine Daten in**
2086 **Aktenkonten**

2087 Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine Daten in
2088 einem Aktenkonto eines Versicherten persistieren.[<=]

2089 **A_26120 -ePA-Aktensystem - Service-VAUs verarbeiten keine Identitätstoken**

2090 Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine
2091 Identitätstoken von Nutzern verarbeiten.[<=]

2092 **A_26123 -ePA-Aktensystem - Service-VAU-Instanzen haben maximale**
2093 **Lebensdauer**

2094 Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen nach einer
2095 definierten Lebensdauer (abhängig von der Funktionalität der Services) keine neuen
2096 Service-Requests mehr annehmen können und, nachdem die laufenden Requests
2097 abgearbeitet wurden, beendet und neu gestartet werden.[<=]

2098 **A_26124 -ePA-Aktensystem - Information über neuen Service-VAU-Typ**

2099 Der Hersteller des ePA-Aktensystems MUSS die gematik über die Absicht der Einführung
2100 eines neuen Service-VAU-Typs informieren und ggf. für diesen neuen Service-VAU-Typ zu
2101 erfüllende Rahmenbedingungen abstimmen.[<=]

2102 Hinweis zu A_26124-*: Hierzu gehört z.B. auch die Festlegung der maximalen
2103 Lebensdauer für den neuen Service-VAU-Typ (siehe A_26123-*).

2104 **A_26125 -ePA-Aktensystem - Starten ausschließlich attestierter Service-VAUs**

2105 Das ePA-Aktensystem MUSS sicherstellen, dass ausschließlich attestierte Service-VAU-
2106 Instanzen gestartet werden können.[<=]

2107 **3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU**

2108 **A_26126 -ePA-Aktensystem - Gesicherte und authentifizierte Verbindung**
2109 **zwischen AK-VAU- und Service-VAU-Instanzen**

2110 Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer Aktenkontoverwaltungs-
2111 VAU-Instanz und einer Service-VAU-Instanz eine beidseitig authentifizierte und
2112 vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe
2113 durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen.[<=]

2114 **A_26127 -ePA-Aktensystem - Kein Kommunikationsaufbau von Service-VAU-**
2115 **Instanzen zu AK-VAU-Instanzen**

2116 Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine
2117 Kommunikation zu einer AK-VAU-Instanz aufbauen kann.[<=]

2118 **A_26128 -ePA-Aktensystem - Kein Aufruf von Schnittstellen von AK-VAU-**
2119 **Instanzen durch Service-VAU-Instanzen**

2120 Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine
2121 Schnittstellen/Services aufrufen kann, die in einer AK-VAU-Instanz ausgeführt
2122 werden.[<=]

2123 **3.6 Umschlüsselung und Überschlüsselung**

2124 Das Kerckhoffs'sche Prinzip von 1883 ist ein Grundpfeiler der Kryptographie. Es besagt u.
2125 a. dass die Sicherheit von kryptographischen Verfahren alleinig von der Geheimhaltung
2126 der Schlüssel abhängen darf, und dass Schlüssel leicht auswechselbar sein müssen. Damit
2127 kryptographische Schlüssel in der Praxis ihre Sicherheitseigenschaft behalten können
2128 müssen sie einen Lebenszyklus besitzen (vgl. bspw. [NIST-SP-800-57P1]), der den
2129 regelmäßigen Austausch (Wechsel) der Schlüssel vorsieht und umsetzt. Jährlich werden
2130 aus diesem Grunde die Masterkey für Akten Daten und die Masterkey für Befugnisse
2131 erneuert (vgl. A_15745-* und A_20519-* (beide aus [gemSpec_Krypt])). Bei dieser
2132 Erneuerung muss eine Umschlüsselung durchgeführt werden:

- 2133 • Schlüssel_alt_KVNR = Ableitung (MK_alt, KVNR),
2134 • Schlüssel_neu_KVNR = Ableitung (MK_neu, KVNR),

- 2135 • Umschlüsselung pro Akte: Schlüssel_alt_KVNR -> Schlüssel_neu_KVNR.
- 2136 Falls eine AK-VAU Zugriff auf eine Akte besitzt und zu diesem Zeitpunkt feststellt neue
2137 Masterkeys (vgl. betreiberspezifische Schlüssel A_15745-*) existieren, muss sie eine
2138 Umschlüsselung durchführen (A_20519-*). Falls eine Akte länger nicht verwendet wird,
2139 kann eine AK-VAU keinen Zugang zu den Klartexten der Akte erhalten, da sie nur nach
2140 erfolgreicher Nutzerauthentisierung vom VAU-HSM die aktenspezifischen
2141 Ableitungsschlüssel erhält. Dann kann eine AK-VAU zunächst auch keine Umschlüsselung
2142 vornehmen. Aus diesem Grunde muss eine VAU (entweder eine AK-VAU oder eine
2143 dedizierte Überschlüsselungs-VAU) eine Überschlüsselung der Chiffre der Akte
2144 vornehmen. Dafür werden Überschlüsselungsschlüssel benötigt. Es gibt analog zu den
2145 anderen betreiberspezifischen Schlüssel (A_15745-*) Masterkeys für eine
2146 Schlüsselableitung für die Überschlüsselung der Chiffre einer Akte.
- 2147 **A_26197 -ePA-Aktensystem - betreiberspezifische Schlüssel:**
2148 **Überschlüsselungs-Masterkeys**
2149 Ein ePA-Aktensystem MUSS sicherstellen, dass die Menge der betreiberspezifischen
2150 Schlüssel aus [gemSpec_Krypt#A_15745-*] um die Kategorie Überschlüsselungs-
2151 Masterkeys erweitert wird. Für die Überschlüsselungsschlüssel MÜSSEN die gleichen
2152 Vorgaben wie für alle betreiberspezifischen Schlüssel gemäß A_15745-* gelten.
2153 Die betreiberspezifischen Schlüssel werden mindestens jährlich aktualisiert (A_20519-*),
2154 die alten Schlüssel MÜSSEN solange im VAU-HSM verfügbar sein, solange Chiffre im
2155 Aktensystem existieren (bspw. Daten einer Akte), die mit diesen Schlüsseln
2156 kryptographisch gesichert sind.[<=]
- 2157 D. h. wie in Abschnitt 3.3 (bspw. A_24611-*) definiert, gibt es bei den Masterkeys drei
2158 Kategorien: (1) Aktenpersistierung, (2) Befugnispersistierung und (3) Überschlüsselung.
2159 Initial startet der Betrieb eines Aktensystems mit je einem Schlüssel in den ersten zwei
2160 Kategorien. Nach maximal einem Jahr (A_20519-*), oder anders formuliert im nächsten
2161 Intervall, werden diese beiden ersten Schlüssel zufällig neu erzeugt. Dabei muss nun ein
2162 neuer Überschlüsselungsmasterkey erzeugt werden. Die Anzahl der Schlüssel nach o. g.
2163 Kategorie ist anschließend (1) 2, (2) 2, (3) 1.
- 2164 **A_26198 -ePA-Aktensystem - neuer Überschlüsselungsschlüssel bei Erneuerung**
2165 **betreiberspezifischen Schlüssel**
2166 Ein ePA-Aktensystem MUSS sicherstellen, dass bei jeder Erneuerung der Masterkeys zur
2167 Aktenpersistierung ein weiterer neuer Überschlüsselungsmasterkey zufällig im VAU-HSM
2168 erzeugt wird.
2169 [<=]
- 2170 Bei einer Erneuerung der betreiberspezifischen Schlüssel gibt es verschiedene
2171 Zeitabschnitte:

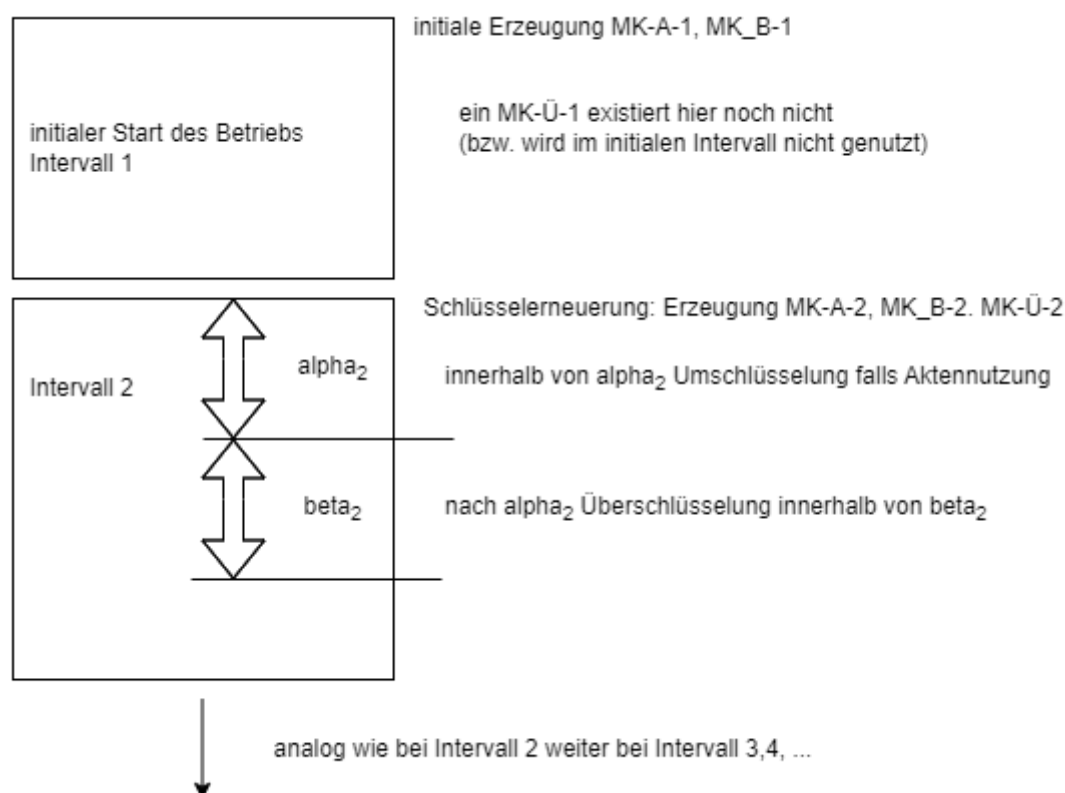


Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung

A_26204 -ePA-Aktensystem - zeitliche Vorgaben zur Durchführung der Umschlüsselung und Überschlüsselung

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

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

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

[<=]

Die folgenden zwei Anforderung geben weitere Details zu A_26204-*.

A_26205 -ePA-Aktensystem - Umschlüsselung

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

2200
 2201 Wenn die AK-VAU eine Akte verwendet und feststellt, dass diese überschlüsselt ist, so
 2202 MUSS die AK-VAU die Überschüsselung entschlüsseln und die nun verfügbaren Chifftrate
 2203 der Akten auf Grundlage des aktuellen Masterkeys umschlüsseln. (Hinweis: nach
 2204 Konstruktion muss die innere Aktenverschlüsselung auf einem älteren Masterkey
 2205 basieren, ansonsten hätte keine Überschüsselung stattgefunden.) Nach erfolgreicher
 2206 Umschlüsselung MÜSSEN die alten Chifftrate (das Überschüsselungschifftrate und das alte
 2207 "innere" Chifftrate der Akte) im Aktensystem gelöscht werden. [\leq]

2208 Hinweis zu A_26205-*: Die notwendigen aktenspezifischen Schlüssel liegen nun in der
 2209 AK-VAU vor. Die Umschlüsselung muss nicht direkt sofort vor Nutzung der Akte erfolgen,
 2210 sondern kann auch einige Minuten später erfolgen. Die konkrete Ausgestaltung liegt beim
 2211 Hersteller.

2212 **A_26206 -ePA-Aktensystem - Überschüsselung**

2213 Ein ePA-Aktensystem MUSS sicherstellen, dass jeweils im aktuellen Intervall nach Ablauf
 2214 des Zeitintervalls alpha Akten, die nicht überschlüsselt sind und deren Verschlüsselung
 2215 auf einem älteren Masterkey (i. S. v. nicht aus dem aktuellen Zeitintervall) basiert,
 2216 überschlüsselt werden auf Basis des aktuellen Überschüsselungs-Masterkeys. Diese
 2217 Umschlüsselung MUSS jeweils innerhalb des Zeitintervalls beta für alle solche Akten
 2218 abgeschlossen werden. Die "alten" Chifftrate (Chifftrate von solchen Akten vor der
 2219 Überschüsselung) MÜSSEN im Aktensystem gelöscht werden. [\leq]

2220 Umschlüsselung einer Überschüsselung: Bei einer Akten, die länger nicht verwendet
 2221 wird, kann es dazu kommen, dass überschlüsselte Akten wieder überschlüsselt werden
 2222 müssen, weil alpha im nächsten Intervall abgelaufen ist. In diesem Fall wird eine
 2223 Umschlüsselung mittels der Überschüssel vorgenommen, d. h. die Verschlüsselungstiefe
 2224 / -kette wird 2 nicht überschreiten -- es gibt maximal eine Überschüsselungsschicht.

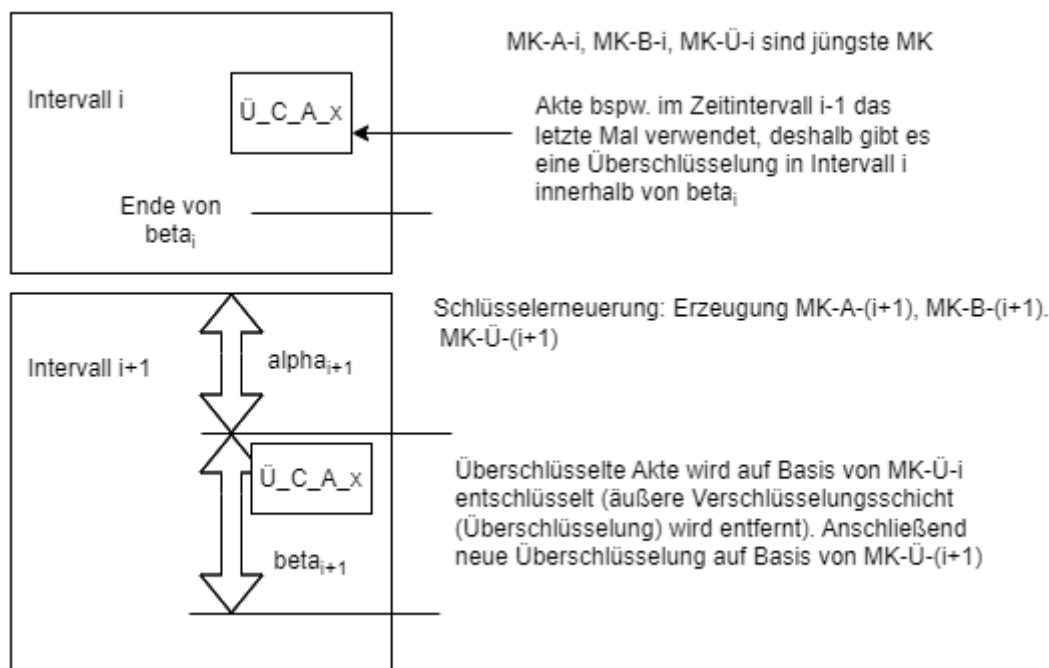


Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer Überschüsselung

2229 **A_26208 -ePA Aktensystem - Umschlüsselung einer Überschüsselung**

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

[<=]

Sollte durch irgendeinen Umstand die Sicherheitseigenschaft der Betreiberschlüssel (A_15745-*) in Frage stehen, so muss ein Aktensystembetreiber die Umschlüsselung bzw. die Überschüsselung aktivieren/starten können.

A_26199 -ePA-Aktensystem - Notfall-Aktivierung Umschlüsselung/Überschüsselung

Ein ePA-Aktensystem MUSS sicherstellen, dass das ePA-Aktensystem es einem ePA-Betreiber ermöglicht eine Erneuerung der betreiberspezifischen Schlüssel zu starten/aktivieren. Es MUSS also dem ePA-Betreiber möglich sein neben der regelmäßigen Erneuerung der betreiberspezifischen Schlüssel (A_205019-*) eine Erneuerung zu initiieren.

[<=]

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

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

A_26223 -ePA-Aktensystem - Metadaten von ePA-spezifischen Chiffren

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

3.7 User Session und Health Record Context

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

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

2277 Wird durch den ePA-Client eine Operation für eine bestimmte Akte aufgerufen (Parameter
2278 x-insurantid) der Operation, wird in der User Session geprüft, ob diese Akte schon
2279 verwendet wird (ein anderer Nutzer gerade mit der Akte arbeitet) oder nicht. Sollte die
2280 Akte noch nicht verwendet werden, wird die Akte in einem Health Record Context
2281 geöffnet und kann durch den ePA-Client in dessen User Session verwendet werden.
2282 Existiert für die Akte schon ein geöffneter Health Record Context, darf es durch den
2283 parallelen Zugriff zu keinen Inkonsistenzen in der Akte kommen.

2284 Innerhalb einer VAU-Instanz dürfen nur eine maximale Anzahl von Health Record
2285 Contexts gleichzeitig aufgebaut sein. Sollte diese Anzahl überschritten werden, wird der
2286 am längsten nicht genutzte Health Record Context geschlossen, um einen neuen Health
2287 Record Context öffnen zu können.

2288 3.8 Consent Decision Management

2289 Das Consent Decision Management des Aktensystems verwaltet die Entscheidungen eines
2290 Versicherten oder eines Vertreters für oder gegen die Nutzung von definiert
2291 widerspruchsfähigen Funktionen gemäß gesetzlicher Vorgaben.

2292 Außerdem werden im Consent Decision Management die Einschränkungen der
2293 Verwendung von Daten auf bestimmte Sekundärnutzungszwecke durch das
2294 Forschungsdatenzentrum Gesundheit verwaltet (siehe 3.8.2- Einschränkung der
2295 Verwendung von Daten auf bestimmte Sekundärnutzungszwecke).

2296 Der Widerspruch gegen die grundsätzliche Nutzung der ePA wird nicht im Consent
2297 Decision Management berücksichtigt. Die Existenz eines Aktenkontos für einen
2298 Versicherten impliziert, dass kein Widerspruch gegen die Nutzung der ePA erteilt wurde.
2299 Der Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger
2300 wird ebenfalls nicht hier verwaltet (siehe zu beiden Widersprüchen auch 3.1.1-
2301 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte).

2302 3.8.1 Widersprüche für Funktionen der ePA

2303 Die vorgehaltenen Entscheidungen zu einer Funktion umfassen dabei den Zustand "kein
2304 Widerspruch erklärt" ("permit") oder "Widerspruch erklärt" ("deny") und den Kontext
2305 einer Funktion. Der Kontext ordnet dabei die einzelnen widerspruchsfähigen Funktionen
2306 einem für die Umsetzung des Widerspruchs betroffenen Nutzerkreis zu und wird bei den
2307 zugreifenden Schnittstellen zur Filterung der Ausgabe verwendet.

2308 Initial, also bei der Erstellung eines neuen Aktenkontos oder bei Übernahme eines
2309 existierenden ePA 2.x Aktenkontos, ist für keine widerspruchsfähige Funktion ein
2310 Widerspruch gegen die Nutzung erklärt. Ein Versicherter oder ein Vertreter kann im
2311 Verlauf der Nutzung des Aktenkontos aktiv der Verwendung von widerspruchsfähigen
2312 Funktionen widersprechen oder einen erteilten Widerspruch zurücknehmen.

2313 Die aktuell erteilten Widersprüche können durch einen Versicherten oder einen Vertreter
2314 jederzeit über ein ePA-FdV eingesehen und geändert werden. Versicherte und Vertreter,
2315 die ein ePA-FdV nicht nutzen möchten, können eine Auskunft über die aktuell erteilten
2316 Widersprüche über die Ombudsstelle erhalten und dort auch Änderungen an den
2317 Entscheidungen im Aktenkonto veranlassen. Die Ansicht oder Änderung der
2318 Widersprüche erfolgt im Aktenkonto stets gesichert innerhalb der VAU, die aktuellen
2319 Entscheidungen zu den widerspruchsfähigen Funktionen der ePA sind
2320 versichertenindividuell mit dem SecureDataStorageKey verschlüsselt abgelegt.

2321 Die Information über relevante erteilte oder nicht erteilte Widersprüche können Clients
 2322 auf einfache Weise (ohne Authentisierung oder Etablierung eines VAU-Kanals) im Vorfeld
 2323 einer Operation über den Information Service abfragen (siehe auch 3.15- Information
 2324 Service).

2325 Das Consent Decision Management des Aktenkontos spiegelt ("cached") die
 2326 Entscheidungen zu den Widersprüchen für die schnelle Abfrage über den Information
 2327 Service in einen Bereich, der ohne den Aufbau eines VAU-Kanals und Verwendung des
 2328 versichertenindividuellen SecureDataStorageKey nutzbar ist.

2329 Das Aktenkonto unterstützt die Durchsetzung eines erteilten Widerspruchs überall dort,
 2330 wo Aktivitäten dediziert als Teil einer widerspruchsfähigen Funktion zugeordnet werden
 2331 können. Beispielsweise wird das Einstellen neuer Verordnungs- und Dispensierdaten in
 2332 die Ordner der Kategorie "medication" immer verhindert, wenn der Teilnahme am digital
 2333 gestützten Medikationsprozess widersprochen wurde. Die konkreten Auswirkungen eines
 2334 Widerspruchs sind in den jeweiligen Kapiteln zur Handhabung von Dokumenten und
 2335 Daten des Aktenkontos dargestellt (siehe 3.13.1- XDS Document Service und 3.13.2-
 2336 FHIR Data Services) .

2337 Die jeweils berücksichtigten widerspruchsfähigen Funktionen sind wie folgt definiert.
 2338 Diese Liste kann in folgenden Versionen der ePA ergänzt oder verändert werden.

2339 **A_23874-01 -Consent Decision Management - Definition der** 2340 **widerspruchsfähigen Funktionen der ePA**

2341 Das Consent Decision Management MUSS die Attribute zu widerspruchsfähigen
 2342 Funktionen der ePA gemäß der folgenden Tabelle verwenden.

2343 **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"

2344 **[<=]**

2345 *Hinweis: Die Bezeichnungen in () sind die Bezeichnungen in den Schnittstellen für den*
 2346 *Abruf und die Verwaltung der Widersprüche. Eine widerspruchsfähige Funktion wird durch*
 2347 *die ID der Funktion eindeutig identifiziert.*

2348 *Hinweis: Die Verwaltung der Widersprüche gegen die Nutzung des Aktenkontos durch*
 2349 *eine spezifische Leistungserbringerinstitution erfolgt über die Befugnisverwaltung (siehe*
 2350 *3.9.4- Befugnisausschluss (Blocked User Policy)).*

2351 Die Entscheidungen zu den widerspruchsfähigen Funktionen "medication" und "erp-
 2352 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. [\leq]

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

A_23766 -Consent Decision Management - Initialisierung der Widerspruchsinformation zur Nutzung von Funktionen der ePA

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

A_24343 -Consent Decision Management - Speichern der Inhalte

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

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

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

- Versorgungsprozess ("healthCareProcess")

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

[\leq]

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

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

- Versorgungsprozess ("healthCareProcess")

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

Widersprüchen. [\leq]

2403 Clients der Ombudsstelle und aus der Umgebung des Versicherten nutzen das Consent
 2404 Decision Management über die Operationen der Schnittstelle
 2405 I_Consent_Decision_Management. Clients aus der Umgebung der LEI und der E-Rezept-
 2406 Fachdienst nutzen für die schnelle Abfrage die Operation der
 2407 Schnittstelle I_Information_Service.

2408 **A_23824 -Aktensystem - Realisierung der Schnittstelle**

2409 **I_Consent_Decision_Management**

2410 Das ePA-Aktensystem MUSS die Operationen der Schnittstelle
 2411 I_Consent_Decision_Management gemäß [I_Consent_Decision_Management]
 2412 umsetzen. [≤]

2413 **A_23919 -Consent Decision Management - unveränderte Übernahme der** 2414 **Widerspruchsentscheidung**

2415 Das Consent Decision Management MUSS die über Operationen der Schnittstellen des
 2416 Consent Managements übermittelten Entscheidungen (consent decisions) zu
 2417 widerspruchsfähigen Funktionen der ePA in das Aktenkonto übernehmen. Die
 2418 Entscheidungen zu den in den Operationen nicht adressierten widerspruchsfähigen
 2419 Funktionen MÜSSEN im Aktenkonto unverändert bleiben. [≤]

2420 **A_24844 -Consent Decision Management - Information über Änderungen der** 2421 **Widerspruchsinformation**

2422 Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung
 2423 einer Widerspruchsinformation, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail
 2424 darüber informieren, dass Widerspruchsinformationen geändert wurden, wann die
 2425 Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im
 2426 Protokoll zu finden sind. [≤]

2427 **A_24055 -Consent Decision Management – Protokollierung geänderter** 2428 **Entscheidungen zu Widersprüchen**

2429 Das Consent Decision Management MUSS Bei Änderungen von Entscheidungen zu den
 2430 widerspruchsfähigen Funktionen der ePA jeweils einen Protokolleintrag gemäß A_24704*
 2431 erzeugen. Für die Wertebelegung ist A_23874* zu berücksichtigen und die
 2432 Protokollstruktur entsprechend zu belegen:

2433 **Tabelle 9: Consent Decision Management Protokollierung - Widersprüche für Funktionen** 2434 **der ePA**

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

	"ConsentDecision"	<consent decision>	"deny" oder "permit"
--	-------------------	-----------------------	----------------------

[<=]

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

A_26293 – Ein Aufruf der Operationen der Schnittstelle I Consent-Decision Management – Weiterleitung zur Änderung der Entscheidung von den Widersprüchen gegen die Sekundärdaten-nutzNutzung von widerspruchsfähigen Funktionen der ePA kann erfolgreich beendet werden, ohne dass eine bisher gespeicherte Entscheidung durch das FDZ
Das zu diesen Widersprüchen im Aktensystem geändert wird. In diesem Fall erfolgt die Protokollierung gemäß A 27883-*,

A 27883 -Consent Decision Management – MUSS die Informa – Protokollierung unveränderter Entscheidungen zu den widerspruchsfähigen Funktionen üben d
einen erklärten PA

Das Consent Decision Management MUSS für jede versuchte Änderung der Entscheidungen zu den Widersprüchen gegen die Sekundärnutzung von datennutzung durch das FDZ über, welche nicht durch einen Fehler abgelehnt wird und welche zu keiner Änderung einer gespeicherten Entscheidung führt ('leere' Änderung, keine Änderung der Einstellungen zu Data-Submission ServiUsagePurposes), einen Protokolleintrag gemäß A 24704* erzeugen:

Tabelle 10: ce an das FDZ weiterleiten-nsent Decision Management Protokollierung - unveränderte Entscheidungen zu widerspruchsfähigen Funktionen der ePA

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

[<=]

3.8.2 Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke

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

2465 Der initiale Zustand nach Aktivierung eines Aktenkontos ist für jeden
2466 Sekundärnutzungszweck "kein Widerspruch erteilt".

2467 Eine Änderung der Widersprüche zu Verwendungszwecken führt dazu, dass diese
2468 Informationen an das Forschungsdatenzentrum Gesundheit übermittelt werden. Die
2469 Widersprüche des Versicherten in die Sekundärnutzungszwecke sind dort bindend für die
2470 Verarbeitung der übermittelten pseudonymisierten medizinischen Daten, siehe auch 3.20-
2471 Data Submission Service .

2472 **A_26286 -Consent Decision Management - Initialisierung der**
2473 **Sekundärnutzungszwecke**

2474 Das Consent Decision Management MUSS jeden in § 303e Absatz 2 SGB V aufgeführten
2475 Sekundärnutzungszweck der elektronischen Patientenakte bei Erstellung eines neuen
2476 Aktenkontos oder bei Übernahme eines existierenden Aktenkontos einer älteren ePA-
2477 Version mit der Entscheidung "kein Widerspruch erklärt" ("permit") initialisieren. [<=]

2478 **A_26287 -Consent Decision Management - Speichern der Entscheidungen zu**
2479 **Sekundärnutzungszwecken**

2480 Das Consent Decision Management MUSS die Entscheidungen
2481 zu Sekundärnutzungszwecken der elektronischen Patientenakte unter Verwendung des
2482 SecureDataStorageKeys gesichert im Aktenkonto ablegen. [<=]

2483 **A_26288 -Consent Decision Management - Übertragen der Entscheidungen zu**
2484 **Sekundärnutzungszwecken an das FDZ**

2485 Das Consent Decision Management MUSS die Entscheidungen
2486 zu Sekundärnutzungszwecken sofort im Anschluss an eine Änderung der Entscheidung im
2487 Consent Decision Management in das Paket zur Übermittlung von pseudonymisierten
2488 medizinischen Daten zu Sekundärnutzungszwecken an das FDZ aufnehmen. [<=]

2489 **A_26291 -Consent Decision Management - unveränderte Übernahme der**
2490 **Widerspruchsentscheidung zu Sekundärnutzungszwecken**

2491 Das Consent Decision Management MUSS die über Operationen der Schnittstellen des
2492 Consent Managements [I_Consent_Decision_Management] übermittelten Entscheidungen
2493 zu Sekundärnutzungszwecken in das Aktenkonto übernehmen. [<=]

2494 **A_26292 -Consent Decision Management - Information über Änderungen der**
2495 **Entscheidungen zu Sekundärnutzungszwecken**

2496 Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung der
2497 Entscheidungen zu Sekundärnutzungszwecken, sofern eine E-Mail-Adresse vorliegt, mit
2498 einer E-Mail darüber informieren, dass Entscheidungen zu Sekundärnutzungszwecken
2499 geändert wurden, wann die Änderung erfolgte und darauf hinweisen, dass nähere
2500 Informationen zur Änderung im Protokoll zu finden sind. [<=]

2501 **A_26294 -Consent Decision Management – Weiterleitung von Widersprüchen**
2502 **gegen Sekundärnutzungszwecken an das FDZ**

2503 Das Consent Decision Management MUSS die Information über einen erklärten
2504 Widerspruch gegen Sekundärnutzungszwecke über den Data Submission Service an das
2505 FDZ weiterleiten. [<=]

2506 **A_26310 -Consent Decision Management – Rücknahme des Widerspruchs gegen**
2507 **die Sekundärdatennutzung durch das FDZ**

2508 Falls ein Widerspruch gegen die Sekundärdatennutzung durch das FDZ zurückgenommen
2509 wird MUSS das Consent Decision Management die Entscheidungen
2510 zu Sekundärnutzungszwecken über den Data Submission Service an das FDZ
2511 weiterleiten. [<=]

2512 **A_26308 -Consent Decision Management – Protokollierung geänderter**
2513 **Entscheidungen zu Sekundärnutzungszwecken**

2514 Das Consent Decision Management MUSS bei jeder Änderung einer
 2515 Widerspruchsentscheidung zur Verwendung der an das Forschungsdatenzentrum
 2516 übermittelten Daten für bestimmte Sekundärnutzungszwecke einen Protokolleintrag
 2517 gemäß A_24704* erzeugen.

2518 **Tabelle 11: Consent Decision Management Protokollierung - Widersprüche zu**
 2519 **Sekundärnutzungszwecken**

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

2520 [**<=**]

2521 Ein Aufruf der Operationen der Schnittstelle I ConsentDecisionManagement zur
 2522 Änderung der Entscheidungen zur den Widersprüchen gegen die Verwendung von Daten
 2523 für Sekundärnutzungszwecke kann erfolgreich beendet
 2524 werden, ohne dass eine bisher gespeicherte Entscheidung zu diesen Widersprüchen im
 2525 Aktensystem geändert wird. In diesem Fall erfolgt die Protokollierung gemäß A_27869-*.

2526 **A_27869 -Consent Decision Management – Protokollierung unveränderter**
 2527 **Entscheidungen zu Sekundärnutzungszwecken**

2528 Das Consent Decision Management MUSS für jede versuchte Änderung der
 2529 Entscheidungen zu den Widersprüchen gegen die Sekundärnutzung von Daten, welche
 2530 nicht durch einen Fehler abgelehnt wird und welche zu keiner Änderung einer
 2531 gespeicherten Entscheidung führt ('leere' Änderung, keine Änderung der Einstellungen
 2532 zu DataUsagePurposes), einen Protokolleintrag gemäß A_24704* erzeugen:

2533 **Tabelle 12: Consent Decision Management Protokollierung - unveränderte**
 2534 **Widersprüche zu Sekundärnutzungszwecken**

<u>Strukturelement</u>	<u>Wert</u>	<u>Erläuterung</u>
<u>AuditEvent.action</u>	<u>U</u>	<u>Update</u>
<u>AuditEvent.entity.name</u>	<u>"DataUsagePurpose"</u>	<u>Protokollierte Aktivität zuDataUsagePurpose</u>

<u>AuditEvent.entity.description</u>	<u><operationId></u>	<u>Id der verwendeten Operation (operationId gemäß Schnittstellenbeschreibung)</u>
--------------------------------------	----------------------------	--

[<=]

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

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

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

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

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

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

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

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

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

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

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

2576 Das Consent Decision Management MUSS die Konfiguration der User Specific Deny Policy
 2577 Medication auf die folgenden Nutzergruppen einschränken:
 2578

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

2579
 2580
 2581 [**<=**]

2582 **A_26405 -Consent Decision Management – Protokollierung geänderter**
 2583 **Entscheidungen der User Specific Deny Policy Medication**

2584 Das Consent Decision Management MUSS für jede Änderung der User Specific Deny
 2585 Policy Medication einen Protokolleintrag gemäß A_24704* erzeugen:

2586 **Tabelle 13: Consent Decision Management Protokollierung - User Specific Deny Policy**
 2587 **Medication**

Strukturelement	Wert	Erläuterung
AuditEvent.action	C, D	Update

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

2588 [**<=**]2589 **3.9 Entitlement Management**

2590 Befugnisse (Entitlements) werden individuell für jeden Nutzer des Aktenkontos erstellt
 2591 (Versicherter, Vertreter, Leistungserbringerinstitutionen, Kostenträger, Ombudsstelle und
 2592 Fachdienste). Eine erteilte Befugnis ist notwendige Voraussetzung für die Nutzung des
 2593 Aktenkontos und zum internen Bezug des Datenpersistierungsschlüssels
 2594 (SecureDataStorageKey) für den Zugriff auf die Dokumenten- und Datenverwaltung.

2595 Eine Befugnis enthält folgende Informationen:

2596 **A_23734-01 -Entitlement Management - Definition einer Befugnis**

2597 Das Entitlement Management MUSS für eine individuelle Befugnis die folgenden Daten
 2598 nutzen und verwalten:

2599 **Tabelle 14: Inhalt einer Befugnis**

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

(displayName)			
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 KVRN	Wird durch das Entitlement Management gesetzt.	nein
Name des Erstellers (issued-displayName)	Name der Institution, des Nutzers	Wird durch das Entitlement Management gesetzt.	nein

2600 **【<=】**

2601 *Hinweis: Ein Nutzer ist der Adressat, für den die Befugnis ausgestellt wird. Der Ersteller*
 2602 *ist der Nutzer, welcher die Befugnisausstellung veranlasst hat. Die Bezeichner in () sind*
 2603 *die Bezeichner in den Schnittstellenbeschreibungen.*

2604 *Hinweis (*): A_23734 definiert eine "vollständige" Befugnis, welche auch Daten enthält,*
 2605 *die für eine Prüfung einer gültigen Befugnis im Kontext einer Schnittstellenoperation*
 2606 *nicht notwendig sind. Für diesen Zweck wird nur der (HSM-) signierte Anteil als Ergebnis*
 2607 *einer Befugnisverifikation verwendet (signiertes Element = ja). Eine gespeicherte*
 2608 *Befugnis enthält jedoch alle Elemente für eine qualifizierte Verwaltung der Befugnisse*
 2609 *durch einen Versicherten oder Vertreter.*

2610 *Hinweis:* Befugnisse können durch das Aktensystem selbst (initiale Befugnisse), durch
 2611 den Versicherten oder einen befugten Vertreter unter Verwendung eines ePA-FdV oder
 2612 durch eine Leistungserbringerinstitution in einer Behandlungssituation erstellt werden.

2613 Eine Befugnis kann nur für Nutzer und Nutzergruppen mit bestimmter Rolle erteilt
 2614 werden. Nutzergruppen mit abweichenden Rollen können nicht befugt werden und
 2615 erhalten keinen Zugriff auf das Aktenkonto.

2616 Erfolgt die Befugniserteilung durch eine Leistungserbringerinstitution in einer
 2617 Behandlungssituation, wird eine vorgegebene Gültigkeitsdauer der Rolle des Befugten
 2618 entsprechend durch das Entitlement Management vergeben. Ein Versicherter oder ein
 2619 befugter Vertreter kann den Gültigkeitszeitraum frei wählen (ausgenommen
 2620 Vertreterbefugnisse).

2621 **A_23941-01 -Entitlement Management - Erteilung von Befugnissen für**
 2622 **berechtigte Nutzergruppen und Nutzer**

2623 Das Entitlement Management MUSS die Erteilung von Befugnissen in der jeweiligen
 2624 Umgebung auf die folgenden Nutzergruppen und Nutzer einschränken:

2625 **Tabelle 15: Befugnisse für berechtigte Nutzergruppen und Nutzer**

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

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

- 2626
 2627 Hinweis:
 2628 'x' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung befugt
 2629 werden
 2630 '-' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung nicht
 2631 befugt werden
 2632
 2633 LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-
 2634 Prüfungsnachweis (Prüfziffer),
 2635 FdV = Versicherter oder Vertreter,
 2636 KTR = Kostenträger
 2637 AS = Aktensystem (systemseitig erteilte Befugnisse)
 2638 Tage = Gültigkeit in Tagen: angegebener Wert ist einschließlich aktuellem Datum, z. B.
 2639 90 Tage bedeutet aktuelles Datum + 89 Tage.
 2640 dauerhaft = Befugnis unbegrenzt gültig (Enddatum = 9999-12-31)
 2641 statisch = Gültigkeit analog 'dauerhaft', Befugnis ist implizit vorhanden.
 2642 var = Gültigkeitsdauer von 1 Tag bis dauerhaft in jeweils ganzen Tagen[<=]
 2643
 2643 Befugnisse werden durch dasEntitlement Management mit dem SecureAdminStorageKey
 2644 verschlüsselt und im Aktenkonto gesichert abgelegt.
 2645
 2645 Einzelne Nutzer können durch den Versicherten, einen befugten Vertreter oder die
 2646 Ombudsstelle explizit von der Befugnisvergabe ausgeschlossen sein (siehe 3.9.4.
 2647 Befugnisauusschluss (Blocked User Policy)). Eine Befugniserstellung ist dann weder für

2648 Leistungserbringerinstitutionen in einer Behandlungssituation, noch durch den
2649 Versicherten oder einen Vertreter möglich.

2650 Die Befugnisse für den Versicherten und den E-Rezept-Fachdienst werden dabei nicht
2651 persistiert. Diese Befugnisse werden als implizit vorhanden und gültig angenommen.

2652 Eine Besonderheit stellt hierbei eine Befugnis EU-Zugriff dar. Es gibt zu einem
2653 Zeitpunkt für ein Aktenkonto maximal eine Befugnis EU-Zugriff. Die Dauer dieser
2654 Befugnis wird durch das Aktensystem festgelegt und beträgt 1 Stunde. Das Ende der
2655 Gültigkeit (validTo) wird ermittelt vom Ausstellungszeitpunkt + 1 Stunde.

2656 **A_26167 -Entitlement Management (EU) - Erteilung der Befugnis EU-Zugriff**

2657 Das Entitlement Management MUSS die Erteilung einer Befugnis EU-Zugriff in der
2658 jeweiligen Umgebung zusätzlich zu A_23941-* auf die folgenden Nutzergruppen und
2659 Nutzer einschränken:

2660 **Tabelle 16: Befugnisse EU-Zugriff für berechnigte Nutzergruppen und Nutzer**

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

2661 Hinweis:
2662 'x' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung befugt
2663 werden
2664 '-' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung nicht
2665 befugt werden

2666
2667 LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-
2668 Prüfungsnachweis (Prüfziffer),

2669 FdV = Versicherter oder Vertreter,

2670 AS = Aktensystem (systemseitig erteilte Befugnisse)[<=]

2671 **A_24371 -Entitlement Management - Verschlüsselung der Befugnisse**

2672 Das Entitlement Management MUSS Befugnisse mit dem versichertenindividuellen
2673 SecureAdminStorageKey verschlüsseln und im Aktenkonto persistieren.[<=]

2674 **A_24372 -Entitlement Management - Keine persistente Ablage 2675 unverschlüsselter Befugnisse**

2676 Das Entitlement Management MUSS sicherstellen, dass Befugnisse ausschließlich
2677 verschlüsselt unter Verwendung des versichertenindividuellen SecureAdminStorageKey
2678 im Aktenkonto gespeichert werden.[<=]

2679 **A_24687 -Entitlement Management - Keine Speicherung oder Verwendung nicht 2680 verifizierter Befugnisse**

2681 Das Entitlement Management MUSS sicherstellen, dass ausschließlich Befugnisse
2682 persistiert oder für eine Befugnisprüfung verwendet werden, die erfolgreich durch das

2683 HSM unter Verwendung der adäquaten Regeln 'rr1 - rr4' gemäß A_24573*
 2684 befugnisverifiziert sind.[<=]

2685 **A_23842 -Entitlement Management - Eindeutigkeit der Befugnisse im** 2686 **Befugniskontext**

2687 Das Entitlement Management MUSS sicherstellen, dass im Befugniskontext keine zwei
 2688 oder mehr Befugnisse existieren, die als Identifier des befugten Nutzers die gleiche
 2689 Identifikation (`actorId`) aufweisen.[<=]

2690 **A_24785 -Entitlement Management - VSDM-Prüfungsnachweis kann höchstens** 2691 **einmal genutzt werden**

2692 Das Entitlement Management MUSS sicherstellen, dass ein VSDM-Prüfungsnachweis
 2693 (Prüfziffer) höchstens einmal zur Registrierung einer Befugnis genutzt werden kann.[<=]

2694 **A_27671 -Entitlement Management - PoPP-Token kann höchstens einmal** 2695 **genutzt werden**

2696 Das Entitlement Management MUSS sicherstellen, dass ein PoPP-Token höchstens einmal
 2697 zur Registrierung einer Befugnis genutzt werden kann.[<=]

2698 **A_27681 -Entitlement Management - Konfigurationsvariable `enforce_popp_only`**

2699 Das Entitlement Management MUSS eine Konfigurationsvariable `enforce_popp_only`
 2700 besitzen, die initial auf `false` gesetzt ist.[<=]

2701 ePA-Clients nutzen zur Befugnisvergabe die Operationen der
 2702 Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`.
 2703 Die initialen Befugnisse des Aktenkontos werden auf organisatorischem Weg direkt im
 2704 Aktenkonto erstellt.

2705 **A_24506 -Entitlement Management- Realisierung der Schnittstelle** 2706 **`I_Entitlement_Management`**

2707 Das Entitlement Management MUSS die Operationen der Schnittstelle
 2708 `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` umsetzen.[<=]

2709 **A_26168 -Entitlement Management (EU)- Realisierung der Schnittstelle** 2710 **`I_Entitlement_Management_EU`**

2711 Das Entitlement Management MUSS die Operationen der Schnittstelle
 2712 `I_Entitlement_Management_EU` gemäß `[I_Entitlement_Management_EU]`
 2713 umsetzen.[<=]

2714 **A_24987-01 -Entitlement Management - Protokolleinträge für Zugriffe auf das** 2715 **Entitlement Management**

2716 Das Entitlement Management MUSS für das Erteilen und Entziehen von Befugnissen und
 2717 das Setzen und Löschen von Befugnisaußschlüssen jeweils einen Protokolleintrag gemäß
 2718 A_24704 erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

2719 **Tabelle 17: Entitlement Management Protokollierung**

Strukturelement	Wert	Erläuterung
<code>AuditEvent.type</code>	"rest"	
<code>AuditEvent.action</code>	C, D, U	ein Code aus den genannten, je nach Operation
<code>AuditEvent.entity.name</code>	"UserBlocking"	Setzen und Löschen von Befugnisaußschlüssen

	"EntitlementManagement"		Erteilen oder Entziehen von Befugnissen
AuditEvent.entity.detail	type	value[x]	
	"blockedUserName"	<Name der LEI>	Name der LEI, für die der Befugnisausschluss gesetzt bzw. der Ausschluss zurückgenommen wurde
	"blockedUserId"	<Telematik-ID der LEI>	Telematik-ID der LEI, für die der Befugnisausschluss gesetzt bzw. der Ausschluss zurückgenommen wurde
	"UserName"	<Name der Institution oder des Vertreters>	Name der Institution oder des Nutzers für die eine Befugnis erteilt oder gelöscht wurden
	"UserId"	<Identifizier der Institution oder des Vertreters>	ID der Institution oder des Nutzers für die eine Befugnis erteilt oder gelöscht wurden
	"entitledValidTo"	<Endzeitpunkt der Gültigkeit der Befugnis>	Angabe des Endes einer erteilten Befugnis, Format gemäß [RFC3339] YYYY-MM-DDThh:mm:ssZ oder YYYY-MM-DDThh:mm:ss+/-time zone

2720

2721 [**<=**]

2722 *Hinweis: Ein Update ("U") eines Entitlements liegt vor, wenn ein existierendes*
 2723 *Entitlement aufgrund des längeren Gültigkeitszeitraums eines neuen Entitlements*
 2724 *überschrieben wird.*

2725 3.9.1 Initiale Befugnisse (static Entitlements)

2726 Einige grundsätzlich notwendige Befugnisse sind zum Zeitpunkt der Aktivierung eines
 2727 Aktenkontos verfügbar.

2728 Zu diesen initialen Befugnissen gehören die Befugnisse für den Versicherten, den E-
 2729 Rezept-Fachdienst, den Kostenträger und die Ombudsstelle. Diese Befugnisse müssen in
 2730 der Phase der Initialisierung eines Aktenkontos durch das Aktensystem erstellt werden.

2731 Diese Befugnisse sind dauerhaft gültig und unveränderbar und können nicht gelöscht
 2732 werden.

A_24145 -Entitlement Management – Implizite initiale (statische) Befugnisse

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

Element	Versicherter	E-Rezept-Fachdienst
Identifizier des befugten Nutzers (actorId)	KVNR des Versicherten (Aktenkontoinhaber)	Telematik-ID der E-Rezept vertrauenswürdigen Ausführungsumgebung
Name des befugten Nutzers (displayName)	Name des Versicherten	Name/ Bezeichnung des E-Rezept-Fachdienstes oder "Fachdienst E-Rezept"
Rolle des Nutzers (oid)	oid_versicherter	oid_erp-vau
Ende der Gültigkeit (validTo)	9999-12-31	9999-12-31

【<=】

A_24374 -Entitlement Management – Signierte initiale (statische) Befugnisse

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

Element	Kostenträger	Ombudsstelle
Identifizier des Aktenkontos (insurantid)	KVNR des Versicherten	KVNR des Versicherten
Identifizier des befugten Nutzers (actorId)	Telematik-ID des Kostenträgers	Telematik-ID der Ombudsstelle
Name des befugten Nutzers (displayName)	Name des Kostenträgers	Name/ Bezeichnung der Ombudsstelle
Rolle des Nutzers (oid)	oid_kostentraeger	oid_ombudsstelle
Ende der Gültigkeit (validTo)	9999-12-31	9999-12-31

2746 [`<=`]

2747 **A_24688-01 -Entitlement Management – Befugnisverifikation signierter initialer**
 2748 **Befugnisse**

2749 Das Entitlement Management MUSS sicherstellen, dass die initialen, signierten
 2750 Befugnisse des Kostenträgers und der Ombudsstelle spätestens beim ersten Zugriff auf
 2751 das Aktenkonto durch das HSM unter Verwendung der Regel 'rr4' gemäß A_24573*
 2752 befugnisverifiziert sind.[`<=`]

2753 **A_24533 -Entitlement Management - Keine Änderung statischer Befugnisse**

2754 Das Entitlement Management MUSS sicherstellen, dass die dauerhaften Befugnisse des
 2755 Versicherten, des E-Rezept-Fachdiensts, des Kostenträgers und der Ombudsstelle nicht
 2756 verändert oder gelöscht werden können.[`<=`]

2757 **A_24784 -Entitlement Management - Höchstens eine Befugnis für KTR und**
 2758 **Ombudsstelle pro Aktenkonto**

2759 Das Entitlement Management MUSS sicherstellen, dass in einem Aktenkonto höchstens
 2760 eine Befugnis für einen Kostenträger und höchstens eine Befugnis für eine Ombudsstelle
 2761 hinterlegt ist.[`<=`]

2762 **A_24955 -Entitlement Management - Befugnis für KTR und Ombudsstelle nur**
 2763 **bei Anlage und betreiberinterner Anbieterwechsel**

2764 Das Entitlement Management MUSS sicherstellen, dass eine signierte Befugnis des
 2765 Kostenträgers und eine signierte Befugnis der Ombudsstelle ausschließlich bei einer
 2766 Anlage eines Aktenkontos (Initialisierung) oder bei einem betreiberinternen
 2767 Anbieterwechsel in die Befugnisse des Aktenkontos aufgenommen werden.
 2768 [`<=`]

2769 **3.9.2 Erstellen einer Befugnis durch Clients**

2770 Die Anforderung zur Vergabe einer neuen Befugnis erfolgt durch die Clients der ePA. Bei
 2771 einer Befugnisvergabe aus der Umgebung der Leistungserbringer ist dieses das
 2772 Primärsystem (PS), aus der Umgebung des Versicherten ist es das ePA-FdV.

2773 Clients verwenden zur Befugnisvergabe signierte JSON Web Token (JWS). Das Token
 2774 wird zur Verifikation an das HSM übergeben. Als Ergebnis der HSM Verarbeitung liegt
 2775 eine bestätigte, CMAC gesicherte Befugnis mit den Elementen `actorId` (Identifiziert des zu
 2776 befugnenden Nutzers), `kvnr` (AktenkontoId) und `validTo` (Gültigkeitszeitraum) für die
 2777 spätere Befugnisprüfung vor. Das HSM Ergebnis wird mit den weiteren Daten gemäß
 2778 A_23734* (`oid`, `displayName`, `issued`-*) ergänzt und gemäß A_24371* mit dem
 2779 SecureAdminStorageKey gesichert im Aktenkonto abgelegt.

2780 **3.9.2.1 Befugnisvergabe durch ein ePA-FdV**

2781 Ein ePA-FdV muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

2782 **A_24587-01 -Entitlement Management - Befugnis durch ein ePA-FdV**

2783 Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ePA-
 2784 FdV über die Schnittstelle `I_Entitlement_Management` durch Verwendung eines gültig
 2785 signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:

Befugnis	Claim Name	Claim	Beispiel
Protected Header			

	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.CH.SIG	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	
	"exp"	Verfalldatum, = "iat" + 20 min	
	"insurantId"	KVNR des Aktenkontos	A123456789
	"actorId"	Identifizier (Telematik-id oder KVNR)	3-883110000092471
	"oid"	professionOid	1.2.276.0.76.4.54
	"displayName"	Name des Befugten	Test-Apotheke
	"validTo"	Ende der Gültigkeit, (Bei unbegrenzter Gültigkeit ist 9999-12-31T00:00:00Z zu verwenden.)	gemäß [RFC3339], z.B. 2025-06-30T21:59:59Z oder 2025-06-30T23:59:59+02:00

2786 **[<=]**

2787 Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve
2788 "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext
2789 der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur
2790 und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

2791 *Hinweis zu A_24587*: Im Falle der Befugnisvergabe für einen NCPeH (EU-Zugriff, "oid"*
2792 *== "oid_ncpeh") wird durch das Aktensystem sichergestellt, dass die vorgeschriebene*
2793 *Gültigkeitsdauer für derartige Befugnisse angewendet wird. Dieses erfolgt durch die*
2794 *Befugnisverifikation gemäß Regel "rr1" im HSM. Die Angabe eines Gültigkeitsendes im*
2795 *"validTo"-Element des JWT wird daher für diesen Fall ignoriert, das Element selbst muss*
2796 *jedoch vorhanden sein.*

2797 **A_24689 -Entitlement Management - Befugnisverifikation einer Befugnis durch** 2798 **ein ePA-FdV**

2799 Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein
2800 ePA-FdV unter Verwendung der Regeln 'rr1' (Befugnisvergabe durch den Versicherten)
2801 bzw. 'rr2' (Befugnisvergabe durch einen Vertreter) des HSM eine Befugnisverifikation
2802 durchführen.[<=]

2803 **A_24535 -Entitlement Management - Befugnisse für Vertreter**

2804 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId`
2805 = KVNR) ausschließlich durch den Versicherten erstellt oder gelöscht werden
2806 können. [`<=`]

2807 **A_26698 -Entitlement Management - maximale Anzahl Befugnisse für Vertreter**

2808 Das Entitlement Management MUSS sicherstellen, dass maximal fünf gültige Befugnisse
2809 für Vertreter gleichzeitig in einem Aktenkonto vorhanden sind. [`<=`]

2810 **A_24536 -Entitlement Management - Gültigkeitsdauer der Befugnisse für**
2811 **Vertreter**

2812 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId`
2813 = KVNR) ausschließlich mit einer unbegrenzten Gültigkeit erstellt werden. [`<=`]

2814 **A_24754 -Entitlement Management - E-Mail-Adresse des Vertreters**

2815 Das Entitlement Management MUSS sicherstellen, dass bei Befugnissen für Vertreter
2816 (`actorId` = KVNR) eine E-Mail-Adresse des Vertreters für dessen Benachrichtigung
2817 angegeben wird. [`<=`]

2818 Die in A_24754 angegebene E-Mail-Adresse wird ausschließlich zur Benachrichtigung des
2819 Vertreters über die eingestellte Befugnis verwendet (vgl. A_24755-*), jedoch nicht für
2820 die Geräteregistrierung. Um eine Vertretung wahrnehmen zu können und hierfür Geräte
2821 zu registrieren, muss der Vertreter in seinem Home-AS eine E-Mail-Adresse hinterlegt
2822 haben.

2823 **A_24755-01 -Entitlement Management - Benachrichtigung des Vertreters bei**
2824 **Befugniserstellung**

2825 Das Entitlement Management MUSS im Anschluss an die erfolgreiche, neue
2826 Befugniserstellung für einen Vertreter eine E-Mail an die E-Mail-Adresse des Vertreters
2827 senden, die diesen über die Befugniserstellung für das Aktenkonto des Versicherten
2828 geeignet informiert. In der Nachricht MUSS der Name des Versicherten enthalten sein
2829 und welche Art von personenbezogenen Daten vom Vertreter im Rahmen der
2830 Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine
2831 Vertreterberechtigung widerrufen kann und gegenüber wem er seine
2832 datenschutzrechtlichen Betroffenenrechte wahrnehmen kann. [`<=`]

2833 Hinweis: Unter Art der personenbezogenen Daten ist z.B. „Krankenversichertennummer,
2834 Name und E-Mail-Adresse“ gemeint, aber nicht die tatsächliche KVNR des Vertreters, der
2835 tatsächliche Name oder die tatsächliche E-Mail-Adresse.

2836 **3.9.2.2 Befugnisvergabe durch ein Primärsystem**

2837 **A_27288-01 -Entitlement Management – Abgleich der KVNR bei Erstellen einer**
2838 **Befugnis**

2839 Das Entitlement Management MUSS sicherstellen, dass für die in `setEntitlementPs` bzw.
2840 `setEntitlementsPsV2` vom Primärsystem in `x-insurantid` übergebene KVNR folgendes
2841 gilt: die KVNR in `x-insurantid` stimmt mit der KVNR überein, die in der CMAC-
2842 gesicherten Befugnis enthalten ist, die als Ergebnis des Aufrufs der Regel `rr3` mit der vom
2843 Primärsystem erhaltenen Befugnis (signiertes JWT) bzw. dem erhaltenen PoPP-Token
2844 vom HSM zurückgegeben wird.
2845 [`<=`]

2846 Ein Primärsystem muss für die Befugnisvergabe mittels VSDM-Prüfziffer ein JWS gemäß
2847 folgender Vorgabe erstellen.

2848 **A_24590-03 -Entitlement Management - Befugnis durch ein Primärsystem**

2849 Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ein
2850 Primärsystem über die Operation `I_Entitlement_Management::setEntitlementPs`
2851 durch die Verwendung eines gültig signierten JWT mit den dargestellten Mindest-Inhalten

2852 erfolgt:
2853

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.

2854 [**<=**]

2855 *Hinweis: Die Parameter "iat" und "exp" sind optional und werden durch das Entitlement*
2856 *Management nicht ausgewertet.*

2857 Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve
2858 "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext
2859 der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur
2860 und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

2861 **A_27321-01 -Entitlement Management – Abgleich hcv bei Erstellen einer** 2862 **Befugnis über VSDM-Prüfziffer in Version 2**

2863 Falls vom Primärsystem in `setEntitlementPs` eine Befugnis (signiertes JWT) mit einer
2864 Prüfziffer in Version 2 übergeben wird und das Ergebnis des Aufrufs der Regel rr3 eine
2865 interne Datenstruktur der VSDM-Prüfziffer zurückliefert, MUSS das Entitlement
2866 Management sicherstellen, dass der Wert im Attribut "hcv" des JWT mit dem Wert von
2867 hcv aus der VSDM-Prüfziffer übereinstimmt und ansonsten die
2868 Operation `setEntitlementPs` abbrechen. [**<=**]

2869 **A_27289 -Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche** 2870 **der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer**

2871 Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer
2872 Stunde maximal fünfmal eine Befugnis (signiertes JWT) über `setEntitlementPs`
2873 übermitteln kann, bei der die mitgelieferte KVNR in `x-insurantId` von der KVNR
2874 abweicht, die in der Prüfziffer der übermittelten Befugnis (signiertes JWT) enthalten ist,
2875 andernfalls für den Nutzer für diesen Zeitraum die Operation `setEntitlementPs`
2876 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]

3.9.3 Löschen von Befugnissen

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

A_24504 -Entitlement Management - Löschen ungültiger Befugnisse

Das Entitlement Management MUSS vorhandene Befugnisse, deren Enddatum der Gültigkeit überschritten ist, unverzüglich aus dem Befugniscontext des Aktenkontos vollständig löschen. [\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 3.9.1- Initiale Befugnisse (static Entitlements) .

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

A_25246 -Entitlement Management - Löschen von Befugnissen durch einen Vertreter

Das Entitlement Management MUSS sicherstellen, dass eine erteilte Befugnis für einen Vertreter (`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]

2922 3.9.4 Befugnisausschluss (Blocked User Policy)

2923 Das Entitlement Management erlaubt die Verwaltung von Widersprüchen des
2924 Versicherten oder eines Vertreters gegen die Nutzung des Aktenkontos durch spezifische
2925 Leistungserbringerinstitutionen.

2926 Ist ein Widerspruch gegen einen bestimmten Nutzer hinterlegt, so kann für diesen keine
2927 Befugnis erstellt werden, bis dieser Widerspruch zurückgenommen wird.

2928 Die Umsetzung dieser Widerspruchsverwaltung bzw. des Befugnisausschlusses erfolgt
2929 durch eine Policy (Blocked User Policy). Die Konfiguration dieser Policy obliegt dem
2930 Versicherten oder einem befugten Vertreter mittels ePA-FdV oder der Ombudsstelle.
2931 Einträge können der Policy hinzugefügt oder entfernt werden. Zum Zeitpunkt der
2932 Erstellung des Aktenkontos enthält die Blocked User Policy keine Einträge.

2933 Ein Eintrag in der Policy referenziert einen bestimmten Nutzer über seinen Identifier
2934 (Telematik-Id). Die Menge der Einträge ist nicht limitiert.

2935 Jeder Eintrag der Blocked User Policy verhindert grundsätzlich die Erstellung einer
2936 Befugnis für den referenzierten Nutzer. Erfolgt der Widerspruch (Anlegen eines neuen
2937 Eintrags) bei bestehender Befugnis für den auszuschließenden Nutzer, wird die
2938 bestehende Befugnis gelöscht.

2939 Bei Rücknahme eines Widerspruchs gegen die Nutzung des Aktenkontos für eine
2940 bestimmte Leistungserbringerinstitution wird der entsprechende Eintrag der Policy
2941 gelöscht. Anschließend kann dieser Nutzer befugt werden.

2942 Ein Widerspruch gegen die Nutzung des Aktenkontos kann nur für Nutzer der folgenden
2943 Nutzergruppen erfolgen.

2944 **A_24463-01 -Entitlement Management - zulässige Rollen für den Widerspruch** 2945 **gegen die Nutzung durch eine Leistungserbringerinstitution**

2946 Das Entitlement Management MUSS den Widerspruch gegen die Nutzung durch eine
2947 Leistungserbringerinstitution ausschließlich für Nutzer der folgenden Nutzergruppen
2948 zulassen:
2949

professionOID / Nutzergruppe
oid_praxis_arzt
oid_krankenhaus
oid_institution-vorsorge-reha
oid_zahnarztpraxis
oid_öffentliche_apotheke
oid_praxis_psychotherapeut
oid_institution-pflege
oid_institution-geburtshilfe

oid_praxis-physiotherapeut
oid_praxis-ergotherapeut
oid_praxis-logopaede
oid_praxis-podologe
oid_praxis-ernaehrungstherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin

2950 **[<=]**

2951 Ein Eintrag der Blocked User Policy enthält Angaben gemäß der folgenden Tabelle:
2952 (Beispiel)

2953 **Tabelle 18: Inhalt eines Blocked User Policy Eintrags**

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

2954 **A_25135 -Entitlement Management - Initialisierung der Blocked User Policy**
2955 Das Entitlement Management MUSS für ein Aktenkonto eine Blocked User Policy ohne
2956 initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policies über die
2957 Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`
2958 ermöglichen. **[<=]**

2959 **A_24514 -Entitlement Management - Keine Befugnis für von einer Befugnis**
2960 **ausgeschlossene Nutzer**

2961 Das Entitlement Management MUSS sicherstellen, dass für keinen durch einen Eintrag
2962 der Blocked User Policy referenzierten Nutzer eine Befugnis existiert oder erstellt werden
2963 kann. **[<=]**

2964 **A_24515 -Entitlement Management- Verschlüsselung der Einträge der Blocked**
2965 **User Policy**

2966 Das Entitlement Management MUSS Einträge der Blocked User Policy mit dem
2967 Befugnispersistierungsschlüssel (`SecureAdminStorageKey`) verschlüsseln und im
2968 Aktenkonto persistieren. **[<=]**

2969 Die Konfiguration der Blocked User Policy erfolgt über die Schnittstelle
2970 `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` durch ein ePA-FdV
2971 bzw. durch die Ömbudsstelle.

A_24965 -Entitlement Management - Information über Änderungen der Blocked User Policy

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

3.9.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)

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

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

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

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

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

A_27311 -Entitlement Management – RateLimit-oid-List

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

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

gespeichert werden. [≤]

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

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

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

- oid_praxis_arzt maximal 200 Befugnisse

- 3018 • oid_krankenhaus maximal 1.000 Befugnisse
- 3019 • oid_institution-vorsorge-reha maximal 1.000 Befugnisse
- 3020 • oid_zahnarztpraxis maximal 200 Befugnisse
- 3021 • oid_öffentliche_apotheke maximal 200 Befugnisse
- 3022 • oid_praxis_psychotherapeut maximal 100 Befugnisse
- 3023 • oid_institution-pflege maximal 100 Befugnisse
- 3024 • oid_institution-geburtshilfe maximal 100 Befugnisse
- 3025 • oid_praxis-physiotherapeut maximal 100 Befugnisse
- 3026 • oid_praxis-ergotherapeut maximal 100 Befugnisse
- 3027 • oid_praxis-logopaede maximal 100 Befugnisse
- 3028 • oid_praxis-podologe maximal 100 Befugnisse
- 3029 • oid_praxis-ernaehrungstherapeut maximal 100 Befugnisse
- 3030 • oid_institution-oegd maximal 100 Befugnisse
- 3031 • oid_institution-arbeitsmedizin maximal 100 Befugnisse

3032 innerhalb einer Stunde durch das Primärsystem im Aktensystem registrieren kann.
 3033 [\leq]

3034 **A_27291-01 -Entitlement Management – RateLimit-oid-List: Maximale Anzahl**
 3035 **von Befugnissen für LEI pro Monat**

3036 Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass

- 3037 • oid_praxis_arzt maximal 10.000 Befugnisse
- 3038 • oid_krankenhaus maximal 200.000 Befugnisse
- 3039 • oid_institution-vorsorge-reha maximal 200.000 Befugnisse
- 3040 • oid_zahnarztpraxis maximal 10.000 Befugnisse
- 3041 • oid_öffentliche_apotheke maximal 25.000 Befugnisse
- 3042 • oid_praxis_psychotherapeut maximal 10000 Befugnisse
- 3043 • oid_institution-pflege maximal 10000 Befugnisse
- 3044 • oid_institution-geburtshilfe maximal 10000 Befugnisse
- 3045 • oid_praxis-physiotherapeut maximal 10000 Befugnisse
- 3046 • oid_praxis-ergotherapeut maximal 10000 Befugnisse
- 3047 • oid_praxis-logopaede maximal 10000 Befugnisse
- 3048 • oid_praxis-podologe maximal 10000 Befugnisse
- 3049 • oid_praxis-ernaehrungstherapeut maximal 10000 Befugnisse
- 3050 • oid_institution-oegd maximal 10000 Befugnisse
- 3051 • oid_institution-arbeitsmedizin maximal 10000 Befugnisse

3052 innerhalb eines Monats durch das Primärsystem im Aktensystem registrieren kann.
 3053 [\leq]

3054 Hinweis zu A_27290-* und A_27291-*: Die Stunde bzw. der Tag müssen sich nicht auf
 3055 die aktuelle Stunde bzw. Kalendertag beziehen, sondern können auch je

3056 Leistungserbringerinstitution auf Requestzeitpunkte bezogen werden. Dann gilt für einen
3057 Monat 30 Tage.

3058 **A_27318 -ePA-Aktensystem - RateLimit-oid-List: Maßnahmen zum Schutz der**
3059 **Konfiguration**

3060 Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen
3061 umsetzen, die eine unautorisierte Änderung der *RateLimit-oid-List* verhindern. [\leq]

3062 **A_27312 -ePA-Aktensystem - RateLimit-oid-List: Konfiguration durch Betreiber**

3063 Der Betreiber des ePA-Aktensystem MUSS sicherstellen, dass die Werte für die Anzahl
3064 der maximalen Befugnisse in der *RateLimit-oid-List* durch den Betreiber des ePA-
3065 Aktensystems ausschließlich im Vier-Augen-Prinzip konfigurierbar sind. [\leq]

3066 Stellen LEI Befugnisse mittels der Operation *setEntitlementsPs* über das Primärsystem
3067 in das ePA-Aktensystem ein, wird für diese LEI geprüft, ob diese bereits das zulässige
3068 Limit erreicht hat. Nur falls dies nicht der Fall ist, kann die Befugnis eingestellt werden.
3069 Hierzu erfasst das ePA-Aktensystem außerhalb der VAU wann ein Nutzer mit welcher
3070 Rolle eine Befugnis registriert hat. Für den Nutzer wird außerhalb der VAU ein
3071 Nutzerpseudonym geführt.

3072 **A_27313-01 -Entitlement Management - Prüfen der RateLimit-oid-List beim**
3073 **Einstellen von Befugnissen**

3074 Das Entitlement Management MUSS bei Aufruf der Operation *setEntitlementsPs* oder
3075 *setEntitlementPsV2* prüfen, ob für das zur LEI gehörende Nutzerpseudonym und die oid
3076 der LEI bereits das in der *RateLimit-oid-List* vorgegebene maximale Limit pro Stunde
3077 oder Monat erreicht wurde. Falls ein Limit erreicht wurde, wird die Operation
3078 *setEntitlementsPs*, bzw. *setEntitlementPsV2*, mit einem Fehler abgebrochen. Falls
3079 kein Limit erreicht wurde, ist die Registrierung für das zur LEI gehörende
3080 Nutzerpseudonym zu vermerken. [\leq]

3081 **A_27310 -ePA-Aktensystem - Erfassung der Nutzer zur Prüfung RateLimit-oid-**
3082 **List**

3083 Das ePA-Aktensystem MUSS sicherstellen dass bei der Erfassung der Nutzerdaten
3084 außerhalb der VAU zur Prüfung der *RateLimit-oid-List* eine Profilierung über die Nutzer
3085 nicht möglich ist und zu diesem Zweck aus der TelematikId eines Nutzers ein
3086 Nutzerpseudonym abgeleitet wird, gemäß gemSpec_Krypt#7.5 Routing auf VAU-
3087 Instanzen.
3088 [\leq]

3089 **3.9.6 EntitlementDenyList**

3090 Ein Primärsystem einer Leistungserbringerinstitution (LEI) kann eine Befugnis für ein
3091 Aktenkonto eines Versicherten in einer Behandlungssituation ("Stecken" der eGK, VSDM-
3092 Prüfungsnachweis) eigenständig erstellen, wenn der Versicherte der Nutzung der ePA
3093 nicht widersprochen hat, für die konkrete Leistungserbringerinstitution im Aktenkonto
3094 kein Befugnisausschluss (3.9.4- Befugnisausschluss (Blocked User Policy)) vorliegt und
3095 die Leistungserbringerinstitution einer grundsätzlich befugbaren Nutzergruppe angehört
3096 (3.9- Entitlement Management).

3097 Die bestimmte LEI deren Telematik-ID auf einer sogenannten EntitlementDenyList
3098 stehen, wird diese Funktionalität durch das Aktensystem unterbunden, in der Weise dass
3099 eine Befugnisvergabe durch das Aktensystem unterbunden wird.

3100 Die Befugnisvergabe durch den Versicherten oder einen Vertreter mittel ePA-FdV ist
3101 durch die EntitlementDenyList nicht eingeschränkt. Über ein ePA-FdV können auch LEI
3102 befugt werden, die einen Eintrag in der EntitlementDenyList haben.

- 3103 Die EntitlementDenyList wird durch das Aktensystem bei jedem Aufruf einer Operation
 3104 zur Befugnisvergabe durch ein Primärsystem ausgewertet. Diese Operation wird mit
 3105 einem Fehler beendet, wenn die zu befugende LEI Bestandteil der Liste ist. Eventuell
 3106 vorhandene Befugnisse dieser LEI, etwa aus einer Befugnisvergabe mittels ePA-FdV,
 3107 verbleiben im Fehlerfall der Operation unverändert.
- 3108 Die EntitlementDenyList wird für alle Aktenkonten eines Aktensystems einheitlich
 3109 verwaltet. Die Verwaltung erfolgt außerhalb der VAU, die Liste muss aber für Operationen
 3110 der Befugnisvergabe innerhalb der VAU zugänglich sein.
- 3111 **A_27730 -ePA-Aktensystem - EntitlementDenyList außerhalb der VAU**
 3112 Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen
 3113 umsetzen, die eine unautorisierte Änderung der EntitlementDenyList verhindern.[<=]
- 3114 **A_27731 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren**
 3115 Das ePA-Aktensystem MUSS sicherstellen, dass falls eine LEI (Telematik-ID) aus der
 3116 EntitlementDenyList entfernt wird, in der VAU nach spätestens 24 Stunden die
 3117 EntitlementDenyList aktualisiert wird.[<=]
- 3118 **A_27732 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren -**
 3119 **Ausschluss einer LEI**
 3120 Falls eine LEI der EntitlementDenyList hinzugefügt wird, MUSS der Betreiber des ePA-
 3121 Aktensystems sicherstellen, dass die EntitlementDenyList in der VAU unverzüglich
 3122 aktualisiert wird.[<=]
- 3123 Hinweise zu A_27732-*:
- 3124 • Die gematik übermittelt die komplette aktuelle EntitlementDenyList an den
 3125 Anbieter des ePA-Aktensystems.
 - 3126 • Die gematik übermittelt die aufgrund von Sicherheitsgründen aktualisierte
 3127 EntitlementDenyList über die etablierten Incident-Prozesse.
- 3128 **A_27714 -Entitlement Management - setEntitlementPs in Abhängigkeit von**
 3129 **EntitlementDenyList**
 3130 Falls der Nutzer auf der EntitlementDenyList enthalten ist, MUSS das Entitlement
 3131 Management die Operation `setEntitlementPs` ohne Erzeugung einer Befugnis mit dem
 3132 HTTP-Statuscode 409requestMismatch abbrechen.
 3133 [<=]

3.10 Legal Policy

- 3134 ~~Die Legal Policy~~
- 3135 Technische Details zur Aktualisierung der EntitlementDenyList im
 3136 Aktensystem:
- 3137 Die gematik liefert regelmäßige Aktualisierungen der EntitlementDenyList an die
 3138 Betreiber der ePA-Aktensysteme. Die gematik möchte automatisiert überwachen können,
 3139 ob in den ePA-Aktensystemen jeweils die aktuelle Version der EntitlementDenylist
 3140 geladen ist. In den ePA-Aktensystemen gibt es jeweils ein Enforcement-Point an dem die
 3141 EntitlementDenyList technisch durchgesetzt wird. Mindestens bei Aktualisierung der
 3142 EntitlementDenyList im ePA-Aktensystem soll solch ein Enforcement-Point Auskunft über
 3143 eine BDE-Meldung darüber geben welche EntitlementDenyList ihm aktuell vorliegt. Dabei
 3144 soll eine hohe Aussagekraft der Information erreicht werden, deshalb wird ein Hashwert
 3145 über die TelematikIDs der aktuellen EntitlementDenyList erzeugt und dieser Hashwert
 3146 wird über die BDE-Daten an die gematik (Betriebsüberwachung) übermittelt.
- 3147 **A_27780 -Übertragungsformat der EntitlementDenyList (gematik->ePA-**
 3148 **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-*:

3. die Einträge in Array "TelematikIDs" alphabetisch aufsteigend sortieren,
4. die Einträge jeweils mit dem Inhalt von "separator" als Verbindungselement zu einer einzigen lange Bytefolge konkatenieren,
5. 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 verbindlichen Regelungen wenden ist.

[**<=**]

Beispiele für A 27281-*:

1)

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

2)

Mit den Daten aus dem oben aufgeführten Beispiel für A 27780-* würde ein Aktensystem pee1nuX5TxSce3QSAwdqs+Pf0L6UMCr80uM3VYtVJdU= berechnen.

A 27782 -EntitlementDenyList: Hashwertberechnung der Telematik-ID-Einträge im Aktensystem

Ein ePA-Aktensystem MUSS sicherstellen, dass bei Aktualisierung der EntitlementDenyList-Daten am Enforcement-Point der Zugriffsrechte bzgl. EntitlementDenyList wie in A 22467-* definiert, eine Meldung an die BDE erzeugt und übermittelt wird. Dabei MUSS es den dabei zu übermittelnden Hashwert wie in A 27781 definiert berechnen. (vgl. auch Hinweise zu A 22782-*)
[<=]

Hinweise zu A 27782-*:

Zum besseren Verständnis, falls der Enforcement-Point die VAU-Instanz ist, so muss beim initialen Starten der VAU-Instanz die EntitlementDenyList in die VAU-Instanz geladen werden. Diese gilt als Aktualisierung der EntitlementDenyList-Daten in der VAU-Instanz. Somit gilt dort A 27782-*.

3.10 Legal Policy

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

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

Beispiele sind:

- Apotheker haben keinen Zugriff auf dasie zahnärztliche Dokumentation in der Datenkategorie "dental".
- Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen noch löschen.

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

A_19303-223 -Legal Policy – gesetzlich vorgegebene Zugriffsrechte

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

Tabelle 19: Legal Policy

Kategorie	Nutzergruppe										
Technischer	Med	Apo	Pfleg	GH	HME	AM	KT	O	DiG	eR	Ver

Identifizier			e				R	M	A	P	
Medical Services (XDS Document Service)	Zugriffsrecht gemäß § 352 SGB V										
reports	CRUD	R	R	R	CRUD	R	-	-	-	-	RD
emp	CRUD	CRUD	R	R	R	R	-	-	-	-	RD
emergency	CRUD	R	R	R	R	R	-	-	-	-	RD
eab	CRUD	R	R	R	R	R	-	-	-	-	RD
dental	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	RD	RD	-	R	R	R	CU	-	-	-	RD
health_risk_analysis	-	-	-	-	-	-	C	-	-	-	RD
diga	R	R	R	R	R	R	-	-	CU	-	RD
care	CRUD	R	CRUD	R	R	R	-	-	-	-	RD
eau	CRUD	-	-	-	-	R	-	-	-	-	RD

rehab	CRUD	-	-	-	-	-	-	-	-	-	RD
transcripts	CRUD	-	-	-	-	-	-	-	-	-	RD
other	CRUD	-	-	-	-	R	-	-	-	-	RD
Medical Services (FHIR Data Services)	Zugriffsrecht										
medication	R	R	R	R	R	R	-	-	-	CU	R
<u>demographics</u>	=	=	=	=	=	=	CU	=	=	=	R
<u>documents</u>	R	R	R	R	R	R	=	=	=	=	R
Basic Services	Zugriffsrecht										
<u>Audit Events</u>	=	=	=	=	=	=	=	X	=	=	X
Consent Decisions	-	-	-	-	-	-	-	X	-	-	X
Constraints	-	-	-	-	-	-	-	-	-	-	X
<u>Devices</u>	=	=	=	=	=	=	=	=	=	=	X
Entitlements	x	x	x	x	x	x	-	-	-	-	x
Entitlements.Blocked User	-	-	-	-	-	-	-	x	-	-	x
Audit Events	-	-	-	-	-	-	-	X	-	-	X
Information	x	x	x	x	x	x	x	x	x	x	-
Devices	-	-	-	-	-	-	-	-	-	-	X

Nutzergruppen:

- Med = Arztpraxis, Zahnarztpraxis, Krankenhaus, Psychotherapeut, Vorsorge- und Rehabilitation, Öffentlicher Gesundheitsdienst
 - (oid_praxis_arzt,, oid_krankenhaus, oid_institution-vorsorge-reha, oid_zahnarztpraxis, oid_praxis_psychotherapeutoid_institution-oegd)
- Apo = Öffentliche Apotheke
 - (oid_öffentliche_apotheke)

- 3248 • Pflege = Gesundheits-, Kranken- und Altenpflege
- 3249 • (oid_institution-pflege)
- 3250 • GH = Geburtshilfe
- 3251 • (oid_institution-geburtshilfe)
- 3252 • HME = Heilmittelerbringer
- 3253 • (oid_praxis-physiotherapeut, oid_praxis-ergotherapeut, oid_praxis-logopaede,
- 3254 oid_praxis-podologe, oid_praxis-ernaehrungstherapeut)
- 3255 • AM = Arbeitsmedizin
- 3256 • (oid_institution-arbeitsmedizin)
- 3257 • KTR = Kostenträger
- 3258 • (oid_kostentraeger)
- 3259 • OM = Ombudsstelle
- 3260 • (oid_ombudsstelle)
- 3261 • DiGA = Digitale Gesundheitsanwendung
- 3262 • (oid_diga)
- 3263 • eRP = E-Rezept vertrauenswürdige Ausführungsumgebung
- 3264 • (oid_erp-vau)
- 3265 • Ver = Versicherter / Vertreter
- 3266 • (oid_versicherter)

3267 Legende:

- 3268 • CRUD = create, read, update, delete; update: Aktualisierung von Metadaten,
- 3269 Aktualisierung eines Dokuments
- 3270 • "-" = keine Zugriffsrechte;
- 3271 • "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den
- 3272 Dienst (Service) definiert)
- 3273 • "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- 3274 • "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung
- 3275 in einer zukünftigen Version der ePA vorgesehen.

3276 Hinweise:

- 3277 • (*) Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann der
- 3278 Versicherte bzw. sein Vertreter oder eine Leistungserbringerinstitution gemäß der
- 3279 zuvor genannten Liste definierter professionOIDs sein. Sofern ein
- 3280 Versicherter/Vertreter der Einsteller der Elternnotiz ist, darf er abweichend von
- 3281 den oben aufgeführten Zugriffsunterbindungsregeln in die Datenkategorie mit
- 3282 dem technischen Identifier 'child' schreiben.

3283 [\leq]

3284 **A_26166-02 -Legal Policy (EU) – EU-Zugriff: gesetzlich vorgegebene**

3285 **Zugriffsrechte**

3286 Das ePA-Aktensystem MUSS zusätzlich zu den Regeln aus A_19303-* alle in der
 3287 folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und
 3288 Dienste des Aktenkontos durchsetzen.

3289 **Tabelle 20: Legal Policy - EU-Zugriff**

Kategorie	Nutzergruppe
Technischer Identifier	NCPeH
Medical Services (XDS Document Service)	Zugriffsrecht gemäß § 352 SGB V
reports	-
emp	-
emergency	R
eab	-
dental	-
child	-
childsrecord	-
pregnancy_childbirth	-
vaccination	-
patient	-
receipt	-
health_risk_analysis	-
diga	-
care	-
eau	-
rehab	-
transcripts	-
other	-
Medical Services (FHIR Data Service)	Zugriffsrecht

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

3290

3291 Nutzergruppen:

3292 • NCPeH = NCPeH-Fachdienst (oid_ncpeh)

3293 Legende:

3294 • CRUD = create, read, update, delete; update: Aktualisierung von Metadaten,
3295 Aktualisierung eines Dokuments

3296 • "-" = keine Zugriffsrechte;

3297 • "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den
3298 Dienst (Service) definiert)

3299 • "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt

3300 • "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung
3301 in einer zukünftigen Version der ePA vorgesehen.3302 [**<=**]

3303 Die folgende Tabelle erläutert die Kategorien aus A_19303-* und A_26166-*:

3304 **Tabelle 21: Beschreibung der Kategorien**

Technischer Identifier	Beschreibung
Medical Services	XDS Document Service
reports	Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen
emp	Elektronischer Medikationsplan

emergency	Daten der elektronischen Notfalldaten nach § 334 Absatz 1 Satz 2 Nummer 5 und 7
eab	Daten in elektronischen Briefen zwischen den an der Versorgung der Versicherten teilnehmenden Ärzten und Einrichtungen (elektronische Arztbriefe)
dental	Daten aus der zahnärztlichen Dokumentation
child	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
childsrecord	Archiv aus ePA 2.x: Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
pregnancy_childbirth	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass) sowie Daten, die sich aus der Versorgung der Versicherten mit Hebammenhilfe ergeben
vaccination	Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation)
patient	Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden
receipt	Bei Kostenträgern gespeicherte Daten über die in Anspruch genommenen Leistungen des Versicherten
health_risk_analysis	Ergebnisse datengestützter Auswertungen der Krankenkassen zu individuellen Gesundheitsrisiken gemäß SGB V § 25b.
diga	Daten des Versicherten aus digitalen Gesundheitsanwendungen des Versicherten nach § 33a.
care	Daten zur pflegerischen Versorgung des Versicherten nach den §§ 24g, 37, 37b, 37c, 39a und 39c und der Haus- oder Heimpflege nach § 44 des Siebten Buches und nach dem Elften Buch
eau	Daten nach § 73 Absatz 2 Satz 1 Nummer 9 ausgestellte Bescheinigung über eine Arbeitsunfähigkeit

rehab	Daten der Heilbehandlung und Rehabilitation nach § 27 Absatz 1 des Siebten Buches
transcripts	Elektronische Abschriften von der Patientenakte eines Primärsystems gemäß §630g Abs. 2 BGB
other	Sonstige von Leistungserbringern für Versicherten bereitgestellte Daten, insbesondere Daten, die sich aus der Teilnahme des Versicherten an strukturierten Behandlungsprogrammen bei chronischen Krankheiten gemäß § 137f ergeben
Medical Services	<u>Medication</u><u>FHIR Data</u> Services
medication	Verordnungs-, Dispensier- und Medikationsdaten in einer elektronischen Medikationsliste (eML) und einem elektronischen Medikationsplan (eMP)
<u>demographics</u>	<u>Bereitstellung demographischer Daten des Versicherten für Medical Services</u>
<u>audit</u>	<u>Protokolle von Zugriffen aller Nutzer auf die Akte des Versicherten</u>
<u>documents</u>	<u>Suche & Bereitstellung (medizinischer) Dokumente aus dem XDS Document Service</u>
Basic Services	Account Management
Consent Decisions	Management der Entscheidungen zu widerspruchsfähigen Funktionen der ePA
Constraints	Management der Konfiguration der General Deny Policy
Entitlements	Management der Befugnisse für Nutzer und Nutzergruppen
Audit Events	Abruf der Protokolleinträge eines Aktenkontos
Information	Informationen für nicht befugte Nutzer
Devices	Management der registrierten Geräte eines Nutzers

3305

3306

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

3307

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

3308

3309

3310

A_24548 -Legal Policy - Durchsetzung der Zugriffsrechte der Legal Policy

3311

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

3312

3313

3314

3.11 Constraint Management

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

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

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

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

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

Das Constraint Management MUSS die Konfiguration der General Deny Policy auf die folgenden Nutzergruppen einschränken:

Nutzergruppe [professionOID] der General Deny Policy

oid_praxis_arzt

oid_krankenhaus

oid_institution-vorsorge-reha

oid_zahnarztpraxis

oid_öffentliche_apotheke

oid_praxis_psychotherapeut

oid_institution-pflege

oid_institution-geburtshilfe

oid_praxis-physiotherapeut

oid_institution-oegd

oid_institution-arbeitsmedizin

oid_diga

oid_praxis-ergotherapeut

oid_praxis-logopaede

oid_praxis-podologe

oid_praxis-ernaehrungstherapeut

[<=]

A_24390-01 -Constraint Management- Anwendung der General Deny Policy

Das Constraint Management MUSS bei jedem Zugriff auf Daten durch den XDS Document Service durch befugte Nutzer oder Nutzergruppen die General Deny Policy anwenden und den Zugriff verhindern, wenn ein Dokument oder dessen assoziierter Ordner oder dessen assoziierte Datenkategorie in der Policy konfiguriert ist.

[<=]

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

Datendienste (Medication Service) können nicht auf Daten- oder Ordner Ebene verborgen werden. Hier gelten die Regelungen bezüglich des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA (siehe 3.8- Consent Decision Management).

Die Kategorie "emp", bzw. einzelne Dokumente dieser Kategorie, des XDS Document Service dürfen nicht verborgen werden. Die Nutzung der Dokumente der Kategorie "emp" wird über das Consent Decision Management, bzw. einen erteilten Widerspruch gegen die widerspruchsfähige Funktion "medication" der ePA verhindert (siehe 3.8- Consent Decision Management).

Die Operationen der Schnittstelle des Constraint Managements erlauben die Konfiguration der General Deny Policy durch den Versicherten oder einen befugten Vertreter.

A_24395 -Constraint Management - Realisierung der Schnittstelle**I_Constraint_Management_Insurant**

Das Constraint Management MUSS die Operationen der Schnittstelle I_Constraint_Management_Insurant gemäß [I_Constraint_Management_Insurant] umsetzen.[<=]

A_24887-01 -Constraint Management - Protokolleinträge für Zugriffe auf das Constraint Management

Das Constraint Management MUSS für das Aufnehmen und Löschen von Einträgen in die General Deny Policy jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertbelegung zu berücksichtigen:

Tabelle 22: Constraint Management Protokollierung

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die API
	"object"		Bei intern ausgelösten Änderungen (XDS Document Service confidentiality code

			("CON"), Löschen von Dokumenten oder Ordnern)
AuditEvent.action	C, D		
AuditEvent.entity.name	"GeneralDenyPolicy"		Eintrag für das Aufnehmen(Create) von Einträgen in die oder Löschen (Delete) von Einträgen aus der General Deny Policy
AuditEvent.entity.detail	type	value[x]	
	"DocumentTitle"	<XDSDocumentEntry.title>	wenn sich der Eintrag (Create oder Delete) der Policy auf ein Dokument bezieht
	"RootDocumentId"	<rootDocumentId>	wenn sich der Eintrag (Create oder Delete) der Policy auf ein Dokument bezieht
	"FolderTitle"	<XDSFolder.title>	wenn sich der Eintrag (Create oder Delete) der Policy auf einen Folder bezieht
	"FolderEntryUUID"	<Folder.entryUUID>	wenn sich der Eintrag (Create oder Delete) der Policy auf einen Folder bezieht
	"CategoryId"	<categoryId>	wenn sich der Eintrag (Create oder Delete) der Policy auf eine Kategorie bezieht

3366

3367 **[<=]**

3368 Für die Policy gelten folgende Vorgaben.

3369 **A_24393-01 -Constraint Management - Initialisierung der General Deny Policy**

3370 Das Constraint Management MUSS für ein Aktenkonto eine General Deny Policy ohne
 3371 initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policy über die

3372 Schnittstelle `I_Constraint_Management_Insurant` gemäß
3373 `[I_Constraint_Management_Insurant]` ermöglichen. [`<=`]

3374 **A_24462-01 -Constraint Management - Konfiguration der General Deny Policy**
3375 **anpassen nach Löschen von Ordnern**

3376 Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn
3377 diese einen Ordner referenzieren und dieser Ordner aus dem Aktenkonto gelöscht
3378 wird. [`<=`]

3379 **A_24461-01 -Constraint Management - Konfiguration der General Deny Policy**
3380 **anpassen nach Löschen von Dokumenten**

3381 Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn
3382 diese ein spezifisches Dokument referenzieren und dieses Dokument aus dem
3383 Aktenkonto gelöscht wird. [`<=`]

3384 **A_24516-01 -Constraint Management - Speichern der Inhalte der General Deny**
3385 **Policy**

3386 Das Constraint Management MUSS Einträge aus der General Deny Policy unter
3387 Verwendung des `SecureDataStorageKeys` gesichert im Aktenkonto ablegen. [`<=`]

3388 **3.11.1 Aktenkontoweites Verbergen (General Deny Policy)**

3389 Die General Deny Policy wird durch das Aktensystem für die in A_24306-* unter "General
3390 Deny Policy" aufgeführten Nutzergruppen angewendet und durchgesetzt. Einträge der
3391 General Deny Policy gelten dabei immer für alle aufgeführten Nutzergruppen gemeinsam.

3392 Die Konfiguration der General Deny Policy erfolgt durch den Versicherten oder einen
3393 befugten Vertreter mittels ePA-FdV. Einträge können hinzugefügt oder entfernt werden.
3394 Zum Zeitpunkt der Erstellung des Aktenkontos enthält die General Deny Policy keine
3395 Einträge.

3396 Ein Eintrag in der General Deny Policy referenziert entweder ein bestimmtes Dokument,
3397 einen dynamischen Ordner oder eine Datenkategorie. Die Menge der Einträge ist nicht
3398 limitiert.

3399 Jeder Eintrag der General Deny Policy verbirgt die betroffenen Daten und verhindert
3400 deren Nutzung durch Nutzergruppen gemäß A_24306-*. Enthält ein Eintrag der Policy
3401 einen dynamischen Ordner oder eine Kategorie, so werden alle in diesem Ordner bzw.
3402 Kategorie enthaltenen Daten verborgen und von der Nutzung ausgeschlossen. Ein
3403 dynamischer Ordner selbst wird ebenfalls verborgen und von der Nutzung
3404 ausgeschlossen, eine Kategorie selbst wird nicht verborgen. Verborgene Daten schränken
3405 die Anwendung der Datenoperationen ein, die konkreten Auswirkungen sind bei den
3406 jeweiligen Operationen definiert.

3407 Beim kategorienbasierten Verbergen von dynamischen Ordnern kann ein einzelner
3408 Ordner oder die Datenkategorie an sich verborgen werden. In letzterem Fall werden alle
3409 assoziierten Ordner verborgen.

3410 Bei Kategorien und Ordnern, die zusammengesetzte MIOs oder strukturierte Dokumente
3411 enthalten (MIOs oder strukturierte Dokumente, deren Inhalt über mehrere XDS
3412 Dokumente mit Zusammenhang verteilt ist - "Passdokumente") ist das Verbergen
3413 einzelner XDS Dokumente des MIOs nicht sinnvoll und daher nicht zulässig. In diesen
3414 Fällen erfolgt das Verbergen der Daten durch das Verbergen der Kategorie bzw. des
3415 dynamischen Ordners. Diese Einschränkung betrifft die Sammlungstypen "mixed" und
3416 "uniform".

3417 Für das erfolgreiche Verbergen von Daten durch Einträge der General Deny Policy muss
3418 das adressierte XDS Dokument, der Ordner oder die Kategorie im Aktensystem

3419 vorhanden sein. Wird im Verlauf von Operationen ein XDS Dokument oder ein Ordner
 3420 gelöscht, so werden auch die referenzierenden Policy-Einträge automatisch entfernt
 3421 (siehe A_24461-* und A_24662-*).

3422 Ein Eintrag der General Deny Policy enthält Angaben gemäß der folgenden Tabelle:

3423 **Tabelle 23: Inhalt eines General Deny Policy Eintrags**

Element		Inhalt	Erläuterung
denyType		"document" oder "folder" oder "category"	Art des zu verbergenden Inhalts,
parameter:			eine technische Referenz passend zu "denyType"
[choice]	rootDocumentId	documentEntry.referenceIdList, Item "rootDocumentUniqueId"	Identifiziert das zu verbergende XDS Dokument
	folderUUID	folder.entryUUID	Identifiziert das zu verbergende dynamische Ordner
	categoryId	categoryId	technischer Identifizierer der zu verbergenden Kategorie

3424

3425 Beispiel:

3426 **Tabelle 24: Verbergen eines Medical Service**

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

3427 3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des 3428 confidentialityCodes

3429 Das Verbergen über den confidentialityCode ist im Kontext der Operationen des XDS
 3430 Document Service definiert und in 3.13.1.10- Verbergen von Dokumenten durch
 3431 Verwendung des confidentialityCode beschrieben.

3.12 Device Management

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

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

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

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

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

A_24828 -Device Management - Realisierung der Schnittstelle

I_Device_Management_Insurant

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

A_25164 -Device Management - Beschränkung der Schnittstellenoperationen auf Geräte des Nutzers

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

A_26153 -Device Management - Nutzen von Device Management auch bei Widerspruch gegen Aktenkonto

Das Device Management MUSS sicherstellen, dass das Device Management auch von Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben. [`<=`]

A_26154-01 -ePA-Aktensystem - Ausschließlich Nutzen von Email Management und Device Management bei Widerspruch

Das ePA-Aktensystem MUSS sicherstellen, dass Versicherte, die einem Aktenkonto widersprochen haben, für sich selbst ausschließlich das Email Management und das Device Management nutzen können. [`<=`]

A_26155 -Device Management - Versicherte nutzen Device Management ausschließlich im Home-AS

Das Device Management des ePA-Aktensystems MUSS sicherstellen, dass das Device Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-Aktensystem das Home-AS ist. [\leq]

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. [\leq]

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.

[\leq]

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. [\leq]

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

A_25270 -Device Management - Erzeugung von Geräteinformationen und Geräteregistrierungscode bei der Geräteregistrierung

Das Device Management MUSS bei der Geräteregistrierung für das zu registrierende Gerät eines Nutzers

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

erzeugen. [\leq]

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:

- deviceIdentifier
- deviceToken
- createdAt (Zeitpunkt der Erzeugung des deviceTokens)
- lastUse
- status
- displayName
- Geräteregistrierungscode,

- 3524 • Fehlerzähler.

3525 [\leq]

3526 Hinweis zu A_25271-*: Für die verschlüsselte Speicherung der Geräteinformationen sind
3527 die Anforderungen aus Abschnitt 3.5.1.3 zu berücksichtigen.

3528 **A_25272 -Device Management - Pseudonyme Speicherung der** 3529 **Geräteinformationen**

3530 Das Device Management MUSS sicherstellen, dass die Zuordnung der außerhalb der VAU
3531 persistierten verschlüsselten Geräteinformationen zum Nutzer eindeutig ist und durch ein
3532 Pseudonym erfolgt. [\leq]

3533 Hinweis: Aus A_25272 folgt, dass die Zuordnung der Speicherung der verschlüsselten
3534 Geräteinformationen nicht über die KVN-R des Nutzers erfolgen darf.

3535 **A_25273 -Device Management - Gültigkeitsdauer des Geräteregistrierungscodes**

3536 Das Device Management MUSS sicherstellen, dass der bei der Geräteregistrierung
3537 erzeugte Geräteregistrierungsscode maximal 6 Stunden nach Erzeugung der DeviceID
3538 (createdAt) für die Verifikation eines Gerätes genutzt werden kann. [\leq]

3539 **A_25274 -Device Management - Löschen nach Gültigkeitsdauer des** 3540 **Geräteregistrierungscodes**

3541 Das Device Management MUSS sicherstellen, dass die Geräteinformationen für eine nicht
3542 bestätigte Geräteregistrierung nach Ende der Gültigkeitsdauer des
3543 Geräteregistrierungscodes gelöscht werden. [\leq]

3544 **A_25275 -Device Management - Versenden des Geräteregistrierungscodes per** 3545 **E-Mail**

3546 Das Device Management MUSS bei der Geräteregistrierung für den Nutzer, für den das
3547 Gerät registriert werden soll, alle im Aktensystem hinterlegten E-Mail-Adressen ermitteln
3548 und an alle ermittelten E-Mail-Adressen eine E-Mail in einer für den Nutzer verständlichen
3549 Form mit folgenden Informationen versenden:

- 3550 • Zweck der E-Mail,
- 3551 • Geräteregistrierungsscode,
- 3552 • Gültigkeitsdauer des Geräteregistrierungscodes.

3553 [\leq]

3554 **A_25276 -Device Management - Bestätigung mittels Geräteregistrierungscodes**

3555 Das Device Management MUSS für einen übergebenen Geräteregistrierungsscode und eine
3556 übergebene DeviceID (deviceIdentifier und deviceToken) prüfen, ob der vom Device
3557 Management bei der Geräteregistrierung erzeugte Geräteregistrierungsscode für das
3558 angegebene Gerät (deviceIdentifier, deviceToken) mit dem übergebenen
3559 Geräteregistrierungsscode übereinstimmt sowie der Geräteregistrierungsscode zeitlich
3560 gültig ist und

3561 1. bei Gleichheit und

3562 a. zeitlicher Gültigkeit

- 3563 • den Status für die Geräteregistrierung wechseln, so dass die erfolgreiche
3564 Bestätigung des Geräts aus dem Status hervorgeht,

- 3565 • den Geräteregistrierungsscode und den Fehlerzähler aus den
3566 Geräteinformationen löschen und

- 3567 • den Zeitpunkt der erfolgreichen Bestätigung in lastUsed erfassen,

3568 b. zeitlicher Ungültigkeit

- 3569 • alle Geräteinformationen zu diesem deviceIdentifier löschen,
3570 2. bei Ungleichheit den Fehlerzähler der Geräteinformation um eins erhöhen und
3571 • falls der Fehlerzähler größer oder gleich fünf ist,
3572 • alle Geräteinformationen zu diesem Gerät löschen.

3573 [<=]

3574 **A_25277 -Device Management - Sperrung bei vermehrter Anzahl von**
3575 **abgebrochenen Geräteregistrierungen**

3576 Falls für einen Nutzer innerhalb von 8 Stunden drei Geräteregistrierungen abgebrochen
3577 werden mussten, MUSS das Device Management sicherstellen, dass dieser Nutzer für 8
3578 Stunden ab dem Zeitpunkt der dritten abgebrochenen Geräteregistrierung keine Geräte
3579 mehr registrieren darf.[<=]

3580 **A_25291 -ePA-Aktensystem - Health Record Context nur mit verifizierten Gerät**

3581 Das ePA-Aktensystem MUSS sicherstellen, dass ein Versicherter (auch wenn er als
3582 Vertreter agiert) einen Health Record Context ausschließlich mit einem verifizierten Gerät
3583 öffnen kann, außer für den Fall, dass sich der Versicherte am ePA-FdV des Vertreters
3584 anmeldet (d.h. x-authorize-representative=True bei der Operation
3585 I_Authorization_Service::sendAuthorizationRequestFdV).[<=]

3586 Eine Geräteregistrierung im Home-AS kann in einem anderen Aktensystem nachgenutzt
3587 werden. Hierzu kann ein ePA-FdV mittels `getDeviceAttestation` eine Device Attestation
3588 vom Home-AS abrufen, welche beim anderen Aktensystem genutzt werden kann.

3589 **A_26157 -Device Management - Device Attestation kann nur mit verifiziertem**
3590 **Gerät abgerufen werden**

3591 Das Device Management MUSS sicherstellen, dass die Operation `getDeviceAttestation`
3592 ausschließlich nach erfolgreicher Authentifizierung des Nutzers und mit einem auf den
3593 Nutzer registrierten und verifizierten Gerät erfolgt.

3594 [<=]

3595 **A_26156 -Device Management - Inhalte der Device Attestation**

3596 Das Device Management MUSS sicherstellen, dass eine von einem ePA-FdV über die
3597 Operation `getDeviceAttestation` abgerufene Device Attestation folgende Inhalte
3598 enthält:

Attribut	Inhalt
actorId	KVNR aus dem ID-Token des angemeldeten Nutzers (bzw. der User Session)
iat	Zeitstempel Ausgabezeitpunkt
exp	Verfalldatum, = "iat" + 2 Stunden

3599 [<=]

3600 **A_26158 -Device Management - Signatur der Device Attestation**

3601 Das Device Management MUSS sicherstellen, dass die über `getDeviceAttestation`
3602 abgerufene Device Attestation mit dem privaten Schlüssel der Signaturidentität der VAU
3603 des Home-AS signiert wird.[<=]

3.13 Medical Services

A_25830-02 -Medical Services - Reihenfolge der Auswertung Legal Policy, Consent Decisions und Constraints

Die Medical Services MÜSSEN bei der Ausführung von Operationen der Schnittstellen der Medical Services sicherstellen, dass die Prüfung zu Bedingungen

1. der Einschränkung der Rolle des Aufrufenden (oid),
2. der Existenz des Aktenkontos (Status UNKNOWN oder INITIALIZED),
3. des Zustands des Aktenkontos (Status ACTIVATED),
4. der Befugnis des Aufrufenden,
5. der Legal Policy,
6. der Entscheidungen zu widerspruchsfähigen Funktionen der ePA,
7. der Einträge der General Deny Policy
8. des Entscheidungen zum nutzerspezifischen Ausschluss von der Teilnahme am digital gestützten Medikationsprozess

in der dargestellten Reihenfolge erfolgt. Diese Reihenfolge MUSS auch eingehalten werden, wenn einzelne Prüfungen für eine Operation nicht anwendbar, bzw. nicht relevant, sind. [≤]

Hinweis: Eine Operation kann nicht erfolgreich ausgeführt werden, weil dieses der Legal Policy widerspricht und weil ein Eintrag der General Deny Policy die Ausführung verhindert. Die Fehlermeldung zum Abbruch der Operation resultiert dann aus der Prüfung der Legal Policy, da die Bedingungen dieser gemäß der definierten Reihenfolge vor den Bedingungen der General Deny Policy geprüft werden müssen.

3.13.1 XDS Document Service

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

Jedes eingestellte Dokument wird vom XDS Document Service mit einer automatischen Zuordnung zu einem statischen Ordner, welcher die Datenkategorie repräsentiert, erweitert. Diese statischen Ordner sind initial bei jedem Aktenkonto eines Versicherten existent. Die serverseitige Zuordnung in diese Ordner erfolgt anhand der XDS-Metadaten in Kombination mit der Nutzergruppe des Einstellers. Das bedeutet weiterhin, dass das Anlegen von statischen Ordnern durch ePA-Clients nicht erlaubt ist, um eine zweifelsfreie Anwendung der Zugriffsregeln auf Grundlage der Datenkategorien zu gewährleisten.

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

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

Die Durchsetzung der Zugriffskontrolle auf die Kategorien, Ordner und Dokumente gemäß der gesetzlichen Vorgaben und ggf. weiterer Beschränkungen durch den Versicherten oder einen Vertreter erfolgt durch das Constraint Management (siehe 3.11-Constraint Management).

3.13.1.1 Formatprüfung beim Einstellen von Dokumenten

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

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

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

[<=]

A_24864-04 -XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten

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

- application/pdf nur PDF/A gemäß A_25233 (pdf)
- text/plain (txt)
- application/xml (xml)
- application/hl7-v3 (xml)
- application/pkcs7-mime (p7s oder p7)
- application/fhir+xml (xml)
- application/fhir+json (json)
- application/json (json)

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

Hinweise zu A_24864-*:

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

3689

A_25009-03 -XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten durch Versicherte

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

- application/pdf nur PDF/A gemäß A_25233 (pdf)
- text/plain (txt)
- application/fhir+xml (xml)
- application/json (json)

Ferner MUSS der XDS Document Service sicherstellen, dass ausschließlich die Elternnotiz des Kinderuntersuchungshefts als FHIR Document mit dem MIME-Type "application/fhir+xml" registriert werden kann - andere FHIR Documents sind nicht zulässig.

[<=]

Hinweise zu A_24864- und A_25009-*: Die Prüfung des zulässigen Dokumentenformats muss mindestens*

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

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

Für XML-Dokumente muss eine Schema-Validierung ausschließlich auf Basis bekannter, intern vorliegender XML Schema-Definitionen durchführen. Gegen nicht intern vorliegende XML Schema-Definitionen wird nicht validiert. Die Schema-Validierung kann innerhalb des Health Record Contexts ohne zusätzliche Isolation erfolgen.

A_24867 -XDS Document Service - Isolation der Formatprüfung

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

[<=]

Hinweise zu A_24867-:*

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

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

3734 Findet eine Dokumentenformatprüfung innerhalb eines Health Record Context statt, wird
 3735 durch den Isolationsmechanismus aus A_24636-* verhindert, dass sich die
 3736 Dokumentenformatprüfung schadhaft auf andere Health Record Contexte auswirkt. Es
 3737 verbleibt dann zur Umsetzung der A_24867-* noch zu gewährleisten, dass sich die
 3738 Dokumentenformatprüfung nicht schadhaft auf den Health Record Context auswirkt, in
 3739 dem die Dokumentenformatprüfung erfolgt.

3740 Wenn Dokumentenprüfungen innerhalb eines Health Record Contexts ohne Isolation
 3741 erfolgen, muss sichergestellt werden, dass sich diese Prüfungen nicht schadhaft auf den
 3742 Health Record Context (oder andere) auswirken können. Dies ist vom Produktgutachter
 3743 zu prüfen und im Produktgutachten zu dokumentieren.

3744 Ein Ausschluss einer schadhaften Auswirkung auf den Health Record Context ist bei
 3745 folgenden Prüfungen des Dokumentenformats denkbar, so dass diese innerhalb des
 3746 Health Record Contexts ohne zusätzliche Isolationsmaßnahmen durchgeführt werden
 3747 können und kein Verstoß gegen die Anforderung A_24867-* vorliegt:

- 3748 • Prüfung der Magic Bytes des Dokuments (wo technisch möglich)
- 3749 • bei txt-, XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es
 3750 bei XML-Dokumenten kein valides UTF8 ist, eine Prüfung auf "restriktives" ISO-
 3751 8859-15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09,
 3752 0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind."
- 3753 • bei XML- und JSON-Dokumenten: Parsen der Dokumente auf valides XML bzw.
 3754 JSON mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert
 3755 und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu
 3756 bestätigen.
- 3757 • bei pkcs7-Dokumenten: Parsen der Dokumente mit Parsern, die entsprechend den
 3758 Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser
 3759 ist durch den Produktgutachter zu bestätigen.

3760 Der Produktgutachter muss bei der Umsetzung der oben genannten Prüfungen
 3761 bestätigen, dass der Ausschluss einer schadhaften Auswirkung auf den Health Record
 3762 Context (oder andere) durch die Umsetzung im Produkt tatsächlich gegeben ist.

3763

3764 **A_25285 -XDS Document Service - Sicheres Löschen von Dokumenten mit** 3765 **unzulässigem Format**

3766 Falls der XDS Document Service bei der Prüfung des Dateiformats (siehe A_24864-*)
 3767 beim Einstellen eines Dokuments ein unzulässiges Format erkennt, MUSS der XDS
 3768 Document Service das Dokument sicher löschen.
 3769 [\leq]

3770 **A_24943 -XDS Document Service - Formatprüfung exponiert keine Daten aus** 3771 **der VAU heraus**

3772 Der XDS Document Service MUSS sicherstellen, dass bei der Formatprüfung (siehe
 3773 A_24864-*) keine innerhalb der VAU verarbeiteten Daten die VAU verlassen. [\leq]

3774 **3.13.1.2 Anforderungen zur Validierung**

3775 **A_15035 -XDS Document Service – Verwendung von SOAP Message Security 1.1**

3776 Der XDS Document Service MUSS die Sicherheitsanforderungen aus SOAP Message
 3777 Security 1.1 [WSS] für die Verarbeitung von SOAP 1.2-Nachrichten umsetzen. [\leq]

3778 **A_15034 -XDS Document Service – Unterstützung von Profilen der Web** 3779 **Services Interoperability Organization (WS-I)**

3780 Der XDS Document Service MUSS das WS-I Basic Profile V2.0 [WSIBP], das WS-I Basic
3781 Security Profile Version V1.1 [WSIBSP] sowie das WS-I Attachment Profile V1.0 [WSIAP]
3782 für die Kommunikation über Web Services berücksichtigen. [≤]

3783 **A_15186 -XDS Document Service – Prüfung der Kombination von WS-**
3784 **Addressing Action und SOAP Body**

3785 Der XDS Document Service MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-
3786 Eingangsnachrichten dahingehend prüfen, ob die angegebene WS-Addressing Action zum
3787 SOAP Body passt. Ist diese Kombination nicht passend, MUSS der XDS Document Service
3788 die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und die
3789 Verarbeitung der Nachricht abbrechen. [≤]

3790 **A_15585 -XDS Document Service – Gleichheit von SOAP Action und WS-**
3791 **Addressing Action**

3792 Der XDS Document Service MUSS SOAP 1.2-Eingangsnachrichten mit einem HTTP-
3793 Statuscode 400 gemäß [RFC7231] quittieren und die Verarbeitung der Nachricht
3794 abbrechen, falls die Werte aus SOAP Action (HTTP Header) und des `Action`-Elements
3795 [WSA] des SOAP Headers nicht übereinstimmen. [≤]

3796 **A_14465-01 -XDS Document Service – XML Schema-Validierung für SOAP-**
3797 **Eingangsnachrichten**

3798 Der XDS Document Service MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-
3799 Eingangsnachrichten einer XML Schema-Validierung auf Basis ausschließlich intern
3800 vorliegender XML Schema-Definitionen unterziehen und gemäß [SOAP] verarbeiten. Sind
3801 Nachrichten nicht wohlgeformt oder ungültig, MUSS der XDS Document Service die
3802 Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren. [≤]

3803 **A_14809 -XDS Document Service – Keine Verwendung des**
3804 **"xsi:schemaLocation"-Attributs**

3805 Der XDS Document Service MUSS SOAP 1.2-Eingangsnachrichten mit einem HTTP-
3806 Statuscode 400 gemäß [RFC7231] quittieren, falls ein `xsi:schemaLocation`-Attribut
3807 gemäß [XMLSchema#2.6.3] enthalten ist. [≤]

3808 **A_14811-01 -XDS Document Service – Ablehnung von SOAP 1.2-Nachrichten**
3809 **ohne UTF-8 Kodierung**

3810 Der XDS Document Service MUSS SOAP 1.2-Nachrichten dahingehend prüfen, dass diese
3811 der Zeichenkodierung UTF-8 entsprechen, und andernfalls die Operation einem
3812 geeigneten HTTP-Statuscode gemäß [RFC7231] ablehnen. [≤]

3813 **A_21200 -XDS Document Service und Clients – UTF-8 Kodierung von SOAP 1.2-**
3814 **Nachrichten**

3815 Der XDS Document Service und Clients des XDS Document Service MÜSSEN
3816 sicherstellen, dass die XML-Inhalte der SOAP 1.2-Nachrichten, die sie senden, der
3817 Zeichenkodierung UTF-8 entsprechen. [≤]

3818 Es ist zu beachten, dass sich die Anzeige der verwendeten Kodierung in der Nachricht
3819 unterscheiden kann, z. B. in Nachrichten, in denen MTOM verwendet wird.

3820 **3.13.1.3 Namensräume**

3821 Für die Spezifikation der Schnittstellen des XDS Document Service werden die folgenden
3822 XML-Präfixe verwendet, um den Namensraum bzw. das Vokabular des XML-Dokuments
3823 zu kennzeichnen.

Präfix	Namensraum

lcm	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0
rmd	urn:ihe:iti:rmd:2017
rs	urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0
wsa	http://schemas.xmlsoap.org/ws/2004/08/addressing
wss	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
xdsb	urn:ihe:iti:xds-b:2007
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

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

3.13.1.4.1 Anforderungen an IHE ITI-Akteure

In diesem Abschnitt werden Anforderungen und Einschränkungen an relevante IHE ITI-Akteure und -Transaktionen des XDS Document Service gestellt, um die geforderte IHE ITI-Semantik zum ePA-Aktensystem zu bewahren. Werden IHE ITI-Akteure mit weiteren Sub-Akteuren gruppiert, so werden die Anforderungen der Sub-Akteure zum gruppierten Akteur übernommen. Eine Übersicht und Herleitung der IHE ITI-Akteure ist 3.13.1.4.2: Überblick über gruppierte IHE ITI-Akteure und Optionen zu entnehmen.

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

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

Der XDS Document Service DARF NICHT vom Verhalten der definierten Außenschnittstellen `I_Document_Management`, sowie `I_Document_Management_Insurant` aus Abschnitt 3.13.1.6 abweichen. Dies schließt über die Anforderungslage hinausgehende Implementierungen von IHE ITI-Akteuren und Optionen innerhalb des XDS Document Service mit ein, sodass zusätzlich implementierte IHE-Funktionalitäten keine Auswirkungen an den definierten Außenschnittstellen aufweisen dürfen. [`<=`]

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

- 3847 Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Registry"
3848 gemäß [IHE-ITI-TF1] implementieren.[<=]
- 3849 **A_14727 -XDS Document Service – Implementierung des IHE ITI-Akteurs XDS**
3850 **Document Repository**
3851 Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Repository"
3852 gemäß [IHE-ITI-TF1] implementieren.[<=]
- 3853 Die § 291a-konforme Protokollierung von Zugriffen erfolgt mit Mechanismen außerhalb
3854 des IHE ITI-TF. Eine technische Protokollierung via ATNA kann gemäß der Anforderung
3855 A_17826 dennoch erfolgen.
- 3856 **A_13809 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3857 **ATNA Audit Record Repository**
3858 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "ATNA Audit Record
3859 Repository" gemäß [IHE-ITI-TF1] implementieren.[<=]
- 3860 Die Mechanismen der IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure
3861 Application" zur Node Authentication werden über das Konzept "Vertrauenswürdige
3862 Ausführungsumgebung" (siehe 3.5- Vertrauenswürdige Ausführungsumgebung (VAU))
3863 umgesetzt, sodass die Nutzung des Integrationsprofils ATNA diesbzgl. eingeschränkt
3864 wird.
- 3865 **A_17166 -XDS Document Service – Keine Implementierung der IHE ITI-Akteure**
3866 **ATNA Secure Node sowie ATNA Secure Application für Node Authentication**
3867 Der XDS Document Service DARF zur Node Authentication die IHE ITI-Akteure "ATNA
3868 Secure Node" sowie "ATNA Secure Application" gemäß [IHE-ITI-TF1] NICHT
3869 implementieren.[<=]
- 3870 Der Zeitdienst der Telematikinfrastruktur unterstützt das Network Time Protocol in
3871 Version 4. Das IHE ITI-TF verlangt hingegen, das Zeitsynchronisierungsprotokoll in
3872 Version 3.
- 3873 **A_14654 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3874 **CT Time Client**
3875 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "CT Time Client"
3876 gemäß [IHE-ITI-TF1] implementieren.[<=]
- 3877 **A_14665 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3878 **XDS Document Source**
3879 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Source"
3880 gemäß [IHE-ITI-TF1] implementieren.[<=]
- 3881 **A_14667 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3882 **XDS Integrated Document Source/Repository**
3883 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Integrated Document
3884 Source/Repository" gemäß [IHE-ITI-TF1] implementieren.[<=]
- 3885 **A_14668 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3886 **XDS Document Consumer**
3887 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Consumer"
3888 gemäß [IHE-ITI-TF1] implementieren.[<=]
- 3889 **A_14666 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3890 **XDS Patient Identity Source**
3891 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Patient Identity
3892 Source" gemäß [IHE-ITI-TF1] implementieren.
3893 [<=]

3894 **A_14669 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3895 **XDS On-Demand Document Source**
3896 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS On-Demand Document
3897 Source" gemäß [IHE-ITI-TF1] implementieren.[<=]

3898 **A_14950 -XDS Document Service – Keine Angabe einer Fehlerlokalisierung im**
3899 **RegistryError-Element**
3900 Der XDS Document Service DARF NICHT das `location`-Attribut im `rs:RegistryError-`
3901 Element in der IHE ITI-Ausgangsnachricht verwenden, sofern ein Fehler bei der
3902 Verarbeitung einer IHE ITI-Eingangsnachricht auftritt. Diese Einschränkung gilt nur für
3903 Error Stack Traces bzw. der Offenbarung von Programmierdetails.[<=]

3904 **A_15081 -XDS Document Service – Implementierung des IHE ITI-Akteurs RMU**
3905 **Update Responder**
3906 Der XDS Document Service MUSS den IHE ITI-Akteur "RMU Update Responder"
3907 gemäß [IHE-ITI-RMU] implementieren.[<=]

3908 3.13.1.4.1.1 Gruppierungen mit anderen IHE ITI-Akteuren
3909 **A_15093-02 -XDS Document Service – Gruppierung RMU Update Responder mit**
3910 **Document Registry**
3911 Der XDS Document Service als RMU-Akteur "Update Responder" MUSS mit dem XDS-
3912 Akteur "Document Registry" gemäß [IHE-ITI-RMU] gruppiert sein.[<=]

3913 3.13.1.4.1.2 Optionen des IHE ITI-Akteurs
3914 **A_15094 -XDS Document Service – RMU Update Responder ohne "Forward**
3915 **Update"-Option**
3916 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option
3917 "Forward Update" unterstützen.
3918 [<=]

3919 **A_15095-02 -XDS Document Service – RMU Update Responder ohne "XCA**
3920 **Persistence"-Option**
3921 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option
3922 "XCA Persistence" unterstützen.[<=]

3923 **A_15096-02 -XDS Document Service – RMU Update Responder mit "XDS**
3924 **Persistence"-Option**
3925 Der XDS Document Service als RMU-Akteur "Update Responder" MUSS die Option "XDS
3926 Persistence" unterstützen.[<=]

3927 **A_15097 -XDS Document Service – RMU Update Responder ohne "XDS Version**
3928 **Persistence"-Option**
3929 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option
3930 "XDS Version Persistence" unterstützen.[<=]

3931 3.13.1.4.1.3 Gruppierungen mit anderen IHE ITI-Akteuren
3932 3.13.1.4.1.4 Optionen des IHE ITI-Akteurs
3933 **A_14637 -XDS Document Service – XDS Document Registry ohne**
3934 **"Asynchronous Web Services Exchange"-Option**
3935 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
3936 "Asynchronous Web Services Exchange" unterstützen.[<=]

3937 **A_14638 -XDS Document Service – XDS Document Registry mit "Reference ID"-**
3938 **Option**
3939 Der XDS Document Service als XDS-Akteur "Document Registry" MUSS die
3940 Option "Reference ID" unterstützen.[<=]

3941 **A_14639 -XDS Document Service – XDS Document Registry ohne "Patient**
3942 **Identity Feed"-Option**

3943 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
 3944 "Patient Identity Feed" unterstützen.
 3945 [\leq]

3946 **A_14640 -XDS Document Service – XDS Document Registry ohne "Patient**
 3947 **Identity Feed HL7v3"-Option**

3948 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
 3949 "Patient Identity Feed HL7v3" unterstützen. [\leq]

3950 **A_14641 -XDS Document Service – XDS Document Registry ohne "On-Demand**
 3951 **Documents"-Option**

3952 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
 3953 "On-Demand Documents" unterstützen. [\leq]

3954 3.13.1.4.1.5 Optionen des IHE ITI-Akteurs

3955 **A_14636 -XDS Document Service – XDS Document Repository ohne**
 3956 **"Asynchronous Web Services Exchange"-Option**

3957 Der XDS Document Service als XDS-Akteur "Document Repository" DARF NICHT die
 3958 Option "Asynchronous Web Services Exchange" unterstützen. [\leq]

3959 *3.13.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen*

3960 Die folgende Tabelle fasst die oben definierten Anforderungen zu Gruppierungen und
 3961 Optionen zusammen. Dabei wird die folgende Notation für Optionalitäten (Opt.)
 3962 verwendet:

3963 **Tabelle 25: Kennzeichnung von Optionalitäten**

Code	Bedeutung
R	Required - Mit "R" gekennzeichnete IHE ITI-Akteure oder Optionen MÜSSEN implementiert oder gruppiert werden.
X	Mit "X" gekennzeichnete IHE ITI-Akteure oder Optionen DÜRFEN NICHT implementiert oder gruppiert werden.

3964

3965 **Tabelle 26: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den**
 3966 **Außerschnittstellen des XDS Document Service**

IHE ITI-Akteur	Opt.			Umzusetzende Option des IHE ITI-Akteurs	Opt.
		Gruppierung mit anderem IHE ITI-Akteur	Opt.		
ATNA Audit Record Repository	X				
CT Time Client	X				

RMU Update Responder	R			Forward Update	X
				XCA Persistence	X
				XDS Persistence	R
				XDS Version Persistence	X
		Document Registry	R		
XDS Document Consumer	X				
XDS Document Registry	R			Asynchronous Web Services Exchange	X
				Document Metadata Update	X
				On-Demand Documents	X
				Patient Identity Feed	X
				Patient Identity Feed HL7v3	X
				Reference ID	R
		ATNA Secure Node oder Secure Application für Node Authentication	X		
XDS Document Repository	R			Asynchronous Web Services Exchange	X
		ATNA Secure Node oder Secure Application für Node	X		

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

3967

3968 *3.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen*3969 **A_17832 -XDS Document Service – Unterstützung MTOM/XOP**

3970 Der XDS Document Service MUSS gemäß den Anforderungen von [IHE-ITI-
 3971 TF2x#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP
 3972 [MTOM] verwenden. [≤]

3973 **A_24524 -XDS Document Service - Migration, Upload: Normalisieren des URI**

3974 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten
 3975 den `DocumentEntry.URI` normalisieren. Dies gilt für `FileURI`, z.
 3976 B. "<file:///C:/path/to/file.html#anchor>" oder "`/C/path/to/file.html#anchor`". Die URI MUSS
 3977 auf den reinen Dateinamen mit Extension (d. h. ohne Pfadangaben) reduziert werden, z.
 3978 B. "`file.html`". Nach der Normalisierung MUSS eine Validierung der Extension
 3979 gemäß A_23447-* erfolgen. [≤]

3980 **A_23447-01 -XDS Document Service - DocumentEntry.URI extension entspricht mimetype**

3981 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten
 3982 das Metadatum `DocumentEntry.URI` daraufhin prüfen, ob `DocumentEntry.URI` eine
 3983 filename extension aufweist, die nicht dem `DocumentEntry.mimeType` entspricht. Zuvor
 3984 muss die URI mittels A_24524-* normalisiert worden sein. Danach MUSS der XDS
 3985 Document Service sicherstellen, dass in `Document.URI` die filename extension dem
 3986 `DocumentEntry.mimeType` entspricht. Im Falle einer Abweichung MUSS an die
 3987 ursprüngliche `DocumentEntry.URI` die filename extension gemäß A_24864-*, bzw.
 3988 A_25009-*, angehängt werden, die dem `mimeType` entspricht. Die Groß-
 3989 /Kleinschreibung der filename extension ist bei der Prüfung nicht relevant. [≤]

3991 **A_24451-01 -XDS Document Service - Automatisches initiales Erzeugen einer**
 3992 **versionsübergreifenden ID für Dokumente**

3993 Der XDS Document Service MUSS beim initialen Einstellen eines Dokumentes die
 3994 DocumentEntry.uniqueId als Eintrag einer ReferenceID in die ReferenceIDList in
 3995 folgendem Format einstellen:

3996 `<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2023:rootDocumentUniqueId`

3997 Beim Upload einer neuen Version des Dokumentes DARF dieser Eintrag in der
 3998 ReferenceIDList, d.h. die rootDocumentUniqueId, NICHT verändert werden. Er bleibt
 3999 über alle Versionen des Dokumentes hinweg unverändert erhalten. Der Versuch eines
 4000 Clients, die rootDocumentUniqueId durch ein Metadata-Update oder im Zuge des
 4001 Einstellens einer neuen Dokumentenversion zu verändern, MUSS mit einem IHE-Error
 4002 XDSRegistryMetadataError abgebrochen werden. Es MUSS im codeContext-Attribut
 4003 des zurückgegebenenXDSRegistryMetadataError-Elements der
 4004 Text „rootDocumentUniqueId must not be changed“ zurückgegeben werden.[<=]

4005 **A_14926-04 -XDS Document Service – Automatisiertes Löschen oder Verbergen** 4006 **von Dokumenten in RPLC-Ketten**

4007 Der XDS Document Service MUSS bei zu löschenden oder zu verbergenden Dokumenten
 4008 und DocumentEntry-Einträgen im selben Zuge auch alle mittels
 4009 urn:ihe:iti:2007:AssociationType:RPLC assoziierten DocumentEntry-Einträge und
 4010 Dokumente löschen bzw. verbergen.[<=]

4011 **A_27683-01 -XDS Document Service – Maximale Länge von Anhangsketten**

4012 Der XDS Document Service MUSS sicherstellen, dass beim Einstellen (über die
 4013 Schnittstelle Provide and Register Document Set-b [ITI-41]) oder Kennzeichnen (über die
 4014 SchnittstelleRestricted Update Document Set [ITI-92]) von neuen Anhängen die gesamte
 4015 Anhangskette inklusive des neuen Anhangdokuments nicht und inklusive des obersten
 4016 Elterndokuments nicht mehr als fünf Dokumente enthält und ansonsten die Operation mit
 4017 dem Fehler XDSMaxAttachmentsExceeded abbrechen.

4018 [

4019 Der Abschnitt 6.1.1. Dokumentenanhänge enthält eine Illustration für diese Anforderung.

4020 3.13.1.4.3.1 Provide and Register Document Set-b [ITI-41]

4021 **A_13715 -XDS Document Service – Ablauflogik für** 4022 **ProvideAndRegisterDocumentSet-b**

4023 Der XDS Document Service MUSS die Umsetzung der
 4024 Operation ProvideAndRegisterDocumentSet-b gemäß den definierten Ablauflogiken
 4025 in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3] und [IHE-ITI-TF2b#3.41.4.2.2 und
 4026 3.41.4.2.3] implementieren.[<=]

4027 **A_15162-06 -XDS Document Service – Keine Registrierung bei Angabe von** 4028 **Document Entry Relationships in Metadaten**

4029 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und
 4030 Dokument(en) ablehnen und mit einem XDSRepositoryMetadataError-Fehlercode
 4031 quittieren, sofern die Metadaten andere Association Types nach [IHE-ITI-TF3#4.2.2.2]
 4032 als die Folgenden enthalten:

- 4033 • urn:ihe:iti:2007:AssociationType:RPLC (Replace)

4034 [

4035 **A_14938-02 -XDS Document Service – Validierung der Metadaten aus ITI** 4036 **Document Sharing-Profilen**

4037 Der XDS Document Service MUSS die SubmissionSet- sowie die DocumentEntry-
 4038 Metadaten der eingehenden Nachricht vor einer Zugriffskontrolle gemäß Konformität zu
 4039 den Nutzungsvorgaben in [A_14760-*] prüfen. Der XDS Document Service MUSS das
 4040 Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit
 4041 einemXDSRepositoryMetadataError quittieren, sofern die Metadaten nicht konform zu
 4042 den Nutzungsvorgaben sind. Es MUSS im codeContext-Attribut

4043 des zurückgegebenen `rs:RegistryError`-Elements angegeben werden, welches
4044 Metadatenattribut nicht den Nutzungsvorgaben entspricht. [`<=`]

4045

4046 **A_24521 -XDS Document Service - Erzeugen von Prüfsummen für Dokumente**

4047 Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes
4048 Dokument seine kryptographische Prüfsumme berechnen und `inDocumentEntry.hash`
4049 hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die
4050 Dokumentengröße `inDocumentEntry.size` berechnet und gesetzt werden. [`<=`]

4051 **A_24988-01 -XDS Document Service - Dublettenprüfung für Dokumente**

4052 Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes
4053 Dokument den hash-Wert vergleichen mit allen bereits in dieser Akte existierenden hash-
4054 Werten der Dokumente und bei einer Übereinstimmung das Einstellen mit dem
4055 Fehlercode `XDSDuplicateDocument` ablehnen. Es MUSS im `codeContext`-Attribut
4056 des zurückgegebenen `rs:RegistryError`-Elements die Liste der UUIDs
4057 (`DocumentEntry.entryUUID`) der identifizierten Dokumente angegeben werden. Der XDS
4058 Document Service MUSS diese Prüfung vor allen anderen Metadatenprüfungen
4059 durchführen. [`<=`]

4060 Hintergrund ist, dass die Information, dass es sich um eine Dublette handelt, für das
4061 einstellende System hilfreicher und spezifischer ist als ein Metadatenfehler, dass bspw.
4062 die angelieferte `uniqueId` "falsch" ist.

4063 **A_24990 -XDS Document Service - Dublettenprüfung für dynamische Ordner**

4064 Der XDS Document Service MUSS beim Anlegen dynamischer Folder prüfen, ob ein
4065 Ordner bereits existiert, der gemäß vom Titel her identisch ist mit demjenigen, den der
4066 Client einzustellen versucht. Im Falle eines identischen Titels MUSS der Einstellversuch
4067 mit dem Fehlercode `XSDuplicateFolder` abgelehnt werden. [`<=`]

4068 **A_14937 -XDS Document Service – Dokumentengröße prüfen**

4069 Der XDS Document Service MUSS die Dateigröße jedes übergebenen Dokuments
4070 ermitteln, bevor das `SubmissionSet` verarbeitet wird. Der XDS Document Service
4071 MUSS die Verarbeitung ablehnen und mit einem `MaxDocSizeExceeded`-
4072 bzw. `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren, wenn die
4073 Gesamtgröße aller übermittelten Dokumente 250 MByte übersteigt oder die Größe
4074 mindestens eines einzelnen Dokuments 25 MByte übersteigt.
4075 [`<=`]

4076 Das bedeutet, dass Dokumente bis zu einer Größe von $25 \text{ MB} = 25 * (1024)^2 \text{ Byte}$ in
4077 die ePA hochgeladen werden. Grundlage für die Berechnung der Dokumentengröße ist
4078 das Dokument ohne Transportcodierung. Größere Dokumente können nicht hochgeladen
4079 werden.

4080 **A_23098-01 -XDS Document Service – Keine Registrierung bei zeitlicher Ungültigkeit von strukturierten Dokumenten**

4081 Der XDS Document Service MUSS beim Einstellen eines strukturierten
4082 Dokuments sicherstellen, dass die Vorgaben gemäß [gemSpec_IG_ePA] hinsichtlich der
4083 zeitlichen Gültigkeit erfüllt werden und andernfalls das Registrieren und Speichern von
4084 Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`
4085 quittieren. Es MUSS im `codeContext`-Attribut
4086 des zurückgegebenen `XDSRepositoryMetadataError`-Elements der Text „Version of
4087 submitted structured document is not supported“ zurückgegeben werden. [`<=`]

4089 **A_21610-03 -Sonderfälle Anlegen von Foldern durch Clientsysteme**

4090 Der XDS Document Service MUSS sicherstellen, dass ausschließlich dynamische Ordner
 4091 vom Typ "Schwangerschaft und Geburt" (Folder.Code = pregnancy_childbirth) durch
 4092 Clients angelegt werden können. [`<=`]

4093

4094 **A_24797-04 -XDS Document Service - Ablehnung Upload bei veränderten**
 4095 **Metadaten bei einer RPLC Assoziation**

4096 Der XDS Document Service MUSS Uploads, die als Resultat ein zum Vorgängerdokument
 4097 verändertes Metadatum enthalten, mit einem XDSRegistryMetadataError ablehnen.
 4098 Einzige Ausnahmen sind:

- 4099 • Metadatenattribute creationTime, entryUUID sowie uniqueId und
 4100 confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491).
- 4101 • Das Metadatenattribut DocumentEntry.referenceIdList DARF ohne die
 4102 rootDocumentUniqueId gesendet werden; in dem Fall wird die
 4103 rootDocumentUniqueId automatisch vom XDS Document Service gesetzt (Wert
 4104 identisch zu dem des ersetzten Dokuments).

4105 [`<=`]

4106 **A_277600-01 -XDS Document Service - Ablehnen von RPLC-Ersetzungen bei**
 4107 **nicht erlaubten Dokumententypen**

4108 Der XDS Document Service MUSS das Ersetzen von Dokumenten via RPLC-Associations
 4109 abmit dem Fehlercode `XDSReplacementForbidden` ablehnen, wenn das zu ersetzende
 4110 Dokument nicht einen der folgenden DocumentEntry.formatCode-Werte besitzt:

Dokume nt	codeSystem	code
eMP	1.3.6.1.4.1.19376.3.276.1 .5.6	urn:gematik:ig:Medikationsplan:r3.1
NFD	1.3.6.1.4.1.19376.3.276.1 .5.6	urn:gematik:ig:Notfalldatensatz:r3.1
DPE	1.3.6.1.4.1.19376.3.276.1 .5.6	urn:gematik:ig:DatensatzPersoenlicheErklaerung en:r3.1
DiGA	1.3.6.1.4.1.19376.3.276.1 .5.6	urn:gematik:ig:diga:v1.1

4111

4112 oder das zu ersetzende Dokument nicht in einen der folgenden Ordner einsortiert ist:

Ordner-Kategorie	Folder.entryUUID	
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d	
<u>technical</u>	<u>f88dc706-d2df-4ca0-a850-491cfaab2d31</u>	

4113 [`<=`]

4114 Seit ePA 3.1.2 ist das Ersetzen von Dokumenten via RPLC-Associations nur noch für die
 4115 oben aufgeführten Dokumententypen bzw. -kategorien erlaubt. Der Versuch, andere
 4116 Dokumententypen zu ersetzen, führt zu einem Fehler. Es kann Altdaten geben, die diese

4117 Regel noch missachten. Neue Ersetzung für diese Altdaten werden jedoch gleichermaßen
 4118 fehlschlagen; d.h. neue Ersetzungen sind nur noch für die oben angegebenen
 4119 Dokumententypen erlaubt.

4120 **A_27761 -XDS Document Service - Potentielle Dokumententypen**
 4121 **(Elterndokumente) für Anhänge**

4122 Der XDS Document Service MUSS das Anhängen von Dokumenten mit dem Fehlercode
 4123 `XDSAttachmentForbidden` ablehnen, wenn das Dokument, an das angehängt wird, nicht
 4124 die folgende Metadatenbelegung besitzt:

IHE-Metadaten	eventCodeList-Eintrag (KDL-Code)				
	Dokumententyp (informativ)	Code System	Code		
	eventCodeList muss einen der folgenden Codes enthalten:				
classCode="BRI" UND typeCode="BERRI" (beide Codes müssen angegeben sein)			KH-Entlassbrief	1.2.276.0.76.5.552	ED110112
	eArztbrief	1.2.276.0.76.5.552	ED110104		
	Anderer Arztbrief	1.2.276.0.76.5.552	AD0101*		

4125 [\leq]

4126 Hinweis 1: AD0101 bezeichnet Codes die mit den Zeichen "AD0101" beginnen, z. B.
 4127 "AD010112" für den "Kurzarztbrief". Der Code "AD0101" als Level 2-Code in KDL ist
 4128 selbst nicht Teil des Value Sets für eventCodeList, das nur die konkreteren Level 3 Codes
 4129 enthält.

4130 Hinweis 2: Die Anforderung schließt sowohl das Einstellen von Anhängen über die
 4131 Operation Provide and Register Document Set-b [ITI-41] als auch Restricted Update
 4132 Document Set [ITI-92] mit ein.

4133 Hinweis 3: Die Dokumente, die als Anhang angehängt werden dürfen, werden ~~abgesehen~~
 4134 ~~von~~über A_27763 (RPLC-fähige Dokumente) ~~nicht~~und A_27764 (Sammlungen)
 4135 eingeschränkt.

4136 **A_27764 -XDS Document Service - Keine Anhangsbeziehungen mit**
 4137 **Sammlungsdokumententypen**

4138 Der XDS Document Service MUSS das Etablieren von Anhangsbeziehungen zu allen
 4139 Dokumententypen, die in Sammlungen (mixed oder uniform) organisiert werden,
 4140 unterbinden und mit dem Fehler `XDSAttachmentForbidden` ablehnen.

4141 [\leq]

4142 **A_27763-01 -XDS Document Service - Keine Anhangsbeziehungen mit RPLC-**
 4143 **fähigen Dokumententypen**

4144 Der XDS Document Service MUSS das Etablieren von Anhangsbeziehungen zu allen
 4145 Dokumententypen, die in RPLC-Ketten verwendet werden dürfen (siehe A_27760)

4146 unterbinoder die bereits aufgrund der Migration von Altdaten (siehe A_27661) in RPLC-
4147 Beziehungen stehen, unterbinden und mit dem Fehler XDSAttachmentForbidden
4148 ablehnen.
4149 [`<=`]

4150 Das heißt, dass RPLC-fähige Dokumente (egal, ob sie bereits Teil einer RPLC-Kette sind
4151 oder nicht) nicht Teil einer Anhangskette sein dürfen, also weder als Anhang genutzt
4152 werden dürfen, noch als Dokument an das selbst angehängt wird. Das trägt der aktuellen
4153 Einschränkung Rechnung, dass alle RPLC-Dokumente in einer RPLC-Kette immer
4154 "identische" Metadaten besitzen und deshalb Anhänge (die über die Metadaten abgebildet
4155 werden) automatisch bei einer Ersetzung "mitvererbt" würden. Da dies fachlich potentiell
4156 zu Problemen führen kann, wird es auf diese Weise unmöglich gemacht, dass Dokumente
4157 gleichzeitig in einer RPLC- als auch in einer Anhangskette sein können.

4158 Da diese Regelung in ePA 3.1.2 eingeführt wurde, können Altdaten noch über Anhänge
4159 verfügen, siehe auch Abschnitt zur [automatischen Datenanpassung](#).

4160 Details zur grundsätzlichen Funktionsweise von Dokumentenanhängen finden sich
4161 in [diesem Abschnitt](#).

4162 **A_24531-04 -Constraint Management - Verbergen von Dokumenten durch** 4163 **confidentialityCode**

4164 Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem =
4165 urn:oid:1.2.276.0.76.5.491) durch eine Nutzergruppe der
4166 Rolle `oid_versichertereingestellt` wird, nicht Bestandteil einer Sammlung, also eines
4167 Ordners der Ausprägung "mixed" oder "uniform" ist, und kein Dokument der Kategorie
4168 "emp" ist, dann MUSS der XDS Document Service sicherstellen, dass das Dokument
4169 durch einen Eintrag in der General Deny Policy verborgen wird. Es MUSS ein Eintrag mit
4170 denyType = "document" für die General Deny Policy erzeugt werden. [`<=`]

4171 **A_25856-02 -XDS Document Service - Fehlerhaftes Verbergen von Dokumenten** 4172 **durch confidentialityCode**

4173 Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem =
4174 urn:oid:1.2.276.0.76.5.491) nicht durch eine Nutzergruppe der
4175 Rolle `oid_versichertereingestellt` wird, oder Bestandteil einer Sammlung, also eines
4176 Ordners der Ausprägung "mixed" oder "uniform" ist, dann MUSS der XDS Document
4177 Service die Operation abbrechen und mit einem Fehlercode ConstraintViolation
4178 beenden. [`<=`]

4179 Das Verbergen von Dokumenten ist in Kapitel 3.13.1.10- Verbergen von Dokumenten
4180 durch Verwendung des confidentialityCode beschrieben.

4181 3.13.1.4.3.1.1 Dokumentenanhänge

4182 Für die Verwaltung von Anhängen wird ein Mechanismus basierend auf
4183 DocumentEntry.referenceIdList verwendet. Zwei Dokumente werden verknüpft, indem in
4184 beiden dazugehörigen DocumentEntrys das jeweils andere Dokument als
4185 "Elterndokument" bzw. "Kinddokument" (=Anhang) eingetragen wird. Dies geschieht
4186 über die Auszeichnung der Referenzen mit den qualifizierenden
4187 Codes `urn:gematik:iti:xds:2025:childDocument` (Verweis auf ein Kinddokument) und
4188 `urn:gematik:iti:xds:2025:parentDocument` (Verweis auf ein Elterndokument).

4189 Ein Verweis auf ein Elternformat hat also das

4190 Format: `<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2025:parentDocument`

4191 Dabei muss das Dokument, auf das per Kind- oder Elternreferenz verwiesen wird,
4192 zusammen mit oder nach dem referenzierten Dokument eingestellt werden. Wenn z. B.
4193 das Elterndokument bereits im Aktensystem gespeichert ist und ein Kinddokument
4194 (Anhang) dazu hochgeladen wird, muss der DocumentEntry des Kinddokuments das

4195 Elterndokument in der referenceIdList referenzieren. Die Markierung des
4196 Elterndokuments (mit dem Verweis auf das Kinddokument) wird dann vom Aktensystem
4197 automatisch vorgenommen. Damit wird vermieden, dass zwei Aufrufe notwendig sind
4198 (Einstellen gefolgt vom Aktualisieren der Metadaten), was zu inkonsistenten Zuständen
4199 im Aktensystem führen kann. Werden Eltern- und Kinddokument gemeinsam eingestellt,
4200 ist der Verweis auf mindestens entweder Elterndokument oder Kinddokument
4201 verpflichtend, da die jeweils andere Seite automatisch vom Aktensystem ergänzt werden
4202 kann.

4203 Die Tiefe von Anhangsketten ist auf fünf Dokumente (inklusive Edem obersten
4204 Elterndokument) begrenzt. Darüberhinaus ist die Verwendung von Anhängen nur für
4205 ausgewählte Dokumententypen erlaubt und kann dann jeweils weiteren Beschränkungen
4206 unterliegen. ~~Beispielsweise können an Arzbriefe zwar beliebig viele Dokumente~~
4207 ~~angehängt werden, jedoch dürfen die Anhänge nicht selbst auch noch über Anhänge~~
4208 ~~verfügen.~~

4209 Neben dem Anhängen während des Einstellens ist es auch möglich, über ein
4210 Metadatenupdate nachträglich zwei Dokumente miteinander über eine Anhangsbeziehung
4211 zu verbinden.

4212 Anhänge, technisch umgesetzt über DocumentEntry.referenceIdList, sind zu
4213 unterscheiden von RPLC (Replace/Ersetzungs)-Ketten, die über RPLC-Associations
4214 abgebildet werden. Ersetzte Dokumente stellen verschiedene Dokumentenversionen dar,
4215 während Anhänge in der Regel eine Ergänzung des Dokuments darstellen, an dem sie
4216 anhängen. Um die beiden Konzepte nicht zu vermischen (aktuell würden alle per RPLC-
4217 Associations verbundene Dokumente zwangsläufig aufgrund identischer Metadaten
4218 immer dieselben Anhänge besitzen), wird verboten, ein Dokument gleichzeitig in eine
4219 Ersetzungskette als auch in eine Anhangskette zu hängen. Dies geschieht über eine
4220 Beschränkung des RPLC-Mechanismus auf wenige ausgewählte Dokumententypen und
4221 der gezielten Verwendung von Anhängen für andere Dokumententypen.

4222 Die letzte Einschränkung bedeutet auch, dass Anhänge nicht an beliebige Dokumente
4223 gehängt werden können. Ziel ist es, Anhänge nur in fachlich kontrollierter Form in der
4224 ePA zu verwenden und auf diese Weise die Datenqualität zu erhöhen.

4225 Anhangsbeziehungen können gelöscht werden, in dem der entsprechende Verweis auf ein
4226 Anhangsdokument aus der referenceIdList (via Restricted Update Document Set) entfernt
4227 wird.

4228 Es kann direkt an einem DocumentEntry erkannt werden, ob ein Dokument
4229 Anhangsbeziehungen zu anderen Dokumenten unterhält oder nicht. Um möglichst einfach
4230 (rekursiv) alle mit einem bestimmten Dokument verbundenen Dokumente zu finden,
4231 existiert eine spezielle Suche (siehe A_27655), die alle entsprechenden DocumentEntries
4232 zurückliefert. Bei dieser und anderen Suchen werden Eltern- oder Kinddokumente zu
4233 einem zurückgegebenen DocumentEntry, die *nicht* für den Anfragenden sichtbar sind (z.
4234 B. aufgrund der Legal Policy oder da sie durch den Versicherten verborgen wurden), vom
4235 Aktensystem automatisch aus dem returnierten DocumentEntry bzw. dessen
4236 referenceIdList entfernt.

4237 **Berechtigungen für Anhangsoperationen**

4238 Es gelten die Regelungen der Legal Policy für die zur Anhangsverwaltung notwendigen
4239 Operationen:

- 4240 • **Lesen:** Um die Anhangsbeziehung zwischen beiden Dokumenten zu erkennen,
4241 müssen beide Dokumente für den Anfragenden lesbar (Berechtigung "R" für
4242 "Read") sein, ansonsten blendet das Aktensystem die Anhangsbeziehung in
4243 zurückgelieferten DocumentEntries aus. Auch wenn das referenzierte Dokumente
4244 verborgen ist, wird die Anhangsbeziehung nicht angezeigt.

- **Einstellen:** Um Dokumente neu einzustellen und sie als Eltern- oder Kinddokument mit einem bestehenden (oder ebenfalls neuen) Dokument zu verknüpfen, wird das "C"-Recht ("Create") für das neue Dokument benötigt, um die Provide and Register Document Set-b Operation ausführen zu können. Zudem muss für das zu verbindende Dokument (sofern es nicht neu mit eingestellt wird) die Berechtigung zum Aktualisieren ("U") vorliegen. Auch in diesem Use Case müssen beide Dokumente für den Einstellenden sichtbar sein.
- **Aktualisieren:** Um zwei Dokumente, die bereits im Aktensystem vorliegen, zu verknüpfen oder zu entknüpfen, wird die Berechtigung "U" ("Update") zur Ausführung der Operation Restricted Update Document Set auf *beiden* Dokumenten benötigt. Beide Dokumente dürfen nicht vom Versicherten verborgen worden sein.
- **Löschen:** Wenn ein Dokument gelöscht werden soll muss die Berechtigung "D" für das zu löschende Dokument vorliegen. Der Verweis aus etwaigen Eltern/Kinddokumenten auf das gelöschte Dokument wird entfernt. Dazu ist beim referenzierten Dokument die Berechtigung "U" notwendig. Die "D"-Berechtigung selbst muss nur für das zu löschende Dokument vorliegen.

Eine wichtige Eigenschaft im Zusammenhang mit Anhängen ist es also, dass das Herstellen und Entfernen von Anhangsbeziehungen von Dokumenten das Update-Recht "U" benötigt (Ausnahme: für neu eingestellte nur Recht "C" notwendig). Das Anhängen oder Abhängen eines Dokuments in/aus einer Anhangskette wird also als Aktualisierung eines Dokuments verstanden.

A_27654 -XDS Document Service – Einstellen von neuen Anhängen oder Anhängen an neue Dokumente

Der XDS Document Service MUSS beim Registrieren und Speichern von Metadaten und Dokument(en) über die Operation ProvideAndRegisterDocumentSet-b die folgenden zusätzlichen Schritte durchführen, wenn das Feld DocumentEntry.referenceIdList einen Wert mit Identifier Type Code urn:gematik:iti:xds:2025:parentDocument (oder urn:gematik:iti:xds:2025:childDocument) enthält; im Folgenden ist der Fall für urn:gematik:iti:xds:2025:parentDocument beschrieben, der Fall childDocument ist analog zu behandeln und jeweils in Klammern angegeben)

1. Prüfung, ob das dort als parentDocument (childDocument) adressierte Dokument (mit entsprechender DocumentEntry.uniqueId) entweder Teil des SubmissionRequests oder bereits im XDS Document Service vorhanden ist. Der XDS Document Service MUSS:
 - a. Wenn das Dokument nicht existiert oder für den Anfragenden nicht sichtbar ist, die Verarbeitung mit dem Fehler XDSNoSuchParent (XDSNoSuchChild) abbrechen;
 - b. Wenn das Dokument bereits vorhanden ist, prüfen ob der Anfragende gemäß Legal Policy die Berechtigung "U" für dieses Dokument besitzt und ansonsten die Verarbeitung mit dem Fehler XDSCannotLinkAttachment abbrechen und im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements als Text die DocumentEntry.uniqueId des referenzierten Dokuments angeben.
2. Prüfung, ob durch das Einstellen des Dokuments kein Verweiszirkel entsteht und ansonsten die Verarbeitung mit dem Fehler XDSAttachmentCycle abbrechen.
3. Prüfung, ob durch das Einstellen des Dokuments der zusätzliche Verweis nicht auf ein Elterndokument (Kinddokument) gemacht wird, das bereits Teil der Elternketten (Kindkette) ist und ansonsten die Verarbeitung mit dem Fehler XDSInvalidAttachmentHierarchy abbrechen.

4294 4. Im referenzierten Dokument die DocumentEntry.uniqueId des einzustellenden
4295 Dokuments in die referenceIdList mit Identifier
4296 Codeurn:gematik:iti:xds:2025:childDocument
4297 (urn:gematik:iti:xds:2025:parentDocument) eintragen, wenn dies nicht bereits
4298 geschehen ist.

4299 [**<=**]

4300 Hinweis 1: Ein Verweiszirkel kann entstehen, wenn ein Kinddokument direkt oder indirekt
4301 (d.h. ggf. über eine Kette von Kinddokumenten hinweg) gegenüber seinem
4302 Elterndokument gleichzeitig auch selbst als Elterndokument auftritt.

4303 Hinweis 2: Der Fehler XDSInvalidAttachmentHierarchy spiegelt die Situation wider,
4304 dass in einer Kette von Anhängen (wie 1<-2<-3) versucht wird, ein Kind (3) zusätzlich
4305 als Kind eines Vorfahren seines Elterndokuments (1) einzuführen.

4306 Hinweis 3: Punkt 4 stellt sicher, dass das referenzierte Dokument passend markiert wird,
4307 egal ob es in der Anfrage enthalten ist oder bereits im Aktensystem hinterlegt ist.

4308 Siehe auch [entsprechende Illustrationen im Anhang](#).

4309 3.13.1.4.3.2 Registry Stored Query [ITI-18]

4310 **A_14913 -XDS Document Service – Ablauflogik für Registry Stored Query**

4311 Der XDS Document Service MUSS die Umsetzung der Operation RegistryStoredQuery
4312 gemäß der definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3]
4313 implementieren. [**<=**]

4314 **A_24761 -XDS Document Service – Ermitteln verknüpfter Approved Documents 4315 für Registry Stored Query**

4316 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp
4317 "GetRelatedApprovedDocuments" mit der Query-ID "urn:uuid:1c1f1cea-ad3a-11ed-afa1-
4318 0242ac120002" mit denselben Parameternutzungsvorgaben der Registry Stored Query
4319 „GetDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.5] mit der Multiplizität 1
4320 unterstützen. Das resultierende DocumentEntry Objekt MUSS

- 4321 • mit dem Ergebnis von GetDocuments übereinstimmen, falls dieses sich im
4322 Zustand approved befindet;
- 4323 • andernfalls über Associations ermittelt werden. Dabei wird jeweils ausgehend von
4324 der übergebenen DocumentEntry.EntryUUID oder DocumentEntry.UniqueId über
4325 die Replace- Associations dasjenige DocumentEntry Objekt ermittelt, das sich im
4326 Zustand approved befindet.

4327 Das wsa:Action-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery"
4328 besitzen.

4329 [**<=**]

4330 **A_24762 -XDS Document Service – Suchanfragen über das Metadatenattribut 4331 DocumentEntry.title**

4332 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "FindDocumentsByTitle"
4333 mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben
4334 Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-
4335 ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter
4336 \$XSDSDocumentEntryTitle unterstützen, sodass eine Suchergebnismenge über das
4337 Attribut XSDSDocumentEntry.title eingeschränkt werden kann. Weiterhin MUSS dieselbe
4338 Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den
4339 Parameter \$XSDSDocumentEntryAuthorPerson. Daswsa:Action-Element MUSS den Wert
4340 "urn:ihe:iti:2007:RegistryStoredQuery" besitzen. [**<=**]

A_25183 -XDS Document Service – Suchanfragen über das Metadatenattribut DocumentEntry.comment

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "FindDocumentsByComment" mit der Query-ID "urn:uuid:2609dda5-2b97-44d5-a795-3e999c24ca99" und denselben Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter \$XDSDocumentEntryComment unterstützen, sodass eine Suchergebnismenge über das Attribut XDSDocumentEntry.comment eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson. Daswsa:Action-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery" besitzen. [\leq]

A_24763 -XDS Document Service – Suche über Author Institution bei Registry Stored Query

Der XDS Document Service MUSS für den Anfragetyp "FindDocumentsByTitle" den weiteren optionalen Parameter \$XDSDocumentEntryAuthorInstitution verarbeiten können, sodass eine Suchergebnismenge über den authorInstitution-Slot der XDSDocumentEntry.author-Classification (Wertemenge des authorInstitution-Sub-Attributs) eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson. [\leq]

A_24764 -XDS Document Service – Rückgabe unscharfer Suchergebnisse für Registry Stored Query

Der XDS Document Service MUSS bei der Ermittlung der Ergebnisse einer Registry Stored Query bei Auswertung der folgenden Queries und deren Suchparametern beim Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d. h. bezogen auf das jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht abweichende Ergebnisse zurück liefern können:

- Query "FindDocuments" und Query "FindDocumentsByTitle" und Query "FindDocumentsByComment"
 - \$XDSDocumentEntryTitle
 - \$XDSDocumentEntryAuthorInstitution
 - \$XDSDocumentEntryAuthorPerson
 - \$XDSDocumentEntry.comment
- Query "FindSubmissionSets"
 - \$XDSSubmissionSetAuthorPerson

Dabei MUSS der XDS Document Service mindestens unscharfe Ergebnisse bezüglich Groß/Kleinschreibung unterstützen, also Groß/Kleinschreibung für die angegebenen Parameter der ausgewählten Query-Typen ignorieren. [\leq]

Das zur Ermittlung weiterer unscharfer Ergebnisse vom XDS Document Service einzusetzende Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu liefern, die ihm möglicherweise sonst wegen beispielsweise falscher Schreibweise eines Namens (z. B. "Meyer" vs. "Maier") vorenthalten worden wäre. Dabei sind Verfahren wie die Kölner Phonetik aber auch andere Mechanismen denkbar.

A_27655 -XDS Document Service – Suche nach Anhangsketten

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "GetDocumentAppendices" mit der Query-ID "urn:uuid:2a6b3197-8ea8-4245-a6de-

4389 daf71b469116" und denselben Parameternutzungsvorgaben der Registry Stored Query "
4390 GetDocumentsAndAssociations" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.8] unterstützen.
4391 Die Suchergebnismenge muss für jedes über \$XDSDocumentEntryEntryUUID oder
4392 \$XDSDocumentEntryUniqueId referenzierte Dokument die Ergebnismenge wie folgt
4393 ermitteln:

- 4394 1. Start: Alle DocumentEntrys der Ergebnismenge hinzufügen, welche auf die
4395 uniqueId des Dokuments aus dem Eingangsparameter in der
4396 DocumentEntry.referenceIdList verweisen (ausgezeichnet als
4397 urn:gematik:iti:xds:2025:childDocument oder
4398 urn:gematik:iti:xds:2025:parentDocument) und sichtbar sind.
- 4399 2. Kindkette: Für jeden im vorher durchgeführten Schritt identifizierten
4400 DocumentEntry D, der über den Eintrag
4401 urn:gematik:iti:xds:2025:childDocument identifiziert wurde, alle
4402 DocumentEntries der Ergebnismenge hinzufügen, welche die uniqueId von D
4403 wiederum als urn:gematik:iti:xds:2025:childDocument in der referenceIdList
4404 enthalten und sichtbar sind. Wenn ein DocumentEntry nicht sichtbar ist, wird
4405 dieser Teil der Kette nicht weiter verfolgt.
- 4406 3. Elternkette: Für jeden im vorher durchgeführten Schritt identifizierten
4407 DocumentEntry E, der über den Eintrag
4408 urn:gematik:iti:xds:2025:parentDocument identifiziert wurde, alle
4409 DocumentEntries der Ergebnismenge hinzufügen, welche die uniqueId von E
4410 wiederum als urn:gematik:iti:xds:2025:parentDocument in der referenceIdList
4411 enthalten und sichtbar sind. Wenn ein DocumentEntry nicht sichtbar ist, wird
4412 dieser Teil der Kette nicht weiter verfolgt.
- 4413 4. Rekursion: Schritte 2 und 3 jeweils wiederholen, bis keine weiteren
4414 DocumentEntries mehr gefunden werden können.

4415 [**<=**]

4416 Hinweis 1: "Sichtbar" im Kontext von Anhängen bedeutet hier, dass die Existenz eines
4417 Dokuments nicht durch fehlende Legal Policy-Berechtigung (Recht "R" ist notwendig),
4418 Verbergen durch den Versicherten, Zugriffsverbot für die zugreifenden Organisation über
4419 ("User Specific Deny Policy") oder gar Widerspruch ("Consent Decision") vor dem
4420 Zugreifenden versteckt werden muss.

4421 Hinweis 2: Wenn als Eingabe eine entryUUID gegeben wird, muss der XDS Document
4422 Service die dazugehörige uniqueID ggf. intern selbst ermitteln. Zur Sichtbarkeit von
4423 Anhängen siehe Hinweis unter A_27655.

4424 Die Suche ermittelt also alle Dokumente, die über Anhangsketten mit dem gegebenen
4425 Dokument verbunden sind.

4426 **A_27762 -XDS Document Service - Ausblenden nicht sichtbarer Anhänge**

4427 Der XDS Document Service MUSS bei der Rückgabe eines DocumentEntries D im Rahmen
4428 einer Stored Query [ITI-18] jedes durch Anhangsbeziehungen in der
4429 DocumentEntry.referenceIdList (urn:gematik:iti:xds:2025:childDocument oder
4430 urn:gematik:iti:xds:2025:parentDocument) mit D verbundene Dokument E
4431 dahingehend prüfen, ob es für den Anfragenden sichtbar ist und wenn nicht, den
4432 entsprechenden Eintrag für E vor der Herausgabe an den Anfragenden aus der
4433 referenceIdList entfernen.

4434 [**<=**]

4435 3.13.1.4.3.3 Remove Metadata [ITI-62]

4436 **A_14908-02 -XDS Document Service – Ablauflogik für Remove Metadata**

4437 Der XDS Document Service MUSS die Umsetzung der Operation RemoveMetadata gemäß
4438 der definierten Ablauflogik in [IHE-ITI-RMD#3.62.4.1.2 und 3.62.4.1.3]
4439 implementieren.[<=]

4440 **A_20701 -XDS Document Service – Unwiderrufliches Löschen bei Remove**
4441 **Metadata**

4442 Der XDS Document Service MUSS sicherstellen, dass einmal gelöschte Dokumente und
4443 Metadatenobjekte nicht wiederhergestellt werden können.[<=]

4444 **A_21715 -XDS Document Service – Kein Löschen von "replaced"-Dokumenten**
4445 **im Status "Deprecated"**

4446 Der XDS Document Service MUSS sicherstellen, dass keine Löschanfrage eines ePA-Client
4447 auf Dokumenten mit dem availabilityStatus = Deprecated ausgeführt werden darf.[<=]

4448 **A_21714-03 -XDS Document Service – Löschen von strukturierten Dokumenten**
4449 **durch ein ePA-FdV**

4450 Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein
4451 ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete
4452 Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert
4453 aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie
4454 zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die
4455 Nachricht mit demXDSRegistryError-Fehlercode zurückgeben werden.Es MUSS im
4456 codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert
4457 "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt
4458 werden.[<=]

4459 **A_21817-02 -XDS Document Service – Löschen von strukturierten Dokumenten**
4460 **durch ein Primärsystem**

4461 Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein
4462 Primärsystem ablehnen, wenn zugehörige Submission Sets, Associations oder
4463 zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners
4464 impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets,
4465 Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben
4466 vor, MUSS die Nachricht mitXDSRegistryError-Fehlercode zurückgeben werden. Es MUSS
4467 im codeContext-Attribut des zurückgegebenenrs:RegistryError-Elements der Wert
4468 "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt
4469 werden.[<=]

4470 **A_24663-01 -XDS Document Service – Bereinigung der General Deny Policy**

4471 Der XDS Document Service MUSS als Folge von erfolgreichen Löschanfragen alle Einträge
4472 der General Deny Policy entfernen, welche die betroffenen Dokumente oder dynamischen
4473 Ordner referenzieren.[<=]

4474 **A_24765 -XDS Document Service – Kein Löschen von statischen Ordnern und**
4475 **Associations**

4476 Der XDS Document Service MUSS sicherstellen, dass eine Löschanfrage keine statischen
4477 Ordner und Assoziationen löschen darf. Dies gilt nicht für dynamische Ordner. Der XDS
4478 Document Service MUSS bei Löschung eines Dokumentes die Assoziation zum Folder
4479 löschen.[<=]

4480 Dynamische Ordner sind beispielsweise Mutterpass (folderCode = pregnancy_childbirth)
4481 oder DiGA (folderCode = diga).

4482 **A_20579-01 -XDS Document Service – Löschen von Ordnern**

4483 Der XDS Document Service MUSS Requests, die darauf abzielen, einen statischen Folder
4484 direkt zu löschen, mit einem XDSRegistryMetadataError ablehnen.[<=]

4485 **A_27656-01 -XDS Document Service – Löschen von Anhangsreferenzen beim**
4486 **Löschen von Dokumenten**

- 4487 Der XDS Document Service MUSS beim Löschen eines Dokuments D, das in der
 4488 DocumentEntry.referenceIdList ein Dokument E via
 4489 urn:gematik:iti:xds:2025:childDocument oder
 4490 urn:gematik:iti:xds:2025:parentDocument referenziert,
- 4491 • für jedes Dokument E-das nicht ebenfalls gelöscht werden soll, prüfen, ob E für
 4492 den Anfragenden sichtbar ist:
 - 4493 • Wenn ja, für Dokument E prüfen, ob E für den Anfragenden gemäß Legal
 4494 Policy das "U"-Recht besitzt, und ansonsten die Verarbeitung mit dem
 4495 FehlerXDSCannotUnlinkAttachment_abbrechen und im codeContext-Attribut
 4496 des zurückgegebenen rs:RegistryError-Elements als Text die
 4497 DocumentEntry.uniqueId des referenzierten Dokuments angeben;
 - 4498 • Wenn nein, die Verarbeitung mit dem FehlerXDSCannotUnlinkAttachment
 4499 abbrechen ohne die DocumentEntry.uniqueId des referenzierten Dokuments E
 4500 preiszugeben.
 - 4501 • im Dokument E-die d, das nicht ebenfalls gelöscht werden soll, die d dazu passende
 4502 rückwärtige Referenz auf D aus E's referenceIdList entfernen.
- 4503 [\leq]
- 4504 Die Anforderung stellt sicher, dass keine "toten" Eltern- und Kindreferenzen im XDS
 4505 Document Service verbleiben.
- 4506 Hinweis: Zum Begriff "sichtbar" siehe analogen Hinweis unter A_27655.
- 4507 Hinweis 2: Ein Dokument kann also nicht gelöscht werden, wenn etwaige
 4508 Anhangsreferenzen ("Backlinks") in den referenzierten Dokumenten nicht gelöscht
 4509 werden können.
- 4510 3.13.1.4.3.4 RetrieveDocumentSet [ITI-43]
 4511 **A_14914 -XDS Document Service – Ablauflogik für Retrieve Document Set**
 4512 Der XDS Document Service MUSS die Umsetzung der Operation RetrieveDocumentSet
 4513 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3] und
 4514 [IHE-ITI-TF2b#3.43.4.2.2 und 3.43.4.2.3] implementieren.[\leq]
- 4515 **A_16201 -XDS Document Service – Prüfung der zurückgegebenen Paketgröße**
 4516 Der XDS Document Service MUSS anhand der übergebenen DocumentUniqueIDs die
 4517 Gesamtgröße ermitteln und bei Überschreitung von 250 MByte die Verarbeitung ablehnen
 4518 und die Nachricht mit einemMaxPkgSizeExceeded-Fehlercode gemäß [IHE-ITI-
 4519 TF3#4.2.4] quittieren.[\leq]
- 4520 3.13.1.4.3.5 Restricted Update Document Set [ITI-92]
 4521 **A_15061-08 -XDS Document Service – Ablauflogik für Restricted Update**
 4522 **Document Set**
 4523 Der XDS Document Service MUSS die Umsetzung der
 4524 OperationRestrictedUpdateDocumentSet gemäß der definierten Ablauflogik in [IHE-ITI-
 4525 RMU#3.92.4.1.2 und 3.92.4.1.3] implementieren und sicherstellen, dass (nur) die
 4526 folgenden Metadatenobjekte gesendet werden:
- 4527 • ein neues SubmissionSet,
 - 4528 • einen DocumentEntry inklusive der entryUUID des zu ändernden DocumentEntry-
 4529 Objekts. Das übermittelte DocumentEntry-Objekt kann sowohl alle vollständigen
 4530 Metadatenattribute als auch nur zu ändernde Metadatenattribute enthalten. In
 4531 jedem Fall dürfen Änderungen ausschließlich gemäß A_15083-* angenommen und
 4532 durchgeführt werden.

- 4533 • für das Hinzufügen, Ändern oder Löschen eines einzelnen oder mehrerer Werte
- 4534 in `DocumentEntry.author`, `DocumentEntry.confidentialityCode`,
- 4535 `DocumentEntry.eventCodeList` und `DocumentEntry.referenceIdList` gilt darüber
- 4536 hinaus:
- 4537 • es MÜSSEN alle und nicht nur die zu ändernden Werte (z. B. Autoren) über
- 4538 ihre jeweiligen `<classification classificationScheme="urn:uuid:...">-XML-`
- 4539 `Elemente` im gewünschten Soll-Zustand gesendet werden.
- 4540 • das Löschen aller Werte (z. B. Autoren) MUSS durch Übertragung ein
- 4541 einzelnen, komplett leeren `<classification="urn:uuid:...">-XML-Elements`
- 4542 signalisiert werden.
- 4543 • eine SS-DE HasMember-Association, die das `SubmissionSet` mit dem geschickten
- 4544 `DocumentEntry` verbindet.
- 4545 • die „lid“ (`logicalID`) DARF NICHT gesendet werden.
- 4546 • der Slot "`PreviousVersion`" MUSS immer mit dem Wert "1" gesendet werden.
- 4547 • der Slot „`AssociationPropagation`“ MUSS auf „no“ gesetzt werden. Zusätzlich
- 4548 MUSS der alternative Slot-Name "`associationPropagation`" akzeptiert werden.
- 4549 Der XDS Document Service DARF die gesendete `Association` und das neue
- 4550 `SubmissionSet` NICHT dauerhaft speichern. [`<=`]
- 4551 Der alternative Slot-Name "`associationPropagation`" wird unterstützt, da alte Versionen von
- 4552 ePA fälschlicherweise, abweichend von [IHE-ITI-RMU] diesen Wert gefordert haben.
- 4553 **A_15082-02 -XDS Document Service – Validierung der Metadaten aus ITI**
- 4554 **Document Sharing-Profilen**
- 4555 Der XDS Document Service MUSS die übermittelten `DocumentEntry`-Metadaten der
- 4556 `OperationRestrictedUpdateDocumentSet` dahingehend prüfen, dass gegenüber den
- 4557 Bestandsdaten die geänderten Metadaten konform zu den Nutzungsvorgaben
- 4558 in [A_14760-*] geändert werden. Der XDS Document Service MUSS das Aktualisieren
- 4559 der Metadatenattribute ablehnen und mit einem `XDSRepositoryMetadataError`
- 4560 quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. Es MUSS
- 4561 im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements angegeben
- 4562 werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht. [`<=`]
- 4563 **A_15083-09 -XDS Document Service – Prüfung auf ausschließliche**
- 4564 **Aktualisierung der erlaubten Metadaten**
- 4565 Der XDS Document Service MUSS die übermittelten `DocumentEntry`-Metadaten der
- 4566 `OperationRestrictedUpdateDocumentSet` dahingehend prüfen, dass gegenüber den
- 4567 Bestandsdaten ausschließlich die folgenden Metadaten geändert werden:
- 4568 • `DocumentEntry.author`
- 4569 • `DocumentEntry.classCode`
- 4570 • `DocumentEntry.comments`
- 4571 • `DocumentEntry.confidentialityCode` (`confidentialityCode` = "CON" (`codeSystem` =
- 4572 `urn:oid:1.2.276.0.76.5.491`) ist nicht erlaubt)
- 4573 • `DocumentEntry.creationTime`
- 4574 • `DocumentEntry.eventCodeList`
- 4575 • `DocumentEntry.formatCode`
- 4576 • `DocumentEntry.healthcareFacilityTypeCode`

- 4577 • DocumentEntry.languageCode
- 4578 • DocumentEntry.legalAuthenticator
- 4579 • DocumentEntry.practiceSettingCode
- 4580 • DocumentEntry.referenceIdList
- 4581 • DocumentEntry.serviceStartTime
- 4582 • DocumentEntry.serviceStopTime
- 4583 • DocumentEntry.title
- 4584 • DocumentEntry.typeCode
- 4585 • DocumentEntry.URI

4586 Wenn das Metadatum DocumentEntry.referenceIdList ohne rootDocumentUniqueId
 4587 gesendet wird, MUSS der XDS Document Service den Wert automatisch setzen (identisch
 4588 zu rootDocumentId in DocumentEntry.referenceIdList des ersetzten Dokuments). Wenn
 4589 die rootDocumentUniqueId gesendet wird, MUSS der XDS Document Service
 4590 sicherstellen, dass der Wert dem ansonsten automatisch gesetzten Wert entspricht.

4591
 4592 Werden unerlaubte Metadatenänderungen geschickt, muss die Operation mit
 4593 einem LocalPolicyRestrictionError-Fehlercode abgebrochen werden. Werden
 4594 Metadatenattribute mit leeren Werten übermittelt, signalisiert dies ein Löschen
 4595 des Metadatoms (z.B. DocumentEntry.comments). Es müssen die Kardinalitäten
 4596 in A_14760-* berücksichtigt bzw. dürfen nicht verletzt werden (Ausnahme für Altdaten:
 4597 eventCodeList darf mehr als einen DMP- oder KDL-Code in der eventCodeList enthalten,
 4598 wenn der alte Metadatenatz bereits dieselben DMP- und KDL-Codes führt). Das
 4599 Metadatum DocumentEntry.referenceIdList MUSS dabei mindestens die
 4600 rootDocumentUniqueId enthalten.

4601 Wenn in der Eingangsnachricht keine Aktualisierung für die erlaubten Metadaten
 4602 enthalten ist, ist die Weiterverarbeitung abzubrechen und die Nachricht mit einem
 4603 LocalPolicyRestrictionError-Fehlercode zu quittieren. [<=]

4604 **A_27657-01 -XDS Document Service – Anhänge hinzufügen oder entfernen mit** 4605 **Restricted Update Document Set**

4606 Der XDS Document Service MUSS beim Aktualisieren eines DocumentEntries die
 4607 folgenden Regeln durchsetzen (der Text bezieht sich auf das Einfügen oder Entfernen
 4608 eines parentDocument; die analoge Handlungsanweisung für childDocument ist jeweils in
 4609 Klammern angegeben):

- 4610 • Wenn dem Feld DocumentEntry.referenceIdList vor der Aktualisierung auf
 4611 ein über urn:gematik:iti:xds:2025:parentDocument
 4612 (urn:gematik:iti:xds:2025:childDocument) ausgezeichnetes Dokument
 4613 verweist, dieses aber für den Anfragenden nicht sichtbar ist, MUSS der XDS
 4614 DocumentService den entsprechenden Eintrag für die weitere Bearbeitung
 4615 automatisch wieder hinzufügen.
- 4616 • Wenn dem Feld DocumentEntry.referenceIdList ein Wert mit der Auszeichnung
 4617 urn:gematik:iti:xds:2025:parentDocument
 4618 (urn:gematik:iti:xds:2025:childDocument) hinzugefügt wird, MUSS der XDS
 4619 Document Service prüfen,
 - 4620 • ob das dem Anfragenden dort referenzierte Dokument nicht existent oder für
 - 4621 das anfragende System nicht sichtbar ist und in diesem Fall die Operation mit
 - 4622 dem Fehler XDSNoSuchParent (XDSNoSuchChild) abbrechen,

- ob für beide betroffenen Dokumente die Berechtigung "U" (gemäß Legal Policy) vorliegt und ansonsten die Verarbeitung mit dem Fehler `XDSCannotUnlinkAttachment` bzw. ~~`XDSCannotLinkAttachment`~~ abbrechen und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements als Text die `DocumentEntry.uniqueId` des referenzierten Dokuments angeben,
 - ob die Kennzeichnung des Dokuments als Anhang einen Verweiszirkel verursachen würde und ggf. die Operation mit dem Fehler `XDSAttachmentCycle` abbrechen;
 - ob durch das Markieren des Dokuments der zusätzliche Verweis nicht auf ein Elterndokument (Kinddokument) gemacht wird, das bereits Teil der Elternketten (Kindkette) ist und ansonsten die Verarbeitung mit dem Fehler `XDSInvalidAttachmentHierarchy` abbrechen.
- ~~• Wenn keiner der genannten Fehlerfälle vorliegt, MUSS der XDS Document Service im referenzierten `DocumentEntry` den passenden `urn:gematik:iti:xds:2025:childDocument` (`urn:gematik:iti:xds:2025:parentDocument` Feld `Document`) – Eintrag auf das ursprünglich aktualisierte Dokument in die `referenceIdList` einfügen.~~
- ~~• Wenn aus dem Feld `DocumentEntry.referenceIdList` ein Wert mit der Auszeichnung `urn:gematik:iti:xds:2025:parentDocument(urn:gematik:iti:xds:2025:childDocument)` entfernt wird, MUSS der XDS Document Service im dort referenzierte prüfen.~~
- ~~• ob für beide betroffenen Dokument den passenden `urn:gematik:iti:xds:2025:childDocument(urn:gematik:iti:xds:2025:parentDocument)` die Berechtigung "U" (gemäß Legal Policy) vorliegt und ansonsten die Verarbeitung mit dem Fehler `XDSCannotUnLinkAttachmentDocument` – Eintrag aus abbrechen und im `codeContext`-Attribut der `referenceIdList` entfernen.~~
- ~~• Wenns zurückgegebenen `rs:RegistryError`-Elements als Text die `DocumentEntry.uniqueId` des referen~~ee~~`IdList` vor der Aktualisierten Dokuments angeben,~~
- ~~• und ansonsten im dort referenzierung auf ein über den Dokument den passenden `urn:gematik:iti:xds:2025:parentchildDocument(urn:gematik:iti:xds:2025:childDocument)` ausgezeichnetes Dok~~parentDoc~~ument verweist, dieses aber für den Anfragenden nicht sichtbar ist, MUS) – Eintrag auS der XDS Document Service den entsprechenden Eintrag nach einer erfolgreichen Aktualisierung automatisch wieder hinzufüg~~referenceIdList~~ entfernen.~~

[<=]

Das Hinzufügen oder Entfernen von bestehenden Anhängen wird also immer entweder über den Verweis auf ein Eltern- oder Kinddokument vorgenommen; das referenzierte Dokument selbst wird immer automatisch angepasst. Wird über RMU die `referenceIdList` so gesetzt, dass die Eltern- und Kinddokumentausszeichnungen unverändert bleiben, ist A_27657 nicht relevant.

Zum Begriff "sichtbar" siehe analogen Hinweis unter A_27655. Die spezielle Behandlung für nicht sichtbare Dokumente ist notwendig, da eine Dokumentensuche eine solche Anhangsbeziehung zum verbundenen Dokument gemäß A_27762 aus der `DocumentEntry.referenceIdList` entfernt. Eine anschließende Aktualisierung des Dokuments kann also in aller Regel auch den Verweis auf das nicht sichtbare Eltern- oder Kinddokument nicht enthalten. Wenn der Anfragende es dennoch mitliefert (aus welcher

Quelle auch immer), gilt wie in der Anforderung beschrieben, dass der gesamte Aufruf mit dem Fehler `XDSNoSuchParent` bzw. `XDSNoSuchChild` abgelehnt werden muss (nicht etwa mit `XDSInvalidAttachmentHierarchy`).

Falls das Ändern der Metadaten zur Folge haben, dass ein Dokument in eine andere Dokumentenkategorie gemäß Legal Policy fällt, wird durch den XDS Document Service bewertet, ob der Anfragende überhaupt Dokumente in diese Kategorie einstellen darf. In dem Zusammenhang ist auch zu bewerten, ob alle per `referenceIdList` "geforderten" Anhänge des Dokuments überhaupt in dieser neuen Kategorie angehängt werden können (Berechtigung "U") und ob auch die Regeln zum Einstellen von Anhängen im Allgemeinen (darf der Dokumententyp bspw. Anhänge besitzen) eingehalten werden.

Beispiel: Für einen PDF/A-Arztbrief mit Anhängen wird der `classCode` auf "ADM" (administratives Dokument) geändert. Das Dokument ist damit nicht mehr als Arztbrief identifizierbar (A_27761) und sofern es nicht als anderer Dokumententyp erkannt wird, für den Anhänge erlaubt sind, ist das Metadatenupdate abzulehnen. Der passenden Fehler wäre in dem Fall wie oben angegeben `"XDSCannotLinkAttachment"`. Ein Client kann ggf. nur zuerst Dokumente "abhängen" und dann die Operation neu starten.

A_21533 -XDS Document Service – Kein Anlegen von Versionen für Restricted Update Document Set

Der XDS Document Service DARF eine echte Versionierung NICHT umsetzen, d. h. er DARF den alten `DocumentEntry` NICHT speichern. Insbesondere DARF der XDS Document Service `DocumentEntry.version` NICHT anlegen und verwalten. [`<=`]

A_21783-03 -XDS Document Service - Vererbung der geänderten Metadaten für Restricted Update Document Set

Der XDS Document Service MUSS die neu gesetzten Metadaten ebenfalls auf alle mit dem geänderten Dokument assoziierten Dokumente setzen. Als assoziierte Dokumente sind im Sinne dieser Anforderung Dokumente einer RPLC-Kette zu betrachten. [`<=`]

Metadaten von Dokumenten einer mixed- oder uniform-Sammlung dürfen nicht geändert werden.

A_25173 -XDS Document Service - Restricted Update Document Set nicht für MIOs

Falls die Operation `RestrictedUpdateDocumentSet` für Dokumente einer mixed- oder uniform-Sammlung aufgerufen wird MUSS der XDS Document Service das Aktualisieren der Metadatenattribute ablehnen, mit einem `XDSRepositoryMetadataError` quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements den Text "Metadata Update for MIOs not allowed" angeben. [`<=`]

3.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen

A_24508-01 -XDS Document Service – Prüfung der Policies bei Suchanfrage

Der XDS Document Service MUSS bei einer Suchanfrage für einen angemeldeten Nutzer die Suchergebnismenge entsprechend der Legal Policy und der General Deny Policy filtern, d. h. die Suchergebnismenge enthält ausschließlich XDS-Metadaten, die für einen angemeldeten Nutzer nicht diesen Policies widersprechen. [`<=`]

A_26222 -XDS Document Service (EU) – Prüfung Zugriffscode bei Suchanfrage EU-Zugriff

Der XDS Document Service MUSS für einen angemeldeten Nutzer mit der Rolle `oid_nceph` bei jeder Suchanfrage und jeder Retrieve-Operation prüfen, dass der im SOAP-Header der Operation übergebene Zugriffscode identisch ist mit dem im Entitlement Management für diesen Nutzer hinterlegten Zugriffscode und andernfalls die Operation mit dem Fehlercode `AccessCodeViolation` beenden. [`<=`]

A_24509 -XDS Document Service - Prüfung der Legal Policy außer Suchanfragen

Der XDS Document Service MUSS die Ausführung einer Operation mit dem Fehlercode LegalPolicyViolation beenden, wenn für den angemeldeten Nutzer die Regeln der Legal Policy nicht erfüllt sind und es sich nicht um eine Suchanfrage handelt.

Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die Liste der UUIDs (DocumentEntry.entryUUID) der identifizierten Dokumente angegeben werden. [<=]

A_24510-02 -XDS Document Service – Prüfung Herunterladen eines verborgenen oder nicht vorhandenen Dokuments

Der XDS Document Service MUSS die Ausführung der Retrieve-Operation mit dem Fehlercode XDSDocumentUniqueIdError beenden, wenn das assoziierte Dokument nicht vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind. [<=]

A_24511-01 -XDS Document Service – Prüfung Löschen eines verborgenen Dokuments oder dynamischen Ordners

Der XDS Document Service MUSS die Ausführung der Remove-Operation mit dem Fehlercode XDSDocumentUniqueIdError beenden, wenn für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.

[<=]

A_24512-02 -XDS Document Service – Prüfung Schreiben eines Dokuments in einen nicht vorhandenen oder verborgenen dynamischen Ordner

Der XDS Document Service MUSS die Ausführung der Provide-Operation mit dem Fehlercode UnresolvedReferenceException beenden, wenn der Ordner nicht existiert oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.

[<=]

A_24513-02 -XDS Document Service – Prüfung Aktualisierung Metadaten eines verborgenen oder nicht vorhandenen Dokuments

Der XDS Document Service MUSS die Ausführung der Update-Operation mit dem Fehlercode UnresolvedReferenceException beenden, wenn das assoziierte Dokument nicht vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind. [<=]

3.13.1.5 Fehlerbehandlung in Schnittstellenoperationen**A_22516-02 -XDS Document Service - Alternative Verwendung von XDSRegistryMetadataError anstelle von XDSDepositoryMetadataError**

Der XDS Document Service KANN alternativ zum Fehler "XDSDepositoryMetadataError" den Fehler "XDSRegistryMetadataError" verwenden. [<=]

A_23148-01 -XDS Document Service – Festlegung zu http-Statuscode bei IHE-Responses

Der XDS Document Service MUSS für den Fall, dass eine IHE-Response in der HTTP-Response enthalten ist, den http-Statuscode 200 zurückgeben. Das gilt auch, wenn die IHE-Response einen IHE-Fehler überträgt. [<=]

A_26324-01 -XDS Document Service - Aktenkonto im Umzug

Falls sich ein Aktenkonto im Zustand SUSPENDED befindet MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem StatusMismatch-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. <= [<=]

A_26325-01 -XDS Document Service - Aktenkonto unbekannt oder im Zustand INITIALIZED

4767 Falls sich ein Aktenkonto im Zustand UNKNOWN oder INITIALIZED befindet MUSS der
 4768 XDS Document Service die Verarbeitung ablehnen und mit einem `NoHealthRecord-`
 4769 Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. `<=[<=]`

4770 **A_25683-01 -XDS Document Service - Prüfung auf Befugnis**

4771 Falls keine gültige Befugnis für den aufrufenden Nutzer vorliegt MUSS der XDS Document
 4772 Service die Verarbeitung ablehnen und mit einem `NotEntitled`-Fehlercode gemäß [IHE-
 4773 ITI-TF3#4.2.4] quittieren. `[<=]`

4774 **A_26459 -XDS Document Service - keine Authentisierung des Nutzers**

4775 Falls keine erfolgreiche Authentifizierung des Nutzers vorliegt MUSS der XDS Document
 4776 Service die Verarbeitung ablehnen und mit einem `InvalidAuth`-Fehlercode gemäß [IHE-ITI-
 4777 TF3#4.2.4] quittieren. `<=[<=]`

4778 **A_27541 -XDS Document Service - keine Geräteregistrierung des Nutzers**

4779 Falls der Nutzer der Versicherte oder ein Vertreter ist (`oid_versicherter`) und keine
 4780 Geräteregistrierung des Nutzers vorliegt, MUSS der XDS Document Service die
 4781 Verarbeitung ablehnen und mit einem `UnregisteredDevice`-Fehlercode gemäß [IHE-ITI-
 4782 TF3#4.2.4] quittieren. `[<=]`

4783 **3.13.1.6 Schnittstellen im XDS Document Service**

4784 In diesem Abschnitt wird die Außenschnittstelle des XDS Document Service festgelegt.
 4785 Einzelne Umsetzungsanforderungen suggerieren eine vermischte Verarbeitung von
 4786 Funktionalitäten, welche bei IHE ITI originär getrennt von einer Document Registry und
 4787 einem Document Repository (bzw. den Responding Gateways) durchgeführt werden. Da
 4788 die Außenschnittstelle des XDS Document Service nicht zwischen Document Registry und
 4789 Document Repository unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit
 4790 differenzierten Pfaden, siehe A_26814-*, werden sonst bei IHE ITI explizite Operationen
 4791 zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne Umsetzung
 4792 angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-Nachricht
 4793 kann an IHE ITI-konforme Akteure ausgerichtet werden.

4794 **3.13.1.6.1 Schnittstelle I_Document_Management**

4795 Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-
 4796 Transaktionen bei mehreren Schnittstellen .

4797 **A_14152-02 -XDS Document Service – Implementierung der Schnittstelle** 4798 **I_Document_Management**

4799 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-
 4800 Service-Schnittstelle für den Zugriff von ePA-Clients, die über das zentrale Netz zugreifen
 4801 implementieren.

4802 **Tabelle 27: Schnittstelle I_Document_Management**

Schnittstelle	I_Document_Management	
Version	2.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung

	ProvideAndRegisterDocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Metadata	Löschen von Dokumenten oder Ordnern
	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
WSDL	[XSDDocumentService]	
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd 	

4803 **[<=]**

4804 Durch die Legal Policy ist geregelt, welche Clients (professionOID) letztendlich zugreifen
4805 dürfen.

4806 3.13.1.6.1.1 Operation I_Document_Management::ProvideAndRegisterDocumentSet-b
4807 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
4808 Transaktion "ProvideAndRegisterDocumentSet-b" [ITI-41] sind [IHE-ITI-TF2x] sowie
4809 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4810 Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner
4811 gesammelt. Das Anlegen eines DiGA-Ordners erfolgt durch den XDS Document Service
4812 unter der Voraussetzung, dass es eine gültige Befugnis für die DiGA gibt. Der DiGA-
4813 Ordner wird vom XDS Document Service mit der Telematik-ID der DiGA verknüpft.
4814 Die Zuordnung von DiGA-Dokumenten beim Schreiben erfolgt implizit über die
4815 TelematikID aus dem IDToken des Nutzers. Da ein DiGA-Ordner im Titel immer den
4816 Namen der DiGA enthält kann ein Client (z.B. LEI) darüber die relevante DiGA auswählen
4817 und auf die Dokumente der DiGA, sofern eine Befugnis für den Nutzer vorliegt, lesend
4818 zugreifen.

4819 Ein Update eines bestehenden Dokuments mit der bekannten DocumentEntry.entryUUID
4820 kann durch einen DiGA-Client erfolgen. Hierzu ist es erforderlich, dass ein DiGA-Client
4821 die DocumentEntry.entryUUID persistiert und keine symbolischen IDs gemäß [IHE-ITI-
4822 TF2b#3.42.4.1.3.7] verwendet.

A_21512-04 -XDS Document Service – dynamisches Anlegen von DiGA-Ordern

Falls eine gültige Befugnis für eine konkrete DiGA vorliegt, MUSS der XDS Document Service beim erstmaligen Einstellen eines Dokumentes für diese DiGA in die Akte des Versicherten (Operation `I_Document_Management::ProvideAndRegisterDocumentSet-b()`) sicherstellen, dass genau ein Ordner für den Versicherten mit den folgenden Eigenschaften angelegt ist:

- DiGA-Ordner der Kategorie `diga` gemäß A_19388 (Belegung `Folder.codeList`) unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A_14760 (Belegung der restlichen Metadatenfelder).
- `Folder.title` wird entsprechend des Attributs `"organizationName"` aus dem `IDToken` der zugreifenden DiGA belegt.
- `Folder.comment` wird belegt mit `"urn:gematik:diga:<Telematik-ID>"`, wobei die Telematik-ID dem Attribut `"idNummer"` des ID-Token entspricht.
- `Folder.EntryUUID` wird mit einer aus der TelematikID abgeleiteten UUID belegt.

Die `folder.EntryUUID` MUSS wie folgend dargestellt aus der TelematikID der DiGA erzeugt werden:

- Algorithmus: Name-Based UUID gemäß [RFC4122#4.3], Version 3 (MD5)
- Namensraum-UUID: `"e2310a38-0b62-415e-8b44-994dc8312965"`
- Name: `"<TelematikId>"`

Eine konkrete DiGA wird identifiziert durch die TelematikID und ist als DiGA durch die `professionOID` gekennzeichnet.

[<=]

A_22994-01 -XDS Document Service - automatische Folder-Zuordnung für DiGA

Der XDS Document Service MUSS beim Einstellen eines DiGA-Dokumentes in die Akte des Versicherten (Operation `I_Document_Management::ProvideAndRegisterDocumentSet-b()`) sicherstellen, dass das DiGA-Dokument in den durch die TelematikID referenzierten DiGA-Ordner abgelegt wird. Die TelematikID des zu adressierenden Ordners entspricht dem Attribut `"idNummer"` des ID-Token. [<=]

A_21713-03 -XDS Document Service – Kein Einstellen von Ordnern

Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) über die Schnittstelle `I_Document_Management::ProvideAndRegisterDocumentSet-b` ablehnen und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder enthalten sind. Ausnahme: Folder der Kategorie `pregnancy_childbirth` in `Folder.codeList`. [<=]

A_24497 -XDS Document Service - Verwendung der korrekten Telematik-ID beim Einstellen

Der XDS Document Service MUSS die Telematik-ID aus dem ID-Token der aktuellen User Session abgleichen mit der Telematik-ID `ausSubmissionSet.authorInstitution` und das Abweichen der Telematik-Ids mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError-Elements` den Text `"Telematik-ID does not match"` angeben. [<=]

A_24456 -XDS Document Service - Durchsetzung von Uniqueness beim Einstellen von Notfalldaten

Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien `"emergency"` sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein

einzelnes NFD- und ein einzelnes DPE-Dokument im Status "approved" gibt. Der Versuch, innerhalb dieses Ordners ein zweites NDF- oder DPE-Dokument einzustellen, MUSS mit dem IHE-ErrorInvalidDocumentContent abgebrochen werden. Es MUSS im codeContext-Attribut des zurückgegebenenInvalidDocumentContent-Elements der Text "Medical information object has to be unique" zurückgegeben werden.[<=]

A_25137 -XDS Document Service - Durchsetzung von Uniqueness beim Einstellen vom Medikationsplan

Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien "emp" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein einzelnes eMP-Dokument im Status "approved" gibt. Der Versuch, innerhalb dieses Ordners ein zweites eMP-Dokument einzustellen, MUSS mit dem IHE-ErrorInvalidDocumentContent abgebrochen werden. Es MUSS im codeContext-Attribut des zurückgegebenenInvalidDocumentContent-Elements der Text "Medical information object has to be unique" zurückgegeben werden.[<=]

3.13.1.6.1.2 Operation I_Document_Management::RegistryStoredQuery
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.1.3 Operation I_Document_Management::RemoveMetadata
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.1.4 Operation I_Document_Management::RetrieveDocumentSet
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.1.5 Operation I_Document_Management::RestrictedUpdateDocumentSet
Weitere Details zur Ausgestaltung dieser Operation finden sich bezüglich der dazugehörigen IHE ITI-Transaktion "RestrictedUpdateDocumentSet" [ITI-92] in [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x].

Weitere Anforderungen zur Umsetzung der Operation RestrictedUpdateDocumentSet befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92] .

3.13.1.6.2 Schnittstelle I_Document_Management_Insurant

Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen .

A_14478-01 -XDS Document Service – Implementierung der Schnittstelle I_Document_Management_Insurant

Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle für den Zugriff des ePA-FdV implementieren .

Tabelle 28: Schnittstelle I_Document_Management_Insurant

Schnittstelle	I_Document_Management_Insurant
Version	2.0.0
Namensraum	urn:ihe:iti:xds-b:2007

Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente im XDS Document Service
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Metadata	Löschen ein oder mehrerer Dokumente oder Folder
	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
WSDL	[XDSDocumentService]	
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd 	

4910

4911 [**<=**]4912 **A_26460 -XDS Document Service - Zugriff über**4913 **I_Document_Management_Insurant mit nicht registriertem Gerät**

4914 Falls Operationen von I_Document_Management_Insurant ohne registriertes Gerät
 4915 aufgerufen werden MUSS der XDS Document Service die Verarbeitung ablehnen und mit
 4916 einemUnregisteredDevice-Fehlercode quittieren.[**<=**]

4917 3.13.1.6.2.1 Operation

4918 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b

4919 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 4920 Transaktion "Provide And Register Document Set-b" [ITI-41] sind [IHE-ITI-TF2x] sowie
 4921 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4922 **A_21481-05 -XDS Document Service – Kein Einstellen von Ordnern und**
 4923 **Associations**

4924 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und
 4925 Dokument(en) über die Schnittstelle
 4926 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b() ablehnen und
 4927 mit einem XDSRegistryMetadataError-Fehlercode quittieren, wenn in der
 4928 Eingangsnachricht ein oder mehrere neu anzulegende Folder oder andere als die
 4929 folgenden Assoziationen

- 4930 • SS-DE
- 4931 • SS-HM
- 4932 • FD-DE
- 4933 • RPLC

4934 enthalten sind. [\leq]

4935 Das Referenzieren bestehender Ordner ist davon nicht berührt, wie dies z. B. beim
 4936 Einstellen von Dokumenten in Sammlungen der Fall ist (z. B. Einstellen eines Dokuments
 4937 in einen Mutterpass).

4938 **A_23144 -XDS Document Service - Automatische Ablage von Dokumenten im** 4939 **Ordner "technical"**

4940 Der XDS Document Service MUSS sicherstellen, dass Dokumente mit einem formatCode
 4941 mit der codeSystem OID "2.25.154081344090540725127779452347992051720",
 4942 unabhängig von weiteren Metadaten, im statischen Ordner "technical" abgelegt
 4943 werden. [\leq]

4944 3.13.1.6.2.2 Operation I_Document_Management_Insurant::RegistryStoredQuery
 4945 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 4946 Transaktion "Registry Stored Query" [ITI-18] sind [IHE-ITI-TF2a], [IHE-ITI-TF2x] sowie
 4947 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4948 3.13.1.6.2.3 Operation I_Document_Management_Insurant::RemoveMetadata
 4949 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 4950 Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-
 4951 ITI-TF2x] zu entnehmen.

4952 3.13.1.6.2.4 Operation I_Document_Management_Insurant::RetrieveDocumentSet
 4953 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 4954 Transaktion "RetrieveDocumentSet" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
 4955 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4956 3.13.1.6.2.5 Operation
 4957 I_Document_Management_Insurant::RestrictedUpdateDocumentSet
 4958 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 4959 Transaktion "RestrictedUpdateDocumentSet" [ITI-92] sind [IHE-ITI-RMU], [IHE-ITI-
 4960 TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4961 Weitere Anforderungen zur Umsetzung der Operation RestrictedUpdateDocumentSet
 4962 befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92].

4963 3.13.1.6.3 Schnittstelle I_Document_Management_Ncpeh

4964 Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-
 4965 Transaktionen bei mehreren Schnittstellen.

4966 **A_27300-01 -XDS Document Service (EU) – Implementierung der Schnittstelle** 4967 **I_Document_Management_Ncpeh**

4968 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-
 4969 Service-Schnittstelle für den Zugriff durch den NCPeH-FD implementieren.

4970 **Tabelle 29: Schnittstelle I_Document_Management_Ncpeh**

Schnittstelle	I_Document_Management_Ncpeh	
Version	2.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
WSDL	[XDSDocumentService]	
XML Schema	<ul style="list-style-type: none">• PRPA_IN201301UV02.xsd• PRPA_IN201302UV02.xsd• PRPA_IN201304UV02.xsd• MCCI_IN000002UV01.xsd• query.xsd• rs.xsd• lcm.xsd• rim.xsd• XDS.b_DocumentRepository.xsd	

4971
4972 **[<=]**

4973 3.13.1.6.3.1 Operation I_Document_Management_Ncpeh::RegistryStoredQuery
4974 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
4975 Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
4976 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4977 3.13.1.6.3.2 Operation I_Document_Management_Ncpeh::RetrieveDocumentSet
4978 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
4979 Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
4980 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4981 **3.13.1.7 Statische Metadaten**

4982 Statische Inhalte werden vor der ersten Nutzung des XDS Document Service angelegt, d.
4983 h. bevor auf XDS Metadaten zugegriffen wird. Sie sind unveränderlich.

4984 **A_24491-02 -XDS Document Service – Anlegen von statischen Ordnern**

4985 Der XDS Document Service MUSS nach der erfolgreichen Anlage der Akte des
4986 Versicherten die Kategorienordner unter Berücksichtigung allgemeiner Vorgaben für

4987 Folder-Metadaten in A_14760* (Belegung der restlichen Metadatenfelder) für den
 4988 Versicherten gemäß der folgenden Tabelle anlegen. Alle statischen Kategorienordner
 4989 werden mit jeweils einem Ordner pro Kategorie angelegt. Alle statischen Ordner sind
 4990 nach dem Anlegen initial leer.
 4991 Das Anlegen von Submission Sets und zugehöriger Associations zu den statischen
 4992 Ordnern ist nicht vorgegeben. Das XDS-Informationsmodell MUSS allerdings hinsichtlich
 4993 der Folder-DocumentEntry- sowie SubmissionSet-HasMember-Associations bei einer
 4994 Verarbeitung durch die Document Consumer (z. B. Querying) erfüllt werden.

4995 **Tabelle 30: Festlegung Folder.entryUUID zu statischen Ordnern**

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
reports	b878db05-49e4-4f74-a329-b3bcdd8082c4
emp	7c1054ea-a4df-4a1b-8e10-209f6d8812ee
emergency	a7bb6be7-d756-46dd-90d4-4020ed55b777
eab	2ed345b1-35a3-49e1-a4af-d71ca4f23e57
dental	af547321-b8e8-4e1d-b9af-51bb4a990bda
child	2c898452-4667-40e3-9d3e-c09d7385b527
vaccination	9c3edaf3-a978-46fe-8e6e-021ff4aca60b
patient	d236c9a2-ab01-4902-a00a-1e1dff439fe7
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d
health_risk_analysis	840a59c7-61d4-4caa-80a7-1857af2f166f
care	2d62bf9e-062a-4aa7-9951-9f33bbc665b5
eau	aa7d10d6-204a-47aa-be73-44bdcb77512f
other	605a9f3c-bfe8-4830-a3e3-25a4ec6612cb

technical	f88dc706-d2df-4ca0-a850-491cfaab2d31
rehab	173f4204-fb93-4a1a-a1f6-316703b79539
transcripts	6A8E383D-8705-4B0E-A140-39A5F144501D

4996
4997

[<=]

4998 *Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner vom Typ*
4999 *"pregnancy_childbirth" und verwenden als Folder.title ein Kennzeichen der*
5000 *Schwangerschaft (A_22515-*).*

5001 **A_20216-04 -XDS Document Service – Unveränderlichkeit von statischen** 5002 **Akteninhalten**

5003 Der XDS Document Service DARF die Metadaten eines statischen Aktenobjekts gemäß
5004 A_24491 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen.
5005 Dabei gelten folgende Ausnahmen:

- 5006 • Folder.lastUpdateTime - Folder.lastUpdateTime wird automatisch vomXDS
5007 Document Service aktualisiert, sobald Dokumente in den Ordner eingestellt (siehe
5008 auch [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6]), daraus gelöscht
5009 oder darin aktualisiert werden.

5010 [<=]

5011 **3.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten**

5012 Für den XDS Document Service werden Vorgaben bezüglich zu verwendender IHE XDS-
5013 Metadatenattribute auf Ebene von Submission Set, Document Entry sowie Folder
5014 vorgenommen. Diese Nutzungsvorgaben referenzieren größtenteils Value Sets der IHE
5015 Deutschland Arbeitsgruppe "XDS Value Sets" [IHE-ITI-VS] und sind für die ePA-
5016 Fachanwendung verbindlich. Diese XDS-Value Sets sind teilweise von IHE-Deutschland
5017 als "offen" gekennzeichnet, um Erweiterungen flexibel einbringen zu können. Für
5018 die ePA-Fachanwendung gelten jedoch definierte Vorgaben, wie neue Codes und Value
5019 Sets sicher über eine Konfigurationsschnittstelle eingebracht werden können. Daher sind
5020 die in dieser Spezifikation beschriebenen Nutzungsvorgaben für Value Sets als fest
5021 anzusehen bzw. die Offenheit der XDS Value Sets wird nicht unterstützt.

5022 **3.13.1.8.1 Allgemeine Metadatenvorgaben**

5023 Die Spalten der unten dargestellten, tabellarischen Übersichten für die Metadaten von
5024 Dokumenten (IHE XDS.b Document Entry) und Übertragungspaketen (IHE XDS.b
5025 Submission Set) haben die folgenden Bedeutungen:

- 5026 • Die Spalte "Metadatenattribut XDS.b" listet alle aus dem IHE ITI TF vorgesehenen
5027 Metadaten für Document Entry- und Submission Set-Elemente auf.
- 5028 • Die Spalten "Mult. PS" (Multiplizität Primärsystem; alle Primärsysteme außer PS-
5029 KTR), "Mult. KTR" (Multiplizität "PS-KTR"), "Mult. DS" (Multiplizität "Document
5030 Service"), "Mult. FV" (Multiplizität "ePA-Frontend des Versicherten") kennzeichnen
5031 die Multiplizität des Metadatenattributs beim Erzeugen oder Verarbeiten durch das
5032 jeweilige System.

- 5033 Die Angabe der jeweiligen Spalte entspricht einem Wertebereich. Die Zeichen [...] für Wertebereich wurden zum Zwecke der besseren Darstellbarkeit weggelassen.
- 5034
- 5035 • Die Spalte "Kurzbeschreibung" beschreibt kurz die Bedeutung des Metadatenattributs.
- 5036
- 5037 • 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.
- 5038
- 5039
- 5040 • 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.
- 5041
- 5042
- 5043
- 5044
- 5045
- 5046 **A_14760-27 -Nutzungsvorgaben für die Verwendung von XDS-Metadaten**
- 5047 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
- 5048
- 5049
- 5050
- 5051
- 5052 • I_Document_Management::ProvideAndRegisterDocumentSet-b sowie
- 5053 • I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- 5054 registriert oder über die Operationen
- 5055 • I_Document_Management::RestrictedUpdateDocumentSet
- 5056 • I_Document_Management_Insurant::RestrictedUpdateDocumentSet
- 5057 geändert werden.
- 5058 Für den Produkttyp DiGA gelten die gleichen Vorgaben wie für die Primärsysteme sofern unter Nutzungsvorgaben keine abweichenden Bedingungen definiert werden.
- 5059
- 5060 **Tabelle 31: Nutzungsvorgaben für Metadatenattribute XDS**

Metadaten- attribut XDS.b		Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
		P S	K T R	D S	F d V			
Metadaten für DocumentEntry								
author		1. .n	1. .1	0. .0	0. .n	Person oder System, welche(s) das Dokument erstellt hat	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.1] genügen. Das Primärsystem MUSS mindestens das Subattribut authorPerson oder authorInstitution inhaltlich belegen.	
	authorPerson	0.	0.	0.	0.	Name des Autors	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt	X

	.1	.1	.0	.1		3.13.1.8.2- Metadaten der Dokumente und SubmissionSets genügen.	
authorInstitution	0. .n	0. .n	0. .0	0. .n	Institution, die dem Autor zugeordnet ist	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 3.13.1.8.2- Metadaten der Dokumente und SubmissionSets (A_21209) genügen.	X
authorRole	0. .n	0. .n	0. .0	0. .n	Rolle des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAutorRoleVS aus [IG_TI_Terminology] entsprechen.	X
authorSpecialty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAutorSpecialtyVS aus [IG_TI_Terminology] entsprechen.	X
authorTelecommunication	0. .n	0. .0	0. .0	0. .n	Telekommunikationsdaten des Autors	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	X
availabilityStatus	0. .0	0. .0	1. .1	0. .0	Status des Dokuments ("Approved" oder "Deprecated")	Der Wert MUSS initial "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
classCode	1. .1	1. .1	0. .0	1. .1	Grobe Klassifizierung des Dokuments	<p>Der Wert MUSS einem Code des Value Sets EPAXDSClassCodeVS aus [IG_TI_Terminology] entsprechen.</p> <p>Sofern das Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9- Strukturierte Dokumente genügen.</p> <p>PS-KTR MUSS für Dokumente</p> <ul style="list-style-type: none"> • der Kategorie receipt ausschließlich den Code "ADM" (Administratives Dokument) verwenden • und für solche der 	X

						Kategorie health_risk_analysis den Code "ASM" (Assessment) verwenden.	
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.4] genügen.	X
confidentialityCode	0. .n	0. .n	0. .1	0. .n	Vertraulichkeitske- nnzeichnung 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 [IG_TI_Terminology] entsprechen. Für ProvideAndRegisterDocuments et-b MUSS für das Verbergen des Dokumentes der Code <ul style="list-style-type: none"> Code = "CON", Display Name = "constraint" aus dem Code System 1.2.276.0.76.5.491 (siehe auch Value Set EPAXDSConfidentialityCodeVS aus [IG_TI_Terminology]) gesetzt werden.	X
creationTime	1. .1	1. .1	0. .0	1. .1	Erstellungszeitpu- nkt des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.6] genügen und DARF NICHT in der Zukunft liegen. Bei der Prüfung ist eine Toleranz von 5 Minuten zulässig.	X
entryUUID	1. .1	1. .1	0. .1	1. .1	Intern verwendete, aktenweit eindeutige Kennung des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.7] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI- TF2b#3.42.4.1.3.7] auflösen.	
eventCodeList	0. .n	0. .0	0. .0	0. .n	Ereignisse, die zur Erstellung des Dokuments geführt haben.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.8] genügen und Codes des Value Set EPAXDSEventCodeVS aus	X

						<p>[IG_TI_Terminology] entsprechen.</p> <p>Der Wert darf höchstens einen KDL-Code ("Klinische Dokumentenklassen-Liste") und höchstens einen DMP-Code ("Disease Management Programm") enthalten.</p> <p>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.</p>	
formatCode	1. .1	1. .1	0. .0	1. .1	<p>Global eindeutiger Code für das Dokumentenformat.</p> <p>Zusammen mit dem DocumentEntry.typeCode eines Dokuments soll es einem potentiellen zugreifenden System erlauben, im Vorfeld festzustellen, ob das Dokument verarbeitet werden kann.</p>	<p>Der Wert MUSS einem Code des Value Sets EPAXDSFormatCode aus [IG_TI_Terminology] entsprechen. Der Wert KANN "urn:ihe:iti:xds:2017:mimeTypeSufficient" (siehe [IHE-ITI-TF-3#4.2.3.2.9]) entsprechen, um anzuzeigen, dass über den MIME-Type hinaus keine genaueren Angaben zum Dokumentenformat gemacht werden können oder der MIME-Type ausreichend ist.</p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9- Strukturierte Dokumente genügen.</p>	
hash	0. .0	0. .0	1. .1	0. .0	Kryptographische Prüfsumme des Dokuments	Der Wert wird vom XDS Document Service beim Einstellen des Dokuments in die Akte berechnet.	
healthcareFacilityTypeCode	1. .1	1. .1	0. .0	1. .1	Art der Einrichtung, in der das dokumentierte Ereignis stattgefunden	<p>Der Wert MUSS einem Code des Value Sets EPAXDSHealthcareFacilityTypeCodeVS aus [IG_TI_Terminology] entsprechen.</p> <p>Das PS-KTR MUSS</p>	X

					hat.	healthcareFacilityTypeCode ausschließlich mit dem Wert "VER" (Versicherungsträger) belegen. Die DiGA MUSS healthcareFacilityTypeCod e mit dem Wert "PAT" belegen.	
homeCommunityId	0. .1	0. .1	0. .0	0. .1		n/a Eine optional übertragene homeCommunityId wird nicht gespeichert.	
languageCode	1. .1	1. .1	0. .0	1. .1	Sprache, in der das Dokument abgefasst ist.	Der Wert MUSS einem Code des Value Sets EPAXDSLlanguageCodeVS aus [IG_TI_Terminology] entsprechen. Es MÜSSEN mindestens die in der Tabelle Tab_LanguageCodes angegebenen Codes unterstützt werden, alle weiteren Codes KÖNNEN unterstützt werden.	X
legalAuthenticator	0. .1	0. .0	0. .0	0. .1	Rechtlich Verantwortlicher für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.14] genügen. Das Attribut DARF NICHT gesetzt werden, falls es sich um ein automatisch erstelltes und nicht durch eine natürliche Person freigegebenes Dokument handelt.	
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierungsattribut, dass das Metadatenelement DocumentEntry nicht den vollständigen Satz an Metadaten enthält.		

mimeType	1. .1	1. .1	0. .0	1. .1	MIME-Type des Dokuments	<p>Ein Wert aus der folgenden Liste gemäß A_24864* und A_25009* MUSS als MIME-Type verwendet werden.</p> <p>PS-KTR MUSS für Dokumente der Kategorie health_risk_analysis ausschließlich den Wert "application/pdf" gemäß A_25009-* verwenden. Als formatCode ist dann entsprechend "urn:ihe:iti:xds:2017:mimeTypeSufficient" zu verwenden</p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9- Strukturierte Dokumente genügen.</p> <p><u>Anmerkung:</u> In Klammern sind die Extensions angegeben, die beim entsprechenden MIME-Type in DocumentEntry.URI für das URI-scheme "file," zu verwenden sind.</p>	
objectType	1. .1	1. .1	0. .0	1. .1	Typ des Dokuments	<p>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].</p>	
patientId	1. .1	1. .1	0. .0	1. .1	Systemweit eindeutige Kennung des Patienten	<p>Der Wert MUSS den Inhalts- und Formatvorgaben aus A_14974* genügen.</p> <p>Außerdem MUSS der Wert der Identität des Akteninhabers entsprechen und MUSS vom XDS Document Service dahingehend bei Registrierung der Metadaten geprüft werden.</p>	

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 EPAXDSPacticeSettingCodeVS aus [IG_TI_Terminology] entsprechen. Die DiGA MUSS practiceSettingCode mit dem Wert "PAT" belegen.	X
referenceIdList	0. .n	0. .1	1. .1	0. .n	Liste von IDs, mit denen das Dokument assoziiert wird.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.28] genügen. Wenn KTR-Clients einen Wert übertragen, muss es sich um die rootDocumentId im Rahmen einer RMU-Operation (Aktualisierung) oder dem Ersetzen (RPLC) eines Dokuments handeln.	
repositoryUniqueid	0. .1	0. .1	1. .1	0. .1	Kennung des Document Repository, in welches das Dokument eingestellt wird/wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.18] genügen.	
serviceStartTime	0. .1	0. .1	0. .0	0. .1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis begonnen wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.19] genügen.	X
serviceStopTime	0. .1	0. .1	0. .0	0. .1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis beendet wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.20] genügen.	X
size	0. .0	0. .0	1. .1	0. .0	Größe des Dokuments in Bytes	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.21] genügen. Der XDS Document Service MUSS die Größe des Dokuments berechnen und in den Metadaten	

						während des Registriervorgangs setzen (vgl. [IHE-ITI-TF2b#3.41.4.1.3])).	
sourcePatientId	0. .1	0. .0	0. .0	0. .0	Kennung des Patienten im Quellsystem	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.22] genügen.	
sourcePatientInfo	0. .n	0. .0	0. .0	0. .0	Demographische Daten zum Patienten im Quellsystem	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.23] genügen.	
title	1. .1	1. .1	1. .1	1. .1	Titel des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.24] genügen. Ein leeres Feld <code>DocumentEntry.title=""</code> bzw. ausschließlich mit nicht druckbaren Zeichen befüllt ist nicht erlaubt.	X
typeCode	1. .1	1. .1	0. .0	1. .1	Art des Dokuments	Der Wert MUSS einem Code des Value Sets EPAXDSTypeCodeVS aus [IG_TI_Terminology] entsprechen. PS-KTR MUSS für Dokumente der Kategorie <code>health_risk_analysis</code> ausschließlich den Code "GRIS" verwenden Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Inhalts- und Formatvorgaben aus Abschnitt 3.13.1.9- Strukturierte Dokumente genügen.	X
uniqueId	1. .1	1. .1	0. .0	1. .1	Eindeutige, aktenweite Kennung des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.26] genügen.	
URI	1. .1	1. .1	0. .0	1. .1	URI für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.27] genügen und mittels A_24524-*	

						normalisiert werden. Die extension der DocumentEntry.URI MUSS wird dem mimetype gemäß A_23447-* angepasst, falls erforderlich.	
Metadaten für SubmissionSet							
author	1. .n	1. .1	0. .0	1. .1	Person oder System, welche(s) das Submission Set erstellt hat.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.1] genügen.	
authorPerson	0. .1	0. .1	0. .0	0. .1	Name der einstellenden Person oder des einstellenden Systems	<p>Der Wert MUSS den Formatvorgaben aus Abschnitt <u>3.13.1.8.2- Metadaten der Dokumente und SubmissionSets</u> genügen.</p> <p>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.</p>	

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>3.13.1.8.2- 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.
authorRole	1. .n	1. .n	0. .0	1. .1	Rolle der einstellenden Person oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAAuthorRoleVS aus [IG_TI_Terminology] entsprechen. Das PS-KTR MUSS den Code "105" (Kostenträgervertreter) verwenden. Das ePA-Frontend des Versicherten MUSS den Code "102" (der Patient selbst) verwenden. Die DiGA MUSS authorRole mit dem Code "12" (dokumentierendes Gerät) verwenden.
authorSpecialty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung der einstellenden Person oder des einstellenden	Der Wert MUSS einem Code des Value Sets EPAXDSAAuthorSpecialtyVS aus [IG_TI_Terminology] entsprechen.

					Systems		
authorTelecom munication	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.	
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
contentTypeCod e	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 [IG_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- TF2b#3.42.4.1.3.7] auflösen.	
homeCommunit yId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
intendedRecipie nt	0. .n	0. .0	0. .0	0. .n	Vorgesehener Adressat des Submission Set	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.3.7] genügen.	
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierung, welche anzeigt, dass das Submission Set nicht den durch das IHE ITI TF vorgegebenen Satz an Metadaten enthält.		

patientId	1. .1	1. .1	0. .0	1. .1	Patienten-ID, zu der das Submission Set gehört	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
sourceId	0. .0	0. .0	0. .0	0. .0	Weltweit eindeutige, unveränderliche Kennung des einstellenden Systems		
submissionTime	1. .1	1. .1	0. .0	1. .1	Zeit, zu der das Submission Set zusammengestellt wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.10] genügen. Der XDS Document Service MUSS prüfen, ob der Wert der aktuellen Systemzeit entspricht. Sollte diese von der lokalen Zeit über mehr als eine Minute abweichen, MUSS der Wert mit der aktuellen Systemzeit ersetzt werden. Diese Systemzeit MUSS dabei synchron zur Systemzeit des Produkttyps Zeitdienst gemäß A_24673 sein.	
title	0. .1	0. .1	0. .0	0. .1	Titel des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.11] genügen.	X
uniqueId	1. .1	1. .1	0. .0	1. .1	Eindeutige Kennung des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.12] genügen.	
Metadaten für dynamische Folder							
availabilityStatus	1. .1	n/ a	0. .0	n/ a	Status des Ordners ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
codeList	1. .1	n/ a	0. .0	n/ a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] und einem Code des Value Sets EPADataCategoryOtherVS aus [IG_TI_Terminology] entsprechen. Bei	

						Folder.codeList=pregnancy_child birth 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 Ordnerns	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI- TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
lastUpdateTime	0. .0	n/ a	1. .1	n/ a	Zeitstempel, an dem der Ordner das letzte mal geändert wurde	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.6] genügen. Der XDS Document Service MUSS den Wert automatisch gemäß [IHE-ITI- TF2b#3.42.4.1.3.6] aktuell halten. Zudem MUSS der XDS Document Service den Wert aktualisieren, wenn ein Dokument aus dem Ordner gelöscht oder dessen Metadaten aktualisiert wurden.	
limitedMetadata	Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden.						
patientId	1. .1	n/ a	0. .0	n/ a	Patienten ID, zu der der Ordner gehört.	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
title	1. .1	n/ a	0. .0	n/ a	Titel des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.8] genügen.	
uniqueId	1. .1	n/ a	0. .0	n/ a	Eindeutige, aktenweite Kennung des Ordnerns	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 EPADDataCategoryOtherVS und EPADDataCategoryMedicalVS aus [IG_TI_Terminology] entsprechen. Der XDS Document Service MUSS codeList gemäß A_19388* setzen.
comments	n/a	n/a	0.1	n/a	Freitextkommentar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen.
entryUUID	n/a	n/a	1.1	n/a	Intern verwendete, aktenweit eindeutige Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId					
lastUpdateTime	n/a	n/a	1.1	n/a	Zeitstempel, an dem der Ordner das letzte mal geändert wurde	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.6] genügen. Der XDS Document Service MUSS den Wert automatisch gemäß [IHE-ITI-TF2b#3.42.4.1.3.6] aktuell halten. Zudem MUSS der XDS Document Service den Wert aktualisieren, wenn ein Dokument aus dem Ordner gelöscht oder dessen Metadaten aktualisiert wurden.
limitedMetadata	Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt					

	werden.					
patientId	n/ a	n/ a	1. .1	n/ a	Patienten ID, zu der der Ordner gehört.	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.
title	n/ a	n/ a	1. .1	n/ a	Titel des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.8] genügen. Der Wert MUSS redundant gefüllt werden mit Folder.Codelist.Code.displayName.
uniqueId	n/ a	n/ a	1. .1	n/ a	Eindeutige, aktenweite Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.9] genügen.

5061
5062**Tabelle 32: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language Codes**

Language / Country Code Kombination	Language / Country Code Kombination
bg-BG(bulgarisch, Bulgarien)	it-IT(italienisch, Italien) it-CH (italienisch, Schweiz)
cs-CZ(tschechisch, Tschechien)	lt-LT(litauisch, Litauen)
da-DK(dänisch, Dänemark)	lb-LU(luxemburgisch, Luxemburg)
de-AT(deutsch, Österreich) de-DE (deutsch, Deutschland) de-CH (deutsch, Schweiz) de-LI (deutsch, Liechtenstein) de-LU (deutsch, Luxemburg)	lv-LV(lettisch, Lettland)
el-GR(griechisch, Griechenland)	mt-MT(maltesisch, Malta)
en-GB(englisch, Vereinigtes Königreich)	nl-NL(niederländisch, Niederlande) nl-BE (niederländisch, Belgien)
es-ES(spanisch, Spanien)	no-NO(norwegisch, Norwegen)
et-EE(estnisch, Estland)	pl-PL(polnisch, Polen)
fi-FI(finnisch, Finnland)	pt-PT(portugiesisch, Portugal)

fr-FR(französisch, Frankreich) fr-CH (französisch, Schweiz) fr-LU (französisch, Luxemburg) fr-BE (französisch, Belgien)	rm-CH(rätoromanisch, Schweiz)
ga-IE(irisches, Irland)	ro-RO(rumänisch, Rumänien)
hr-HR(kroatisch, Kroatien)	sk-SK(slowakisch, Slowakei)
hu-HU(ungarisch, Ungarn)	sl-SI(slowenisch, Slowenien)
is-IS(isländisch, Island)	sv-SE(schwedisch, Schweden)

5063

5064 [**<=**]5065 *3.13.1.8.2 Metadaten der Dokumente und SubmissionSets*5066 **A_23369-02 -XDS Document Service – Verpflichtender Dokumententitel in DocumentEntry.title**

5067 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
 5068 Dokumenten und dem Ändern von Metadaten an Dokumenten `DocumentEntry.title`
 5069 befüllen. Der Titel des Dokumentes soll eine fachliche Beschreibung des Dokumentes
 5070 enthalten. Bei `DocumentEntry.title` MÜSSEN führende und endende Leerzeichen
 5071 entfernt werden. In `DocumentEntry.title` DARF NICHT leer sein (`!= ""`) (insbesondere
 5072 auch nicht nach etwaigen Entfernen von Leerzeichen vorne und hinten). In
 5073 `Document.title` DÜRFEN keine nicht-druckbaren Zeichen enthalten sein. [**<=**]
 5074

5075 **A_25188 -XDS Document Service - Input Sanitization**

5076 Der XDS Document Service MUSS sicherstellen, dass bei Anlage und Aktualisierung
 5077 (Ändern) von Metadaten:

- 5078 1. führende (leading) und endende (trailing) Whitespace von den Attributen
 5079 automatisch entfernt werden.
- 5080 2. die notwendigen Attribute nichtleer sind (insbeondere auch noch Whitespace-
 5081 Entfernung aus 1.). und
- 5082 3. Die Attribute nur druckbare Zeichen enthalten.

5083 [**<=**]5084 **A_14762-05 -XDS Document Service – Nutzungsvorgabe für authorPerson als Teil von DocumentEntry.author und SubmissionSet.author**

5085 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
 5086 Dokumenten und dem Ändern von Dokumenten-Metadaten an `authorPerson` unterhalb
 5087 von `DocumentEntry.author` und `SubmissionSet.author` neben [IHE-ITI-
 5088 TF3#4.2.3.1.4.2] auch die folgenden Vorgaben beachten.
 5089

5090

5091 **Bei Leistungserbringer als Autor:**

- 5092 1. Lebenslange Identifikationsnummer eines Arztes (Lebenslange Arztnummer -
 5093 LANR 9 Stellen) oder im Falle eines Zahnarztes die Zentrale Zahnarzt Nummer
 5094 (ZANR)- sofern die ZANR bekannt ist
- 5095 2. "^"

- 5096 3. Nachname
- 5097 4. "^"
- 5098 5. Vorname
- 5099 6. "^"
- 5100 7. Weiterer Vorname
- 5101 8. "^"
- 5102 9. Namenszusatz
- 5103 10. "^"
- 5104 11. Titel
- 5105 12. "^^^&" - sofern LANR oder ZANR angegeben, ansonsten "^^^"
- 5106 13. "1.2.276.0.76.4.16" - sofern LANR angegeben oder "1.2.276.0.76.4.296", falls
- 5107 ZANR angegeben
- 5108 14. "&ISO" - sofern LANR oder ZANR angegeben

5109 Beispiele:
 5110 165746304^Weber^Thilo^^^Dr.^^^&1.2.276.0.76.4.16&ISO
 5111 ^Zahnschmerz^Eberhard^^^Dr.^^^

5113 **Bei Versichertem als Autor:**

- 5114 1. Der unveränderbare Teil der KVNR (10 Stellen)
- 5115 2. "^"
- 5116 3. Nachname
- 5117 4. "^"
- 5118 5. Vorname
- 5119 6. "^"
- 5120 7. Weiterer Vorname
- 5121 8. "^"
- 5122 9. Namenszusatz
- 5123 10. "^"
- 5124 11. Titel
- 5125 12. "^^^&"
- 5126 13. "1.2.276.0.76.4.8"
- 5127 14. "&ISO"

5128 Beispiel: G995030566^Gundlach^Monika^^^^^^&1.2.276.0.76.4.8&ISO
 5129 Sowohl beim LE als auch beim Versicherten müssen Vorname und Nachname belegt
 5130 werden.

5132 **Software-Komponente bzw. Gerät als Autor**

5133 Beim (automatisierten) Einstellen von Dokumenten MUSS der max. 256-Zeichen lange
 5134 Name der Software-Komponente bzw. des Geräts als Nachname und ggf. als Vorname(n)
 5135 eingetragen werden.

5136 Beispiel: ^PHR-Gerät-XY^PHR-Software-XY

5137 Im Falle einer DiGA MUSS das Feld Autor folgendermaßen aufgebaut sein:

- 5138 1. Telematik-ID der DiGA
- 5139 2. "^"
- 5140 3. Name der DiGA (Name der Verordnungseinheit)
- 5141 4. "^"
- 5142 5. Name des DiGA-Herstellers
- 5143 6. "^"
- 5144 7. optionale Ergänzung der Bezeichnung der SW
- 5145 8. "^"
- 5146 9. optionale Ergänzung der Bezeichnung der SW
- 5147 10. "^"
- 5148 11. optionale Ergänzung der Bezeichnung der SW
- 5149 12. "^^^&"
- 5150 13. <OID für DiGAs, wie in professionOID>
- 5151 14. "&ISO"

5152 Für alle drei Arten von Autoren (Versicherter, LE, Gerät) MUSS jeweils Vorname und
5153 Nachname angegeben sein. [<=]

5155 **A_14763-03 -XDS Document Service - Nutzungsvorgabe für**
5156 **SubmissionSet.authorInstitution**

5157 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
5158 Dokumenten und dem Ändern von Dokumenten-Metadaten an
5159 SubmissionSet.authorInstitution neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die
5160 folgenden Vorgaben beachten.

- 5161 1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
- 5162 2. "^^^^^&"
- 5163 3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine
5164 Telematik-ID)
- 5165 4. "&ISO^^^^"
- 5166 5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

5167 Beispiele:

- 5168 • Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^^1-2c47sd-
5169 e518
- 5170 • gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^^8-
5171 34923902a

5172 [<=]

5173 **A_21511-01 -Nutzungsvorgabe SubmissionSet.authorInstitution für DIGAs**

5174 Der XDS Document Service MUSS sicherstellen, dass DiGAs beim Upload von
5175 Dokumenten, die folgenden Nutzungsvorgaben für das Metadatenattribut
5176 DocumentEntry.authorInstitution sowie SubmissionSet.authorInstitution berücksichtigen.

5177 Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.1.4.1] genügen und ist inhaltlich
5178 nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen.

- 5179 1. Name des Anbieters der DiGA
- 5180 2. "^^^^^&"
- 5181 3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine
5182 Telematik-ID)
- 5183 4. "&ISO^^^^"
- 5184 5. Telematik-ID der DiGA

5185 [**<=**]

5186 **A_21209-02 -XDS Document Service - Nutzungsvorgabe für** 5187 **DocumentEntry.authorInstitution**

5188 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
5189 Dokumenten und dem Ändern von Dokumenten-Metadaten an
5190 `DocumentEntry.authorInstitution` neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die
5191 folgenden Vorgaben beachten.

- 5192 1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
- 5193 2. "^^^^^&"
- 5194 3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine
5195 Telematik-ID)
- 5196 4. "&ISO^^^^"
- 5197 5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

5198 Die Komponenten 2.-5. sind nur anzugeben, wenn die Telematik ID (5.) der
5199 Autoreninstitution bekannt ist oder ad-hoc ermittelt werden kann, bspw. über den
5200 Verzeichnisdienst der TI-Plattform (VZD). Ansonsten wird ausschließlich der Name
5201 gesetzt.

5202 Beispiele:

- 5203 • Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-
5204 e518
- 5205 • gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^8-
5206 34923902a
- 5207 • Arztpraxis Dr. Wiebke Werner

5208 [**<=**]

5209 **A_22408-02 -XDS Document Service - DocumentEntry.authorInstitution ohne** 5210 **Telematik-ID**

5211 Der XDS Document Service MUSS Nachrichten zum Registrieren von Dokumenten bei
5212 fehlender Telematik-ID in `DocumentEntry.authorInstitution` akzeptieren und
5213 daraufhin alle Zeichen hinter dem Namen der `authorInstitution` abschneiden und
5214 verwerfen.[**<=**]

5215 **A_14974-02 -XDS Document Service - Nutzungsvorgabe für** 5216 **DocumentEntry.patientId und SubmissionSet.patientId**

5217 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
5218 Dokumenten und dem Ändern von Dokumenten-Metadaten die folgenden
5219 Nutzungsvorgaben für `DocumentEntry.patientId` und `SubmissionSet.patientId`
5220 berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.2.16] bzw. [IHE-

- 5221 ITI-TF3#4.2.3.3.8] genügen und ist inhaltlich nach der folgenden Vorschrift
 5222 zusammenzufügen bzw. zu belegen:
- 5223 1. Der unveränderbare Teil der KVNR des Akteninhabers (10 Stellen)
 - 5224 2. "^^^&"
 - 5225 3. "1.2.276.0.76.4.8" (OID zur Kennzeichnung einer unveränderbaren KVNR)
 - 5226 4. "&ISO"

5227 Beispiel: G995030566^^^1.2.276.0.76.4.8&ISO[<=]

5228 **A_27759 -XDS Document Service - Verarbeitung von Code System Version**

5229 Der XDS Document Service MUSS Metadaten vom Typ Coded Attribute im Slot
 5230 "codingScheme" bei Angabe einer System URL oder Canonical URL eine per Pipe-Symbol
 5231 (|) angehängte Version akzeptieren und für eine Terminologievalidierung
 5232 verwenden.[<=]

5233 Beispiel: <http://dvmd.de/fhir/CodeSystem/kdl|2025>

5234 *3.13.1.8.3 Metadaten für Datenkategorien*

5235 **A_19388-21 -Nutzungsvorgaben für die Verwendung von Datenkategorien**

5236 Der XDS Document Service MUSS beim Einstellen eines Dokuments und beim Ändern von
 5237 Metadaten die folgende Zuordnung zu einer Datenkategorie (d. h. Assoziierung mit einem
 5238 bestimmten Folder) vornehmen. Dabei haben Auswertungs- und Zuordnungsregeln, die
 5239 sich aus A_14761-* und damit verbunden aus [gemSpec_IG_ePA] ableiten, immer den
 5240 Vorrang gegenüber anderen Auswertungsregeln. Ferner MUSS der XDS Document
 5241 Service sicherstellen, dass bei einer Aktualisierung eines Dokuments derselbe Ordner des
 5242 zu ersetzenden Dokuments zugeordnet wird.

5243 Für eine eindeutige Zuordnung zu einer Datenkategorie MUSS die Auswertung der
 5244 Metadatenvorgaben in der Reihenfolge der folgend dargestellten Einsortierungskriterien
 5245 erfolgen:

5247 **Tabelle 33: Einsortierung_Datenkategorien**

Datenkategorie/Technischer Identifier/Foldercode	Einsortierkriterium (anzuwenden auf DocumentEntry, wenn nicht anders angegeben. Oder-Verknüpfungen, wenn nicht "und" angegeben)
receipt	healthcareFacilityTypeCode = VER und typeCode = ABRE und DocumentEntry.authorRole=105 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 = <ul style="list-style-type: none"> • ED110102 (KDL-Code Notfalldatenmanagement (NFDM)) • AU190104 (KDL-Code Notfalldatensatz) • AD020105 (KDL-Code Notfall-/Vertretungsschein)
transcripts	eventCodeList = <ul style="list-style-type: none"> • UB999997 (KDL-Code Gesamtdokumentation stationäre Versorgung) oder • UB999998 (KDL-Code Gesamtdokumentation ambulante Versorgung)
reports	classCode = ANF, ASM, BEF, BIL, DOK, DUR, LAB oder PLA
other	Alle Dokumente, die in keine andere Kategorien eingeordnet werden können

5248 *Falls Basiskonzepte angegeben werden, dann gelten automatisch alle Subkonzepte, z.B.
5249 gilt für die Kategorie "care" die Einsortierregel bei PracticeSettingCode = PFL wie auch für
5250 die Sub-Konzepte ALT (Altenpflege) und KIN (Kinderpflege).[<=]

5251 3.13.1.8.4 Automatisches Umschreiben von Daten

5252 Dieser Abschnitt enthält Vorgaben für Datenanpassungen, die für bestehende Daten im
5253 XDS Document Service vorgenommen werden müssen (z. B. wenn sie durch Änderungen
5254 im Rahmen einer neuen Version des XDS Document Service notwendig werden).

5255 **A_27482-01 -XDS Document Service – Metadatenkorrektur bei vorhandenen** 5256 **elektronischen Arztbriefen**

5257 Der XDS Document Service MUSS die Metadaten (DocumentEntry) von bestehenden
5258 Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief)
5259 gemäß [gemSpec_IG_ePA] derartig anpassen, dass DocumentEntry.eventCodeList
5260 zusätzlich um den KDL-Code (code: ED110104, codeSystem: 1.2.276.0.76.5.552,
5261 displayName: eArztbrief) erweitert wird, wenn dieser nicht bereits vorhanden ist.[<=]

5262 **A_27661 -XDS Document Service – Umwandeln von APND-Assoziationen**

- 5263 Der XDS Document Service MUSS sobald möglich Associations vom Typ
 5264 "urn:ihe:iti:2007:AssociationType:APND" wie folgt ersetzen:
- 5265 1. Wenn ein Association.sourceObject oder Association.targetObject auf ein
 5266 DocumentEntry im Status "deprecated" zeigt, oder auf einen DocumentEntry, der
 5267 zu einer Sammlung (mixed oder uniform) gehört, wird nur Schritt 4 durchgeführt
 5268 (Association wird gelöscht), ansonsten weiter bei Schritt 2.
 - 5269 2. Der DocumentEntry, auf den Association.sourceObject zeigt (der "Anhang"), MUSS
 5270 in DocumentEntry.referenceIdList mit dem
 5271 mittels `urn:gematik:iti:xds:2025:parentDocument` ausgezeichneten Wert der
 5272 DocumentEntry.uniqueId desjenigen Dokuments ergänzt werden, auf das
 5273 Association.targetObject zeigt.
 - 5274 3. Der DocumentEntry, auf den Association.targetObject zeigt (der
 5275 "Hauptdokument"), MUSS in DocumentEntry.referenceIdList mit dem mittels
 5276 `urn:gematik:iti:xds:2025:childDocument` ausgezeichneten Wert der
 5277 DocumentEntry.uniqueId desjenigen Dokuments ergänzt werden, auf das
 5278 Association.sourceObject zeigt.
 - 5279 4. Anschließend ist die APND-Association zu löschen.

5280 [`<=`]

5281 APND-Associations werden mit ePA Version 3.1.2 durch einen Anhangsmechanismus
 5282 mittels DocumentEntry.referenceIdList abgelöst. Beim automatischen Umschreiben der
 5283 APND-Associations auf die DocumentEntry.referenceIdList können Anhangsketten
 5284 entstehen, die länger als insgesamt fünf Dokumente sind. Das ist über das Einstellen von
 5285 Dokumenten über Provide and Register Document Set [ITI-41] oder Restricted Update
 5286 Document Set [ITI-92] nicht möglich. Entsprechend lange Ketten können also nur aus
 5287 der Anpassung von Altdaten entstehen.

5288 Wie aus A_27661 hervorgeht, werden Anhänge von "deprecated"-Dokumenten (d.h.
 5289 durch Ersetzen via RPLC-Association durch neue Versionen ersetzte Dokumente)
 5290 abgetrennt. Das ist notwendig, da die identischen Metadateneinträge der Dokumente in
 5291 der RPLC-Dokumentenkette bei jedem Dokument zwangsläufig auf identische Anhänge
 5292 zeigen müssen. Das kleinere Übel ist hier, die Anhänge für die aktuellste Version
 5293 zumindest intakt zu halten. Neue Ersetzungen in Verbindung mit Anhängen verhindert
 5294 das Aktensystem ab Version 3.1.2, da die Menge an RPLC-fähigen Dokumenten und die
 5295 Dokumente, die Anhangsbeziehungen eingehen können, disjunkt spezifiziert sind.

5296 3.13.1.9 Strukturierte Dokumente

5297 Die elektronische Patientenakte unterstützt unterschiedliche sogenannte "strukturierte
 5298 Dokumente", deren Aufbau über Implementation Guides genau vorgegeben ist. Der
 5299 Umfang der unterstützten strukturierten Dokumente wird durch den Umfang der
 5300 veröffentlichten Implementation Guides festgelegt (3.13.1.9.2- Konfigurierbarkeit). Für
 5301 alle strukturierten Dokumente gelten spezifische Metadatenvorgaben, um sie eindeutig zu
 5302 identifizieren und gezielt verarbeiten zu können.

5303 **A_14761-08 -Nutzungsvorgaben für die Verwendung von IHE ITI XDS- 5304 Metadaten bei strukturierten Dokumenten**

5305 Der XDS Document Service MUSS die Nutzungsvorgaben für strukturierte Dokumente
 5306 unter [gemSpec_IG_ePA] berücksichtigen. Dabei ist das Format des Dokuments, welches
 5307 über einen Code des Metadatenattributs `formatCode` ausgedrückt wird, führend. Das
 5308 bedeutet, bei Registrierung eines strukturierten Dokuments mit einem `formatCode`
 5309 MÜSSEN die weiteren Metadatenattribute `classCode`, `typeCode`, `mimeType` sowie
 5310 `eventCodeList` entsprechend belegt werden. Der XDS Document Service MUSS eine

5311 solche Registrierung diesbzgl. prüfen und im Fehlerfall analog zu A_14938-*
 5312 antworten.[<=]

5313 3.13.1.9.1 Sammlungstypen

5314 Je nach Art ihrer Zusammensetzung und ihrer Handhabung existieren unterschiedliche
 5315 Typen strukturierter Dokumente, sogenannte medizinische Informationsobjekte. Ein
 5316 medizinisches Informationsobjekt (MIO) ist eine **Sammlung** von Informationen zu
 5317 medizinischen, strukturellen oder administrativen Sachverhalten, die in sich geschlossen
 5318 oder entsprechend verschachtelt vorliegt. Zudem ist ein MIO eine klar definierte Vorgabe,
 5319 wie diese Informationssammlung in der elektronischen Patientenakte gespeichert wird,
 5320 damit semantische und syntaktische Interoperabilität gewährleistet werden. Die
 5321 Festlegung dieser Vorgaben ist gemäß SGB V Aufgabe der KBV. Beispiele für
 5322 medizinische Informationsobjekte sind der Impfpass, das Kinderuntersuchungsheft, der
 5323 Mutterpass, das zahnärztliche Bonusheft, oder DiGA. MIOs werden über Sammlungen
 5324 und Sammlungstypen umgesetzt.

5325 Einige strukturierte Dokumente sind für sich genommen vollständig und schlüssig wie z.
 5326 B. ein Elektronischer Arztbrief. Sie sind ohne Zuhilfenahme weiterer Dokumente in der
 5327 ePA für einen Benutzer sinnvoll zu verwenden. Andere Typen strukturierter Dokumente
 5328 müssen hingegen fast immer in Kombination betrachtet werden, z. B.
 5329 Impfpassdokumente. Bei letzteren spiegelt jedes Impfpassdokument ein oder mehrere
 5330 Impfungen wieder. Ein Impfpass, wie er in der analogen Welt geläufig und als logisches
 5331 Konstrukt sinnvoll ist, besteht immer aus der gemeinsamen Betrachtung
 5332 aller Impfpassdokumente und somit aller vorhandenen Impfeinträge. Die Kombination ein
 5333 oder mehrerer strukturierter Dokumente ergeben eine Sammlung.

5334 Eine Sammlungsinstanz (z. B. der Mutterpass der ersten Schwangerschaft der Patientin
 5335 Martha Mustermann) ist eine konkrete Ausprägung der Information, die zwischen den
 5336 beteiligten Akteuren ausgetauscht wird. Nicht jede Sammlung besteht zwangsläufig aus
 5337 Dokumenten desselben Formats: Ein Kinderuntersuchungsheft beispielsweise besteht aus
 5338 Dokumenten mit drei verschiedenen strukturierten Dokumenttypen. Zentral für alle
 5339 Sammlungstypen ist immer mindestens ein strukturiertes Dokument mit einem
 5340 festgelegten Dokumentenformat. Für eine technische Umsetzung sind die
 5341 Sammlungstypen "mixed" und "uniform" zu unterscheiden, die technisch unterschiedlich
 5342 umgesetzt werden und zum Teil unterschiedliche Operationen erlauben.

5343 Der Sammlungstyp "mixed" fasst semantisch zusammengehörige, strukturierte
 5344 Dokumente unterschiedlicher Struktur mittels Ordner zu einer Sammlung zusammen. Der
 5345 Sammlungstyp "uniform" wird ebenfalls intern über Ordner abgebildet. Dies stellt sicher,
 5346 dass zukünftige Versionen dieser strukturierten Dokumente/Pässe oder DiGA verlässlich
 5347 verarbeitet werden können. Ordner gelten als "statische Ordner", bis auf Sammlungen
 5348 der Kategorie Mutterpass und DiGA ("dynamische Ordner"). Der dynamische Ordner für
 5349 einen konkreten Mutterpass wird durch den Client angelegt, weil es aus Gründen, die nur
 5350 der Client kennt (Anzahl der Schwangerschaften), mehrere Ordner dieses Typs geben
 5351 kann ("nicht-statische Ordner", vgl. A_21610-*). Die Version der Struktur eines
 5352 Dokuments ist am Format Code erkennbar.

5353 **A_20577-06 -Definition und Zuweisung von Sammlungstypen**

5354 Der XDS Document Service MUSS jeder Sammlung einen von zwei Sammlungstypen
 5355 zuweisen:

5356 **Tabelle 34: TAB_EPA_Sammlungstypen**

Sammlungstyp	Definition
--------------	------------

mixed	Ordner, die einer Sammlung des Typs "mixed" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) mit einem für die Sammlung festgelegten Code in der Folder.codeList abgelegt werden.
uniform	Ordner, die einer Sammlung des Typs "uniform" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) abgelegt werden.

5357
5358 Es gelten die Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA]. In den
5359 unter [gemSpec_IG_ePA] gemachten Vorgaben werden auch Ordner-Kardinalitäten für
5360 spezifische Sammlungen festgelegt. Diese Angaben sagen aus, wie viele Instanzen einer
5361 Sammlung (d. h. minimal und maximal) registriert werden können. [\leq]

5362 **A_20707-04 -XDS Document Service – Keine unpassenden Dokumente in nicht-** 5363 **statische Ordner**

5364 Falls das Dokument nicht den Vorgaben der Metadaten für strukturierte Dokumente
5365 gemäß [gemSpec_IG_ePA] entspricht, MUSS der XDS Document Service das Registrieren
5366 und Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-
5367 Fehlercode `BadFolderAssociation` quittieren. Es MUSS im `codeContext`-Attribut
5368 des zurückgegebenen `rs:RegistryError`-Elements die UUID (DocumentEntry.entryUUID)
5369 des identifizierten Dokuments angegeben werden. [\leq]

5370 **A_20581-06 -XDS Document Service – Löschen von Dokumenten aus** 5371 **Sammlungen der Typen "mixed" und "uniform" durch ein ePA-FdV**

5372 Der XDS Document Service MUSS beim Löschen eines Dokuments der Sammlungstypen
5373 "mixed" und "uniform" durch das ePA-FdV sicherstellen, dass die Operation mit dem
5374 Fehler `ReferencesExistException` abgebrochen wird, wenn die Löschanfrage nicht alle
5375 Dokumente der Sammlung enthält. Es besteht folgende Ausnahme: Das Löschen einer
5376 Elternnotiz im Kinderuntersuchungsheft ist erlaubt. [\leq]

5377 Nur Leistungserbringern ist es erlaubt, einzelne Dokumente aus Sammlungen der Typen
5378 "mixed" und "uniform" zu löschen, um die medizinische Interpretation der gesamten
5379 Sammlungsinstanz nicht zu gefährden.

5380 *Hinweis: Die zeitliche Gültigkeit ergibt sich aus den Attributen "validFrom" und (optional)*
5381 *"clientReadOnlyFromDate" der Vorgaben in [gemSpec_IG_ePA].*

5382 **3.13.1.9.2 Konfigurierbarkeit**

5383 **A_17546-02 -Konfigurierbarkeit von strukturierten Dokumenten**

5384 Der XDS Document Service MUSS die Liste strukturierter Dokumente konfigurierbar
5385 machen, indem dieser die Unterstützung strukturierter Dokumente unter Angabe
5386 folgender Eigenschaften ermöglicht:

- 5387 • Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA]
5388 konfigurativ hinzufügen bzw. entfernen,
- 5389 • Sammlungen zu TAB_EPA_Sammlungstypen
5390 gemäß [gemSpec_IG_ePA] konfigurativ hinzufügen bzw. entfernen.

5391 [\leq]

5392 Das Entfernen der Unterstützung von strukturierten Dokumenten oder
5393 Sammlungen bedeutet, dass diese zu einem früheren Zeitpunkt in das Aktensystem

5394 geschrieben werden konnten, aber durch Erreichen von "clientReadOnlyFromDate" nicht
5395 mehr geschrieben werden dürfen. Das Schreiben umfasst das Aktualisieren oder neu
5396 Anlegen. Das Lesen ist weiterhin erlaubt.

5397 **A_17551-01 -Prüfanforderungen zur Konfigurierbarkeit von Value Sets**

5398 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die zu konfigurierenden
5399 Value Sets des XDS Document Service gemäß der Anforderung A_17546-* den
5400 folgenden Prüfkriterien unterliegen, bevor bestehende, im XDS Document Service
5401 verarbeitete Value Sets verändert werden:

- 5402 • Es DÜRFEN KEINE Codes der Value Sets gelöscht werden, lediglich das Hinzufügen
5403 von Codes zu existierenden Value Sets ist aus Kompatibilitätsgründen erlaubt.
- 5404 • Neue Codes MÜSSEN den Formatvorgaben gemäß Tabelle 4.2.3.1.7-2 in [IHE-ITI-
5405 TF3#4.2.3.1.7] entsprechen und gegenüber einer internen Referenzliste validiert
5406 werden. Dies schließt auch Prüfungen zur Zeichenkodierung, der Datentypen als
5407 auch zu den Längenbeschränkungen ein.

5408 [**<=**]

5409 **A_21212-01 -Restriktionen zur Konfigurierbarkeit von Metadaten für**
5410 **strukturierte Dokumente und Sammlungen**

5411 Der XDS Document Service MUSS durch technische Maßnahmen sicherstellen, dass
5412 Änderungen an den in den Implementierungsvorgaben in [gemSpec_IG_ePA]
5413 spezifizierten Codes ausgeschlossen sind. [**<=**]

5414 **A_21214-03 -Konfiguration strukturierter Dokumente im Rahmen der**
5415 **Veröffentlichung durch die gematik**

5416 Der Anbieter des ePA-Aktensystems MUSS durch organisatorische Maßnahmen
5417 sicherstellen, dass die Konfiguration im Aktensystem zur Unterstützung strukturierter
5418 Dokumente aus [gemSpec_IG_ePA] ausschließlich im Rahmen der Veröffentlichung der
5419 Implementation Guides durch die gematik erfolgt. [**<=**]

5420 Bei Einführung neuer strukturierter Dokumente werden die beschriebenen
5421 Konfigurationsmöglichkeiten so verwendet, dass eine Erweiterung der Spezifikation und
5422 daraus resultierend eine Änderung des ePA-Aktensystems mit erneuter Zulassung nicht
5423 erforderlich sind.

5424 *3.13.1.9.3 Verarbeitungsvorgaben für spezifische Dokumente*

5425 **A_27686 -Einstellen des eArztbriefs mit Dokumentenanhängen**

5426 Der XDS Document Service MUSS beim Einstellen eines eArztbriefs (gemäßig-eab.json in
5427 [gemSpec_IG_ePA]) sicherstellen,

- 5428 • dass alle zusätzlich in der Anfrage enthaltenen Dokumente mit dem enthaltenen
5429 eArztbrief-Dokument über die Kennzeichnung als Anhang verbunden
5430 werden (urn:gematik:iti:xds:2025:childDocument/parentDocument),
- 5431 • dass kein Dokument (via urn:gematik:iti:xds:2025:parentDocument) auf ein
5432 Elterndokument referenziert, dass nicht der eArztbrief selbst ist.

5433 und ansonsten die Verarbeitung mit dem Fehler XDSInvalidAttachmentHierarchy
5434 abbrechen.

5435 [**<=**]

5436 Unter anderem müssen also die Anhänge immer direkt unter den Arztbrief "gehängt"
5437 werden; ein "Anhang am Anhang" ist nicht erlaubt.

5438 **A_27765 -Nachträgliches Anhängen an einen eArztbrief**

5439 Der XDS Document Service MUSS ein Anhängen von Dokumenten an einen eArztbrief
5440 (gemäßig-eab.json in [gemSpec_IG_ePA]) mit dem Fehler `XDSAttachmentForbidden`
5441 ablehnen, wenn die Anhangsbeziehung nicht mit demselben SubmissionSet hergestellt
5442 wird, mit dem der eArztbrief eingestellt wird.

5443 [`<=`]

5444 Hierdurch wird ein nachträgliches Anhängen von Dokumenten an einen bestehenden
5445 Arztbrief über die Operationen Provide and Register Document Set-b oder Restricted
5446 Update Document Set unterbunden.

5447 **A_27758 -XDS Document Service - Metadatenerweiterung bei neuen** 5448 **elektronischen Arztbriefen**

5449 Der XDS Document Service MUSS die Metadaten (DocumentEntry) von neuen
5450 Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief)
5451 gemäß [gemSpec_IG_ePA] derartig anpassen, dass DocumentEntry.eventCodeList
5452 zusätzlich um den aktuellen KDL-Code nach [IG_TI_Terminology] mit den Werten

- 5453 • code: ED110104,
- 5454 • codeSystem: [http://dvmd.de/fhir/CodeSystem/kdl|\[version\]](http://dvmd.de/fhir/CodeSystem/kdl|[version]) (präferiert) oder die
5455 entsprechende OID,
- 5456 • displayName: eArztbriefablehnen

5457 erweitert wird, wenn dieser nicht bereits vorhanden ist.

5458 [`<=`]

5459 Dabei muss bei obiger Anforderung "[version]" mit der aktuellen Version der KDL belegt
5460 werden, z.B.:

5461 **Canonical URL für Version 2025**

5462 <http://dvmd.de/fhir/CodeSystem/kdl|2025>

5463 **OID für Version 2025**

5464 1.2.276.0.76.5.553

5465 **3.13.1.10 Verbergen von Dokumenten durch Verwendung des** 5466 **confidentialityCode**

5467 Der Versicherte oder ein Vertreter kann vorhandene Dokumente des Aktenkontos durch
5468 die Verwendung der General Deny Policy des Constraint Managements verbergen oder
5469 sichtbar machen.

5470 Der Versicherte oder ein Vertreter kann ein neues Dokument auch direkt beim Einstellen
5471 in das Aktenkonto verbergen. Dazu wird durch den XDS Document Service beim
5472 Einstellen bzw. Aktualisieren (Replace) eines Dokuments der
5473 DocumentEntry.confidentialityCode der Dokumentmetadaten ausgewertet. Enthält der
5474 confidentialityCode beim Einstellen bzw. Aktualisieren den Wert "CON" (constraint), wird
5475 durch das Aktensystem ein Eintrag in der General Deny Policy erzeugt und das Dokument
5476 verborgen.

5477 Diese zusätzliche Art des direkten Verbergens ist dabei grundsätzlich nur auf
5478 Dokumententypen anwendbar, welche durch einen Versicherten oder einen Vertreter
5479 über ein ePA-FdV eingestellt werden können (keine MIOs oder strukturierten
5480 Dokumente).

5481 Das Metadatum DocumentEntry.confidentialityCode = "CON" (codeSystem =
5482 urn:oid:1.2.276.0.76.5.491:

- 5483 1. Führt beim Einstellen und Replace eines Dokuments zum Verbergen des
5484 Dokuments, d.h. das Dokument wird auf die General Deny Policy des Aktenkontos
5485 gesetzt.
- 5486 2. Wird im Aktensystem nicht persistiert sondern über dort intern über eine General
5487 Deny Policy umgesetzt.
- 5488 3. Wird im ePA-FdV nicht zur Anzeige gebracht und kann dort auch nicht geändert
5489 werden.
- 5490 4. Eine LEI darf DocumentEntry.confidentialityCode = "CON" nicht verwenden.

5491 3.13.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf 5492 die Dokumente des Aktenkontos

5493 Wird ein Widerspruch gegen die Nutzung einer Funktion der ePA erklärt, verhindert der
5494 XDS Document Service, abhängig von der jeweils widersprochenen Funktion, deren
5495 weitere Nutzung.

5496 Im Falle eines Widerspruchs gilt:

5497 **Tabelle 35: Auswirkungen bei Widerspruch gegen eine Funktion der ePA**

widerspruchsfähige Funktion	Auswirkung bei erteiltem Widerspruch
Teilnahme am digital gestützten Medikationsprozess ("medication")	Das Einstellen, Verändern, Lesen oder Suchen von Dokumenten des Ordners "emp" (elektronischer Medikationsplan) wird durch den XDS Document Service abgelehnt. Ausgenommen hiervon sind der Versicherte und befugte Vertreter.
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst ("erp-submission")	Alle vorhandenen Dokumente des Ordners "emp" (elektronischer Medikationsplan) werden gelöscht.

5498 *Hinweis zum Medikationsprozess: Dadurch wird verhindert, dass Leistungserbringer im*
5499 *Versorgungsprozess veraltete oder unvollständige Daten verwenden.*

5500 **A_23860 -XDS Document Service - Löschen der Dokumente des** 5501 **Medikationsprozesses**

5502 Der XDS Document Service des Aktensystems MUSS alle Dokumente aus dem Ordner
5503 elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code =
5504 "eMP") löschen, wenn der Status der widerspruchsfähigen Funktion "Einstellen von
5505 Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst" (Id ==
5506 "erp-submission") auf "Widerspruch erklärt" ("deny") geändert wird. [**<=**]

5507 **A_23895-02 -XDS Document Service - Keine Operationen mit Dokumenten des** 5508 **Medikationsprozesses bei Widerspruch**

5509 Falls ein Widerspruch zur widerspruchsfähigen Funktion "Teilnahme am
5510 Medikationsprozess" (Id ="medication" und status ="deny") vorliegt, MUSS der XDS
5511 Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von
5512 Dokumenten des Ordners elektronischer Medikationsplan (codeSystem =
5513 "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für alle Nutzer, ausgenommen der
5514 Versicherte oder befugte Vertreter (oid_versicherter), ablehnen und die Operation mit
5515 dem Fehlercode ConsentDecisionViolation abrechnen.

5516 [**<=**]

A_25151-01 -XDS Document Service – Prüfung der Widersprüche bei Suchanfrage

Der XDS Document Service MUSS bei einer Suchanfrage die Suchergebnismenge für alle Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid_versicherter), filtern und sicherstellen, dass diese keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält, wenn ein Widerspruch gegen die widerspruchsfähige Funktion "Teilnahme am digital gestützten Medikationsprozess" (Id ="medication" und status ="deny") vorliegt.

[<=]

3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI auf die Dokumente des Aktenkontos

Wird ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI erklärt, verhindert der XDS Document Service, dass auf die Dokumente der Kategorie "emp" zugegriffen werden kann.

A_26429 -XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für diese LEI, ablehnen und die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.

[<=]

A_26430 -XDS Document Service – Prüfung des Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI bei Suchanfrage

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service bei einer Suchanfrage die Suchergebnismenge für diese LEI filtern und sicherstellen, dass die Suchergebnismenge keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält.

[<=]

3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service**A_24715-02 -XDS Document Service - Protokolleinträge für Zugriffe auf den XDS Document Service**

Der XDS Document Service MUSS für die Operationen

- ProvideAndRegisterDocumentSet-b,
- RetrieveDocumentSet,
- RemoveMetadata,
- RestrictedUpdateDocumentSet,
- RegistryStoredQuery (entfällt, wenn Nutzung durch den Versicherten erfolgt)

Protokolleinträge gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

5562 **Tabelle 36: XDS Document Service Protokollierung**

Strukturelement	Wert	Erläuterung	
AuditEvent.type	"document"		
AuditEvent.action	C	Für ProvideAndRegisterDocumentSet-b ohne Replace Option	
	U	Für ProvideAndRegisterDocumentSet-b mit Replace Option	
	U	Für RestrictedUpdateDocumentSet	
	R	Für RegistryStoredQuery	
	R	Für RetrieveDocumentSet	
	D	Für Zugriffe mit RemoveMetadata	
AuditEvent.entity.name	"XDS Document Service"	Service Name	
AuditEvent.entity.description	<Operation>	ein Wert aus {ProvideAndRegisterDocumentSet-b, RetrieveDocumentSet, RemoveMetadata, RestrictedUpdateDocumentSet, RegistryStoredQuery}	
Parameterwerte für die Operationen ProvideAndRegisterDocumentSet-b, RetrieveDocumentSet und RemoveMetadata			
AuditEvent.entity.detail	type	value[x]	
	"DocumentFormatCode"	<DocumentEntry.formatCode>	wenn in der entity Struktur ein XDSDocument beschrieben wird. kodiert als Datentyp „Coded String“ gemäß [IHE-ITI- TF3]. Wenn es sich beim Wert von DocumentEntry.formatCode um den Code urn:ihe:iti:xds:2017:mimeTypeSufficient (Code System 1.3.6.1.4.1.19376.1.2.3) handelt, MUSS stattdessen der Wert von DocumentEntry.mimeType hier eingetragen werden.
	"DocumentUniqueId"	<Document.uniqueId>	wenn in der entity Struktur ein XDSDocument beschrieben wird
	"DocumentEntryTitle"	<DocumentEntry.title>	wenn in der entity Struktur ein XDSDocument beschrieben wird

	"FolderTitle"	<Folder.title>	wenn in der entity Struktur ein XDSFolder beschrieben wird
	"FolderCodeList"	<Folder.codeList>	wenn in der entity Struktur ein XDSFolder beschrieben wird kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3] z.B. "pregnancy_childbirth^^^&1.2.276.0.76.5.512&ISO"
	"FolderEntryUID"	<Folder.entryUUID>	wenn in der entity Struktur ein XDSFolder beschrieben wird

Parameterwerte für die Operation RegistryStoredQuery der Schnittstellen I_Document_Management und I_Document_Management_Insurant (nur Vertreter)

AuditEvent.entity.detail	type	value[x]	
	"Query Id"	<Parameter Query ID>	Der Wert MUSS der Parameter Query ID gemäß [IHE-ITI-TF2] #3.18.4.1.2.4 und für das Aktensystem definierten Anfragetypen entsprechen.

Parameterwerte für die Operation RestrictedUpdateDocumentSet

Alle Metadaten, die **geändert** wurden, sind mit altem und neuem Wert mit den Parameternamen AuditEvent.entity.detail.**type** und **.value[x]** zu protokollieren. In A_15083* sind die Metadaten genannt, die geändert werden können. Der Parameter type ist ein Kompositum aus Objekt (Document) + Attribut in Groß/Kleinschreibung. Wird das geänderte Metadatum adressiert, wird noch der Präfix "prev" ergänzt.
z.B. Metadatum: DocumentEntry.formatCode -> Parameter **valuetype**: DocumentFormatCode und prevDocumentFormatCode.
Attributunterstrukturen werden ebenfalls in gemischter Groß/Kleinschreibung zusammengesetzt (z.B. author.Person -> AuthorPerson).

5563 [**<=**]

5564 *Hinweis: In der AuditEvent.entity Struktur sind Dokumente und/oder Folder zu*
5565 *berücksichtigen, die in der zu protokollierenden Operation referenziert werden.*

5566 **A_24925 -XDS Document Service - Protokolleinträge für Zugriffe gleicher Art**

5567 Werden mehrere XDS Dokumente bzw Folder in der zu protokollierenden Operation
5568 referenziert und die Zugriffe sind gleicher Art (AuditEvent.action) KANN der XDS
5569 Document Service einen Protokolleintrag erzeugen, der mehreren AuditEvent.entity
5570 Strukturen enthält. [**<=**]

5571 Das bedeutet, wenn in einer ProvideAndRegisterDocumentSet-b Operation zehn
5572 Dokumente eingestellt werden, kann für diesen Zugriff ein AuditEvent mit zehn Entity
5573 Strukturen erzeugt werden. Werden zehn Dokumente eingestellt und das zehnte
5574 Dokument ersetzt ein bereits vorhandenes, kann in einem Protokolleintrag das Einstellen
5575 (Create) mit neun Entity Strukturen dokumentiert und muss in einem weiteren
5576 Protokolleintrag ein Ersetzen (Update) (zehnte Dokument) protokolliert werden.

5577 **A_25007 -XDS Document Service - Nicht zu protokollierende Zugriffe**

5578 Werden mit der Operation RestrictedUpdateDocumentSet keine geänderten Metadaten
5579 eines referenzierten DocumentEntry gesendet, d.h. die gesendeten Metadateninhalte
5580 unterscheiden sich nicht von bereits persistierten Werten, DARF der XDS Document
5581 Service diesen Zugriff NICHT protokollieren.[<=]

5582 **A_27253-01 -XDS Document Service - Nicht zu protokollierende Zugriffe auf**
5583 **Ordner "technical"**

5584 Der XDS Document Service DARF Zugriffe auf den statischen Ordner "technical" oder
5585 dessen Inhalte NICHT protokollieren.[<=]

5586 **A_27254-01 -XDS Document Service - Protokollierung von Nutzerzugriffen auf**
5587 **den Ordner "technical"**

5588 Der XDS Document Service MUSS Nutzerzugriffe auf den Ordner "technical" dann
5589 protokollieren, wenn durch den Zugriff Dokumente Protokolldokumente einer ePA-2.6
5590 Aktenkontomigration betroffen sind. Diese Protokollierung MUSS gemäß der Vorgaben in
5591 A_24715-* erfolgen.[<=]

5592 **3.13.1.14 Unterstützungsleistung für das ePA-FdV**

5593 Der XDS Document Service akzeptiert aus Sicherheitsgründen nur bestimmte
5594 Dokumentenformate. Das schränkt auch das Format PDF auf bestimmte PDF/A-Varianten
5595 ein (siehe auch A_25233*). Daher müssen PDF-Dokumente des Versicherten unter
5596 Umständen vor dem Einstellen in die ePA konvertiert werden.

5597 Um das ePA-FdV dabei zu entlasten und Komplexität aus dem ePA-FdV zu nehmen, wird
5598 eine Funktion angeboten, durch die ein PDF in ein PDF/A konvertiert werden kann. Das
5599 ePA-FdV muss aber berücksichtigen, dass die Konvertierung ggf. technisch nicht
5600 durchgeführt werden kann oder das Ergebnis der Konvertierung durch ein geändertes
5601 Layout ggf. nicht verwendbar ist.

5602 **A_25456 -XDS Document Service - Keine negativen Auswirkungen auf**
5603 **Folgekonvertierungen von PDF zu PDF/A**

5604 Der XDS Document Service MUSS sicherstellen, dass eine Konvertierung eines PDF-
5605 Dokuments sich nicht schädlich auf folgende Konvertierungen auswirken kann.[<=]

5606 Hinweis zu A_25456*: Die Anforderung soll erreichen, dass ein potentiell über ein PDF-
5607 Dokument eingebrachter Schadcode nach der Konvertierung gelöscht wird, z.B. durch
5608 Zurücksetzen der Sandbox oder der VAU-Instanz

5609 **A_25455 -XDS Document Service - Isolation der Konvertierung von PDF zu**
5610 **PDF/A**

5611 Der XDS Document Service MUSS die Verarbeitung von PDF-Dokumenten, die im
5612 Rahmen der Konvertierung in ein PDF/A durchgeführt wird, in einer separaten VAU-
5613 Instanz durchführen, die ausschließlich eine Verbindung zu einem ePA-FdV besitzen
5614 darf.[<=]

5615 **A_25454 -XDS Document Service - Realisierung der Schnittstelle**
5616 **I_Tool_Convert_PDF_Insurant**

5617 Der XDS Document Service MUSS die Operationen der Schnittstelle
5618 I_Tool_Convert_PDF_Insurant gemäß [I_Tool_Convert_PDF_Insurant] umsetzen[<=]

5619 **A_26129 -ePA-Aktensystem - Rahmenbedingungen bei Nutzung einer Service-**
5620 **VAU für PDF-Konvertierung**

5621 Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV
5622 für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU
5623 verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die vom ePA-
5624 FdV übermittelten PDF-Dokumente in der Aktenkontoverwaltungs-VAU ausschließlich
5625 weitergeleitet aber ansonsten nicht verarbeitet werden. Gleiches gilt für die von der
5626 Service-VAU an das ePA-FdV übermittelten konvertierten PDF/A-Dokumente.[<=]

A_26130 -ePA-Aktensystem - maximale Lebensdauer einer Service-VAU für PDF-Konvertierung

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die Lebensdauer einer solchen Service-VAU-Instanz maximal 12 Stunden beträgt. [\leq]

A_26131 -ePA-Aktensystem - Keine Speicherung von in der Service-VAU für PDF-Konvertierung verarbeiteten Daten

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass weder die vom ePA-FdV übermittelten und zu konvertierenden PDF-Dokumente noch die daraus konvertierten PDF/A-Dokumente von der "PDF-VAU" im ePA-Aktensystem gespeichert werden. [\leq]

A_26121 -ePA-Aktensystem - Keine Verarbeitung von Geräteinformationen

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass keine Geräteinformationen (Device Management) von Nutzern verarbeitet werden. [\leq]

3.13.2 FHIR Data Services

3.13.2.1 Patient Service

A_26252-03 -Patient Service - Realisierung der Schnittstelle des FHIR IG ePA Basisfunktionalitäten

Der Patient Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide ePA Basisfunktionalitäten (Patient Service) gemäß [IG_Basic] umsetzen. [\leq]

A_26254-01 -Patient Service - Protokolleinträge für Zugriffe auf den Patient Service

Der Patient Service MUSS einen Protokolleintrag gemäß A_24704* erzeugen und dabei folgende Wertbelegung berücksichtigen:

Tabelle 37: Patient Service Protokollierung

Strukturelement	Wert	Erläuterung
AuditEvent.type	"rest"	
AuditEvent.action	U	Update
AuditEvent.entity.name	Patient	Service Name
AuditEvent.entity.description	upsertPatient	operationId der zu ausgeführten Operation

[\leq]

3.13.2.2 Medication Service

A_26253-01 -Medication Service - Realisierung der Schnittstellen des FHIR IG Medication Service

Der Medication Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide für den Medication Service [IG_Medication_Service] umsetzen. [≤]

A_26317 -Medication Service - Erzeugung eines xHTML-Exports

Der Medication Service MUSS gemäß den Vorgaben von [IG_Medication_Service] für die Generierung der Medikationsliste im xHTML-Format nach [XHTML] sicherstellen, dass kein ausführbarer Code im Export enthalten ist. [≤]

A_24820 -Medication Service - Ablehnung von Request bei vorliegendem Widerspruch

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID != oid_erp-vau, oid_versicherter mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("medication") die Entscheidung ("deny") gesetzt ist. [≤]

A_25152 -Medication Service - Ablehnung neuer Daten bei vorliegendem Widerspruch

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID == oid_erp-vau mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny") gesetzt ist. [≤]

A_25153 -Medication Service - Löschen der Daten des Medication Service

Der Medication Service MUSS alle vorhandenen fachlichen Daten des Medication Service löschen, wenn im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny") gesetzt wird. [≤]

A_26399 -Medication Service - Ablehnung von Request bei vorliegendem Widerspruch gegen die Nutzung durch eine spezifische LEI

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID gemäß A_26406-* mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management die LEI der User Session in der User Specific Deny Policy des Medication Service enthalten ist. [≤]

A_24841-03 -Medication Service - Schemavalidierung

Der Medication Service MUSS im Body der HTTP-POST-Operation die übertragenen Parameter auf Schadcode prüfen und fachfremde Daten (d.h. Schemavalidierung) prüfen und im Fehlerfall das Ausführen der Operation mit dem HTTP Status Code 400 abbrechen. [≤]

A_27894 -Medication Service - Nutzung der FHIR-Operationen durch den E-Rezept-Fachdienst

Der Medication Service MUSS sicherstellen, dass die folgenden FHIR-Operationen ausschließlich durch den E-Rezept-Fachdienst mit der professionOID oid_erp-vau genutzt werden dürfen:

- providePrescription MedicationSvc
- cancelPrescription MedicationSvc
- provideDispensation MedicationSvc
- cancelDispensation MedicationSvc.

[≤]

A_24849-045 -Medication Service - Protokolleinträge für Zugriffe auf den Medication Service

Der Medication Service MUSS einen Protokolleintrag gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 38: Medication Service Protokollierung

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
type		"rest"	
action	OperationId: providePrescription_MedicationSvc	"C"	Einstellen von Verschreibungsdate n
	OperationId: provideDispensation_MedicationSvc	"C"	Einstellen einer Medikamentenabgab e
	OperationId: cancelPrescription_MedicationSvc	"U"	Stornieren von Verschreibungsdate n
	OperationId: cancelDispensation_MedicationSvc	"U"	Stornieren einer Medikamentenabgab e
	OperationId: getMedicationList_MedicationSvc	"R"	Abruf der Medikationsliste
	OperationId:- renderMedicationListToHTML_MedicationSvc	"R"	Abruf der Medikationsliste im HTML-Format
	OperationId: renderMedicationListToPDF_MedicationSvc	"R"	Abruf der Medikationsliste im PDF-Format
	OperationId: listMedications_MedicationSvc	"R"	Abruf von Medikamenteninformationen
	OperationId: listMedicationDispenses_MedicationSvc	"R"	Abruf von Medikamentenabgab einformationen

	OperationId: listMedicationRequests_MedicationSvc	"R"	Abruf von Verschreibungsinformationen
	<u>OperationId: addEMLEntry_MedicationSvc</u>	<u>"C"</u>	<u>Eintrag in Medikationsliste hinzufügen</u>
	<u>OperationId: updateEMLEntry_MedicationSvc</u>	<u>"U"</u>	<u>Eintrag in Medikationsliste aktualisieren</u>
	<u>OperationId: addEMPEntry_MedicationSvc</u>	<u>"C"</u>	<u>Eintrag in Medikationsplan hinzufügen</u>
	<u>OperationId: updateEMPEntry_MedicationSvc</u>	<u>"U"</u>	<u>Eintrag in Medikationsplan aktualisieren</u>
	<u>OperationId: linkEMP_MedicationSvc</u>	<u>"U"</u>	<u>Eintragsverknüpfung Medikationsplan/Medikationsliste</u>
	<u>OperationId: unlinkEMP_MedicationSvc</u>	<u>"U"</u>	<u>Aufhebung Eintragsverknüpfung Medikationsplan/Medikationsliste</u>
	<u>OperationId: renderMedicationListToPDF_MedicationSvc</u>	<u>"R"</u>	<u>Abruf des Medikationsplans im PDF-Format</u>
	<u>OperationId: getMedicationPlan_MedicationSvc</u>	<u>"R"</u>	<u>Abruf des Medikationsplans</u>
entity.name		"Medication Service"	Service Name
entity.description		<operationId>	operationId der ausgeführten Operation
Nur bei FHIR Query API:			
entity.detail.type		"search-parameters"	
entity.detail		<ResourceName>?parameter1=<	Suchkriterien in

.value[x]		value>¶meter2=<value>& ...mehr	URL-Query-Notation
-----------	--	-----------------------------------	--------------------

5710
5711 Falls ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF der
5712 Medication Service einen Protokolleintrag NICHT erzeugen. [**<=**]

5713 Ereignisse, die gemäß A_26298* zu einer Übertragung neuer oder geänderter Daten an
5714 das FDZ führen, erzeugen grundsätzlich einen eigenen Protokolleintrag für den Vorgang
5715 gemäß der Vorgaben in A_24849*. Liegt kein Widerspruch des Versicherten gegen die
5716 Übermittlung der Daten an das FDZ vor und ist eine Übertragung der Daten des
5717 Ereignisses aufgrund der Pseudonymisierbarkeit dieser Daten möglich, so folgt auf das
5718 ursächliche Ereignis automatisch der Export der pseudonymisierten Daten.

5719 Diese Übertragung der Daten muss für einen Versicherten aus der Protokollierung
5720 ersichtlich sein. Anstelle eines dedizierten Protokolleintrags für die Datenübertragung
5721 wird die Datenübertragung als ergänzendes entity.detail des auslösenden Ereignisses
5722 protokolliert. Aus dem Protokolleintrag des Ereignisses ist dann ersichtlich, ob die
5723 betroffenen Daten in pseudonymisierter Form auch der sekundären Datennutzung
5724 zugeführt wurden.

5725 **A_27188 -Medication Service - Protokollierung des Datenexports an das FDZ**
5726 Der Medication Service MUSS einen Protokolleintrag gemäß A_24849* um das folgend
5727 aufgeführte entity.detail mit dem Wert true ergänzen, wenn aus der Operation eine
5728 Übertragung von Daten an das FDZ folgt. Diese Ergänzung MUSS entweder den Wert
5729 false haben oder entfallen, wenn aus der Operation keine Übertragung von Daten an
5730 das FDZ folgt.
5731

Strukturelement		Wert	Erläuterung
entity.detail.type		"data-submission"	Export an das Forschungsdatenzentrum
entity.detail.value[x]		"true" oder "false"	

5732 [**<=**]

5733 3.13.2.3 MHD Service

5734 **A_27667-01 -MHD Service - Realisierung der Schnittstellen des FHIR IG** 5735 **Medication-ServiceHD**

5736 Der MHD Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide
5737 für den MHD Service [IG_MHD_Service] umsetzen. [**<=**]

5738 Hinweis zu A_27667-*: Auch für den MHD Service sind die übergreifenden
5739 Anforderungen A_15159 zum Schutz gegen die OWASP Risiken und A_24783 zur
5740 Eingabvalidierung zu berücksichtigen, um zu verhindern, dass Schadcode über
5741 Suchanfragen ins Aktensystem eingebracht werden kann.

5742 **A_27892 -MHD Service - Durchsetzen der Zugriffskontrolle für XDS Document** 5743 **Service**

5744 Der MHD Service MUSS bei einer Suchanfrage durch einen Nutzer alle Zugriffsregeln
5745 durchsetzen, die für den Zugriff dieses Nutzers bzgl. des XDS Document Service
5746 gelten. [**<=**]

Hinweis zu A_27892-*: Nutzer dürfen durch den MHD Service keinen Zugriff auf Dokumente erhalten, auf den sie über den XDS Document Service nicht zugreifen dürften. So dürfen Nutzer mittels des MHD Services keinen Zugriff auf Dokumente einer Dokumentenkategorie erhalten, auf die sie nach der Legal Policy nicht zugreifen dürfen. Genauso dürfen sie über den MHD Service keine Dokumente finden, die auf der General Deny Policy stehen.

A_27668 -MHD Service - Filtern von verborgenen Metadaten und Dokumenten

Der MHD Service MUSS bei einer Suchanfrage bei jedem Dokument einer verborgenen Datenkategorie die Metadaten (bzw. korrespondierende FHIR-Ressource DocumentReference filtern sowie den Dokumentenabruf ausDocumentReferences.content.attachment.url verhindern (HTTP Code 404 not found).[<=]

A_27669 -MHD Service – Protokolleinträge für Zugriffe auf den MHD Service

Der MHD Service MUSS einen Protokolleintrag gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 39: MHD Service Protokollierung

Strukturelement [AuditEvent.]	Operationen der FHIR Query API	Wert	Erläuterung
type		"rest"	
action	OperationId: findDocumentReferences_MHDSvc	"R"	Suche von Dokumenten
	OperationId: retrieveDocument_MHDSvc	"R"	Abruf eines Dokuments
entity.name		"MHD Service"	
entity.detail.type		"search-parameters"	
entity.detail.value[x]		<ResourceName>?parameter1=<value>¶meter2=<value>& ...mehr	Suchkriterien in URL-Query-Notation

Falls ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF der MHD Service NICHT einen Protokolleintrag erzeugen.[<=]

3.13.2.4 Audit-Event-Serviceübergreifende Festlegungen

A_27886 -FHIR Data Service – Durchführung von Datenbestandsmigrations

3.14 Wenn Migrationsvorgaben für den Datenbestand eines FHIR Data Services für verschiedene Versionen des Services existieren, MUSS der FHIR Data Service

Ere alle bislang nicht angewandten Datenbestandsmigrationsvorgaben in der richtigen Reihenfolge (d.h. nacheinander die jeweils für die Version benannten Migrationsschritte beginnend mit der kleinsten Versionsnummer hin zur höchsten Versionsnummer) ausführen oder, alternativ eine Migration der Daten vornehmen, die zum selben Ergebnis führt.
[<=]

3.14 Audit Event Service

Ereignisse und Zugriffe auf die ePA eines Versicherten werden im ePA Aktensystem protokolliert. Die Protokollierung dient der Datenschutzkontrolle für den Versicherten. Der Audit Event Service ist ein FHIR Data Service und ermöglicht dem Versicherten, befugten Vertretern bzw. der Ombudsstelle den Zugriff auf diese Protokollinformationen.

A_24704-02 -Audit Event Service - Realisierung der Schnittstelle des FHIR IG ePA Basisfunktionalitäten

Der Audit Event Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide ePA Basisfunktionalitäten (Audit Event Service) gemäß [IG_Basic] umsetzen.[<=]

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

Tabelle 40 : Inhaltliche Definitionen eines AuditEvent

Information	Strukturelement
Wann ist der Zugriff erfolgt bzw. hat das Ereignis stattgefunden?	AuditEvent.recorded
Wer war der Akteur/Auslöser?	AuditEvent.agent
Welcher Art Service wurde angefragt?	AuditEvent.type
Worauf wurde zugegriffen?	AuditEvent.source
Welcher Art war der Zugriff?	AuditEvent.action
War der Zugriff erfolgreich?	AuditEvent.outcome
Informationen zu Daten/Dokumente/Objekte	AuditEvent.entity

5792 Die spezifische Befüllung eines Audit Events gemäß A_24704* wird durch die jeweiligen
 5793 Services vorgegeben. Allgemeine Elemente sind wie folgt zu befüllen:

5794 **A_25154-04 -ePA-Aktensystem - Befüllung der Elemente recorded, agent und**
 5795 **source eines Audit Events**

5796 Das ePA-Aktensystem MUSS die Audit Event Elemente AuditEvent.recorded,
 5797 AuditEvent.agent und AuditEvent.source wie folgt befüllen.

5798 **Tabelle 41 Befüllung AuditEvent**

Element [AuditEvent.]		Beschreibung	Beispiel
recorded		Systemzeit bei Erstellung des AuditEvents im Format YYYY-MM-DDThh:mm:ssZ	"2025-01-15T14:52:04.928Z"
purposeOfEvent		Zweck(e) des protokollierten Ereignisses gemäß des zulässigen Value-Sets. Nur zu belegen, wenn explizit bei entsprechender Protokollierungsanforderung gefordert.	
	system	Das verwendete Codesystem	" https://gematik.de/fhir/epa/ValueSet/epa-auditevent-purpose-of-event-vs "
	code	Der verwendete Code aus dem Codesystem	"EXPORTFDZ"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Export für das Forschungsdatenzentrum Gesundheit"
agent[client].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem; Fest vorgegebener Wert: "http://dicom.nema.org/resources/ontology/DCM"	"http://dicom.nema.org/resources/ontology/DCM"
	code	Der verwendete Code aus dem Codesystem; Fest vorgegebener Wert: "110150"	"110150"

	display	Der Bezeichner zur Anzeige aus dem Codesystem; Fest vorgegebener Wert: "Application"	"Application"
agent[client].who.identifizier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/sid/telematik-id"
	value	<Telematik-Id>	"1-883110000092404"
agent[client].	altId	<value> aus agent.who.identifizier	"1-883110000092404"
agent[client].	name	<ul style="list-style-type: none"> <display_name> des auslösenden Akteurs aus dem ID-Token der UserSession "Elektronische Patientenakte Fachdienst" für intern ausgelöste AuditEvents 	1) "E-Rezept-Fachdienst" 2) "Elektronische Patientenakte Fachdienst" 3) "Portugal" (Beispiel EU-Zugriff)
agent[client].	requestor	Fest vorgegebener Wert "false"	"false"
agent[user].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	" http://terminology.hl7.org/CodeSystem/v3-RoleClass "
	code	Der verwendete Code aus dem Codesystem	"PROV"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"healthcare provider"
agent[user].who.identifizier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/sid/telematik-id"
	value	<Telematik-Id> oder <KVN-R>	1) "2-121212121212121"

			2) "Z123456789"
agent[user].	altId	<value> aus agent.who.identifizier	1) "2-121212121212121" 2) "Z123456789"
agent[user].role. coding		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthProfessionalRole.	
	system	Das verwendete Codesystem	"urn:oid:1.3.6.1.4.1.12559.11 .10.1.3.2.2.2"
	code	Der verwendete Code aus dem Codesystem	"Resident Physician"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Resident Physician"
agent[user].extension		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthcareFacilityType; extension mit url="https://gematik.de/fhir/dev- epa/StructureDefinition/epa- healthcare-facility-type- extension">	
	system	Das verwendete Codesystem	"urn:oid:2.16.840.1.113883.2 .9.6.2.7"
	code	Der verwendete Code aus dem Codesystem	"221"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Medical Doctors"
agent[user].	name	Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: <leiName> / <healthProfessionalName> Andernfalls: <display_name> des auslösenden Akteurs aus dem ID-Token der UserSession	EU-Zugriff: "Dr. Manuel Dos Santos / Clínica de Dos Santos" Andernfalls: "John Doe"
agent[user].	requestor	Fest vorgegebener Wert "false"	false

agent[internal].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/epa/CodeSystem/epa-auditevent-sourcetype-cs"
	code	Der verwendete Code aus dem Codesystem	"DATASUBSVC"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Data Submission Service"
agent[internal].altId		Fest vorgegebener Wert "ePA"	"ePA"
agent[internal].name		Fest vorgegebener Wert "ePA"	"ePA"
agent[internal].requestor		Fest vorgegebener Wert "false"	"false"
source		Informationen zum auslösenden Service des Aktensystems	
source.observer.display		Fester Wert "Elektronische Patientenakte Fachdienst"	"Elektronische Patientenakte Fachdienst"
source.type.		Der auslösende Service gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs"
	code	Der verwendete Code aus dem Codesystem	"CDMGMT"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Consent Decision Management"

5799

5800 Hinweis:

5801

5802 agent[client]: Angaben zur Applikation, z. B. eRezept-Fachdienst, NCPeH

5803 agent[user]: Angaben zu LEI oder Vertreter oder Versicherter

5804 agent[internal]: Angaben zu systemeigenen Prozessen, z. B. Datenexport für das FDZ

5805 [**<=**]5806 **A_27689 -Protokollierung von nicht erfolgreichen Zugriffen**

5807 Falls für eine Operation ein Protokolleintrag gefordert ist und mit einem Fehler

5808 abgebrochen wird, MUSS der Audit Event Service jeweils einen Protokolleintrag gemäß

5809 A_24704* erzeugen. Darüberhinaus und ergänzend zu den Vorgaben aus dem Profil
 5810 EPAAuditEvent gemäß [IG_Basic] sind folgende Werte entsprechend zu belegen:

5811 **Tabelle 42 Audit Event Management Protokollierung - Fehler**

Strukturelement	Wert	Erläuterung
AuditEvent.action	C, R, U, D	Create Read Update Delete
AuditEvent.entity.name	<service name>	Service Name, wie für Protokollierung im Service gefordert
AuditEvent.entity.description	<operationId>	OperationId der mit einem Fehler abgebrochenen Operation, z. B. "providePrescription_MedicationSvc"
Nur bei FHIR Query API:		
entity.detail.type	"search-parameters"	
entity.detail.value[x]	<ResourceName>?parameter1=<value>parameter2=<value>& ...mehr	Suchkriterien in URL-Query-Notation

5812
 5813 Falls ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF bei
 5814 nicht erfolgreichen Zugriffen ein Protokolleintrag NICHT erzeugt werden.

5815
 5816 Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A_25172* entfällt, wenn ein
 5817 Protokolleintrag mangels eines befugten Nutzers (kein Bezug des
 5818 SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann.
 5819 [**<=**]

5820 **A_24503 -ePA-Aktensystem - Aufbewahrungsdauer der Protokolleinträge**

5821 Das ePa-Aktensystem MUSS die zum Zwecke der Datenschutzkontrolle für den
 5822 Versicherten erstellten
 5823 Protokolleinträge für drei Jahre aufbewahren. Danach sind sie vom Aktensystem
 5824 automatisch zu löschen. [**<=**]

5825 Die Protokolleinträge können durch den Versicherten oder durch einen befugten Vertreter
 5826 mittels ePA-FdV eingesehen werden. Versicherte ohne ePA-FdV können bei ihrer
 5827 zuständigen Ombudsstelle beantragen, die Protokolldaten zur Verfügung gestellt zu
 5828 bekommen.

5829 Für eine Abfrage der Protokolleinträge als strukturierte Einträge nutzen ein ePA-FdV und
 5830 die Ombudsstelle den Audit Event Service [IG_Basic].

5831 **A_24714-01 -Audit Event Service - Realisierung der Query API: AuditEvent**

5832 Der Audit Event Service MUSS die "Query API: AuditEvent" des FHIR Implementation
 5833 Guide für den Audit Event Service [IG_Basic] umsetzen. [**<=**]

5834 **A_24750-02 -Audit Event Service - Realisierung der Render API: PDF Audit**

5835 Der Audit Event Service MUSS die "Render API: PDF Audit" des FHIR Implementation
5836 Guide für den Audit Event Service [IG_Basic] umsetzen. [≤]

5837 **A_25172 -Audit Event Service - Speicherung der Protokolldaten**

5838 Der Audit Event Service MUSS die Daten der Protokolleinträge verschlüsselt im
5839 SecureDataStorage persistieren. [≤]

5840 Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A_25172* entfällt, wenn ein
5841 Protokolleintrag mangels eines befugten Nutzers (kein Bezug des
5842 SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann.

5843 **A_25018 -Audit Event Service - PAdES-Signatur in renderAuditEventsToPDF**

5844 Der Audit Event Service MUSS bei der Operation `renderAuditEventsToPDF` beim
5845 Signieren eines Protokolls im PDF/A-Format eine PAdES-Signatur gemäß [PAdES-3] und
5846 [PAdES Baseline Profile] erstellen. Bei der Signaturerstellung ist das Attribut `signing`
5847 `certificate reference` gemäß den Vorgaben aus [PAdES-3] Kapitel 4.4.3 „Signing
5848 Certificate Reference Attribute“ anzulegen. [≤]

5849 Durch die Baseline-Profilierung [PAdES Baseline Profile] wird festgelegt, wie der
5850 Signaturzeitpunkt, gemessen als Systemzeit des ePA-Aktensystems, in die Signatur
5851 eingebracht wird.

5852 **A_24991 -Audit Event Service – Protokollierung von Zugriffen auf die**
5853 **Protokolldaten**

5854 Der Audit Event Service MUSS für die Zugriffe der Ombudsstelle oder eines Vertreters auf
5855 die protokollierten Daten jeweils einen Protokolleintrag gemäß A_24704* erzeugen.

5856 **Tabelle 43: Audit Event Service Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		
AuditEvent.action	R		Read
AuditEvent.entity.name	"AuditEvent"		Service Name
AuditEvent.entity.description	Passend zur ausgeführten Operation ein Wert aus folgender Liste: <ul style="list-style-type: none"> • <code>listAuditEvents</code> • <code>getAuditEventById</code> • <code>renderAuditEventsToPDF</code> 		operationId der zu protokollierenden Operation
AuditEvent.entity.detail	type	value[x]	
	parameters	parameter1=<value>¶meter2=<value>& ...mehr	Nur bei <code>getAuditEventList</code>

	identifizier	<id> des AuditEvents	Nur bei getAuditEvent
--	--------------	----------------------	--------------------------

5857 [**<=**]

5858 *Hinweis: Zugriffe des Versicherten auf die Protokolle des Aktenkontos werden nicht*
5859 *protokolliert.*

5860

5861 3.15 Information Service

5862 3.15.1 Information Service

5863 Der Information Service ist ohne die Nutzung eines VAU-Kanals nutzbar. Die über den
5864 Information Service genutzten Daten sind ausschließlich persistierte Daten des
5865 Aktenkontos, die weder mit dem SecureAdminStorageKey noch mit dem
5866 SecureDataStorageKey gesichert sind.

5867 Der Zugang erfolgt durch Nutzung der Schnittstelle `I_Information_Service`.

5868 **A_24344 -Information Service - Realisierung der Schnittstelle** 5869 **I_Information_Service**

5870 Der Information Service MUSS die Operationen der Schnittstelle `I_Information_Service`
5871 gemäß `[I_Information_Service]` umsetzen. [**<=**]

5872 **A_24345 -Information Service - Kein Zugriff auf verschlüsselte Daten des** 5873 **Aktenkontos**

5874 Der Information Service DARF NICHT auf Daten zugreifen, die nicht explizit für die
5875 Verwendung durch den Informationsdienst bereitgestellt wurden. Dazu gehören
5876 insbesondere alle Daten des Aktenkontos, die mit den versichertenindividuellen
5877 Schlüsseln zur Daten- oder Befugnispersistierung (`SecureDataStorageKey` oder
5878 `SecureAdminStorageKey`) gesichert sind. [**<=**]

5879 3.15.1.1 Informationen zu Widersprüchen (Consent Decisions)

5880 Die Widersprüche eines Versicherten gegen die Nutzung von Funktionen der
5881 elektronischen Patientenakte werden durch das Consent Decision Management gesichert
5882 administriert. Änderungen an den Widersprüchen erfolgen dort.

5883 Der Information Service bietet für die Nutzergruppen der ePA eine einfache
5884 Abfragemöglichkeit der aktuell erteilten oder nicht erteilten Widersprüche auch ohne die
5885 Nutzung des Consent Decision Managements an. Liegt ein Widerspruch gegen die
5886 Nutzung einer Funktion vor, kann auf die Ausführung der zur Nutzung dieser Funktion
5887 notwendigen Aktionen mit der ePA eines Versicherten durch den Client verzichtet
5888 werden.

5889 Für diese vereinfachte Abfragemöglichkeit der aktuellen Widersprüche verwendet der
5890 Information Service den durch das Consent Decision Management persistent
5891 übertragenen Zustand der Widersprüche ("Cache" des Zustands der Widersprüche).
5892 Berücksichtigt wird dabei die Widerspruchsinformation, für die eine vereinfachte Abfrage
5893 vorgesehen ist (Widersprüche der Klasse "Versorgungsprozess").

3.15.1.2 Informationen zur Anwenderperformance (UX Performance)

Der Information Service stellt für die Umgebung der Leistungserbringer die Operation zur Sammlung der Messwerte zu den Anwendungsfällen der Nutzererfahrung zur Verfügung. Die Weiterverarbeitung der gesammelten Daten ist in 2.8- Performance aus Anwendersicht definiert und vorgegeben.

3.15.2 Information Service - Account

Die Operationen der Information Service - Account werden für den Umzug eines existierenden Aktenkontos zu einem neuen Anbieter verwendet. Die Nutzung der Operationen erfolgt exklusiv durch die Aktensystembetreiber.

Die Verwendung der einzelnen Operationen erfolgt im Verbund mit den Operationen der Schnittstelle I_Health_Record_Relocation_Service für die Umsetzung der Anwendungsfälle eines automatischen Aktenkontoumzugs und sind in 3.2- Health Record Relocation Service erläutert.

A_24424 -Information Service Account - Realisierung der Schnittstelle I_Information_Service_Accounts

Der Information Service MUSS die Operationen der Schnittstelle I_Information_Service_Accounts gemäß [I_Information_Service_Accounts] umsetzen. [<=]

A_24665 -Information Service Account - Nutzung beidseitig authentisiertes TLS

Der Information Service MUSS sicherstellen, dass die Operationen der Schnittstelle I_Information_Service_Accounts ausschließlich unter Verwendung einer beidseitig authentisierten TLS-Verbindung zwischen den beteiligten Aktensystemen genutzt werden und die Operationen ansonsten abgebrochen und mit einer Fehlermeldung gemäß Vorgaben in [I_Information_Service_Accounts] beantwortet werden. [<=]

A_25054 -Information Service Account - Gegenseitige Authentisierung Aktensysteme

Die Information Service Account Dienste der Aktensysteme MÜSSEN sich mit der TLS-Identität mit professionOID oid_epa_mgmt mittels des Zertifikats C.FD-TLS-S gegenseitig authentisieren. [<=]

A_25053 -Information Service Account - Prüfung der TLS-Zertifikate

Der Information Service Account MUSS bei der Authentifizierung eines jeweils anderen Aktensystems die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC_PKI_018 durchführen. Zur Prüfung des TLS-Zertifikats C.FD-TLS-S sind dabei die Parameter PolicyList=oid_fd_tls_s, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-serverAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD-TLS-C sind dabei die Parameter PolicyList=oid_fd_tls_c, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-clientAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden. [<=]

3.16 Email Management

Das Email Management ermöglicht einem FdV-Nutzer die Verwaltung seiner E-Mail-Adresse und einem Kostenträger die Verwaltung von E-Mail-Adressen von Versicherten, die bei diesem Kostenträger versichert sind.

- 5939 Die Schnittstelle zum Verwalten der E-Mail-Adressen durch den Kostenträger dient dem
5940 ausschließlichen Zweck des Einstellens, Lesens und der Änderung von E-Mail-Adressen
5941 auf Verlangen des Versicherten. Dies ermöglicht dem Kostenträger, seinen Versicherten
5942 die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte auf Berichtigung und
5943 Auskunft bzgl. der im Aktensystem verarbeiteten E-Mail-Adresse zu gewährleisten.
- 5944 Für einen Versicherten kann nur genau eine E-Mail Adresse hinterlegt werden.
- 5945 **A_25435 -Email Management - Realisierung der Schnittstelle**
5946 **I_Email_Management**
5947 Das Email Management MUSS die Operationen der Schnittstelle I_Email_Management
5948 gemäß [I_Email_Management] umsetzen.[<=]
- 5949 **A_25438 -Email Management - Beschränkung der Schnittstellenoperationen auf**
5950 **E-Mail-Adressen des FdV-Nutzers**
5951 Das Email Management MUSS die Operationen der Schnittstelle I_Email_Management
5952 gemäß [I_Email_Management] auf die E-Mail-Adresse des aufrufenden Nutzers
5953 einschränken, sofern der Nutzer ein FdV-Nutzer ist.[<=]
- 5954 **A_26161 -Email Management - Nutzen von Email Management auch bei**
5955 **Widerpruch**
5956 Das Email Management MUSS sicherstellen, dass das Email Management auch von
5957 Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben.[<=]
- 5958 **A_26162 -Email Management - Versicherte nutzen Email Management**
5959 **ausschließlich im Home-AS**
5960 Das Email Management des ePA-Aktensystems MUSS sicherstellen, dass das Email
5961 Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-
5962 Aktensystem das Home-AS ist.[<=]
- 5963 Hinweis: Für das Email Management ist auch Anforderung A_26154* umzusetzen.
- 5964 **A_25439 -Email Management - Kostenträger kann ausschließlich E-Mail-**
5965 **Adressen der eigenen Versicherten verwalten**
5966 Das Email Management MUSS sicherstellen, dass ein Kostenträger mittels der
5967 Operationen der Schnittstelle I_Email_Management gemäß [I_Email_Management]
5968 ausschließlich E-Mail-Adressen von Versicherten verwalten kann, die beim Kostenträger
5969 versichert sind.[<=]
- 5970 **A_25440-01 -Email Management - Benachrichtigung bei Änderung der E-Mail-**
5971 **Adresse**
5972 Falls eine E-Mail-Adresse a) ersetzt oder b) ergänzt wird, MUSS das Device Management
5973 bei a) eine E-Mail an die alte und die neue E-Mail-Adresse senden und bei b) eine E-Mail
5974 an die neue E-Mail-Adresse senden, in der bei a) über die Ersetzung bzw. bei b) die
5975 Ergänzung einer E-Mail-Adresse informiert wird. In der E-Mail MUSS darüber informiert
5976 werden, wann und ob der FdV-Nutzer selbst oder der Kostenträger die E-Mail ersetzt
5977 bzw. ergänzt hat.[<=]
- 5978 **A_25441 -Email Management - Information bzgl. der Ergänzung bei E-Mail-**
5979 **Adressen**
5980 Das Email Management MUSS sicherstellen, dass der FdV-Nutzer für eine im Email
5981 Management hinterlegte E-Mail-Adresse erkennen kann, wann und von wem diese E-
5982 Mail-Adresse ergänzt wurde.[<=]
- 5983 **A_25968-01 -Email Management - Maximale Anzahl E-Mail-Adressen**
5984 Das Email Management MUSS sicherstellen, dass für einen Nutzer maximal eine E-Mail-
5985 Adresse hinterlegt werden kann.[<=]
- 5986 **A_26163 -Email Management - Keine Persistierung einer im Rahmen der**
5987 **Vertretereinrichtung übergebenen E-Mail-Adresse**

5988 Das Email Management MUSS sicherstellen, dass eine im Rahmen des Anwendungsfalls
5989 der Vertretereinrichtung vom Nutzer übermittelte E-Mail-Adresse nicht persitiert und
5990 spätestens bei Beendigung der User Session gelöscht wird. [<=]

5991 **A_26164 -Email Management - Keine Gerätereistrierung mit der im Rahmen**
5992 **der Vertretereinrichtung übergebenen E-Mail-Adresse**

5993 Das Email Management MUSS sicherstellen, dass keine E-Mail-Adressen zur Übermittlung
5994 eines Gerätereistrierungscodes genutzt werden, die dem ePA-Aktensystem im Rahmen
5995 des Anwendungsfalls der Vertretereinrichtung übermittelt wurden. [<=]

5996 Hinweis zu A_26163 und A_26164: Die im Rahmen des Anwendungsfalls der
5997 Vertretereinrichtung übermittelte E-Mail-Adresse wird ausschließlich zur Information des
5998 Vertreters über die Einrichtung der Vertretung genutzt (vgl. A_24755-*).

5999 **3.17 Zusätzliche Anforderungen an den Authorization Service**

6000 Der ePA Authorization Service wird sowohl für die Authentisierung der Versicherten über
6001 das FdV als auch für die Authentisierung von Leistungserbringern und Kostenträgern über
6002 deren Primärsystem benötigt. Ebenso muss die Zugriffsautorisierung für andere
6003 Fachdienste wie z.B. E-Rezept geprüft werden. Die Festlegungen für den Authorization
6004 Server finden sich in [gemSpec_IDP_FD]. Dieser Abschnitt des vorliegenden Dokuments
6005 enthält spezifische Anforderungen, die vom Authorization Service des Aktensystems
6006 zusätzlich umzusetzen sind.

6007 **A_24923 -Authorization Service - I_Authorization_Service**

6008 Der Authorization Service MUSS die Operationen der
6009 Schnittstelle `I_Authorization_Service` implementieren gemäß
6010 [I_Authorization_Service]. [<=]

6011 **A_25283 -Authorization Service - Konvertieren von ID-Token**

6012 Der Authorization Service MUSS sicherstellen, dass für ein nach erfolgreicher
6013 Authentifizierung des Nutzers vorliegendes ID-Token mittels Regel `rr0` gemäß
6014 `Tab_AS_Entitlement_Registration_Rules` ein HSM-ID-Token erstellt wird, bevor das ID-
6015 Token zeitlich ungültig ist. [<=]

6016 **3.17.1 Anforderungen an den Authorization Service für die**
6017 **Authentisierung von Versicherten (FdV)**

6018 Im Rahmen der Authentisierung des Versicherten erfolgt die Prüfung der
6019 Gerätereistrierung (Verifikation) direkt. Das Gerät muss dafür die Geräteparameter
6020 eines zuvor ausgeführten und bestätigten Registrierungsprozesses verwenden

6021 Bisher nicht registrierte Geräte, bzw. Geräteparameter einer bisher nicht bestätigten
6022 Gerätereistrierung, können unter Verwendung des Device Management registriert, bzw.
6023 bestätigt werden (siehe Kapitel 3.12. Device Management).

6024

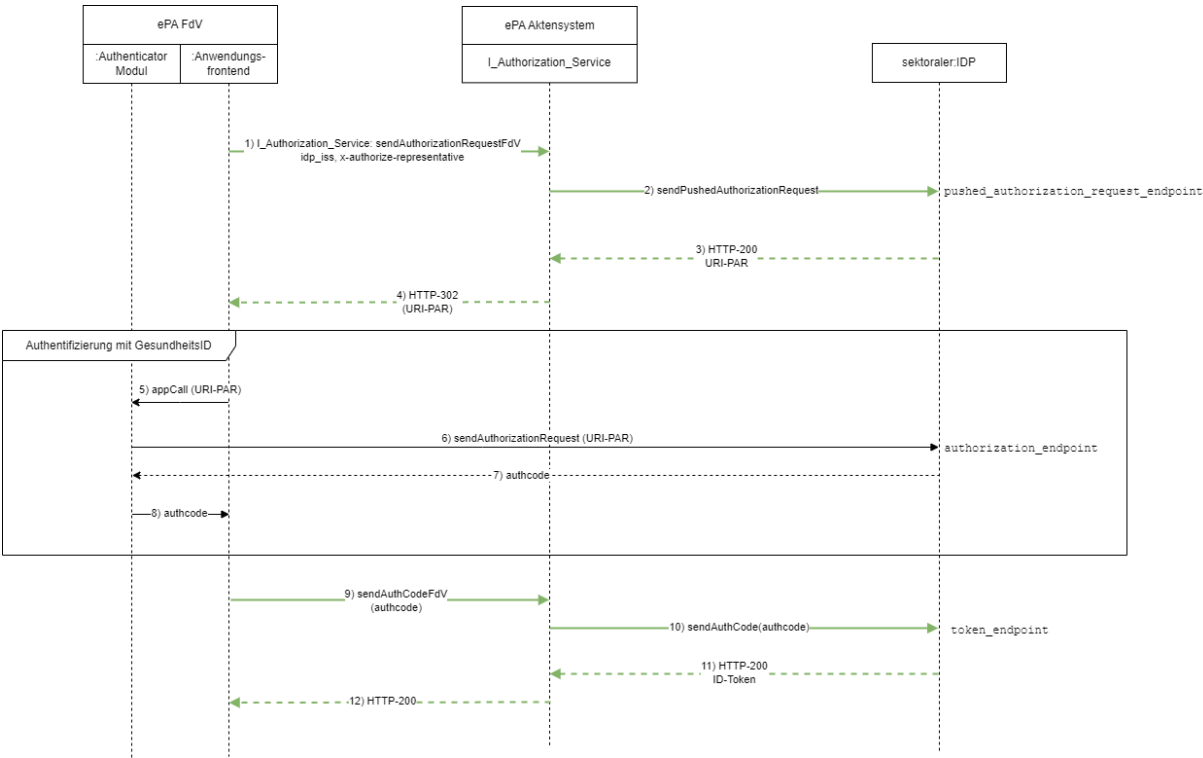


Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP

A_25717-03 -Authorization Service - Pushed Authorization-Request des Authorization Service an sektorale Identity Provider

Der ePA Authorization Service MUSS den Pushed Authorization Request (PAR) an durch den vom ePA-FdV übergebenen Parameter idp-iss adressierten sektoralen IDP gemäß [gemSpec_IDP_FD#AF_10117] mit folgenden Parametern aufrufen:

Parameter	Wert	Anmerkung
scope	"openid urn:telematik:display_name urn:telematik:versicherter urn:telematik:family_name urn:telematik:given_name"	Notwendige Scopes für den Zugriff für die Autorisierung von Nutzern am ePA-Aktensystem
acr_values	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung
redirect_uri	Inhalt des Parameters x-redirecturi [sendAuthorizationRequestFdV in I_Authorization_Service], 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.
--	--	--------

6032 [**<=**]

6033 Hinweis 1: An die `redirect_uri` im Pushed Authorization Request sendet der sektorale IDP
6034 den ausgestellten Authorization Code (siehe [`gemSpec_IDP_Sek`])

6035 Hinweis 2: Der Redirectaufruf, der vom Authenticator Modul an die `redirect_uri`
6036 ausgeführt wird, wird vom ePA-FdV über Plattformmechanismen (`deeplink/universallink`)
6037 gefangen und stellt selbst einen POST-Request an den Endpunkt des Authorization
6038 Service.

6039 **A_26584 -Authorization Service - Liste der `redirect_uris` im Entity Statement**

6040 Der Authorization Service MUSS in seinem Entity Statement im `claim redirect_uris`
6041 die `redirect_uris` aller Mandanten auflisten, welche bei der Registrierung an einem
6042 beliebigen ePA Authorization Service eine eigene `redirect_uri` angegeben haben. Über
6043 Änderungen des `claim redirect_uris` MUSS der Anbieter des Federation Master vor
6044 produktiver Verwendung informiert werden[**<=**]

6045 Hinweis: Im Registrierungsprozess eines Mandanten mit eigener `redirect_uri` muss
6046 sichergestellt sein,

- 6047 • dass alle Anbieter von ePA Authorization Servern (ePA Aktensystem Anbieter)
6048 entsprechend informiert sind und das Entity Statement anpassen
- 6049 • dem Hersteller des Federation Master über ein ITSM Change bekannt gemacht
6050 wird, dass sich die Entity Statements aller ePA Authorization Server ändern

6051 **A_27145 -Synchronisation "`redirect_URI`" mit Marktteilnehmer - E-Mail-Adresse**

6052 Der Anbieter ePA-Aktensystem MUSS der gematik eine E-Mail-Adresse mitteilen, über
6053 welche er die eigenverantwortliche Registrierung (von `redirect-URIs` im Entity-
6054 Statement) durchführt und über die der Anbieter bei Änderungen erreichbar ist.

6055
6056 Hinweis: Diese E-Mail-Adressen werden durch das Provider Management der gematik
6057 anschließend unter den relevanten Anbietern verteilt bzw. können dort erfragt werden.
6058 Die Änderung der E-Mail-Adressen ist ebenfalls zu kommunizieren.

6059
6060 Hintergrund: Für Stellvertretung via ePA-FdV ist eine Synchronisierung der `redirect_URIs`
6061 notwendig.[**<=**]

6062 **A_27186 -Synchronisation "`redirect_URI`" mit Marktteilnehmer - Information**

6063 Der Anbieter ePA-Aktensystem MUSS bei Änderungen der `redirect_URIs` im eigenen
6064 Entity Statement allen anderen Marktteilnehmern des gleichen Fachdiensttyps diese
6065 Änderung innerhalb 24 Stunden mitteilen.[**<=**]

6066 **A_27187 -Synchronisation "`redirect_URI`" mit Marktteilnehmer - Aktualisierung**

6067 Der Anbieter ePA-Aktensystem MUSS nach dem Empfang der Mitteilungen über
6068 Änderungen der Redirect URIs in einem externen Entity Statement diese Änderung
6069 binnen 24 Stunden in den Redirect URIs des eigenen Entity Statement synchronisieren.

6070
6071 Hinweis: Diese Änderung erfordert anschließend keine Information nach A_27186.[**<=**]

6072 **A_24878-01 -Authorization Service - Authentifizierung eines Versicherten am ePA-FdV des Vertreters**

6073 Falls der Eingangsparameter `x-authorize-representative=True` der Operation
6074 `I_Authorization_Service::sendAuthorizationRequestFdV` gesetzt ist, MUSS der
6075 Authorization Service im PAR als Parameter `amr` mit den Werten
6076 `urn:telematik:auth:guest:eGK` belegt sein, um sicherzustellen, dass sich der Nutzer
6077 nur über eGK+PIN authentisieren darf.[**<=**]
6078

A_26189-01 -Authorization Service - Authentifizierung eines Versicherten im Gastmodus mit eGK und PIN

Falls der Eingangsparameter `x-authorize-egk=True` der Operation `I_Authorization_Service::sendAuthorizationRequestFdV` gesetzt ist, MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:guest:eGK` belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [`<=`]

A_24937-01 -Authorization Service - Einschränkung bei Authentifizierung eines Versicherten am ePA-FdV des Vertreters

Der Authorization Service MUSS sicherstellen, dass ein mit `x-authorize-representative=True` authentisierter Nutzer ausschließlich Zugriff auf das Entitlement Management erhält. [`<=`]

A_26159 -Authorization Service - Prüfen der Device Attestation

Der Authorization Service MUSS sicherstellen, dass von einem anderen ePA-Aktensystem signierte Device Attestations ausschließlich akzeptiert werden, wenn

- die Device Attestation gemäß A_25042-* valide von einer Signaturidentität der VAU eines anderen ePA-Aktensystems signiert wurde,
- die KVN-R in der Device Attestation mit der KVN-R im ID-Token des angemeldeten Nutzers übereinstimmt,
- die Device Attestation zeitlich gültig ist.

[`<=`]

A_26160 -Authorization Service - Keine Persistierung der Device Attestation

Der Authorization Service MUSS sicherstellen, dass die von einem anderen ePA-Aktensystem signierte Device Attestation und deren Inhalte spätestens bei Beendigung der User Session gelöscht und nicht persistiert werden. [`<=`]

A_25310-01 -Authorization Service - Einschränkung bei Authentifizierung mit einem unregistrierten Gerät

Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wird und der Nutzer nicht mit `x-authorize-representative=True` authentisiert wurde, MUSS der Authorization Service sicherstellen, dass der Nutzer ausschließlich Zugriff auf das Device Management erhält. [`<=`]

Hinweis:

Ein vollständiger Zugriff eines authentisierten Nutzers auf alle Dienste des Aktensystems kann nur mit einem Gerät erfolgen, dessen Geräteregistrierung bei der Authentifizierung des Nutzers erfolgreich verifiziert wurde.

Ein Nachweis einer Geräteregistrierung ist entweder DeviceID (`deviceIdentifier` und `deviceToken`), die für den Nutzer im Aktensystem bekannt sind oder die vom Client übergebene Device Attestation (`deviceAttestation`), die zuvor am Device Management des Home Aktensystems durch den Client abgerufen wurde.

A_24804-01 -Authorization Service - Prüfung auf registriertes Gerät

Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des Vertreters handelt und im Operationsaufruf

`I_Authorization_Service::sendAuthCodeFdV` eine DeviceID (`deviceIdentifier` und `deviceToken`) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer registriert und bestätigt ist und übereinstimmt. [`<=`]

A_24914-03 -Authorization Service - Prüfung auf registriertes Gerät - kein registriertes Gerät

Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wurde, MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung abbrechen und die User Session beenden.[<=]

A_24915-01 -Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht bestätigt
Falls als Nachweis einer Geräteregistrierung eine DeviceID (deviceIdentifier und deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status == 'pending'), MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung abbrechen und die User Session beenden.[<=]

3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B

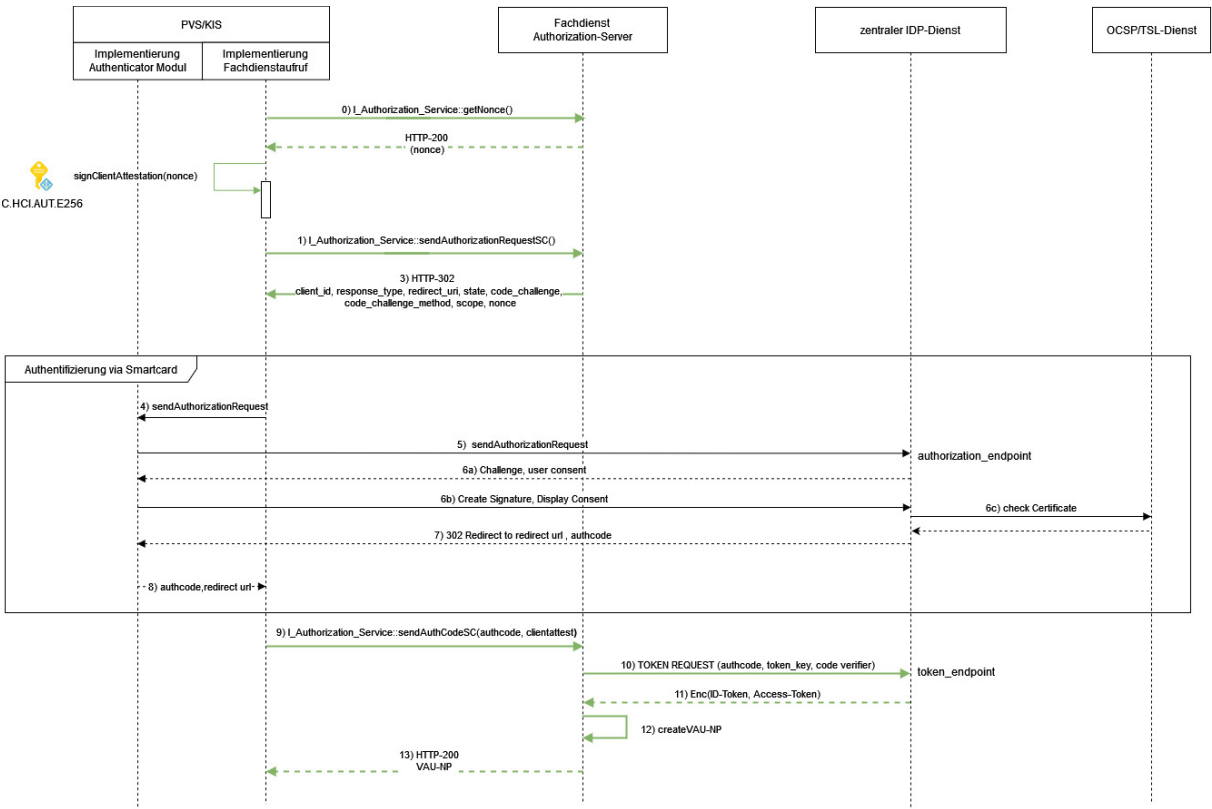


Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP

A_24717 -Authorization Service: IDToken vom IDP-Dienst nur mit Client-Attestation nutzbar

Der Authorization Service MUSS sicherstellen, dass ein vom IDP-Dienst abgerufenes ID-Token für Nutzer "TelematikID_X" nur dann akzeptiert wird, falls im Authorization Service auch eine Client-Attestation vom Nutzer "TelematikID_X" vorliegt.[<=]

A_24718 -Authorization Service: Client-Attestation nur einmal nutzbar (Replay Angriffe)

Der Authorization Service MUSS sicherstellen, dass eine Client-Attestation eines Nutzers im Authorization Service mit dem ID-Token nur einmalig für die Aktivierung einer User Session verwendet wird. [≤]

A_25444-01 -Authorization Service - JWT Client Attestation

Der Authorization Service MUSS bei der Authentifizierung einer Leistungserbringerinstitution prüfen, dass das übermittelte JWT der Client Attestierung mindestens die folgenden Inhalte aufweist.

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256" oder "PS256"	
	"x5c"	Signaturzertifikat C.HCI.AUT	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"exp"	Verfalldatum, = "iat" + 20 min	Beispiel: "1705675744"
	"nonce"	Nonce aus einer getNonce Operation	siehe [I_Authorization_Service]

[≤]

Für das Signaturzertifikat zu "x5c" (AUT-Zertifikat der SMC-B) gilt: Basiert der öffentlichen Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

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

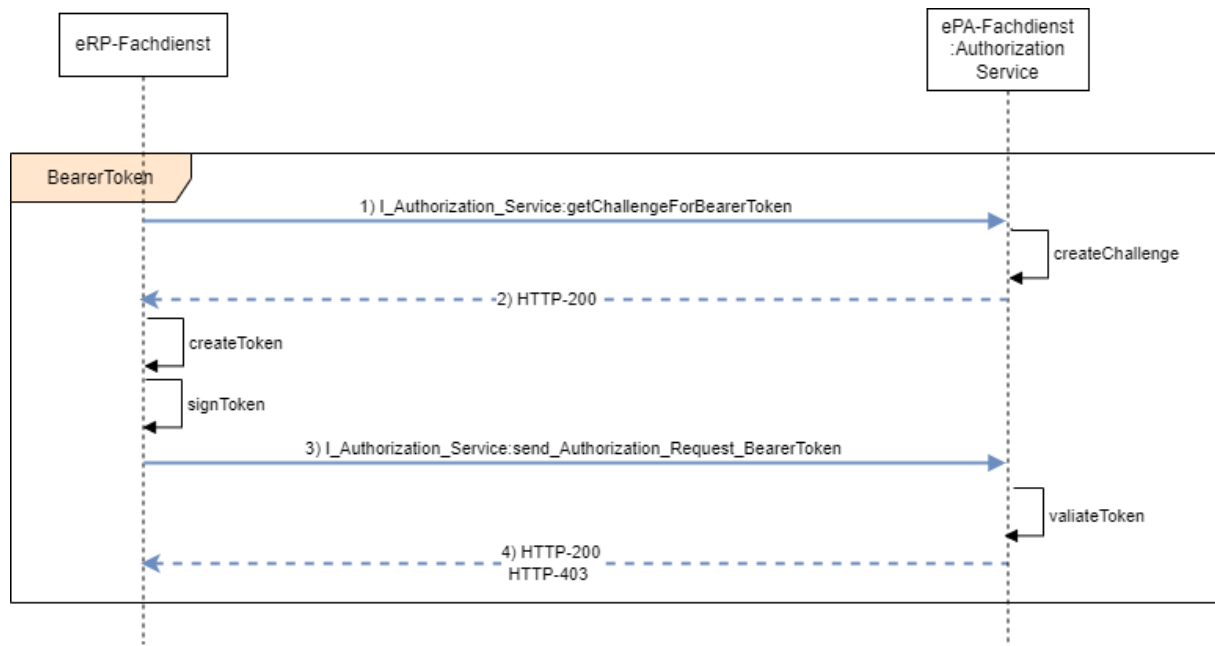


Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes

A_25165-03 -Authorization Service: JWT Bearer-Token des E-Rezept-Fachdienstes

Das Authorization Service MUSS sicherstellen, dass die Authentifizierung des E-Rezept-Fachdienstes über die Schnittstelle `I_Authorization_Service` durch Verwendung eines gültig signierten JWT Bearer Token mit den dargestellten Mindest-Inhalten und Prüfung durch Regel 'rr0' des Befugnisverifikations-Moduls erfolgt. Die Claims in 'Payload' MÜSSEN dazu die Vorgaben aus [gemSpec_Krypt], A_24658* befolgen.

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"

	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Krypt]
	"sub"	Telematik-ID des E-Rezept-Fachdienstes	

6179 [**<=**]

6180 Das Signaturzertifikat zu "x5c" (AUT-Zertifikat der E-Rezept-VAU) kommt aus der
 6181 Komponenten-PKI der TI. Basiert der öffentlichen Schlüssel auf der ECC-Kurve
 6182 brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve
 6183 und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß
 6184 [RFC7515] zu erstellen.

6185 **3.18 Anbindung Verzeichnisdienst FHIR-Directory**

6186 **A_25176 -ePA-Aktensystem - Anbindung Verzeichnisdienst FHIR-Directory**

6187 Das ePA-Aktensystem MUSS bei der Suche des Versicherten nach Einträgen
 6188 im Verzeichnisdienst FHIR-Directory und bei der initialen Anlage einer Akte den
 6189 Anwendungsfall "AF_10219* - Versicherter sucht Einträge im FHIR-Directory" gemäß
 6190 [gemSpec_VZD_FHIR_Directory] als Fachdienst unterstützen und dabei für die Client
 6191 Anfrage von search-access_token die Operation getFHIRVZDtoken gemäß
 6192 [I_Authorization_Service.yaml] bereitstellen. [**<=**]

6193 **3.19 Access Gateway**

6194 Das Access Gateway ermöglicht den Versicherten bzw. deren berechtigten Vertretern den
 6195 Zugang zum zugehörigen Aktensystem über das Internet. Auf der einen Seite dient es
 6196 der Abschottung des ePA-Aktensystems in Richtung Internet, auf der anderen Seite
 6197 regelt es den kontrollierten Zugriff der Versicherten auf das Aktensystem mit seinen
 6198 funktionalen Komponenten.

6199 **3.19.1 Paketfilter**

6200 **3.19.1.1 Funktion**

6201 Der Paketfilter stellt die Anbindung des ePA-Aktensystems an das Internet her und
 6202 gewährleistet die Abschottung des ePA-Aktensystems in Richtung Internet.

6203 **A_14017 -Access Gateway, Sicherung zum Transportnetz Internet durch Paketfilter**

6204 Das ePA-Aktensystem MUSS zum Transportnetz Internet durch einen Paketfilter (ACL)
 6205 gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der
 6206 Paketfilter der Komponente Access Gateway MUSS frei konfigurierbar sein auf der
 6207 Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse,
 6208 IP-Protokoll sowie Quell- und Zielport. [**<=**]

6210 **A_14018 -Access Gateway, Platzierung des Paketfilters Internet**

6211 Der Paketfilter der Komponente Access Gateway, zum Schutz in Richtung Transportnetz
 6212 Internet, DARF NICHT auf den anderen, zum Access Gateway gehörenden, physischen
 6213 Komponenten implementiert werden. [**<=**]

A_14019-02 -Access Gateway, Richtlinien für den Paketfilter zum Internet

Der Paketfilter der Komponente Access Gateway MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

1. HTTPS, und
2. OCSP-Zugriffe für das OCSP-Stapling (vgl. Hinweis nach A_14019-02), ggf. notwendige DNS Anfragen (und Antworten).

Ein Verbindungsaufbau aus dem ePA-Aktensystem über das Access Gateway in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 .[<=]

Hinweis zu A_14019-02: Der Aktensystem-Anbieter muss für seine HTTPS-Schnittstelle ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-Zertifikate also über einen aktuellen Webbrowser prüfbar ist, vgl. A_14776). Für dieses TLS-Zertifikat fragt das Access Gateway (die HTTPS-Schnittstelle ist Teil davon) regelmäßig für das OCSP-Stapling (vgl. [gemSpec_Krypt#A_24913-]) den OCSP-Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält das Access Gateway eine OCSP-Response. Diese wird nach A_19126 geprüft und anschließend von der HTTPS-Schnittstelle verwendet (vgl.*

<https://tools.ietf.org/html/rfc6066#section-8> und bspw. http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling).

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

A_19126-02 -Access Gateway, OCSP-Status für das OCSP-Stapling

Der Paketfilter der Komponente Access Gateway MUSS bezüglich des OCSP-Stapling (vgl.A_24913-*) folgende Vorgaben umsetzen:

1. Für das vom Aktensystem-Anbieter erworbene TLS-Zertifikat (vgl. Hinweis zu A_14019-01) MUSS die Komponente initial die IP-Adresse (ggf. die IP-Adressen) des entsprechenden OCSP-Responers ermitteln.
2. Diese IP-Adresse(n) MÜSSEN gemäß A_14019-01 per stateful-Firewalling Verbindungen von der HTTPS-Schnittstelle an den OCSP-Responder erlaubt werden.
3. Gemäß OCSP-Stapling (<https://tools.ietf.org/html/rfc6066#section-8>) MUSS die Komponente regelmäßig eine OCSP-Response vom entsprechenden OCSP-Responder beziehen (Die Regelmäßigkeit wird vom zertifikatsausgebenden TSP und der Gültigkeitsdauer dessen OCSP-Responses bestimmt).
4. Die OCSP-Responses MÜSSEN von der Komponente geprüft werden (Signaturprüfung, CertID in der OCSP-Response passt zum angefragten Zertifikat). Falls eine der Prüfung ein nicht-positives Ergebnis liefert, so MUSS die erhaltene OCSP-Response verworfen werden.
5. Sollte die letzte in der Komponente vorhandene OCSP-Response zeitlich nicht mehr gültig sein (bspw. der OCSP-Responder im Internet war länger nicht erreichbar), so MUSS diese OCSP-Response verworfen werden und ein von einem Klienten (ePA FdV) initiiertes TLS-Verbindungsaufbau der HTTPS-Schnittstelle ohne OCSP-Stapling durchgeführt werden.

[<=]

A_14776 -Access Gateway, Richtlinien zum TLS-Verbindungsaufbau

Die Komponente Access Gateway MUSS sich beim TLS-Verbindungsaufbau gegenüber dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren. Das Zertifikat MUSS an die Schnittstelle der Proxy-Komponente gebunden werden.[<=]

3.19.1.2 Redundanz

Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf#3.18.1.3]. Die Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Access Gateways.

Die Auswahl der Access Gateways wird durch das ePA-Frontend des Versicherten aus einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des Access Gateways kann der Anbieter des ePA-Aktensystems durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn jeder Versicherte mit existierendem Konto beim Anbieter des ePA-Aktensystems oder dessen berechtigter Vertreter die Möglichkeit zum Verbindungsaufbau hat.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen Access Gateways ist über grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern einzusetzen, so dass jedes einzelne Access Gateway im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

A_14026 -Access Gateway, Redundanz der Paketfilter im Access Gateway

Die Komponente Access Gateway MUSS sicherstellen, dass bei Ausfall eines von mehreren Paketfiltern die verbleibenden Paketfilter in dem-selben Standort den Datenverkehr aller Mandanten des ausgefallenen Paketfilters zusätzlich übernehmen können.[<=]

3.19.1.3 Konfiguration

A_14030 -Access Gateway, Verhalten des Access Gateways bei Vollauslastung

Die Komponente Access Gateway MUSS den Paketfilter Internet so konfigurieren, dass bei Vollauslastung der Systemressourcen im ePA-Aktensystem keine weiteren Verbindungen angenommen werden.[<=]

Durch die Zurückweisung von Verbindungen wird sichergestellt, dass das ePA-Frontend des Versicherten einen Verbindungsaufbau mit einem anderen Access Gateway des jeweiligen ePA-Aktensystems versucht, bei dem die erforderlichen Ressourcen zur Verfügung stehen.

3.19.1.4 Adressierung

3.19.1.4.1 Access Gateway zum Transportnetz Internet

A_14031 -Access Gateway, IPv4-Adressierung der Internetschnittstellen des Access Gateways

Der Anbieter des ePA-Aktensystems MUSS jedem Access Gateway genau eine öffentliche IPv4-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentlichen IP-Adressen des Access Gateways MÜSSEN vom Anbieter des ePA-Aktensystems zur Verfügung gestellt werden.[<=]

A_14032 -Access Gateway, IPv6-Adressierung der Internetschnittstellen des Access Gateways

Der Anbieter des ePA-Aktensystems SOLL jedem Access Gateway eine IPv6-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentliche IPv6-Adresse MUSS vom Anbieter des Access Gateways zur Verfügung gestellt werden.[<=]

6306 3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz

6307 Die Adressen des ePA-Aktensystems am Übergang zur TI werden vom Anbieter des
6308 Zentralen Netzes aus dem Adressblock TI_Zentral zugewiesen.

6309 3.19.2 Proxy für das VAU-Protokoll

6310 Das Access Gateway leitet Anfragen vom ePA-FdV über den VAU-Kanal an die zuständige
6311 VAU-Instanz weiter, damit diese dort in der User Session des Versicherten verarbeitet
6312 werden können.

6313 A_24331 -Access Gateway - Data Proxy

6314 Das Access Gateway MUSS die VAU-Protokoll-Kommunikation des ePA-Frontend des
6315 Versicherten an die zuständige VAU-Instanz weiterleiten. [≤]

6316

6317 3.19.3 Tracing in Nichtproduktivumgebungen

6318 Für die Fehlersuche - insbesondere bei IOP-Problemen zwischen Produkten verschiedener
6319 Hersteller in einer fortgeschrittenen Entwicklungsphase - hat es sich als notwendig
6320 erwiesen, dass ein Fehlersuchender den Klartext der Kommunikation zwischen ePA-Client
6321 und VAU-Instanz mitlesen kann. (vgl. auch 2.5- Tracing in Nichtproduktivumgebungen)

6322 Das Access Gateway stellt Informationen über die aktuell verfügbaren Sensorpunkte im
6323 AS bereit. Weiterhin exponiert das Access Gateway die Daten der Sensorpunkte über TCP
6324 (i. S. v. nicht TLS-gesichert) bspw. über Port 8001,...,8009. Die dort von den
6325 Sensorpunkten ge-streamten Daten sind nur Testdaten, also keine Echtdaten, d. h. sie
6326 haben keinen Schutzbedarf bezüglich Vertraulichkeit. Um die exponierten Sensordaten-
6327 Punkte vor DoS-Angriffen zu schützen, erlaubt das Access Gateway im Fall der Fälle die
6328 TCP-Ports auf IP-Layer über Firewall-Regeln abzusichern.

6329 A_21890-01 -Access Gateway, Sensorpunkt für Nichtproduktivumgebungen

6330 Die Komponente Access Gateway MUSS genau in Nichtproduktivumgebungen:

- 6331 • die Daten der Sensorpunkte des Aktensystems auf TCP-Ports (bspw. ab Port
6332 8000) öffentlich (ggf. auch ohne TLS-Sicherung) im Internet zur Verfügung
6333 stellen, indem die aktuell an den Sensorpunkten auflaufenden Daten auf dem
6334 TCP-Port am Access Gateway öffentlich gestreamt werden.
- 6335 • die Möglichkeit bieten, den Zugriff auf diese TCP-Ports durch Firewall-
6336 Einstellungen auf IP-Layer zu beschränken.

6337 Weiterhin MUSS das Access Gateway über die URL /tracingpoints Informationen über die
6338 aktuell im AS verfügbaren und damit auch im Access Gateway öffentlich exponierten
6339 Sensorpunkt-Daten als JSON-Array (=> Response-Type 'application/json') der folgenden
6340 Form bereitstellen:

```
6341 [
6342 {"name" : "zentraler Tigerproxy",
6343  "port" : 8001,
6344  "DoS-protection-type" : „secret_url“
6345  "DoS-protection-port" : „udp/46789“
6346 },
6347 {"name" : "Extra Senor VAU RZ2/B1/R1",
6348  "port" : 8002,
6349  "DoS-protection-type" : „ssh_tunnel“
6350  "DoS-protection-port" : „tcp/46790“
6351 }, ...
```

6352]
 6353 Sollten keine Sensorpunkte aktuell im AS aktiviert sein (bspw. bei Lasttests) so ist das
 6354 Array leer: [].
 6355 Sollte es keinen optionalen DoS-Schutzmechanismus gemäß A_22582-* geben, so fallen
 6356 die DoS-* Attribute in der o. g. Datenstruktur weg (sind nicht existent).
 6357 Die einzelnen Felder des Arrays sind associative array (oder auch maps oder dictionaries
 6358 genannt). Diese KÖNNEN neben "name" und "port" beliebige vom AS definierbare,
 6359 weitere key-value-Paare enthalten. Der Eintrag "port" gibt an, an welchem öffentlich
 6360 erreichbaren TCP-Port des Access Gateway die Sensordaten des entsprechenden Sensors
 6361 abrufbar sind (gestreamt werden).
 6362 [**<=**]

6363 *Hinweis zu A_21890-*: Die semistatische JSON-Datei, welche ein Client unter dem Pfad*
 6364 *„/tracingpoints“ erhalten kann, ist eine einfache Form von Service-Discovery. Damit kann*
 6365 *ein Client (Fehlersuchende(r)) erfahren, welche Tracing-Quellen es aktuell im AS gibt i.*
 6366 *S. v. welche Tracing-Quellen ein Client zur Fehlersuche aktuell verwenden kann.*

6367 **A_22582 -Tracing in Nichtproduktivumgebungen, DoS-Schutz**

6368 Die Komponente Access Gateway KANN Sicherheitsmechanismen bereitstellen und
 6369 aktivieren, die es genau in Nichtproduktiv-umgebungen ermöglichen, temporär,
 6370 automatisiert und nur nach erfolgreicher Authentifizierung die TCP-Ports für das
 6371 Streaming der Sensorpunkte für Clients nach A_21890-* freizuschalten.**[<=]**

6372 *Hinweis zu A_22582-*: In den Nichtproduktivumgebungen darf es keine Echt Daten*
 6373 *geben. Es dürfen sich dort nur Daten befinden, deren Schutzbedarf bezüglich*
 6374 *Vertraulichkeit niedrig ist. Der optionale Schutzmechanismus nach A_22582-* braucht*
 6375 *nur einen einfachen DoS-Schutz leisten gegen einen Angreifer mit niedrigen*
 6376 *Angriffspotential. Der Anbieter ist, sofern er einen solchen Mechanismus einsetzen*
 6377 *möchte, frei, dafür den Mechanismus selbst zu wählen. Er wählt dann bei "DoS-*
 6378 *protection-type" (vgl. A_21890-*) einen selbstdefinierten (möglichst sprechenden)*
 6379 *Namen.*

6380 Beispiele für Umsetzungsmöglichkeiten:

- 6381 1. Es gibt im Access Gateway eine geheime URL (bspw.
 6382 /tracing/964b059de83d20581f43dd1b867d740c). Ein Client kennt das Geheimnis
 6383 und ruft diese URL auf. Daraufhin wird im Access Gateway für die IP-Adresse des
 6384 Clients die Tracing-Quelle im Access Gateway frei geschaltet (TCP-Port 8000, ...).
- 6385 2. Die gematik stellt eine Beispielimplementierung zur Verfügung. Dort gibt es einen
 6386 UDP-Server (Access Gateway) und einen UDP-Client (Fehlersuchende), die beide
 6387 ein gemeinsames HMAC-Geheimnis teilen. Wenn der Client die aktuelle Zeit und
 6388 dessen IP-Adresse per HMAC authentisiert dem UDP-Server sendet, so schaltet
 6389 der UDP-Server nach erfolgreicher Prüfung des HMACs den entsprechenden TCP-
 6390 Port für die authentifizierte IP-Adresse des Clients frei.
- 6391 3. Auf dem Access Gateway läuft ein SSH-Daemon. Der öffentliche
 6392 Authentisierungsschlüssel eines Clients ist dort als gültiger Nutzer konfiguriert
 6393 (Login-Shell: /bin/false). Die Tracing-Quellen im Access Gateway sind so
 6394 konfiguriert, dass sie nur mittels authentisierten SSH-Port-Forwarding
 6395 (<https://www.ssh.com/academy/ssh/tunneling/example>) erreichbar sind.

6396 **3.19.4 Übergreifende Festlegungen**

6397 **A_14249 -Komponente Access Gateway - Separierung der Schnittstellen für**
 6398 **verschiedene Umgebungen**

- 6399 Die Komponente Access Gateway MUSS die Bereitstellung von Schnittstellen für die
6400 Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen
6401 Umgebungen der TI (RU/TU, PU) sicherstellen und voneinander separieren. [<=]
- 6402 **A_14034 -Access Gateway, Übergang des ePA-Aktensystems zur TI**
6403 Die Komponente Access Gateway MUSS sicherstellen, dass der Zugriff auf Dienste der TI
6404 ausschließlich über einen Sicheren Zentralen Zugangspunkt (SZZP) erfolgt. [<=]
- 6405 **A_14036 -Access Gateway, Synchronisierung der Komponenten mit den**
6406 **Stratum-1-NTP-Servern der TI**
6407 Die Komponente Access Gateway MUSS alle Komponenten seines Access Gateways mit
6408 den Stratum-1-NTP-Servern der TI synchronisieren. [<=]
- 6409 **A_13879 -Access Gateway, Serverseitige Authentisierung**
6410 Die Komponente Access Gateway MUSS sich gegenüber dem ePA-Frontend des
6411 Versicherten beim Aufbau der TLS-Session durch sein ExtendedValidation-
6412 Zertifikat authentisieren. Die Beschaffung des Zertifikats erfolgt durch den Anbieter über
6413 eine öffentliche CA. [<=]
- 6414 **A_14033 -Access Gateway, TLS Verschlüsselung**
6415 Die Komponente Access Gateway MUSS sicherstellen, dass jede Kommunikation mit dem
6416 ePA-Frontend des Versicherten TLS verschlüsselt erfolgt. [<=]
- 6417 Die Verwendung der SoapAction ermöglicht einer Reverse-Proxy-Komponente innerhalb
6418 des Access Gateways, die Nachrichten zu verarbeiten, ohne die http-Payload zu
6419 untersuchen.
- 6420 **A_13876 -Access Gateway, Kein direkter Zugriff auf Dienste der zentralen TI-**
6421 **Plattform**
6422 Die Komponente Access Gateway MUSS einen direkten Zugriff aus dem Internet auf
6423 Dienste der zentralen TI-Plattform verhindern. [<=]
- 6424 **A_14016 -Access Gateway , Schutz vor Angriffen aus dem Internet**
6425 Die Komponente Access Gateway MUSS für alle vom Internet erreichbaren Schnittstellen
6426 Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere
6427 Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS
6428 Lösungen verhindert werden. [<=]
- 6429 **A_15196 -Access Gateway, Schutz vor volumetrischen DoS-Angriffen**
6430 Die Komponente Access Gateway MUSS bei Beauftragung eines qualifizierten
6431 Dienstleisters zum Schutz vor volumetrischen DoS-Angriffen Kriterien des BSI zur
6432 Auswahl qualifizierter Dienstleister umsetzen. [<=]
- 6433 Als Maßnahme gegen volumetrische Denial-of-Service-Angriffe wird die Verwendung von
6434 DNS- oder BGP-Routing-Diensten empfohlen. Hinweise des BSI:
6435 [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-Gefahren/DDoS/ddos_node.html)
6436 [und-Empfehlungen/Empfehlungen-nach-Gefahren/DDoS/ddos_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/DDoS/ddos_node.html).

6437 3.20 Data Submission Service

- 6438 Die Daten der elektronischen Patientenakten sollen nach § 363 Absatz 1 SGB V für die in
6439 § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszwecke zugänglich gemacht und
6440 hierfür in pseudonymisierter Form automatisiert von den ePA-Aktensystemen an das
6441 Forschungsdatenzentrum Gesundheit (FDZ) nach § 303d SGB V übermittelt werden,
6442 sofern Versicherte dem nicht widersprochen haben.
- 6443 Neben dem FDZ und den ePA-Aktensystemen ist die Vertrauensstelle (VST) nach § 303c
6444 SGB V im Prozess involviert. Deren Aufgabe ist es, die von den ePA-Aktensystemen

6445 erhaltenen Lieferpseudonyme in periodenübergreifende Pseudonyme umzuwandeln und
6446 diese an das FDZ zu übermitteln.

6447 Der Data Submission Service im Aktensystem übernimmt in der Übermittlung der
6448 pseudonymisierten medizinischen Daten folgende Aufgaben:

- 6449 • Erstellung der Lieferpseudonyme (auf Basis der KVNR) und der Arbeitsnummern
- 6450 • Registrierung der Arbeitsnummer mit dem zugehörigen Lieferpseudonym bei der
- 6451 Vertrauensstelle
- 6452 • Pseudonymisierung der medizinischen Daten
- 6453 • Verknüpfung der pseudonymisierten medizinischen Daten mit der Arbeitsnummer
- 6454 • Übermittlung der pseudonymisierten medizinischen Daten und der zugehörigen
- 6455 Arbeitsnummern an das Forschungsdatenzentrum Gesundheit

6456 Die Übermittlung der Daten erfolgt blockweise. D.h. es wird ein Paket von
6457 pseudonymisierten medizinischen Daten mit zugehörigen Arbeitsnummern aus
6458 verschiedenen Aktenkonten zusammengestellt (Datenpaket FDZ) und alle für dieses
6459 Paket benötigten Arbeitsnummern und Lieferpseudonyme mit einem Mal bei der VST
6460 registriert (Datenpaket VST). Die Datenpakete haben eine anbieterübergreifend
6461 eindeutige SubmissionID und die SubmissionID zusammengehöriger Datenpakete VST
6462 und FDZ ist identisch.

6463 Für die Übermittlung wird zwischen Aktensystem und VST, sowie Aktensystem und FDZ
6464 jeweils ein beidseitig authentisierter VAU-Kanal aufgebaut, auf dem sich die Dienste VST
6465 und FDZ mit einer Identität ID.FD.AUT mit ihren entsprechenden Rollen authentisieren.

6466 Der Versicherte kann mit Hilfe seines ePA-FdVs oder über die Ombudsstelle des
6467 Kostenträgers der Übermittlung seiner pseudonymisierten medizinischen Daten an das
6468 FDZ widersprechen oder die möglichen Sekundärnutzungszwecke seiner übermittelten
6469 pseudonymisierten medizinischen Daten im FDZ einschränken. Dies erfolgt über das
6470 Consent Decision Management im Aktensystem.

6471 **3.20.1 Erstellung von Arbeitsnummern und Lieferpseudonymen**

6472 Der Data Submission Service erzeugt eindeutige Arbeitsnummern und Lieferpseudonyme,
6473 um die pseudonymisierten medizinischen Daten in der Übermittlung an das FDZ eindeutig
6474 zuordnen zu können.

6475 **A_26211 -Data Submission Service - Erstellung des Lieferpseudonyms**

6476 Der Data Submission Service MUSS das Lieferpseudonym des Versicherten gemäß
6477 [I_VST] unter Verwendung der KVNR des Versicherten erstellen.[<=]

6478 **A_26409 -Data Submission Service - keine Erstellung von LP für** 6479 **Validierungsaktenkonten**

6480 Der Data Submission Service DARF KEINE Lieferpseudonyme für KVNRn
6481 von Validierungsaktenkonten erstellen.[<=]

6482 **A_26212 -Data Submission Service - Erstellung der Arbeitsnummer**

6483 Der Data Submission Service MUSS für die Arbeitsnummer einen Zufallswert mit einer
6484 Mindestentropie von 120 Bit erzeugen und die Kodierung aus [I_VST] verwenden.[<=]

6485 **A_26410 -Data Submission Service - keine Erstellung von AN für** 6486 **Validierungsaktenkonten**

6487 Der Data Submission Service DARF KEINE Arbeitsnummern für Daten
6488 aus Validierungsaktenkonten erstellen.[<=]

A_26255 -Data Submission Service - Verwendungsdauer von Lieferpseudonymen und Arbeitsnummern

Der Data Submission Service MUSS für jedes in einem Datenpaket FDZ übermittelte pseudonymisierte medizinische Datum zu einer KVNR eine neue Arbeitsnummer und ein neues Lieferpseudonym generieren. [≤]

A_26256 -Data Submission Service - Registrierung von Arbeitsnummern

Der Data Submission Service MUSS jede Arbeitsnummer zusammen mit dem zugehörigen Lieferpseudonym in das entsprechende Datenpaket VST aufnehmen und an die Vertrauensstelle übermitteln. [≤]

3.20.2 Auswahl von medizinischen Daten

Der Data Submission Service muss bestimmte neue und geänderte FHIR-Ressourcen an den FDZ übertragen. Dies betrifft im ersten Schritt die Medikationsdaten aus der E-Medikationsliste und wird subsequent weiter ausgebaut.

Der Medication Service, als Quelle der Medikationsdaten zur Übertragung an den FDZ, erlaubt flexible, datenbasierte Operationen auf einzelnen FHIR-Ressourcen. Dies erfordert entsprechende Implementierung um effizient und zuverlässig die neuen und geänderten Ressourcen identifizieren können um daraus die Auswahl für die zu übertragende FHIR-Ressourcen treffen zu können.

A_26296 -Data Submission Service - Übertragung neuer und geänderter FHIR-Ressourcen

Der Data Submission Service MUSS neue und geänderte FHIR-Ressourcen identifizieren können und daraus die Auswahl für die Übermittlung der Daten an FDZ treffen können. [≤]

A_26297 -Data Submission Service - Einschränkung der FHIR-Ressourcen nach Änderungsdatum

Der Data Submission Service MUSS den Zeitpunkt der letzten Übermittlung (lastSubmissionTimestamp) merken und in nachfolgenden Übermittlungen nur die Ressourcen, die sich seit diesem Zeitpunkt geändert haben, berücksichtigen. Hierfür ist das FHIR-Element meta.lastUpdated in der jeweiligen FHIR-Ressource zu verwenden. [≤]

Hinweis: Ressourcen, die im Rahmen eines Anbieterwechsels in ein Aktenkonto übernommen werden, sind nicht erneut zu übermitteln.

A_26298 -Data Submission Service - FHIR-Ressourcen zur Übermittlung an FDZ

Der Data Submission Service MUSS die FHIR-Ressourcen gemäß der Tabelle "Auswahl der zu übertragenden FHIR-Ressourcen" an FDZ übertragen, dabei sind die Filter-Bedingungen (Spalte 'Filter Expression') und zu inkludierende referenzierte Ressourcen zu berücksichtigen (Spalte 'Include' sowie Tabelle "Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen"). [≤]

Tabelle 44: Auswahl der zu übertragenden FHIR-Ressourcen

Ressourcentyp /Profil	Filter Expression	Include
MedicationRequest \${epa-	status != 'active' and identifier.where(system='https://gematik.de/fhir/epa-medication/sid/rx-prescription-process-	MedicationRequest:medication

medication}/e pa- medication- request	identifizier').hasValue()	
MedicationDisp ense \${epa- medication}/e pa- medication- response	status != 'in-progress' and extension('https://gematik.de/fhir/epa- medication/StructureDefinition/rx- prescription-process-identifizier- extension').hasValue()	MedicationDispense:me dication

6529

6530

Tabelle 45: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen

Ressourcentyp/Profil	Anmerkung
Medication \${epa-medication}/epa- medication	Referenziert durch MedicationRequest, MedicationDispense

6531

6532

3.20.3 Protokollierung des Datenexports an das FDZ

6533

6534

6535

6536

Ein Datenexport erfolgt immer in Verbindung mit dem Einstellen neuer oder der Änderung existierender Daten für ein Aktenkonto. Ein Datenexport nach Auswahl der Daten gemäß A_26298 wird als Bestandteil der Protokollierung des auslösenden Ereignisses protokolliert (siehe dazu: 3.13.2.2- Medication Service)

6537

3.20.4 Pseudonymisierung von medizinischen Daten

6538

6539

Bevor medizinische Daten an das FDZ übermittelt werden dürfen, müssen diese pseudonymisiert werden und Daten mit direktem Personenbezug entfernt werden.

6540

6541

A_26300 -Data Submission Service - Pseudonymisierung von medizinischen Daten

6542

6543

Der Data Submission Service MUSS an das FDZ zu übermittelnde medizinische Daten gemäß der Vorgaben aus [DataPseudonymization] pseudonymisieren. [\leq]

6544

6545

A_26408 -Data Submission Service - keine Pseudonymisierung von Daten aus Validierungsaktenkonten

6546

6547

Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem. Kapitel 2.4) pseudonymisieren. [\leq]

6548

6549

A_26315 -Data Submission Service - Randomisierung der Reihenfolge des Datenpakets FDZ

6550

6551

6552

6553

Das ePA-Aktensystem MUSS sicherstellen, dass in einem Datenpaket FDZ vor der Übermittlung die Einträge nach Arbeitsnummer (AN) aufsteigend sortiert werden. Die Arbeitsnummer (32-Byte Zufallswert, A_26212-*) wird dabei als natürliche Zahl (byteorder=big) interpretiert. [\leq]

6554

Verständnishinweis:

6555 Die Akten werden regelmäßig nach zu übermittelnden Daten vom ePA-Aktensystem
6556 durchsucht. Dabei kann es passiert, dass in einer Akte mehrere Daten zur Übermittlung
6557 anfallen, die nach der Pseudonymisierung in einer Reihenfolge in das Datenpaket FDZ
6558 gelangen. Deshalb kann die Reihenfolge der Einträge im Datenpaket FDZ statistisch
6559 relevante Informationen über den Zusammenhang von Einträgen geben. Durch eine
6560 Randomisierung der Reihenfolge der Einträge innerhalb des Datenpakets wird dies
6561 verhindert. Die AN werden zufällig erzeugt, eine Sortierung nach AN ist deshalb eine
6562 Randomisierung der Reihenfolge.

6563 **3.20.5 Übermittlung der pseudonymisierten medizinischen Daten**

6564 Die Übermittlung von Datenpaketen an VST und FDZ erfolgt gemäß den Vorgaben des
6565 RKI (VST) und BfArM (FDZ) und deren Schnittstellenspezifikationen.

6566 Die Übermittlung der pseudonymisierten Daten eines Aktenkontos für
6567 Sekundärnutzungszwecke erfolgt automatisch, sofern kein Widerspruch gegen
6568 Sekundärdatennutzung vorliegt. Die Voreinstellung ist dabei "kein Widerspruch erteilt"
6569 (siehe: 3.8.1- Widersprüche für Funktionen der ePA). Vor der allerersten Übermittlung
6570 solcher Daten wird dem Versicherten daher eine Frist gewährt, gegebenenfalls einen
6571 Widerspruch gegen diese Sekundärdatennutzung zu formulieren.

6572 **A_26462 -Data Submission Service - Übermittlung Datenpaket nach Ablauf der** 6573 **Widerspruchsfrist**

6574 Der Data Submission Service MUSS sicherstellen, dass vor der erstmaligen Übermittlung
6575 von Daten eines Aktenkontos die Widerspruchsfrist gemäß den Vorgaben des
6576 Kostenträgers abgelaufen ist. [<=]

6577 Hinweis: Die erste Datenübermittlung ist die erste automatisiert mögliche Übermittlung
6578 (nach Aktivierung des Aktenkontos) und nicht die erste Datenübermittlung nach
6579 Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung.

6580 HInweis: Für eine Übermittlung nach Ablauf dieser Widerspruchsfrist oder nach
6581 Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung werden immer nur ab
6582 diesem Zeitpunkt neu angefallene Daten berücksichtigt, Es erfolgt keine Übermittlung
6583 von vorhandenen Daten des Aktenkontos.

6584 **A_26214 -Data Submission Service - Erstellung der SubmissionID**

6585 Der Data Submission Service MUSS für zusammengehörige Datenpakete VST und FDZ
6586 eine gemeinsame anbieterübergreifend eindeutige SubmissionID erzeugen und diese mit
6587 den Datenpaketen übertragen. [<=]

6588 **A_26304 -Data Submission Service - Zufällige SubmissionID**

6589 Der Data Submission Service MUSS sicherstellen, dass die SubmissionID ein zufällig
6590 gewählter 256-Bit Wert mit einer Mindestentropie von 120 Bit ist. [<=]

6591 **A_26215 -Data Submission Service - Übermittlung Datenpaket VST**

6592 Der Data Submission Service MUSS das Datenpaket VST gemäß [I_VST] an die
6593 Vertrauensstelle übermitteln. [<=]

6594 **A_26407 -Data Submission Service - keine Übermittlung von Daten aus** 6595 **Validierungsaktenkonten**

6596 Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem.
6597 Kapitel 2.4) an das Forschungsdatenzentrum übermitteln. [<=]

6598 **A_26216 -Data Submission Service - Realisierung der Schnittstelle**

6599 **I_Data_Submission_Service**

6600 Der Data Submission Service MUSS die Operationen der Schnittstelle
6601 I_Data_Submission_Service gemäß [I_Data_Submission_Service] umsetzen. [<=]

A_26217 -Data Submission Service - Verbindung zur Vertrauensstelle

Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des Datenpakets VST ausschließlich über einen VAU-Kanal erfolgt in dem sich die Vertrauensstelle über ein Zertifikat C.FD.AUT mit professionOID gleich oid_epa_vst authentisiert hat. [<=]

A_26218 -Data Submission Service - Verbindung zum Forschungsdatenzentrum Gesundheit

Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des Datenpakets FDZ ausschließlich über einen VAU-Kanal erfolgt in dem sich das Forschungsdatenzentrum Gesundheit über ein Zertifikat C.FD.AUT mit professionOID gleich oid_epa_fdz authentisiert hat. [<=]

A_26299 -Data Submission Service - Wechsel des Verschlüsselungsschlüssels für Datenpakete

Falls die Datenpakete VST und FDZ außerhalb der VAU im System des Aktensystembetreibers gespeichert werden, MUSS der Data Submission Service sicherstellen, dass ein Schlüssel für die Verschlüsselung der Datenpakete VST bzw. FDZ maximal 4 Wochen genutzt werden kann und danach ein neuer Verschlüsselungsschlüssel mittels der Regel hsm-r8 mit Hilfe eines geänderten Ableitungsvektors abgeleitet wird. [<=]

A_26312 -Data Submission Service - Timeout in der Übermittlung

Der Data Submission Service MUSS die Übermittlung der Pakete VST und FDZ erneut starten, wenn das Datenpaket FDZ nicht innerhalb von 30 Minuten nach erfolgreicher Übermittlung des Datenpakets VST abgerufen wird. [<=]

A_26313 -Data Submission Service - Konfiguration der Intervalle und maximalen Größe eines Datenpakets

Der Data Submission Service MUSS folgende Parameter konfigurierbar gestalten:

- das Intervall in dem Datenpakete VST und FDZ übermittelt werden
- eine maximale Größe eines Datenpakets FDZ bei deren Erreichen die Datenpakete übermittelt werden

[<=]

A_26244 -Data Submission Service - Löschen von Datenpaketen nach Übermittlung

Der Data Submission Service MUSS nach erfolgreicher Übermittlung des Datenpakets FDZ an das Forschungsdatenzentrum Gesundheit das übermittelte Datenpaket FDZ und das zugehörige Datenpaket VST lokal löschen. [<=]

A_26245 -Data Submission Service - Löschen von Datenpaketen bei Nicht-Übermittlung

Der Data Submission Service MUSS das Datenpaket FDZ und das zugehörige Datenpaket VST lokal löschen, wenn das Datenpaket FDZ länger als 72 Stunden nicht an das Forschungsdatenzentrum Gesundheit übermittelt werden konnte. Die enthaltenen Widersprüche MÜSSEN in die aktuell in Erstellung befindlichen Datenpakete VST und FDZ übernommen werden. [<=]

Hinweis: Wenn Widersprüche in ein neues Datenpaket übernommen werden, muss für jeden der Widersprüche eine neue Arbeitsnummer (AN) und ein Lieferpseudonym (LP) erstellt werden, da die bisherigen AN und LP im Kontext des zu löschenden Paketes stehen.

A_26246 -Data Submission Service - Aufnahme von Widersprüchen

Der Data Submission Service MUSS Widersprüche gegen die Freigabe von Daten zur Sekundärnutzung durch das FDZ oder Änderungen zu Sekundärnutzungszwecken, aus

dem Consent Decision Management, in die aktuell in Erstellung befindlichen Datenpakete VST und FDZ übernehmen. Es MUSS sichergestellt werden, dass in einem Datenpaket FDZ für eine KVN immer nur die zuletzt erklärten Widersprüche gegen die Übermittlung von Daten zur Sekundärnutzung durch das FDZ bzw. zu Sekundärnutzungszwecken enthalten sind. [≤]

Hinweis: Sollte während der Erstellung eines Datenpakets FDZ mehrfach die Widersprüche für eine KVN geändert werden, wird immer nur der letzte Stand übermittelt.

A_26307 -Data Submission Service - Durchsetzung von Widersprüchen

Falls für ein Aktenkonto ein Widerspruch gegen die Übermittlung an das FDZ eingestellt wird, MUSS der Data Submission Service sicherstellen, dass in allen zukünftig zu übermittelnden Datenpaketen VST und FDZ außer den Daten für den Widerspruch keine Daten für dieses Aktenkonto enthalten sind.

[≤]

Hinweis zu A_26307: Zum Zeitpunkt des Eingangs des Widerspruchs im Aktensystems bereits in der Übermittlung befindliche Datenpakete sind von der Anforderung ausgeschlossen. Betroffen sind jedoch auch die aktuell in Erstellung befindlichen Datenpakete VST und FDZ, bei denen die Übermittlung an die VST bzw. das FDZ noch nicht begonnen hat.

3.21 Push Notification Management

Nutzer von Anwendungen für Versicherte (ePA-FdV) können mittels Push Notifications direkt über Ereignisse in bestimmten Fachdiensten der TI oder des Kostenträgers auf ihren Endgeräten informiert werden. Diese Notifications erreichen einen Nutzer auch außerhalb aktiver Anmeldungen in diesen Fachdiensten. Die Ereignisse von Interesse zur Benachrichtigung des Nutzers sind dabei individuell abonnierbar.

Der Versand einer Push Notification erfolgt stets durch die einzelnen Fachdienste für Ereignisse ihrer Domäne. Die Übertragung in das Endgerät des Nutzers unter Einbindung der plattformspezifischen, externen Push-Dienste und betreiberspezifischen Push-Gateways wird für alle beteiligten Fachdienste gemeinsam durch ein Push Notification System realisiert. Dieses anwendungsübergreifende System und seine Komponenten für Push Notifications im Gesundheitswesen sind in [gemF_PushNotification] und [PushNotificationConcept] detailliert beschrieben.

Dort sind auch die normativen Vorgaben für unterstützende Anwendungen und Fachdienste in Bezug auf Registrierung von Applikationen und Ereignissen für Push Nachrichten, Schnittstellen, sicherheitstechnische Anforderungen und notwendige Artefakte für einen interoperablen Betrieb formuliert.

3.21.1 Push Notification Management des ePA-Aktensystems

Das Push Notification Management des ePA-Aktensystems ist als ein spezifischer Fachdienst in dieses übergreifende System eingebunden und bedient die in [gemF_PushNotification] geforderten und in [PushNotificationConcept] beschriebenen Schnittstellen und Verfahren.

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

6695 Der Nutzung des Push Notification Managements der ePA kann nicht widersprochen
6696 werden. Dieser Dienst gehört nicht zu den widerspruchsfähigen Funktionen der ePA.
6697 Versicherte, die keine Benachrichtigungen der ePA erhalten möchten, können die
6698 Benachrichtigungen durch Abwahl der Benachrichtigungskanäle oder auch generell durch
6699 den Verzicht des ePA-FdV auf eine Registrierung für Push Notifications unterbinden.

6700 Schnittstellen, die das Push Notification Management der ePA zur Nutzung durch Clients
6701 (ePA-FdV) anbietet, sind um ePA-spezifische Verfahren und Anforderungen ergänzt und
6702 als OpenApi gemäß [I_Push_Notification_Management] verfügbar.

6703 **A_27637 -Push Notification Management - Realisierung der Schnittstelle** 6704 **I_Push_Notification_Management**

6705 Das Push Notification Management MUSS die Operationen der Schnittstelle
6706 I_Push_Notification_Management gemäß [I_Push_Notification_Management]
6707 umsetzen.[<=]

6708 **3.21.2 Registrierung eines ePA-FdV als Pusher**

6709 (siehe auch: [gemF_PushNotification]#Kapitel "Pusher registrieren")

6710 Ein Versicherter kann registrierte Geräte (im Sinne des Device Managements gemäß 3.12.
6711 Device Management) zur Nutzung seiner aktivierten elektronischen Patientenakte auch
6712 für den Erhalt von Push Nachrichten nutzen, sofern das übergreifende Push Notification
6713 System die technologische Infrastruktur für Benachrichtigungen an den Geräte-, bzw.
6714 Betriebssystemtyp des Versichertengeräts unterstützt. Dazu kann die ePA-FdV-
6715 Anwendung jedes dieser Geräte als ePA-FdV Instanz, bzw. 'Pusher', im eigenen
6716 Aktenkonto des Versicherten registriert werden.

6717 Die ePA-FdV Instanz Registrierung eines Gerätes als Pusher erfolgt immer durch und für
6718 das auf diesem Gerät installierte ePA-FdV und unter Nutzung der Schnittstelle
6719 [I_Push_Notification_Management]. Über diese Schnittstelle werden existierende
6720 Registrierungen auch aktualisiert und wieder entfernt.

6721 Die Daten der Registrierungen, inklusive des kryptographischen Materials der
6722 Schlüsselableitungen und der Auswahl der Benachrichtigungskanäle, sind Bestandteil des
6723 Aktenkontos und werden dort gespeichert. Pro registriertem Gerät kann jeweils nur eine
6724 ePA-FdV Instanz im Aktenkonto hinterlegt sein und eine Registrierung gilt immer nur für
6725 genau eine bestimmte ePA-FdV Instanz. Eine ePA-FdV Instanz Registrierung ist daher
6726 fest an eine Device Registration gebunden.

6727 **A_27638 -Push Notification Management- Speicherung der Daten**

6728 Das Push Notification Management MUSS alle Daten des Dienstes für einen Versicherten
6729 im SecureDataStorage des Aktenkontos des Versicherten speichern.[<=]

6730 **A_27640 -Push Notification Management - automatisches Löschen der** 6731 **Registrierung einer ePA-FdV Instanz**

6732 Das Push Notification Management MUSS sicherstellen, dass eine existierende
6733 Registrierung einer ePA-FdV Instanz und die dazugehörigen Daten vollständig und
6734 automatisch gelöscht werden, wenn die Device Registration des assoziierten Geräts im
6735 Device Management des Aktensystems gelöscht wird.[<=]

6736 **A_27639 -Push Notification Management - eindeutiger pushKey**

6737 Das Push Notification Management MUSS sicherstellen, dass der `pushKey` einer
6738 Registrierung einer ePA-FdV Instanz eindeutig ist und es keine zwei oder mehr
6739 Registrierungen mit gleichem `pushKey` gibt.[<=]

6740 Bei jedem Versand einer Push Nachricht an das Push Gateway kann dieses in den
6741 Rückgabewerten der Push Operation einen Eintrag oder eine Liste veralteter, bzw.

6742 ungültiger `pushKeys` melden. Eine weitere Nutzung solcher Registrierungen, bzw.
 6743 `pushKeys`, soll unterbleiben. Die assoziierten Registrierungen von ePA-FdV-Instanzen
 6744 werden daher aus dem Aktenkonto entfernt.

6745 **A_27682 -Push Notification Management - Entfernen ungültiger `pushKeys`**
 6746 Das Push Notification Management MUSS Registrierungen von ePA-FdV-Instanzen
 6747 löschen, wenn `pushKeys` dieser Registrierungen durch das Push Gateway als ungültig
 6748 gemeldet werden. [`<=`]

6749 *Hinweis: Es werden nur Registrierungen aus dem versendenden Aktenkonto entfernt.*
 6750 *Ebventuelle Rückmeldungen des Push Gateways zu `pushKeys`, die nicht oder nicht mehr*
 6751 *mit dem versendenden Aktenkonto verbunden sind, werden ignoriert.*

6752 3.21.3 Push Notification Channels

6753 (siehe auch: [`gemF_PushNotification`]#Kapitel "Channel/ Trigger Konfiguration")

6754 Das ePA-Aktensystem bietet eine Auswahl an Channels zu Ereignissen, über deren
 6755 Aktivität ein Versicherter durch Push-Benachrichtigungen informiert werden kann. Der
 6756 jeweilige Nachrichteninhalt beschreibt dabei in Kurzform das auslösende Ereignis.

6757 Die Grundeinstellung für den Versand von Push-Benachrichtigungen an neu erstellten
 6758 Registrierungen für ePA-FdV-Instanzen lautet für jeden Channel zunächst deaktiviert
 6759 ('disabled' - keine Benachrichtigung für diesen Kanal). Ein Versicherter kann diese
 6760 Grundeinstellung individuell für jede seiner ePA-FdV-Instanzen jederzeit ändern und die
 6761 Benachrichtigung pro Channel aktivieren ('enabled' - Benachrichtigungen für diesen
 6762 Kanal), bzw. auch wieder deaktivieren.

6763 Die Verwaltung der individuellen Channelkonfiguration des ePA-Aktenkontos für eine
 6764 registrierte ePA-FdV-Instanz erfolgt über die Schnittstelle
 6765 [`I_Push_Notification_Management`].

6766 **A_27641-01 -Push Notification Management - Push Notification Channels**
 6767 Das Push Notification Management MUSS ausschließlich für die folgenden Ereignisse Push
 6768 Nachrichten erstellen können, wenn das Ereignis durch einen Nutzer der definierten
 6769 Nutzergruppe ausgelöst wird und die damit verbundene Operation erfolgreich (nicht
 6770 durch einen Fehler abgebrochen) ist.
 6771

Ereignis	channelId	Beschreibung	Nutzergruppen
Neues Dokument eingestellt	xds.put	Ein Dokument wurde durch einen Nutzer neu eingestellt.	alle, außer Versicherter
Dokument aktualisiert	xds.update	Ein aktualisiertes Dokument wurde durch einen Nutzer eingestellt.	alle, außer Versicherter
Befugnis erstellt	entitle.put	Eine Befugnis wurde durch das ePA-FdV erstellt.	nur Vertreter
Befugnis gelöscht	entitle.del	Eine existierende Befugnis wurde durch das ePA-FdV gelöscht.	nur Vertreter

Befugniserstellung im Behandlungskontext	entitle.ps	Eine Befugnis wurde mittels VSDM-Prüfnachweis, bzw. PoPP, erstellt.	alle, außer FdV Nutzer
Verbergen aufgehoben (Dokument)	constraint.del	Ein zuvor verborgenes Dokument ist wieder sichtbar.	nur Vertreter
Verbergen aufgehoben (dynamischer Ordner)		Ein zuvor verborgener dynamischer Ordner ist wieder sichtbar.	nur Vertreter
Verbergen aufgehoben (Kategorie)		Eine zuvor verborgene Kategorie wieder sichtbar.	nur Vertreter

6772 [**<=**]6773 **3.21.4 Push Notification Nachrichteninhalte**

6774 (siehe auch: [gemF_PushNotification]#Kapitel "Operation Notify")

6775 Für jedes ausgelöste Ereignis eines Push Channels wird eine Push Notification erstellt. Die
 6776 Nachrichtendaten für ein Ereignis werden strukturiert gemäß Schema angeordnet und
 6777 nach den Vorgaben in [gemF_PushNotification#A_27610-*] auf konstante Länge
 6778 aufgefüllt.

6779 **A_27645 -Push Notification Management - Push Notification Datenstruktur**

6780 Das Push Notification Management MUSS die Nachrichtendaten einer Push Nachricht für
 6781 den Versand gemäß [Schema_PushNotifications] strukturieren.**[<=]**

6782 Es gibt eine maximal erlaubte Größe für Nachrichteninhalte, die durch das Push
 6783 Notification System [gemF_PushNotification] vorgegeben wird. Es muss sichergestellt
 6784 werden, dass erzeugte Nachrichteninhalte diese Größe nicht übersteigen.

6785 **A_27673 -Push Notification Management - Verkürzung der Nachrichteninhalte**

6786 Falls der erzeugte Nachrichteninhalt die maximal erlaubte Größe für Nachrichteninhalte
 6787 übersteigt MUSS das Push Notification Management die Elemente `actor`, `title`, `who`,
 6788 `folderTitle` so verkürzen, dass die maximal erlaubte Größe für Nachrichteninhalte
 6789 gerade nicht überschritten wird.**[<=]**

6790 *Hinweis: Es müssen nicht alle aufgeführten Elemente gleichzeitig verkürzt werden.*

6791 **A_27674 -Push Notification Management - Art der Verkürzung**

6792 Falls Elemente einer Nachricht verkürzt werden, dann sollen diese so verkürzt werden,
 6793 dass:

- 6794 • am Ende der Zeichenkette Zeichen entfernt werden
- 6795 • die Verkürzung mit "..." angezeigt wird.

6796 [**<=**]

6797 *Hinweis: Es kann sinnvoll sein, nur das längste kürzbare Element zu kürzen. Es wird*
 6798 *empfohlen eine Mindestlänge von 50 Bytes nicht zu unterschreiten.*

6799 3.21.5 Versenden von Push Nachrichten

6800 (siehe auch: [gemF_PushNotification]#Kapitel "Operation Notify" und [PushNotificationConcept]#Concept:
6801 "Verschlüsselung des Benachrichtigungsinhalts")

6802 Eine erstellte Push Nachricht wird an jede ePA-FdV-Instanz mit einer Registrierung im
6803 Aktenkonto gesendet, wenn für diese der assoziierte Kanal abonniert wurde
6804 (Konfiguration channelId == enabled).

6805 Die längenkorigierte Nachricht wird jeweils mit dem für den aktuellen Monat gültigen
6806 SchlüsselAES/CGM-Schlüssel-Jahr-Monat der Registrierung für jede adressierte ePA-
6807 FdV-Instanz verschlüsselt. Das Verschlüsselungsergebnis ist der Inhalt von ciphertext
6808 der notification für den Versand ([I_Push_Gateway]).

6809 **A_27651 -Push Notification Management - verpflichtende Verschlüsselung der** 6810 **Nachrichteninhalte**

6811 Das Push Notification Management MUSS sicherstellen, dass ausschließlich verschlüsselte
6812 Nachrichteninhalte als Push Nachricht versendet werden. [<=]

6813 Jedes einer Push Nachricht zugrundeliegenden Ereignis erzeugt auch einen
6814 Protokolleintrag im Audit Event Service. Die Menge der korrespondierenden
6815 Protokolleinträge ergibt dadurch im Aktenkonto ein Archiv der Push Ereignisse. Damit
6816 Clients ein Push Ereignis zu einem späteren Zeitpunkt, also nachdem die Push Nachricht
6817 im Client selbst schon gelöscht ist, restaurieren können, wird jeder Push Nachricht auch
6818 der Identifier des Protokolleintrags angehängt.

6819 **A_27644 -Push Notification Management - Referenz auf Protokolleintrag**

6820 Das Push Notification Management MUSS den eindeutigen Identifier Resource.id des zu
6821 einem Push Notification Ereignis gehörenden Protokolleintrags (AuditEvent) des
6822 Aktenkontos im Feld notification/identifizier einer Push Notification angeben. [<=]

6823 3.21.6 Protokollierung

6824 **A_27636 -Push Notification Management- Protokollierung der ePA-FdV-Instanz-** 6825 **Registrierung**

6826 Das Push Notification Management MUSS für Erstellung und Änderung (CUD) von ePA-
6827 FdV-Instanz-Registrierungen jeweils einen Protokolleintrag gemäß A_24704* erzeugen.
6828 Dabei ist folgende Wertbelegung zu berücksichtigen:

6829 **Tabelle 46: Constraint Management Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die API
	"object"		Bei intern ausgelösten Änderungen (internes Löschen einer ePA-FdV-Instanz-Registrierung nach Löschen Device Registration)

AuditEvent.action	C, U, D		
AuditEvent.entity.name	"PushNotificationManagement"		
AuditEvent.entity.detail	type	value[x]	
	"DisplayNamePusher"	<device_display_name aus der Pusher Registrierung>	
	"DisplayNameDevice"	<displayName der Device Registration>	

6830 [**<=**]6831 *Hinweis: DisplayNamePusher und DisplayNameDevice können gleich lauten.*

6832 **A_27662 -Push Notification Management- Protokollierung von Änderungen der Channel Konfiguration**

6833 Das Push Notification Management MUSS für Änderungen der Channel-Konfiguration
 6834 jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende
 6835 Wertebelegung zu berücksichtigen:
 6836

6837 **Tabelle 47: Constraint Management Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die API
	"object"		Bei intern ausgelösten Änderungen (internes Löschen einer ePA-FdV-Instanz-Registrierung nach Löschen Device Registration)
AuditEvent.action	U		
AuditEvent.entity.name	"PushNotificationManagement"		
AuditEvent.entity.detail	type	value[x]	
	"channelId"	<[enabled, disabled]>	value wird auf den neuen Wert gesetzt

	Die Kardinalität der <channelId> <value> Paare ist 1 .. *. Für jeden geänderte Wert eines Channels ist ein Eintrag erforderlich. Erfolgt der Protokolleintrag aufgrund Löschung eines Pushers, so sind die Channels zu erfassen, die vor der Löschung den Wert <code>enabled</code> hatten		
	"DisplayNamePusher"	<device_display_name aus der Pusher Registrierung>	
	"DisplayNameDevice"	<displayName der Device Registration>	

6838 [**<=**]

6839 *Hinweis: Die Speicherung von Protokolleinträgen erfordert einen berechtigten Benutzer,*
 6840 *um den Zugriff auf den sicheren Datenspeicher zu gewährleisten. Daher wird die*
 6841 *Erstellung von Protokolleinträgen immer übersprungen und es wird kein Protokolleintrag*
 6842 *gespeichert, wenn diese Bedingung nicht erfüllt ist.*

6843 **3.22 Schnittstellen (OpenAPI)**

6844 Hinweis: Die Vorgaben in den beschreibenden Dateien der REST-Schnittstellen (yaml)
 6845 sind normativ für den Anbieter der Schnittstellen. Die Anforderungen im vorliegenden
 6846 Dokument ergänzen diese Vorgaben, insbesondere, wenn diese für sicherheitstechnische
 6847 Gutachten erforderlich sind.

6848 **3.22.1 Übersicht der Schnittstellen des Aktensystems**6849 **Tabelle 48: Übersicht der Schnittstellen des Aktensystems**

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)
I_Consent_Decision_Management

Schnittstelle des Consent Decision Managements gemäß
[I_Consent_Decision_Management]

updateConsentDecision	Diese Operation erlaubt dem FdV und der Ombudsstelle die Änderung des Zustand des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA für eine Funktion.
getConsentDecisions	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen aller Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der ePA.
getConsentDecision	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen eines Widerspruchs einer Funktion gegen die Nutzung von widerspruchsfähigen Funktionen.
updateDataUsagePurposes	Diese Operation erlaubt dem FdV und der Ombudsstelle die Änderung der Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden.
getDataUsagePurposes	Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht der aktuellen Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden bzw. wurden.
getUserSpecificMedicationDenyList	Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht, welche LEI keinen Zugriff auf den Medication Service haben.
setUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI in die Liste der LEIs aufzunehmen, die keinen Zugriff auf den Medication Service haben.
getUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine bestimmte LEI aus der Liste der LEIs anzuzeigen, die keinen Zugriff auf den Medication Service haben.

deleteUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI aus der Liste der LEIs zu entfernen, damit diese LEI wieder Zugriff auf den Medication Service haben kann.
I_Constraint_Management_Insurant	
Schnittstelle des Constraint Managements gemäß [I_Constraint_Management_Insurant]	
getDenyPolicyAssignments	Diese Operation gibt eine Liste aller konfigurierten Einträge der General Deny Policy aus.
setPolicyAssignment	Diese Operation fügt der General Deny Policy einen neuen Eintrag hinzu.
deletePolicyAssignment	Diese Operation löscht einen bestimmten Eintrag der General Deny Policy.
I_Entitlement_Management	
Schnittstelle des Entitlement Management gemäß [I_Entitlement_Management] zur Vergabe von Befugnissen und Befugnisausschlüssen	
setEntitlementPs	Diese Operation fügt eine Befugnis für eine Leistungserbringerinstitution in einer Behandlungssituation hinzu (VSDM Prüfnachweis).
setEntitlementPsV2	Diese Operation fügt eine Befugnis für eine Leistungserbringerinstitution in einer Behandlungssituation hinzu (PoPP).
getEntitlements	Diese Operation erlaubt dem FdV den Abruf aller aktuellen Befugnisse.
getEntitlement	Diese Operation erlaubt dem FdV den Abruf einer bestimmten Befugnis.
setEntitlement	Diese Operation erlaubt dem FdV das Setzen einer Befugnis für einen Nutzer.
deleteEntitlement	Diese Operation erlaubt dem FdV den Abruf das Löschen einer existierenden Befugnis.
getBlockedUserPolicyAssignments	Diese Operation erlaubt dem FdV den Abruf der aktuell vorhandenen Befugnisausschlüsse.

setBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Befugnisausschluss für einen Nutzer.
getBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Abruf eines bestimmten Befugnisausschlusses.
deleteBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV die Aufhebung eines Befugnisausschlusses.
I_Entitlement_Management_EU	
Schnittstelle des Entitlement Management EU-Zugriff gemäß [I_Entitlement_Management_EU] zur Verwaltung Befugnis EU-Zugriff	
setEntitlementEu	Diese Operation erlaubt dem FdV das Setzen einer Befugnis EU-Zugriff für einen Versicherten.
getAccessCode	Diese Operation erlaubt dem FdV den Abruf des Zugriffscodes für die Befugnis EU-Zugriff.
Render API: PDF Audit	
Schnittstelle des Audit Event Service gemäß [IG_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 [IG_Basic] zum Abruf der Protokolldaten im FHIR-Format	
listAuditEvents_AuditEventSvc	Diese Operation ermöglicht die Suche nach AuditEvent Instanzen.
getAuditEventById_AuditEventSvc	Diese Operation ermöglicht das Lesen einer AuditEvent Instanz.
I_Health_Record_Relocation_Service	
Schnittstelle zur Steuerung des Aktenumzugs aus der Umgebung des Kostenträgers	
startPackageCreation	Diese Operation initiiert die Erstellung

	eines Export Pakets für den Umzug eines Aktenkontos zu einem neuen Anbieter.
startPackageImport	Diese Operation initiiert den Import eines Export Pakets in ein neu erstelltes Aktenkonto.
I_Device_Management_Insurant	
Schnittstelle zur Geräteverwaltung aus der Umgebung des Versicherten	
getDevice	Diese Operation ruft eine bestimmte Geräteregistrierung ab.
getDevices	Diese Operation ruft alle Geräteregistrierungen ab.
updateDevice	Diese Operation ändert den Displayname einer Geräteregistrierung.
deleteDevice	Diese Operation löscht eine bestimmte Geräteregistrierung.
registerDevice	Diese Operation erzeugt eine neue Geräteregistrierung und neue Geräteparameter
confirmPendingDevice	Diese Operation bestätigt eine neue Geräteregistrierung mit einem Geräteregistrierungscode
getDeviceAttestation	Diese Operation ruft die Bestätigung einer Geräteregistrierung am Home-AS ab.
I_Authorization_Service	
Schnittstelle der Autorisierung für den Login	
getFHIRVZDtoken	Diese Operation bezieht das search-access-token für den Zugriff auf den FHIR VZD vom Aktensystem
getNonce	Diese Operation bezieht einen eindeutigen einmalig generierten Zufallswert für die Client Attestierung
sendAuthorizationRequestSC	Diese Operation initiiert die Authentifizierung eines Leistungserbringers

sendAuthorizationRequestFdV	Diese Operation initiiert die Authentifizierung eines ePA-FdV
getFreshnessParameter	Diese Operation erzeugt einen Frischeparameter für die Authentisierung mittels Bearer Token
sendAuthorizationRequestBearerToken	Diese Operation 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	
getEmailAdress	Diese Operation ruft die hinterlegte E-Mail-Adresse des Versicherten ab.
replaceEmailAddress	Diese Operation setzt oder ändert die E-Mail Adresse für einen Versicherten ab.
I_Tool_Convert_PDF_Insurant	
Schnittstelle des XDS Document Managements gemäß [I_Tool_Convert_PDF_Insurant]	
convertPDF	Diese Operation konvertiert ein PDF in ein PDF/A Format
I_Data_Submission_Service	

Schnittstelle des Data Submission Service gemäß [I_Data_Submission_Service]	
getSubmissionPackage	Diese Operation stellt dem FDZ ein Datenpaket für eine bestimmte SubmissionID bereit.
I_Push_Notification_Management_Insurant	
Schnittstelle des Push Notification Managements gemäß [I_Push_Notification_Management]	
getPushers	Diese Operation gibt alle Pusher Registrierungen eines Aktenkontos aus
updatePusher	Diese Operation setzt, aktualisiert oder löscht eine Pusher Registrierung
getChannelsOfPusher	Diese Operation gibt die aktuelle 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

6850

Schnittstellen des Aktensystems (Nutzung ohne VAU-Kanal)

I_Information_Service

Schnittstelle des Informationsdienstes gemäß [I_Information_Service]

getConsentDecisionInformation	Diese Operation liest den aktuellen Zustand der Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der Funktionsklasse "Versorgungsprozess" aus.
setUserExperienceResult	Die Operation dient der Sammlung von Client Performancedaten aus der Umgebung der Leistungserbringer.
getRecordStatus	Diese Operation fragt Existenz und Status eines bestimmten Aktenkontos bei einem Betreiber an.

I_Information_Service_Accounts

Schnittstelle des Information Service gemäß [I_Information_Service_Accounts] für Anbieter Aktensystem im Kontext eines Aktenkontoumzugs

getGeneralConsentDecision	Diese Operation dient der Abfrage eines Widerspruchs gegen die Nutzung der ePA bei einem anderen Aktensystemanbieter.
startRelocation	Diese Operation initiiert die Erstellung eines Export Pakets für die Relocation.
deleteExportPackage	Diese Operation schließt den Vorgang der Relocation erfolgreich ab.
postExportPackageIncident	Diese Operation erhält Benachrichtigungen zum Relocation-Prozess.
putDownloadUrlForExportPackage	Diese Operation initiiert den Import eines Export Packages.
postPackageDeliveryIncident	Diese Operation erhält Benachrichtigungen zum Relocation-Prozess.
getProviderList	Diese Operation gibt eine Liste von FQDNs der Versicherungen / ePA-Anbieter aus

6851 Die Schnittstellen (REST) und Operationen sind funktional in den Beschreibungen der
 6852 jeweiligen Schnittstelle beschrieben. Darüber hinaus gelten die folgenden übergreifenden
 6853 Anforderungen.

6854 **3.22.2 Übergreifende Festlegungen zu den Schnittstellen**6855 **A_23918 -Schnittstellen (OpenApi) - Prüfung der Befugnis**

6856 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6857 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6858 eine vorhandene und gültige Befugnis (entitlement) für den Nutzer der Operation fordern
6859 und diese nicht vorliegt. [\leq]

6860 *Hinweis: A_23918 deckt auch die Fehlersituationen "kein VAU-Kanal" und "keine User*
6861 *Session" ab, da diese eine Vorbedingung für den Nachweis einer gültigen Befugnis sind.*

6862 **A_24365 -Schnittstellen (OpenApi) - Prüfung des Aktenkontos**

6863 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6864 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6865 die Existenz des adressierten Aktenkontos fordern und diese nicht für den
6866 Operationsaufruf verwendet wird. [\leq]

6867 *Hinweis A_24365 deckt auch die Fehlersituation "kein Health Record Context" ab, da*
6868 *dieses nur infolge eines nicht vorhandenen Aktenkontos auftritt.*

6869 **A_24538 -Schnittstellen (OpenApi) - Prüfung des Aktenkontostatus**

6870 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6871 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6872 einen vorgegebenen Status des Aktenkontos fordern und dieser nicht vorhanden ist. [\leq]

6873 **A_24366 -Schnittstellen (OpenApi) - Prüfung der Rolle**

6874 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6875 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6876 die Zulässigkeit der Operation auf bestimmte Rollen (professionOID) einschränken und
6877 der Nutzer der Operation diese nicht nachweist. [\leq]

6878 **A_24367 -Schnittstellen(OpenApi) - Prüfung des Identifiers**

6879 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6880 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6881 die Zulässigkeit der Operation auf bestimmte Identifier (KVNR oder Telematik-ID)
6882 einschränken und der Nutzer der Operation diese nicht nachweist. [\leq]

6883 **A_24580 -Schnittstellen (OpenApi) - Protokollierung der Operationen**

6884 Das ePA-Aktensystem MUSS nach der Ausführung der Operationen der REST-
6885 Schnittstellen eine Protokolleintrag erstellen, wenn die Protokollierung in den
6886 Nachbedingungen (Postconditions) der Operationen gefordert ist (log-entry). [\leq]

6887

4 Informationsmodelle

6888

Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten wird nicht benötigt.

6889

6890

5 Anhang A – Verzeichnisse

6891

5.1 Abkürzungen

Kürzel	Erläuterung
AdV	Anwendungen des Versicherten
AN	Arbeitsnummer in der Übermittlung von Daten zur Sekundärnutzung
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BGP	Border Gateway Protokoll
BPPC	Basic Patient Privacy Consents
CRUD	Create Read Update Delete
DiGA	Digitale Gesundheitsanwendung
ePA-FdV	ePA-Frontend des Versicherten
ePA-FdV AdV	ePA-Frontend des Versicherten im KTR-AdV-Terminal
FDZ	Forschungsdatenzentrum Gesundheit
HL7	Health Level Seven
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IHE ITI TF	IHE IT Infrastructure Technical Framework
JWT	JSON-Web-Token
JWS	signiertes JSON-Web-Token

KTR	Kostenträger
LP	Lieferpseudonym in der Übermittlung von Daten zur Sekundärnutzung
MIO	Medizinisches Informationsobjekt
MHD	Mobile access to Health Documents (FHIR-Service im Aktensystem u.a. für Volltextsuche)
MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
PDSG	Patientendaten-Schutz-Gesetz
PHR	Personal Health Record
RMU	Restricted Metadata Update Profile
SAML	Security Assertion Markup Language
TLS	Transport Layer Security
UUID	Universally Unique Identifier
VAU	Vertrauenswürdige Ausführungsumgebung
VST	Vertrauensstelle Elektronische Patientenakte für Datenausleitung an das FDZ
W3C	World Wide Web Consortium
WS-I	Web-Services Interoperability Consortium
XCA	Cross-Community Access Profile
XDS	Cross-Enterprise Document Sharing Profile
XDW	Cross-Enterprise Document Workflow Profile
XOP	XML-binary Optimized Packaging
XSPA	Cross-Enterprise Security and Privacy Authorization Profile

6892 **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]).

6893 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung
 6894 gestellt.

6895 **5.3 Abbildungsverzeichnis**

6896	Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls.....	46
6897	Abbildung 2 - Überblick Service-VAUs	72
6898	Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung	76
6899	Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer	
6900	Überschlüsselung	77
6901	Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP ..	210
6902	Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP	213
6903	Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes	215
6904	Abbildung 8: Dokumente mit Anhangsbeziehungen.....	255
6905	Abbildung 9: Beispiel Verweiszirkel und doppelte Eltern.....	257
6906	Abbildung 10: Beispiel Anhangskette zu lang	258
6907		

6908 **5.4 Tabellenverzeichnis**

6909	Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat	18
6910	Tabelle 2: Zustandswechsel im Lebenszyklus eines Aktenkontos.....	27
6911	Tabelle 3 : Health Record Relocation Service Protokollierung	36
6912	Tabelle 4: Tab_AS_VAU_Token_Modul_Rules -Prüfregeln VAU Token	47
6913	Tabelle 5: Überblick über die Regeln des Befugnisverifikations-Moduls	51
6914	Tabelle 6: Tab_AS_Entitlement_Registration_Rules - Regeln zur Registrierung von	
6915	Befugnissen	53
6916	Tabelle 7: Tab_AS_SDS-Key_Rules Key Rules - Regeln zur Ableitung der	
6917	versichertenindividuellen Persistierungsschlüssel	60
6918	Tabelle 8: Widerspruchsfähige Funktionen der elektronischen Patientenakte	80

6919	Tabelle 9: Consent Decision Management Protokollierung - Widersprüche für Funktionen	
6920	der ePA	82
6921	Tabelle 10: consent Decision Management Protokollierung - unveränderte	
6922	Entscheidungen zu widerspruchsfähigen Funktionen der ePA.....	83
6923	Tabelle 11: Consent Decision Management Protokollierung - Widersprüche zu	
6924	Sekundärnutzungszwecken	85
6925	Tabelle 12: Consent Decision Management Protokollierung - unveränderte Widersprüche	
6926	zu Sekundärnutzungszwecken.....	85
6927	Tabelle 13: Consent Decision Management Protokollierung - User Specific Deny Policy	
6928	Medication	87
6929	Tabelle 14: Inhalt einer Befugnis	88
6930	Tabelle 15: Befugnisse für berechtigte Nutzergruppen und Nutzer	90
6931	Tabelle 16: Befugnisse EU-Zugriff für berechtigte Nutzergruppen und Nutzer	92
6932	Tabelle 17: Entitlement Management Protokollierung	93
6933	Tabelle 18: Inhalt eines Blocked User Policy Eintrags	102
6934	Tabelle 19: Legal Policy	108
6935	Tabelle 20: Legal Policy - EU-Zugriff	112
6936	Tabelle 21: Beschreibung der Kategorien.....	113
6937	Tabelle 22: Constraint Management Protokollierung.....	117
6938	Tabelle 23: Inhalt eines General Deny Policy Eintrags	120
6939	Tabelle 24: Verbergen eines Medical Service.....	120
6940	Tabelle 25: Kennzeichnung von Optionalitäten	133
6941	Tabelle 26: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den	
6942	Außerschnittstellen des XDS Document Service	133
6943	Tabelle 27: Schnittstelle I_Document_Management	153
6944	Tabelle 28: Schnittstelle I_Document_Management_Insurant	156
6945	Tabelle 29: Schnittstelle I_Document_Management_Ncpeh.....	159
6946	Tabelle 30: Festlegung Folder.entryUUIDzu statischen Ordnern	160
6947	Tabelle 31: Nutzungsvorgaben für Metadatenattribute XDS	162
6948	Tabelle 32: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language	
6949	Codes	176
6950	Tabelle 33: Einsortierung_Datenkategorien.....	181
6951	Tabelle 34: TAB_EPA_Sammlungstypen	184
6952	Tabelle 35: Auswirkungen bei Widerspruch gegen eine Funktion der ePA.....	188
6953	Tabelle 36: XDS Document Service Protokollierung.....	190
6954	Tabelle 37: Patient Service Protokollierung	193
6955	Tabelle 38: Medication Service Protokollierung	195
6956	Tabelle 39: MHD Service Protokollierung	198
6957	Tabelle 40 : Inhaltliche Definitionen eines AuditEvent	199

6958	Tabelle 41 Befüllung AuditEvent	200
6959	Tabelle 42 Audit Event Management Protokollierung - Fehler	204
6960	Tabelle 43: Audit Event Service Protokollierung	205
6961	Tabelle 44: Auswahl der zu übertragenden FHIR-Ressourcen	223
6962	Tabelle 45: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen	224
6963	Tabelle 46: Constraint Management Protokollierung	231
6964	Tabelle 47: Constraint Management Protokollierung	232
6965	Tabelle 48: Übersicht der Schnittstellen des Aktensystems	233
6966		

6967 5.5 Referenzierte Dokumente

6968 5.5.1 Dokumente der gematik

6969 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 6970 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/tree/ePA-3.1.2
[I_Consent_Decision_Management]	gematik: I_Consent_Decision_Management REST-Schnittstelle zum Management der Widersprüche zu Versorgungsprozessen siehe [ePA_Basic] Path: src/openapi/I_Consent_Decision_Management.yaml
[I_Entitlement_Management]	gematik: I_Entitlement_Management REST-Schnittstelle zur Verwaltung von Befugnissen und Befugnisausschlüssen siehe [ePA_Basic] Path: src/openapi/I_Entitlement_Management.yaml
[I_Entitlement_Management_EU]	gematik: I_Entitlement_Management_EU REST-Schnittstelle zur Verwaltung von Befugnissen EU-Zugriff siehe [ePA_Basic] Path: src/openapi/I_Entitlement_Management_EU.yaml
[I_Device_Management_Insurant]	gematik: I_Device_Management_Insurant.yaml REST-Schnittstelle zur Geräteverwaltung siehe [ePA_Basic] Path: src/openapi/I_Device_Management_Insurant.yaml
[I_Health_Record_Relocation_Service]	gematik: I_Health_Record_Relocation_Service REST-Schnittstelle zum Aktenumzug siehe [ePA_Basic] Path: src/openapi/I_Health_Record_Relocation_Service.yaml
[I_Information_Service_Accounts]	Schnittstellenspezifikation Information Service für Betreiber siehe [ePA_Basic] Path: src/openapi/I_Information_Service_Accounts.yaml
[I_Information_Service]	Schnittstellenspezifikation Information Service siehe [ePA_Basic]

	Path: src/openapi/I_Information_Service.yaml
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung und impliziten Geräteregistrierung siehe [ePA_Basic] Path: src/openapi/I_Authorization_Service.yaml
[I_Email_Management]	gematik: I_Email_Management REST-Schnittstelle zum Management von E-Mail-Adressen eines Versicherten siehe [ePA_Basic] Path: src/openapi/I_Email_Management.yaml
[ePA_XDS_Document]	gematik: GitHub Repository "ePA-xds-document" https://github.com/gematik/ePA-XDS-Document/tree/ePA-3.1.2
[I_Constraint_Management_Insurant]	gematik: I_Constraint_Management_Insurant.yaml REST-Schnittstelle zum Verbergen und Sichtbarmachen von Dokumenten siehe [ePA_XDS_Document] Path: src/openapi/I_Constraint_Management_Insurant.yaml
[I_Tool_Comvert_PDF_Insurant]	gematik: I_Tool_Convert_PDF_Insurant Schnittstelle für die PDF Formatkonvertierung siehe [ePA_XDS_Document] Path: src/openapi/ I_Tool_Convert_PDF_Insurant.yaml
[XDSDocumentService]	gematik: XDSDocumentService.wsdl IHE-Schnittstelle des XDSDocumentService siehe [ePA_XDS_Document] Path: src/schema
[HealthRecordMigration]	gematik: ref-ePA-HealthRecordMigration Referenzimplementierung und Vorgaben für das Exportpaket bei einem Anbieterwechsel GitHub: https://github.com/gematik/ref-ePA-HealthRecordMigration/tree/ePA-3.1
[IG_Basic]	gematik: FHIR Implementation Guide "ePA Basisfunktionalitäten" https://gematik.de/fhir/epa/1.1.5
[IG_Medication_Service]	gematik: FHIR Implementation Guide "ePA Medication Service" https://gematik.de/fhir/epa-medication/1.1.5

[IG_MHD_Service]	gematik: FHIR Implementation Guide "ePA MHD Service" https://gematik.de/fhir/epa-mhd/1.0.0
[IG_TI_Terminology]	gematik: Implementation Guide "TITerminology" https://gematik.de/fhir/terminology/1.0.6
[DataPseudonymization]	gematik: epa-research Vorgaben zur Pseudonymisierung von Daten zur Sekundärnutzung GitHub: https://github.com/gematik/epa-research/tree/ePA-3.1 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/1.0.0/#concept/concept.html und https://gematik.github.io/gem-push-notifications-concept/1.0.0/#concept/concept.html%23_priorit%C3%A4t
[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/1.0.0/#push_gateway_openapi.html
[Schema_PushNotifications]	gematik: PushNotificationSchema Strukturvorgaben für Nachrichteninhalte des Push Notification Managements siehe [ePA_Basic] Path: src/schema/PushNotificationSchema.yaml

6971 **5.5.2 Weitere Dokumente**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-RMD]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.6 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-RMU]	IHE International (2021): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.3 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf
[IHE-ITI-TF1]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Profile definition, use-case analysis, actor definition, and use of transactions and content, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume1/
[IHE-ITI-TF2]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume2/
[IHE-ITI-TF3]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Document Sharing Metadata and Content Profiles, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume3/
[I_VST]	Vertrauensstelle ePA – Pseudonymisierungskonzept Datenausleitung ePA zu Forschungszwecken Version 2.0 (12.07.2024), Herausgeber: Robert Koch-Institut, Nordufer 20,13353 Berlin
[MIO-UH]	Kassenärztliche Bundesvereinigung (2022): Kinderuntersuchungsheft, 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/
[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/

6972

6 Anhang B – Erläuternde Informationen

6973
6974

Dieser Anhang enthält nicht normative Informationen, die dazu dienen, das Verständnis der Spezifikation zu vereinfachen.

6975

6.1 Dokumentenanhänge

6976
6977
6978

Der vorliegende Abschnitt enthält einige Abbildungen, die das Konzept der Dokumentenanhänge in der ePA für alle visuell erläutern und damit leichter verständlich machen sollen.

6979

6.2 Überblick

6980
6981
6982

Die folgende Abbildung zeigt fünf Dokumente (bzw. DocumentEntries), die teilweise über Anhangsbeziehungen miteinander verbunden sind:

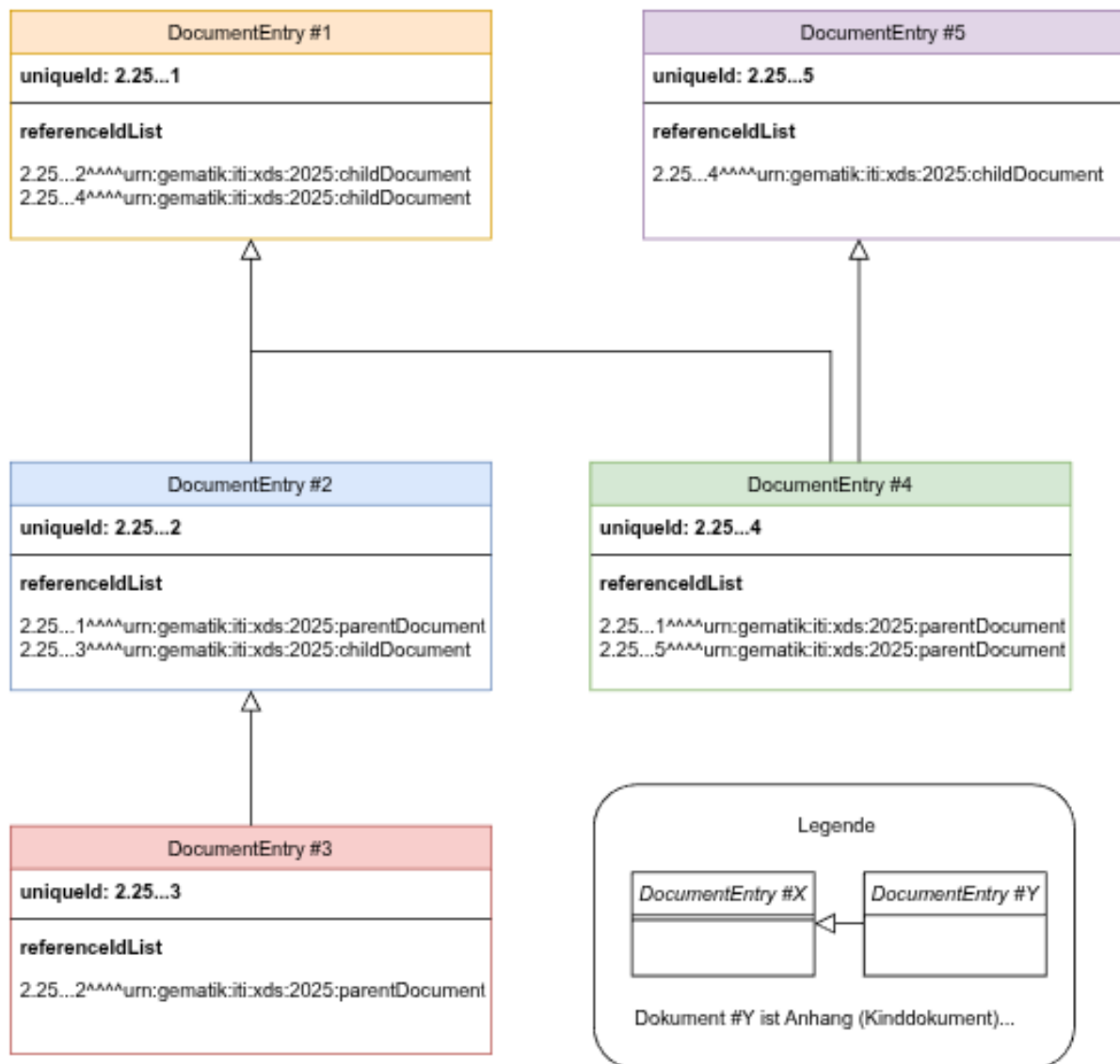


Abbildung 8: Dokumente mit Anhangsbeziehungen

zu einige Hinweise:

- Dokument #1
 - besitzt zwei Anhänge (Dokumente #2 und #4)
 - ist selbst an kein Dokument angehängt.
- Dokument #2
 - besitzt einen Anhang (Dokument #3).
- Dokument #3
 - besitzt keine Anhänge.
- Dokument #4
 - ist selbst an Dokument #2 angehängt.
- Dokument #5

- 7005 • besitzt keine Anhänge.
- 7006 • ist selbst an zwei Dokumente angehängt (Dokumente #1 und #5)
- 7007 • Dokument #5
- 7008 • besitzt einen Anhang (Dokument #4).

7009 **Notation**

7010 Jedes Dokument verweist auf Dokumentenanhänge über einen Eintrag in seiner
 7011 referenceIdList
 7012 (`<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2025:childDocument`), wobei
 7013 `DocumentEntry.uniqueId` sich auf die eindeutige Kennung des Anhangsdokuments
 7014 bezieht. In der Spezifikation wird der Anhang manchmal als Kinddokument bezeichnet,
 7015 und das Dokument, an dem es hängt als Elterndokument. In diesem Sinne ist Dokument
 7016 #3 bspw. das Kinddokument von Dokument #2.

7017 **Anzahl Anhänge**

7018 Wie aus der Abbildung hervorgeht, kann ein Dokument mehrere Anhänge besitzen; im
 7019 Beispiel verfügt Dokument über zwei Anhänge. Umgekehrt kann auch jeder Anhang an
 7020 mehr als einem Dokument hängen (im Beispiel ist Dokument #4 Anhang sowohl für
 7021 Dokument #1 also auch Dokument #5).

7022 Die Beziehung zwischen Eltern- und Kinddokumenten ist also m:n: Ein Dokument kann
 7023 beliebig viele Anhänge besitzen und ein Anhang kann an beliebig vielen Dokumenten
 7024 anhängen.

7025 **6.3 Ungültige Anhänge**

7026 Dieser Abschnitt illustriert einige nicht erlaubte Anhangsszenarien.

6.3.1 Verweiszirkel und doppelte Eltern

Die folgende Abbildung demonstriert Anhänge, wie sie nicht in den XDS Document Service eingebracht werden können:

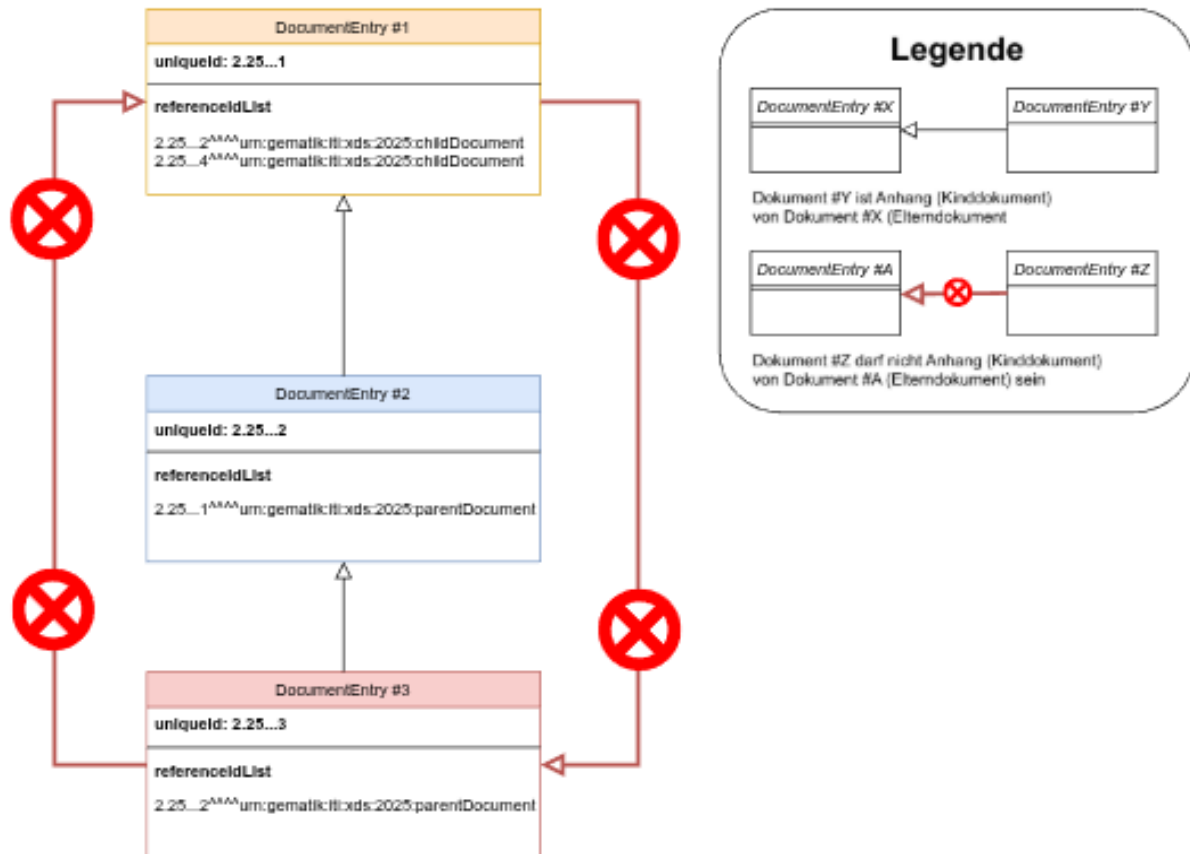


Abbildung 9: Beispiel Verweiszirkel und doppelte Eltern

- Ausgangssituation (unproblematisch):
 - Dokument #3 ist Anhang zu Dokument #2.
 - Dokument #2 ist Anhang zu Dokument #1.
- Falls nun anschließend versucht wird, Dokument #3 als Kind von Dokument #1 einzutragen (roter Pfeil auf der linken Seite), ist dies nicht erlaubt, da ein Dokument nicht Anhang zu zweien seiner "Vorfahren" in der Anhangskette sein darf (denn Dokument #3 ist bereits Anhang von Dokument #2, das wiederum an Dokument #1 hängt).
- Auch der Versuch, Dokument #1 als Anhang zu Dokument #3 zu markieren schlägt fehl, denn es würde ein Verweiszirkel entstehen, in dem ein Kinddokument gleichzeitig Elterndokument für eines seiner Vorfahren ist.

6.3.2 Anhangskette zu lang

Die maximale Länge der Anhangsketten ist auf fünf beschränkt. Die folgende Abbildung zeigt, in welchem Fall das Hinzufügen eines weiteren Anhangs zu Problemen führt (und wann nicht):

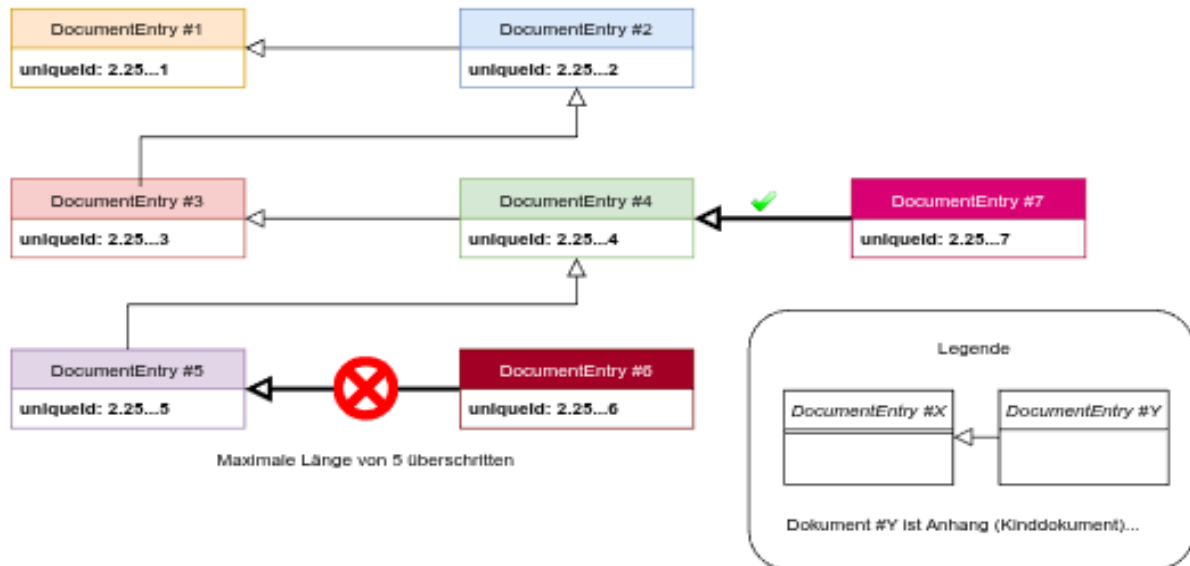


Abbildung 10: Beispiel Anhangskette zu lang

- Ausgangssituation (Dokumente #1-#5) unproblematisch. Länge der Anhangskette ist fünf.
- Wenn versucht wird, Dokument #6 einzufügen, ist die Anhangskette zu lang.
 - Das würde auch gelten, wenn der Einstellende bspw. Dokumente #1 und #2 gar nicht sehen könnte (Legal Policy, Verbergen)
 - Es würde ein Fehler zurückgegeben.
- Das Einstellen von Dokument #7 wäre unproblematisch.
 - Die Anhangskette von Dokument #7 hätte fünf Dokumente, Dokument #6 gehört also nicht mit dazu.
 - Das Dokument könnte auf diese Weise als Anhang an Dokument #4 eingestellt werden.