

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Aktensystem ePA für alle

Version:	1.6.0 CC2
Revision:	1318465 <u>1318636</u>
Stand:	15-07 <u>01.08</u> .2025
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_Aktensystem_ePAfueralle

26

Dokumentinformationen

27

Änderungen zur Vorversion

28

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

29

30

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.01.2024		ePA für alle	gematik
1.1.0	28.03.2024		ePA für alle - Release 3.0.1	gematik
1.2.0	12.07.2024		ePA für alle - Release 3.0.2, Zuordnungen für Release E-Rezept 1.6.5	gematik
1.3.0	14.08.2024		ePA für alle - Release 3.1.0	gematik
1.4.0	28.02.2025		ePA für alle - Release 3.0.5	gematik
1.5.0	27.05.2025		ePA für alle - Release 3.1.2	gematik
1.6.0 CC	15.07.2025		ePA für alle - Release 3.1.2-1	gematik
<u>1.6.0</u> <u>CC2</u>	<u>01.08.2025</u>		<u>ePA für alle - Release 3.1.3</u>	<u>gematik</u>

Inhaltsverzeichnis

31		
32	1 Einführung	8
33	1.1 Zielsetzung	8
34	1.2 Zielgruppe	8
35	1.3 Geltungsbereich	8
36	1.4 Abgrenzungen	8
37	1.5 Methodik	9
38	2 Übergreifende Festlegungen	10
39	2.1 Aktensystem- und Service-Lokalisierung	12
40	2.2 Redundanz	14
41	2.3 Datenschutz und Sicherheit	14
42	2.4 Validierungsaktenkonto	19
43	2.5 Tracing in Nichtproduktivumgebungen	22
44	2.6 Benutzerführung	23
45	2.7 Useragent	24
46	2.8 Performance aus Anwendersicht	24
47	3 Funktionsmerkmale	26
48	3.1 Aktenkonto eines Versicherten (Health Record)	26
49	3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen	
50	Patientenakte	26
51	3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den	
52	Kostenträger	26
53	3.1.2 Lebenszyklus und Zustände eines Aktenkontos	27
54	3.1.3 Anlage eines neuen Aktenkontos	28
55	3.1.4 Löschen eines Aktenkontos	31
56	3.2 Health Record Relocation Service	32
57	3.2.1 Ablauf eines Aktenkontoumzugs	37
58	3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter	37
59	3.2.1.2 Start Transfer eines existierenden Aktenkontos	38
60	3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen Anbieter	38
61	3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den neuen	
62	Anbieter	38
63	3.2.1.5 Import des Exportpakets durch den neuen Anbieter	39
64	3.2.1.6 Abschluss des Transfers durch beide Anbieter	39
65	3.2.1.7 Fehlersituationen und Handhabung	39
66	3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich	
67	oder derzeit nicht möglich	40
68	3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter	40
69	3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen	
70	Anbieter	41

71	3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter	42
72	3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM	
73	43
74	3.4 Befugnisverifikations-Modul	46
75	3.4.1 VAU-Token-Modul	47
76	3.4.2 Regeln des Befugnisverifikations-Moduls	54
77	3.5 Vertrauenswürdige Ausführungsumgebung (VAU)	72
78	3.5.1 Übergreifende VAU-Anforderungen	73
79	3.5.1.1 Schutz der Integrität der VAU	73
80	3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU	74
81	3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU.....	75
82	3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM.....	75
83	3.5.1.5 Logging und Monitoring.....	76
84	3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU.....	77
85	3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU ...	77
86	3.5.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-VAU.....	78
87	3.5.2.3 Konsistenz des Systemzustands	79
88	3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU.....	79
89	3.5.4 Zusätzliche Anforderungen an eine Service-VAU	80
90	3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU.....	82
91		
92	3.6 Umschlüsselung und Überschlüsselung	83
93	3.7 User Session und Health Record Context.....	87
94	3.8 Consent Decision Management.....	87
95	3.8.1 Widersprüche für Funktionen der ePA	88
96	3.8.2 Einschränkung der Verwendung von Daten auf bestimmte	
97	Sekundärnutzungszwecke	92
98	3.8.3 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny	
99	Policy Medication).....	95
100	3.9 Entitlement Management.....	97
101	3.9.1 Initiale Befugnisse (static Entitlements)	104
102	3.9.2 Erstellen einer Befugnis durch Clients	105
103	3.9.2.1 Befugnisvergabe durch ein ePA-FdV.....	106
104	3.9.2.2 Befugnisvergabe durch ein Primärsystem	108
105	3.9.3 Löschen von Befugnissen	109
106	3.9.4 Befugnisausschluss (Blocked User Policy)	110
107	3.9.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)	112
108	3.9.6 EntitlementDenyList	115
109	3.10 Legal Policy	117
110	3.11 Constraint Management.....	125
111	3.11.1 Aktenkontoweites Verbergen (General Deny Policy)	129
112	3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes	
113	130
114	3.12 Device Management	131
115	3.13 Medical Services	135
116	3.13.1 XDS Document Service	135
117	3.13.1.1 Formatprüfung beim Einstellen von Dokumenten	136
118	3.13.1.2 Anforderungen zur Validierung	138
119	3.13.1.3 Namensräume.....	140

120	3.13.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von	
121	Dokumenten	140
122	3.13.1.4.1 Anforderungen an IHE ITI-Akteure	140
123	3.13.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen	143
124	3.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen ...	146
125	3.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen	163
126	3.13.1.5 Fehlerbehandlung in Schnittstellenoperationen	164
127	3.13.1.6 Schnittstellen im XDS Document Service	165
128	3.13.1.6.1 Schnittstelle I_Document_Management	165
129	3.13.1.6.2 Schnittstelle I_Document_Management_Insurant	168
130	3.13.1.6.3 Schnittstelle I_Document_Management_Ncpeh	171
131	3.13.1.7 Statische Metadaten	172
132	3.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten	173
133	3.13.1.8.1 Allgemeine Metadatenvorgaben	174
134	3.13.1.8.2 Metadaten der Dokumente und SubmissionSets	193
135	3.13.1.8.3 Metadaten für Datenkategorien	197
136	3.13.1.8.4 Automatisches Umschreiben von Daten	199
137	3.13.1.9 Strukturierte Dokumente	200
138	3.13.1.9.1 Sammlungstypen	200
139	3.13.1.9.2 Konfigurierbarkeit	202
140	3.13.1.9.3 Verarbeitungsvorgaben für spezifische Dokumente	203
141	3.13.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode	
142	204
143	3.13.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die	
144	Dokumente des Aktenkontos	204
145	3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication	
146	Service durch eine spezifische LEI auf die Dokumente des Aktenkontos	205
147	3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service	206
148	3.13.1.14 Unterstützungsleistung für das ePA-FdV	209
149	3.13.2 FHIR Data Services	210
150	3.13.2.1 Patient Service	210
151	3.13.2.2 Medication Service	210
152	3.13.2.3 MHD Service	215
153	3.13.2.4 Dienstübergreifende Festlegungen	217
154	3.14 Audit Event Service	218
155	3.15 Information Service	225
156	3.15.1 Information Service	225
157	3.15.1.1 Informationen zu Widersprüchen (Consent Decisions)	225
158	3.15.1.2 Informationen zur Anwenderperformance (UX Performance)	226
159	3.15.2 Information Service - Account	226
160	3.16 Email Management	227
161	3.17 Zusätzliche Anforderungen an den Authorization Service	228
162	3.17.1 Anforderungen an den Authorization Service für die Authentisierung von	
163	Versicherten (FdV)	228

164	3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B	
165	233
166	3.17.3 Anforderungen an den Authorization Service für die Authentisierung des E-	
167	Rezept-Fachdienstes	235
168	3.18 Anbindung Verzeichnisdienst FHIR-Directory	236
169	3.19 Access Gateway	236
170	3.19.1 Paketfilter	236
171	3.19.1.1 Funktion	236
172	3.19.1.2 Redundanz	238
173	3.19.1.3 Konfiguration	238
174	3.19.1.4 Adressierung	238
175	3.19.1.4.1 Access Gateway zum Transportnetz Internet	238
176	3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz	239
177	3.19.2 Proxy für das VAU-Protokoll	239
178	3.19.3 Tracing in Nichtproduktivumgebungen	239
179	3.19.4 Übergreifende Festlegungen	241
180	3.20 Data Submission Service	242
181	3.20.1 Erstellung von Arbeitsnummern und Lieferpseudonymen	242
182	3.20.2 Auswahl von medizinischen Daten	243
183	3.20.3 Protokollierung des Datenexports an das FDZ	244
184	3.20.4 Pseudonymisierung von medizinischen Daten	244
185	3.20.5 Übermittlung der pseudonymisierten medizinischen Daten	245
186	3.21 Push Notification Management	247
187	3.21.1 Push Notification Management des ePA-Aktensystems	248
188	3.21.2 Registrierung eines ePA-FdV als Pusher	248
189	3.21.3 Push Notification Channels	249
190	3.21.4 Push Notification Nachrichteninhalte	250
191	3.21.5 Versenden von Push Nachrichten	251
192	3.21.6 Protokollierung	252
193	3.22 Schnittstellen (OpenAPI)	254
194	3.22.1 Übersicht der Schnittstellen des Aktensystems	255
195	3.22.2 Übergreifende Festlegungen zu den Schnittstellen	264
196	4 Informationsmodelle	265
197	5 Anhang A – Verzeichnisse	266
198	5.1 Abkürzungen	266
199	5.2 Glossar	268
200	5.3 Abbildungsverzeichnis	268
201	5.4 Tabellenverzeichnis	268
202	5.5 Referenzierte Dokumente	270
203	5.5.1 Dokumente der gematik	270
204	5.5.2 Weitere Dokumente	274
205	6 Anhang B – Erläuternde Informationen	277
206	6.1 Dokumentenanhänge	277
207	6.1.1 Überblick	277

208	6.1.2 Ungültige Anhänge	279
209	6.1.2.1 Verweiszirkel und doppelte Eltern	280
210	6.1.2.2 Anhangskette zu lang	280

211 |

212 1 Einführung

213 1.1 Zielsetzung

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

216 1.2 Zielgruppe

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

220 1.3 Geltungsbereich

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

226 Schutzrechts-/Patentrechtshinweis

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

235 1.4 Abgrenzungen

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

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

243 1.5 Methodik

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

248
249 **<AFO-ID> - <Titel der Afo>**
250 Text / Beschreibung
251 [**<=**]

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

2 Übergreifende Festlegungen

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

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

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

A_25149-01 -ePA-Aktensystem - Rollentrennung ePA-Aktensystem und sektoraler IDP

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

A_24673 -Zeitsynchronisation über Zeitdienst in der TI

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

A_25612 -ePA-Aktensystem - Authentisierung gegenüber einem Client innerhalb der TI

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

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

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

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

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

Die Formatvorgaben zum Useragent sind in A_22470* definiert.

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

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

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

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

A_27701 -Requestkennung in HTTP Header außerhalb des VAU-Kanals

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

A_27702 -Requestkennung in HTTP Header innerhalb des VAU-Kanals

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

A_27703 -Requestkennung in der Response

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

A_27712 -Requestkennung - betriebliche Protokollierung

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

~~A_27443-01A_27443~~ -Nutzung Terminologiepaket

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

Hinweis zu A_27443: ~~:-*~~

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

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

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

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

Diese Formatvorgabe betrifft nicht die Bestandsdatenlieferung. [<=]

345 Beispiele für Datentyp datetime:
346 2025-04-12T15:20:50Z
347 2025-06-30T23:59:59+01:00

348 **A_27868 -ePA-Aktensystem – fehlerhafter URL-Pfad**

349 Falls ein URL-Pfad adressiert wird, der keinem für das Aktensystem spezifizierten
350 Services zugeordnet werden kann, MUSS das ePA-Aktensystem den Aufruf mit dem
351 HTTP-Statuscode 404 mit Errorcode `pathNotFound` ablehnen.
352 [**<=**]

353 **2.1 Aktensystem- und Service-Lokalisierung**

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

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

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

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

370 **A_24592-02 -Anbieter ePA-Aktensystem -Registrierung an übergreifender ePA- 371 Domäne**

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

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

381 Die "ePA-Anbieter-Zahl" wird durch die gematik festgelegt.
382 [**<=**]

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

ePA-Anbieter-Zahl	Anbieter / Betreiber
1	IBM

ePA-Anbieter-Zahl	Anbieter / Betreiber
2	Bitmarck Technik

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

Beispiele der Dienstlokalisierung

PU :

Aktensystem A

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

Aktensystem B

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

TU :

Aktensystem 1

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

...

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

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

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

[<=]

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

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

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

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

A_22687 -Aktensystem, Konfiguration Schnittstellen über /.well-known/

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

A_26814 -ePA-Aktensystem - Schnittstellenadressierung

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

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

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

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

A_24801 -Aktensystem, Liste von FQDN im Internet

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

2.2 Redundanz

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

2.3 Datenschutz und Sicherheit**A_15128 -Anbieter ePA-Aktensystem - Schutz der transportierten Daten im ePA-Aktensystem**

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

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

A_15103 -Anbieter ePA-Aktensystem - Konzept zur Verhinderung von Profilbildung

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

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

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

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

A_15104 -Anbieter ePA-Aktensystem - Ordnungsgemäße IT-Administration

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

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

A_15824 -Anbieter ePA-Aktensystem - Sichere Speicherung von Daten

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

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

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

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

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

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

A_15119 -Anbieter ePA-Aktensystem - Löschkonzept

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

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

[≤]

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

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

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

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

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

Der Anbieter des ePA-Aktensystems MUSS mindestens einmal im Jahr Werte zu einer Standard-Aktennutzung von LE und Versicherten durch die Profilierung anonymer

515 Zugriffsstatistiken auf das ePA-Aktensystem zum Zweck der Erkennung von Zugriffen
516 gemäß A_15155 ermitteln. [≤]

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

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

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

524 **A_24778 -Anbieter ePA-Aktensystem - Einsatz zertifizierter HSM**

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

- 530 1. FIPS 140-2 Level 3 oder
 - 531 2. FIPS 140-3 Level 3 oder
 - 532 3. Common Criteria EAL 4+ (mit AVA_VAN.5)
- 533 entsprechen. [≤]

534 **A_15157 -Anbieter ePA-Aktensystem - Sicherer Betrieb und Nutzung eines**
535 **HSMs**

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

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

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

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

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

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

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

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

557 **A_15167 -Anbieter ePA-Aktensystem - Social Engineering Angriffen**
558 **entgegenwirken**

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

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

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

A_15168 -ePA-Aktensystem - Verbot vom dynamischen Inhalt

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

A_17080 -Verhindern von Session Hijacking

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

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

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

A_24781 -Sicherer Betrieb des Produkts nach Handbuch

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

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

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

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

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

A_21106 -Anbieter ePA-Aktensystem – Signaturschlüssel für Protokolle

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

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

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

A_22409 -Anbieter ePA-Aktensystem - CA-Anbieterwechsel

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

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

Die Komponenten des ePA-Aktensystems, die XML-Signaturen prüfen, MÜSSEN geeignete Maßnahmen gegen XSW-Angriffe umsetzen. Mindestens MÜSSEN sie die FastXPath-

610 Auswertung der XML-Daten und XML-Signaturen gemäß [GJLS-2009] (vgl. auch [BSI-
611 XSpRES]) umsetzen. [≤]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

639 Das ePA-Aktensystem MUSS bei der Prüfung von Signaturen

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

643 [≤]

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

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

647 **Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat**

Parameter	C.FD.SIG	C.CH.SIG	C.HCI.OSIG	C.HCI.AUT
PolicyList	oid_fd_sig	oid_egk_sig	oid_smc_b_osig	oid_smc_b_aut
intendedKeyUsage	digitalSignatur	nonRepudiation	nonRepudiation	digitalSignatur

Parameter	C.FD.SIG	C.CH.SIG	C.HCI.OSIG	C.HCI.AUT
intendedExtendedKeyUsage	(leer)	(leer)	(leer)	id-kp-clientAuth
OCSP-Graceperiod	24 Stunden	24 Stunden	24 Stunden	24 Stunden
Offline-Modus	nein	nein	nein	nein
Prüfmodus	OCSP	OCSP	OCSP	OCSP

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

A_27498 -Anbieter ePA-Aktensystem - Offline-Datensicherung

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

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

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

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

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

A_27500 -Anbieter ePA-Aktensystem - Rollentrennung Administratoren für Backup- und Produktionsdaten

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

2.4 Validierungsaktenkonto

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

685 Nummernkreisen, bzw. die Ausgabe einer KVNR in Form einer Prüfkarte, erfolgt durch die
686 gematik.

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

694 Folgende Anwendungsfälle sollen mit den Validierungsaktenkonten adressiert werden:

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

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

703 **A_18168-01 -Anbieter des ePA-Aktensystem - Validierungsaktenkonto für** 704 **gematik**

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

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

711 [**<=**]

712 **A_18169-02 -Anbieter des ePA-Aktensystem - Validierungsaktenkonto für** 713 **eigene Zwecke**

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

718 [**<=**]

719 **A_22522-01 -Anbieter des ePA-Aktensystems - Validierungskonto für Dritte**

720 Der Anbieter des ePA-Aktensystems MUSS auf Antrag der gematik

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

726 [**<=**]

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

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

733 **A_26187 -Anlage von Validierungsaktenkonten**

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

736 **A_26188 -Anbieter des ePA-Aktensystems -Aktivierung von**
737 **Validierungsaktenkonten**

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

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

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

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

753 **A_22684-01 -Validierungsaktenkonten im Store-Review der FdVs**

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

760 **A_22942 -Besonderheiten bei Validierungskonten für StoreReviews**

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

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

771 [<=]

772 **A_26209 -Prüfung auf Vertretungsberechtigung für Prüfidentität**

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

A_24539 -Nutzung von Validierungsaktenkonten via FdV

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

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

2.5 Tracing in Nichtproduktivumgebungen

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

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

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

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

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

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

[≤]

A_21891-01 -Tracing, Tiger-Standalone-Proxy

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

A_22581 -Tracing, Abschaltbarkeit

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

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

2.6 Benutzerführung

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

A_15842 -Anbieter ePA-Aktensystem - Ergonomie der Benutzerführung

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

DIN-Normen und Verordnungen zur Beachtung:

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

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

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

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

BITV 2.0 - Barrierefreie Informationstechnik-Verordnung

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

Insbesondere sollen deshalb neben der Übernahme der international anerkannten Standards für barrierefreie Webinhalte, die Web Content Accessibility Guidelines (WCAG)

862 2.1, auch die Belange gehörloser, hör-, lern- und geistig behinderter Menschen
863 berücksichtigt werden.

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

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

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

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

874 2.7 Useragent

875 **A_22470-06 -Definition x-useragent**

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

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

884 Beispiel: "CLIENTID1234567890AB/2.1.12-45"

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

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

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

901 2.8 Performance aus Anwendersicht

902 Im Gegensatz zu den Performancevorgaben, welche in [gemSpec_Perf] gemacht werden
903 und welche lediglich die Aktivitäten im Aktensystem berücksichtigen, stellt sich die

904 Leistungsfähigkeit und Nutzbarkeit in der Wahrnehmung der Clients oftmals anders dar.
 905 Aus diesem Grund werden die Endgeräte (Primärsystem und FdV) für definierte
 906 Anwendungsfälle (sogenannte UX-Usecases) dazu verpflichtet, eigene Messungen
 907 durchzuführen und diese Messwerte an eine definierte Schnittstelle im Aktensystem zu
 908 übermitteln. Das Aktensystem verarbeitet diese Informationen und leitet das
 909 konsolidierte Ergebnis im Rahmen der Betriebsdatenlieferung weiter an die gematik. Auf
 910 diese Weise erhalten sowohl die gematik (im Rahmen der Gesamt-
 911 Produktverantwortung) als auch die Anbieter der Aktensysteme Informationen darüber,
 912 wie die Anwendung ePA bei den Nutzern (insb. in der LEU und bei Versicherten)
 913 hinsichtlich bestimmter Kernfunktionalitäten wahrgenommen wird.

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

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

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

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

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

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

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

939

3 Funktionsmerkmale

940

3.1 Aktenkonto eines Versicherten (Health Record)

941
942
943
944
945

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

946
947

3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte

948
949
950
951
952

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

953
954
955
956

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

957
958
959
960

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

961
962
963
964
965

A_23886 -Anbieter ePA-Aktensystem - Keine Aktenkontoanlage bei Widerspruch des Versicherten

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

966
967
968

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

969
970
971
972
973

A_25181 -Anbieter ePA-Aktensystem - Aktenkontoanlage bei Zurücknahme des Widerspruchs des Versicherten

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

974
975

3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger

976
977
978
979

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

3.1.2 Lebenszyklus und Zustände eines Aktenkontos

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

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

Tabelle 2: Zustandswechsel im Lebenszyklus eines Aktenkontos

Zustand	Erläuterung	zulässige Transitionen	Folgezustand
UNKNOWN	Für einen Versicherten existiert kein Aktenkonto.	Konto initialisieren	Initialized <u>INITIALIZED</u>
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 <u>UNKNOWN</u>
		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 <u>ACTIVATED</u>
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 <u>SUSPENDED</u>
		Widerspruch gegen die Nutzung der ePA	Unknown <u>UNKNOWN</u>

Zustand	Erläuterung	zulässige Transitionen	Folgezustand
		<u>Eine Datenmigration kann nicht durchgeführt werden.</u>	<u>MAINTENANCE</u>
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 <u>UNKNOWN</u>
		Der Bereitstellungszeitraum des Exportpakets ist abgelaufen.	Activated <u>ACTIVATED</u>
<u>MAINTENANCE</u>	<u>Das Aktenkonto kann aus Wartungsgründen derzeit nicht verwendet werden.</u> <u>Dies kann z. B. der Fall sein, wenn Datenmigrationen bei der Aktualisierung auf eine neuere ePA-Versionen noch nicht durchgeführt werden konnte.</u>	<u>Maintenance wird erfolgreich durchgeführt.</u>	<u>ACTIVATED</u>
		<u>Vorbereitung des Umzugs des Aktenkontos zu einem anderen Anbieter (Erstellung des Exportpakets)</u>	<u>SUSPENDED</u>
		<u>Widerspruch gegen die Nutzung der ePA</u>	<u>UNKNOWN</u>

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

991 3.1.3 Anlage eines neuen Aktenkontos

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

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

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

A_24336 -Anbieter ePA-Aktensystem—Identifizierung eines

~~Aktenkontos~~Anbieter ePA-Aktensystem - Identifizierung eines Aktenkontos

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

A_23775 -Anbieter ePA-Aktensystem - Neues Aktenkonto anlegen

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

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

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

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

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

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

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

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

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

A_24790-01 -Anbieter ePA-Aktensystem - keine unbegründeter Import eines Aktenkontos

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

A_15870-02 -Anbieter ePA-Aktensystem - Abbruch bei Nichtverfügbarkeit anderer Anbieter

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

A_27344 -Anbieter ePA-Aktensystem - Abbruch bei fehlgeschlagenem Import

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

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_24369-01A_24369 -Anbieter ePA-Aktensystem - Initialisierung des** 1072 **Aktenkontos**

1073 Der Anbieter des ePA-Aktensystems MUSS die Initialisierung der Bestandteile

- 1074 • Consent Decision Management (initiale Entscheidungen)
- 1075 • Constraint Management (Policies)
- 1076 • Entitlement Management (initiale Befugnisse und Befugnisausschlüsse)
- 1077 • Information Service (initiale Entscheidungen "Versorgungsprozess")
- 1078 • XDS Document Service (statische Aktenkontoinhalte)
- 1079 • Device Management
- 1080 • Authorization Service
- 1081 • Audit Event Service
- 1082 • Medication Service

- 1083 • MHD Service

- 1084 • Patient Service

1085 vor der Aktivierung eines Aktenkontos durchführen. Die genannten Bestandteile MÜSSEN
1086 nach der Aktivierung des Aktenkontos sofort nutzbar sein. [<=]

1087 Im Zustand INITIALIZED obliegt es dem Anbieter, ein Aktenkonto mittels administrativer
1088 Eingriffe in die verschiedenen Bestandteile des Aktensystems und -kontos auf die
1089 Aktivierung vorzubereiten bzw. zu konfigurieren.

1090 **A_26005 -ePA-Aktensystem – Optionale Schnittstelle zum Einbringen von** 1091 **initialen Befugnissen**

1092 Das ePA-Aktensystem KANN eine Schnittstelle für Kostenträger anbieten, über die
1093 Kostenträger die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle
1094 ins ePA-Aktensystem einbringen können. [<=]

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

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

[<=]

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

A_24335 -Anbieter ePA-Aktensystem - Neues Aktenkonto aktivieren

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

3.1.4 Löschen eines Aktenkontos

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

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

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

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

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

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

A_25289 -Anbieter ePA-Aktensystem - Löschen des Aktenkontos durch den Kostenträger

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

3.2 Health Record Relocation Service

Transfer eines Aktenkontos zu einem neuen Anbieter (Aktenkontoumzug).

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

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

A_24786 -Health Record Relocation Service - Realisierung der Schnittstelle I_Health_Record_Relocation_Service

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

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

A_24821 -Health Record Relocation Service - Suspendierung des Aktenkontos

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

A_24827 -Health Record Relocation Service - Reaktivierung des Aktenkontos

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

Falls der Vorgängerstatus zu SUSPENDED der Status MAINTENANCE war, ist dennoch ein Wechsel nach ACTIVATED unproblematisch. Ggf. stellt das Aktensystem anschließend dann erneut fest (z. B. aufgrund einer fehlschlagenden Datenmigration), dass das Aktenkonto in den Zustand MAINTENANCE versetzt werden muss.

A_25005-04A_25005-03 -Health Record Relocation Service - Daten des Exportpakets

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

- XDS Document Service
- Medication Service
- Consent Management
- Constraint Management

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

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

[<=]

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

A_25605 -Health_Record_Relocation_Service - Erstellung des Exportpakets

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

A_25012 -Health Record Relocation Service - Signatur der Befugnisse

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

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

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

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

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

Befugnis	Claim Name	Claim	Beispiel
	"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

1211 [\leq]

1212 Der Wert "ES256" (JWS-Parameters "alg") gilt auch für die Kurve "brainpoolP256r1" (also
1213 nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu
1214 erstellen."

1215 **A_24787-01 -Health Record Relocation Service - Verschlüsselung des** 1216 **Exportpaketes**

1217 Der Health Record Relocation Service MUSS sicherstellen, dass Exportpakete
1218 ausschließlich verschlüsselt für den Download zu einem anderen Betreiber zur Verfügung
1219 stehen. Für die Verschlüsselung MUSS das kryptographische Material des ENC-Zertifikats
1220 verwendet werden, welches mittels der Regel hsm-r7 vom VAU-HSM abgerufen
1221 wurde.[\leq]

1222 **A_24942 -Health Record Relocation Service – Prüfung Provider ENC Zertifikat**

1223 Der Health Record Relocation Service MUSS das übergebene Provider ENC-Zertifikat
1224 mittels TUC_PKI_018 (OCSP-Graceperiod=12h, PolicyList= oid_fd_enc, professionOID =
1225 oid_epa_vau) prüfen und ungültige Zertifikate mit der Fehlermeldung "
1226 CERTIFICATE_INVALID " ablehnen.[\leq]

1227 **A_21750 -Health Record Relocation Service – Integritätsschutz Exportpaket**

1228 Der Health Record Relocation Service MUSS das erstellte Exportpaket mit einem "Digest"
1229 HTTP Response Header (<https://tools.ietf.org/html/rfc5843>) als
1230 Integritätsschutz versehen und dabei als Digest Algorithmus SHA-256verwenden.
1231 Beispiel Digest-Header:
1232 Digest: SHA-
1233 256=MWVkmWQxYTRiMzk5MDQ0MzI3NGU5NDEyZTk5OWY1ZGFmNzgyZTJlODYzYjRjYzFh
1234 OTlMNTQwYzI2M2QwM2U2MQ==
1235 [\leq]

1236 **A_15051 -Health Record Relocation Service - Authentisierung gegenüber einem** 1237 **neuen Aktenanbieter**

1238 Der Health Record Relocation Service, welcher das Exportpaket zur Verfügung stellt,
1239 MUSS sich beim Abruf des Exportpakets durch ein anderes ePA-Aktensystem mit der
1240 TLS-Identität oid_epa_mgmt und Zertifikatsprofil C.FD.TLS-S authentisieren.
1241 [\leq]

1242 **A_15048 -Health Record Relocation Service - Authentifizierung des neuen** 1243 **Aktenanbieters**

1244 Der Health Record Relocation Service MUSS den Abruf des Exportpakets durch ein
1245 anderes ePA-Aktensystem ablehnen, wenn sich der abrufende Client nicht als ePA-

1246 Aktensystem in der Rolle `oid_epa_mgmt` in einem TLS-Zertifikat C.FD.TLS-C
 1247 authentisiert. [`<=`]

1248 **A_17236 -Health Record Relocation Service - Prüfung der TLS-Zertifikate**

1249 Der Health Record Relocation Service MUSS bei der Authentifizierung eines anderen
 1250 Aktensystems beim Abruf des Exportpakets die Prüfung der verwendeten TLS-Zertifikate
 1251 entsprechend TUC_PKI_018 durchführen. Zur Prüfung des TLS-Zertifikats C.FD-TLS-S
 1252 sind dabei die Parameter `PolicyList=oid_fd_tls_s`, `IntendedKeyUsage=digitalSignature`,
 1253 `intendedExtendedKeyUsage=id-kp-serverAuth`, `OCSP-Graceperiod=60 Minuten`, `Offline-`
 1254 `Modus=nein` zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD-TLS-C sind dabei die
 1255 Parameter `PolicyList=oid_fd_tls_c`, `IntendedKeyUsage=digitalSignature`,
 1256 `intendedExtendedKeyUsage=id-kp-clientAuth`, `OCSP-Graceperiod=60 Minuten`, `Offline-`
 1257 `Modus=nein` zu verwenden.
 1258 [`<=`]

1259 **A_15703 -Health Record Relocation Service - Verfügbarkeit Export-Paket**

1260 Der Health Record Relocation Service MUSS ein erstelltes Export-Paket für maximal
 1261 sieben Kalendertage zum Abruf durch einen anderen Anbieter eines ePA-Aktensystems
 1262 bereithalten. [`<=`]

1263 **A_21239 -Health Record Relocation Service – Verhalten bei Nichtabholen des Exportpakets**

1264 Der Health Record Relocation Service MUSS nach Ablauf des Bereithaltungszeitraums
 1265 entsprechend A_15703* ein erstelltes Export-Paket löschen und den Status des
 1266 Aktensystems von `SUSPENDED` auf `ACTIVATED` zurücksetzen. [`<=`]

1268 *Hinweis: siehe dazu auch 3.2.1.7.3- Nicht erfolgter Download oder fehlende*
 1269 *Rückmeldung durch den neuen Anbieter*

1270 **A_14905-04 -Health Record Relocation Service – Import des Exportpakets des vorhergehenden Aktenkontos**

1271 Der Health Record Relocation Service MUSS das vom vorhergehenden Anbieter ePA-
 1272 Aktensystem des Versicherten bezogene Exportpaket, in das neue
 1273 Aktenkonto importieren und dazu:

- 1275 • das Exportpaket mittels des privaten ENC-VAU-Schlüssels des neuen
 1276 Betreibers entschlüsseln,
- 1277 • den Digest gemäß A_21750-* prüfen,
- 1278 • die Befugnisse mit Regel "rr5" (siehe Tab_AS_Entitlement_Registration_Rules im
 1279 Aktensystem) registrieren und
- 1280 • falls `DocumentEntry.originalURI` im Exportpaket vorhanden ist, wird für jedes
 1281 Dokument eines `SubmissionSet` der Inhalt von `DocumentEntry.URI` durch den
 1282 Inhalt von `DocumentEntry.originalURI` ersetzt. (Hinweis:
 1283 `DocumentEntry.originalURI` darf nicht als eigenständiges Metadatum in die
 1284 Registry übernommen werden, da es lediglich dem Transport des Originalwertes
 1285 von `DocumentEntry.URI` aus dem alten Aktensystem dient.

1286 [`<=`]

1287 **A_28045 -Health Record Relocation Service - Übernahme von Widersprüchen**

1288 Der Health Record Relocation Service MUSS sicherstellen, dass beim Import von
 1289 Widersprüchen zur Sekundärdatennutzung berücksichtigt wird, ob das Feature in der
 1290 abgebenden Akte bzw. in der aufnehmenden Akte unterstützt wird. Dabei MUSS wie folgt
 1291 vorgegangen werden:

- 1292 • Alt unterstützt, neu unterstützt: Die Widersprüche werden unverändert
 1293 übernommen.

- Alt nicht unterstützt, neu nicht unterstützt: Die Widersprüche werden unverändert übernommen.
- Alt unterstützt, neu nicht unterstützt: Die Widersprüche werden als "erteilt" gesetzt.
- Alt nicht unterstützt, neu unterstützt: Die Widersprüche werden als "nicht erteilt" gesetzt.

[<=]

A_27616 -Health Record Relocation Service - Abbruch des Imports eines Exportpakets

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

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

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

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

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

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

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

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

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

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

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

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

Der Health Record Relocation Service des neuen (importierenden) Aktensystems MUSS nach der erfolgreichen oder einer abgebrochenen Übertragung der Inhalte eines Aktenkontos vom bisherigen Anbieter einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

Tabelle 3 : Health Record Relocation Service Protokollierung

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

[<=]

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

3.2.1 Ablauf eines Aktenkontoumzugs

3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter

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

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

- 1362 Die Abfrage eines existierenden Widerspruchs des Versicherten bei einem anderen
1363 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

1364 3.2.1.2 Start Transfer eines existierenden Aktenkontos

- 1365 Hat der Versicherte bei keinem Anbieter einen Widerspruch gegen die Nutzung der ePA
1366 erklärt und existiert bei einem bisherigen Anbieter (alt) ein Aktenkonto, wird der Transfer
1367 der Daten durch das Aktensystem (neu) initiiert.

- 1368 Das Aktensystem (alt), bei welchem das Aktenkonto existiert, bestätigt diese Anfrage
1369 zum Transfer mit einer Vorgangs-ID.

Starten des Transfers	
I_Information_Service_Accounts (bisheriges Aktensystem)	
startRelocation	initiiieren der Exportpaketerstellung

1370 3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen 1371 Anbieter

- 1372 Das Aktensystem (alt) informiert den Anbieter (alt) über die Anfrage zum Transfer und
1373 die Vorgangsnummer. Der Anbieter (alt) öffnet das existierende Aktenkonto des
1374 Versicherten und stößt in der VAU die Erzeugung des Exportpakets an. Der Health Record
1375 Relocation Service beantwortet diese Anfrage durch Rückgabe einer URL für den späteren
1376 Download des Exportpakets durch den neuen Anbieter und startet die Erzeugung des
1377 Exportpakets. Das Aktenkonto wird vor der Paketerstellung auf den Status SUSPENDED
1378 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

- 1379 In dieses Exportpaket werden alle Daten des Aktenkontos gemäß A_25005*
1380 übernommen. Das fertige Exportpaket wird mittels ENC-Zertifikat, welches im VAU-HSM
1381 eingebracht und gespeichert wurde, verschlüsselt und am vorbereiteten Downloadpunkt
1382 bereitgestellt.

1383 3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den 1384 neuen Anbieter

- 1385 Der Anbieter (alt) veranlasst nach Erhalt der Download-URL über das Aktensystem (alt)
1386 den Versand der ~~URL~~ an das Aktensystem (neu).

- 1387 Das Aktensystem (alt) prüft vor der Übermittlung der Download-URL an das Aktensystem
 1388 (neu), ob das Exportpaket für den Download bereitsteht, ggf. wird auf den Abschluss der
 1389 Paketerstellung gewartet. Ist dieses der Fall, erfolgt die Benachrichtigung des
 1390 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

1391 3.2.1.5 Import des Exportpakets durch den neuen Anbieter

- 1392 Der Information Service des Aktensystems (neu) nimmt die Download-URL entgegen und
 1393 übermittelt diese an den Kostenträger (neu). Dieser öffnet den Zugang zum Aktenkonto
 1394 (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

1395 3.2.1.6 Abschluss des Transfers durch beide Anbieter

- 1396 Das Aktensystem (neu) startet den Download des Exportpakets, entschlüsselt dieses und
 1397 übernimmt die Daten in das initialisierte Aktenkonto des Versicherten. Nach
 1398 erfolgreichem Abschluss wird (kann) das Aktenkonto (neu) in den Status ACTIVATED
 1399 überführt werden.

- 1400 Unter Verwendung des Information Service wird das Aktensystem (alt) über den
 1401 erfolgreichen Import und den Abschluss des Transfers informiert. Das Aktenkonto (alt)
 1402 kann daraufhin, ggf. unter Einhaltung weiterer Bedingungen des Kostenträgers bzw.
 1403 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)

1404 3.2.1.7 Fehlersituationen und Handhabung

- 1405 Der gesamte Austausch von Informationen zwischen Aktensystemen und Anbietern kann
 1406 durch die in Schritt 1 erzeugte Vorgangs-ID genau einem konkreten Relocation Vorgang
 1407 zugeordnet werden. Diese Vorgangsnummer wird auch verwendet, wenn das jeweils
 1408 andere Aktensystem über Fehler im Ablauf benachrichtigt werden muss (Incidents).

1409 3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich oder
1410 derzeit nicht möglich

1411 Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter
1412 (alt) das Exportpaket voraussehbar nicht importieren oder widerspricht der Versicherte
1413 nach der Initialisierung des Aktenkontos beim neuen Kostenträger der Nutzung der ePA,
1414 so kann durch Übertragung eines Incidents an das Aktensystem (alt) dieser Sachverhalt
1415 mitgeteilt werden, so dass der Transfervorgang abgebrochen und das Exportpaket nicht
1416 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

1417 Das Aktenkonto wird bei Anbieter (alt) wieder in den Status ACTIVATED gesetzt, um eine
1418 weitere Nutzung zu ermöglichen.

1419 Für einen Transfer zu einem späteren Zeitpunkt muss der Anbieter (neu) den Vorgang
1420 durch Anfrage bei den weiteren Anbietern (alt) und Übermittlung eines ENC-Zertifikats
1421 erneut starten.

1422 3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter

1423 Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter
1424 (alt) das Exportpaket unter Verwendung der übertragenen Download-URL nicht oder
1425 nicht vollständig laden oder die Inhalte des Exportpaketes aufgrund fehlerhafter
1426 Verschlüsselung oder fehlerhafter Struktur oder Inhalte nicht erfolgreich integrieren oder

- 1427 der Anbieter (neu) hat keine Download-URL vom Anbieter (alt) bezogen, so kann durch
 1428 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

- 1429 Das Aktenkonto verbleibt beim neuen Anbieter in Status INITIALIZED. Die
 1430 Incidentmeldung an den Anbieter (alt) kann durch Kommunikation der Anbieter und/oder
 1431 Betreiber untereinander zum Zweck der Problemlösung ergänzt werden.
- 1432 Der Anbieter (alt) meldet die Korrektur durch erneuten Versand einer Download-URL an
 1433 den Anbieter (neu) für den unterbrochenen Vorgang.
- 1434 Es obliegt dem Anbieter (alt), bei zeitlich aufwendigen Korrekturen das Aktenkonto
 1435 zunächst für eine weitere Nutzung wieder zu aktivieren (Status ACTIVATED) und nach
 1436 Abschluss der Korrektur wieder in den Status SUSPENDED zu überführen.
- 1437 Es obliegt dem Anbieter (alt) auch, bei zeitlich aufwendigen Korrekturen den Transfer
 1438 durch Senden des Incidents "relocationAborted" an den Anbieter (neu) abubrechen und
 1439 das Aktenkonto zur weiteren Nutzung wieder zu aktivieren (Status ACTIVATED). Der
 1440 Transfer muss dann durch den Anbieter (neu) erneut gestartet werden.
- 1441 *3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter*
- 1442 Ruft ein neuer Anbieter ein bereitgestelltes Exportpaket nicht ab oder erfolgt durch den
 1443 neuen Anbieter keine Benachrichtigung über einen erfolgreichen Abschluss des Transfers

1444 oder einen Fehler beim Import des Exportpakets, dann kann eine Benachrichtigung an
1445 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.

1446 Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei
1447 Anbieter (alt) auf den Status ACTIVATED gesetzt, um eine weitere Nutzung zu
1448 ermöglichen. Exportpaket und Downloadlink können gelöscht werden. Der Transfer muss
1449 durch den Anbieter (neu) erneut gestartet werden.

1450 *3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter*

1451 Ein Anbieter (alt) kann den Abbruch eines angeforderten Transfers an den Anbieter (neu)
1452 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.

1453 Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei
1454 Anbieter (alt) auf den Status ACTIVATED zurückgesetzt, wenn dieses schon den Status

1455 SUSPENDED hat, um eine weitere Nutzung zu ermöglichen. Exportpaket und
1456 Downloadlink können gelöscht werden. Der Transfer muss durch den Anbieter (neu)
1457 erneut gestartet werden.

1458 **3.3 Sichere Speicherung sensibler Schlüssel und Informationen im** 1459 **VAU-HSM**

1460 Im Folgenden wird beschrieben, welche Informationen in einem HSM (als VAU-HSM
1461 bezeichnet) zu speichern sind.

1462 Verständnishinweis: Die HMAC-Schlüssel (symmetrische Schlüssel) für die Prüfung der
1463 VSDM+-Prüfnachweise [gemSpec_SST_FD_VSDM], [C_11321] werden von den VSDM-
1464 Betreibern erzeugt und für die ePA-VAUs der ePA-Betreiber verschlüsselt exportiert. Die
1465 Schlüssel und auch die Export/Import-Vorgänge (Mehr-Augen-Prinzip) sind die gleichen
1466 wie sie auch für/bei der E-Rezept-VAU verwendet werden.

1467 **A_24611-06 -ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und** 1468 **Informationen für VAU-Betrieb**

1469 Das ePA-Aktensystem MUSS sicherstellen, dass folgende, für den Betrieb der VAU
1470 notwendigen Schlüssel und Informationen in einem HSM (als VAU-HSM bezeichnet)
1471 gespeichert werden:

- 1472 • privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
1473 (u.a. genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- 1474 • ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- 1475 • ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- 1476 • privater Schlüssel der Verschlüsselungsidentität der VAU
- 1477 • privater Schlüssel der Signaturidentität der VAU
- 1478 • Zertifikat C.FD.ENC mit professionOID `oid_epa_vau` für die
1479 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- 1480 • Zertifikat C.ZD.SIG mit professionOID `oid_popp-token` für die Token-Signatur-
1481 Identität des PoPP-Services
- 1482 • Masterkeys für die Ableitung der versichertenindividuellen
1483 Datenpersistierungsschlüssel
- 1484 • Masterkeys für die Ableitung der versichertenindividuellen
1485 Befugnispersistierungsschlüssel
- 1486 • Masterkeys für die Ableitung der versichertenindividuellen
1487 Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und
1488 Überschlüsselung")
- 1489 • symmetrische Schlüssel für die HMAC-Prüfung der VSDM-Prüfziffern (jeweils einen
1490 pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als
1491 gemeinsames Geheimnis bezeichnet werden.
- 1492 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- 1493 • Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für
1494 die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf.
1495 für Service-VAUs)
- 1496 • Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

1497 [\leq]

1498 Hinweis:

1499 Es gelten die Anforderungen aus [gemSpec_Krypt#3.18 VSDM-Prüfziffer Version 2] für
 1500 ein ePA-Aktensystem in der Rolle "Prüfziffer Version 2 prüfendes System". Aus den ins
 1501 HSM importierten gemeinsamen Geheimnissen erfolgt im HSM eine Schlüsselableitung
 1502 (A_27299-*) der für die Entschlüsselung der Prüfziffer Version 2 benötigten AES/GCM-
 1503 Schlüssel.

1504 **A_26109 -ePA-Aktensystem - Unterschiedliche private**

1505 **Authentisierungsschlüssel für AK-, Befugnisverifikations- und Service-VAU**

1506 Das ePA-Aktensystem MUSS sicherstellen, dass für die Authentisierungsidentitäten für
 1507 Aktenkontoverwaltungs-VAUs, Befugnisverifikations-VAUs und Service-VAUs
 1508 unterschiedliche private Schlüssel verwendet werden. [\leq]

1509 **A_26110 -ePA-Aktensystem - Unterschiedliche private**

1510 **Authentisierungsschlüssel für unterschiedliche Service-VAUs**

1511 Das ePA-Aktensystem MUSS sicherstellen, dass für unterschiedliche Typen von Service-
 1512 VAUs unterschiedliche private Schlüssel für die Authentisierung genutzt werden. [\leq]

1513 Hinweis zu A_26110: Ein Typ einer Service-VAU könnte beispielsweise eine PDF-
 1514 Konvertierungs-Service-VAU oder eine Pseudonymisierungs-Service-VAU für Daten zur
 1515 Sekundärnutzung sein. Alle Instanzen einer PDF-Konvertierungs-Service-VAU nutzen
 1516 denselben privaten Authentisierungsschlüssel. Die Instanzen der Pseudonymisierungs-
 1517 Service-VAU dürfen den Authentisierungsschlüssel der PDF-Konvertierungs-Service-VAU
 1518 jedoch nicht verwenden.

1519 **A_24612-05 -ePA-Aktensystem - Erzwingen von 4-Augen-Prinzip für Einbringen**
 1520 **und Verwalten von Informationen ins VAU-HSM**

1521 Das ePA-Aktensystem MUSS technisch erzwingen, dass die folgenden, für den Betrieb der
 1522 VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip in das
 1523 VAU-HSM eingebracht und verwaltet werden können:

- 1524 • privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- 1525 • ggf. privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- 1526 • ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- 1527 • privater Schlüssel der Verschlüsselungsidentität der VAU
- 1528 • privater Schlüssel der Signaturidentität der VAU
- 1529 • Zertifikat C.FD.ENC mit professionOID oid_epa_vau für die
 1530 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- 1531 • Zertifikat C.ZD.SIG mit professionOID oid_popp-token für die Token-Signatur-
 1532 Identität des PoPP-Services
- 1533 • symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-
 1534 Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames
 1535 Geheimnis bezeichnet werden.
- 1536 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- 1537 • Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für
 1538 die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf.
 1539 für Service-VAUs)
- 1540 • Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

1541 [\leq]

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

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

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

[<=]

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

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

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

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

- privater Schlüssel der Authentisierungsidentität der VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU ausschließlich durch eine Befugnisverifikations-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität eines Service-VAU-Typs ausschließlich durch eine Service-VAU-Instanz dieses Service-VAU-Typs
- privater Schlüssel der Verschlüsselungsidentität der VAUausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz

- 1587 • privater Schlüssel der Signaturidentität der VAUausschließlich durch eine
1588 Aktenkontoverwaltungs-VAU-Instanz
- 1589 • Zertifikat C.FD.ENC mit professionOID `oid_epa_vau` für die
1590 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibersausschließlich
1591 durch eine Aktenkontoverwaltungs-VAU-Instanz
- 1592 • Zertifikat C.ZD.SIG mit professionOID `oid_popp-token` für die Token-Signatur-
1593 Identität des PoPP-Services
- 1594 • Masterkeys für die Ableitung der versichertenindividuellen
1595 Datenpersistierungsschlüsselausschließlich durch eine Aktenkontoverwaltungs-
1596 VAU-Instanz
- 1597 • Masterkeys für die Ableitung der versichertenindividuellen
1598 Befugnispersistierungsschlüsselausschließlich durch eine Aktenkontoverwaltungs-
1599 VAU-Instanz
- 1600 • Masterkeys für die Ableitung der versichertenindividuellen
1601 Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und
1602 Überschlüsselung") ausschließlich durch die Aktenkontoverwaltungs-VAU-Instanz
1603 oder durch eine dedizierte Überschlüsselungs-VAU
- 1604 • symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-
1605 Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames
1606 Geheimnis bezeichnet werden,ausschließlich durch eine Aktenkontoverwaltungs-
1607 VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz
- 1608 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten
1609 Befugnisse)ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder
1610 eine Befugnisverifikations-VAU-Instanz.
- 1611 [`<=`]

1612 3.4 Befugnisverifikations-Modul

1613 Das Befugnisverifikations-Modul enthält die Regeln zur Befugnisregistrierung (entitlement
1614 registration rules) und die Regeln zum Abruf der versichertenindividuellen
1615 Persistierungsschlüssel (key rules).

1616 Die folgende Abbildung zeigt die zwei möglichen Architekturvarianten für die Ausführung
1617 des Befugnisverifikations-Moduls. In Variante 1 wird es direkt im VAU-HSM ausgeführt. In
1618 Variante 2 wird es in einer Befugnisverifikations-VAU ausgeführt, die zwischen einer
1619 Aktenkontoverwaltungs-VAU und einem VAU-HSM vermittelt und Prüfungen für das VAU-
1620 HSM übernimmt (z. B. prüfen der ID-Token oder registrieren neuer Befugnisse).

1621 In beiden Varianten ist ein Zugriff auf die Schlüssel im VAU-HSM nur durch integrale und
1622 attestierte VAUs möglich. Die Prüfung der VAU-Attestierungstoken verbleibt in beiden
1623 Varianten im VAU-HSM (VAU-Token-Modul). Das VAU-HSM speichert in Variante 2 neben
1624 den Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware
1625 für die VAU der Aktenkontoverwaltung zusätzlich auch die Hashwertrepräsentationen der
1626 erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der
1627 Befugnisverifikations-VAU. Ein Zugriff auf das HSM ist dann nur mit einem validen
1628 Attestierungstoken für die Aktenkontoverwaltung-VAU und die Befugnisverifikations-VAU
1629 möglich.

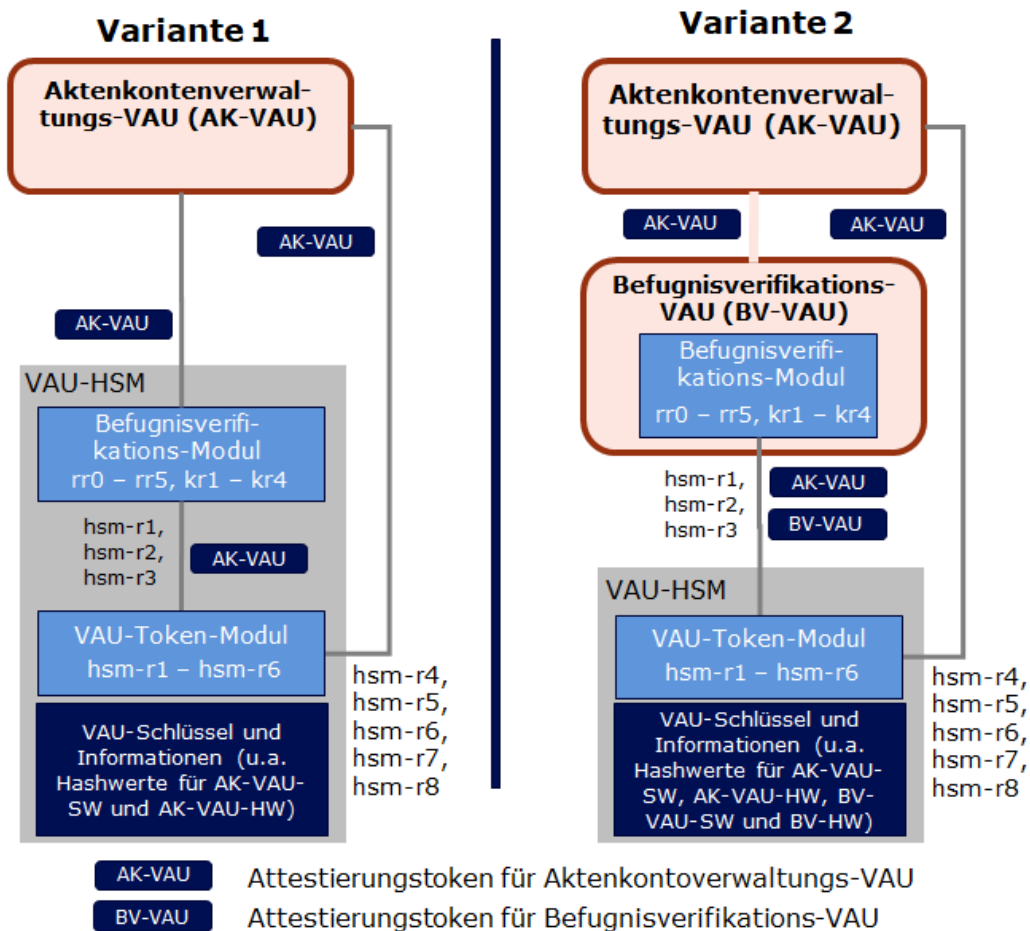


Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls

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

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

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

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

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

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

3.4.1 VAU-Token-Modul

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

A_24712-01 -ePA-Aktensystem - VAU-Token-Modul nur durch Befugnisverifikations-Modul oder Aktenkontoverwaltungs-VAU aufrufbar

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

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

Das VAU-Token-Modul MUSS die in Tabelle *Tab_AS_VAU-Token-Modul_Rules* definierten Regeln umsetzen. [\leq]

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"> prüfen der Signatur(en)des(r) VAU-Attestierungstoken (herstellerspezifisch) prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 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>

Regel	Beschreibung
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 Datenpersistierungsschlüssel <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>

Regel	Beschreibung
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 erfolgreicher 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>

Regel	Beschreibung
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 • 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>

Regel	Beschreibung
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>

Regel	Beschreibung
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"> • <i>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder einer Service-VAU</i> • <i>Ableitungsvektor dv</i> • <i>Label für Masterkey (opt.)</i> <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>

1659

1660 **A_24667 -ePA-Aktensystem -VAU-HSM - Prüfen des VAU-Attestierungstokens**
 1661 Das VAU-HSM MUSS bei der Prüfung eines VAU-Attestierungstokens sicherstellen, dass
 1662 dieses zeitlich gültig ist und Replay-Attacken abwehren.[<=]

1663 **A_26303 -ePA-Aktensystem - Abgeleitete Verschlüsselungsschlüssel sind**
 1664 **ausschließlich einer VAU zugänglich**
 1665 Das ePA-Aktensystem MUSS sicherstellen, dass ein mit Regel hsm-r8 abgeleiteter
 1666 Schlüssel ausschließlich einer VAU zugänglich ist und ausschließlich mittels AES/GCM
 1667 analog [gemSpec_Krypt#GS-A_4389] verwendet wird.[<=]

1668 3.4.2 Regeln des Befugnisverifikations-Moduls

1669 Die folgende Tabelle zeigt die Regeln des Befugnisverifikations-Moduls im Überblick.

1670 **Tabelle 5: Überblick über die Regeln des Befugnisverifikations-Moduls**

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
rr0	Mit dieser Regel werden ID-Token im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr1	Mit dieser Regel werden vom Aktenkontoinhaber am ePA-FdV erstellte Befugnisse im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr2	Mit dieser Regel werden vom Vertreter am ePA-FdV erstellte Befugnisse für das Aktenkonto des Versicherten im Aktensystem registriert. Die im ePA-FdV erstellen Befugnisse sind vom Vertreter mittels Signaturdienst signiert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr3	Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das Stecken der eGK in einer Leistungserbringerumgebung oder aufgrund eines PoPP-Tokens ergeben.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr4	Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der Anlage eines Aktenkontos im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>

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

1671

1672 **A_24573-03 -ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls**

1673 Das Befugnisverifikations-Modul MUSS die in den
 1674 Tabellen *Tab_AS_Entitlement_Registration_Rules* und *Tab_AS_SDS-Key_Rules* definierten
 1675 Regeln umsetzen. [<=]

1676
1677

Tabelle 6: Tab_AS_Entitlement_Registration_Rules - Regeln zur Registrierung von 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-Fachdiensts (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 (oid_idpd_sek, oid_idpd oder oid_erp-vau). b. ruft das Befugnisverifikations-Modul die VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und dem HSM-ID-Token auf. <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><i>Mit dieser Regel werden vom Aktenkontoinhaber am ePA-FdV erstellte Befugnisse im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.</i></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 oder KVNR, Gültigkeitszeitraum) signiert vom Versicherten <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis2 = (KVNR Aktenkonto, Telematik-ID oder KVNR, 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 KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt <p>oder prüfen des HSM-ID-Tokens</p> <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 KVNR im HSM-ID-Token mit der KVNR 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 KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der "KVNR Aktenkonto" in der Befugnis1 übereinstimmt. d. prüfen, dass das JWT gemäß A_24587-* zeitlich gültig ist ($iat - 15s \leq \text{aktuelle Zeit} \leq exp + 15s$) 3. Falls die Prüfungen in 1) bis 2) erfolgreich waren, erstellt das Befugnisverifikations-Modul die Befugnis2. Die Inhalte werden aus Befugnis1 übernommen mit folgender Ausnahme:
-----	---

Regel	Beschreibung
	<p>Für eine Befugnis1 mit oid = oid_ncpeh wird die Gültigkeit validTo in Befugnis2 auf aktuelle Zeit + 1 Stunde gesetzt.</p> <ol style="list-style-type: none">4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und 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.5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

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"> 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 KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt <p>oder prüfen des HSM-ID-Tokens</p> <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 KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt. 2. prüfen der Befugnis1 und Befugnis2 <ol style="list-style-type: none"> a. prüfen der Signatur von Befugnis1 gemäß A_25042-* (Zertifikatsprofil C.CH.SIG) b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_versicherter</code> ist c. prüfen des CMAC von Befugnis2 d. prüfen, dass die Telematik-ID in Befugnis 1 keine KVNR ist (Vertreter dürfen keine weiteren Vertreter befugen) e. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der „KVNR Vertreter“ in der Befugnis2 übereinstimmt
-----	---

Regel	Beschreibung
	<ul style="list-style-type: none"> f. prüfen, ob die „KVNR Aktenkonto“ in Befugnis 1 mit der „KVNR Aktenkonto“ in Befugnis2 übereinstimmt g. prüfen, dass das JWT gemäß A_24587-* zeitlich gültig ist ($i_{at} - 15s \leq \text{aktuelle Zeit} \leq e_{exp} + 15s$) 3. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis3 vom Befugnisverifikations-Modul erstellt. Die Inhalte werden aus Befugnis1 übernommen. 4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis3 <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 <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. prüfen der inneren Struktur nach Prüfschritt 6 gemäß A_27279-* (d.h. eGK ist nicht gesperrt) 5. prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer (prüfziffer.iat) nicht länger als 20 Minuten zurückliegt (prüfziffer.iat - 30s <= aktuelle Zeit < prüfziffer.iat + 20 Minuten + 15s, Hinweis in der Prüfziffer gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben) 6. prüfen des prüfziffer.hcv nach Prüfschritt 8 gemäß A_27279-* bzgl. des hcv im JWT 7. Falls die Prüfungen in 1) bis 6) erfolgreich waren, und die VAU-HSM Regel hsm-r3 den Klartext der inneren Struktur der Prüfziffer zurückgeliefert hat, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt: <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.
-----	---

Regel	Beschreibung
	<p>8. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis</p> <p>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> <p>9. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis sowie die entschlüsselte innere Struktur der Prüfziffer im Klartext gemäß A_27278-* als Ergebnis des Regelaufrufs zurück.</p> <p><u>Szenario PoPP-Token:</u></p> <ol style="list-style-type: none"> 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 (PoPP-Token.iat - 30s <= aktuelle Zeit < PoPP-Token.iat + 20 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. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis <p>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis zurück.

Regel	Beschreibung
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 <code>oid_kostentraeger</code> bzw. <code>oid_ombudsstelle</code> ist c. prüfen, ob die Telematik-ID im Signaturzertifikat C.HCI.OSIG der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle mit der Telematik-ID in der Befugnis1 übereinstimmt 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 erstellt. Die Inhalte der Befugnis2 sind: <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 <code>hsm-r1</code> 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.

Regel	Beschreibung
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"> Prüfen der Befugnis1 <ol style="list-style-type: none"> prüfen der Signatur gemäß A_25042-* (C.FD.SIG) prüfen, ob im Signaturzertifikat C.FD.SIG der professionOIDoid_epa_vauist prüfen, dass das Signaturzertifikat C.FD.SIG nicht auf das importierende Aktensystem ausgestellt ist. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 mit den Inhalten aus Befugnis1 erstellt. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 <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 Befugnis2 als Ergebnis des Regelaufrufs zurück.

1678

1679 **A_24690-01 -ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen des ID-Tokens**

1680 Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung eines ID-Tokens durchführen:

- 1683 • 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),
- 1684 • das ID-Token muss zeitlich gültig sein (Felder: iat, exp),
- 1685 • das ID-Token muss im Feldauddas ePA-Aktensystem eingetragen haben.

1688 [**<=**]

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

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

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

[<=]

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

1705 **Tabelle 7: Tab_AS_SDS-Key_Rules Key Rules - Regeln zur Ableitung der**
1706 **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 <code>oid_idpd_sek</code> ist oder prüfen des HSM-ID-Tokens b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <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 KVN-R aus dem ID-Token und den Labeln der zu verwendenden Befugnispersistierungs- und Datenpersistierungs-Masterkeys zur Ableitung von Befugnis- und Datenpersistierungsschlüssel aufgerufen. <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert die abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.

Regel	Beschreibung
kr2	<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 hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR und dem Label des Befugnispersistierungs-Masterkeys zur Ableitung des Befugnispersistierungsschlüssels <ol style="list-style-type: none"> 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> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • 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 <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. gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) oder prüfen des HSM-ID-Tokens <ol style="list-style-type: none"> 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"> 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 <ol style="list-style-type: none"> a. prüfen des CMAC der Befugnis mittels VAU-HSM Regel hsm-r1 <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. b. prüfen, ob dieNutzer-ID im ID-Token bzw. im HSM-ID-Token (KVNR oder Telematik-ID) mit der Befugten-ID in der Befugnis übereinstimmt. c. prüfen, ob die Befugnis noch gültig ist, falls die Befugnis zeitlich begrenzt ist (d. h. ein Gültigkeitszeitraum in der Befugnis enthalten ist). 3. Falls alle Prüfungen in 1) bis 2) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR aus dem ID-Tokenbzw. im HSM-ID-
-----	--

Regel	Beschreibung
	<p>Token und dem Label für den Datenpersistierungs-Masterkey zur Ableitung des Datenpersistierungsschlüssels aufgerufen.</p> <p>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> <p>4. Das Befugnisverifikations-Modul liefert den abgeleiteten Datenpersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.</p>

Regel	Beschreibung
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 • KVN-R (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 Signatur gemäß A_25042-* (C.FD.AUT) b. prüfen, ob die professionOID im Zertifikat C.FD.AUT gleich <code>oid_erp-vau</code> ist c. prüfen des ID-Tokens gemäß A_24658-* oder prüfen des HSM-ID-Tokens d. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <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 KVN-R 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.

Regel	Beschreibung
kr5	<p>Diese Regel wird für die Überschlüsselung verwendet (ggf. mit Umschlüsselung einer Überschlüsselung).</p> <p>Diese Regel kann von einer VAU (AK-VAU oder dedizierte Überschlüsselungs-VAU) verwendet werden um verschlüsselte Akten zu überschlüsseln (vgl. Abschnitt 3.6- Umschlüsselung und Überschlüsselung). Dabei kann es auch zu einer Umschlüsselung einer älteren Überschlüsselung kommen.</p> <p>Sei <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.)</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • 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) <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Liste von Paaren: versichertenindividueller Überschlüsselungsschlüssel (Secure Data Storage Key), Label für verwendeten Überschlüsselungs-Masterkey <p>(Hinweis: Die Liste enthält mindestens ein Element -- im Fall der ersten Überschlüsselung in Intervall 2 (vgl. Abschnitt 3.6))</p> <p>Ablauf: Das VAU-HSM muss des VAU-Attestierungstoken prüfen, ob es sich um eine AK-VAU oder dedizierte Überschlüsselungs-VAU handelt. Falls nein, Abbruch.</p> <p>Das VAU-HSM durchläuft die Label-Liste und führt mit dem entsprechenden Label verbundenen Überschlüsselungs-Masterkey und der KVNR eine Schlüsselableitung durch. Dabei wird im VAU-HSM das spezielle Symbol "<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.</p>

1707

1708 3.5 Vertrauenswürdige Ausführungsumgebung (VAU)

1709 Eine Vertrauenswürdige Ausführungsumgebung (VAU) gewährleistet mit technischen
 1710 Maßnahmen, dass Daten serverseitig im ePA-Aktensystem im Klartext verarbeitet werden
 1711 können, ohne dass einzelne Mitarbeiter des Betreibers auf diese Daten zugreifen können.

1712 Die Datenverarbeitungen der Aktenkontoverwaltung müssen in einer VAU ausgeführt
1713 werden. Diese VAU wird im folgenden als Aktenkontoverwaltungs-VAU bezeichnet. Des
1714 weiteren kann das Befugnisverifikations-Modul in einer VAU ausgeführt werden. Diese
1715 VAU wird im folgenden als Befugnisverifikations-VAU bezeichnet.

1716 **A_25716-02 -ePA-Aktensystem - Services ausschließlich in der VAU**

1717 Das ePA-Aktensystem MUSS sicherstellen, dass die folgenden Services ausschließlich
1718 innerhalb einer VAU ausgeführt werden können und ein Zugriff auf die Schnittstellen
1719 ausschließlich über einen VAU-Kanal erfolgen kann:

- 1720 • Consent Decision Management Service
- 1721 • Entitlement Management
- 1722 • Constraint Management
- 1723 • Device Management
- 1724 • E-Mail Management
- 1725 • Audit Event Service
- 1726 • Authorization Service
- 1727 • Health Record Relocation Service
- 1728 • alle Medical Services
- 1729 • Data Submission Service
- 1730 • Push Notification Management

1731 [**<=**]

1732 In den folgenden Abschnitten werden zunächst die Anforderungen an eine VAU
1733 beschrieben, die sowohl von einer Aktenkontoverwaltungs-VAU als auch
1734 einer Befugnisverifikations-VAU zu erfüllen sind. Die speziellen Anforderungen an eine
1735 Aktenkontoverwaltungs-VAU bzw. an eine Befugnisverifikations-VAU folgen darauf in
1736 separaten Abschnitten.

1737 **3.5.1 Übergreifende VAU-Anforderungen**

1738 **3.5.1.1 Schutz der Integrität der VAU**

1739 Die folgenden Anforderungen stellen die Integrität der VAU sicher.

1740 **A_24613 -ePA-Aktensystem - Bildung Hashwertrepräsentation des VAU-Images**

1741 Der Hersteller des VAU-Images MUSS für seine zugelassenen VAU-Images
1742 Hashwertrepräsentationen bilden. Diese MÜSSEN signiert und die signierten
1743 Hashwertrepräsentationen an die gematik übermitteln. Dabei SOLLEN bezüglich der
1744 kryptographischen Vorgaben zur Signatur die Vorgaben aus [gemSpec_Krypt]
1745 eingehalten werden. [**<=**]

1746 Erläuterung zu A_24613-*:

1747 Bei Intel-SGX sind die durch die Intel-Hardware erzeugten Signaturen RSA-3072-Bit-
1748 Signaturen, bei denen der öffentliche Exponent 3 ist. Dies entspricht nicht den Vorgaben
1749 in [gemSpec_Krypt] für allgemeine RSA-Signaturen (also nicht im SGX-Kontext). Deshalb
1750 steht in A_24613-* diesbezüglich nur eine SOLL-Formulierung. Im Kontext SGX ist der
1751 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. [<=]

1797 **A_24651 -ePA-Aktensystem - Betreiber ergreift Maßnahmen gegen physische**
1798 **Angriffe auf die VAU**

1799 Der Betreiber des ePA-Aktensystems MUSS mit technischen und/oder organisatorischen
1800 Maßnahmen ausschließen, dass ein einzelner Innentäter beim Betreiber des ePA-
1801 Aktensystems physische Angriffe auf eine VAU ausführen kann. [\leq]

1802 **A_24641 -ePA-Aktensystem - Löschen aller Daten beim Beenden einer VAU-**
1803 **Instanz**

1804 Das ePA-Aktensystem MUSS sicherstellen, dass beim Beenden einer VAU-Instanz
1805 sämtliche Daten dieser VAU-Instanz aus flüchtigen Speichern sicher gelöscht werden
1806 oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [\leq]

1807 **A_25244 -ePA-Aktensystem - x-insurantId nicht außerhalb des VAU-Kanals**

1808 Das ePA-Aktensystem MUSS sicherstellen, dass das HTTP Header-Element mit dem
1809 Namen "x-insurantId" nicht außerhalb des VAU-Kanals gesendet wird. [\leq]

1810 **3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU**

1811 **A_26314 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**
1812 **gespeicherten Daten**

1813 Das ePA-Aktensystem MUSS sicherstellen, dass eine VAU-Daten, die im System des
1814 Aktensystembetreibers gespeichert werden sollen und für die keine spezifischen
1815 Anforderungen zum Schutz der gespeicherten Daten existieren, ausschließlich
1816 verschlüsselt gespeichert werden und der verwendete Verschlüsselungsschlüssel mittels
1817 der Regel hsm-r8 vom VAU-HSM abgeleitet wird. [\leq]

1818 Hinweise zu A_26314:

- 1819 • Spezifische Anforderungen zum Schutz der gespeicherten Daten gibt es z.B. für
1820 die Aktenkontoverwaltungs-VAU in Abschnitt 3.5.2.2 und die durch die VAU für
1821 den Betrieb erstellten Protokolle in Abschnitt 3.5.1.5.
- 1822 • Außerhalb der VAU verschlüsselt gespeicherte Daten der ePA3.0, die bisher nicht
1823 mit Regel hsm-r8 verschlüsselt sein konnten, sind beim Öffnen der Akte
1824 umzuschlüsseln und mit einem Schlüssel zu sichern, der mit Regel hsm-r8
1825 abgeleitet wird. Eine Umschlüsselung ohne Öffnen der Akte ist nicht erforderlich.

1826 **A_26322 -ePA-Aktensystem - Unterschiedliche Schlüssel für die**
1827 **Verschlüsselung von außerhalb der VAU gespeicherten Daten bei**
1828 **unterschiedlichen Verarbeitungszwecken**

1829 Falls Daten außerhalb der VAU im System des Aktensystembetreibers gespeichert
1830 werden, MUSS das ePA-Aktensystem sicherstellen, dass für die Verschlüsselung von
1831 Daten, die zu unterschiedlichen Zwecken verarbeitet werden, unterschiedliche
1832 Verschlüsselungsschlüssel genutzt werden. [\leq]

1833 Hinweis zu A_26322: Verarbeitungszwecke für Daten sind beispielsweise die
1834 Verarbeitung von Daten zum Zwecke der Sekundärnutzung (sieheData Submission
1835 Service) oder die Verarbeitung von Daten für die Nutzerverwaltung im Aktensystem
1836 (insbesondere Geräteinformationen und E-Mail-Adressen).

1837 **3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM**

1838 **A_24653 -ePA-Aktensystem - Sichere Verbindung zwischen VAU und VAU-HSM**

1839 Das ePA-Aktensystem MUSS technisch sicherstellen, dass zwischen einer VAU und einem
1840 VAU-HSM eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die
1841 vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des
1842 Betreibers des Aktensystems schützen. [\leq]

3.5.1.5 Logging und Monitoring

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

A_24910 -ePA-Aktensystem - Erlaubte Zwecke der Betreiberprotokolle

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

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

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

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

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

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

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

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

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

A_24911 -Löschfristen Protokolle

Das ePA-Aktensystem MUSS sicherstellen, dass die

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

[\leq]

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

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

gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik

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

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

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

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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

- 1937 VAU-Instanz auswirken können.
1938 [\leq]
- 1939 **A_24637 -ePA-Aktensystem - Maximale Health Record Context in einer VAU-**
1940 **Instanz**
1941 Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Health Record Context
1942 gleichzeitig in einer VAU-Instanz laufen können.
1943 [\leq]
- 1944 **A_25028 -ePA-Aktensystem - Keine Kommunikation zwischen**
1945 **Aktenkontoverwaltungs-VAUs**
1946 Das ePA-Aktensystem MUSS sicherstellen, dass es keine direkte Kommunikation
1947 zwischen VAU-Instanzen von Aktenkontoverwaltungs-VAUs gibt. [\leq]
- 1948 **A_26111 -ePA-Aktensystem - Keine Kommunikation zwischen Health Record**
1949 **Contexts**
1950 Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer
1951 Aktenkontoverwaltungs-VAU-Instanz keine Kommunikation zwischen Health Record
1952 Contexts gibt. [\leq]
- 1953 **A_24639 -ePA-Aktensystem - Löschen aller Daten beim Beenden eines Health**
1954 **Record Context**
1955 Die VAU MUSS sicherstellen, dass beim Beenden eines Health Record Context sämtliche
1956 Daten dieses Health Record Context aus flüchtigen Speichern sicher gelöscht werden
1957 oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [\leq]
- 1958 **A_24640 -ePA-Aktensystem - Löschen aller Daten beim Beenden einer User**
1959 **Session**
1960 Die VAU MUSS sicherstellen, dass beim Beenden einer User Session sämtliche Daten
1961 dieser User Session aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf
1962 diese Daten technisch ausgeschlossen ist. [\leq]
- 1963 *Hinweis zu A_24639-*, A_24640-* und A_24648-*: Eine zeitliche Verzögerung des*
1964 *Löschens ist tolerabel, sofern ein sofortiges Löschen aufgrund der Architektur des*
1965 *Aktensystemherstellers aus Performanzgründen nicht sinnvoll ist. In diesem Fall ist ein*
1966 *geeigneter Kompromiss zwischen dem Löschzeitpunkt und der Performanz zu wählen.*
- 1967 **A_25231 -ePA-Aktensystem - Schließen des Health Record Context beim**
1968 **Beenden einer User Session**
1969 Die VAU MUSS sicherstellen, dass beim Beenden einer User Session alle mit dieser User
1970 Session verknüpften Health Record Context beendet werden, wenn der jeweilige Health
1971 Record Context nicht mit mindestens einer weiteren User Session verknüpft ist. [\leq]
- 1972 **A_25051 -ePA-Aktensystem - VAU-Kanal endet immer in einer**
1973 **Aktenkontoverwaltungs-VAU**
1974 Die VAU MUSS sicherstellen, dass ein VAU-Kanal von einem Client der ePA (ePA-Client
1975 oder ePA-FdV) ausschließlich in einer Aktenkontoverwaltungs-VAU endet. [\leq]
- 1976 Hinweis: Der VAU-Kanal darf z.B. nicht in einer Befugnisverifikations-VAU enden.
- 1977 **3.5.2.2 Schutz der Daten bei Speicherung außerhalb der**
1978 **Aktenkontoverwaltungs-VAU**
1979 Die folgenden Anforderungen gewährleisten den Schutz der beim Betreiber des ePA-
1980 Aktensystems persistierten Daten von Aktenkonten. Die Verschlüsselung der Daten eines
1981 Versicherten erfolgt mit seinem versichertenindividuellen Daten- und
1982 Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel sind
1983 in [gemSpec_Krypt#3.15.2] festgelegt.

- 1984 **A_24643 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**
 1985 **gespeicherten Daten mit dem Datenpersistierungsschlüssel**
 1986 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten
- 1987 1. Daten des FHIR-Data Service
 - 1988 2. Daten des XDS Document Service
 - 1989 3. Daten des Audit Event Service (Protokolle für den Versicherten zum Zwecke der
 - 1990 Datenschutzkontrolle)
 - 1991 4. Daten des Constraint Managements (Policies zu verborgenen Daten)
 - 1992 5. Daten des Consent Managements (Widersprüche des Versicherten)
- 1993 vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb
 1994 des Health Record Context mit dem zum Health Record gehörenden
 1995 versichertenindividuellen Datenpersistierungsschlüssel verschlüsselt werden.
 1996 [\leq]
- 1997 **A_24644 -ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**
 1998 **gespeicherten Befugnissen mit dem Befugnispersistierungsschlüssel**
 1999 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten
 2000 Daten des Entitlement Managements, d. h. Befugnisse und Befugnisverbote, vor der
 2001 Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health
 2002 Record Context mit dem zum Health Record gehörenden versichertenindividuellen
 2003 Befugnispersistierungsschlüssel verschlüsselt werden.[\leq]
- 2004 **3.5.2.3 Konsistenz des Systemzustands**
- 2005 **A_24650 -ePA-Aktensystem - Konsistenter Systemzustand eines Health Record**
 2006 **Context**
 2007 Die VAU MUSS sicherstellen, dass ein konsistenter Zustand eines Health Record Context
 2008 auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw.
 2009 wiederhergestellt werden kann.[\leq]
- 2010 **A_24696 -ePA-Aktensystem - Konsistenz bei parallelen Zugriffen**
 2011 Die VAU MUSS auch bei parallelen Zugriffen auf dasselbe Aktenkonto durch mehrere
 2012 Nutzer immer einen konsistenten Zustand des Aktenkontos gewährleisten.[\leq]
- 2013 **3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-**
 2014 **VAU**
- 2015 Eine Befugnisverifikations-VAU ist eine spezielle VAU, in der ausschließlich das
 2016 Befugnisverifikations-Modul ausgeführt wird.
- 2017 **A_24646 -ePA-Aktensystem - Befugnisverifikations-VAU verarbeitet**
 2018 **ausschließlich ein Befugnisverifikations-Modul**
 2019 Das ePA-Aktensystem MUSS sicherstellen, dass in einer Befugnisverifikations-VAU
 2020 ausschließlich ein Befugnisverifikations-Modul ausgeführt wird.[\leq]
- 2021 **A_24647 -ePA-Aktensystem - Befugnisverifikations-VAU speichert keine Daten**
 2022 Eine Befugnisverifikations-VAU DARF die Daten, die sie im Rahmen der Regeln des
 2023 Befugnisverifikations-Moduls verarbeitet, NICHT außerhalb der Befugnisverifikations-VAU
 2024 speichern.[\leq]
- 2025 Eine Befugnisverifikations-VAU darf insbesondere die vom VAU-HSM abgeleiteten
 2026 versichertenindividuellen Persistierungsschlüssel nicht speichern.

A_24648 -ePA-Aktensystem - Befugnisverifikations-VAU löscht Daten nach Regelbearbeitung

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

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

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

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

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

3.5.4 Zusätzliche Anforderungen an eine Service-VAU

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

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

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

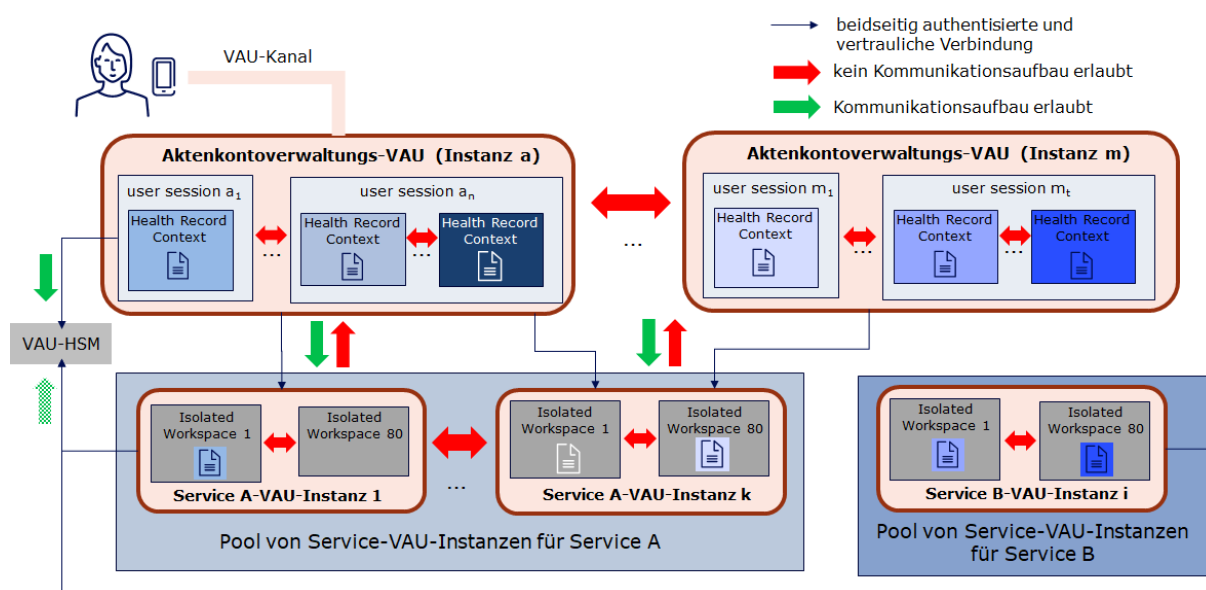


Abbildung 2 - Überblick Service-VAUs

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

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

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

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

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

[<=]

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

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

A_26114 -ePA-Aktensystem - Isolation zwischen unterschiedlichen Service-VAU-Instanzen

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

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

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

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

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

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

A_26117 -ePA-Aktensystem - Keine Kommunikation zwischen Isolated Workspaces

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

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

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

A_26119 -ePA-Aktensystem - Service-VAUs speichern keine Daten in Aktenkonten

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

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

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

A_26123 -ePA-Aktensystem - Service-VAU-Instanzen haben maximale Lebensdauer

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

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

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

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

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

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

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

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

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

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

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

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

3.6 Umschlüsselung und Überschlüsselung

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

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

Falls eine AK-VAU Zugriff auf eine Akte besitzt und zu diesem Zeitpunkt feststellt neue Masterkeys (vgl. betreiberspezifische Schlüssel A_15745-*) existieren, muss sie eine Umschlüsselung durchführen (A_20519-*). Falls eine Akte länger nicht verwendet wird, kann eine AK-VAU keinen Zugang zu den Klartexten der Akte erhalten, da sie nur nach erfolgreicher Nutzerauthentisierung vom VAU-HSM die aktenspezifischen Ableitungsschlüssel erhält. Dann kann eine AK-VAU zunächst auch keine Umschlüsselung vornehmen. Aus diesem Grunde muss eine VAU (entweder eine AK-VAU oder eine dedizierte Überschlüsselungs-VAU) eine Überschlüsselung der Chiffre der Akte vornehmen. Dafür werden Überschlüsselungsschlüssel benötigt. Es gibt analog zu den anderen betreiberspezifischen Schlüssel (A_15745-*) Masterkeys für eine Schlüsselableitung für die Überschlüsselung der Chiffre einer Akte.

A_26197 -ePA-Aktensystem - betreiberspezifische Schlüssel: Überschlüsselungs-Masterkeys

Ein ePA-Aktensystem MUSS sicherstellen, dass die Menge der betreiberspezifischen Schlüssel aus [gemSpec_Krypt#A_15745-*] um die Kategorie Überschlüsselungs-Masterkeys erweitert wird. Für die Überschlüsselungsschlüssel MÜSSEN die gleichen Vorgaben wie für alle betreiberspezifischen Schlüssel gemäß A_15745-* gelten. Die betreiberspezifischen Schlüssel werden mindestens jährlich aktualisiert (A_20519-*), die alten Schlüssel MÜSSEN solange im VAU-HSM verfügbar sein, solange Chiffre im Aktensystem existieren (bspw. Daten einer Akte), die mit diesen Schlüsseln kryptographisch gesichert sind.[<=]

D. h. wie in Abschnitt 3.3 (bspw. A_24611-*) definiert, gibt es bei den Masterkeys drei Kategorien: (1) Aktenpersistierung, (2) Befugnispersistierung und (3) Überschlüsselung. Initial startet der Betrieb eines Aktensystems mit je einem Schlüssel in den ersten zwei Kategorien. Nach maximal einem Jahr (A_20519-*), oder anders formuliert im nächsten

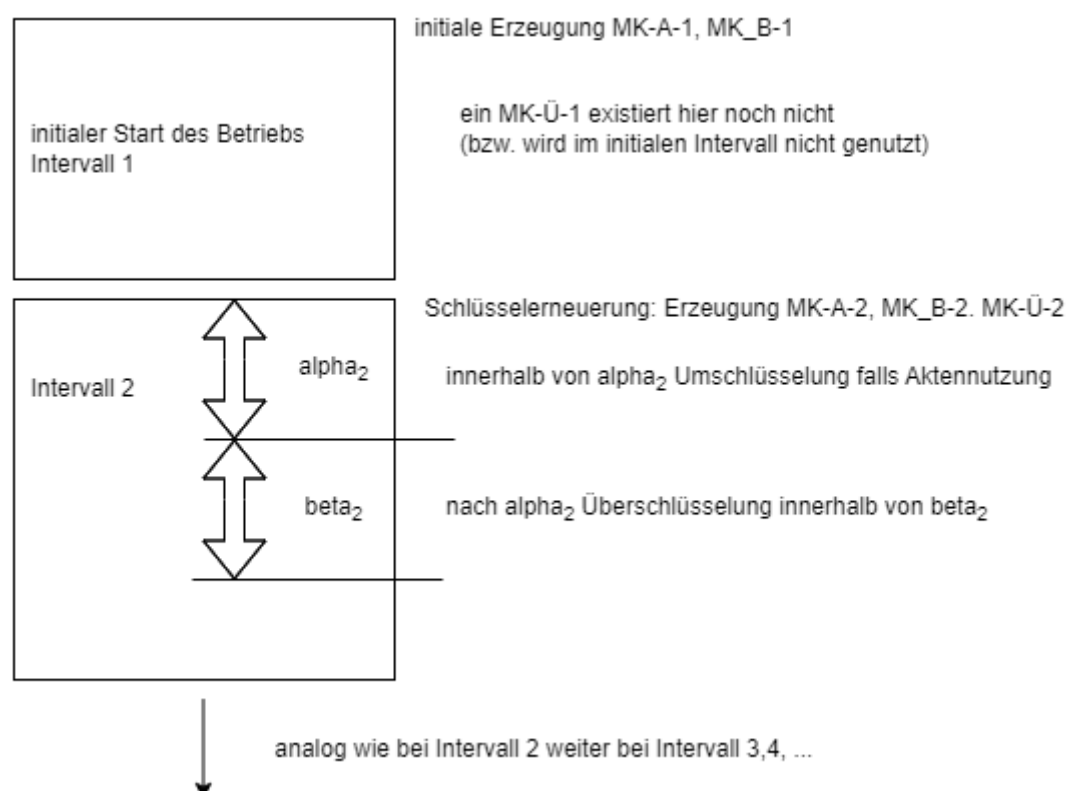
2184 Intervall, werden diese beiden ersten Schlüssel zufällig neu erzeugt. Dabei muss nun ein
2185 neuer Überschlüsselungsmasterkey erzeugt werden. Die Anzahl der Schlüssel nach o. g.
2186 Kategorie ist anschließend (1) 2, (2) 2, (3) 1.

2187 **A_26198 -ePA-Aktensystem - neuer Überschlüsselungsschlüssel bei Erneuerung**
2188 **betreiberspezifischen Schlüssel**

2189 Ein ePA-Aktensystem MUSS sicherstellen, dass bei jeder Erneuerung der Masterkeys zur
2190 Aktenpersistierung ein weiterer neuer Überschlüsselungsmasterkey zufällig im VAU-HSM
2191 erzeugt wird.

2192 [\leq]

2193 Bei einer Erneuerung der betreiberspezifischen Schlüssel gibt es verschiedene
2194 Zeitabschnitte:



2195

2196 **Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung**

2197 **A_26204 -ePA-Aktensystem - zeitliche Vorgaben zur Durchführung der**
2198 **Umschlüsselung und Überschlüsselung**

2199 Ein ePA-Aktensystem MUSS sicherstellen, dass es ein konfigurierbares Zeitintervall alpha
2200 gibt, so dass nach einer Schlüsselerneuerung der betreiberspezifischen Schlüssel
2201 innerhalb von alpha bei einer Aktennutzung eine Umschlüsselung in einer AK-VAU
2202 vorgenommen wird, falls die Verschlüsselung der Akte auf einem älteren Masterkey
2203 basiert. Das Zeitintervall alpha startet jeweils direkt mit jedem neuen Intervall
2204 (Schlüsselerneuerung der betreiberspezifischen Schlüssel).

2205 Weiter MUSS es sicherstellen, dass es ein konfigurierbares Zeitintervall beta gibt
2206 beginnend direkt nach alpha, so dass nach ablaufen von alpha eine Überschlüsselung von
2207 Chiffren von Akten, bei denen keine Umschlüsselung (wegen Nichtaktennutzung
2208 innerhalb von alpha) durchgeführt werden konnte, vorgenommen wird.

2209
2210 Der Default-Wert für die Länge von alpha MUSS 100 Tage und für die Länge von beta 60

2211 Tage betragen. ("Default-Wert" bedeutet, Wert wenn der AS-Betreiber dort keinen
2212 anderen Wert konfigurieren möchte.)

2213 [\leq]

2214 Die folgenden zwei Anforderung geben weitere Details zu A_26204-*.

2215 **A_26205 -ePA-Aktensystem - Umschlüsselung**

2216 Ein ePA-Aktensystem MUSS sicherstellen, dass wenn die AK-VAU eine Akte verwendet
2217 und feststellt, dass diese Akte nicht überschlüsselt ist und die versichertenindividuelle
2218 Aktenverschlüsselung auf einem älteren Masterkey (i. S. v. eben nicht aus dem aktuellen
2219 Intervall kommend) basiert, die AK-VAU eine Umschlüsselung vornimmt. Die alten
2220 Chiffre der Akten (also die Chiffre die auf Basis eines älteren Masterkeys
2221 verschlüsselt sind), MÜSSEN im Aktensystem nach erfolgreicher Umschlüsselung gelöscht
2222 werden.

2223
2224 Wenn die AK-VAU eine Akte verwendet und feststellt, dass diese überschlüsselt ist, so
2225 MUSS die AK-VAU die Überschüsselung entschlüsseln und die nun verfügbaren Chiffre
2226 der Akten auf Grundlage des aktuellen Masterkeys umschlüsseln. (Hinweis: nach
2227 Konstruktion muss die innere Aktenverschlüsselung auf einem älteren Masterkey
2228 basieren, ansonsten hätte keine Überschüsselung stattgefunden.) Nach erfolgreicher
2229 Umschlüsselung MÜSSEN die alten Chiffre (das Überschüsselungschiffre und das alte
2230 "innere" Chiffre der Akte) im Aktensystem gelöscht werden. [\leq]

2231 Hinweis zu A_26205-*: Die notwendigen aktenspezifischen Schlüssel liegen nun in der
2232 AK-VAU vor. Die Umschlüsselung muss nicht direkt sofort vor Nutzung der Akte erfolgen,
2233 sondern kann auch einige Minuten später erfolgen. Die konkrete Ausgestaltung liegt beim
2234 Hersteller.

2235 **A_26206 -ePA-Aktensystem - Überschüsselung**

2236 Ein ePA-Aktensystem MUSS sicherstellen, dass jeweils im aktuellen Intervall nach Ablauf
2237 des Zeitintervalls alpha Akten, die nicht überschlüsselt sind und deren Verschlüsselung
2238 auf einem älteren Masterkey (i. S. v. nicht aus dem aktuellen Zeitintervall) basiert,
2239 überschlüsselt werden auf Basis des aktuellen Überschüsselungs-Masterkeys. Diese
2240 Umschlüsselung MUSS jeweils innerhalb des Zeitintervalls beta für alle solche Akten
2241 abgeschlossen werden. Die "alten" Chiffre (Chiffre von solchen Akten vor der
2242 Überschüsselung) MÜSSEN im Aktensystem gelöscht werden. [\leq]

2243 Umschlüsselung einer Überschüsselung: Bei einer Akten, die länger nicht verwendet
2244 wird, kann es dazu kommen, dass überschlüsselte Akten wieder überschlüsselt werden
2245 müssen, weil alpha im nächsten Intervall abgelaufen ist. In diesem Fall wird eine
2246 Umschlüsselung mittels der Überschüssel vorgenommen, d. h. die Verschlüsselungstiefe
2247 / -kette wird 2 nicht überschreiten -- es gibt maximal eine Überschüsselungsschicht.

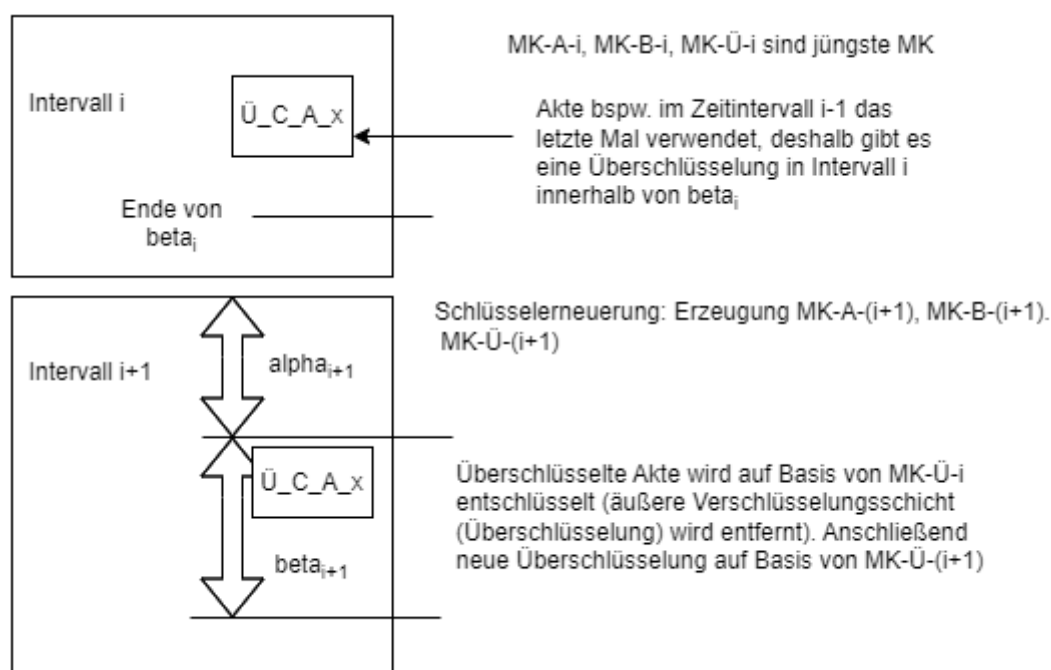


Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer Überschlüsselung

A_26208 -ePA Aktensystem - Umschlüsselung einer Überschlüsselung

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

[<=]

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

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

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

[<=]

2278 Nach A_20519-* muss es mindestens jährlich eine Schlüsselerneuerung geben. Mit
2279 26199-* kann ein ePA-Betreiber im Notfall sozusagen den Zyklus "beschleunigen" -- ein
2280 neues Intervall sofort einleiten/erzeugen.

2281 Da die Chiffre in einem ePA-Aktensystem mit Verschlüsselungsschlüsseln, die aus
2282 unterschiedlichen Masterkeys (aus unterschiedlichen Intervallen) abgeleitet werden,
2283 erzeugt werden können, muss an den äußeren Meta-Daten eines Chiffrats ersichtlich sein
2284 auf welchem Masterkeys sie basieren (vom welchem Masterkey sind sie abgeleitet sind).

2285 **A_26223 -ePA-Aktensystem - Metadaten von ePA-spezifischen Chiffraten**

2286 Ein ePA-Aktensystem MUSS sicherstellen, dass bei ePA-spezifischen Daten
2287 (Datenpersistierung von Akten, überschlüsselte Aktenchiffre, verschlüsselte Befugnisse
2288 etc.) an den äußeren (also unverschlüsselten) Meta-Daten des Chiffrats erkennbar ist
2289 mithilfe welches (oder welcher) Masterkeys die Chiffre entschlüsselbar sind. [=]

2290 **3.7 User Session und Health Record Context**

2291 Die Verarbeitungen innerhalb einer VAU werden über User Sessions und Health Record
2292 Contexts voneinander getrennt.

2293 Wenn ein ePA-Client einen VAU-Kanal zum Aktensystem aufbaut, wird dieser einer
2294 bestimmten VAU-Instanz zugeordnet, in welcher dann eine User Session für den Nutzer
2295 des ePA-Clients erzeugt wird. Nach erfolgreicher Authentifizierung des Nutzers unter
2296 Verwendung des sektoralen IDPs (Versicherte) oder des IDP-Dienstes (LEI) ist die User
2297 Session etabliert und kann durch den ePA-Client genutzt werden. Alle Verbindungen für
2298 diesen VAU-Kanal werden immer an dieselbe VAU-Instanz geleitet, die die User Session
2299 verwaltet. Eine VAU-Instanz kann mehrere User Sessions verwalten.

2300 Wird durch den ePA-Client eine Operation für eine bestimmte Akte aufgerufen (Parameter
2301 x-insurantid) der Operation, wird in der User Session geprüft, ob diese Akte schon
2302 verwendet wird (ein anderer Nutzer gerade mit der Akte arbeitet) oder nicht. Sollte die
2303 Akte noch nicht verwendet werden, wird die Akte in einem Health Record Context
2304 geöffnet und kann durch den ePA-Client in dessen User Session verwendet werden.
2305 Existiert für die Akte schon ein geöffneter Health Record Context, darf es durch den
2306 parallelen Zugriff zu keinen Inkonsistenzen in der Akte kommen.

2307 Innerhalb einer VAU-Instanz dürfen nur eine maximale Anzahl von Health Record
2308 Contexts gleichzeitig aufgebaut sein. Sollte diese Anzahl überschritten werden, wird der
2309 am längsten nicht genutzte Health Record Context geschlossen, um einen neuen Health
2310 Record Context öffnen zu können.

2311 **3.8 Consent Decision Management**

2312 Das Consent Decision Management des Aktensystems verwaltet die Entscheidungen eines
2313 Versicherten oder eines Vertreters für oder gegen die Nutzung von definiert
2314 widerspruchsfähigen Funktionen gemäß gesetzlicher Vorgaben.

2315 Außerdem werden im Consent Decision Management die Einschränkungen der
2316 Verwendung von Daten auf bestimmte Sekundärnutzungszwecke durch das
2317 Forschungsdatenzentrum Gesundheit verwaltet (siehe 3.8.2- Einschränkung der
2318 Verwendung von Daten auf bestimmte Sekundärnutzungszwecke).

2319 Der Widerspruch gegen die grundsätzliche Nutzung der ePA wird nicht im Consent
2320 Decision Management berücksichtigt. Die Existenz eines Aktenkontos für einen

2321 Versicherten impliziert, dass kein Widerspruch gegen die Nutzung der ePA erteilt wurde.
2322 Der Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger
2323 wird ebenfalls nicht hier verwaltet (siehe zu beiden Widersprüchen auch 3.1.1-
2324 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte).

2325 3.8.1 Widersprüche für Funktionen der ePA

2326 Die vorgehaltenen Entscheidungen zu einer Funktion umfassen dabei den Zustand "kein
2327 Widerspruch erklärt" ("permit") oder "Widerspruch erklärt" ("deny") und den Kontext
2328 einer Funktion. Der Kontext ordnet dabei die einzelnen widerspruchsfähigen Funktionen
2329 einem für die Umsetzung des Widerspruchs betroffenen Nutzerkreis zu und wird bei den
2330 zugreifenden Schnittstellen zur Filterung der Ausgabe verwendet.

2331 Initial, also bei der Erstellung eines neuen Aktenkontos oder bei Übernahme eines
2332 existierenden ePA 2.x Aktenkontos, ist für keine widerspruchsfähige Funktion ein
2333 Widerspruch gegen die Nutzung erklärt. Ein Versicherter oder ein Vertreter kann im
2334 Verlauf der Nutzung des Aktenkontos aktiv der Verwendung von widerspruchsfähigen
2335 Funktionen widersprechen oder einen erteilten Widerspruch zurücknehmen.

2336 Die aktuell erteilten Widersprüche können durch einen Versicherten oder einen Vertreter
2337 jederzeit über ein ePA-FdV eingesehen und geändert werden. Versicherte und Vertreter,
2338 die ein ePA-FdV nicht nutzen möchten, können eine Auskunft über die aktuell erteilten
2339 Widersprüche über die Ombudsstelle erhalten und dort auch Änderungen an den
2340 Entscheidungen im Aktenkonto veranlassen. Die Ansicht oder Änderung der
2341 Widersprüche erfolgt im Aktenkonto stets gesichert innerhalb der VAU, die aktuellen
2342 Entscheidungen zu den widerspruchsfähigen Funktionen der ePA sind
2343 versichertenindividuell mit dem SecureDataStorageKey verschlüsselt abgelegt.

2344 Die Information über relevante erteilte oder nicht erteilte Widersprüche können Clients
2345 auf einfache Weise (ohne Authentisierung oder Etablierung eines VAU-Kanals) im Vorfeld
2346 einer Operation über den Information Service abfragen (siehe auch 3.15- Information
2347 Service).

2348 Das Consent Decision Management des Aktenkontos spiegelt ("cached") die
2349 Entscheidungen zu den Widersprüchen für die schnelle Abfrage über den Information
2350 Service in einen Bereich, der ohne den Aufbau eines VAU-Kanals und Verwendung des
2351 versichertenindividuellen SecureDataStorageKey nutzbar ist.

2352 Das Aktenkonto unterstützt die Durchsetzung eines erteilten Widerspruchs überall dort,
2353 wo Aktivitäten dediziert als Teil einer widerspruchsfähigen Funktion zugeordnet werden
2354 können. Beispielsweise wird das Einstellen neuer Verordnungs- und Dispensierdaten in
2355 die Ordner der Kategorie "medication" immer verhindert, wenn der Teilnahme am digital
2356 gestützten Medikationsprozess widersprochen wurde. Die konkreten Auswirkungen eines
2357 Widerspruchs sind in den jeweiligen Kapiteln zur Handhabung von Dokumenten und
2358 Daten des Aktenkontos dargestellt (siehe 3.13.1- XDS Document Service und 3.13.2-
2359 FHIR Data Services) .

2360 Die jeweils berücksichtigten widerspruchsfähigen Funktionen sind wie folgt definiert.
2361 Diese Liste kann in folgenden Versionen der ePA ergänzt oder verändert werden.

2362 A_23874-01 -Consent Decision Management - Definition der 2363 widerspruchsfähigen Funktionen der ePA

2364 Das Consent Decision Management MUSS die Attribute zu widerspruchsfähigen
2365 Funktionen der ePA gemäß der folgenden Tabelle verwenden.

2366 **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"

2367 **[<=]**

2368 *Hinweis: Die Bezeichnungen in () sind die Bezeichnungen in den Schnittstellen für den*
 2369 *Abruf und die Verwaltung der Widersprüche. Eine widerspruchsfähige Funktion wird durch*
 2370 *die ID der Funktion eindeutig identifiziert.*

2371 *Hinweis: Die Verwaltung der Widersprüche gegen die Nutzung des Aktenkontos durch*
 2372 *eine spezifische Leistungserbringerinstitution erfolgt über die Befugnisverwaltung (siehe*
 2373 *3.9.4- Befugnisausschluss (Blocked User Policy)).*

2374 Die Entscheidungen zu den widerspruchsfähigen Funktionen "medication" und "erp-
 2375 submission" sind durch das Aktensystem dabei abhängig assoziiert:

2376 **A_25300 -Consent Decision Management - Untereinander abhängige**
 2377 **Entscheidungen zu Widersprüchen**

2378 Das Consent Decision Management MUSS durch interne Maßnahmen sicherstellen, dass
 2379 bei Erteilung eines Widerspruchs gegen die Nutzung der Funktion der elektronischen
 2380 Patientenakte 'erp-submission' ('deny') auch der Widerspruch gegen die Nutzung der
 2381 Funktion 'medication' gesetzt wird ('deny') und dass bei der Rücknahme ('permit') des
 2382 Widerspruchs gegen die Nutzung der Funktion 'medication' auch der Widerspruch gegen
 2383 die Nutzung der Funktion 'erp-submission' zurückgenommen wird. **[<=]**

2384 *Hinweis zu A_25300*: Die Änderung der Entscheidung zur Nutzung der "führenden"*
 2385 *Funktion hat automatisch eine Entscheidung zur Nutzung der "abhängigen" Funktion zur*
 2386 *Folge. Dieses gilt nur für die aufgeführten Entscheidungsänderungen. Alle weiteren, nicht*
 2387 *aufgeführten, Änderungen zu Entscheidungen haben keine "abhängige" Auswirkung auf*
 2388 *weitere Entscheidungen zu Funktionen. Beispiel: Wird die Entscheidung für 'medication'*
 2389 *von 'permit' auf 'deny' gesetzt, so hat dieses keine weiteren Änderungen an*
 2390 *Entscheidungen zur Folge.*

2391 **A_23766 -Consent Decision Management - Initialisierung der**
 2392 **Widerspruchsinformation zur Nutzung von Funktionen der ePA**

2393 Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen
 2394 bezüglich der Nutzung von Funktionen der elektronischen Patientenakte bei Erstellung
 2395 eines neuen Aktenkontos oder bei Übernahme eines existierenden Aktenkontos einer
 2396 älteren ePA-Version für alle Funktionen, gegen die der Versicherte nicht widersprochen
 2397 hat mit der Entscheidung "kein Widerspruch erklärt" ("permit") initialisieren sowie alle

2398 Funktionen, gegen die der Versicherte widersprochen hat, mit "deny" initialisieren.
2399 [\leq]

2400 **A_28043 -Consent Decision Management - Initialisierung der**
2401 **Widerspruchsinformation zur Sekundärdatennutzung (PKV)**
2402 Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen
2403 bezüglich der Sekundärdatennutzung bei Erstellung eines neuen Aktenkontos mit "deny"
2404 initialisieren, wenn die Akte durch einen Kostenträger verantwortet wird, der rechtlich
2405 keine Sekundärdatennutzung anbieten darf. [\leq]

2406 **A_24343 -Consent Decision Management - Speichern der Inhalte**
2407 Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen
2408 bezüglich der Nutzung von Funktionen der elektronischen Patientenakte unter
2409 Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen. [\leq]

2410 **A_23712 -Consent Decision Management - Übertrag der**
2411 **Widerspruchsinformation zur Nutzung von Funktionen der ePA für den**
2412 **Informationsdienst**

2413 Das Consent Decision Management MUSS die aktuellen Entscheidungen
2414 zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen
2415 Patientenakte der Funktionsklassen

2416

- Versorgungsprozess ("healthCareProcess")

2417 sofort im Anschluss an eine Änderung der Entscheidung im Consent Decision
2418 Management für die Abfrage durch den Information Service des Aktensystems ohne
2419 Nutzung der VAU und des SecureAdminStorageKeys verfügbar machen.
2420 [\leq]

2421 **A_24040 -Consent Decision Management - Periodischer Übertrag der**
2422 **Widerspruchsinformation zur Nutzung von Funktionen der ePA für den**
2423 **Informationsdienst**

2424 Das Consent Decision Management MUSS die aktuellen Entscheidungen
2425 zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen
2426 Patientenakte der Funktionsklassen

2427

- Versorgungsprozess ("healthCareProcess")

2428 bei jedem Start der VAU (des VAU-Kanals) für die Abfrage durch den Information Service
2429 des Aktensystems ohne Nutzung der VAU und des SecureAdminStorageKeys verfügbar
2430 machen, unabhängig von einer Änderung der Entscheidungen zu den
2431 Widersprüchen. [\leq]

2432 Clients der Ombudsstelle und aus der Umgebung des Versicherten nutzen das Consent
2433 Decision Management über die Operationen der Schnittstelle
2434 `I_Consent_Decision_Management`. Clients aus der Umgebung der LEI und der E-Rezept-
2435 Fachdienst nutzen für die schnelle Abfrage die Operation der
2436 Schnittstelle `I_Information_Service`.

2437 **A_23824 -Aktensystem - Realisierung der Schnittstelle**

2438 **I_Consent_Decision_Management**

2439 Das ePA-Aktensystem MUSS die Operationen der Schnittstelle
2440 `I_Consent_Decision_Management` gemäß `[I_Consent_Decision_Management]`
2441 umsetzen. [\leq]

2442 **A_23919 -Consent Decision Management - unveränderte Übernahme der**
2443 **Widerspruchsentscheidung**

2444 Das Consent Decision Management MUSS die über Operationen der Schnittstellen des
2445 Consent Managements übermittelten Entscheidungen (consent decisions) zu
2446 widerspruchsfähigen Funktionen der ePA in das Aktenkonto übernehmen. Die

2447 Entscheidungen zu den in den Operationen nicht adressierten widerspruchsfähigen
2448 Funktionen MÜSSEN im Aktenkonto unverändert bleiben. [<=]

2449 **A_24844 -Consent Decision Management - Information über Änderungen der**
2450 **Widerspruchsinformation**

2451 Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung
2452 einer Widerspruchsinformation, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail
2453 darüber informieren, dass Widerspruchsinformationen geändert wurden, wann die
2454 Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im
2455 Protokoll zu finden sind. [<=]

2456 **A_24055 -Consent Decision Management – Protokollierung geänderter**
2457 **Entscheidungen zu Widersprüchen**

2458 Das Consent Decision Management MUSS Bei Änderungen von Entscheidungen zu den
2459 widerspruchsfähigen Funktionen der ePA jeweils einen Protokolleintrag gemäß A_24704*
2460 erzeugen. Für die Wertebelegung ist A_23874* zu berücksichtigen und die
2461 Protokollstruktur entsprechend zu belegen:

2462 **Tabelle 9: Consent Decision Management Protokollierung - Widersprüche für Funktionen**
2463 **der ePA**

Strukturelement	Wert		Erläuterung
AuditEvent.action	U		Update
AuditEvent.entity.name	"ConsentDecision"		Eintrag protokolliert eine Widerspruchentscheidung
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"

2464 [<=]

2465 *Hinweis: Die initiale Entscheidung zu den Widersprüchen bei Anlage eines Aktenkontos*
2466 *wird nicht protokolliert. Die spezifische Protokollierung erfolgt für Folgeänderungen.*

2467 Ein Aufruf der Operationen der Schnittstelle I_ConsentDecisionManagement zur Änderung
2468 der Entscheidungen zur den Widersprüchen gegen die Nutzung von widerspruchsfähigen
2469 Funktionen der ePA kann erfolgreich beendet werden, ohne dass eine bisher gespeicherte
2470 Entscheidung zu diesen Widersprüchen im Aktensystem geändert wird. In diesem Fall
2471 erfolgt die Protokollierung gemäß A_27883-.*.

2472 **A_27883 -Consent Decision Management – Protokollierung unveränderter**
2473 **Entscheidungen zu den widerspruchsfähigen Funktionen der ePA**

2474 **Das Consent Decision Management MUSS für jede versuchte Änderung der**
2475 **Entscheidungen zu den Widersprüchen gegen die Sekundärnutzung von Daten,**

welche nicht durch einen Fehler abgelehnt wird und welche zu keiner Änderung einer gespeicherten Entscheidung führt ('leere' Änderung, keine Änderung der Einstellungen zu DataUsagePurposes), einen Protokolleintrag gemäß A_24704* erzeugen:

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

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

[<=]

3.8.2 Einschränkung der Verwendung von Daten auf bestimmte Sekundärnutzungszwecke

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

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

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

A_26286 -Consent Decision Management - Initialisierung der Sekundärnutzungszwecke

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

A_28044 -Consent Decision Management - Initialisierung der Sekundärnutzungszwecke (PKV)

Das Consent Decision Management MUSS jeden in § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszweck der elektronischen Patientenakte bei Erstellung eines neuen Aktenkontos mit "deny" initialisieren, wenn die Akte durch einen Kostenträger verantwortet wird, der rechtlich keine Sekundärdatennutzung anbieten darf. [<=]

A_26287 -Consent Decision Management - Speichern der Entscheidungen zu Sekundärnutzungszwecken

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

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

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

A_26291 -Consent Decision Management - unveränderte Übernahme der Widerspruchsentscheidung zu Sekundärnutzungszwecken

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

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

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

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

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

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

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

~~A_26308-01~~A_26308 -Consent Decision Management – Protokollierung geänderter Entscheidungen zu Sekundärnutzungszwecken

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

Tabelle 11: Consent Decision Management Protokollierung - Widersprüche zu Sekundärnutzungszwecken

Strukturelement	Wert	Erläuterung
AuditEvent.action	U	Update

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

2550 [**<=**]

2551 Ein Aufruf der Operationen der Schnittstelle I_ConsentDecisionManagement zur Änderung
 2552 der Entscheidungen zur den Widersprüchen gegen die Verwendung von Daten für
 2553 Sekundärnutzungszwecke kann erfolgreich beendet werden, ohne dass eine bisher
 2554 gespeicherte Entscheidung zu diesen Widersprüchen im Aktensystem geändert wird. In
 2555 diesem Fall erfolgt die Protokollierung gemäß A_27869-*

2556 **A_27869 -Consent Decision Management – Protokollierung unveränderter** 2557 **Entscheidungen zu Sekundärnutzungszwecken**

2558 Das Consent Decision Management MUSS für jede versuchte Änderung der
 2559 Entscheidungen zu den Widersprüchen gegen die Sekundärnutzung von Daten, welche
 2560 nicht durch einen Fehler abgelehnt wird und welche zu keiner Änderung einer
 2561 gespeicherten Entscheidung führt ('leere' Änderung, keine Änderung der Einstellungen
 2562 zu DataUsagePurposes), einen Protokolleintrag gemäß A_24704* erzeugen:

2563 **Tabelle 12: Consent Decision Management Protokollierung - unveränderte Widersprüche**
 2564 **zu Sekundärnutzungszwecken**

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

2565 [**<=**]

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 berechnete Nutzergruppen und Nutzer

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

Nutzergruppe [professionOID] der User Specific Deny Policy Medication

oid_praxis_arzt

Nutzergruppe [professionOID] der User Specific Deny Policy Medication
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

2609
2610
2611

[<=]

2612
2613
2614
2615
2616
2617

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

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

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

Strukturelement	Wert	Erläuterung
AuditEvent.action	C, D	Update
AuditEvent.entity.name	"UdpMedication"	Eintrag protokolliert eine Änderung der User Specific Deny Policy für Medication Service

Strukturelement	Wert		Erläuterung
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

2618 [**<=**]2619 **3.9 Entitlement Management**

2620 Befugnisse (Entitlements) werden individuell für jeden Nutzer des Aktenkontos erstellt
 2621 (Versicherter, Vertreter, Leistungserbringerinstitutionen, Kostenträger, Ombudsstelle und
 2622 Fachdienste). Eine erteilte Befugnis ist notwendige Voraussetzung für die Nutzung des
 2623 Aktenkontos und zum internen Bezug des Datenpersistierungsschlüssels
 2624 (SecureDataStorageKey) für den Zugriff auf die Dokumenten- und Datenverwaltung.

2625 Eine Befugnis enthält folgende Informationen:

2626 **A_23734-01 -Entitlement Management - Definition einer Befugnis**

2627 Das Entitlement Management MUSS für eine individuelle Befugnis die folgenden Daten
 2628 nutzen und verwalten:

2629 **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 (displayName)	Name der Institution, des Nutzers		nein
Rolle des Nutzers (oid)	OID der Nutzerrolle (professionOID)		nein

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

2630 **[<=]**

2631 *Hinweis: Ein Nutzer ist der Adressat, für den die Befugnis ausgestellt wird. Der Ersteller*
 2632 *ist der Nutzer, welcher die Befugnisausstellung veranlasst hat. Die Bezeichner in () sind*
 2633 *die Bezeichner in den Schnittstellenbeschreibungen.*

2634 *Hinweis (*): A_23734 definiert eine "vollständige" Befugnis, welche auch Daten enthält,*
 2635 *die für eine Prüfung einer gültigen Befugnis im Kontext einer Schnittstellenoperation*
 2636 *nicht notwendig sind. Für diesen Zweck wird nur der (HSM-) signierte Anteil als Ergebnis*
 2637 *einer Befugnisverifikation verwendet (signiertes Element = ja). Eine gespeicherte*
 2638 *Befugnis enthält jedoch alle Elemente für eine qualifizierte Verwaltung der Befugnisse*
 2639 *durch einen Versicherten oder Vertreter.*

2640 *Hinweis:* Befugnisse können durch das Aktensystem selbst (initiale Befugnisse), durch
 2641 den Versicherten oder einen befugten Vertreter unter Verwendung eines ePA-FdV oder
 2642 durch eine Leistungserbringerinstitution in einer Behandlungssituation erstellt werden.

2643 Eine Befugnis kann nur für Nutzer und Nutzergruppen mit bestimmter Rolle erteilt
 2644 werden. Nutzergruppen mit abweichenden Rollen können nicht befugt werden und
 2645 erhalten keinen Zugriff auf das Aktenkonto.

2646 Erfolgt die Befugniserteilung durch eine Leistungserbringerinstitution in einer
 2647 Behandlungssituation, wird eine vorgegebene Gültigkeitsdauer der Rolle des Befugten
 2648 entsprechend durch das Entitlement Management vergeben. Ein Versicherter oder ein
 2649 befugter Vertreter kann den Gültigkeitszeitraum frei wählen (ausgenommen
 2650 Vertreterbefugnisse).

2651 **A_23941-01 -Entitlement Management - Erteilung von Befugnissen für** 2652 **berechtigte Nutzergruppen und Nutzer**

2653 Das Entitlement Management MUSS die Erteilung von Befugnissen in der jeweiligen
 2654 Umgebung auf die folgenden Nutzergruppen und Nutzer einschränken:

2655 **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

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-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

2656

2657

Hinweis:

2658

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

2659

2660

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

2661

2662

2663

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

2664

FdV = Versicherter oder Vertreter,

2665

- 2666 KTR = Kostenträger
 2667 AS = Aktensystem (systemseitig erteilte Befugnisse)
 2668 Tage = Gültigkeit in Tagen: angegebener Wert ist einschließlich aktuellem Datum, z. B.
 2669 90 Tage bedeutet aktuelles Datum + 89 Tage.
 2670 dauerhaft = Befugnis unbegrenzt gültig (Enddatum = 9999-12-31)
 2671 statisch = Gültigkeit analog 'dauerhaft', Befugnis ist implizit vorhanden.
 2672 var = Gültigkeitsdauer von 1 Tag bis dauerhaft in jeweils ganzen Tagen[<=]
 2673 Befugnisse werden durch das Entitlement Management mit dem SecureAdminStorageKey
 2674 verschlüsselt und im Aktenkonto gesichert abgelegt.
 2675 Einzelne Nutzer können durch den Versicherten, einen befugten Vertreter oder die
 2676 Ombudsstelle explizit von der Befugnisvergabe ausgeschlossen sein (siehe 3.9.4-
 2677 Befugnisausschluss (Blocked User Policy)). Eine Befugniserstellung ist dann weder für
 2678 Leistungserbringerinstitutionen in einer Behandlungssituation, noch durch den
 2679 Versicherten oder einen Vertreter möglich.
 2680 Die Befugnisse für den Versicherten und den E-Rezept-Fachdienst werden dabei nicht
 2681 persistiert. Diese Befugnisse werden als implizit vorhanden und gültig angenommen.
 2682 Eine Besonderheit stellt hierbei eine Befugnis EU-Zugriff dar. Es gibt zu einem
 2683 Zeitpunkt für ein Aktenkonto maximal eine Befugnis EU-Zugriff. Die Dauer dieser
 2684 Befugnis wird durch das Aktensystem festgelegt und beträgt 1 Stunde. Das Ende der
 2685 Gültigkeit (validTo) wird ermittelt vom Ausstellungszeitpunkt + 1 Stunde.
 2686 **A_26167 -Entitlement Management (EU) - Erteilung der Befugnis EU-Zugriff**
 2687 Das Entitlement Management MUSS die Erteilung einer Befugnis EU-Zugriff in der
 2688 jeweiligen Umgebung zusätzlich zu A_23941-* auf die folgenden Nutzergruppen und
 2689 Nutzer einschränken:
 2690 **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

- 2691 Hinweis:
 2692 'x' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung befugt
 2693 werden
 2694 '-' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung nicht
 2695 befugt werden
 2696
 2697 LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-
 2698 Prüfungsnachweis (Prüfziffer),
 2699 FdV = Versicherter oder Vertreter,
 2700 AS = Aktensystem (systemseitig erteilte Befugnisse)[<=]

- 2701 **A_24371 -Entitlement Management - Verschlüsselung der Befugnisse**
2702 Das Entitlement Management MUSS Befugnisse mit dem versichertenindividuellen
2703 SecureAdminStorageKey verschlüsseln und im Aktenkonto persistieren.[<=]
- 2704 **A_24372 -Entitlement Management - Keine persistente Ablage**
2705 **unverschlüsselter Befugnisse**
2706 Das Entitlement Management MUSS sicherstellen, dass Befugnisse ausschließlich
2707 verschlüsselt unter Verwendung des versichertenindividuellen SecureAdminStorageKey
2708 im Aktenkonto gespeichert werden.[<=]
- 2709 **A_24687 -Entitlement Management - Keine Speicherung oder Verwendung nicht**
2710 **verifizierter Befugnisse**
2711 Das Entitlement Management MUSS sicherstellen, dass ausschließlich Befugnisse
2712 persistiert oder für eine Befugnisprüfung verwendet werden, die erfolgreich durch das
2713 HSM unter Verwendung der adäquaten Regeln 'rr1 - rr4' gemäß A_24573*
2714 befugnisverifiziert sind.[<=]
- 2715 **A_23842 -Entitlement Management - Eindeutigkeit der Befugnisse im**
2716 **Befugnikontext**
2717 Das Entitlement Management MUSS sicherstellen, dass im Befugnikontext keine zwei
2718 oder mehr Befugnisse existieren, die als Identifier des befugten Nutzers die gleiche
2719 Identifikation (`actorId`) aufweisen.[<=]
- 2720 **A_24785 -Entitlement Management - VSDM-Prüfungsnachweis kann höchstens**
2721 **einmal genutzt werden**
2722 Das Entitlement Management MUSS sicherstellen, dass ein VSDM-Prüfungsnachweis
2723 (Prüfziffer) höchstens einmal zur Registrierung einer Befugnis genutzt werden kann.[<=]
- 2724 **A_27671 -Entitlement Management - PoPP-Token kann höchstens einmal**
2725 **genutzt werden**
2726 Das Entitlement Management MUSS sicherstellen, dass ein PoPP-Token höchstens einmal
2727 zur Registrierung einer Befugnis genutzt werden kann.[<=]
- 2728 **A_27681 -Entitlement Management - Konfigurationsvariable `enforce_popp_only`**
2729 Das Entitlement Management MUSS eine Konfigurationsvariable `enforce_popp_only`
2730 besitzen, die initial auf `false` gesetzt ist.[<=]
- 2731 ePA-Clients nutzen zur Befugnisvergabe die Operationen der
2732 Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`.
2733 Die initialen Befugnisse des Aktenkontos werden auf organisatorischem Weg direkt im
2734 Aktenkonto erstellt.
- 2735 **A_24506 -Entitlement Management- Realisierung der Schnittstelle**
2736 **`I_Entitlement_Management`**
2737 Das Entitlement Management MUSS die Operationen der Schnittstelle
2738 `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` umsetzen.[<=]
- 2739 **A_26168 -Entitlement Management (EU)- Realisierung der Schnittstelle**
2740 **`I_Entitlement_Management_EU`**
2741 Das Entitlement Management MUSS die Operationen der Schnittstelle
2742 `I_Entitlement_Management_EU` gemäß `[I_Entitlement_Management_EU]`
2743 umsetzen.[<=]
- 2744 **A_24987-01 -Entitlement Management - Protokolleinträge für Zugriffe auf das**
2745 **Entitlement Management**
2746 Das Entitlement Management MUSS für das Erteilen und Entziehen von Befugnissen und
2747 das Setzen und Löschen von Befugnisausschlüssen jeweils einen Protokolleintrag gemäß
2748 A_24704 erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

2749 **Tabelle 17: Entitlement Management Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		
AuditEvent.action	C, D, U		ein Code aus den genannten, je nach Operation
AuditEvent.entity.name	"UserBlocking"		Setzen und Löschen von Befugnisausschlüssen
	"EntitlementManagement"		Erteilen oder Entziehen von Befugnissen
AuditEvent.entity.detail	type	value[x]	
	"blockedUserName"	<Name der LEI>	Name der LEI, für die der Befugnisausschluss gesetzt bzw. der Ausschluss zurückgenommen wurde
	"blockedUserId"	<Telematik-ID der LEI>	Telematik-ID der LEI, für die der Befugnisausschluss gesetzt bzw. der Ausschluss zurückgenommen wurde
	"UserName"	<Name der Institution oder des Vertreters>	Name der Institution oder des Nutzers für die eine Befugnis erteilt oder gelöscht wurden
	"UserId"	<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

2750
2751 [**<=**]

2752 *Hinweis: Ein Update ("U") eines Entitlements liegt vor, wenn ein existierendes*
 2753 *Entitlement aufgrund des längeren Gültigkeitszeitraums eines neuen Entitlements*
 2754 *überschrieben wird.*

2755 3.9.1 Initiale Befugnisse (static Entitlements)

2756 Einige grundsätzlich notwendige Befugnisse sind zum Zeitpunkt der Aktivierung eines
 2757 Aktenkontos verfügbar.

2758 Zu diesen initialen Befugnissen gehören die Befugnisse für den Versicherten, den E-
 2759 Rezept-Fachdienst, den Kostenträger und die Ombudsstelle. Diese Befugnisse müssen in
 2760 der Phase der Initialisierung eines Aktenkontos durch das Aktensystem erstellt werden.

2761 Diese Befugnisse sind dauerhaft gültig und unveränderbar und können nicht gelöscht
 2762 werden.

2763 **A_24145 -Entitlement Management – Implizite initiale (statische) Befugnisse**

2764 Das Entitlement Management MUSS sicherstellen, dass der Versicherte (KVNR des
 2765 Akteninhabers, oid_versicherter), und der E-Rezept-Fachdienst (registrierte Telematik-
 2766 ID, oid_erp-vau) dauerhaft den versichertenindividuellen SecureDataStorageKey
 2767 beziehen können und Zugriff auf die Dokumenten- und Datenverwaltung erhalten. Die
 2768 Befugnisse MÜSSEN den Vorgaben der folgenden Tabelle entsprechen:
 2769

Element	Versicherter	E-Rezept-Fachdienst
Identifizier des befugten Nutzers (actorId)	KVNR des Versicherten (Aktenkontoinhaber)	Telematik-ID der E-Rezept vertrauenswürdig 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

2770 [**<=**]

2771 **A_24374 -Entitlement Management – Signierte initiale (statische) Befugnisse**

2772 Das Entitlement Management MUSS sicherstellen, dass für den Kostenträger und die
 2773 Ombudsstelle gültige Befugnisse mit unbegrenzter Gültigkeitsdauer zum Zeitpunkt der
 2774 Aktivierung des Aktenkontos gemäß der Vorgaben der folgenden Tabelle vorliegen:
 2775

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

Element	Kostenträger	Ombudsstelle
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

2776 [\leq]

2777 **A_24688-01 -Entitlement Management – Befugnisverifikation signierter initialer**
 2778 **Befugnisse**

2779 Das Entitlement Management MUSS sicherstellen, dass die initialen, signierten
 2780 Befugnisse des Kostenträgers und der Ombudsstelle spätestens beim ersten Zugriff auf
 2781 das Aktenkonto durch das HSM unter Verwendung der Regel 'rr4' gemäß A_24573*
 2782 befugnisverifiziert sind. [\leq]

2783 **A_24533 -Entitlement Management - Keine Änderung statischer Befugnisse**

2784 Das Entitlement Management MUSS sicherstellen, dass die dauerhaften Befugnisse des
 2785 Versicherten, des E-Rezept-Fachdiensts, des Kostenträgers und der Ombudsstelle nicht
 2786 verändert oder gelöscht werden können. [\leq]

2787 **A_24784 -Entitlement Management - Höchstens eine Befugnis für KTR und**
 2788 **Ombudsstelle pro Aktenkonto**

2789 Das Entitlement Management MUSS sicherstellen, dass in einem Aktenkonto höchstens
 2790 eine Befugnis für einen Kostenträger und höchstens eine Befugnis für eine Ombudsstelle
 2791 hinterlegt ist. [\leq]

2792 **A_24955 -Entitlement Management - Befugnis für KTR und Ombudsstelle nur**
 2793 **bei Anlage und betreiberinterner Anbieterwechsel**

2794 Das Entitlement Management MUSS sicherstellen, dass eine signierte Befugnis des
 2795 Kostenträgers und eine signierte Befugnis der Ombudsstelle ausschließlich bei einer
 2796 Anlage eines Aktenkontos (Initialisierung) oder bei einem betreiberinternen
 2797 Anbieterwechsel in die Befugnisse des Aktenkontos aufgenommen werden.
 2798 [\leq]

2799 **3.9.2 Erstellen einer Befugnis durch Clients**

2800 Die Anforderung zur Vergabe einer neuen Befugnis erfolgt durch die Clients der ePA. Bei
 2801 einer Befugnisvergabe aus der Umgebung der Leistungserbringer ist dieses das
 2802 Primärsystem (PS), aus der Umgebung des Versicherten ist es das ePA-FdV.

2803 Clients verwenden zur Befugnisvergabe signierte JSON Web Token (JWS). Das Token
 2804 wird zur Verifikation an das HSM übergeben. Als Ergebnis der HSM Verarbeitung liegt
 2805 eine bestätigte, CMAC gesicherte Befugnis mit den Elementen `actorId` (Identifizier des zu
 2806 befugenden Nutzers), `kvn` (AktenkontoId) und `validTo` (Gültigkeitszeitraum) für die
 2807 spätere Befugnisprüfung vor. Das HSM Ergebnis wird mit den weiteren Daten gemäß

2808 A_23734* (oid, displayName, issued-*) ergänzt und gemäß A_24371* mit dem
 2809 SecureAdminStorageKey gesichert im Aktenkonto abgelegt.

2810 3.9.2.1 Befugnisvergabe durch ein ePA-FdV

2811 Ein ePA-FdV muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

2812 A_24587-01 -Entitlement Management - Befugnis durch ein ePA-FdV

2813 Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ePA-
 2814 FdV über die Schnittstelle I_Entitlement_Management durch Verwendung eines gültig
 2815 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

2816 [<=]

2817 Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve
 2818 "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext

2819 der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur
2820 und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

2821 *Hinweis zu A_24587*: Im Falle der Befugnisvergabe für einen NCPeH (EU-Zugriff, "oid"*
2822 *== "oid_ncpeh") wird durch das Aktensystem sichergestellt, dass die vorgeschriebene*
2823 *Gültigkeitsdauer für derartige Befugnisse angewendet wird. Dieses erfolgt durch die*
2824 *Befugnisverifikation gemäß Regel "rr1" im HSM. Die Angabe eines Gültigkeitsendes im*
2825 *"validTo"-Element des JWT wird daher für diesen Fall ignoriert, das Element selbst muss*
2826 *jedoch vorhanden sein.*

2827 **A_24689 -Entitlement Management - Befugnisverifikation einer Befugnis durch** 2828 **ein ePA-FdV**

2829 Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein
2830 ePA-FdV unter Verwendung der Regeln 'rr1' (Befugnisvergabe durch den Versicherten)
2831 bzw. 'rr2' (Befugnisvergabe durch einen Vertreter) des HSM eine Befugnisverifikation
2832 durchführen.[<=]

2833 **A_24535 -Entitlement Management - Befugnisse für Vertreter**

2834 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId`
2835 = KVNR) ausschließlich durch den Versicherten erstellt oder gelöscht werden
2836 können.[<=]

2837 **A_26698 -Entitlement Management - maximale Anzahl Befugnisse für Vertreter**

2838 Das Entitlement Management MUSS sicherstellen, dass maximal fünf gültige Befugnisse
2839 für Vertreter gleichzeitig in einem Aktenkonto vorhanden sind.[<=]

2840 **A_24536 -Entitlement Management - Gültigkeitsdauer der Befugnisse für** 2841 **Vertreter**

2842 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId`
2843 = KVNR) ausschließlich mit einer unbegrenzten Gültigkeit erstellt werden.[<=]

2844 **A_24754 -Entitlement Management - E-Mail-Adresse des Vertreters**

2845 Das Entitlement Management MUSS sicherstellen, dass bei Befugnissen für Vertreter
2846 (`actorId` = KVNR) eine E-Mail-Adresse des Vertreters für dessen Benachrichtigung
2847 angegeben wird.[<=]

2848 Die in A_24754 angegebene E-Mail-Adresse wird ausschließlich zur Benachrichtigung des
2849 Vertreters über die eingestellte Befugnis verwendet (vgl. A_24755-*), jedoch nicht für
2850 die Geräteregistrierung. Um eine Vertretung wahrnehmen zu können und hierfür Geräte
2851 zu registrieren, muss der Vertreter in seinem Home-AS eine E-Mail-Adresse hinterlegt
2852 haben.

2853 **A_24755-01 -Entitlement Management - Benachrichtigung des Vertreters bei** 2854 **Befugniserstellung**

2855 Das Entitlement Management MUSS im Anschluss an die erfolgreiche, neue
2856 Befugniserstellung für einen Vertreter eine E-Mail an die E-Mail-Adresse des Vertreters
2857 senden, die diesen über die Befugniserstellung für das Aktenkonto des Versicherten
2858 geeignet informiert. In der Nachricht MUSS der Name des Versicherten enthalten sein
2859 und welche Art von personenbezogenen Daten vom Vertreter im Rahmen der
2860 Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine
2861 Vertreterberechtigung widerrufen kann und gegenüber wem er seine
2862 datenschutzrechtlichen Betroffenenrechte wahrnehmen kann.[<=]

2863 Hinweis: Unter Art der personenbezogenen Daten ist z.B. „Krankenversichertennummer,
2864 Name und E-Mail-Adresse“ gemeint, aber nicht die tatsächliche KVNR des Vertreters, der
2865 tatsächliche Name oder die tatsächliche E-Mail-Adresse.

3.9.2.2 Befugnisvergabe durch ein Primärsystem

A_27288-01 -Entitlement Management – Abgleich der KVNR bei Erstellen einer Befugnis

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

[<=]

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

A_24590-03 -Entitlement Management - Befugnis durch ein Primärsystem

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

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 <code>ReadVSD</code> gemäß A_27352-* berechnet wird. Der berechnete hcv-Wert MUSS base64 kodiert werden.

[<=]

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

Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve "brainpoolP256r1" basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext

2889 der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur
2890 und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

2891 **A_27321-01 -Entitlement Management – Abgleich hcv bei Erstellen einer**
2892 **Befugnis über VSDM-Prüfziffer in Version 2**

2893 Falls vom Primärsystem in `setEntitlementPs` eine Befugnis (signiertes JWT) mit einer
2894 Prüfziffer in Version 2 übergeben wird und das Ergebnis des Aufrufs der Regel `rr3` eine
2895 interne Datenstruktur der VSDM-Prüfziffer zurückliefert, MUSS das Entitlement
2896 Management sicherstellen, dass der Wert im Attribut "hcv" des JWT mit dem Wert von
2897 hcv aus der VSDM-Prüfziffer übereinstimmt und ansonsten die
2898 Operation `setEntitlementPs` abbrechen.[<=]

2899 **A_27289 -Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche**
2900 **der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer**

2901 Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer
2902 Stunde maximal fünfmal eine Befugnis (signiertes JWT) über `setEntitlementPs`
2903 übermitteln kann, bei der die mitgelieferte KVNR in `x-insurantId` von der KVNR
2904 abweicht, die in der Prüfziffer der übermittelten Befugnis (signiertes JWT) enthalten ist,
2905 andernfalls für den Nutzer für diesen Zeitraum die Operation `setEntitlementPs`
2906 abbrechen.[<=]

2907 **A_27322 -Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche**
2908 **der VSD-Update-Zeit bei Erstellen einer Befugnis über VSDM-Prüfziffer in**
2909 **Version 2**

2910 Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer
2911 Stunde maximal fünfmal eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2
2912 über `setEntitlementPs` übermitteln kann, bei der die Operation `setEntitlementPs`
2913 gemäß A_27321-* abbricht.[<=]

2914

2915 **A_27679 -Entitlement Management - Telematik-ID im PoPP-Token ist gleich der**
2916 **Telematik-ID des angemeldeten Nutzers**

2917 Das Entitlement Management MUSS bei der Befugnisvergabe durch ein Primärsystem
2918 unter Verwendung eines PoPP-Tokens sicherstellen, dass die Telematik-ID in PoPP-
2919 Token.actorID gleich der Telematik-ID des Nutzers der User Session ist.[<=]

2920 **A_24537 -Entitlement Management - Standardgültigkeitsdauer für Befugnisse**

2921 Das Entitlement Management MUSS sicherstellen, dass neue Befugnisse, die unter
2922 Verwendung der Schnittstelle `I_Entitlement_Management` gemäß
2923 `[I_Entitlement_Management]` erstellt werden, eine vorgegebene, rollenspezifische
2924 Befugnisdauer gemäß A_23941-* erhalten.[<=]

2925 **3.9.3 Löschen von Befugnissen**

2926 Erteilte Befugnisse werden grundsätzlich nach Erreichen des Endzeitpunkts ihrer
2927 Gültigkeit durch das Aktensystem gelöscht.

2928 **A_24504 -Entitlement Management - Löschen ungültiger Befugnisse**

2929 Das Entitlement Management MUSS vorhandene Befugnisse, deren Enddatum der
2930 Gültigkeit überschritten ist, unverzüglich aus dem Befugnis Kontext des Aktenkontos
2931 vollständig löschen.[<=]

2932 Das explizite Löschen von Befugnissen innerhalb ihres Gültigkeitszeitraums kann
2933 ausschließlich durch den Versicherten oder einen Vertreter mittels eines ePA-FdV
2934 erfolgen. Es können alle erteilten Befugnisse gelöscht werden, ausgenommen die initialen
2935 Befugnisse gemäß 3.9.1- Initiale Befugnisse (static Entitlements) .

2936 Für das Löschen von Befugnissen durch einen Vertreter gilt darüber hinaus folgende
2937 Einschränkung:

2938 **A_25246 -Entitlement Management - Löschen von Befugnissen durch einen**
2939 **Vertreter**

2940 Das Entitlement Management MUSS sicherstellen, dass eine erteilte Befugnis für einen
2941 Vertreter (`actorId` der Befugnis == KVNR) durch einen Vertreter nur dann gelöscht
2942 werden kann, wenn die KVNR des löschenden Vertreters der KVNR der `actorId` zu
2943 löschenden Befugnis entspricht. [`<=`]

2944 *Hinweis: Ein Vertreter darf nur seine eigene Befugnis löschen, nicht aber die Befugnis*
2945 *weiterer Vertreter.*

2946 **A_25269 -Entitlement Management - Benachrichtigung des Versicherten bei**
2947 **Löschen einer Vertreterbefugnis durch Vertreter**

2948 Falls ein Vertreter seine eigene Vertreterbefugnis löscht MUSS das Entitlement
2949 Management für den Fall, dass für den Versicherten mindestens eine E-Mail-Adresse
2950 hinterlegt ist, den Versicherten über das Löschen der Vertreterbefugnis an alle seine
2951 hinterlegten E-Mail-Adressen informieren. [`<=`]

2952 **3.9.4 Befugnisausschluss (Blocked User Policy)**

2953 Das Entitlement Management erlaubt die Verwaltung von Widersprüchen des
2954 Versicherten oder eines Vertreters gegen die Nutzung des Aktenkontos durch spezifische
2955 Leistungserbringerinstitutionen.

2956 Ist ein Widerspruch gegen einen bestimmten Nutzer hinterlegt, so kann für diesen keine
2957 Befugnis erstellt werden, bis dieser Widerspruch zurückgenommen wird.

2958 Die Umsetzung dieser Widerspruchsverwaltung bzw. des Befugnisausschlusses erfolgt
2959 durch eine Policy (Blocked User Policy). Die Konfiguration dieser Policy obliegt dem
2960 Versicherten oder einem befugten Vertreter mittels ePA-FdV oder der Ombudsstelle.
2961 Einträge können der Policy hinzugefügt oder entfernt werden. Zum Zeitpunkt der
2962 Erstellung des Aktenkontos enthält die Blocked User Policy keine Einträge.

2963 Ein Eintrag in der Policy referenziert einen bestimmten Nutzer über seinen Identifier
2964 (Telematik-Id). Die Menge der Einträge ist nicht limitiert.

2965 Jeder Eintrag der Blocked User Policy verhindert grundsätzlich die Erstellung einer
2966 Befugnis für den referenzierten Nutzer. Erfolgt der Widerspruch (Anlegen eines neuen
2967 Eintrags) bei bestehender Befugnis für den auszuschließenden Nutzer, wird die
2968 bestehende Befugnis gelöscht.

2969 Bei Rücknahme eines Widerspruchs gegen die Nutzung des Aktenkontos für eine
2970 bestimmte Leistungserbringerinstitution wird der entsprechende Eintrag der Policy
2971 gelöscht. Anschließend kann dieser Nutzer befugt werden.

2972 Ein Widerspruch gegen die Nutzung des Aktenkontos kann nur für Nutzer der folgenden
2973 Nutzergruppen erfolgen.

2974 **A_24463-01 -Entitlement Management - zulässige Rollen für den Widerspruch**
2975 **gegen die Nutzung durch eine Leistungserbringerinstitution**

2976 Das Entitlement Management MUSS den Widerspruch gegen die Nutzung durch eine
2977 Leistungserbringerinstitution ausschließlich für Nutzer der folgenden Nutzergruppen

2978 zulassen:
2979

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

2980 **[<=]**

2981 Ein Eintrag der Blocked User Policy enthält Angaben gemäß der folgenden Tabelle:
2982 (Beispiel)

2983 **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

Element	Inhalt	Beispiel
at	Zeitpunkt des Widerspruchs (wird durch das Entitlement Management gesetzt)	2025-01-01T12:00:00Z

2984 **A_25135 -Entitlement Management - Initialisierung der Blocked User Policy**

2985 Das Entitlement Management MUSS für ein Aktenkonto eine Blocked User Policy ohne
 2986 initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policies über die
 2987 Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`
 2988 ermöglichen. [`<=`]

2989 **A_24514 -Entitlement Management - Keine Befugnis für von einer Befugnis ausgeschlossene Nutzer**

2991 Das Entitlement Management MUSS sicherstellen, dass für keinen durch einen Eintrag
 2992 der Blocked User Policy referenzierten Nutzer eine Befugnis existiert oder erstellt werden
 2993 kann. [`<=`]

2994 **A_24515 -Entitlement Management- Verschlüsselung der Einträge der Blocked User Policy**

2996 Das Entitlement Management MUSS Einträge der Blocked User Policy mit dem
 2997 Befugnispersistierungsschlüssel (`SecureAdminStorageKey`) verschlüsseln und im
 2998 Aktenkonto persistieren. [`<=`]

2999 Die Konfiguration der Blocked User Policy erfolgt über die Schnittstelle
 3000 `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` durch ein ePA-FdV
 3001 bzw. durch die Ombudsstelle.

3002 **A_24965 -Entitlement Management - Information über Änderungen der Blocked User Policy**

3004 Das Entitlement Management MUSS den Aktenkontoinhaber bei einer Änderung der
 3005 Blocked User Policy, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber
 3006 informieren, dass ein Befugnisausschluss geändert wurde, wann die Änderung erfolgte
 3007 und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden
 3008 sind. [`<=`]

3009 **3.9.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)**

3010 Die Erstellung von Befugnissen durch Primärsysteme der Leistungserbringerinstitutionen
 3011 wird durch das Aktensystem mengenmäßig über einen Zeitraum begrenzt. Diese
 3012 Maßnahme verhindert den massenhaften Zugriff auf Aktenkonten durch Fehlbedienung
 3013 seitens eines Primärsystems oder durch unzulässige Nutzung der Aktensysteme.

3014 Die maximal zulässige Befugnismenge ist dabei so bemessen, dass die intendierte
 3015 Nutzung der ePA durch Leistungserbringerinstitutionen im Versorgungsalltag nicht
 3016 eingeschränkt wird. Diese maximale Befugnismenge ist pro Nutzerrolle separat
 3017 festgelegt.

3018 Jedes Aktensystem führt dazu aktensystemweit Zähler für erteilte Befugnisse aus der
 3019 Umgebung der Leistungserbringer pro Telematik-ID. Die Erfassung erfolgt somit pro
 3020 Leistungserbringerinstitution separat. Die Zuordnung erfolgt zur Telematik-ID der
 3021 befugniserstellenden Nutzer (nicht des zu befugnenden Nutzers). Die Befugnisvergabe aus
 3022 der Umgebung des Versicherten mittels ePA-FdV wird nicht erfasst und geht nicht in die
 3023 Zählerstände ein.

3024 Das Entitlement Management wertet diese Menge der erfassten Befugnisvergaben im Falle
 3025 einer weiteren Befugnisvergabe durch ein Primärsystem aus der Umgebung der LEI aus

3026 und verhindert die Befugniserstellung bei Erreichen der maximal zulässigen
3027 Befugnismenge.

3028 Die zulässige Befugnisrate limitiert dabei einerseits die Menge der innerhalb einer Stunde
3029 erstellbaren Befugnisse, als auch die Menge der insgesamt monatlich erstellbaren. Die
3030 Zählung erfolgt aktensystemweit pro Aktensystem eines Herstellers und unabhängig vom
3031 adressierten Aktenkonto und berücksichtigt nur erfolgreiche Befugnisvergaben. Der
3032 Zeitraum pro Stunde, bzw. pro Monat, bezieht sich dabei auf den Zeitraum der aktuellen
3033 Stunde, bzw. des aktuellen Monats.

3034 **A_27311 -Entitlement Management – RateLimit-oid-List**

3035 Das Entitlement Management MUSS eine *RateLimit-oid-List* führen, in der pro oid

- 3036 • der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden
3037 Befugnisse innerhalb einer Stunde,
- 3038 • der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden
3039 Befugnisse innerhalb eines Monats und
- 3040 • der Zeitpunkt der letzten Änderung der Werte

3041 gespeichert werden.[<=]

3042 Initial ist die RateLimit-oid-List mit folgenden Werten zu belegen:

3043 **A_27290-01 -Entitlement Management – RateLimit-oid-List: Maximale Anzahl** 3044 **von Befugnissen für LEI pro Stunde**

3045 Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass eine LEI
3046 mit der Rolle

- 3047 • oid_praxis_arzt maximal 200 Befugnisse
- 3048 • oid_krankenhaus maximal 1.000 Befugnisse
- 3049 • oid_institution-vorsorge-reha maximal 1.000 Befugnisse
- 3050 • oid_zahnarztpraxis maximal 200 Befugnisse
- 3051 • oid_öffentliche_apotheke maximal 200 Befugnisse
- 3052 • oid_praxis_psychotherapeut maximal 100 Befugnisse
- 3053 • oid_institution-pflege maximal 100 Befugnisse
- 3054 • oid_institution-geburtshilfe maximal 100 Befugnisse
- 3055 • oid_praxis-physiotherapeut maximal 100 Befugnisse
- 3056 • oid_praxis-ergotherapeut maximal 100 Befugnisse
- 3057 • oid_praxis-logopaede maximal 100 Befugnisse
- 3058 • oid_praxis-podologe maximal 100 Befugnisse
- 3059 • oid_praxis-ernaehrungstherapeut maximal 100 Befugnisse
- 3060 • oid_institution-oegd maximal 100 Befugnisse
- 3061 • oid_institution-arbeitsmedizin maximal 100 Befugnisse

3062 innerhalb einer Stunde durch das Primärsystem im Aktensystem registrieren kann.
3063 [<=]

3064 **A_27291-01 -Entitlement Management – RateLimit-oid-List: Maximale Anzahl** 3065 **von Befugnissen für LEI pro Monat**

3066 Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass

- 3067 • oid_praxis_arzt maximal 10.000 Befugnisse
- 3068 • oid_krankenhaus maximal 200.000 Befugnisse
- 3069 • oid_institution-vorsorge-reha maximal 200.000 Befugnisse
- 3070 • oid_zahnarztpraxis maximal 10.000 Befugnisse
- 3071 • oid_öffentliche_apotheke maximal 25.000 Befugnisse
- 3072 • oid_praxis_psychotherapeut maximal 10000 Befugnisse
- 3073 • oid_institution-pflege maximal 10000 Befugnisse
- 3074 • oid_institution-geburtshilfe maximal 10000 Befugnisse
- 3075 • oid_praxis-physiotherapeut maximal 10000 Befugnisse
- 3076 • oid_praxis-ergotherapeut maximal 10000 Befugnisse
- 3077 • oid_praxis-logopaede maximal 10000 Befugnisse
- 3078 • oid_praxis-podologe maximal 10000 Befugnisse
- 3079 • oid_praxis-ernaehrungstherapeut maximal 10000 Befugnisse
- 3080 • oid_institution-oegd maximal 10000 Befugnisse
- 3081 • oid_institution-arbeitsmedizin maximal 10000 Befugnisse

3082 innerhalb eines Monats durch das Primärsystem im Aktensystem registrieren kann.
 3083 [`<=`]

3084 Hinweis zu A_27290-* und A_27291-*: Die Stunde bzw. der Tag müssen sich nicht auf
 3085 die aktuelle Stunde bzw. Kalendertag beziehen, sondern können auch je
 3086 Leistungserbringerinstitution auf Requestzeitpunkte bezogen werden. Dann gilt für einen
 3087 Monat 30 Tage.

3088 **A_27318 -ePA-Aktensystem - RateLimit-oid-List: Maßnahmen zum Schutz der** 3089 **Konfiguration**

3090 Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen
 3091 umsetzen, die eine unautorisierte Änderung der *RateLimit-oid-List* verhindern. [`<=`]

3092 **A_27312 -ePA-Aktensystem - RateLimit-oid-List: Konfiguration durch Betreiber**
 3093 Der Betreiber des ePA-Aktensystem MUSS sicherstellen, dass die Werte für die Anzahl
 3094 der maximalen Befugnisse in der *RateLimit-oid-List* durch den Betreiber des ePA-
 3095 Aktensystems ausschließlich im Vier-Augen-Prinzip konfigurierbar sind. [`<=`]

3096 Stellen LEI Befugnisse mittels der Operation `setEntitlementsPs` über das Primärsystem
 3097 in das ePA-Aktensystem ein, wird für diese LEI geprüft, ob diese bereits das zulässige
 3098 Limit erreicht hat. Nur falls dies nicht der Fall ist, kann die Befugnis eingestellt werden.
 3099 Hierzu erfasst das ePA-Aktensystem außerhalb der VAU wann ein Nutzer mit welcher
 3100 Rolle eine Befugnis registriert hat. Für den Nutzer wird außerhalb der VAU ein
 3101 Nutzerpseudonym geführt.

3102 **A_27313-01 -Entitlement Management - Prüfen der RateLimit-oid-List beim** 3103 **Einstellen von Befugnissen**

3104 Das Entitlement Management MUSS bei Aufruf der Operation `setEntitlementsPs` oder
 3105 `setEntitlementPsV2` prüfen, ob für das zur LEI gehörende Nutzerpseudonym und die oid
 3106 der LEI bereits das in der *RateLimit-oid-List* vorgegebene maximale Limit pro Stunde
 3107 oder Monat erreicht wurde. Falls ein Limit erreicht wurde, wird die Operation
 3108 `setEntitlementsPs`, bzw. `setEntitlementPsV2`, mit einem Fehler abgebrochen. Falls
 3109 kein Limit erreicht wurde, ist die Registrierung für das zur LEI gehörende
 3110 Nutzerpseudonym zu vermerken. [`<=`]

3111 **A_27310 -ePA-Aktensystem - Erfassung der Nutzer zur Prüfung RateLimit-oid-**
3112 **List**

3113 Das ePA-Aktensystem MUSS sicherstellen dass bei der Erfassung der Nutzerdaten
3114 außerhalb der VAU zur Prüfung der *RateLimit-oid-List* eine Profilierung über die Nutzer
3115 nicht möglich ist und zu diesem Zweck aus der TelematikId eines Nutzers ein
3116 Nutzerpseudonym abgeleitet wird, gemäß gemSpec_Krypt#7.5 Routing auf VAU-
3117 Instanzen.

3118 [\leq]

3119 **3.9.6 EntitlementDenyList**

3120 Ein Primärsystem einer Leistungserbringerinstitution (LEI) kann eine Befugnis für ein
3121 Aktenkonto eines Versicherten in einer Behandlungssituation ("Stecken" der eGK, VSDM-
3122 Prüfungsnachweis) eigenständig erstellen, wenn der Versicherte der Nutzung der ePA
3123 nicht widersprochen hat, für die konkrete Leistungserbringerinstitution im Aktenkonto
3124 kein Befugnisausschluss (3.9.4- Befugnisausschluss (Blocked User Policy)) vorliegt und
3125 die Leistungserbringerinstitution einer grundsätzlich befugbaren Nutzergruppe angehört
3126 (3.9- Entitlement Management).

3127 Die bestimmte LEI deren Telematik-ID auf einer sogenannten EntitlementDenyList
3128 stehen, wird diese Funktionalität durch das Aktensystem unterbunden, in der Weise dass
3129 eine Befugnisvergabe durch das Aktensystem unterbunden wird.

3130 Die Befugnisvergabe durch den Versicherten oder einen Vertreter mittel ePA-FdV ist
3131 durch die EntitlementDenyList nicht eingeschränkt. Über ein ePA-FdV können auch LEI
3132 befugt werden, die einen Eintrag in der EntitlementDenyList haben.

3133 Die EntitlementDenyList wird durch das Aktensystem bei jedem Aufruf einer Operation
3134 zur Befugnisvergabe durch ein Primärsystem ausgewertet. Diese Operation wird mit
3135 einem Fehler beendet, wenn die zu befugende LEI Bestandteil der Liste ist. Eventuell
3136 vorhandene Befugnisse dieser LEI, etwa aus einer Befugnisvergabe mittels ePA-FdV,
3137 verbleiben im Fehlerfall der Operation unverändert.

3138 Die EntitlementDenyList wird für alle Aktenkonten eines Aktensystems einheitlich
3139 verwaltet. Die Verwaltung erfolgt außerhalb der VAU, die Liste muss aber für Operationen
3140 der Befugnisvergabe innerhalb der VAU zugänglich sein.

3141 **A_27730 -ePA-Aktensystem - EntitlementDenyList außerhalb der VAU**

3142 Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen
3143 umsetzen, die eine unautorisierte Änderung der EntitlementDenyList verhindern. [\leq]

3144 **A_27731 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren**

3145 Das ePA-Aktensystem MUSS sicherstellen, dass falls eine LEI (Telematik-ID) aus der
3146 EntitlementDenyList entfernt wird, in der VAU nach spätestens 24 Stunden die
3147 EntitlementDenyList aktualisiert wird. [\leq]

3148 **A_27732 -ePA-Aktensystem - EntitlementDenyList in VAU aktualisieren -**
3149 **Ausschluss einer LEI**

3150 Falls eine LEI der EntitlementDenyList hinzugefügt wird, MUSS der Betreiber des ePA-
3151 Aktensystems sicherstellen, dass die EntitlementDenyList in der VAU unverzüglich
3152 aktualisiert wird. [\leq]

3153 Hinweise zu A_27732-*:

- 3154 • Die gematik übermittelt die komplette aktuelle EntitlementDenyList an den
3155 Anbieter des ePA-Aktensystems.
- 3156 • Die gematik übermittelt die aufgrund von Sicherheitsgründen aktualisierte
3157 EntitlementDenyList über die etablierten Incident-Prozesse.

A_27714 -Entitlement Management - setEntitlementPs in Abhängigkeit von EntitlementDenyList

Falls der Nutzer auf der EntitlementDenyList enthalten ist, MUSS das Entitlement Management die Operation `setEntitlementPs` ohne Erzeugung einer Befugnis mit dem HTTP-Statuscode 409requestMismatch abbrechen.

[<=]

Technische Details zur Aktualisierung der EntitlementDenyList im Aktensystem:

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

A_27780 -Übertragungsformat der EntitlementDenyList (gematik->ePA-Aktensystem).

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

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

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

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

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

Beispiel für eine EntitlementDenyList gemäß A_27780-*:

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

```
3211         "3-07.2.1234567890.123",
3212         "3-14.2.1234567890.123"
3213     ],
3214     "TruncatedHash": "pee1nuX5TxSce3QSawdqs+Pf0L6UMCr8"
3215 }
3216
```

3217 **A_27781 -Hashwertberechnung der Telematik-ID-Einträge in einer**

3218 **EntitlementDenyList**

3219 Eine ePA-Aktensystem MUSS bei der Berechnung des Hashwertes für die BDE-
3220 Datenlieferung gemäß A_22469-*:

- 3221 1. die Einträge in Array "TelematikIDs" alphabetisch aufsteigend sortieren,
- 3222 2. die Einträge jeweils mit dem Inhalt von "separator" als Verbindungselement zu
3223 einer einzigen lange Bytefolge konkatenieren,
- 3224 3. von dieser langen Bytefolge den SHA-256-Hashwert berechnen.

3225 Der berechnete Hashwert MUSS Base64 kodiert werden. Das Ergebnis ist dann der
3226 Hashwert der für die BDE-Datenlieferung gemäß A_22469-* und A_27782-* zu
3227 verwenden ist.

3228 [**<=**]

3229 Beispiele für A_27281-*:

3230 1)

3231 Wäre separator="AAA" und TelematikIDs=["1", "2", "3"], dann wären die
3232 dtbh="1AAA2AAA3". Der Base64-kodierte Hashwert wäre
3233 dann NFtIcjtAGzo8tL5goB6QMXpHkNCjDSFK5oTzILjXu8k=

3234 2)

3235 Mit den Daten aus dem oben aufgeführten Beispiel für A_27780-* würde ein
3236 Aktensystem pee1nuX5TxSce3QSawdqs+Pf0L6UMCr80uM3VYtVJdU= berechnen.

3237 **A_27782 -EntitlementDenyList: Hashwertberechnung der Telematik-ID-Einträge**

3238 **im Aktensystem**

3239 Ein ePA-Aktensystem MUSS sicherstellen, dass bei Aktualisierung der
3240 EntitlementDenyList-Daten am Enforcement-Point der EntitlementDenyList wie in
3241 A_22467-* definiert, eine Meldung an die BDE erzeugt und übermittelt wird. Dabei MUSS
3242 es den dabei zu übermittelnden Hashwert wie in A_27781 definiert berechnen. (vgl. auch
3243 Hinweise zu A_22782-*)

3244 [**<=**]

3245 Hinweise zu A_27782-*:

3246 Zum besseren Verständnis, falls der Enforcement-Point die VAU-Instanz ist, so muss
3247 beim initialen Starten der VAU-Instanz die EntitlementDenyList in die VAU-Instanz
3248 geladen werden. Diese gilt als Aktualisierung der EntitlementDenyList-Daten in der VAU-
3249 Instanz. Somit gilt dort A_27782-*.

3250 **3.10 Legal Policy**

3251 Die Legal Policy enthält die gesetzlich verbindlichen Regelungen der Zugriffsrechte bzgl.
3252 der Berufsgruppen und Datenkategorien gemäß§ 341 Absatz 2 SGB V.

3253 Für die Datenkategorien sind die grundsätzlichen Zugriffsrechte der Zugriffsoperationen
3254 (CRUD - create, read, update, delete) vorgegeben. Diese Zugriffsrechte wirken
3255 ausnahmslos für jeden befugten Nutzer.

3256 Beispiele sind:

- 3257 • Apotheker haben keinen Zugriff auf die zahnärztliche Dokumentation in der
3258 Datenkategorie "dental".
- 3259 • Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen
3260 noch löschen.

3261 Die Legal Policy wird durch das Aktensystem durchgesetzt und ist jederzeit vorhanden.
3262 Die Konfiguration kann durch Clients oder Bestandteile des Aktensystems nicht verändert
3263 werden.

3264 **A_19303-23 -Legal Policy – gesetzlich vorgegebene Zugriffsrechte**

3265 Das ePA-Aktensystem MUSS alle in der folgenden Tabelle aufgeführten Regeln der Legal
3266 Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

3267 **Tabelle 19: Legal Policy**

Kategorie	Nutzergruppe										
Technischer Identifier	Med	Apo	Pflege	GH	HME	AM	KT R	O M	DiG A	eR P	Ver
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

Kategorie	Nutzergruppe										
vaccination	CRU D	CRU D	R	R	-	CRU D	-	-	-	-	RD
patient	RD	R	R	R	R	R	C	-	-	-	CRU D
receipt	RD	RD	-	R	R	R	CU	-	-	-	RD
health_risk_analys is	-	-	-	-	-	-	C	-	-	-	RD
diga	R	R	R	R	R	R	-	-	CU	-	RD
care	CRU D	R	CRUD	R	R	R	-	-	-	-	RD
eau	CRU D	-	-	-	-	R	-	-	-	-	RD
rehab	CRU D	-	-	-	-	-	-	-	-	-	RD
transcripts	CRU D	-	-	-	-	-	-	-	-	-	RD
other	CRU D	-	-	-	-	R	-	-	-	-	RD
Medical Services (FHIR Data Services)	Zugriffsrecht										
medication	R	R	R	R	R	R	-	-	-	CU	R
demographics	-	-	-	-	-	-	CU	-	-	-	R
documents	R	R	R	R	R	R	-	-	-	-	R
Basic Services	Zugriffsrecht										
Audit Events	-	-	-	-	-	-	-	x	-	-	x
Consent Decisions	-	-	-	-	-	-	-	x	-	-	x
Constraints	-	-	-	-	-	-	-	-	-	-	x
Devices	-	-	-	-	-	-	-	-	-	-	x

Kategorie	Nutzergruppe										
Entitlements	x	x	x	x	x	x	-	-	-	-	x
Entitlements.Blocked User	-	-	-	-	-	-	-	x	-	-	x
Information	x	x	x	x	x	x	x	x	x	x	-

Nutzergruppen:

- Med = Arztpraxis, Zahnarztpraxis, Krankenhaus, Psychotherapeut, Vorsorge- und Rehabilitation, Öffentlicher Gesundheitsdienst
- (oid_praxis_arzt,, oid_krankenhaus, oid_institution-vorsorge-reha, oid_zahnarztpraxis, oid_praxis_psychotherapeutoid_institution-oegd)
- Apo = Öffentliche Apotheke
- (oid_öffentliche_apotheke)
- Pflege = Gesundheits-, Kranken- und Altenpflege
- (oid_institution-pflege)
- GH = Geburtshilfe
- (oid_institution-geburtshilfe)
- HME = Heilmittelerbringer
- (oid_praxis-physiotherapeut, oid_praxis-ergotherapeut, oid_praxis-logopaede, oid_praxis-podologe, oid_praxis-ernaehrungstherapeut)
- AM = Arbeitsmedizin
- (oid_institution-arbeitsmedizin)
- KTR = Kostenträger
- (oid_kostentraeger)
- OM = Ombudsstelle
- (oid_ombudsstelle)
- DiGA = Digitale Gesundheitsanwendung
- (oid_diga)
- eRP = E-Rezept vertrauenswürdige Ausführungsumgebung
- (oid_erp-vau)
- Ver = Versicherter / Vertreter
- (oid_versicherter)

Legende:

- CRUD = create, read, update, delete; update: Aktualisierung von Metadaten, Aktualisierung eines Dokuments
- "-" = keine Zugriffsrechte;

- 3299 • "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den
3300 Dienst (Service) definiert)
- 3301 • "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- 3302 • "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung
3303 in einer zukünftigen Version der ePA vorgesehen.

3304 Hinweise:

- 3305 • (*) Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann der
3306 Versicherte bzw. sein Vertreter oder eine Leistungserbringerinstitution gemäß der
3307 zuvor genannten Liste definierter professionOIDs sein. Sofern ein
3308 Versicherter/Vertreter der Einsteller der Elternnotiz ist, darf er abweichend von
3309 den oben aufgeführten Zugriffsunterbindungsregeln in die Datenkategorie mit
3310 dem technischen Identifier 'child' schreiben.

3311 [\leq]

3312 **A_26166-02 -Legal Policy (EU) – EU-Zugriff: gesetzlich vorgegebene**
3313 **Zugriffsrechte**

3314 Das ePA-Aktensystem MUSS zusätzlich zu den Regeln aus A_19303-* alle in der
3315 folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und
3316 Dienste des Aktenkontos durchsetzen.

3317 **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	-

Kategorie	Nutzergruppe
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	-

3318

3319 Nutzergruppen:

3320 • NCPeH = NCPeH-Fachdienst (oid_ncpeh)

3321 Legende:

3322 • CRUD = create, read, update, delete; update: Aktualisierung von Metadaten,
3323 Aktualisierung eines Dokuments

3324 • "-" = keine Zugriffsrechte;

- 3325 • "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den
- 3326 Dienst (Service) definiert)
- 3327 • "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- 3328 • "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung
- 3329 in einer zukünftigen Version der ePA vorgesehen.

3330 [**<=**]

3331 Die folgende Tabelle erläutert die Kategorien aus A_19303-* und A_26166-*:

3332 **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)

Technischer Identifier	Beschreibung
pregnancy_childbirth	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass) sowie Daten, die sich aus der Versorgung der Versicherten mit Hebammenhilfe ergeben
vaccination	Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation)
patient	Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden
receipt	Bei Kostenträgern gespeicherte Daten über die in Anspruch genommenen Leistungen des Versicherten
health_risk_analysis	Ergebnisse datengestützter Auswertungen der Krankenkassen zu individuellen Gesundheitsrisiken gemäß SGB V § 25b.
diga	Daten des Versicherten aus digitalen Gesundheitsanwendungen des Versicherten nach § 33a.
care	Daten zur pflegerischen Versorgung des Versicherten nach den §§ 24g, 37, 37b, 37c, 39a und 39c und der Haus- oder Heimpflege nach § 44 des Siebten Buches und nach dem Elften Buch
eau	Daten nach § 73 Absatz 2 Satz 1 Nummer 9 ausgestellte Bescheinigung über eine Arbeitsunfähigkeit
rehab	Daten der Heilbehandlung und Rehabilitation nach § 27 Absatz 1 des Siebten Buches
transcripts	Elektronische Abschriften von der Patientenakte eines Primärsystems gemäß §630g Abs. 2 BGB
other	Sonstige von Leistungserbringern für Versicherten bereitgestellte Daten, insbesondere Daten, die sich aus der Teilnahme des Versicherten an strukturierten Behandlungsprogrammen bei chronischen Krankheiten gemäß § 137f ergeben
Medical Services	FHIR Data Services
medication	Verordnungs-, Dispensier- und Medikationsdaten in einer elektronischen Medikationsliste (eML) und einem elektronischen Medikationsplan (eMP)

Technischer Identifier	Beschreibung
demographics	Bereitstellung demographischer Daten des Versicherten für Medical Services
audit	Protokolle von Zugriffen aller Nutzer auf die Akte des Versicherten
documents	Suche & Bereitstellung (medizinischer) Dokumente aus dem XDS Document Service
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

3333

3334 **A_21211-01 -Legal Policy - Änderungen der Legal Policy nicht erlauben**

3335 Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass
 3336 Änderungen der Konfiguration der Legal Policy gemäß A_19303-* ausgeschlossen
 3337 sind. [≤]

3338 **A_24548 -Legal Policy - Durchsetzung der Zugriffsrechte der Legal Policy**

3339 Das ePA-Aktensystem MUSS sicherstellen, dass Operationen auf Daten und Operationen
 3340 der Dienste eines Aktenkontos abgebrochen und mit einer Fehlermeldung beendet
 3341 werden, wenn diese Operation durch die Vorgaben der Legal Policy gemäß A_19303-* für
 3342 die Nutzergruppe des Aufrufers der Operation nicht zulässig ist. [≤]

3343 **3.11 Constraint Management**

3344 Das Constraint Management des Aktenkontos stellt sicher, dass nur Zugriffe auf Daten in
 3345 Ordern des XDS Document Service über die Vorgaben der Legal Policy hinaus
 3346 zugelassen werden, welche nicht vom Versicherten oder einem Vertreter unterbunden
 3347 (verborgen) wurden.

3348 Die Umsetzung dieser Beschränkungen erfolgt anhand der **General Deny Policy** für
 3349 jeden befugten Nutzer der betroffenen Nutzergruppen des Aktenkontos.

3350 Die General Deny Policy adressiert Nutzergruppen (professionOID) und Metadaten
 3351 der Daten. Es können einzelne Dokumente, Kategorien oder Ordner verborgen werden.

3352 Bei jedem Zugriff auf Daten in Ordnern wird diese Policy bezüglich der Rolle eines
 3353 Nutzers und der betroffenen Dokumente ausgewertet und durchgesetzt.

3354 Die folgende Anforderung zeigt eine Übersicht der Nutzergruppen, für welche Dokumente
 3355 durch Einträge in der General Deny Policy vor einem Zugriff verborgen werden können.

3356 **A_24306-02 -Constraint Management - Policy für berechtigte Nutzergruppen**
 3357 **und Nutzer**

3358 Das Constraint Management MUSS die Konfiguration der General Deny Policy auf die
 3359 folgenden Nutzergruppen einschränken:
 3360

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

3361
 3362
 3363 **[<=]**

3364 **A_24390-01 -Constraint Management- Anwendung der General Deny Policy**

3365 Das Constraint Management MUSS bei jedem Zugriff auf Daten durch den XDS Document
 3366 Service durch befugte Nutzer oder Nutzergruppen die General Deny Policy anwenden und

3367 den Zugriff verhindern, wenn ein Dokument oder dessen assoziierter Ordner oder dessen
 3368 assoziierte Datenkategorie in der Policy konfiguriert ist.

3369 [**<=**]

3370 Dienste des Aktenkontos (Basic Services) können nicht verborgen werden. Hier gelten die
 3371 Zugriffsregelungen gemäß Legal Policy und die Beschränkungen der Schnittstellen.

3372 Datendienste (Medication Service) können nicht auf Daten- oder Ordner Ebene verborgen
 3373 werden. Hier gelten die Regelungen bezüglich des Widerspruchs gegen die Nutzung von
 3374 widerspruchsfähigen Funktionen der ePA (siehe 3.8- Consent Decision Management).

3375 Die Kategorie "emp", bzw. einzelne Dokumente dieser Kategorie, des XDS Document
 3376 Service dürfen nicht verborgen werden. Die Nutzung der Dokumente der Kategorie "emp"
 3377 wird über das Consent Decision Management, bzw. einen erteilten Widerspruch gegen die
 3378 widerspruchsfähige Funktion "medication" der ePA verhindert (siehe 3.8- Consent
 3379 Decision Management).

3380 Die Operationen der Schnittstelle des Constraint Managements erlauben die
 3381 Konfiguration der General Deny Policy durch den Versicherten oder einen befugten
 3382 Vertreter.

3383 **A_24395 -Constraint Management - Realisierung der Schnittstelle**

3384 **I_Constraint_Management_Insurant**

3385 Das Constraint Management MUSS die Operationen der Schnittstelle
 3386 I_Constraint_Management_Insurant gemäß [I_Constraint_Management_Insurant]
 3387 umsetzen. [**<=**]

3388 **A_24887-01 -Constraint Management - Protokolleinträge für Zugriffe auf das** 3389 **Constraint Management**

3390 Das Constraint Management MUSS für das Aufnehmen und Löschen von Einträgen in die
 3391 General Deny Policy jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist
 3392 folgende Wertbelegung zu berücksichtigen:

3393 **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		

Strukturelement	Wert		Erläuterung
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

3394

3395 **[<=]**

3396 Für die Policy gelten folgende Vorgaben.

3397 **A_24393-01 -Constraint Management - Initialisierung der General Deny Policy**

3398 Das Constraint Management MUSS für ein Aktenkonto eine General Deny Policy ohne
 3399 initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policy über die
 3400 Schnittstelle `I_Constraint_Management_Insurant` gemäß

3401 `[I_Constraint_Management_Insurant]` ermöglichen.**[<=]**

A_24462-01 -Constraint Management - Konfiguration der General Deny Policy anpassen nach Löschen von Ordnern

Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn diese einen Ordner referenzieren und dieser Ordner aus dem Aktenkonto gelöscht wird. [≤]

A_24461-01 -Constraint Management - Konfiguration der General Deny Policy anpassen nach Löschen von Dokumenten

Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn diese ein spezifisches Dokument referenzieren und dieses Dokument aus dem Aktenkonto gelöscht wird. [≤]

A_24516-01 -Constraint Management - Speichern der Inhalte der General Deny Policy

Das Constraint Management MUSS Einträge aus der General Deny Policy unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen. [≤]

3.11.1 Aktenkontoweites Verbergen (General Deny Policy)

Die General Deny Policy wird durch das Aktensystem für die in A_24306-* unter "General Deny Policy" aufgeführten Nutzergruppen angewendet und durchgesetzt. Einträge der General Deny Policy gelten dabei immer für alle aufgeführten Nutzergruppen gemeinsam.

Die Konfiguration der General Deny Policy erfolgt durch den Versicherten oder einen befugten Vertreter mittels ePA-FdV. Einträge können hinzugefügt oder entfernt werden. Zum Zeitpunkt der Erstellung des Aktenkontos enthält die General Deny Policy keine Einträge.

Ein Eintrag in der General Deny Policy referenziert entweder ein bestimmtes Dokument, einen dynamischen Ordner oder eine Datenkategorie. Die Menge der Einträge ist nicht limitiert.

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

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

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

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

3450 Ein Eintrag der General Deny Policy enthält Angaben gemäß der folgenden Tabelle:

3451 **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 Identifiziert der zu verbergende Kategorie

3452

3453 Beispiel:

3454 **Tabelle 24: Verbergen eines Medical Service**

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

3455 3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des 3456 confidentialityCodes

3457 Das Verbergen über den confidentialityCode ist im Kontext der Operationen des XDS
3458 Document Service definiert und in 3.13.1.10- Verbergen von Dokumenten durch
3459 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 deviceIdentifizier 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,

3552 • Fehlerzähler.

3553 [<=]

3554 Hinweis zu A_25271-*: Für die verschlüsselte Speicherung der Geräteinformationen sind
3555 die Anforderungen aus Abschnitt 3.5.1.3 zu berücksichtigen.

3556 **A_25272 -Device Management - Pseudonyme Speicherung der**
3557 **Geräteinformationen**

3558 Das Device Management MUSS sicherstellen, dass die Zuordnung der außerhalb der VAU
3559 persistierten verschlüsselten Geräteinformationen zum Nutzer eindeutig ist und durch ein
3560 Pseudonym erfolgt.[<=]

3561 Hinweis: Aus A_25272 folgt, dass die Zuordnung der Speicherung der verschlüsselten
3562 Geräteinformationen nicht über die KVN-R des Nutzers erfolgen darf.

3563 **A_25273 -Device Management - Gültigkeitsdauer des Geräteregistrierungscodes**

3564 Das Device Management MUSS sicherstellen, dass der bei der Geräteregistrierung
3565 erzeugte Geräteregistrierungsscode maximal 6 Stunden nach Erzeugung der DeviceID
3566 (createdAt) für die Verifikation eines Gerätes genutzt werden kann.[<=]

3567 **A_25274 -Device Management - Löschen nach Gültigkeitsdauer des**
3568 **Geräteregistrierungscodes**

3569 Das Device Management MUSS sicherstellen, dass die Geräteinformationen für eine nicht
3570 bestätigte Geräteregistrierung nach Ende der Gültigkeitsdauer des
3571 Geräteregistrierungscodes gelöscht werden.[<=]

3572 **A_25275 -Device Management - Versenden des Geräteregistrierungscodes per**
3573 **E-Mail**

3574 Das Device Management MUSS bei der Geräteregistrierung für den Nutzer, für den das
3575 Gerät registriert werden soll, alle im Aktensystem hinterlegten E-Mail-Adressen ermitteln
3576 und an alle ermittelten E-Mail-Adressen eine E-Mail in einer für den Nutzer verständlichen
3577 Form mit folgenden Informationen versenden:

- 3578 • Zweck der E-Mail,
- 3579 • Geräteregistrierungsscode,
- 3580 • Gültigkeitsdauer des Geräteregistrierungscodes.

3581 [<=]

3582 **A_25276 -Device Management - Bestätigung mittels Geräteregistrierungscodes**

3583 Das Device Management MUSS für einen übergebenen Geräteregistrierungsscode und eine
3584 übergebene DeviceID (deviceIdentifizier und deviceToken) prüfen, ob der vom Device
3585 Management bei der Geräteregistrierung erzeugte Geräteregistrierungsscode für das
3586 angegebene Gerät (deviceIdentifizier, deviceToken) mit dem übergebenen
3587 Geräteregistrierungsscode übereinstimmt sowie der Geräteregistrierungsscode zeitlich
3588 gültig ist und

3589 1. bei Gleichheit und

3590 a. zeitlicher Gültigkeit

3591 • den Status für die Geräteregistrierung wechseln, so dass die erfolgreiche
3592 Bestätigung des Geräts aus dem Status hervorgeht,

3593 • den Geräteregistrierungsscode und den Fehlerzähler aus den
3594 Geräteinformationen löschen und

3595 • den Zeitpunkt der erfolgreichen Bestätigung in lastUsed erfassen,

3596 b. zeitlicher Ungültigkeit

- 3597 • alle Geräteinformationen zu diesem deviceIdentifier löschen,
3598 2. bei Ungleichheit den Fehlerzähler der Geräteinformation um eins erhöhen und
3599 • falls der Fehlerzähler größer oder gleich fünf ist,
3600 • alle Geräteinformationen zu diesem Gerät löschen.

3601 [<=]

3602 **A_25277 -Device Management - Sperrung bei vermehrter Anzahl von**
3603 **abgebrochenen Geräteregistrierungen**

3604 Falls für einen Nutzer innerhalb von 8 Stunden drei Geräteregistrierungen abgebrochen
3605 werden mussten, MUSS das Device Management sicherstellen, dass dieser Nutzer für 8
3606 Stunden ab dem Zeitpunkt der dritten abgebrochenen Geräteregistrierung keine Geräte
3607 mehr registrieren darf.[<=]

3608 **A_25291 -ePA-Aktensystem - Health Record Context nur mit verifizierten Gerät**

3609 Das ePA-Aktensystem MUSS sicherstellen, dass ein Versicherter (auch wenn er als
3610 Vertreter agiert) einen Health Record Context ausschließlich mit einem verifizierten Gerät
3611 öffnen kann, außer für den Fall, dass sich der Versicherte am ePA-FdV des Vertreters
3612 anmeldet (d.h. x-authorize-representative=True bei der Operation
3613 I_Authorization_Service::sendAuthorizationRequestFdV).[<=]

3614 Eine Geräteregistrierung im Home-AS kann in einem anderen Aktensystem nachgenutzt
3615 werden. Hierzu kann ein ePA-FdV mittels `getDeviceAttestation` eine Device Attestation
3616 vom Home-AS abrufen, welche beim anderen Aktensystem genutzt werden kann.

3617 **A_26157 -Device Management - Device Attestation kann nur mit verifiziertem**
3618 **Gerät abgerufen werden**

3619 Das Device Management MUSS sicherstellen, dass die Operation `getDeviceAttestation`
3620 ausschließlich nach erfolgreicher Authentifizierung des Nutzers und mit einem auf den
3621 Nutzer registrierten und verifizierten Gerät erfolgt.

3622 [<=]

3623 **A_26156 -Device Management - Inhalte der Device Attestation**

3624 Das Device Management MUSS sicherstellen, dass eine von einem ePA-FdV über die
3625 Operation `getDeviceAttestation` abgerufene Device Attestation folgende Inhalte
3626 enthält:

Attribut	Inhalt
actorId	KVNR aus dem ID-Token des angemeldeten Nutzers (bzw. der User Session)
iat	Zeitstempel Ausgabezeitpunkt
exp	Verfalldatum, = "iat" + 2 Stunden

3627 [<=]

3628 **A_26158 -Device Management - Signatur der Device Attestation**

3629 Das Device Management MUSS sicherstellen, dass die über `getDeviceAttestation`
3630 abgerufene Device Attestation mit dem privaten Schlüssel der Signaturidentität der VAU
3631 des Home-AS signiert wird.[<=]

3.13 Medical Services

A 25830-03A_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 oder MAINTENANCE),
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.*

3717

A_25009-03 -XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten durch Versicherte

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

- application/pdf nur PDF/A gemäß A_25233 (pdf)
- text/plain (txt)
- application/fhir+xml (xml)
- application/json (json)

Ferner MUSS der XDS Document Service sicherstellen, dass ausschließlich die Elternnotiz des Kinderuntersuchungshefts als FHIR Document mit dem MIME-Type "application/fhir+xml" registriert werden kann - andere FHIR Documents sind nicht zulässig.

[<=]

Hinweise zu A_24864- und A_25009-*: Die Prüfung des zulässigen Dokumentenformats muss mindestens*

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

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

Für XML-Dokumente muss eine Schema-Validierung ausschließlich auf Basis bekannter, intern vorliegender XML Schema-Definitionen durchführen. Gegen nicht intern vorliegende XML Schema-Definitionen wird nicht validiert. Die Schema-Validierung kann innerhalb des Health Record Contexts ohne zusätzliche Isolation erfolgen.

A_24867 -XDS Document Service - Isolation der Formatprüfung

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

[<=]

Hinweise zu A_24867-:*

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

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

3762 Findet eine Dokumentenformatprüfung innerhalb eines Health Record Context statt, wird
3763 durch den Isolationsmechanismus aus A_24636-* verhindert, dass sich die
3764 Dokumentenformatprüfung schadhaft auf andere Health Record Contexte auswirkt. Es
3765 verbleibt dann zur Umsetzung der A_24867-* noch zu gewährleisten, dass sich die
3766 Dokumentenformatprüfung nicht schadhaft auf den Health Record Context auswirkt, in
3767 dem die Dokumentenformatprüfung erfolgt.

3768 Wenn Dokumentenprüfungen innerhalb eines Health Record Contexts ohne Isolation
3769 erfolgen, muss sichergestellt werden, dass sich diese Prüfungen nicht schadhaft auf den
3770 Health Record Context (oder andere) auswirken können. Dies ist vom Produktgutachter
3771 zu prüfen und im Produktgutachten zu dokumentieren.

3772 Ein Ausschluss einer schadhaften Auswirkung auf den Health Record Context ist bei
3773 folgenden Prüfungen des Dokumentenformats denkbar, so dass diese innerhalb des
3774 Health Record Contexts ohne zusätzliche Isolationsmaßnahmen durchgeführt werden
3775 können und kein Verstoß gegen die Anforderung A_24867-* vorliegt:

- 3776 • Prüfung der Magic Bytes des Dokuments (wo technisch möglich)
- 3777 • bei txt-, XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es
3778 bei XML-Dokumenten kein valides UTF8 ist, eine Prüfung auf "restriktives" ISO-
3779 8859-15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09,
3780 0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind."
- 3781 • bei XML- und JSON-Dokumenten: Parsen der Dokumente auf valides XML bzw.
3782 JSON mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert
3783 und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu
3784 bestätigen.
- 3785 • bei pkcs7-Dokumenten: Parsen der Dokumente mit Parsern, die entsprechend den
3786 Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser
3787 ist durch den Produktgutachter zu bestätigen.

3788 Der Produktgutachter muss bei der Umsetzung der oben genannten Prüfungen
3789 bestätigen, dass der Ausschluss einer schadhaften Auswirkung auf den Health Record
3790 Context (oder andere) durch die Umsetzung im Produkt tatsächlich gegeben ist.

3791

3792 **A_25285 -XDS Document Service - Sicheres Löschen von Dokumenten mit** 3793 **unzulässigem Format**

3794 Falls der XDS Document Service bei der Prüfung des Dateiformats (siehe A_24864-*)
3795 beim Einstellen eines Dokuments ein unzulässiges Format erkennt, MUSS der XDS
3796 Document Service das Dokument sicher löschen.

3797 [\leq]

3798 **A_24943 -XDS Document Service - Formatprüfung exponiert keine Daten aus** 3799 **der VAU heraus**

3800 Der XDS Document Service MUSS sicherstellen, dass bei der Formatprüfung (siehe
3801 A_24864-*) keine innerhalb der VAU verarbeiteten Daten die VAU verlassen. [\leq]

3802 **3.13.1.2 Anforderungen zur Validierung**

3803 **A_15035 -XDS Document Service – Verwendung von SOAP Message Security 1.1**

3804 Der XDS Document Service MUSS die Sicherheitsanforderungen aus SOAP Message
3805 Security 1.1 [WSS] für die Verarbeitung von SOAP 1.2-Nachrichten umsetzen. [\leq]

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

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

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

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

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

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

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

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

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

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

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

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

A_21200 -XDS Document Service und Clients – UTF-8 Kodierung von SOAP 1.2-Nachrichten

Der XDS Document Service und Clients des XDS Document Service MÜSSEN sicherstellen, dass die XML-Inhalte der SOAP 1.2-Nachrichten, die sie senden, der Zeichenkodierung UTF-8 entsprechen. [≤]

Es ist zu beachten, dass sich die Anzeige der verwendeten Kodierung in der Nachricht unterscheiden kann, z. B. in Nachrichten, in denen MTOM verwendet wird.

3.13.1.3 Namensräume

Für die Spezifikation der Schnittstellen des XDS Document Service werden die folgenden XML-Präfixe verwendet, um den Namensraum bzw. das Vokabular des XML-Dokuments zu kennzeichnen.

Präfix	Namensraum
lcm	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0
rmd	urn:ihe:iti:rmd:2017
rs	urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0
wsa	http://schemas.xmlsoap.org/ws/2004/08/addressing
wss	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
xdsb	urn:ihe:iti:xds-b:2007
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

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

3.13.1.4.1 Anforderungen an IHE ITI-Akteure

In diesem Abschnitt werden Anforderungen und Einschränkungen an relevante IHE ITI-Akteure und -Transaktionen des XDS Document Service gestellt, um die geforderte IHE ITI-Semantik zum ePA-Aktensystem zu bewahren. Werden IHE ITI-Akteure mit weiteren Sub-Akteuren gruppiert, so werden die Anforderungen der Sub-Akteure zum gruppierten Akteur übernommen. Eine Übersicht und Herleitung der IHE ITI-Akteure ist [3.13.1.4.2-Überblick über gruppierte IHE ITI-Akteure und Optionen](#) zu entnehmen.

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

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

Der XDS Document Service DARF NICHT vom Verhalten der definierten Außenschnittstellen `I_Document_Management`, sowie `I_Document_Management_Insurant` aus Abschnitt 3.13.1.6 abweichen. Dies schließt über die Anforderungslage hinausgehende Implementierungen von IHE ITI-Akteuren und Optionen innerhalb des XDS Document Service mit ein, sodass zusätzlich implementierte IHE-Funktionalitäten keine Auswirkungen an den definierten Außenschnittstellen aufweisen dürfen. [≤]

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

Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Registry" gemäß [IHE-ITI-TF1] implementieren. [≤]

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

Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]

Die § 291a-konforme Protokollierung von Zugriffen erfolgt mit Mechanismen außerhalb des IHE ITI-TF. Eine technische Protokollierung via ATNA kann gemäß der Anforderung A_17826 dennoch erfolgen.

A_13809 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs ATNA Audit Record Repository

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "ATNA Audit Record Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]

Die Mechanismen der IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure Application" zur Node Authentication werden über das Konzept "Vertrauenswürdige Ausführungsumgebung" (siehe 3.5- Vertrauenswürdige Ausführungsumgebung (VAU)) umgesetzt, sodass die Nutzung des Integrationsprofils ATNA diesbzgl. eingeschränkt wird.

A_17166 -XDS Document Service – Keine Implementierung der IHE ITI-Akteure ATNA Secure Node sowie ATNA Secure Application für Node Authentication

Der XDS Document Service DARF zur Node Authentication die IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure Application" gemäß [IHE-ITI-TF1] NICHT implementieren. [≤]

Der Zeitdienst der Telematikinfrastruktur unterstützt das Network Time Protocol in Version 4. Das IHE ITI-TF verlangt hingegen, das Zeitsynchronisierungsprotokoll in Version 3.

A_14654 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs CT Time Client

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "CT Time Client" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14665 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs XDS Document Source

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Source" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14667 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs XDS Integrated Document Source/Repository

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Integrated Document Source/Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]

3913 **A_14668 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3914 **XDS Document Consumer**

3915 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Consumer"
3916 gemäß [IHE-ITI-TF1] implementieren. [≤]

3917 **A_14666 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3918 **XDS Patient Identity Source**

3919 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Patient Identity
3920 Source" gemäß [IHE-ITI-TF1] implementieren.
3921 [≤]

3922 **A_14669 -XDS Document Service – Keine Implementierung des IHE ITI-Akteurs**
3923 **XDS On-Demand Document Source**

3924 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS On-Demand Document
3925 Source" gemäß [IHE-ITI-TF1] implementieren. [≤]

3926 **A_14950 -XDS Document Service – Keine Angabe einer Fehlerlokalisierung im**
3927 **RegistryError-Element**

3928 Der XDS Document Service DARF NICHT das `location`-Attribut im `rs:RegistryError`-
3929 Element in der IHE ITI-Ausgangsnachricht verwenden, sofern ein Fehler bei der
3930 Verarbeitung einer IHE ITI-Eingangsnachricht auftritt. Diese Einschränkung gilt nur für
3931 Error Stack Traces bzw. der Offenbarung von Programmierdetails. [≤]

3932 **A_15081 -XDS Document Service – Implementierung des IHE ITI-Akteurs RMU**
3933 **Update Responder**

3934 Der XDS Document Service MUSS den IHE ITI-Akteur "RMU Update Responder"
3935 gemäß [IHE-ITI-RMU] implementieren. [≤]

3936 3.13.1.4.1.1 Gruppierungen mit anderen IHE ITI-Akteuren

3937 **A_15093-02 -XDS Document Service – Gruppierung RMU Update Responder mit**
3938 **Document Registry**

3939 Der XDS Document Service als RMU-Akteur "Update Responder" MUSS mit dem XDS-
3940 Akteur "Document Registry" gemäß [IHE-ITI-RMU] gruppiert sein. [≤]

3941 3.13.1.4.1.2 Optionen des IHE ITI-Akteurs

3942 **A_15094 -XDS Document Service – RMU Update Responder ohne "Forward**
3943 **Update"-Option**

3944 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option
3945 "Forward Update" unterstützen.
3946 [≤]

3947 **A_15095-02 -XDS Document Service – RMU Update Responder ohne "XCA**
3948 **Persistence"-Option**

3949 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option
3950 "XCA Persistence" unterstützen. [≤]

3951 **A_15096-02 -XDS Document Service – RMU Update Responder mit "XDS**
3952 **Persistence"-Option**

3953 Der XDS Document Service als RMU-Akteur "Update Responder" MUSS die Option "XDS
3954 Persistence" unterstützen. [≤]

3955 **A_15097 -XDS Document Service – RMU Update Responder ohne "XDS Version**
3956 **Persistence"-Option**

3957 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option
3958 "XDS Version Persistence" unterstützen. [≤]

- 3959 3.13.1.4.1.3 Gruppierungen mit anderen IHE ITI-Akteuren
- 3960 3.13.1.4.1.4 Optionen des IHE ITI-Akteurs
- 3961 **A_14637 -XDS Document Service – XDS Document Registry ohne**
- 3962 **"Asynchronous Web Services Exchange"-Option**
- 3963 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
- 3964 "Asynchronous Web Services Exchange" unterstützen.[<=]
- 3965 **A_14638 -XDS Document Service – XDS Document Registry mit "Reference ID"-**
- 3966 **Option**
- 3967 Der XDS Document Service als XDS-Akteur "Document Registry" MUSS die
- 3968 Option "Reference ID" unterstützen.[<=]
- 3969 **A_14639 -XDS Document Service – XDS Document Registry ohne "Patient**
- 3970 **Identity Feed"-Option**
- 3971 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
- 3972 "Patient Identity Feed" unterstützen.
- 3973 [<=]
- 3974 **A_14640 -XDS Document Service – XDS Document Registry ohne "Patient**
- 3975 **Identity Feed HL7v3"-Option**
- 3976 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
- 3977 "Patient Identity Feed HL7v3" unterstützen.[<=]
- 3978 **A_14641 -XDS Document Service – XDS Document Registry ohne "On-Demand**
- 3979 **Documents"-Option**
- 3980 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option
- 3981 "On-Demand Documents" unterstützen.[<=]
- 3982 3.13.1.4.1.5 Optionen des IHE ITI-Akteurs
- 3983 **A_14636 -XDS Document Service – XDS Document Repository ohne**
- 3984 **"Asynchronous Web Services Exchange"-Option**
- 3985 Der XDS Document Service als XDS-Akteur "Document Repository" DARF NICHT die
- 3986 Option "Asynchronous Web Services Exchange" unterstützen.[<=]
- 3987 *3.13.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen*
- 3988 Die folgende Tabelle fasst die oben definierten Anforderungen zu Gruppierungen und
- 3989 Optionen zusammen. Dabei wird die folgende Notation für Optionalitäten (Opt.)
- 3990 verwendet:
- 3991 **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.

3992

3993
3994

Tabelle 26: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen des XDS Document Service

IHE ITI-Akteur	Opt.			Umzusetzende Option des IHE ITI-Akteurs	Opt.
		Gruppierung mit anderem IHE ITI-Akteur	Opt.		
ATNA Audit Record Repository	X				
CT Time Client	X				
RMU Update Responder	R			Forward Update	X
				XCA Persistence	X
				XDS Persistence	R
				XDS Version Persistence	X
		Document Registry	R		
XDS Document Consumer	X				
XDS Document Registry	R			Asynchronous Web Services Exchange	X
				Document Metadata Update	X
				On-Demand Documents	X
				Patient Identity Feed	X

IHE ITI-Akteur	Opt.			Umzusetzende Option des IHE ITI-Akteurs	Opt.
		Gruppierung mit anderem IHE ITI-Akteur	Opt.		
				Patient Identity Feed HL7v3	X
				Reference ID	R
		ATNA Secure Node oder Secure Application für Node Authentication	X		
XDS Document Repository	R			Asynchronous Web Services Exchange	X
		ATNA Secure Node oder Secure Application für Node Authentication	X		
XDS Document Source	X				
XDS Integrated Document Source / Repository	X				
XDS On-Demand Document Source	X				
XDS Patient Identity Source	X				

3995

3996 3.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen

3997 **A_17832 -XDS Document Service – Unterstützung MTOM/XOP**

3998 Der XDS Document Service MUSS gemäß den Anforderungen von [IHE-ITI-
3999 TF2x#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP
4000 [MTOM] verwenden.[<=]

4001 **A_24524 -XDS Document Service - Migration, Upload: Normalisieren des URI**

4002 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten
4003 den `DocumentEntry.URI` normalisieren. Dies gilt für `FileURI`, z.
4004 B. "<file:///C:/path/to/file.html#anchor>" oder "`/C/path/to/file.html#anchor`". Die URI MUSS
4005 auf den reinen Dateinamen mit Extension (d. h. ohne Pfadangaben) reduziert werden, z.
4006 B. "`file.html`". Nach der Normalisierung MUSS eine Validierung der Extension
4007 gemäß A_23447-* erfolgen.[<=]

4008 **A_23447-01 -XDS Document Service - DocumentEntry.URI extension entspricht**
4009 **mimetype**

4010 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten
4011 das Metadatum `DocumentEntry.URI` daraufhin prüfen, ob `DocumentEntry.URI` eine
4012 `filename extension` aufweist, die nicht dem `DocumentEntry.mimetype` entspricht. Zuvor
4013 muss die URI mittels A_24524-* normalisiert worden sein. Danach MUSS der XDS
4014 Document Service sicherstellen, dass in `Document.URI` die `filename extension` dem
4015 `DocumentEntry.mimeType` entspricht. Im Falle einer Abweichung MUSS an die
4016 ursprüngliche `DocumentEntry.URI` die `filename extension` gemäß A_24864-*, bzw.
4017 A_25009-*, angehängt werden, die dem `mimeType` entspricht. Die Groß-
4018 /Kleinschreibung der `filename extension` ist bei der Prüfung nicht relevant.[<=]

4019 **A_24451-01 -XDS Document Service - Automatisches initiales Erzeugen einer**
4020 **versionsübergreifenden ID für Dokumente**

4021 Der XDS Document Service MUSS beim initialen Einstellen eines Dokumentes die
4022 `DocumentEntry.uniqueId` als Eintrag einer `ReferenceID` in die `ReferenceIDList` in
4023 folgendem Format einstellen:

4024 `<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2023:rootDocumentUniqueId`

4025 Beim Upload einer neuen Version des Dokumentes DARF dieser Eintrag in der
4026 `ReferenceIDList`, d.h. die `rootDocumentUniqueId`, NICHT verändert werden. Er bleibt
4027 über alle Versionen des Dokumentes hinweg unverändert erhalten. Der Versuch eines
4028 Clients, die `rootDocumentUniqueId` durch ein `Metadata-Update` oder im Zuge des
4029 Einstellens einer neuen Dokumentenversion zu verändern, MUSS mit einem IHE-Error
4030 `XDSRegistryMetadataError` abgebrochen werden. Es MUSS im `codeContext`-Attribut
4031 des zurückgegebenen `XDSRegistryMetadataError`-Elements der
4032 Text „`rootDocumentUniqueId must not be changed`“ zurückgegeben werden.[<=]

4033 **A_14926-04 -XDS Document Service – Automatisiertes Löschen oder Verbergen**
4034 **von Dokumenten in RPLC-Ketten**

4035 Der XDS Document Service MUSS bei zu löschenden oder zu verbergenden Dokumenten
4036 und `DocumentEntry`-Einträgen im selben Zuge auch alle mittels
4037 `urn:ihe:iti:2007:AssociationType:RPLC` assoziierten `DocumentEntry`-Einträge und
4038 Dokumente löschen bzw. verbergen.[<=]

4039 **A_27683-01 -XDS Document Service – Maximale Länge von Anhangsketten**

4040 Der XDS Document Service MUSS sicherstellen, dass beim Einstellen (über die
4041 Schnittstelle `Provide and Register Document Set-b` [ITI-41]) oder Kennzeichnen (über die
4042 Schnittstelle `Restricted Update Document Set` [ITI-92]) von neuen Anhängen die gesamte
4043 Anhangskette inklusive des neuen Anhangdokuments und inklusive des obersten
4044 Elterndokuments nicht mehr als fünf Dokumente enthält und ansonsten die Operation mit
4045 dem Fehler `XDSMaxAttachmentsExceeded` abbrechen.
4046 [<=]

4047 Der Abschnitt 6.1- Dokumentenanhänge enthält eine Illustration für diese Anforderung.

4048 3.13.1.4.3.1 Provide and Register Document Set-b [ITI-41]

4049 **A_13715 -XDS Document Service – Ablauflogik für**

4050 **ProvideAndRegisterDocumentSet-b**

4051 Der XDS Document Service MUSS die Umsetzung der

4052 Operation ProvideAndRegisterDocumentSet-b gemäß den definierten Ablauflogiken

4053 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

4054 3.41.4.2.3] implementieren.[<=]

4055 **A_15162-06 -XDS Document Service – Keine Registrierung bei Angabe von**
 4056 **Document Entry Relationships in Metadaten**

4057 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und

4058 Dokument(en) ablehnen und mit einem XDSRepositoryMetadataError-Fehlercode

4059 quittieren, sofern die Metadaten andere Association Types nach [IHE-ITI-TF3#4.2.2.2]

4060 als die Folgenden enthalten:

4061 • urn:ihe:iti:2007:AssociationType:RPLC (Replace)

4062 [<=]

4063 **A_14938-02 -XDS Document Service – Validierung der Metadaten aus ITI**
 4064 **Document Sharing-Profilen**

4065 Der XDS Document Service MUSS die SubmissionSet- sowie die DocumentEntry-

4066 Metadaten der eingehenden Nachricht vor einer Zugriffskontrolle gemäß Konformität zu

4067 den Nutzungsvorgaben in [A_14760-*] prüfen. Der XDS Document Service MUSS das

4068 Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit

4069 einemXDSRepositoryMetadataError quittieren, sofern die Metadaten nicht konform zu

4070 den Nutzungsvorgaben sind. Es MUSS im codeContext-Attribut

4071 des zurückgegebenenrs:RegistryError-Elements angegeben werden, welches

4072 Metadatenattribut nicht den Nutzungsvorgaben entspricht.[<=]

4073

4074 **A_24521 -XDS Document Service - Erzeugen von Prüfsummen für Dokumente**

4075 Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes

4076 Dokument seine kryptographische Prüfsumme berechnen und inDocumentEntry.hash

4077 hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die

4078 Dokumentengröße inDocumentEntry.size berechnet und gesetzt werden.[<=]

4079 **A_24988-02A_24988-01 -XDS Document Service - Dublettenprüfung für**
 4080 **Dokumente**

4081 Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes

4082 Dokument den hash-Wert vergleichen mit allen bereits in dieser Akte existierenden hash-

4083 Werten der Dokumente und bei einer Übereinstimmung das Einstellen mit dem

4084 Fehlercode XDSDuplicateDocument ablehnen-, sofern nicht der Parameter

4085 "EnableDocumentReuse=true" (siehe A_27700) verwendet wird.

4086

4087 Es MUSS im codeContext-Attribut des zurückgegebenenrs:RegistryError-Elements die

4088 Liste der UUIDs (DocumentEntry.entryUUID) der identifizierten Dokumente angegeben

4089 werden. Der XDS Document Service MUSS diese Prüfung vor allen anderen

4090 Metadatenprüfungen durchführen.[<=]

4091 **A_27700 -XDS Document Service - Option zum Akzeptieren von Duplikaten**

4092 Der XDS Document Service MUSS in der Lage sein Duplikate, das heißt Dokumente, bei

4093 dem der DocumentEntry.hash eines einzustellenden Dokuments identisch ist mit einem

4094 existierenden Dokument, ohne Fehler zu akzeptieren, wenn

4095 die Anfrage in der <RequestSlotList> den folgenden Parameter enthält

```

4096
4097 <Slotname="urn:gematik:iti:xds:EnableDocumentReuse">
4098 <ValueList>
4099   <Value>true</Value>
4100 </ValueList>
4101 </Slot>

```

und wenn

- die Anfrage auch erfolgreich wäre, wenn die Dokumente noch nicht vorhanden wären,
- das bestehende Dokument in derselben Kategorie existiert, in die auch das neue einsortiert würde,
- das bestehende Dokumente sichtbar ist für das einstellende System,
- das Einstellen einer etwaigen Anhangsbeziehung nicht die Anforderungen an Anhänge verletzt (etwa durch Überschreiten der maximalen Länge von Anhangsketten durch das Hinzufügen des Dokuments als Anhang oder Hauptdokument).

Wird der SubmissionRequest gemäß der obigen Bedingungen akzeptiert, MUSS der XDS Document Service

- Anhangsbeziehungen, die noch nicht in den Metadaten des bestehenden Dokuments vorhanden sind, dort und in der Gegenreferenz im referenzierten Dokument nachtragen (bestehende Anhangsbeziehungen werden davon nicht berührt),
- das Dokument und den DocumentEntry aus der Anfrage verwerfen und stattdessen das bestehende Dokument weiter verwenden (ohne die Metadaten des bestehenden Dokuments zu verändern),
- den dazugehörigen einzustellenden DocumentEntry und die Association, die ihn mit dem mitgelieferten SubmissionSet verbindet, aus dem mitgelieferten SubmissionSet entfernen,
- das SubmissionSet selbst verwerfen, sofern keine Associations, DocumentEntries oder Folders neu gespeichert werden (es also im Endeffekt "leer" wäre),
- die Antwort (mit dem üblichen Status "Success") in der<RegistryResponse> um folgende <ResponseSlotList> ergänzen (mit einem Slot für jedes vorhandene Dokument):

```

4131 <ResponseSlotList>
4132 <Slotname="urn:gematik:iti:xds:ReusedDocumentMapping">
4133 <ValueList>
4134   <Value>$uniqueId_neu|$uniqueId_alt</Value>
4135 </ValueList>
4136 </Slot>
4137 </ResponseSlotList>

```

wobei \$uniqueId_neu die DocumentEntry.uniqueId des Dokuments aus dem SubmissionRequest ist, während \$uniqueId_alt die DocumentEntry.uniqueId des bestehenden Dokuments darstellt.

Wird das Dokument nicht akzeptiert, MUSS der XDS Document Service

- mit dem Fehler `XDSRegistryMetadataError` antworten, wenn die Kategorie des neuen Dokuments abweicht,
- mit dem Fehler `XDSInvalidRequest` antworten, wenn der Parameter `"EnableDocumentReuse"` mit einem anderen Wert als `"true"` verwendet wird,
- ansonsten mit dem üblichen Fehler antworten, der auch sonst beim Einstellen der Anfrage (d.h. ohne `EnableDocumentReuse`) zurückgegeben würde.

[<=]

Hintergrund ist, dass die Information, dass es sich um eine Dublette handelt, für das einstellende System hilfreicher und spezifischer ist als ein Metadatenfehler, dass bspw. die angelieferte `uniqueId` "falsch" ist.

A_24990 -XDS Document Service - Dublettenprüfung für dynamische Ordner

Der XDS Document Service MUSS beim Anlegen dynamischer Folder prüfen, ob ein Ordner bereits existiert, der gemäß vom Titel her identisch ist mit demjenigen, den der Client einzustellen versucht. Im Falle eines identischen Titels MUSS der Einstellversuch mit dem Fehlercode `XDSDuplicateFolder` abgelehnt werden. [<=]

A_14937 -XDS Document Service – Dokumentengröße prüfen

Der XDS Document Service MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das `SubmissionSet` verarbeitet wird. Der XDS Document Service MUSS die Verarbeitung ablehnen und mit einem `MaxDocSizeExceeded-` bzw. `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren, wenn die Gesamtgröße aller übermittelten Dokumente 250 MByte übersteigt oder die Größe mindestens eines einzelnen Dokuments 25 MByte übersteigt.

[<=]

Das bedeutet, dass Dokumente bis zu einer Größe von 25 MB = $25 * (1024)^2$ Byte in die ePA hochgeladen werden. Grundlage für die Berechnung der Dokumentengröße ist das Dokument ohne Transportcodierung. Größere Dokumente können nicht hochgeladen werden.

A_23098-01 -XDS Document Service – Keine Registrierung bei zeitlicher Ungültigkeit von strukturierten Dokumenten

Der XDS Document Service MUSS beim Einstellen eines strukturierten Dokuments sicherstellen, dass die Vorgaben gemäß [gemSpec_IG_ePA] hinsichtlich der zeitlichen Gültigkeit erfüllt werden und andernfalls das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `XDSRepositoryMetadataError`-Elements der Text „Version of submitted structured document is not supported“ zurückgegeben werden. [<=]

A_21610-03 -Sonderfälle Anlegen von Foldern durch Clientsysteme

Der XDS Document Service MUSS sicherstellen, dass ausschließlich dynamische Ordner vom Typ "Schwangerschaft und Geburt" (`Folder.Code = pregnancy_childbirth`) durch Clients angelegt werden können. [<=]

A_24797-04 -XDS Document Service - Ablehnung Upload bei veränderten Metadaten bei einer RPLC Assoziation

Der XDS Document Service MUSS Uploads, die als Resultat ein zum Vorgängerdokument verändertes Metadatum enthalten, mit einem `XDSRegistryMetadataError` ablehnen. Einzige Ausnahmen sind:

- Metadatenattribute `creationTime`, `entryUUID` sowie `uniqueId` und `confidentialityCode = "CON"` (`codeSystem = urn:oid:1.2.276.0.76.5.491`).

- Das Metadatenattribut DocumentEntry.referenceIdList DARF ohne die rootDocumentUniqueId gesendet werden; in dem Fall wird die rootDocumentUniqueId automatisch vom XDS Document Service gesetzt (Wert identisch zu dem des ersetzten Dokuments).

[<=]

A_27760-01 -XDS Document Service - Ablehnen von RPLC-Ersetzungen bei nicht erlaubten Dokumententypen

Der XDS Document Service MUSS das Ersetzen von Dokumenten via RPLC-Associations mit dem Fehlercode `XDSReplacementForbidden` ablehnen, wenn das zu ersetzende Dokument nicht einen der folgenden DocumentEntry.formatCode-Werte besitzt:

Dokument	codeSystem	code
eMP	1.3.6.1.4.1.19376.3.2 76.1.5.6	urn:gematik:ig:Medikationsplan:r3.1
NFD	1.3.6.1.4.1.19376.3.2 76.1.5.6	urn:gematik:ig:Notfalldatensatz:r3.1
DPE	1.3.6.1.4.1.19376.3.2 76.1.5.6	urn:gematik:ig:DatensatzPersoenlicheErkl aerungen:r3.1
DiGA	1.3.6.1.4.1.19376.3.2 76.1.5.6	urn:gematik:ig:diga:v1.1
<u>Notizen</u> <u>Kinderuntersuchun</u> <u>gsheft</u>	<u>1.3.6.1.4.1.19376.3.2</u> <u>76.1.5.6</u>	<u>urn:gematik:ig:KinderuntersuchungsheftN</u> <u>otizen:v1.0.1</u>

oder das zu ersetzende Dokument nicht in einen der folgenden Ordner einsortiert ist:

Ordner-Kategorie	Folder.entryUUID
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31

[<=]

Seit ePA 3.1.2 ist das Ersetzen von Dokumenten via RPLC-Associations nur noch für die oben aufgeführten Dokumententypen bzw. -kategorien erlaubt. Der Versuch, andere Dokumententypen zu ersetzen, führt zu einem Fehler. Es kann Altdaten geben, die diese Regel noch missachten. Neue Ersetzung für diese Altdaten werden jedoch gleichermaßen fehlschlagen; d.h. neue Ersetzungen sind nur noch für die oben angegebenen Dokumententypen erlaubt.

A_27761 -XDS Document Service - Potentielle Dokumententypen (Elterndokumente) für Anhänge

Der XDS Document Service MUSS das Anhängen von Dokumenten mit dem Fehlercode `XDSAttachmentForbidden` ablehnen, wenn das Dokument, an das angehängt wird, nicht die folgende Metadatenbelegung besitzt:

IHE-Metadaten	eventCodeList-Eintrag (KDL-Code)		
	Dokumente ntyp (informativ)	Code System	Code
	eventCodeList muss einen der folgenden Codes enthalten:		
classCode="BRI" UND typeCode="BERI" (beide Codes müssen angegeben sein)			
		KH-Entlassbrief	1.2.276.0.76.5.552 ED110 112
	eArztbrief	1.2.276.0.76.5.552	ED110 104
	Anderer Arztbrief	1.2.276.0.76.5.552	AD010 1*

[<=]

Hinweis 1: AD0101 bezeichnet Codes die mit den Zeichen "AD0101" beginnen, z. B. "AD010112" für den "Kurzarztbrief". Der Code "AD0101" als Level 2-Code in KDL ist selbst nicht Teil des Value Sets für eventCodeList, das nur die konkreteren Level 3 Codes enthält.

Hinweis 2: Die Anforderung schließt sowohl das Einstellen von Anhängen über die Operation Provide and Register Document Set-b [ITI-41] als auch Restricted Update Document Set [ITI-92] mit ein.

Hinweis 3: Die Dokumente, die als Anhang angehängt werden dürfen, werden über A_27763 (RPLC-fähige Dokumente) und A_27764 (Sammlungen) eingeschränkt.

A_27764 -XDS Document Service - Keine Anhangsbeziehungen mit Sammlungsdocumententypen

Der XDS Document Service MUSS das Etablieren von Anhangsbeziehungen zu allen Dokumententypen, die in Sammlungen (mixed oder uniform) organisiert werden, unterbinden und mit dem Fehler `XDSAttachmentForbidden` ablehnen.

[<=]

Dokumententypen, die zu Sammlungen gehören, dürfen also weder als Anhang an ein Dokument gehängt werden noch selbst über Anhänge verfügen.

A_27763-01 -XDS Document Service - Keine Anhangsbeziehungen mit RPLC-fähigen Dokumententypen

Der XDS Document Service MUSS das Etablieren von Anhangsbeziehungen zu allen Dokumententypen, die in RPLC-Ketten verwendet werden dürfen (siehe A_27760) oder

4238 die bereits aufgrund der Migration von Altdaten (siehe A_27661) in RPLC-Beziehungen
4239 stehen, unterbinden und mit dem Fehler `XDSAttachmentForbidden` ablehnen.

4240 [`<=`]

4241 Das heißt, dass RPLC-fähige Dokumente (egal, ob sie bereits Teil einer RPLC-Kette sind
4242 oder nicht) nicht Teil einer Anhangskette sein dürfen, also weder als Anhang genutzt
4243 werden dürfen, noch als Dokument an das selbst angehängt wird. Das trägt der aktuellen
4244 Einschränkung Rechnung, dass alle RPLC-Dokumente in einer RPLC-Kette immer
4245 "identische" Metadaten besitzen und deshalb Anhänge (die über die Metadaten abgebildet
4246 werden) automatisch bei einer Ersetzung "mitvererbt" würden. Da dies fachlich potentiell
4247 zu Problemen führen kann, wird es auf diese Weise unmöglich gemacht, dass Dokumente
4248 gleichzeitig in einer RPLC- als auch in einer Anhangskette sein können.

4249 Da diese Regelung in ePA 3.1.2 eingeführt wurde, können Altdaten noch über Anhänge
4250 verfügen, siehe auch Abschnitt zur [automatischen Datenanpassung](#).

4251 Details zur grundsätzlichen Funktionsweise von Dokumentenanhängen finden sich
4252 in [diesem Abschnitt](#).

4253 **A_24531-04 -Constraint Management - Verbergen von Dokumenten durch** 4254 **confidentialityCode**

4255 Falls das Dokument, welches mit `confidentialityCode = "CON"` (`codeSystem =`
4256 `urn:oid:1.2.276.0.76.5.491`) durch eine Nutzergruppe der
4257 Rolle `oid_versichertereingestellt` wird, nicht Bestandteil einer Sammlung, also eines
4258 Ordners der Ausprägung "mixed" oder "uniform" ist, und kein Dokument der Kategorie
4259 "emp" ist, dann MUSS der XDS Document Service sicherstellen, dass das Dokument
4260 durch einen Eintrag in der General Deny Policy verborgen wird. Es MUSS ein Eintrag mit
4261 `denyType = "document"` für die General Deny Policy erzeugt werden. [`<=`]

4262 **A_25856-02 -XDS Document Service - Fehlerhaftes Verbergen von Dokumenten** 4263 **durch confidentialityCode**

4264 Falls das Dokument, welches mit `confidentialityCode = "CON"` (`codeSystem =`
4265 `urn:oid:1.2.276.0.76.5.491`) nicht durch eine Nutzergruppe der
4266 Rolle `oid_versichertereingestellt` wird, oder Bestandteil einer Sammlung, also eines
4267 Ordners der Ausprägung "mixed" oder "uniform" ist, dann MUSS der XDS Document
4268 Service die Operation abbrechen und mit einem Fehlercode `ConstraintViolation`
4269 beenden. [`<=`]

4270 Das Verbergen von Dokumenten ist in Kapitel 3.13.1.10- Verbergen von Dokumenten
4271 durch Verwendung des confidentialityCode beschrieben.

4272 3.13.1.4.3.1.1 Dokumentenanhänge

4273 Für die Verwaltung von Anhängen wird ein Mechanismus basierend auf
4274 `DocumentEntry.referenceIdList` verwendet. Zwei Dokumente werden verknüpft, indem in
4275 beiden dazugehörigen `DocumentEntry`s das jeweils andere Dokument als
4276 "Elterndokument" bzw. "Kinddokument" (=Anhang) eingetragen wird. Dies geschieht
4277 über die Auszeichnung der Referenzen mit den qualifizierenden
4278 Codes `urn:gematik:iti:xds:2025:childDocument` (Verweis auf ein Kinddokument) und
4279 `urn:gematik:iti:xds:2025:parentDocument` (Verweis auf ein Elterndokument).

4280 Ein Verweis auf ein Elternformat hat also das Format ~~`<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2025:parentDocument`~~
4281 `<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2025:parentDocument`

4282 Dabei muss das Dokument, auf das per Kind- oder Elternreferenz verwiesen wird,
4283 zusammen mit oder nach dem referenzierten Dokument eingestellt werden. Wenn z. B.
4284 das Elterndokument bereits im Aktensystem gespeichert ist und ein Kinddokument
4285 (Anhang) dazu hochgeladen wird, muss der `DocumentEntry` des Kinddokuments das
4286 Elterndokument in der `referenceIdList` referenzieren. Die Markierung des

4287 Elterndokuments (mit dem Verweis auf das Kinddokument) wird dann vom Aktensystem
4288 automatisch vorgenommen. Damit wird vermieden, dass zwei Aufrufe notwendig sind
4289 (Einstellen gefolgt vom Aktualisieren der Metadaten), was zu inkonsistenten Zuständen
4290 im Aktensystem führen kann. Werden Eltern- und Kinddokument gemeinsam eingestellt,
4291 ist der Verweis auf mindestens entweder Elterndokument oder Kinddokument
4292 verpflichtend, da die jeweils andere Seite automatisch vom Aktensystem ergänzt werden
4293 kann.

4294 Die Tiefe von Anhangsketten ist auf fünf Dokumente (inklusive dem obersten
4295 Elterndokument) begrenzt. Darüberhinaus ist die Verwendung von Anhängen nur für
4296 ausgewählte Dokumententypen erlaubt und kann dann jeweils weiteren Beschränkungen
4297 unterliegen.

4298 Neben dem Anhängen während des Einstellens ist es auch möglich, über ein
4299 Metadatenupdate nachträglich zwei Dokumente miteinander über eine Anhangsbeziehung
4300 zu verbinden.

4301 Anhänge, technisch umgesetzt über `DocumentEntry.referenceIdList`, sind zu
4302 unterscheiden von RPLC (Replace/Ersetzungs)-Ketten, die über RPLC-Associations
4303 abgebildet werden. Ersetzte Dokumente stellen verschiedene Dokumentenversionen dar,
4304 während Anhänge in der Regel eine Ergänzung des Dokuments darstellen, an dem sie
4305 anhängen. Um die beiden Konzepte nicht zu vermischen (aktuell würden alle per RPLC-
4306 Associations verbundene Dokumente zwangsläufig aufgrund identischer Metadaten
4307 immer dieselben Anhänge besitzen), wird verboten, ein Dokument gleichzeitig in eine
4308 Ersetzungskette als auch in eine Anhangskette zu hängen. Dies geschieht über eine
4309 Beschränkung des RPLC-Mechanismus auf wenige ausgewählte Dokumententypen und
4310 der gezielten Verwendung von Anhängen für andere Dokumententypen.

4311 Die letzte Einschränkung bedeutet auch, dass Anhänge nicht an beliebige Dokumente
4312 gehängt werden können. Ziel ist es, Anhänge nur in fachlich kontrollierter Form in der
4313 ePA zu verwenden und auf diese Weise die Datenqualität zu erhöhen.

4314 Anhangsbeziehungen können gelöscht werden, in dem der entsprechende Verweis auf ein
4315 Anhangsdokument aus der `referenceIdList` (via `Restricted Update Document Set`) entfernt
4316 wird.

4317 Es kann direkt an einem `DocumentEntry` erkannt werden, ob ein Dokument
4318 Anhangsbeziehungen zu anderen Dokumenten unterhält oder nicht. Um möglichst einfach
4319 (rekursiv) alle mit einem bestimmten Dokument verbundenen Dokumente zu finden,
4320 existiert eine spezielle Suche (siehe A_27655), die alle entsprechenden `DocumentEntries`
4321 zurückliefert. Bei dieser und anderen Suchen werden Eltern- oder Kinddokumente zu
4322 einem zurückgegebenen `DocumentEntry`, die *nicht* für den Anfragenden sichtbar sind (z.
4323 B. aufgrund der Legal Policy oder da sie durch den Versicherten verborgen wurden), vom
4324 Aktensystem automatisch aus dem returnierten `DocumentEntry` bzw. dessen
4325 `referenceIdList` entfernt.

4326 **Berechtigungen für Anhangsoperationen**

4327 Es gelten die Regelungen der Legal Policy für die zur Anhangsverwaltung notwendigen
4328 Operationen:

- 4329 • **Lesen:** Um die Anhangsbeziehung zwischen beiden Dokumenten zu erkennen,
4330 müssen beide Dokumente für den Anfragenden lesbar (Berechtigung "R" für
4331 "Read") sein, ansonsten blendet das Aktensystem die Anhangsbeziehung in
4332 zurückgelieferten `DocumentEntries` aus. Auch wenn das referenzierte Dokumente
4333 verborgen ist, wird die Anhangsbeziehung nicht angezeigt.
- 4334 • **Einstellen:** Um Dokumente neu einzustellen und sie als Eltern- oder
4335 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 vor dem Anfragenden 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. Beim Löschen beider Dokument im selben Aufruf ist die "D"-Berechtigung für das referenzierte Dokument ausreichend, d.h. die "U"-Berechtigung ist für dieses Dokument dann nicht mehr notwendig.

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

- 4384 Elternketten (Kindkette) ist und ansonsten die Verarbeitung mit dem Fehler
4385 `XDSInvalidAttachmentHierarchy` abbrechen.
- 4386 4. Im referenzierten Dokument die `DocumentEntry.uniqueId` des einzustellenden
4387 Dokuments in die `referenceIdList` mit Identifier
4388 `Codeurn:gematik:iti:xds:2025:childDocument`
4389 `(urn:gematik:iti:xds:2025:parentDocument)` eintragen, wenn dies nicht bereits
4390 geschehen ist.
- 4391 [`<=`]
- 4392 Hinweis 1: Ein Verweiszirkel kann entstehen, wenn ein Kinddokument direkt oder indirekt
4393 (d.h. ggf. über eine Kette von Kinddokumenten hinweg) gegenüber seinem
4394 Elterndokument gleichzeitig auch selbst als Elterndokument auftritt.
- 4395 Hinweis 2: Der Fehler `XDSInvalidAttachmentHierarchy` spiegelt die Situation wider,
4396 dass in einer Kette von Anhängen (wie 1<-2<-3) versucht wird, ein Kind (3) zusätzlich
4397 als Kind eines Vorfahren seines Elterndokuments (1) einzuführen.
- 4398 Hinweis 3: Punkt 4 stellt sicher, dass das referenzierte Dokument passend markiert wird,
4399 egal ob es in der Anfrage enthalten ist oder bereits im Aktensystem hinterlegt ist.
- 4400 Siehe auch [entsprechende Illustrationen im Anhang](#).
- 4401 3.13.1.4.3.2 Registry Stored Query [ITI-18]
4402 **A_14913 -XDS Document Service – Ablauflogik für Registry Stored Query**
4403 Der XDS Document Service MUSS die Umsetzung der Operation `RegistryStoredQuery`
4404 gemäß der definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3]
4405 implementieren. [`<=`]
- 4406 **A_24761 -XDS Document Service – Ermitteln verknüpfter Approved Documents**
4407 **für Registry Stored Query**
4408 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp
4409 `"GetRelatedApprovedDocuments"` mit der Query-ID `"urn:uuid:1c1f1cea-ad3a-11ed-afa1-`
4410 `0242ac120002"` mit denselben Parameternutzungsvorgaben der Registry Stored Query
4411 `„GetDocuments"` gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.5] mit der Multiplizität 1
4412 unterstützen. Das resultierende `DocumentEntry` Objekt MUSS
- 4413 • mit dem Ergebnis von `GetDocuments` übereinstimmen, falls dieses sich im
4414 Zustand `approved` befindet;
 - 4415 • andernfalls über `Associations` ermittelt werden. Dabei wird jeweils ausgehend von
4416 der übergebenen `DocumentEntry.EntryUUID` oder `DocumentEntry.UniqueId` über
4417 die `Replace-Associations` dasjenige `DocumentEntry` Objekt ermittelt, das sich im
4418 Zustand `approved` befindet.
- 4419 Das `wsa:Action-Element` MUSS den Wert `"urn:ihe:iti:2007:RegistryStoredQuery"`
4420 besitzen.
4421 [`<=`]
- 4422 **A_24762 -XDS Document Service – Suchanfragen über das Metadatenattribut**
4423 **`DocumentEntry.title`**
4424 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp `"FindDocumentsByTitle"`
4425 mit der Query-ID `"urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405"` und denselben
4426 Parameternutzungsvorgaben der Registry Stored Query `"FindDocuments"` gemäß [IHE-
4427 ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter
4428 `$XDSDocumentEntryTitle` unterstützen, sodass eine Suchergebnismenge über das
4429 Attribut `XDSDocumentEntry.title` eingeschränkt werden kann. Weiterhin MUSS dieselbe
4430 Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den

4431 Parameter \$XDSDocumentEntryAuthorPerson. Das_{wsa:Action}-Element MUSS den Wert
4432 "urn:ihe:iti:2007:RegistryStoredQuery" besitzen.[<=]

4433 **A_25183 -XDS Document Service – Suchanfragen über das Metadatenattribut**
4434 **DocumentEntry.comment**

4435 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp
4436 "FindDocumentsByComment" mit der Query-ID "urn:uuid:2609dda5-2b97-44d5-a795-
4437 3e999c24ca99" und denselben Parameternutzungsvorgaben der Registry Stored Query
4438 "FindDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren
4439 verpflichtenden Suchparameter \$XDSDocumentEntryComment unterstützen, sodass eine
4440 Suchergebnismenge über das Attribut XDSDocumentEntry.comment eingeschränkt
4441 werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert
4442 sein, wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson.
4443 Das_{wsa:Action}-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery"
4444 besitzen.[<=]

4445 **A_24763 -XDS Document Service – Suche über Author Institution bei Registry**
4446 **Stored Query**

4447 Der XDS Document Service MUSS für den Anfragetyp "FindDocumentsByTitle" den
4448 weiteren optionalen Parameter \$XDSDocumentEntryAuthorInstitution verarbeiten
4449 können, sodass eine Suchergebnismenge über den authorInstitution-Slot der
4450 XDSDocumentEntry.author-Classification (Wertemenge des authorInstitution-Sub-
4451 Attributs) eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels
4452 Platzhalter implementiert sein, wie für Suchanfragen über den Parameter
4453 \$XDSDocumentEntryAuthorPerson.[<=]

4454 **A_24764 -XDS Document Service – Rückgabe unscharfer Suchergebnisse für**
4455 **Registry Stored Query**

4456 Der XDS Document Service MUSS bei der Ermittlung der Ergebnisse einer Registry
4457 Stored Query bei Auswertung der folgenden Queries und deren Suchparametern beim
4458 Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d. h. bezogen auf das
4459 jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht
4460 abweichende Ergebnisse zurück liefern können:

- 4461 • Query "FindDocuments" und Query "FindDocumentsByTitle" und Query
4462 "FindDocumentsByComment"
- 4463 • \$XDSDocumentEntryTitle
- 4464 • \$XDSDocumentEntryAuthorInstitution
- 4465 • \$XDSDocumentEntryAuthorPerson
- 4466 • \$XDSDocumentEntry.comment
- 4467 • Query "FindSubmissionSets"
- 4468 • \$XDSSubmissionSetAuthorPerson

4469 Dabei MUSS der XDS Document Service mindestens unscharfe Ergebnisse bezüglich
4470 Groß/Kleinschreibung unterstützen, also Groß/Kleinschreibung für die angegebenen
4471 Parameter der ausgewählten Query-Typen ignorieren.
4472 [<=]

4473 Das zur Ermittlung weiterer unscharfer Ergebnisse vom XDS Document Service
4474 einzusetzende Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu
4475 liefern, die ihm möglicherweise sonst wegen beispielsweise falscher Schreibweise eines
4476 Namens (z. B. "Meyer" vs. "Maier") vorenthalten worden wäre. Dabei sind Verfahren wie
4477 die Kölner Phonetik aber auch andere Mechanismen denkbar.

A_27655 -XDS Document Service – Suche nach Anhangsketten

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "GetDocumentAppendices" mit der Query-ID "urn:uuid:2a6b3197-8ea8-4245-a6de-daf71b469116" und denselben Parameternutzungsvorgaben der Registry Stored Query "GetDocumentsAndAssociations" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.8] unterstützen. Die Suchergebnismenge muss für jedes über \$XDSDocumentEntryEntryUUID oder \$XDSDocumentEntryUniqueId referenzierte Dokument die Ergebnismenge wie folgt ermitteln:

1. Start: Alle DocumentEntrys der Ergebnismenge hinzufügen, welche auf die uniqueId des Dokuments aus dem Eingangsparameter in der DocumentEntry.referenceIdList verweisen (ausgezeichnet als urn:gematik:iti:xds:2025:childDocument oder urn:gematik:iti:xds:2025:parentDocument) und sichtbar sind.
2. Kindkette: Für jeden im vorher durchgeführten Schritt identifizierten DocumentEntry D, der über den Eintrag urn:gematik:iti:xds:2025:childDocument identifiziert wurde, alle DocumentEntries der Ergebnismenge hinzufügen, welche die uniqueId von D wiederum als urn:gematik:iti:xds:2025:childDocument in der referenceIdList enthalten und sichtbar sind. Wenn ein DocumentEntry nicht sichtbar ist, wird dieser Teil der Kette nicht weiter verfolgt.
3. Elternkette: Für jeden im vorher durchgeführten Schritt identifizierten DocumentEntry E, der über den Eintrag urn:gematik:iti:xds:2025:parentDocument identifiziert wurde, alle DocumentEntries der Ergebnismenge hinzufügen, welche die uniqueId von E wiederum als urn:gematik:iti:xds:2025:parentDocument in der referenceIdList enthalten und sichtbar sind. Wenn ein DocumentEntry nicht sichtbar ist, wird dieser Teil der Kette nicht weiter verfolgt.
4. Rekursion: Schritte 2 und 3 jeweils wiederholen, bis keine weiteren DocumentEntries mehr gefunden werden können.

[<=]

Hinweis 1: "Sichtbar" im Kontext von Anhängen bedeutet hier, dass die Existenz eines Dokuments nicht durch fehlende Legal Policy-Berechtigung (Recht "R" ist notwendig), Verbergen durch den Versicherten, Zugriffsverbot für die zugreifenden Organisation über ("User Specific Deny Policy") oder gar Widerspruch ("Consent Decision") vor dem Zugreifenden versteckt werden muss.

Hinweis 2: Wenn als Eingabe eine entryUUID gegeben wird, muss der XDS Document Service die dazugehörige uniqueID ggf. intern selbst ermitteln. Zur Sichtbarkeit von Anhängen siehe Hinweis unter A_27655.

Die Suche ermittelt also alle Dokumente, die über Anhangsketten mit dem gegebenen Dokument verbunden sind.

A_27762 -XDS Document Service - Ausblenden nicht sichtbarer Anhänge

Der XDS Document Service MUSS bei der Rückgabe eines DocumentEntries D im Rahmen einer Stored Query [ITI-18] jedes durch Anhangsbeziehungen in der DocumentEntry.referenceIdList (urn:gematik:iti:xds:2025:childDocument oder urn:gematik:iti:xds:2025:parentDocument) mit D verbundene Dokument E dahingehend prüfen, ob es für den Anfragenden sichtbar ist und wenn nicht, den entsprechenden Eintrag für E vor der Herausgabe an den Anfragenden aus der referenceIdList entfernen.

[<=]

4527 3.13.1.4.3.3 Remove Metadata [ITI-62]

4528 **A_14908-02 -XDS Document Service – Ablauflogik für Remove Metadata**

4529 Der XDS Document Service MUSS die Umsetzung der Operation RemoveMetadata gemäß
4530 der definierten Ablauflogik in [IHE-ITI-RMD#3.62.4.1.2 und 3.62.4.1.3]
4531 implementieren.[<=]

4532 **A_20701 -XDS Document Service – Unwiderrufliches Löschen bei Remove**
4533 **Metadata**

4534 Der XDS Document Service MUSS sicherstellen, dass einmal gelöschte Dokumente und
4535 Metadatenobjekte nicht wiederhergestellt werden können.[<=]

4536 **A_21715 -XDS Document Service – Kein Löschen von "replaced"-Dokumenten**
4537 **im Status "Deprecated"**

4538 Der XDS Document Service MUSS sicherstellen, dass keine Löschanfrage eines ePA-Client
4539 auf Dokumenten mit dem availabilityStatus = Deprecated ausgeführt werden darf.[<=]

4540 **A_21714-03 -XDS Document Service – Löschen von strukturierten Dokumenten**
4541 **durch ein ePA-FdV**

4542 Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein
4543 ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete
4544 Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert
4545 aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie
4546 zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die
4547 Nachricht mit demXDSRegistryError-Fehlercode zurückgeben werden.Es MUSS im
4548 codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert
4549 "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt
4550 werden.[<=]

4551 **A_21817-02 -XDS Document Service – Löschen von strukturierten Dokumenten**
4552 **durch ein Primärsystem**

4553 Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein
4554 Primärsystem ablehnen, wenn zugehörige Submission Sets, Associations oder
4555 zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners
4556 impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets,
4557 Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben
4558 vor, MUSS die Nachricht mitXDSRegistryError-Fehlercode zurückgeben werden. Es MUSS
4559 im codeContext-Attribut des zurückgegebenenrs:RegistryError-Elements der Wert
4560 "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt
4561 werden.[<=]

4562 **A_24663-01 -XDS Document Service – Bereinigung der General Deny Policy**

4563 Der XDS Document Service MUSS als Folge von erfolgreichen Löschanfragen alle Einträge
4564 der General Deny Policy entfernen, welche die betroffenen Dokumente oder dynamischen
4565 Ordner referenzieren.[<=]

4566 **A_24765 -XDS Document Service – Kein Löschen von statischen Ordnern und**
4567 **Associations**

4568 Der XDS Document Service MUSS sicherstellen, dass eine Löschanfrage keine statischen
4569 Ordner und Assoziationen löschen darf. Dies gilt nicht für dynamische Ordner. Der XDS
4570 Document Service MUSS bei Löschung eines Dokumentes die Assoziation zum Folder
4571 löschen.[<=]

4572 Dynamische Ordner sind beispielsweise Mutterpass (folderCode = pregnancy_childbirth)
4573 oder DiGA (folderCode = diga).

4574 **A_20579-01 -XDS Document Service – Löschen von Ordnern**

4575 Der XDS Document Service MUSS Requests, die darauf abzielen, einen statischen Folder
4576 direkt zu löschen, mit einem XDSRegistryMetadataError ablehnen.[<=]

A_27656-01 -XDS Document Service – Löschen von Anhangsreferenzen beim Löschen von Dokumenten

Der XDS Document Service MUSS beim Löschen eines Dokuments D, das in der `DocumentEntry.referenceIdList` ein Dokument E via

`urn:gematik:iti:xds:2025:childDocument` oder

`urn:gematik:iti:xds:2025:parentDocument` referenziert,

- für jedes Dokument E, das nicht ebenfalls gelöscht werden soll, prüfen, ob E für den Anfragenden sichtbar ist:
- Wenn ja, für Dokument E prüfen, ob E für den Anfragenden gemäß Legal Policy das "U"-Recht besitzt, und ansonsten die Verarbeitung mit dem Fehler `XDSCannotUnlinkAttachment` abbrechen und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements als Text die `DocumentEntry.uniqueId` des referenzierten Dokuments angeben;
- Wenn nein, die Verarbeitung mit dem Fehler `XDSCannotUnlinkAttachment` abbrechen ohne die `DocumentEntry.uniqueId` des referenzierten Dokuments E preiszugeben.
- im Dokument E, das nicht ebenfalls gelöscht werden soll, die dazu passende rückwärtige Referenz auf D aus E's `referenceIdList` entfernen.

[<=]

Die Anforderung stellt sicher, dass keine "toten" Eltern- und Kindreferenzen im XDS Document Service verbleiben.

Hinweis: Zum Begriff "sichtbar" siehe analogen Hinweis unter A_27655.

Hinweis 2: Ein Dokument kann also nicht gelöscht werden, wenn etwaige Anhangsreferenzen ("Backlinks") in den referenzierten Dokumenten nicht gelöscht werden können.

3.13.1.4.3.4 RetrieveDocumentSet [ITI-43]

A_14914 -XDS Document Service – Ablauflogik für Retrieve Document Set

Der XDS Document Service MUSS die Umsetzung der Operation `RetrieveDocumentSet` gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3] und [IHE-ITI-TF2b#3.43.4.2.2 und 3.43.4.2.3] implementieren. [**<=**]

A_16201 -XDS Document Service – Prüfung der zurückgegebenen Paketgröße

Der XDS Document Service MUSS anhand der übergebenen `DocumentUniqueIDs` die Gesamtgröße ermitteln und bei Überschreitung von 250 MByte die Verarbeitung ablehnen und die Nachricht mit einem `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. [**<=**]

3.13.1.4.3.5 Restricted Update Document Set [ITI-92]

A_15061-08 -XDS Document Service – Ablauflogik für Restricted Update Document Set

Der XDS Document Service MUSS die Umsetzung der Operation `RestrictedUpdateDocumentSet` gemäß der definierten Ablauflogik in [IHE-ITI-RMU#3.92.4.1.2 und 3.92.4.1.3] implementieren und sicherstellen, dass (nur) die folgenden Metadatenobjekte gesendet werden:

- ein neues `SubmissionSet`,
- einen `DocumentEntry` inklusive der `entryUUID` des zu ändernden `DocumentEntry`-Objekts. Das übermittelte `DocumentEntry`-Objekt kann sowohl alle vollständigen Metadatenattribute als auch nur zu ändernde Metadatenattribute enthalten. In

- 4623 jedem Fall dürfen Änderungen ausschließlich gemäß A_15083-* angenommen und
4624 durchgeführt werden.
- 4625 • für das Hinzufügen, Ändern oder Löschen eines einzelnen oder mehrerer Werte
4626 in `DocumentEntry.author`, `DocumentEntry.confidentialityCode`,
4627 `DocumentEntry.eventCodeList` und `DocumentEntry.referenceIdList` gilt darüber
4628 hinaus:
- 4629 • es MÜSSEN alle und nicht nur die zu ändernden Werte (z. B. Autoren) über
4630 ihre jeweiligen `<classification classificationScheme="urn:uuid:...>-XML-`
4631 Elemente im gewünschten Soll-Zustand gesendet werden.
- 4632 • das Löschen aller Werte (z. B. Autoren) MUSS durch Übertragung ein
4633 einzelnen, komplett leeren `<classification="urn:uuid:...>-XML-Elements`
4634 signalisiert werden.
- 4635 • eine SS-DE HasMember-Association, die das `SubmissionSet` mit dem geschickten
4636 `DocumentEntry` verbindet.
- 4637 • die „lid“ (`logicalID`) DARF NICHT gesendet werden.
- 4638 • der Slot "`PreviousVersion`" MUSS immer mit dem Wert "1" gesendet werden.
- 4639 • der Slot „`AssociationPropagation`“ MUSS auf „no“ gesetzt werden. Zusätzlich
4640 MUSS der alternative Slot-Name "`associationPropagation`" akzeptiert werden.
- 4641 Der XDS Document Service DARF die gesendete `Association` und das neue
4642 `SubmissionSet` NICHT dauerhaft speichern. [`<=`]
- 4643 Der alternative Slot-Name "`associationPropagation`" wird unterstützt, da alte Versionen von
4644 ePA fälschlicherweise, abweichend von [IHE-ITI-RMU] diesen Wert gefordert haben.
- 4645 **A_15082-02 -XDS Document Service – Validierung der Metadaten aus ITI**
4646 **Document Sharing-Profilen**
- 4647 Der XDS Document Service MUSS die übermittelten `DocumentEntry`-Metadaten der
4648 `OperationRestrictedUpdateDocumentSet` dahingehend prüfen, dass gegenüber den
4649 Bestandsdaten die geänderten Metadaten konform zu den Nutzungsvorgaben
4650 in [A_14760-*] geändert werden. Der XDS Document Service MUSS das Aktualisieren
4651 der Metadatenattribute ablehnen und mit einem `XDSRepositoryMetadataError`
4652 quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. Es MUSS
4653 im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements angegeben
4654 werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht. [`<=`]
- 4655 **A_15083-09 -XDS Document Service – Prüfung auf ausschließliche**
4656 **Aktualisierung der erlaubten Metadaten**
- 4657 Der XDS Document Service MUSS die übermittelten `DocumentEntry`-Metadaten der
4658 `OperationRestrictedUpdateDocumentSet` dahingehend prüfen, dass gegenüber den
4659 Bestandsdaten ausschließlich die folgenden Metadaten geändert werden:
- 4660 • `DocumentEntry.author`
- 4661 • `DocumentEntry.classCode`
- 4662 • `DocumentEntry.comments`
- 4663 • `DocumentEntry.confidentialityCode` (`confidentialityCode` = "CON" (`codeSystem` =
4664 `urn:oid:1.2.276.0.76.5.491`) ist nicht erlaubt)
- 4665 • `DocumentEntry.creationTime`
- 4666 • `DocumentEntry.eventCodeList`

- 4667 • DocumentEntry.formatCode
- 4668 • DocumentEntry.healthcareFacilityTypeCode
- 4669 • DocumentEntry.languageCode
- 4670 • DocumentEntry.legalAuthenticator
- 4671 • DocumentEntry.practiceSettingCode
- 4672 • DocumentEntry.referenceIdList
- 4673 • DocumentEntry.serviceStartTime
- 4674 • DocumentEntry.serviceStopTime
- 4675 • DocumentEntry.title
- 4676 • DocumentEntry.typeCode
- 4677 • DocumentEntry.URI

4678 Wenn das Metadatum DocumentEntry.referenceIdList ohne rootDocumentUniqueId
 4679 gesendet wird, MUSS der XDS Document Service den Wert automatisch setzen (identisch
 4680 zu rootDocumentId in DocumentEntry.referenceIdList des ersetzten Dokuments). Wenn
 4681 die rootDocumentUniqueId gesendet wird, MUSS der XDS Document Service
 4682 sicherstellen, dass der Wert dem ansonsten automatisch gesetzten Wert entspricht.

4683
 4684 Werden unerlaubte Metadatenänderungen geschickt, muss die Operation mit
 4685 einem LocalPolicyRestrictionError-Fehlercode abgebrochen werden. Werden
 4686 Metadatenattribute mit leeren Werten übermittelt, signalisiert dies ein Löschen
 4687 des Metadatums (z.B. DocumentEntry.comments). Es müssen die Kardinalitäten
 4688 in A_14760-* berücksichtigt bzw. dürfen nicht verletzt werden (Ausnahme für Altdaten:
 4689 eventCodeList darf mehr als einen DMP- oder KDL-Code in der eventCodeList enthalten,
 4690 wenn der alte Metadatenatz bereits dieselben DMP- und KDL-Codes führt). Das
 4691 Metadatum DocumentEntry.referenceIdList MUSS dabei mindestens die
 4692 rootDocumentUniqueId enthalten.

4693 Wenn in der Eingangsnachricht keine Aktualisierung für die erlaubten Metadaten
 4694 enthalten ist, ist die Weiterverarbeitung abzubrechen und die Nachricht mit einem
 4695 LocalPolicyRestrictionError-Fehlercode zu quittieren. [<=]

4696 **A_27657-01 -XDS Document Service – Anhänge hinzufügen oder entfernen mit** 4697 **Restricted Update Document Set**

4698 Der XDS Document Service MUSS beim Aktualisieren eines DocumentEntries die
 4699 folgenden Regeln durchsetzen (der Text bezieht sich auf das Einfügen oder Entfernen
 4700 eines parentDocument; die analoge Handlungsanweisung für childDocument ist jeweils in
 4701 Klammern angegeben):

- 4702 • Wenn die DocumentEntry.referenceIdList vor der Aktualisierung auf ein
 4703 überurn:gematik:iti:xds:2025:parentDocument
 4704 (urn:gematik:iti:xds:2025:childDocument) ausgezeichnetes Dokument
 4705 verweist, dieses aber für den Anfragenden nicht sichtbar ist, MUSS der XDS
 4706 Document Service den entsprechenden Eintrag für die weitere Bearbeitung
 4707 automatisch wieder hinzufügen.
- 4708 • Wenn dem Feld DocumentEntry.referenceIdList ein Wert mit der Auszeichnung
 4709 urn:gematik:iti:xds:2025:parentDocument
 4710 (urn:gematik:iti:xds:2025:childDocument) hinzugefügt wird, MUSS der XDS
 4711 Document Service prüfen,

- 4712 • ob das vom Anfragenden dort referenzierte Dokument nicht existent oder für
4713 das anfragende System nicht sichtbar ist und in diesem Fall die Operation mit
4714 dem Fehler `XDSNoSuchParent` (`XDSNoSuchChild`) abbrechen,
- 4715 • ob für beide betroffenen Dokumente die Berechtigung "U" (gemäß Legal
4716 Policy) vorliegt und ansonsten die Verarbeitung mit dem Fehler
4717 `XDSCannotLinkAttachment` abbrechen und im `codeContext`-Attribut
4718 des zurückgegebenen `rs:RegistryError`-Elements als Text die
4719 `DocumentEntry.uniqueId` des referenzierten Dokuments angeben,
- 4720 • ob die Kennzeichnung des Dokuments als Anhang einen Verweiszirkel
4721 verursachen würde und ggf. die Operation mit dem Fehler
4722 `XDSAttachmentCycle` abbrechen;
- 4723 • ob durch das Markieren des Dokuments der zusätzliche Verweis nicht auf ein
4724 Elterndokument (Kinddokument) gemacht wird, das bereits Teil der
4725 Elternketten (Kindkette) ist und ansonsten die Verarbeitung mit dem Fehler
4726 `XDSInvalidAttachmentHierarchy` abbrechen.
- 4727 • Wenn aus dem Feld `DocumentEntry.referenceIdList` ein Wert mit der
4728 Auszeichnung
4729 `urn:gematik:iti:xds:2025:parentDocument(urn:gematik:iti:xds:2025:chil`
4730 `dDocument)` entfernt wird, MUSS der XDS Document Service prüfen,
- 4731 • ob für beide betroffenen Dokumente die Berechtigung "U" (gemäß Legal
4732 Policy) vorliegt und ansonsten die Verarbeitung mit dem
4733 Fehler `XDSCannotUnLinkAttachment` abbrechen und im `codeContext`-Attribut
4734 des zurückgegebenen `rs:RegistryError`-Elements als Text die
4735 `DocumentEntry.uniqueId` des referenzierten Dokuments angeben,
- 4736 • und ansonsten im dort referenzierten Dokument den passenden
4737 `urn:gematik:iti:xds:2025:childDocument(urn:gematik:iti:xds:2025:pa`
4738 `rentDocument)`-Eintrag aus der `referenceIdList` entfernen.

4739 **[<=]**

4740 Das Hinzufügen oder Entfernen von bestehenden Anhängen wird also immer entweder
4741 über den Verweis auf ein Eltern- oder Kinddokument vorgenommen; das referenzierte
4742 Dokument selbst wird immer automatisch angepasst. Wird über RMU die `referenceIdList`
4743 so gesetzt, dass die Eltern- und Kinddokumentausszeichnungen unverändert bleiben, ist
4744 `A_27657` nicht relevant.

4745 Bei einer Kette $A \rightarrow B \rightarrow C \rightarrow D$ und Löschen der mittleren Referenz verbleiben die beiden
4746 unzusammenhängenden Ketten $A \rightarrow B$ und $C \rightarrow D$.

4747 Zum Begriff "sichtbar" siehe analogen Hinweis unter `A_27655`. Die spezielle Behandlung
4748 für nicht sichtbare Dokumente ist notwendig, da eine Dokumentensuche eine solche
4749 Anhangsbeziehung zum verbundenen Dokument gemäß `A_27762` aus der
4750 `DocumentEntry.referenceIdList` entfernt. Eine anschließende Aktualisierung des
4751 Dokuments kann also in aller Regel auch den Verweis auf das nicht sichtbare Eltern- oder
4752 Kinddokument nicht enthalten. Wenn der Anfragende es dennoch mitliefert (aus welcher
4753 Quelle auch immer), gilt wie in der Anforderung beschrieben, dass der gesamte Aufruf
4754 mit dem Fehler `XDSNoSuchParent` bzw. `XDSNoSuchChild` abgelehnt werden muss (nicht
4755 etwa mit `XDSInvalidAttachmentHierarchy`).

4756 Falls das Ändern der Metadaten zur Folge hat, dass ein Dokument in eine andere
4757 Dokumentenkategorie gemäß Legal Policy fällt, wird durch den XDS Document Service
4758 bewertet, ob der Anfragende überhaupt Dokumente in diese Kategorie einstellen darf. In
4759 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. Anhänge besitzen) eingehalten werden. Für das "Neu-Einstellen" in die neue Kategorie benötigt der Anfragende ausschließlich die Berechtigung "C" für das neue Dokument und das gleichzeitige Einhängen einer Referenz. Bei neu-Kategorisierung benötigt der Anfragende die Berechtigung "C" für das Dokument und zusätzlich "U" für die zu übersiedelnden Referenzen.

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_ncpeh` bei jeder Suchanfrage und jeder Retrieve-Operation prüfen, dass der im SOAP-Header der Operation übergebene Zugriffscode identisch ist mit dem im Entitlement Management für diesen Nutzer hinterlegten Zugriffscode und andernfalls die Operation mit dem Fehlercode `AccessCodeViolation` beenden. [`<=`]

A_24509 -XDS Document Service - Prüfung der Legal Policy außer Suchanfragen

Der XDS Document Service MUSS die Ausführung einer Operation mit dem Fehlercode LegalPolicyViolation beenden, wenn für den angemeldeten Nutzer die Regeln der Legal Policy nicht erfüllt sind und es sich nicht um eine Suchanfrage handelt.

Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die Liste der UUIDs (DocumentEntry.entryUUID) der identifizierten Dokumente angegeben werden. [<=]

A_24510-02 -XDS Document Service – Prüfung Herunterladen eines verborgenen oder nicht vorhandenen Dokuments

Der XDS Document Service MUSS die Ausführung der Retrieve-Operation mit dem Fehlercode 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 XDSDocumentMetadataError**

Der XDS Document Service KANN alternativ zum Fehler "XDSDocumentMetadataError" 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_26324-03 -XDS Document Service - Aktenkonto im Umzug oder im Wartungsmodus

~~**A_26324-01 -XDS Document Service – Aktenkonto im Umzug**~~ Falls sich ein Aktenkonto im Zustand SUSPENDED oder im Status MAINTENANCE befindet MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem StatusMismatch-

Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements den passenden Fehlertext angeben:

<u>Aktenkontostatus</u>	<u>Wert für <code>codeContext</code> in <code>rs:RegistryError</code></u>
<u>SUSPENDED</u>	<u>"Health Record Relocation in progress"</u>
<u>MAINTENANCE</u>	<u>"Health Record Maintenance in progress"</u>

`<=`, `<=>` [`<=`]

A_26325-01 -XDS Document Service - Aktenkonto unbekannt oder im Zustand INITIALIZED

Falls sich ein Aktenkonto im Zustand UNKNOWN oder INITIALIZED befindet MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem `NoHealthRecord`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. `<=` [`<=`]

A_25683-01 -XDS Document Service - Prüfung auf Befugnis

Falls keine gültige Befugnis für den aufrufenden Nutzer vorliegt MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem `NotEntitled`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. `<=`]

A_26459 -XDS Document Service - keine Authentisierung des Nutzers

Falls keine erfolgreiche Authentifizierung des Nutzers vorliegt MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem `InvalidAuth`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. `<=` [`<=`]

A_27541 -XDS Document Service - keine Geräteregistrierung des Nutzers

Falls der Nutzer der Versicherte oder ein Vertreter ist (`oid_versicherter`) und keine Geräteregistrierung des Nutzers vorliegt, MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem `UnregisteredDevice`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. `<=`]

3.13.1.6 Schnittstellen im XDS Document Service

In diesem Abschnitt wird die Außenschnittstelle des XDS Document Service festgelegt. Einzelne Umsetzungsanforderungen suggerieren eine vermischte Verarbeitung von Funktionalitäten, welche bei IHE ITI originär getrennt von einer Document Registry und einem Document Repository (bzw. den Responding Gateways) durchgeführt werden. Da die Außenschnittstelle des XDS Document Service nicht zwischen Document Registry und Document Repository unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit differenzierten Pfaden, siehe A_26814-*, werden sonst bei IHE ITI explizite Operationen zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne Umsetzung angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-Nachricht kann an IHE ITI-konforme Akteure ausgerichtet werden.

3.13.1.6.1 Schnittstelle `I_Document_Management`

Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen.

A_14152-02 -XDS Document Service – Implementierung der Schnittstelle `I_Document_Management`

Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle für den Zugriff von ePA-Clients, die über das zentrale Netz zugreifen implementieren.

4893 **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 	

4894 **[<=]**

4895 Durch die Legal Policy ist geregelt, welche Clients (professionOID) letztendlich zugreifen
 4896 dürfen.

4897 3.13.1.6.1.1 Operation I_Document_Management::ProvideAndRegisterDocumentSet-b
 4898 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 4899 Transaktion "ProvideAndRegisterDocumentSet-b" [ITI-41] sind [IHE-ITI-TF2x] sowie
 4900 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4901 Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner
4902 gesammelt. Das Anlegen eines DiGA-Ordners erfolgt durch den XDS Document Service
4903 unter der Voraussetzung, dass es eine gültige Befugnis für die DiGA gibt. Der DiGA-
4904 Ordner wird vom XDS Document Service mit der Telematik-ID der DiGA verknüpft.
4905 Die Zuordnung von DiGA-Dokumenten beim Schreiben erfolgt implizit über die
4906 TelematikID aus dem IDToken des Nutzers. Da ein DiGA-Ordner im Titel immer den
4907 Namen der DiGA enthält kann ein Client (z.B. LEI) darüber die relevante DiGA auswählen
4908 und auf die Dokumente der DiGA, sofern eine Befugnis für den Nutzer vorliegt, lesend
4909 zugreifen.

4910 Ein Update eines bestehenden Dokuments mit der bekannten DocumentEntry.entryUUID
4911 kann durch einen DiGA-Client erfolgen. Hierzu ist es erforderlich, dass ein DiGA-Client
4912 die DocumentEntry.entryUUID persistiert und keine symbolischen IDs gemäß [IHE-ITI-
4913 TF2b#3.42.4.1.3.7] verwendet.

4914 **A_21512-04 -XDS Document Service – dynamisches Anlegen von DiGA-Ordern**

4915 Falls eine gültige Befugnis für eine konkrete DiGA vorliegt, MUSS der XDS Document
4916 Service beim erstmaligen Einstellen eines Dokumentes für diese DiGA in die Akte des
4917 Versicherten (Operation `I_Document_Management::ProvideAndRegisterDocumentSet-`
4918 `b()`) sicherstellen, dass genau ein Ordner für den Versicherten mit den folgenden
4919 Eigenschaften angelegt ist:

- 4920 • DiGA-Ordner der Kategorie diga gemäß A_19388 (Belegung `Folder.codeList`) unter
4921 Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A_14760
4922 (Belegung der restlichen Metadatenfelder).
- 4923 • `Folder.title` wird entsprechend des Attributs "organizationName" aus dem IDToken
4924 der zugreifenden DiGA belegt.
- 4925 • `Folder.comment` wird belegt mit "urn:gematik:diga:<Telematik-ID>", wobei die
4926 Telematik-ID dem Attribut "idNummer" des ID-Token entspricht.
- 4927 • `Folder.EntryUUID` wird mit einer aus der TelematikID abgeleiteten UUID belegt.

4928 Die `folder.EntryUUID` MUSS wie folgend dargestellt aus der TelematikID der DiGA erzeugt
4929 werden:

- 4930 • Algorithmus: Name-Based UUID gemäß [RFC4122#4.3], Version 3 (MD5)
- 4931 • Namensraum-UUID: "e2310a38-0b62-415e-8b44-994dc8312965"
- 4932 • Name: "<TelematikId>"

4933 Eine konkrete DiGA wird identifiziert durch die TelematikID und ist als DiGA durch die
4934 professionOID gekennzeichnet.
4935 [`<=`]

4936 **A_22994-01 -XDS Document Service - automatische Folder-Zuordnung für DiGA**

4937 Der XDS Document Service MUSS beim Einstellen eines DiGA-Dokumentes in die Akte
4938 des Versicherten (Operation
4939 `I_Document_Management::ProvideAndRegisterDocumentSet-b()`) sicherstellen, dass das
4940 DiGA-Dokument in den durch die TelematikID referenzierten DiGA-Ordner abgelegt wird.
4941 Die TelematikID des zu adressierenden Ordners entspricht dem Attribut "idNummer" des
4942 ID-Token .[`<=`]

4943 **A_21713-03 -XDS Document Service – Kein Einstellen von Ordnern**

4944 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und
4945 Dokument(en) über die
4946 Schnittstelle `I_Document_Management::ProvideAndRegisterDocumentSet-b` ablehnen
4947 und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der

4948 Eingangsnachricht ein oder mehrere neu anzulegende Folder enthalten sind. Ausnahme:
4949 Folder der Kategorie `pregnancy_childbirth` in `Folder.codeList.[<=]`

4950 **A_24497 -XDS Document Service - Verwendung der korrekten Telematik-ID** 4951 **beim Einstellen**

4952 Der XDS Document Service MUSS die Telematik-ID aus dem ID-Token der aktuellen User
4953 Session abgleichen mit der Telematik-ID aus `SubmissionSet.authorInstitution` und
4954 das Abweichen der Telematik-Ids mit einem `XDSRepositoryMetadataError`-Fehlercode
4955 quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError-`
4956 Elements den Text "Telematik-ID does not match" angeben. [`<=`]

4957 **A_24456 -XDS Document Service - Durchsetzung von Uniqueness beim** 4958 **Einstellen von Notfalldaten**

4959 Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien
4960 "emergency" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein
4961 einzelnes NFD- und ein einzelnes DPE-Dokument im Status "approved" gibt. Der Versuch,
4962 innerhalb dieses Ordners ein zweites NDF- oder DPE-Dokument einzustellen, MUSS mit
4963 dem IHE-Error `InvalidDocumentContent` abgebrochen werden. Es MUSS im
4964 `codeContext`-Attribut des zurückgegebenen `InvalidDocumentContent`-Elements der Text
4965 "Medical information object has to be unique" zurückgegeben werden. [`<=`]

4966 ~~**A_25137 -XDS Document Service - Durchsetzung von Uniqueness beim**~~ 4967 ~~**Einstellen vom Medikationsplan**~~

4968 ~~3.13.1.6.1.2 Der XDS Document Service MUSS beim Einstellen eines Dokumentes der~~
4969 ~~Kategorien "emp" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein~~
4970 ~~einzelnes eMP-Dokument im Status "approved" gibt. Der Versuch, innerhalb dieses~~
4971 ~~Ordners ein zweites eMP-Dokument einzustellen, MUSS mit dem IHE-~~
4972 ~~Error `InvalidDocumentContent` abgebrochen werden. Es MUSS im `codeContext`-Attribut~~
4973 ~~des zurückgegebenen `InvalidDocumentContent`-Elements der Text "Medical information~~
4974 ~~object has to be unique" zurückgegeben werden. [`<=`]~~

4975 3.13.1.6.1.3 Operation `I_Document_Management::RegistryStoredQuery`
4976 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
4977 Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
4978 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4979 3.13.1.6.1.4 Operation `I_Document_Management::RemoveMetadata`
4980 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
4981 Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-
4982 ITI-TF2x] zu entnehmen.

4983 3.13.1.6.1.5 Operation `I_Document_Management::RetrieveDocumentSet`
4984 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
4985 Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
4986 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4987 3.13.1.6.1.6 Operation `I_Document_Management::RestrictedUpdateDocumentSet`
4988 Weitere Details zur Ausgestaltung dieser Operation finden sich bezüglich der
4989 dazugehörigen IHE ITI-Transaktion "RestrictedUpdateDocumentSet" [ITI-92] in [IHE-ITI-
4990 RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x].

4991 Weitere Anforderungen zur Umsetzung der Operation `RestrictedUpdateDocumentSet`
4992 befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92] .

4993 3.13.1.6.2 Schnittstelle `I_Document_Management_Insurant`

4994 Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-
4995 Transaktionen bei mehreren Schnittstellen .

4996 **A_14478-01 -XDS Document Service – Implementierung der Schnittstelle**
 4997 **I_Document_Management_Insurant**
 4998 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-
 4999 Service-Schnittstelle für den Zugriff des ePA-FdV implementieren .

5000 **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 	

5001
 5002 [**<=**]

- 5003 **A_26460 -XDS Document Service - Zugriff über**
5004 **I_Document_Management_Insurant mit nicht registriertem Gerät**
5005 Falls Operationen von I_Document_Management_Insurant ohne registriertes Gerät
5006 aufgerufen werden MUSS der XDS Document Service die Verarbeitung ablehnen und mit
5007 einemUnregisteredDevice-Fehlercode quittieren.[<=]
- 5008 3.13.1.6.2.1 Operation
5009 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
5010 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
5011 Transaktion "Provide And Register Document Set-b" [ITI-41] sind [IHE-ITI-TF2x] sowie
5012 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.
- 5013 **A_21481-05 -XDS Document Service – Kein Einstellen von Ordern und**
5014 **Associations**
5015 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und
5016 Dokument(en) über die Schnittstelle
5017 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b() ablehnen und
5018 mit einem XDSRegistryMetadataError-Fehlercode quittieren, wenn in der
5019 Eingangsnachricht ein oder mehrere neu anzulegende Folder oder andere als die
5020 folgenden Assoziationen
- 5021 • SS-DE
 - 5022 • SS-HM
 - 5023 • FD-DE
 - 5024 • RPLC
- 5025 enthalten sind.[<=]
- 5026 Das Referenzieren bestehender Ordner ist davon nicht berührt, wie dies z. B. beim
5027 Einstellen von Dokumenten in Sammlungen der Fall ist (z. B. Einstellen eines Dokuments
5028 in einen Mutterpass).
- 5029 **A_23144 -XDS Document Service - Automatische Ablage von Dokumenten im**
5030 **Ordner "technical"**
5031 Der XDS Document Service MUSS sicherstellen, dass Dokumente mit einem formatCode
5032 mit der codeSystem OID "2.25.154081344090540725127779452347992051720",
5033 unabhängig von weiteren Metadaten, im statischen Ordner "technical" abgelegt
5034 werden.[<=]
- 5035 3.13.1.6.2.2 Operation I_Document_Management_Insurant::RegistryStoredQuery
5036 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
5037 Transaktion "Registry Stored Query" [ITI-18] sind [IHE-ITI-TF2a], [IHE-ITI-TF2x] sowie
5038 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.
- 5039 3.13.1.6.2.3 Operation I_Document_Management_Insurant::RemoveMetadata
5040 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
5041 Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-
5042 ITI-TF2x] zu entnehmen.
- 5043 3.13.1.6.2.4 Operation I_Document_Management_Insurant::RetrieveDocumentSet
5044 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
5045 Transaktion "RetrieveDocumentSet" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
5046 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5047 3.13.1.6.2.5 Operation
 5048 I_Document_Management_Insurant::RestrictedUpdateDocumentSet
 5049 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 5050 Transaktion "RestrictedUpdateDocumentSet" [ITI-92] sind [IHE-ITI-RMU], [IHE-ITI-
 5051 TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.
 5052 Weitere Anforderungen zur Umsetzung der Operation RestrictedUpdateDocumentSet
 5053 befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92].

5054 3.13.1.6.3 Schnittstelle I_Document_Management_Ncpeh

5055 Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-
 5056 Transaktionen bei mehreren Schnittstellen .

5057 **A_27300-01 -XDS Document Service (EU) – Implementierung der Schnittstelle**
 5058 **I_Document_Management_Ncpeh**

5059 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-
 5060 Service-Schnittstelle für den Zugriff durch den NCPeH-FD implementieren.

5061 **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 	

5062
 5063 [**<=**]

5064 3.13.1.6.3.1 Operation I_Document_Management_Ncpeh::RegistryStoredQuery
 5065 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 5066 Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
 5067 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5068 3.13.1.6.3.2 Operation I_Document_Management_Ncpeh::RetrieveDocumentSet
 5069 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 5070 Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
 5071 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5072 3.13.1.7 Statische Metadaten

5073 Statische Inhalte werden vor der ersten Nutzung des XDS Document Service angelegt, d.
 5074 h. bevor auf XDS Metadaten zugegriffen wird. Sie sind unveränderlich.

5075 A_24491-02 -XDS Document Service – Anlegen von statischen Ordnern

5076 Der XDS Document Service MUSS nach der erfolgreichen Anlage der Akte des
 5077 Versicherten die Kategorienordner unter Berücksichtigung allgemeiner Vorgaben für
 5078 Folder-Metadaten in A_14760* (Belegung der restlichen Metadatenfelder) für den
 5079 Versicherten gemäß der folgenden Tabelle anlegen. Alle statischen Kategorienordner
 5080 werden mit jeweils einem Ordner pro Kategorie angelegt. Alle statischen Ordner sind
 5081 nach dem Anlegen initial leer.
 5082 Das Anlegen von Submission Sets und zugehöriger Associations zu den statischen
 5083 Ordnern ist nicht vorgegeben. Das XDS-Informationsmodell MUSS allerdings hinsichtlich
 5084 der Folder-DocumentEntry- sowie SubmissionSet-HasMember-Associations bei einer
 5085 Verarbeitung durch die Document Consumer (z. B. Querying) erfüllt werden.

5086 **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

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
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

5087

5088 [\leq]

5089 *Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner vom Typ*
 5090 *"pregnancy_childbirth" und verwenden als Folder.title ein Kennzeichen der*
 5091 *Schwangerschaft (A_22515-*).*

5092 **A_20216-04 -XDS Document Service – Unveränderlichkeit von statischen** 5093 **Akteninhalten**

5094 Der XDS Document Service DARF die Metadaten eines statischen Aktenobjekts gemäß
 5095 A_24491 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen.
 5096 Dabei gelten folgende Ausnahmen:

- 5097 • Folder.lastUpdateTime - Folder.lastUpdateTime wird automatisch vomXDS
 5098 Document Service aktualisiert, sobald Dokumente in den Ordner eingestellt (siehe
 5099 auch [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6]), daraus gelöscht
 5100 oder darin aktualisiert werden.

5101 [\leq]

5102 **3.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten**

5103 Für den XDS Document Service werden Vorgaben bezüglich zu verwendender IHE XDS-
 5104 Metadatenattribute auf Ebene von Submission Set, Document Entry sowie Folder

5105 vorgenommen. Diese Nutzungsvorgaben referenzieren größtenteils Value Sets der IHE
5106 Deutschland Arbeitsgruppe "XDS Value Sets" [IHE-ITI-VS] und sind für die ePA-
5107 Fachanwendung verbindlich. Diese XDS-Value Sets sind teilweise von IHE-Deutschland
5108 als "offen" gekennzeichnet, um Erweiterungen flexibel einbringen zu können. Für
5109 die ePA-Fachanwendung gelten jedoch definierte Vorgaben, wie neue Codes und Value
5110 Sets sicher über eine Konfigurationsschnittstelle eingebracht werden können. Daher sind
5111 die in dieser Spezifikation beschriebenen Nutzungsvorgaben für Value Sets als fest
5112 anzusehen bzw. die Offenheit der XDS Value Sets wird nicht unterstützt.

5113 3.13.1.8.1 Allgemeine Metadatenvorgaben

5114 Die Spalten der unten dargestellten, tabellarischen Übersichten für die Metadaten von
5115 Dokumenten (IHE XDS.b Document Entry) und Übertragungspaketen (IHE XDS.b
5116 Submission Set) haben die folgenden Bedeutungen:

- 5117 • Die Spalte "Metadatenattribut XDS.b" listet alle aus dem IHE ITI TF vorgesehenen
5118 Metadaten für Document Entry- und Submission Set-Elemente auf.
- 5119 • Die Spalten "Mult. PS" (Multiplizität Primärsystem; alle Primärsysteme außer PS-
5120 KTR), "Mult. KTR" (Multiplizität "PS-KTR"), "Mult. DS" (Multiplizität "Document
5121 Service"), "Mult. FV" (Multiplizität "ePA-Frontend des Versicherten") kennzeichnen
5122 die Multiplizität des Metadatenattributs beim Erzeugen oder Verarbeiten durch das
5123 jeweilige System.
5124 Die Angabe der jeweiligen Spalte entspricht einem Wertebereich. Die Zeichen [...]
5125 für Wertebereich wurden zum Zwecke der besseren Darstellbarkeit weggelassen.
- 5126 • Die Spalte "Kurzbeschreibung" beschreibt kurz die Bedeutung des
5127 Metadatenattributs.
- 5128 • Die Spalte "Nutzungsvorgabe" macht Bedingungen für die Verwendung eines
5129 Metadatenattributs (z. B. erlaubte Wertebereiche und Formatangaben), welche
5130 über die im IHE ITI TF definierten Vorgaben hinausgehen.
- 5131 • Die Spalte "FV Edit" beschreibt, ob ein bestimmtes Metadatenattribut beim
5132 Einstellen eines Dokuments über das ePA-FdV durch den Versicherten veränderbar
5133 gestaltet werden muss. Es sollten dabei immer nur die für den aktuellen Workflow
5134 relevanten Metadatenattribute angezeigt werden, um die Komplexität für den
5135 Versicherten gering zu halten. Veränderbar gestaltete Metadatenattribute müssen
5136 mit sinnvollen Default-Werten vorbelegt werden.

5137 **A_14760-27 -Nutzungsvorgaben für die Verwendung von XDS-Metadaten**

5138 Der XDS Document Service MUSS sicherstellen, dass Primärsysteme und das ePA-
5139 Frontend des Versicherten zur Registrierung von Dokumenten die nachstehenden
5140 Nutzungsvorgaben für Metadaten berücksichtigen. Der XDS Document Service MUSS
5141 diese Metadaten verarbeiten können und diese Metadaten ggf. während des
5142 Registriervorgangs ergänzen. Metadaten können über die Operationen

- 5143 • `I_Document_Management::ProvideAndRegisterDocumentSet-b` sowie
- 5144 • `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b`

5145 registriert oder über die Operationen

- 5146 • `I_Document_Management::RestrictedUpdateDocumentSet`
- 5147 • `I_Document_Management_Insurant::RestrictedUpdateDocumentSet`

5148 geändert werden.

5149 Für den Produkttyp DiGA gelten die gleichen Vorgaben wie für die Primärsysteme sofern
5150 unter Nutzungsvorgaben keine abweichenden Bedingungen definiert werden.

5151 **Tabelle 31: Nutzungsvorgaben für Metadatenattribute XDS**

Metadaten- attribut XDS.b		Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
		P S	K T R	D S	F d V			
Metadaten für DocumentEntry								
author		1. .n	1. .1	0. .0	0. .n	Person oder System, welche(s) das Dokument erstellt hat	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.1] genügen. Das Primärsystem MUSS mindestens das Subattribut authorPerson oder authorInstitution inhaltlich belegen.	
	authorPerson	0. .1	0. .1	0. .0	0. .1	Name des Autors	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 3.13.1.8.2- <u>Metadaten der Dokumente und SubmissionSets</u> genügen.	X
	authorInstitution	0. .n	0. .n	0. .0	0. .n	Institution, die dem Autor zugeordnet ist	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 3.13.1.8.2- <u>Metadaten der Dokumente und SubmissionSets</u> (A_21209) genügen.	X
	authorRole	0. .n	0. .n	0. .0	0. .n	Rolle des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS aus [IG_TI_Terminology] entsprechen.	X
	authorSpecialty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorSpecialtyVS 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

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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 Kategorie health_risk_analysis den Code "ASM" (Assessment) verwenden. 	X
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.4] genügen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
confidentialityCode	0. .n	0. .n	0. .1	0. .n	Vertraulichkeitskennzeichnung des Dokuments	<p>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.</p> <p>Für ProvideAndRegisterDocuments et-b MUSS für das Verbergen des Dokumentes der Code</p> <ul style="list-style-type: none"> Code = "CON", Display Name = "constraint" <p>aus dem Code System 1.2.276.0.76.5.491 (siehe auch Value Set EPAXDSConfidentialityCodeVS aus [IG_TI_Terminology]) gesetzt werden.</p>	X
creationTime	1. .1	1. .1	0. .0	1. .1	Erstellungszeitpunkt des Dokuments	<p>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.</p>	X
entryUUID	1. .1	1. .1	0. .1	1. .1	Intern verwendete, aktenweit eindeutige Kennung des Dokuments	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.7] genügen.</p> <p>Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.</p>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
eventCodeList	0. .n	0. .0	0. .0	0. .n	Ereignisse, die zur Erstellung des Dokuments geführt haben.	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.8] genügen und Codes des Value Set EPAXDSEventCodeVS aus [IG_TI_Terminology] entsprechen.</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>	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
formatCode	1. .1	1. .1	0. .0	1. .1	Global eindeutiger Code für das Dokumentenform at. Zusammen mit dem DocumentEntry.t ypeCode eines Dokuments soll es einem potentiellen zugreifenden System erlauben, im Vorfeld festzustellen, ob das Dokument verarbeitet werden kann.	Der Wert MUSS einem Code des Value Sets EPAXDSFormatCode aus [IG_TI_Terminology] entsprechen. Der Wert KANN "urn:ihe:iti:xds:2017:mimeT ypeSufficient" (siehe [IHE- ITI-TF-3#4.2.3.2.9]) entsprechen, um anzuzeigen, dass über den MIME-Type hinaus keine genaueren Angaben zum Dokumentenformat gemacht werden können oder der MIME- Type ausreichend ist. Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9- Strukturierte Dokumente genügen.	
hash	0. .0	0. .0	1. .1	0. .0	Kryptographische Prüfsumme des Dokuments	Der Wert wird vom XDS Document Service beim Einstellen des Dokuments in die Akte berechnet.	
healthcareFacilit yTypeCode	1. .1	1. .1	0. .0	1. .1	Art der Einrichtung, in der das dokumentierte Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSHealthcareFacilityTypeC odeVS aus [IG_TI_Terminology] entsprechen. Das PS-KTR MUSS healthcareFacilityTypeCode ausschließlich mit dem Wert "VER" (Versicherungsträger) belegen. Die DiGA MUSS healthcareFacilityTypeCo de mit dem Wert "PAT" belegen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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	Markierungsattri- but, dass das Metadateneleme- nt DocumentEntry nicht den vollständigen Satz an Metadaten enthält.		

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
contentType	1. .1	1. .1	0. .0	1. .1	MIME-Type des Dokuments	<p>Ein Wert aus der folgenden Liste gemäß A_24864* und A_25009* MUSS als MIME-Type verwendet werden.</p> <p>PS-KTR MUSS für Dokumente der Kategorie health_risk_analysis ausschließlich den Wert "application/pdf" gemäß A_25009-* verwenden. Als formatCode ist dann entsprechend "urn:ihe:iti:xds:2017:mimeTypeSufficient" zu verwenden</p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9-Strukturierte Dokumente genügen. <u>Anmerkung:</u> In Klammern sind die Extensions angegeben, die beim entsprechenden MIME-Type in DocumentEntry.URI für das URI-scheme "file," zu verwenden sind.</p>	
objectType	1. .1	1. .1	0. .0	1. .1	Typ des Dokuments	<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>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
patientId	1. .1	1. .1	0. .0	1. .1	Systemweit eindeutige Kennung des Patienten	Der Wert MUSS den Inhalts- und Formatvorgaben ausA_14974* genügen. Außerdem MUSS der Wert der Identität des Akteninhabers entsprechen und MUSS vom XDS Document Service dahingehend bei Registrierung der Metadaten geprüft werden.	
practiceSettingC ode	1. .1	0. .0	0. .0	1. .1	Art der Fachrichtung der erstellenden Einrichtung, in der das dokumentiere Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSPracticeSettingCodeVS 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.	
repositoryUniqu eId	0. .1	0. .1	1. .1	0. .1	Kennung des Document Repository, in welches das Dokument eingestellt wird/wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.18] genügen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
serviceStartTime	0. .1	0. .1	0. .0	0. .1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis begonnen wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.19] genügen.	X
serviceStopTime	0. .1	0. .1	0. .0	0. .1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis beendet wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.20] genügen.	X
size	0. .0	0. .0	1. .1	0. .0	Größe des Dokuments in Bytes	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.21] genügen. Der XDS Document Service MUSS die Größe des Dokuments berechnen und in den Metadaten während des Registriervorgangs setzen (vgl. [IHE-ITI-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

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
typeCode	1. .1	1. .1	0. .0	1. .1	Art des Dokuments	<p>Der Wert MUSS einem Code des Value Sets EPAXDSTypeCodeVS aus [IG_TI_Terminology] entsprechen.</p> <p>PS-KTR MUSS für Dokumente der Kategorie health_risk_analysis ausschließlich den Code "GRIS" verwenden</p> <p>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.</p>	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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorPerson	0. .1	0. .1	0. .0	0. .1	Name der einstellenden Per son 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.</p> <p>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>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorInstitution	0. .1	0. .1	0. .0	0. .0	Institution, welcher die einstellende Pers on 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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorRole	1. .n	1. .n	0. .0	1. .1	Rolle der einstellenden Per son oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS aus [IG_TI_Terminology] entsprechen. Das PS-KTR MUSS den Code "105" (Kostenträgervertreter) verwenden. Das ePA-Frontend des VersichertenMUSS den Code "102" (der Patient selbst) verwenden. Die DiGA MUSS authorRole mit dem Code "12" (dokumentierendes Gerät) verwenden.	
authorSpecial ty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung der einstellenden Per son oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorSpecialtyVS aus [IG_TI_Terminology] entsprechen.	
authorTeleco mmunication	0. .n	0. .0	0. .0	0. .n	Telekommunikati onsdaten der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.1.4.5] genügen.	
availabilityStatu s	0. .0	0. .0	1. .1	0. .0	Status des Submission Sets ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approved" entsprechen.	
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

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
contentTypeCode	0. .1	0. .1	0. .0	0. .1	Klinische Aktivität, die zum Einstellen des Submission Set geführt hat.	Der Wert MUSS einem Code des Value Sets EPAXDSContentTypeCodeVS aus [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.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
intendedRecipient	0. .n	0. .0	0. .0	0. .n	Vorgesehener Adressat des Submission Set	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.3.7] genügen.	
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierung, welche anzeigt, dass das Submission Set nicht den durch das IHE ITI TF vorgegebenen Satz an Metadaten enthält.		
patientId	1. .1	1. .1	0. .0	1. .1	Patienten-ID, zu der das Submission Set gehört	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
sourceId	0. .0	0. .0	0. .0	0. .0	Weltweit eindeutige, unveränderliche Kennung des einstellenden Systems		

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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_childbirth MUSS das Primärsystem diese Codes angeben.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
comments	0. .1	n/ a	0. .0	n/ a	Freitextkommentar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen.	
entryUUID	1. .1	n/ a	1. .1	n/ a	Intern verwendete, aktenweit eindeutige Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.	
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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
uniqueId	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 Ordnerns ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approved" entsprechen.	
codeList	n/ a	n/ a	1. .1	n/ a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI- TF3#4.2.3.4.2] und einem Code des Value Sets EPADataCategoryOtherVS und EPADataCategoryMedicalVS aus [IG_TI_Terminology] entsprechen. Der XDS Document Service MUSS codeList gemäß A_19388* setzen.	
comments	n/ a	n/ a	0. .1	n/ a	Freitextkomment ar 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 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						

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
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.	

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)

Language / Country Code Kombination	Language / Country Code Kombination
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)

5154

5155 [**<=**]

5156 3.13.1.8.2 Metadaten der Dokumente und SubmissionSets

5157 **A_23369-02 -XDS Document Service – Verpflichtender Dokumententitel in**

5158 **DocumentEntry.title**

5159 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
 5160 Dokumenten und dem Ändern von Metadaten an Dokumenten `DocumentEntry.title`
 5161 befüllen. Der Titel des Dokumentes soll eine fachliche Beschreibung des Dokumentes
 5162 enthalten. Bei `DocumentEntry.title` MÜSSEN führende und endende Leerzeichen
 5163 entfernt werden. In `DocumentEntry.title` DARF NICHT leer sein (!= "") (insbesondere
 5164 auch nicht nach etwaigen Entfernen von Leerzeichen vorne und hinten). In
 5165 `Document.title` DÜRFEN keine nicht-druckbaren Zeichen enthalten sein. [**<=**]

A_25188 -XDS Document Service - Input Sanitization

Der XDS Document Service MUSS sicherstellen, dass bei Anlage und Aktualisierung (Ändern) von Metadaten:

1. führende (leading) und endende (trailing) Whitespace von den Attributen automatisch entfernt werden.
2. die notwendigen Attribute nichtleer sind (insbeondere auch noch Whitespace-Entfernung aus 1.). und
3. Die Attribute nur druckbare Zeichen enthalten.

[<=]

A_14762-05 -XDS Document Service – Nutzungsvorgabe für authorPerson als Teil von DocumentEntry.author und SubmissionSet.author

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an `authorPerson` unterhalb von `DocumentEntry.author` und `SubmissionSet.author` neben [IHE-ITI-TF3#4.2.3.1.4.2] auch die folgenden Vorgaben beachten.

Bei Leistungserbringer als Autor:

1. Lebenslange Identifikationsnummer eines Arztes (Lebenslange Arztnummer - LANR 9 Stellen) oder im Falle eines Zahnarztes die Zentrale Zahnarzt Nummer (ZANR)- sofern die ZANR bekannt ist
2. "^"
3. Nachname
4. "^"
5. Vorname
6. "^"
7. Weiterer Vorname
8. "^"
9. Namenszusatz
10. "^"
11. Titel
12. "^^^&" - sofern LANR oder ZANR angegeben, ansonsten "^^^"
13. "1.2.276.0.76.4.16" - sofern LANR angegeben oder "1.2.276.0.76.4.296", falls ZANR angegeben
14. "&ISO" - sofern LANR oder ZANR angegeben

Beispiele:

165746304^Weber^Thilo^^^Dr.^^^&1.2.276.0.76.4.16&ISO
^Zahnschmerz^Eberhard^^^Dr.^^^

Bei Versichertem als Autor:

1. Der unveränderbare Teil der KVNR (10 Stellen)
2. "^"
3. Nachname

- 5208 4. "^"
- 5209 5. Vorname
- 5210 6. "^"
- 5211 7. Weiterer Vorname
- 5212 8. "^"
- 5213 9. Namenszusatz
- 5214 10. "^"
- 5215 11. Titel
- 5216 12. "^^^&"
- 5217 13. "1.2.276.0.76.4.8"
- 5218 14. "&ISO"

5219 Beispiel: G995030566^Gundlach^Monika^^^^^&1.2.276.0.76.4.8&ISO
 5220 Sowohl beim LE als auch beim Versicherten müssen Vorname und Nachname belegt
 5221 werden.

5222
 5223 **Software-Komponente bzw. Gerät als Autor**

5224 Beim (automatisierten) Einstellen von Dokumenten MUSS der max. 256-Zeichen lange
 5225 Name der Software-Komponente bzw. des Geräts als Nachname und ggf. als Vorname(n)
 5226 eingetragen werden.

5227 Beispiel: ^PHR-Gerät-XY^PHR-Software-XY

5228 Im Falle einer DiGA MUSS das Feld Autor folgendermaßen aufgebaut sein:

- 5229 1. Telematik-ID der DiGA
- 5230 2. "A"
- 5231 3. Name der DiGA (Name der Verordnungseinheit)
- 5232 4. "A"
- 5233 5. Name des DiGA-Herstellers
- 5234 6. "A"
- 5235 7. optionale Ergänzung der Bezeichnung der SW
- 5236 8. "A"
- 5237 9. optionale Ergänzung der Bezeichnung der SW
- 5238 10. "A"
- 5239 11. optionale Ergänzung der Bezeichnung der SW
- 5240 12. "^^^&"
- 5241 13. <OID für DiGAs, wie in professionOID>
- 5242 14. "&ISO"

5243
 5244 Für alle drei Arten von Autoren (Versicherter, LE, Gerät) MUSS jeweils Vorname und
 5245 Nachname angegeben sein. [<=]

A_14763-03 -XDS Document Service - Nutzungsvorgabe für SubmissionSet.authorInstitution

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an `SubmissionSet.authorInstitution` neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

Beispiele:

- Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-e518
- gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^8-34923902a

[<=]

A_21511-01 -Nutzungsvorgabe SubmissionSet.authorInstitution für DiGAs

Der XDS Document Service MUSS sicherstellen, dass DiGAs beim Upload von Dokumenten, die folgenden Nutzungsvorgaben für das Metadatenattribut `DocumentEntry.authorInstitution` sowie `SubmissionSet.authorInstitution` berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.1.4.1] genügen und ist inhaltlich nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen.

1. Name des Anbieters der DiGA
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der DiGA

[<=]

A_21209-02 -XDS Document Service - Nutzungsvorgabe für DocumentEntry.authorInstitution

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an `DocumentEntry.authorInstitution` neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

5289 Die Komponenten 2.-5. sind nur anzugeben, wenn die Telematik ID (5.) der
 5290 Autoreninstitution bekannt ist oder ad-hoc ermittelt werden kann, bspw. über den
 5291 Verzeichnisdienst der TI-Plattform (VZD). Ansonsten wird ausschließlich der Name
 5292 gesetzt.

5293 Beispiele:

5294 • Arztpraxis Dr. Thilo Weber^^^^^1.2.276.0.76.4.188&ISO^^^^1-2c47sd-
 5295 e518

5296 • gematik Betriebskrankenkasse^^^^^1.2.276.0.76.4.188&ISO^^^^8-
 5297 34923902a

5298 • Arztpraxis Dr. Wiebke Werner

5299 [`<=`]

5300 **A_22408-02 -XDS Document Service - DocumentEntry.authorInstitution ohne** 5301 **Telematik-ID**

5302 Der XDS Document Service MUSS Nachrichten zum Registrieren von Dokumenten bei
 5303 fehlender Telematik-ID in `DocumentEntry.authorInstitution` akzeptieren und
 5304 daraufhin alle Zeichen hinter dem Namen der `authorInstitution` abschneiden und
 5305 verwerfen.[`<=`]

5306 **A_14974-02 -XDS Document Service - Nutzungsvorgabe für** 5307 **DocumentEntry.patientId und SubmissionSet.patientId**

5308 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
 5309 Dokumenten und dem Ändern von Dokumenten-Metadaten die folgenden
 5310 Nutzungsvorgaben für `DocumentEntry.patientId` und `SubmissionSet.patientId`
 5311 berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.2.16] bzw. [IHE-
 5312 ITI-TF3#4.2.3.3.8] genügen und ist inhaltlich nach der folgenden Vorschrift
 5313 zusammenzufügen bzw. zu belegen:

- 5314 1. Der unveränderbare Teil der KVNR des Akteninhabers (10 Stellen)
- 5315 2. "^^^&"
- 5316 3. "1.2.276.0.76.4.8" (OID zur Kennzeichnung einer unveränderbaren KVNR)
- 5317 4. "&ISO"

5318 Beispiel: G995030566^^^&1.2.276.0.76.4.8&ISO[`<=`]

5319 **A_27759 -XDS Document Service - Verarbeitung von Code System Version**

5320 Der XDS Document Service MUSS Metadaten vom Typ Coded Attribute im Slot
 5321 "codingScheme" bei Angabe einer System URL oder Canonical URL eine per Pipe-Symbol
 5322 (|) angehängte Version akzeptieren und für eine Terminologievalidierung
 5323 verwenden.[`<=`]

5324 Beispiel: <http://dvmd.de/fhir/CodeSystem/kdl|2025>

5325 *3.13.1.8.3 Metadaten für Datenkategorien*

5326 **A_19388-21 -Nutzungsvorgaben für die Verwendung von Datenkategorien**

5327 Der XDS Document Service MUSS beim Einstellen eines Dokuments und beim Ändern von
 5328 Metadaten die folgende Zuordnung zu einer Datenkategorie (d. h. Assoziierung mit einem
 5329 bestimmten Folder) vornehmen. Dabei haben Auswertungs- und Zuordnungsregeln, die
 5330 sich aus A_14761-* und damit verbunden aus [gemSpec_IG_ePA] ableiten, immer den
 5331 Vorrang gegenüber anderen Auswertungsregeln. Ferner MUSS der XDS Document
 5332 Service sicherstellen, dass bei einer Aktualisierung eines Dokuments derselbe Ordner des
 5333 zu ersetzenden Dokuments zugeordnet wird.

5334
 5335 Für eine eindeutige Zuordnung zu einer Datenkategorie MUSS die Auswertung der
 5336 Metadatenvorgaben in der Reihenfolge der folgend dargestellten Einsortierungskriterien
 5337 erfolgen:

5338 **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)

Datenkategorie/Technischer Identifier/Foldercode	Einsortierkriterium (anzuwenden auf DocumentEntry, wenn nicht anders angegeben. Oder-Verknüpfungen, wenn nicht "und" angegeben)
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

5339 *Falls Basiskonzepte angegeben werden, dann gelten automatisch alle Subkonzepte, z.B.
5340 gilt für die Kategorie "care" die Einsortierregel bei PracticeSettingCode = PFL wie auch für
5341 die Sub-Konzepte ALT (Altenpflege) und KIN (Kinderpflege).[<=]

5342 3.13.1.8.4 Automatisches Umschreiben von Daten

5343 Dieser Abschnitt enthält Vorgaben für Datenanpassungen, die für bestehende Daten im
5344 XDS Document Service vorgenommen werden müssen (z. B. wenn sie durch Änderungen
5345 im Rahmen einer neuen Version des XDS Document Service notwendig werden).

5346 **A_27482-01 -XDS Document Service – Metadatenkorrektur bei vorhandenen** 5347 **elektronischen Arztbriefen**

5348 Der XDS Document Service MUSS die Metadaten (DocumentEntry) von bestehenden
5349 Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief)
5350 gemäß [gemSpec_IG_ePA] derartig anpassen, dass DocumentEntry.eventCodeList
5351 zusätzlich um den KDL-Code (code: ED110104, codeSystem: 1.2.276.0.76.5.552,
5352 displayName: eArztbrief) erweitert wird, wenn dieser nicht bereits vorhanden ist.[<=]

5353 **A_27661 -XDS Document Service – Umwandeln von APND-Assoziationen**

5354 Der XDS Document Service MUSS sobald möglich Associations vom Typ
5355 "urn:ihe:iti:2007:AssociationType:APND" wie folgt ersetzen:

- 5356 1. Wenn ein Association.sourceObject oder Association.targetObject auf ein
5357 DocumentEntry im Status "deprecated" zeigt, oder auf einen DocumentEntry, der
5358 zu einer Sammlung (mixed oder uniform) gehört, wird nur Schritt 4 durchgeführt
5359 (Association wird gelöscht), ansonsten weiter bei Schritt 2.
- 5360 2. Der DocumentEntry, auf den Association.sourceObject zeigt (der "Anhang"), MUSS
5361 in DocumentEntry.referenceIdList mit dem
5362 mittelsurn:gematik:iti:xds:2025:parentDocument ausgezeichneten Wert der
5363 DocumentEntry.uniqueId desjenigen Dokuments ergänzt werden, auf das
5364 Association.targetObject zeigt.
- 5365 3. Der DocumentEntry, auf den Association.targetObject zeigt (der
5366 "Hauptdokument"), MUSS in DocumentEntry.referenceIdList mit dem mittels
5367 urn:gematik:iti:xds:2025:childDocument ausgezeichneten Wert der
5368 DocumentEntry.uniqueId desjenigen Dokuments ergänzt werden, auf das
5369 Association.sourceObject zeigt.

5370 4. Anschließend ist die APND-Association zu löschen.

5371 [**<=**]

5372 APND-Associations werden mit ePA Version 3.1.2 durch einen Anhangsmechanismus
5373 mittels DocumentEntry.referenceListId abgelöst. Beim automatischen Umschreiben der
5374 APND-Associations auf die DocumentEntry.referenceIdList können Anhangsketten
5375 entstehen, die länger als insgesamt fünf Dokumente sind. Das ist über das Einstellen von
5376 Dokumenten über Provide and Register Document Set [ITI-41] oder Restricted Update
5377 Document Set [ITI-92] nicht möglich. Entsprechend lange Ketten können also nur aus
5378 der Anpassung von Altdaten entstehen.

5379 Wie aus A_27661 hervorgeht, werden Anhänge von "deprecated"-Dokumenten (d.h.
5380 durch Ersetzen via RPLC-Association durch neue Versionen ersetzte Dokumente)
5381 abgetrennt. Das ist notwendig, da die identischen Metadateneinträge der Dokumente in
5382 der RPLC-Dokumentenketten bei jedem Dokument zwangsläufig auf identische Anhänge
5383 zeigen müssen. Das kleinere Übel ist hier, die Anhänge für die aktuellste Version
5384 zumindest intakt zu halten. Neue Ersetzungen in Verbindung mit Anhängen verhindert
5385 das Aktensystem ab Version 3.1.2, da die Menge an RPLC-fähigen Dokumenten und die
5386 Dokumente, die Anhangsbeziehungen eingehen können, disjunkt spezifiziert sind.

5387 **3.13.1.9 Strukturierte Dokumente**

5388 Die elektronische Patientenakte unterstützt unterschiedliche sogenannte "strukturierte
5389 Dokumente", deren Aufbau über Implementation Guides genau vorgegeben ist. Der
5390 Umfang der unterstützten strukturierten Dokumente wird durch den Umfang der
5391 veröffentlichten Implementation Guides festgelegt (3.13.1.9.2- Konfigurierbarkeit). Für
5392 alle strukturierten Dokumente gelten spezifische Metadatenvorgaben, um sie eindeutig zu
5393 identifizieren und gezielt verarbeiten zu können.

5394 **A_14761-08 -Nutzungsvorgaben für die Verwendung von IHE ITI XDS- 5395 Metadaten bei strukturierten Dokumenten**

5396 Der XDS Document Service MUSS die Nutzungsvorgaben für strukturierte Dokumente
5397 unter [gemSpec_IG_ePA] berücksichtigen. Dabei ist das Format des Dokuments, welches
5398 über einen Code des Metadatenattributs `formatCode` ausgedrückt wird, führend. Das
5399 bedeutet, bei Registrierung eines strukturierten Dokuments mit einem `formatCode`
5400 MÜSSEN die weiteren Metadatenattribute `classCode`, `typeCode`, `mimeType` sowie
5401 `eventCodeList` entsprechend belegt werden. Der XDS Document Service MUSS eine
5402 solche Registrierung diesbzgl. prüfen und im Fehlerfall analog zu A_14938-*
5403 antworten. [**<=**]

5404 **3.13.1.9.1 Sammlungstypen**

5405 Je nach Art ihrer Zusammensetzung und ihrer Handhabung existieren unterschiedliche
5406 Typen strukturierter Dokumente, sogenannte medizinische Informationsobjekte. Ein
5407 medizinisches Informationsobjekt (MIO) ist eine **Sammlung** von Informationen zu
5408 medizinischen, strukturellen oder administrativen Sachverhalten, die in sich geschlossen
5409 oder entsprechend verschachtelt vorliegt. Zudem ist ein MIO eine klar definierte Vorgabe,
5410 wie diese Informationssammlung in der elektronischen Patientenakte gespeichert wird,
5411 damit semantische und syntaktische Interoperabilität gewährleistet werden. Die
5412 Festlegung dieser Vorgaben ist gemäß SGB V Aufgabe der KBV. Beispiele für
5413 medizinische Informationsobjekte sind der Impfpass, das Kinderuntersuchungsheft, der
5414 Mutterpass, das zahnärztliche Bonusheft, oder DiGA. MIOs werden über Sammlungen
5415 und Sammlungstypen umgesetzt.

5416 Einige strukturierte Dokumente sind für sich genommen vollständig und schlüssig wie z.
5417 B. ein Elektronischer Arztbrief. Sie sind ohne Zuhilfenahme weiterer Dokumente in der

ePA für einen Benutzer sinnvoll zu verwenden. Andere Typen strukturierter Dokumente müssen hingegen fast immer in Kombination betrachtet werden, z. B. Impfpassdokumente. Bei letzteren spiegelt jedes Impfpassdokument ein oder mehrere Impfungen wieder. Ein Impfpass, wie er in der analogen Welt geläufig und als logisches Konstrukt sinnvoll ist, besteht immer aus der gemeinsamen Betrachtung aller Impfpassdokumente und somit aller vorhandenen Impfeinträge. Die Kombination ein oder mehrerer strukturierter Dokumente ergeben eine Sammlung.

Eine Sammlungsinstanz (z. B. der Mutterpass der ersten Schwangerschaft der Patientin Martha Mustermann) ist eine konkrete Ausprägung der Information, die zwischen den beteiligten Akteuren ausgetauscht wird. Nicht jede Sammlung besteht zwangsläufig aus Dokumenten desselben Formats: Ein Kinderuntersuchungsheft beispielsweise besteht aus Dokumenten mit drei verschiedenen strukturierten Dokumenttypen. Zentral für alle Sammlungstypen ist immer mindestens ein strukturiertes Dokument mit einem festgelegten Dokumentenformat. Für eine technische Umsetzung sind die Sammlungstypen "mixed" und "uniform" zu unterscheiden, die technisch unterschiedlich umgesetzt werden und zum Teil unterschiedliche Operationen erlauben.

Der Sammlungstyp "mixed" fasst semantisch zusammengehörige, strukturierte Dokumente unterschiedlicher Struktur mittels Ordner zu einer Sammlung zusammen. Der Sammlungstyp "uniform" wird ebenfalls intern über Ordner abgebildet. Dies stellt sicher, dass zukünftige Versionen dieser strukturierten Dokumente/Pässe oder DiGA verlässlich verarbeitet werden können. Ordner gelten als "statische Ordner", bis auf Sammlungen der Kategorie Mutterpass und DiGA ("dynamische Ordner"). Der dynamische Ordner für einen konkreten Mutterpass wird durch den Client angelegt, weil es aus Gründen, die nur der Client kennt (Anzahl der Schwangerschaften), mehrere Ordner dieses Typs geben kann ("nicht-statische Ordner", vgl. A_21610-*). Die Version der Struktur eines Dokuments ist am Format Code erkennbar.

A_20577-06 -Definition und Zuweisung von Sammlungstypen

Der XDS Document Service MUSS jeder Sammlung einen von zwei Sammlungstypen zuweisen:

Tabelle 34: TAB_EPA_Sammlungstypen

Sammlungstyp	Definition
mixed	Ordner, die einer Sammlung des Typs "mixed" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) mit einem für die Sammlung festgelegten Code in der Folder.codeList abgelegt werden.
uniform	Ordner, die einer Sammlung des Typs "uniform" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) abgelegt werden.

Es gelten die Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA]. In den unter [gemSpec_IG_ePA] gemachten Vorgaben werden auch Ordner-Kardinalitäten für spezifische Sammlungen festgelegt. Diese Angaben sagen aus, wie viele Instanzen einer Sammlung (d. h. minimal und maximal) registriert werden können. [≤]

A_20707-04 -XDS Document Service – Keine unpassenden Dokumente in nicht-statische Ordner

Falls das Dokument nicht den Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA] entspricht, MUSS der XDS Document Service das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-Fehlercode `BadFolderAssociation` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die UUID (`DocumentEntry.entryUUID`) des identifizierten Dokuments angegeben werden. [\leq]

A_20581-06 -XDS Document Service – Löschen von Dokumenten aus Sammlungen der Typen "mixed" und "uniform" durch ein ePA-FdV

Der XDS Document Service MUSS beim Löschen eines Dokuments der Sammlungstypen "mixed" und "uniform" durch das ePA-FdV sicherstellen, dass die Operation mit dem Fehler `ReferencesExistException` abgebrochen wird, wenn die Löschanfrage nicht alle Dokumente der Sammlung enthält. Es besteht folgende Ausnahme: Das Löschen einer Elternnotiz im Kinderuntersuchungsheft ist erlaubt. [\leq]

Nur Leistungserbringern ist es erlaubt, einzelne Dokumente aus Sammlungen der Typen "mixed" und "uniform" zu löschen, um die medizinische Interpretation der gesamten Sammlungsinstanz nicht zu gefährden.

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

3.13.1.9.2 Konfigurierbarkeit**A_17546-02 -Konfigurierbarkeit von strukturierten Dokumenten**

Der XDS Document Service MUSS die Liste strukturierter Dokumente konfigurierbar machen, indem dieser die Unterstützung strukturierter Dokumente unter Angabe folgender Eigenschaften ermöglicht:

- Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA] konfiguratativ hinzufügen bzw. entfernen,
- Sammlungen zu `TAB_EPA_Sammlungstypen` gemäß [gemSpec_IG_ePA] konfiguratativ hinzufügen bzw. entfernen.

[\leq]

Das Entfernen der Unterstützung von strukturierten Dokumenten oder Sammlungen bedeutet, dass diese zu einem früheren Zeitpunkt in das Aktensystem geschrieben werden konnten, aber durch Erreichen von "clientReadOnlyFromDate" nicht mehr geschrieben werden dürfen. Das Schreiben umfasst das Aktualisieren oder neu Anlegen. Das Lesen ist weiterhin erlaubt.

A_17551-01 -Prüfanforderungen zur Konfigurierbarkeit von Value Sets

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die zu konfigurierenden Value Sets des XDS Document Service gemäß der Anforderung A_17546-* den folgenden Prüfkriterien unterliegen, bevor bestehende, im XDS Document Service verarbeitete Value Sets verändert werden:

- Es DÜRFEN KEINE Codes der Value Sets gelöscht werden, lediglich das Hinzufügen von Codes zu existierenden Value Sets ist aus Kompatibilitätsgründen erlaubt.
- Neue Codes MÜSSEN den Formatvorgaben gemäß Tabelle 4.2.3.1.7-2 in [IHE-ITI-TF3#4.2.3.1.7] entsprechen und gegenüber einer internen Referenzliste validiert werden. Dies schließt auch Prüfungen zur Zeichenkodierung, der Datentypen als auch zu den Längenbeschränkungen ein.

[\leq]

A_21212-01 -Restriktionen zur Konfigurierbarkeit von Metadaten für strukturierte Dokumente und Sammlungen

Der XDS Document Service MUSS durch technische Maßnahmen sicherstellen, dass Änderungen an den in den Implementierungsvorgaben in [gemSpec_IG_ePA] spezifizierten Codes ausgeschlossen sind. [\leq]

A_21214-03 -Konfiguration strukturierter Dokumente im Rahmen der Veröffentlichung durch die gematik

Der Anbieter des ePA-Aktensystems MUSS durch organisatorische Maßnahmen sicherstellen, dass die Konfiguration im Aktensystem zur Unterstützung strukturierter Dokumente aus [gemSpec_IG_ePA] ausschließlich im Rahmen der Veröffentlichung der Implementation Guides durch die gematik erfolgt. [\leq]

Bei Einführung neuer strukturierter Dokumente werden die beschriebenen Konfigurationsmöglichkeiten so verwendet, dass eine Erweiterung der Spezifikation und daraus resultierend eine Änderung des ePA-Aktensystems mit erneuter Zulassung nicht erforderlich sind.

*3.13.1.9.3 Verarbeitungsvorgaben für spezifische Dokumente***A_27686 -Einstellen des eArztbriefs mit Dokumentenanhängen**

Der XDS Document Service MUSS beim Einstellen eines eArztbriefs (gemäßig-eab.json in [gemSpec_IG_ePA]) sicherstellen,

- dass alle zusätzlich in der Anfrage enthaltenen Dokumente mit dem enthaltenen eArztbrief-Dokument über die Kennzeichnung als Anhang verbunden werden (`urn:gematik:iti:xds:2025:childDocument/parentDocument`),
- dass kein Dokument (via `urn:gematik:iti:xds:2025:parentDocument`) auf ein Elterndokument referenziert, dass nicht der eArztbrief selbst ist.

und ansonsten die Verarbeitung mit dem Fehler `XDSInvalidAttachmentHierarchy` abbrechen.
[\leq]

Unter anderem müssen also die Anhänge immer direkt unter den Arztbrief "gehängt" werden; ein "Anhang am Anhang" ist nicht erlaubt.

A_27765 -Nachträgliches Anhängen an einen eArztbrief

Der XDS Document Service MUSS ein Anhängen von Dokumenten an einen eArztbrief (gemäßig-eab.json in [gemSpec_IG_ePA]) mit dem Fehler `XDSAttachmentForbidden` ablehnen, wenn die Anhangsbeziehung nicht mit demselben SubmissionSet hergestellt wird, mit dem der eArztbrief eingestellt wird.

[\leq]

Hierdurch wird ein nachträgliches Anhängen von Dokumenten an einen bestehenden Arztbrief über die Operationen Provide and Register Document Set-b oder Restricted Update Document Set unterbunden.

A_27758 -XDS Document Service - Metadatenerweiterung bei neuen elektronischen Arztbriefen

Der XDS Document Service MUSS die Metadaten (DocumentEntry) von neuen Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief) gemäß [gemSpec_IG_ePA] derartig anpassen, dass DocumentEntry.eventCodeList zusätzlich um den aktuellen KDL-Code nach [IG_TI_Terminology] mit den Werten

- code: ED110104,
- codeSystem: [http://dvmd.de/fhir/CodeSystem/kdl/\[version\]](http://dvmd.de/fhir/CodeSystem/kdl/[version]) (präferiert) oder die entsprechende OID,

- displayName: eArztbrief

erweitert wird, wenn dieser nicht bereits vorhanden ist.

[<=]

Dabei muss bei obiger Anforderung "[version]" mit der aktuellen Version der KDL belegt werden, z.B.:

Canonical URL für Version 2025

<http://dvmd.de/fhir/CodeSystem/kdl|2025>

OID für Version 2025

1.2.276.0.76.5.553

3.13.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode

Der Versicherte oder ein Vertreter kann vorhandene Dokumente des Aktenkontos durch die Verwendung der General Deny Policy des Constraint Managements verbergen oder sichtbar machen.

Der Versicherte oder ein Vertreter kann ein neues Dokument auch direkt beim Einstellen in das Aktenkonto verbergen. Dazu wird durch den XDS Document Service beim Einstellen bzw. Aktualisieren (Replace) eines Dokuments der DocumentEntry.confidentialityCode der Dokumentmetadaten ausgewertet. Enthält der confidentialityCode beim Einstellen bzw. Aktualisieren den Wert "CON" (constraint), wird durch das Aktensystem ein Eintrag in der General Deny Policy erzeugt und das Dokument verborgen.

Diese zusätzliche Art des direkten Verbergens ist dabei grundsätzlich nur auf Dokumententypen anwendbar, welche durch einen Versicherten oder einen Vertreter über ein ePA-FdV eingestellt werden können (keine MIOs oder strukturierten Dokumente).

Das Metadatum DocumentEntry.confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491:

1. Führt beim Einstellen und Replace eines Dokuments zum Verbergen des Dokuments, d.h. das Dokument wird auf die General Deny Policy des Aktenkontos gesetzt.
2. Wird im Aktensystem nicht persistiert sondern über dort intern über eine General Deny Policy umgesetzt.
3. Wird im ePA-FdV nicht zur Anzeige gebracht und kann dort auch nicht geändert werden.
4. Eine LEI darf DocumentEntry.confidentialityCode = "CON" nicht verwenden.

3.13.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die Dokumente des Aktenkontos

Wird ein Widerspruch gegen die Nutzung einer Funktion der ePA erklärt, verhindert der XDS Document Service, abhängig von der jeweils widersprochenen Funktion, deren weitere Nutzung.

Im Falle eines Widerspruchs gilt:

5588 **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.

5589 *Hinweis zum Medikationsprozess: Dadurch wird verhindert, dass Leistungserbringer im*
 5590 *Versorgungsprozess veraltete oder unvollständige Daten verwenden.*

5591 **A_23860 -XDS Document Service - Löschen der Dokumente des**
 5592 **Medikationsprozesses**

5593 Der XDS Document Service des Aktensystems MUSS alle Dokumente aus dem Ordner
 5594 elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code =
 5595 "eMP") löschen, wenn der Status der widerspruchsfähigen Funktion "Einstellen von
 5596 Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst" (Id ==
 5597 "erp-submission") auf "Widerspruch erklärt" ("deny") geändert wird. [\leq]

5598 **A_23895-02 -XDS Document Service - Keine Operationen mit Dokumenten des**
 5599 **Medikationsprozesses bei Widerspruch**

5600 Falls ein Widerspruch zur widerspruchsfähigen Funktion "Teilnahme am
 5601 Medikationsprozess" (Id ="medication" und status ="deny") vorliegt, MUSS der XDS
 5602 Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von
 5603 Dokumenten des Ordners elektronischer Medikationsplan (codeSystem =
 5604 "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für alle Nutzer, ausgenommen der
 5605 Versicherte oder befugte Vertreter (oid_versicherter), ablehnen und die Operation mit
 5606 dem Fehlercode ConsentDecisionViolation abrechnen.
 5607 [\leq]

5608 **A_25151-01 -XDS Document Service – Prüfung der Widersprüche bei**
 5609 **Suchanfrage**

5610 Der XDS Document Service MUSS bei einer Suchanfrage die Suchergebnismenge für alle
 5611 Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid_versicherter), filtern
 5612 und sicherstellen, dass diese keinerlei XDS-Metadaten von Dokumenten des Ordners
 5613 elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code =
 5614 "eMP") enthält, wenn ein Widerspruch gegen die widerspruchsfähige Funktion "Teilnahme
 5615 am digital gestützten Medikationsprozess" (Id ="medication" und status ="deny")
 5616 vorliegt.
 5617 [\leq]

5618 **3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des**
 5619 **Medication Service durch eine spezifische LEI auf die Dokumente des**
 5620 **Aktenkontos**

5621 Wird ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische
 5622 LEI erklärt, verhindert der XDS Document Service, dass auf die Dokumente der Kategorie
 5623 "emp" zugegriffen werden kann.

A_26429 -XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für diese LEI, ablehnen und die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.
[<=]

A_26430 -XDS Document Service – Prüfung des Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI bei Suchanfrage

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service bei einer Suchanfrage die Suchergebnismenge für diese LEI filtern und sicherstellen, dass die Suchergebnismenge keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält.
[<=]

3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service

A_24715-02 -XDS Document Service - Protokolleinträge für Zugriffe auf den XDS Document Service

Der XDS Document Service MUSS für die Operationen

- ProvideAndRegisterDocumentSet-b,
- RetrieveDocumentSet,
- RemoveMetadata,
- RestrictedUpdateDocumentSet,
- RegistryStoredQuery (entfällt, wenn Nutzung durch den Versicherten erfolgt)

Protokolleinträge gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 36: XDS Document Service Protokollierung

Strukturelement	Wert	Erläuterung
AuditEvent.type	"document"	
AuditEvent.action	C	Für ProvideAndRegisterDocumentSet-b ohne Replace Option
	U	Für ProvideAndRegisterDocumentSet-b mit Replace Option
	U	Für RestrictedUpdateDocumentSet
	R	Für RegistryStoredQuery

Strukturelement	Wert	Erläuterung
	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"
	"FolderEntryUUID"	<Folder.entryUUID>	wenn in der entity Struktur ein XDSFolder beschrieben wird

Strukturelement	Wert	Erläuterung
Parameterwerte für die Operation RegistryStoredQuery der Schnittstellen I_Document_Management und I_Document_Management_Insurant (nur Vertreter)		
AuditEvent.entity.detail	type	value[x]
	"QueryId"	<Parameter Query ID>
		Der Wert MUSS der Parameter Query ID gemäß [IHE-ITI-TF2]#3.18.4.1.2.4 und für das Aktensystem definierten Anfragetypen entsprechen.
Parameterwerte für die Operation RestrictedUpdateDocumentSet		
<p>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).</p>		

5654 [**<=**]

5655 *Hinweis: In der AuditEvent.entity Struktur sind Dokumente und/oder Folder zu*
5656 *berücksichtigen, die in der zu protokollierenden Operation referenziert werden.*

5657 **A_24925 -XDS Document Service - Protokolleinträge für Zugriffe gleicher Art**

5658 Werden mehrere XDS Dokumente bzw Folder in der zu protokollierenden Operation
5659 referenziert und die Zugriffe sind gleicher Art (AuditEvent.action) KANN der XDS
5660 Document Service einen Protokolleintrag erzeugen, der mehreren AuditEvent.entity
5661 Strukturen enthält. [**<=**]

5662 Das bedeutet, wenn in einer ProvideAndRegisterDocumentSet-b Operation zehn
5663 Dokumente eingestellt werden, kann für diesen Zugriff ein AuditEvent mit zehn Entity
5664 Strukturen erzeugt werden. Werden zehn Dokumente eingestellt und das zehnte
5665 Dokument ersetzt ein bereits vorhandenes, kann in einem Protokolleintrag das Einstellen
5666 (Create) mit neun Entity Strukturen dokumentiert und muss in einem weiteren
5667 Protokolleintrag ein Ersetzen (Update) (zehnte Dokument) protokolliert werden.

5668 **A_25007 -XDS Document Service - Nicht zu protokollierende Zugriffe**

5669 Werden mit der Operation RestrictedUpdateDocumentSet keine geänderten Metadaten
5670 eines referenzierten DocumentEntry gesendet, d.h. die gesendeten Metadateninhalte
5671 unterscheiden sich nicht von bereits persistierten Werten, DARF der XDS Document
5672 Service diesen Zugriff NICHT protokollieren. [**<=**]

5673 **A_27253-01 -XDS Document Service - Nicht zu protokollierende Zugriffe auf Ordner "technical"**

5674 Der XDS Document Service DARF Zugriffe auf den statischen Ordner "technical" oder
5675 dessen Inhalte NICHT protokollieren. [**<=**]
5676

A_27254-01 -XDS Document Service - Protokollierung von Nutzerzugriffen auf den Ordner "technical"

Der XDS Document Service MUSS Nutzerzugriffe auf den Ordner "technical" dann protokollieren, wenn durch den Zugriff Dokumente Protokolldokumente einer ePA-2.6 Aktenkontomigration betroffen sind. Diese Protokollierung MUSS gemäß der Vorgaben in A_24715-* erfolgen.[<=]

3.13.1.14 Unterstützungsleistung für das ePA-FdV

Der XDS Document Service akzeptiert aus Sicherheitsgründen nur bestimmte Dokumentenformate. Das schränkt auch das Format PDF auf bestimmte PDF/A-Varianten ein (siehe auch A_25233*). Daher müssen PDF-Dokumente des Versicherten unter Umständen vor dem Einstellen in die ePA konvertiert werden. Um das ePA-FdV dabei zu entlasten und Komplexität aus dem ePA-FdV zu nehmen, wird eine Funktion angeboten, durch die ein PDF in ein PDF/A konvertiert werden kann. Das ePA-FdV muss aber berücksichtigen, dass die Konvertierung ggf. technisch nicht durchgeführt werden kann oder das Ergebnis der Konvertierung durch ein geändertes Layout ggf. nicht verwendbar ist.

A_25456 -XDS Document Service - Keine negativen Auswirkungen auf Folgekonvertierungen von PDF zu PDF/A

Der XDS Document Service MUSS sicherstellen, dass eine Konvertierung eines PDF-Dokuments sich nicht schädlich auf folgende Konvertierungen auswirken kann.[<=]

Hinweis zu A_25456*: Die Anforderung soll erreichen, dass ein potentiell über ein PDF-Dokument eingebrachter Schadcode nach der Konvertierung gelöscht wird, z.B. durch Zurücksetzen der Sandbox oder der VAU-Instanz

A_25455 -XDS Document Service - Isolation der Konvertierung von PDF zu PDF/A

Der XDS Document Service MUSS die Verarbeitung von PDF-Dokumenten, die im Rahmen der Konvertierung in ein PDF/A durchgeführt wird, in einer separaten VAU-Instanz durchführen, die ausschließlich eine Verbindung zu einem ePA-FdV besitzen darf.[<=]

A_25454 -XDS Document Service - Realisierung der Schnittstelle I_Tool_Convert_PDF_Insurant

Der XDS Document Service MUSS die Operationen der Schnittstelle I_Tool_Convert_PDF_Insurant gemäß [I_Tool_Convert_PDF_Insurant] umsetzen[<=]

A_26129 -ePA-Aktensystem - Rahmenbedingungen bei Nutzung einer Service-VAU für PDF-Konvertierung

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die vom ePA-FdV übermittelten PDF-Dokumente in der Aktenkontoverwaltungs-VAU ausschließlich weitergeleitet aber ansonsten nicht verarbeitet werden. Gleiches gilt für die von der Service-VAU an das ePA-FdV übermittelten konvertierten PDF/A-Dokumente.[<=]

A_26130 -ePA-Aktensystem - maximale Lebensdauer einer Service-VAU für PDF-Konvertierung

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die Lebensdauer einer solchen Service-VAU-Instanz maximal 12 Stunden beträgt.[<=]

A_26131 -ePA-Aktensystem - Keine Speicherung von in der Service-VAU für PDF-Konvertierung verarbeiteten Daten

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass weder die vom ePA-FdV übermittelten und zu konvertierenden PDF-Dokumente noch die daraus konvertierten PDF/A-Dokumente von der "PDF-VAU" im ePA-Aktensystem gespeichert werden. [\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 ImplementierungsvorgabenAnforderungen 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 ImplementierungsvorgabenAnforderungen des FHIR Implementation Guide für den Medication Service [IG_Medication_Service] umsetzen. [\leq]

5756 A_26317 -Medication Service - Erzeugung eines xHTML-Exports

5757 Der Medication Service MUSS gemäß den Vorgaben von [IG_Medication_Service] für die
5758 Generierung der Medikationsliste im xHTML-Format nach [XHTML] sicherstellen, dass
5759 kein ausführbarer Code im Export enthalten ist. [≤]

**5760 A_24820 -Medication Service - Ablehnung von Request bei vorliegendem
5761 Widerspruch**

5762 Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID !=
5763 oid_erp-vau, oid_versicherter mit dem HTTP Status Code 423 (LOCKED) abbrechen,
5764 sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess")
5765 mit der Funktion ("medication") die Entscheidung ("deny") gesetzt ist. [≤]

**5766 A_25152 -Medication Service - Ablehnung neuer Daten bei vorliegendem
5767 Widerspruch**

5768 Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID ==
5769 oid_erp-vau mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent
5770 Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion
5771 ("erp-submission") die Entscheidung ("deny") gesetzt ist. [≤]

5772 A_25153 -Medication Service - Löschen der Daten des Medication Service

5773 Der Medication Service MUSS alle vorhandenen fachlichen Daten des Medication Service
5774 löschen, wenn im Consent Decision Management in der Funktionsklasse
5775 ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny")
5776 gesetzt wird. [≤]

**5777 A_26399 -Medication Service - Ablehnung von Request bei vorliegendem
5778 Widerspruch gegen die Nutzung durch eine spezifische LEI**

5779 Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID
5780 gemäß A_26406-* mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im
5781 Consent Decision Management die LEI der User Session in der User Specific Deny Policy
5782 des Medication Service enthalten ist. [≤]

5783 A_24841-03 -Medication Service - Schemavalidierung

5784 Der Medication Service MUSS im Body der HTTP-POST-Operation die übertragenen
5785 Parameter auf Schadcode prüfen und fachfremde Daten (d.h. Schemavalidierung) prüfen
5786 und im Fehlerfall das Ausführen der Operation mit dem HTTP Status Code 400
5787 abbrechen. [≤]

**5788 A_27894 -Medication Service - Nutzung der FHIR-Operationen durch den E-
5789 Rezept-Fachdienst**

5790 Der Medication Service MUSS sicherstellen, dass die folgenden FHIR-Operationen
5791 ausschließlich durch den E-Rezept-Fachdienst mit der professionOID oid_erp-vau genutzt
5792 werden dürfen:

- 5793 • providePrescription_MedicationSvc
- 5794 • cancelPrescription_MedicationSvc
- 5795 • provideDispensation_MedicationSvc
- 5796 • cancelDispensation_MedicationSvc.

5797 [≤]

**5798 A_24849-05 -Medication Service - Protokolleinträge für Zugriffe auf den
5799 Medication Service**

5800 Der Medication Service MUSS einen Protokolleintrag gemäß A_24704* erzeugen und
5801 dabei folgende Wertebelegung berücksichtigen:

5802 **Tabelle 38: Medication Service Protokollierung**

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_R ender und FHIR Query API	Wert	Erläuterung
type		"rest"	
action	OperationId: providePrescription_Medicatio nSvc	"C"	Einstellen von Verschreibungs daten
	OperationId: provideDispensation_Medicatio nSvc	"C"	Einstellen einer Medikamentena bgabe
	OperationId: cancelPrescription_Medication Svc	"U"	Stornieren von Verschreibungs daten
	OperationId: cancelDispensation_Medicatio nSvc	"U"	Stornieren einer Medikamentena bgabe
	OperationId: getMedicationList_MedicationS vc	"R"	Abruf der Medikationsliste
	OperationId: renderMedicationListToHTML_ MedicationSvc	"R"	Abruf der Medikationsliste im HTML- Format
	OperationId: renderMedicationListToPDF_M edicationSvc	"R"	Abruf der Medikationsliste im PDF-Format
	OperationId: listMedications_MedicationSvc	"R"	Abruf von Medikamenten informationen
	OperationId: listMedicationDispenses_Medic ationSvc	"R"	Abruf von Medikamentena bgabeinformatio nen

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_R ender und FHIR Query API	Wert	Erläuterung
	OperationId: listMedicationRequests_MedicationSvc	"R"	Abruf von Verschreibungsinformationen
	<u>OperationId: listMedicationStatements_MedicationSvc</u>	<u>"R"</u>	<u>Abruf von Medikationsinformationen</u>
	<u>OperationId: listOrganizations_MedicationSvc</u>	<u>"R"</u>	<u>Abruf von Leistungserbringereinrichtungen</u>
	<u>OperationId: listPractitioners_MedicationSvc</u>	<u>"R"</u>	<u>Abruf von Leistungserbringern</u>
	<u>OperationId: listPractitionerRoles_MedicationSvc</u>	<u>"R"</u>	<u>Abruf von Zuordnungen von Leistungserbringenden zu Leistungserbringereinrichtungen</u>
	<u>OperationId: listProvenances_MedicationSvc</u>	<u>"R"</u>	<u>Abruf von Änderungs- oder Medikationsplan chronologieeinträgen</u>
	OperationId: addEMLEntry_MedicationSvc	"C"	Eintrag in Medikationsliste hinzufügen
	OperationId: updateEMLEntry_MedicationSvc	"U"	Eintrag in Medikationsliste aktualisieren
	OperationId: addEMPEntry_MedicationSvc	"C"	Eintrag in Medikationsplan hinzufügen

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_R ender und FHIR Query API	Wert	Erläuterung
	OperationId: updateEMPEntry_MedicationSvc	"U"	Eintrag in Medikationsplan aktualisieren
	OperationId: linkEMP_MedicationSvc	"U"	Eintragsverknüpfung Medikationsplan /Medikationsliste
	OperationId: unlinkEMP_MedicationSvc	"U"	Aufhebung Eintragsverknüpfung Medikationsplan /Medikationsliste
	OperationId: renderMedicationListToPDFrenderMedicationPlanToPDF_MedicationSvc	"R"	Abruf des Medikationsplans im PDF- Format
	OperationId: getMedicationPlan_MedicationSvc	"R"	Abruf des Medikationsplans
	OperationId: getMedicationPlanChronologyLog_MedicationSvc	"R"	Abruf der Medikationsplan chronologie
entity.name		"Medication Service"	Service Name
entity.description		<operationId>	operationId der ausgeführten Operation
Nur bei FHIR Query API:			
entity.detail.type		"search-parameters"	

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_R ender und FHIR Query API	Wert	Erläuterung
entity.detail.value [x]		<ResourceName>?parameter1=<value>¶meter2=<value>& ...mehr	Suchkriterien in URL-Query-Notation

5803

5804

5805

Falls ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF der Medication Service einen Protokolleintrag NICHT erzeugen. [**<=**]

5806

5807

5808

5809

5810

5811

Ereignisse, die gemäß A_26298* zu einer Übertragung neuer oder geänderter Daten an das FDZ führen, erzeugen grundsätzlich einen eigenen Protokolleintrag für den Vorgang gemäß der Vorgaben in A_24849*. Liegt kein Widerspruch des Versicherten gegen die Übermittlung der Daten an das FDZ vor und ist eine Übertragung der Daten des Ereignisses aufgrund der Pseudonymisierbarkeit dieser Daten möglich, so folgt auf das ursächliche Ereignis automatisch der Export der pseudonymisierten Daten.

5812

5813

5814

5815

5816

5817

Diese Übertragung der Daten muss für einen Versicherten aus der Protokollierung ersichtlich sein. Anstelle eines dedizierten Protokolleintrags für die Datenübertragung wird die Datenübertragung als ergänzendes entity.detail des auslösenden Ereignisses protokolliert. Aus dem Protokolleintrag des Ereignisses ist dann ersichtlich, ob die betroffenen Daten in pseudonymisierter Form auch der sekundären Datennutzung zugeführt wurden.

5818

5819

5820

5821

5822

5823

5824

A_27188 -Medication Service - Protokollierung des Datenexports an das FDZ

Der Medication Service MUSS einen Protokolleintrag gemäß A_24849* um das folgend aufgeführte entity.detail mit dem Wert true ergänzen, wenn aus der Operation eine Übertragung von Daten an das FDZ folgt. Diese Ergänzung MUSS entweder den Wert false haben oder entfallen, wenn aus der Operation keine Übertragung von Daten an das FDZ folgt.

Strukturelement		Wert	Erläuterung
entity.detail.type		"data-submission"	Export an das Forschungsdatenzentrum
entity.detail.value[x]		"true" oder "false"	

5825

[**<=**]

5826

3.13.2.3 MHD Service

5827

5828

5829

A_27667-01 -MHD Service - Realisierung der Schnittstellen des FHIR IG MHD

Der MHD Service MUSS die **ImplementierungsvorgabenAnforderungen** des FHIR Implementation Guide für den MHD Service [IG_MHD_Service] umsetzen. [**<=**]

5830

5831

Hinweis zu A_27667-*: Auch für den MHD Service sind die übergreifenden Anforderungen A_15159 zum Schutz gegen die OWASP Risiken und A_24783 zur

5832 Eingabevalidierung zu berücksichtigen, um zu verhindern, dass Schadcode über
5833 Suchanfragen ins Aktensystem eingebracht werden kann.

5834 **A_27892 -MHD Service - Durchsetzen der Zugriffskontrolle für XDS Document**
5835 **Service**

5836 Der MHD Service MUSS bei einer Suchanfrage durch einen Nutzer alle Zugriffsregeln
5837 durchsetzen, die für den Zugriff dieses Nutzers bzgl. des XDS Document Service
5838 gelten. [\leq]

5839 Hinweis zu A_27892-*: Nutzer dürfen durch den MHD Service keinen Zugriff auf
5840 Dokumente erhalten, auf den sie über den XDS Document Service nicht zugreifen
5841 dürften. So dürfen Nutzer mittels des MHD Services keinen Zugriff auf Dokumente einer
5842 Dokumentenkategorie erhalten, auf die sie nach der Legal Policy nicht zugreifen dürfen.
5843 Genauso dürfen sie über den MHD Service keine Dokumente finden, die auf der General
5844 Deny Policy stehen.

5845 **A_27668 -MHD Service - Filtern von verborgenen Metadaten und Dokumenten**

5846 Der MHD Service MUSS bei einer Suchanfrage bei jedem Dokument einer verborgenen
5847 Datenkategorie die Metadaten (bzw. korrespondierende FHIR-Ressource
5848 DocumentReference filtern sowie den Dokumentenabruf
5849 ausDocumentReferences.content.attachment.url verhindern (HTTP Code 404 not
5850 found). [\leq]

5851 **A_27669 -MHD Service – Protokolleinträge für Zugriffe auf den MHD Service**

5852 Der MHD Service MUSS einen Protokolleintrag gemäß A_24704* erzeugen und dabei
5853 folgende Wertebelegung berücksichtigen:

5854
5855

5856 **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"	

Strukturelement [AuditEvent.]	Operationen der FHIR Query API	Wert	Erläuterung
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 Dienstübergreifende Festlegungen

A_27886 -~~FHIR Data Service~~ – Durchführung von Datenbestandsmigrationen **FHIR Data Service – Durchführung von Datenmigrationen**

Wenn Migrationsvorgaben für den Datenbestand eines FHIR Data Services für verschiedene Versionen des Services existieren, MUSS der FHIR Data Service alle bislang nicht angewandten Datenbestandsmigrationsvorgaben Datenmigrationsvorgaben 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.
[≤]

A_28039 -FHIR Data Service – Aktenkontostatus bei fehlerhafter Datenmigration

Wenn bei der Durchführung von Migrationen gemäß A_27886* Fehler auftreten, die eine Migration des Datenbestands verhindern, MUSS das ePA-Aktensystem in den Aktenkontostatus MAINTENANCE wechseln und einen entsprechenden Fehler zurückgeben. [≤]

Die verschiedenen Schnittstellen (z. B. XDS Document Service oder Consent Decision Management Service) definieren konkrete Fehlercodes.

A_28042 -FHIR Data Service – Erneute Datenmigration

Falls das ePA-Aktensystem aufgrund einer fehlgeschlagenen Datenmigration gemäß A_28039* im Status MAINTENANCE ist, MUSS das ePA-Aktensystem in der Lage sein, die Datenmigration erneut anzustoßen. Wenn die Datenmigration dann erfolgreich beendet werden kann, MUSS das ePA-Aktensystem wieder den Aktenkontostatus ACTIVATED gesetzt werden (ansonsten verbleibt es im Status MAINTENANCE). [≤]

Das Ziel ist es, bei fehlgeschlagenen Datenmigrationen durch eine angepasste Software und/oder Spezifikation mit einem weiteren Versuch die erfolgreiche Durchführung zu ermöglichen. Der Auslöser, einen neuen Datenmigrationsversuch zu unternehmen, kann bspw. ein abgelaufener Timer sein ("mindestens 24h seit dem letztem Versuch") oder das Einspielen einer neuen ePA-Aktensystemsoftware-Version. Die Datenmigration kann nur erneut angestoßen werden, wenn das Aktenkonto geöffnet ist, sich also ein Benutzer im Aktenkonto angemeldet hat.

5894 Ansonsten kann der Status MAINTENANCE nur über einen Anbieterwechsel (Status
 5895 SUSPENDED) oder mit dem Widerspruch zur Nutzung der ePA über den Status UNKNOWN
 5896 verlassen werden.

5897 3.14 Audit Event Service

5898 Ereignisse und Zugriffe auf die ePA eines Versicherten werden im ePA Aktensystem
 5899 protokolliert. Die Protokollierung dient der Datenschutzkontrolle für den Versicherten.
 5900 Der Audit Event Service ist ein FHIR Data Service und ermöglicht dem Versicherten,
 5901 befugten Vertretern bzw. der Ombudsstelle den Zugriff auf diese Protokollinformationen.

5902 **A_24704-02 -Audit Event Service - Realisierung der Schnittstelle des FHIR IG** 5903 **ePA Basisfunktionalitäten**

5904 Der Audit Event Service MUSS die ImplementierungsvorgabenAnforderungen des FHIR
 5905 Implementation Guide ePA Basisfunktionalitäten (Audit Event Service) gemäß
 5906 [IG_Basic] umsetzen. [\leq]

5907 In der Struktur eines Protokolleintrages (AuditEvents) sind folgende
 5908 Zugriffsinformationen hinterlegt:

5909 **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

5910 Die spezifische Befüllung eines Audit Events gemäß A_24704* wird durch die jeweiligen
 5911 Services vorgegeben. Allgemeine Elemente sind wie folgt zu befüllen:

5912 **A_25154-04 -ePA-Aktensystem - Befüllung der Elemente recorded, agent und** 5913 **source eines Audit Events**

5914 Das ePA-Aktensystem MUSS die Audit Event Elemente AuditEvent.recorded,
 5915 AuditEvent.agent und AuditEvent.source wie folgt befüllen.

5916 **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"

Element [AuditEvent.]		Beschreibung	Beispiel
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"

Element [AuditEvent.]		Beschreibung	Beispiel
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:1.3.6.1.4.1.12559.1 1.10.1.3.2.2.2"
	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"

Element [AuditEvent.]		Beschreibung	Beispiel
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"

5917
5918
5919

Hinweis:

5920 agent[client]: Angaben zur Applikation, z. B. eRezept-Fachdienst, NCPeH
 5921 agent[user]: Angaben zu LEI oder Vertreter oder Versicherter
 5922 agent[internal]: Angaben zu systemeigenen Prozessen, z. B. Datenexport für das FDZ
 5923 [\leq]

5924 **A_27689 -Protokollierung von nicht erfolgreichen Zugriffen**

5925 Falls für eine Operation ein Protokolleintrag gefordert ist und mit einem Fehler
 5926 abgebrochen wird, MUSS der Audit Event Service jeweils einen Protokolleintrag gemäß
 5927 A_24704* erzeugen. Darüberhinaus und ergänzend zu den Vorgaben aus dem Profil
 5928 EPAAuditEvent gemäß [IG_Basic] sind folgende Werte entsprechend zu belegen:

5929 **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

5930 Falls ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF bei
 5931 nicht erfolgreichen Zugriffen ein Protokolleintrag NICHT erzeugt werden.

5932 Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A_25172* entfällt, wenn ein
 5933 Protokolleintrag mangels eines befugten Nutzers (kein Bezug des
 5934 SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann.
 5935 [\leq]

5938 **A_24503 -ePA-Aktensystem - Aufbewahrungsdauer der Protokolleinträge**

5939 Das ePa-Aktensystem MUSS die zum Zwecke der Datenschutzkontrolle für den
 5940 Versicherten erstellten
 5941 Protokolleinträge für drei Jahre aufbewahren. Danach sind sie vom Aktensystem
 5942 automatisch zu löschen. [\leq]

5943 Die Protokolleinträge können durch den Versicherten oder durch einen befugten Vertreter
 5944 mittels ePA-FdV eingesehen werden. Versicherte ohne ePA-FdV können bei ihrer
 5945 zuständigen Ombudsstelle beantragen, die Protokolldaten zur Verfügung gestellt zu
 5946 bekommen.

5947 Für eine Abfrage der Protokolleinträge als strukturierte Einträge nutzen ein ePA-FdV und
5948 die Ombudsstelle den Audit Event Service [IG_Basic].

5949 **A_24714-01 -Audit Event Service - Realisierung der Query API: AuditEvent**
5950 Der Audit Event Service MUSS die "Query API: AuditEvent" des FHIR Implementation
5951 Guide für den Audit Event Service [IG_Basic] umsetzen. [<=]

5952 **A_24750-02 -Audit Event Service - Realisierung der Render API: PDF Audit**
5953 Der Audit Event Service MUSS die "Render API: PDF Audit" des FHIR Implementation
5954 Guide für den Audit Event Service [IG_Basic] umsetzen. [<=]

5955 **A_25172 -Audit Event Service - Speicherung der Protokolldaten**
5956 Der Audit Event Service MUSS die Daten der Protokolleinträge verschlüsselt im
5957 SecureDataStorage persistieren. [<=]

5958 Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A_25172* entfällt, wenn ein
5959 Protokolleintrag mangels eines befugten Nutzers (kein Bezug des
5960 SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann.

5961 **A_25018 -Audit Event Service - PAdES-Signatur in renderAuditEventsToPDF**
5962 Der Audit Event Service MUSS bei der Operation `renderAuditEventsToPDF` beim
5963 Signieren eines Protokolls im PDF/A-Format eine PAdES-Signatur gemäß [PAdES-3] und
5964 [PAdES Baseline Profile] erstellen. Bei der Signaturerstellung ist das Attribut `signing`
5965 `certificate reference` gemäß den Vorgaben aus [PAdES-3] Kapitel 4.4.3 „Signing
5966 Certificate Reference Attribute“ anzulegen. [<=]

5967 Durch die Baseline-Profilierung [PAdES Baseline Profile] wird festgelegt, wie der
5968 Signaturzeitpunkt, gemessen als Systemzeit des ePA-Aktensystems, in die Signatur
5969 eingebracht wird.

5970 **A_24991 -Audit Event Service – Protokollierung von Zugriffen auf die**
5971 **Protokolldaten**
5972 Der Audit Event Service MUSS für die Zugriffe der Ombudsstelle oder eines Vertreters auf
5973 die protokollierten Daten jeweils einen Protokolleintrag gemäß A_24704* erzeugen.

5974 **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"> • listAuditEvents • getAuditEventById • renderAuditEventsToPDF 	operationId der zu protokollierenden Operation

Strukturelement	Wert		Erläuterung
AuditEvent.entity.detail	type	value[x]	
	parameters	parameter1=<value>¶meter2=<value>& ...mehr	Nur bei getAuditEventList
	identifizier	<id> des AuditEvents	Nur bei getAuditEvent

5975 [**<=**]

5976 *Hinweis: Zugriffe des Versicherten auf die Protokolle des Aktenkontos werden nicht*
 5977 *protokolliert.*

5978

5979 3.15 Information Service

5980 3.15.1 Information Service

5981 Der Information Service ist ohne die Nutzung eines VAU-Kanals nutzbar. Die über den
 5982 Information Service genutzten Daten sind ausschließlich persistierte Daten des
 5983 Aktenkontos, die weder mit dem SecureAdminStorageKey noch mit dem
 5984 SecureDataStorageKey gesichert sind.

5985 Der Zugang erfolgt durch Nutzung der Schnittstelle `I_Information_Service`.

5986 **A_24344 -Information Service - Realisierung der Schnittstelle**

5987 **`I_Information_Service`**

5988 Der Information Service MUSS die Operationen der Schnittstelle `I_Information_Service`
 5989 gemäß [`I_Information_Service`] umsetzen. [**<=**]

5990 **A_24345 -Information Service - Kein Zugriff auf verschlüsselte Daten des** 5991 **Aktenkontos**

5992 Der Information Service DARF NICHT auf Daten zugreifen, die nicht explizit für die
 5993 Verwendung durch den Informationsdienst bereitgestellt wurden. Dazu gehören
 5994 insbesondere alle Daten des Aktenkontos, die mit den versichertenindividuellen
 5995 Schlüsseln zur Daten- oder Befugnispersistierung (`SecureDataStorageKey` oder
 5996 `SecureAdminStorageKey`) gesichert sind. [**<=**]

5997 3.15.1.1 Informationen zu Widersprüchen (Consent Decisions)

5998 Die Widersprüche eines Versicherten gegen die Nutzung von Funktionen der
 5999 elektronischen Patientenakte werden durch das Consent Decision Management gesichert
 6000 administriert. Änderungen an den Widersprüchen erfolgen dort.

6001 Der Information Service bietet für die Nutzergruppen der ePA eine einfache
 6002 Abfragemöglichkeit der aktuell erteilten oder nicht erteilten Widersprüche auch ohne die
 6003 Nutzung des Consent Decision Managements an. Liegt ein Widerspruch gegen die

6004 Nutzung einer Funktion vor, kann auf die Ausführung der zur Nutzung dieser Funktion
6005 notwendigen Aktionen mit der ePA eines Versicherten durch den Client verzichtet
6006 werden.

6007 Für diese vereinfachte Abfragemöglichkeit der aktuellen Widersprüche verwendet der
6008 Information Service den durch das Consent Decision Management persistent
6009 übertragenen Zustand der Widersprüche ("Cache" des Zustands der Widersprüche).
6010 Berücksichtigt wird dabei die Widerspruchsinformation, für die eine vereinfachte Abfrage
6011 vorgesehen ist (Widersprüche der Klasse "Versorgungsprozess").

6012 **3.15.1.2 Informationen zur Anwenderperformance (UX Performance)**

6013 Der Information Service stellt für die Umgebung der Leistungserbringer die Operation zur
6014 Sammlung der Messwerte zu den Anwendungsfällen der Nutzererfahrung zur Verfügung.
6015 Die Weiterverarbeitung der gesammelten Daten ist in 2.8- Performance aus
6016 Anwendersicht definiert und vorgegeben.

6017 **3.15.2 Information Service - Account**

6018 Die Operationen der Information Service - Account werden für den Umzug eines
6019 existierenden Aktenkontos zu einem neuen Anbieter verwendet. Die Nutzung der
6020 Operationen erfolgt exklusiv durch die Aktensystembetreiber.

6021 Die Verwendung der einzelnen Operationen erfolgt im Verbund mit den Operationen der
6022 Schnittstelle I_Health_Record_Relocation_Service für die Umsetzung der
6023 Anwendungsfälle eines automatischen Aktenkontoumzugs und sind in 3.2- Health Record
6024 Relocation_Service erläutert.

6025 **A_24424 -Information Service Account - Realisierung der Schnittstelle** 6026 **I_Information_Service_Accounts**

6027 Der Information Service MUSS die Operationen der Schnittstelle
6028 I_Information_Service_Accounts gemäß [I_Information_Service_Accounts]
6029 umsetzen. [<=]

6030 **A_24665 -Information Service Account - Nutzung beidseitig authentisiertes TLS**

6031 Der Information Service MUSS sicherstellen, dass die Operationen der Schnittstelle
6032 I_Information_Service_Accounts ausschließlich unter Verwendung einer beidseitig
6033 authentisierten TLS-Verbindung zwischen den beteiligten Aktensystemen genutzt werden
6034 und die Operationen ansonsten abgebrochen und mit einer Fehlermeldung gemäß
6035 Vorgaben in [I_Information_Service_Accounts] beantwortet werden. [<=]

6036 **A_25054 -Information Service Account - Gegenseitige Authentisierung** 6037 **Aktensysteme**

6038 Die Information Service Account Dienste der Aktensysteme MÜSSEN sich mit der TLS-
6039 Identität mit professionOID oid_epa_mgmt mittels des Zertifikats C.FD-TLS-S gegenseitig
6040 authentisieren.
6041 [<=]

6042 **A_25053 -Information Service Account - Prüfung der TLS-Zertifikate**

6043 Der Information Service Account MUSS bei der Authentifizierung eines jeweils anderen
6044 Aktensystems die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC_PKI_018
6045 durchführen. Zur Prüfung des TLS-Zertifikats C.FD-TLS-S sind dabei die
6046 Parameter PolicyList=oid_fd_tls_s, IntendedKeyUsage=digitalSignature,
6047 intendedExtendedKeyUsage=id-kp-serverAuth, OCSP-Graceperiod=60 Minuten, Offline-
6048 Modus=nein zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD-TLS-C sind dabei die
6049 Parameter PolicyList=oid_fd_tls_c, IntendedKeyUsage=digitalSignature,
6050 intendedExtendedKeyUsage=id-kp-clientAuth, OCSP-Graceperiod=60 Minuten, Offline-

6051 Modus=nein zu verwenden.
6052 [\leq]

6053 3.16 Email Management

6054 Das Email Management ermöglicht einem FdV-Nutzer die Verwaltung seiner E-Mail-
6055 Adresse und einem Kostenträger die Verwaltung von E-Mail-Adressen von Versicherten,
6056 die bei diesem Kostenträger versichert sind.

6057 Die Schnittstelle zum Verwalten der E-Mail-Adressen durch den Kostenträger dient dem
6058 ausschließlichen Zweck des Einstellens, Lesens und der Änderung von E-Mail-Adressen
6059 auf Verlangen des Versicherten. Dies ermöglicht dem Kostenträger, seinen Versicherten
6060 die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte auf Berichtigung und
6061 Auskunft bzgl. der im Aktensystem verarbeiteten E-Mail-Adresse zu gewährleisten.

6062 Für einen Versicherten kann nur genau eine E-Mail Adresse hinterlegt werden.

6063 **A_25435 -Email Management - Realisierung der Schnittstelle**

6064 **I_Email_Management**

6065 Das Email Management MUSS die Operationen der Schnittstelle `I_Email_Management`
6066 gemäß `[I_Email_Management]` umsetzen.[\leq]

6067 **A_25438 -Email Management - Beschränkung der Schnittstellenoperationen auf** 6068 **E-Mail-Adressen des FdV-Nutzers**

6069 Das Email Management MUSS die Operationen der Schnittstelle `I_Email_Management`
6070 gemäß `[I_Email_Management]` auf die E-Mail-Adresse des aufrufenden Nutzers
6071 einschränken, sofern der Nutzer ein FdV-Nutzer ist.[\leq]

6072 **A_26161 -Email Management - Nutzen von Email Management auch bei** 6073 **Widerpruch**

6074 Das Email Management MUSS sicherstellen, dass das Email Management auch von
6075 Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben.[\leq]

6076 **A_26162 -Email Management - Versicherte nutzen Email Management** 6077 **ausschließlich im Home-AS**

6078 Das Email Management des ePA-Aktensystems MUSS sicherstellen, dass das Email
6079 Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-
6080 Aktensystem das Home-AS ist.[\leq]

6081 Hinweis: Für das Email Management ist auch Anforderung A_26154* umzusetzen.

6082 **A_25439 -Email Management - Kostenträger kann ausschließlich E-Mail-** 6083 **Adressen der eigenen Versicherten verwalten**

6084 Das Email Management MUSS sicherstellen, dass ein Kostenträger mittels der
6085 Operationen der Schnittstelle `I_Email_Management` gemäß `[I_Email_Management]`
6086 ausschließlich E-Mail-Adressen von Versicherten verwalten kann, die beim Kostenträger
6087 versichert sind.[\leq]

6088 **A_25440-01 -Email Management - Benachrichtigung bei Änderung der E-Mail-** 6089 **Adresse**

6090 Falls eine E-Mail-Adresse a) ersetzt oder b) ergänzt wird, MUSS das Device Management
6091 bei a) eine E-Mail an die alte und die neue E-Mail-Adresse senden und bei b) eine E-Mail
6092 an die neue E-Mail-Adresse senden, in der bei a) über die Ersetzung bzw. bei b) die
6093 Ergänzung einer E-Mail-Adresse informiert wird. In der E-Mail MUSS darüber informiert
6094 werden, wann und ob der FdV-Nutzer selbst oder der Kostenträger die E-Mail ersetzt
6095 bzw. ergänzt hat.[\leq]

6096 **A_25441 -Email Management - Information bzgl. der Ergänzung bei E-Mail-**
6097 **Adressen**

6098 Das Email Management MUSS sicherstellen, dass der FdV-Nutzer für eine im Email
6099 Management hinterlegte E-Mail-Adresse erkennen kann, wann und von wem diese E-
6100 Mail-Adresse ergänzt wurde. [<=]

6101 **A_25968-01 -Email Management - Maximale Anzahl E-Mail-Adressen**

6102 Das Email Management MUSS sicherstellen, dass für einen Nutzer maximal eine E-Mail-
6103 Adresse hinterlegt werden kann. [<=]

6104 **A_26163 -Email Management - Keine Persistierung einer im Rahmen der**
6105 **Vertretereinrichtung übergebenen E-Mail-Adresse**

6106 Das Email Management MUSS sicherstellen, dass eine im Rahmen des Anwendungsfalls
6107 der Vertreterereinrichtung vom Nutzer übermittelte E-Mail-Adresse nicht persistiert und
6108 spätestens bei Beendigung der User Session gelöscht wird. [<=]

6109 **A_26164 -Email Management - Keine Geräteregistrierung mit der im Rahmen**
6110 **der Vertreterereinrichtung übergebenen E-Mail-Adresse**

6111 Das Email Management MUSS sicherstellen, dass keine E-Mail-Adressen zur Übermittlung
6112 eines Geräteregistrierungscodes genutzt werden, die dem ePA-Aktensystem im Rahmen
6113 des Anwendungsfalls der Vertreterereinrichtung übermittelt wurden. [<=]

6114 Hinweis zu A_26163 und A_26164: Die im Rahmen des Anwendungsfalls der
6115 Vertreterereinrichtung übermittelte E-Mail-Adresse wird ausschließlich zur Information des
6116 Vertreters über die Einrichtung der Vertretung genutzt (vgl. A_24755-*).

6117 **3.17 Zusätzliche Anforderungen an den Authorization Service**

6118 Der ePA Authorization Service wird sowohl für die Authentisierung der Versicherten über
6119 das FdV als auch für die Authentisierung von Leistungserbringern und Kostenträgern über
6120 deren Primärsystem benötigt. Ebenso muss die Zugriffsautorisierung für andere
6121 Fachdienste wie z.B. E-Rezept geprüft werden. Die Festlegungen für den Authorization
6122 Server finden sich in [gemSpec_IDP_FD]. Dieser Abschnitt des vorliegenden Dokuments
6123 enthält spezifische Anforderungen, die vom Authorization Service des Aktensystems
6124 zusätzlich umzusetzen sind.

6125 **A_24923 -Authorization Service - I_Authorization_Service**

6126 Der Authorization Service MUSS die Operationen der
6127 Schnittstelle `I_Authorization_Service` implementieren gemäß
6128 `[I_Authorization_Service]`. [<=]

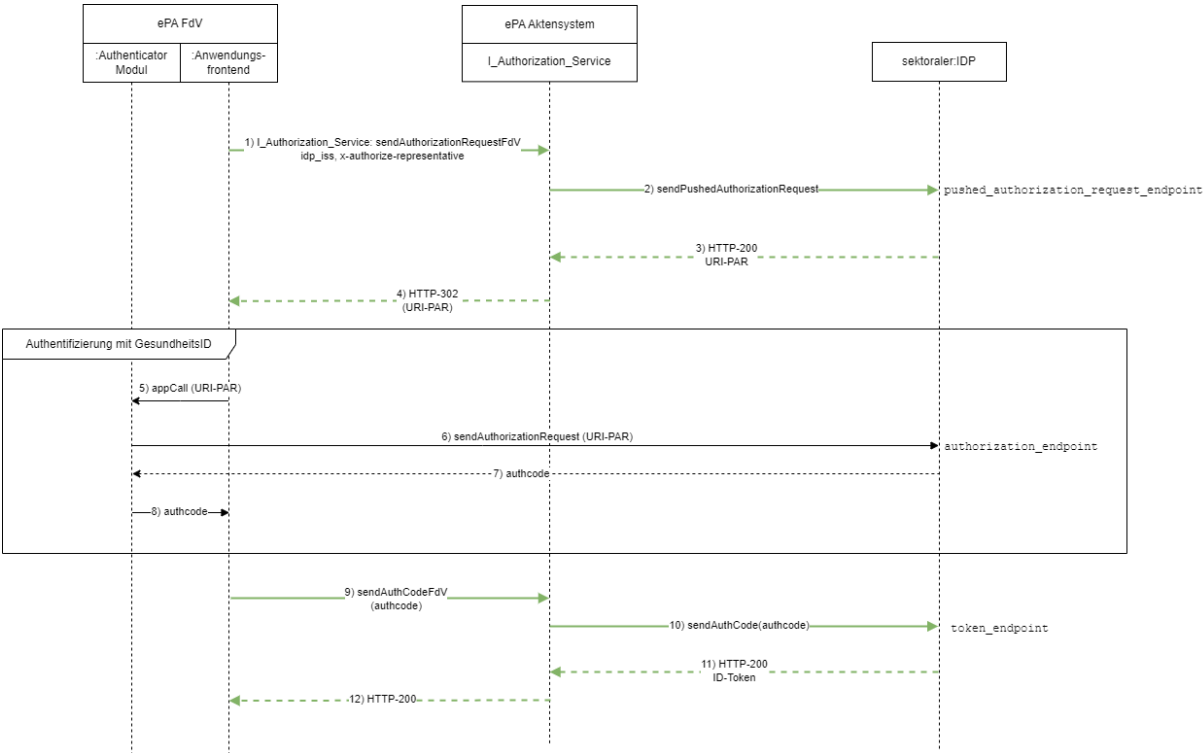
6129 **A_25283 -Authorization Service - Konvertieren von ID-Token**

6130 Der Authorization Service MUSS sicherstellen, dass für ein nach erfolgreicher
6131 Authentifizierung des Nutzers vorliegendes ID-Token mittels Regel `rr0` gemäß
6132 `Tab_AS_Entitlement_Registration_Rules` ein HSM-ID-Token erstellt wird, bevor das ID-
6133 Token zeitlich ungültig ist. [<=]

6134 **3.17.1 Anforderungen an den Authorization Service für die**
6135 **Authentisierung von Versicherten (FdV)**

6136 Im Rahmen der Authentisierung des Versicherten erfolgt die Prüfung der
6137 Geräteregistrierung (Verifikation) direkt. Das Gerät muss dafür die Geräteparameter
6138 eines zuvor ausgeführten und bestätigten Registrierungsprozesses verwenden

6139 Bisher nicht registrierte Geräte, bzw. Geräteparameter einer bisher nicht bestätigten
6140 Geräteregistrierung, können unter Verwendung des Device Management registriert, bzw.
6141 bestätigt werden (siehe Kapitel3.12- Device Management).
6142



6143
6144 **Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP**

6145 **A_25717-03 -Authorization Service - Pushed Authorization-Request des**
6146 **Authorization Service an sektorale Identity Provider**

6147 Der ePA Authorization Service MUSS den Pushed Authorization Request (PAR) am durch
6148 den vom ePA-FdV übergebenen Parameter idp-iss adressierten sektoralen IDP gemäß
6149 [gemSpec_IDP_FD#AF_10117] mit folgenden Parametern aufrufen:

Parameter	Wert	Anmerkung
scope	"openid urn:telematik:display_name urn:telematik:versicherter urn:telematik:family_name urn:telematik:given_name"	Notwendige Scopes für den Zugriff für die Autorisierung von Nutzern am ePA- Aktensystem
acr_values	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung

Parameter	Wert	Anmerkung
redirect_uri	Inhalt des Parameters x-redirecturi [sendAuthorizationRequestFdV in I_Authorization_Service], andernfalls eine herstellerspezifische Standard-redirect_uri.	Diese URI muss unter dem claim redirect_uris im Entity Statement des Authorization Service enthalten sein. Mandanten, welche eine eigene redirect_uri verwenden [sendAuthorizationRequestFdV in I_Authorization_Service], müssen diese im Rahmen des Registrierungsprozesses beim Authorization Service bekannt geben.

6150 [**<=**]

6151 Hinweis 1: An die redirect_uri im Pushed Authorization Request sendet der sektorale IDP
6152 den ausgestellten Authorization Code (siehe [gemSpec_IDP_Sek])

6153 Hinweis 2: Der Redirectaufruf, der vom Authenticator Modul an die redirect_uri
6154 ausgeführt wird, wird vom ePA-FdV über Plattformmechanismen (deeplink/universallink)
6155 gefangen und stellt selbst einen POST-Request an den Endpunkt des Authorization
6156 Service.

6157 **A_26584 -Authorization Service - Liste der redirect_uris im Entity Statement**

6158 Der Authorization Service MUSS in seinem Entity Statement im claim redirect_uris
6159 die redirect_uris aller Mandanten auflisten, welche bei der Registrierung an einem
6160 beliebigen ePA Authorization Service eine eigene redirect_uri angegeben haben. Über
6161 Änderungen des claim redirect_uris MUSS der Anbieter des Federation Master vor
6162 produktiver Verwendung informiert werden[**<=**]

6163 Hinweis: Im Registrierungsprozess eines Mandanten mit eigener redirect_uri muss
6164 sichergestellt sein,

- 6165 • dass alle Anbieter von ePA Authorization Servern (ePA Aktensystem Anbieter)
6166 entsprechend informiert sind und das Entity Statement anpassen
- 6167 • dem Hersteller des Federation Master über ein ITSM Change bekannt gemacht
6168 wird, dass sich die Entity Statements aller ePA Authorization Server ändern

6169 **A_27145 -Synchronisation "redirect_URI" mit Marktteilnehmer - E-Mail-Adresse**

6170 Der Anbieter ePA-Aktensystem MUSS der gematik eine E-Mail-Adresse mitteilen, über
6171 welche er die eigenverantwortliche Registrierung (von redirect-URIs im Entity-
6172 Statement) durchführt und über die der Anbieter bei Änderungen erreichbar ist.

6173
6174 Hinweis: Diese E-Mail-Adressen werden durch das Provider Management der gematik
6175 anschließend unter den relevanten Anbietern verteilt bzw. können dort erfragt werden.
6176 Die Änderung der E-Mail-Adressen ist ebenfalls zu kommunizieren.

6177
6178 Hintergrund: Für Stellvertretung via ePA-FdV ist eine Synchronisierung der redirect_URIs
6179 notwendig.[**<=**]

6180 **A_27186 -Synchronisation "redirect_URI" mit Marktteilnehmer - Information**
6181 Der Anbieter ePA-Aktensystem MUSS bei Änderungen der redirect URIs im eigenen
6182 Entity Statement allen anderen Marktteilnehmern des gleichen Fachdiensttyps diese
6183 Änderung innerhalb 24 Stunden mitteilen.[<=]

6184 **A_27187 -Synchronisation "redirect_URI" mit Marktteilnehmer - Aktualisierung**
6185 Der Anbieter ePA-Aktensystem MUSS nach dem Empfang der Mitteilungen über
6186 Änderungen der Redirect URIs in einem externen Entity Statement diese Änderung
6187 binnen 24 Stunden in den Redirect URIs des eigenen Entity Statement synchronisieren.
6188

6189 Hinweis: Diese Änderung erfordert anschließend keine Information nach A_27186.[<=]

6190 **A_24878-01 -Authorization Service - Authentifizierung eines Versicherten am**
6191 **ePA-FdV des Vertreters**

6192 Falls der Eingangsparameter x-authorize-representative=True der Operation
6193 I_Authorization_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der
6194 Authorization Service im PAR als Parameter amr mit den Werten
6195 urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer
6196 nur über eGK+PIN authentisieren darf.[<=]

6197 **A_26189-01 -Authorization Service - Authentifizierung eines Versicherten im**
6198 **Gastmodus mit eGK und PIN**

6199 Falls der Eingangsparameter x-authorize-egk=True der Operation
6200 I_Authorization_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der
6201 Authorization Service im PAR als Parameter amr mit den Werten
6202 urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer
6203 nur über eGK+PIN authentisieren darf.[<=]

6204 **A_24937-01 -Authorization Service - Einschränkung bei Authentifizierung eines**
6205 **Versicherten am ePA-FdV des Vertreters**

6206 Der Authorization Service MUSS sicherstellen, dass ein mit x-authorize-
6207 representative=True authentisierter Nutzer ausschließlich Zugriff auf das Entitlement
6208 Management erhält.[<=]

6209 **A_26159 -Authorization Service - Prüfen der Device Attestation**

6210 Der Authorization Service MUSS sicherstellen, dass von einem anderen ePA-Aktensystem
6211 signierte Device Attestations ausschließlich akzeptiert werden, wenn

- 6212 • die Device Attestation gemäß A_25042-* valide von einer Signaturidentität der
6213 VAU eines anderen ePA-Aktensystems signiert wurde,
- 6214 • die KVN-R in der Device Attestation mit der KVN-R im ID-Token des angemeldeten
6215 Nutzers übereinstimmt,
- 6216 • die Device Attestation zeitlich gültig ist.

6217 [<=]

6218 **A_26160 -Authorization Service - Keine Persistierung der Device Attestation**

6219 Der Authorization Service MUSS sicherstellen, dass die von einem anderen ePA-
6220 Aktensystem signierte Device Attestation und deren Inhalte spätestens bei Beendigung
6221 der User Session gelöscht und nicht persistiert werden.[<=]

6222 **A_25310-01 -Authorization Service - Einschränkung bei Authentifizierung mit**
6223 **einem unregistrierten Gerät**

6224 Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wird und der Nutzer
6225 nicht mit x-authorize-representative=True authentisiert wurde, MUSS der
6226 Authorization Service sicherstellen, dass der Nutzer ausschließlich Zugriff auf das Device
6227 Management erhält.[<=]

6228 Hinweis:
6229 Ein vollständiger Zugriff eines authentisierten Nutzers auf alle Dienste des Aktensystems
6230 kann nur mit einem Gerät erfolgen, dessen Geräteregistrierung bei der Authentifizierung
6231 des Nutzers erfolgreich verifiziert wurde.
6232 Ein Nachweis einer Geräteregistrierung ist entweder DeviceID (deviceIdentifier und
6233 deviceToken), die für den Nutzer im Aktensystem bekannt sind oder die vom Client
6234 übergebene Device Attestation (deviceAttestation), die zuvor am Device Management des
6235 Home Aktensystems durch den Client abgerufen wurde.

6236 **A_24804-01 -Authorization Service - Prüfung auf registriertes Gerät**
6237 Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des
6238 Vertreters handelt und im Operationsaufruf
6239 `I_Authorization_Service::sendAuthCodeFdV` eine DeviceID (deviceIdentifier und
6240 deviceToken) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung
6241 eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer
6242 registriert und bestätigt ist und übereinstimmt. [`<=`]

6243 **A_24914-03 -Authorization Service - Prüfung auf registriertes Gerät - kein**
6244 **registriertes Gerät**
6245 Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wurde, MUSS
6246 der Authorization Service die Operation `sendAuthCodeFdV` mit einer Fehlermeldung
6247 abbrechen und die User Session beenden. [`<=`]

6248

6249 **A_24915-01 -Authorization Service - Prüfung auf registriertes Gerät -**
6250 **registriertes Gerät nicht bestätigt**
6251 Falls als Nachweis einer Geräteregistrierung eine DeviceID (deviceIdentifier und
6252 deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status ==
6253 'pending'), MUSS der Authorization Service die Operation `sendAuthCodeFdV` mit einer
6254 Fehlermeldung abbrechen und die User Session beenden. [`<=`]

6255

3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B

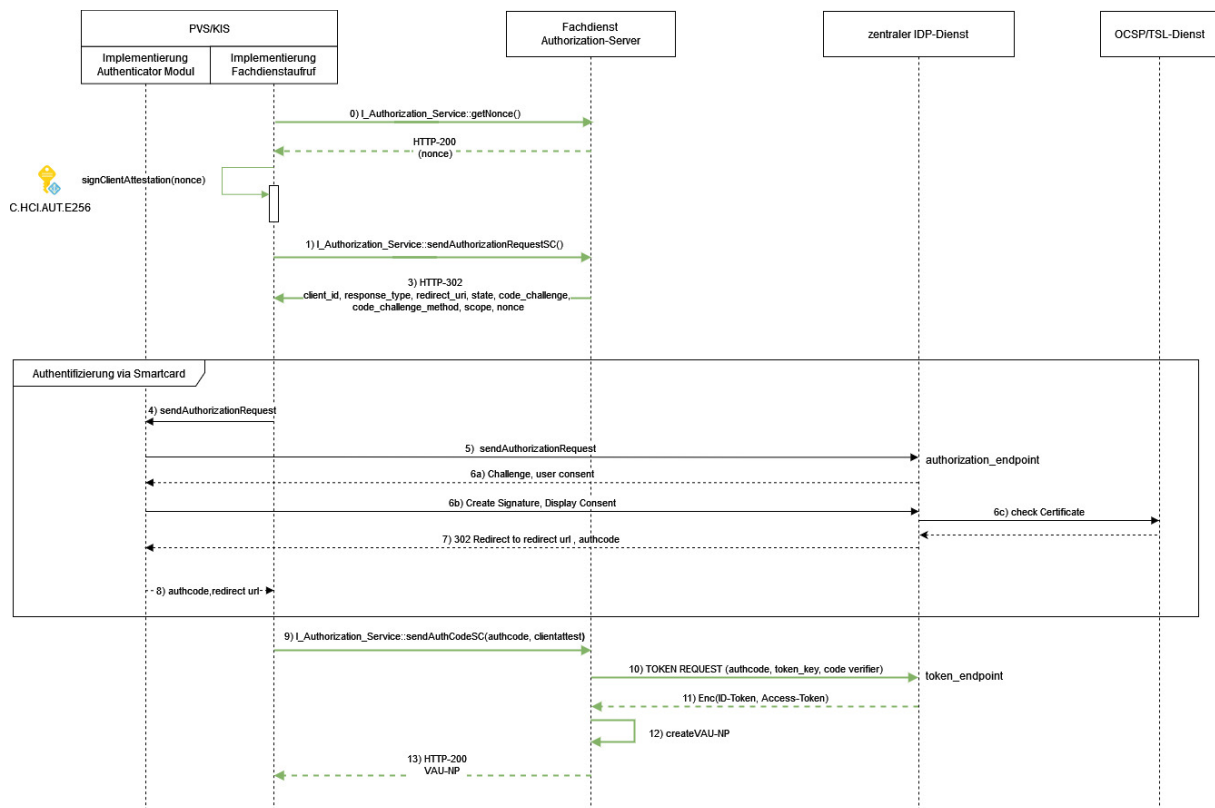


Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP

A_24717 -Authorization Service: IDToken vom IDP-Dienst nur mit Client-Attestation nutzbar

Der Authorization Service MUSS sicherstellen, dass ein vom IDP-Dienst abgerufenen 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_25444-03A_25444-01 -Authorization Service - JWT Client Attestation

Der Authorization Service MUSS bei der Authentifizierung einer Leistungserbringerinstitution prüfen, dass das übermittelte JWT der Client Attestierung

6277 mindestens die folgenden Inhalte aufweist.
6278

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 <code>getNonce</code> Operation	siehe [I_Authorization_Service]

6279 **[<=]**

6280 Für das Signaturzertifikat zu "x5c" (AUT-Zertifikat der SMC-B) gilt: Basiert der
6281 öffentlichen Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert "ES256"
6282 (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-256. Die
6283 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

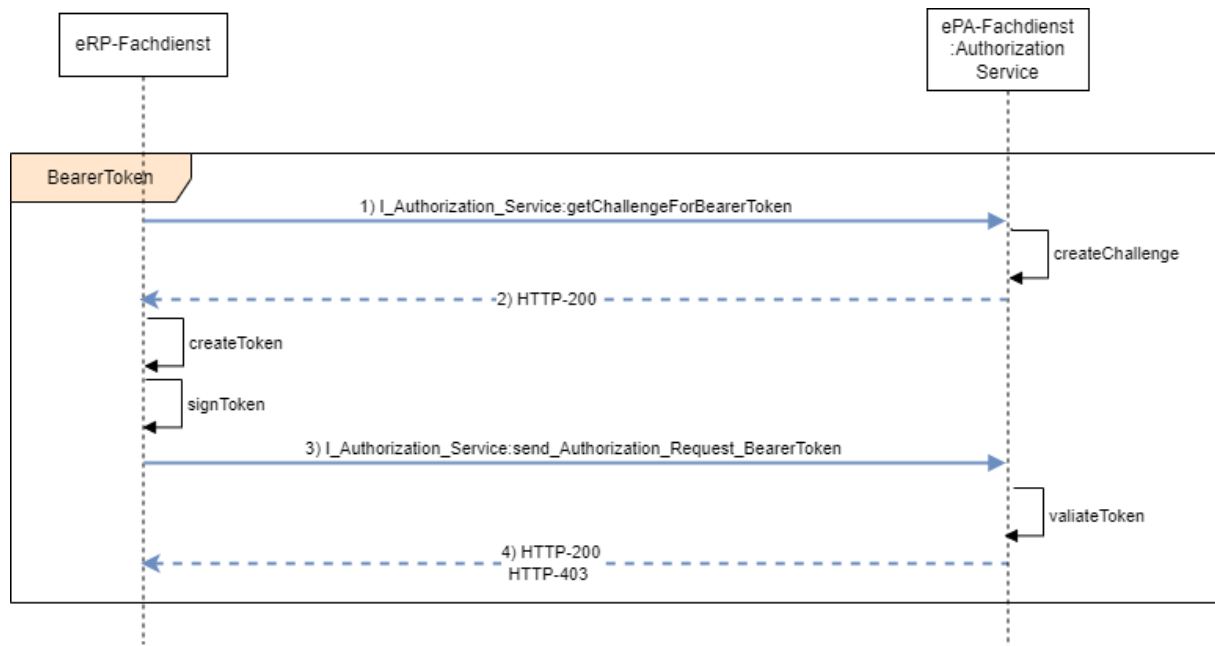


Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes

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"

Part	Claim Name	Claim	Anmerkung
	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Krypt]
	"sub"	Telematik-ID des E-Rezept-Fachdienstes	

6297 [**<=**]

6298 Das Signaturzertifikat zu "x5c" (AUT-Zertifikat der E-Rezept-VAU) kommt aus der
 6299 Komponenten-PKI der TI. Basiert der öffentlichen Schlüssel auf der ECC-Kurve
 6300 brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve
 6301 und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß
 6302 [RFC7515] zu erstellen.

6303 **3.18 Anbindung Verzeichnisdienst FHIR-Directory**

6304 **A_25176 -ePA-Aktensystem - Anbindung Verzeichnisdienst FHIR-Directory**

6305 Das ePA-Aktensystem MUSS bei der Suche des Versicherten nach Einträgen
 6306 im Verzeichnisdienst FHIR-Directory und bei der initialen Anlage einer Akte den
 6307 Anwendungsfall "AF_10219* - Versicherter sucht Einträge im FHIR-Directory" gemäß
 6308 [gemSpec_VZD_FHIR_Directory] als Fachdienst unterstützen und dabei für die Client
 6309 Anfrage von search-access_token die Operation getFHIRVZDtoken gemäß
 6310 [I_Authorization_Service.yaml] bereitstellen. [**<=**]

6311 **3.19 Access Gateway**

6312 Das Access Gateway ermöglicht den Versicherten bzw. deren berechtigten Vertretern den
 6313 Zugang zum zugehörigen Aktensystem über das Internet. Auf der einen Seite dient es
 6314 der Abschottung des ePA-Aktensystems in Richtung Internet, auf der anderen Seite
 6315 regelt es den kontrollierten Zugriff der Versicherten auf das Aktensystem mit seinen
 6316 funktionalen Komponenten.

6317 **3.19.1 Paketfilter**

6318 **3.19.1.1 Funktion**

6319 Der Paketfilter stellt die Anbindung des ePA-Aktensystems an das Internet her und
 6320 gewährleistet die Abschottung des ePA-Aktensystems in Richtung Internet.

6321 **A_14017 -Access Gateway, Sicherung zum Transportnetz Internet durch Paketfilter**

6322 Das ePA-Aktensystem MUSS zum Transportnetz Internet durch einen Paketfilter (ACL)
 6323 gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der
 6324 Paketfilter der Komponente Access Gateway MUSS frei konfigurierbar sein auf der
 6325 Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse,
 6326 IP-Protokoll sowie Quell- und Zielport. [**<=**]

A_14018 -Access Gateway, Platzierung des Paketfilters Internet

Der Paketfilter der Komponente Access Gateway, zum Schutz in Richtung Transportnetz Internet, DARF NICHT auf den anderen, zum Access Gateway gehörenden, physischen Komponenten implementiert werden. [≤]

A_14019-02 -Access Gateway, Richtlinien für den Paketfilter zum Internet

Der Paketfilter der Komponente Access Gateway MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

1. HTTPS, und
2. OCSP-Zugriffe für das OCSP-Stapling (vgl. Hinweis nach A_14019-02), ggf. notwendige DNS Anfragen (und Antworten).

Ein Verbindungsaufbau aus dem ePA-Aktensystem über das Access Gateway in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2. [≤]

Hinweis zu A_14019-02: Der Aktensystem-Anbieter muss für seine HTTPS-Schnittstelle ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-Zertifikate also über einen aktuellen Webbrowser prüfbar ist, vgl. A_14776). Für dieses TLS-Zertifikat fragt das Access Gateway (die HTTPS-Schnittstelle ist Teil davon) regelmäßig für das OCSP-Stapling (vgl. [gemSpec_Krypt#A_24913-]) den OCSP-Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält das Access Gateway eine OCSP-Response. Diese wird nach A_19126 geprüft und anschließend von der HTTPS-Schnittstelle verwendet (vgl. <https://tools.ietf.org/html/rfc6066#section-8> und bspw. http://nginx.org/en/docs/http/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-Responser 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.

[≤]

6375 **A_14776 -Access Gateway, Richtlinien zum TLS-Verbindungsaufbau**
6376 Die Komponente Access Gateway MUSS sich beim TLS-Verbindungsaufbau gegenüber
6377 dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB
6378 Forum] authentisieren. Das Zertifikat MUSS an die Schnittstelle der Proxy-Komponente
6379 gebunden werden.[<=]

6380 **3.19.1.2 Redundanz**

6381 Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf#3.18.1.3]. Die
6382 Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Access
6383 Gateways.

6384 Die Auswahl der Access Gateways wird durch das ePA-Frontend des Versicherten aus
6385 einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des Access
6386 Gateways kann der Anbieter des ePA-Aktensystems durch die Konfiguration und
6387 Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn
6388 jeder Versicherte mit existierendem Konto beim Anbieter des ePA-Aktensystems oder
6389 dessen berechtigter Vertreter die Möglichkeit zum Verbindungsaufbau hat.

6390 Eine hardwaretechnische Hochverfügbarkeit der einzelnen Access Gateways ist über
6391 grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht
6392 dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische
6393 Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern
6394 einzusetzen, so dass jedes einzelne Access Gateway im Ergebnis eine höhere
6395 Verfügbarkeit oder Leistungsfähigkeit besitzt.

6396 **A_14026 -Access Gateway, Redundanz der Paketfilter im Access Gateway**

6397 Die Komponente Access Gateway MUSS sicherstellen, dass bei Ausfall eines von
6398 mehreren Paketfiltern die verbleibenden Paketfilter in dem-selben Standort den
6399 Datenverkehr aller Mandanten des ausgefallenen Paketfilters zusätzlich übernehmen
6400 können.[<=]

6401 **3.19.1.3 Konfiguration**

6402 **A_14030 -Access Gateway, Verhalten des Access Gateways bei Vollauslastung**

6403 Die Komponente Access Gateway MUSS den Paketfilter Internet so konfigurieren, dass
6404 bei Vollauslastung der Systemressourcen im ePA-Aktensystem keine weiteren
6405 Verbindungen angenommen werden.[<=]

6406 Durch die Zurückweisung von Verbindungen wird sichergestellt, dass das ePA-Frontend
6407 des Versicherten einen Verbindungsaufbau mit einem anderen Access Gateway des
6408 jeweiligen ePA-Aktensystems versucht, bei dem die erforderlichen Ressourcen zur
6409 Verfügung stehen.

6410 **3.19.1.4 Adressierung**

6411 *3.19.1.4.1 Access Gateway zum Transportnetz Internet*

6412 **A_14031 -Access Gateway, IPv4-Adressierung der Internetschnittstellen des** 6413 **Access Gateways**

6414 Der Anbieter des ePA-Aktensystems MUSS jedem Access Gateway genau eine öffentliche
6415 IPv4-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum
6416 Internet konfiguriert werden. Die öffentlichen IP-Adressen des Access Gateways MÜSSEN
6417 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. [\leq]

3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz

Die Adressen des ePA-Aktensystems am Übergang zur TI werden vom Anbieter des Zentralen Netzes aus dem Adressblock TI_Zentral zugewiesen.

3.19.2 Proxy für das VAU-Protokoll

Das Access Gateway leitet Anfragen vom ePA-FdV über den VAU-Kanal an die zuständige VAU-Instanz weiter, damit diese dort in der User Session des Versicherten verarbeitet werden können.

A_24331 -Access Gateway - Data Proxy

Das Access Gateway MUSS die VAU-Protokoll-Kommunikation des ePA-Frontend des Versicherten an die zuständige VAU-Instanz weiterleiten. [\leq]

3.19.3 Tracing in Nichtproduktivumgebungen

Für die Fehlersuche - insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase - hat es sich als notwendig erwiesen, dass ein Fehlersuchender den Klartext der Kommunikation zwischen ePA-Client und VAU-Instanz mitlesen kann. (vgl. auch 2.5- Tracing in Nichtproduktivumgebungen)

Das Access Gateway stellt Informationen über die aktuell verfügbaren Sensorpunkte im AS bereit. Weiterhin exponiert das Access Gateway die Daten der Sensorpunkte über TCP (i. S. v. nicht TLS-gesichert) bspw. über Port 8001,...,8009. Die dort von den Sensorpunkten ge-streamten Daten sind nur Testdaten, also keine Echtdaten, d. h. sie haben keinen Schutzbedarf bezüglich Vertraulichkeit. Um die exponierten Sensordaten-Punkte vor DoS-Angriffen zu schützen, erlaubt das Access Gateway im Fall der Fälle die TCP-Ports auf IP-Layer über Firewall-Regeln abzusichern.

A_21890-01 -Access Gateway, Sensorpunkt für Nichtproduktivumgebungen

Die Komponente Access Gateway MUSS genau in Nichtproduktivumgebungen:

- die Daten der Sensorpunkte des Aktensystems auf TCP-Ports (bspw. ab Port 8000) öffentlich (ggf. auch ohne TLS-Sicherung) im Internet zur Verfügung stellen, indem die aktuell an den Sensorpunkten auflaufenden Daten auf dem TCP-Port am Access Gateway öffentlich gestreamt werden.
- die Möglichkeit bieten, den Zugriff auf diese TCP-Ports durch Firewall-Einstellungen auf IP-Layer zu beschränken.

Weiterhin MUSS das Access Gateway über die URL /tracingpoints Informationen über die aktuell im AS verfügbaren und damit auch im Access Gateway öffentlich exponierten Sensorpunkt-Daten als JSON-Array (=> Response-Type 'application/json') der folgenden Form bereitstellen:

```
[
{"name" : "zentraler Tigerproxy",
"port" : 8001,
```

```

6462     "DoS-protection-type" : „secret_url“
6463     "DoS-protection-port" : „udp/46789“
6464 },
6465 { "name" : "Extra Sensor VAU RZ2/B1/R1",
6466   "port" : 8002,
6467   "DoS-protection-type" : „ssh_tunnel“
6468   "DoS-protection-port" : „tcp/46790“
6469 }, ...
6470 ]

```

6471 Sollten keine Sensorpunkte aktuell im AS aktiviert sein (bspw. bei Lasttests) so ist das
 6472 Array leer: [].

6473 Sollte es keinen optionalen DoS-Schutzmechanismus gemäß A_22582-* geben, so fallen
 6474 die DoS-* Attribute in der o. g. Datenstruktur weg (sind nicht existent).

6475 Die einzelnen Felder des Arrays sind associative array (oder auch maps oder dictionaries
 6476 genannt). Diese KÖNNEN neben "name" und "port" beliebige vom AS definierbare,
 6477 weitere key-value-Paare enthalten. Der Eintrag "port" gibt an, an welchem öffentlich
 6478 erreichbaren TCP-Port des Access Gateway die Sensordaten des entsprechenden Sensors
 6479 abrufbar sind (gestreamt werden).

6480 [**<=**]

6481 *Hinweis zu A_21890-*: Die semistatische JSON-Datei, welche ein Client unter dem Pfad*
 6482 *„/tracingpoints“ erhalten kann, ist eine einfache Form von Service-Discovery. Damit kann*
 6483 *ein Client (Fehlersuchende(r)) erfahren, welche Tracing-Quellen es aktuell im AS gibt i.*
 6484 *S. v. welche Tracing-Quellen ein Client zur Fehlersuche aktuell verwenden kann.*

6485 **A_22582 -Tracing in Nichtproduktivumgebungen, DoS-Schutz**

6486 Die Komponente Access Gateway KANN Sicherheitsmechanismen bereitstellen und
 6487 aktivieren, die es genau in Nichtproduktiv-umgebungen ermöglichen, temporär,
 6488 automatisiert und nur nach erfolgreicher Authentifizierung die TCP-Ports für das
 6489 Streaming der Sensorpunkte für Clients nach A_21890-* freizuschalten. [**<=**]

6490 *Hinweis zu A_22582-*: In den Nichtproduktivumgebungen darf es keine Echtdaten*
 6491 *geben. Es dürfen sich dort nur Daten befinden, deren Schutzbedarf bezüglich*
 6492 *Vertraulichkeit niedrig ist. Der optionale Schutzmechanismus nach A_22582-* braucht*
 6493 *nur einen einfachen DoS-Schutz leisten gegen einen Angreifer mit niedrigen*
 6494 *Angriffspotential. Der Anbieter ist, sofern er einen solchen Mechanismus einsetzen*
 6495 *möchte, frei, dafür den Mechanismus selbst zu wählen. Er wählt dann bei "DoS-*
 6496 *protection-type" (vgl. A_21890-*) einen selbstdefinierten (möglichst sprechenden)*
 6497 *Namen.*

6498 Beispiele für Umsetzungsmöglichkeiten:

- 6499 1. Es gibt im Access Gateway eine geheime URL (bspw.
 6500 /tracing/964b059de83d20581f43dd1b867d740c). Ein Client kennt das Geheimnis
 6501 und ruft diese URL auf. Daraufhin wird im Access Gateway für die IP-Adresse des
 6502 Clients die Tracing-Quelle im Access Gateway frei geschaltet (TCP-Port 8000, ...).
- 6503 2. Die gematik stellt eine Beispielimplementierung zur Verfügung. Dort gibt es einen
 6504 UDP-Server (Access Gateway) und einen UDP-Client (Fehlersuchende), die beide
 6505 ein gemeinsames HMAC-Geheimnis teilen. Wenn der Client die aktuelle Zeit und
 6506 dessen IP-Adresse per HMAC authentisiert dem UDP-Server sendet, so schaltet
 6507 der UDP-Server nach erfolgreicher Prüfung des HMACs den entsprechenden TCP-
 6508 Port für die authentifizierte IP-Adresse des Clients frei.
- 6509 3. Auf dem Access Gateway läuft ein SSH-Daemon. Der öffentliche
 6510 Authentisierungsschlüssel eines Clients ist dort als gültiger Nutzer konfiguriert
 6511 (Login-Shell: /bin/false). Die Tracing-Quellen im Access Gateway sind so

6512 konfiguriert, dass sie nur mittels authentisierten SSH-Port-Forwarding
6513 (<https://www.ssh.com/academy/ssh/tunneling/example>) erreichbar sind.

6514 3.19.4 Übergreifende Festlegungen

6515 **A_14249 -Komponente Access Gateway - Separierung der Schnittstellen für** 6516 **verschiedene Umgebungen**

6517 Die Komponente Access Gateway MUSS die Bereitstellung von Schnittstellen für die
6518 Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen
6519 Umgebungen der TI (RU/TU, PU) sicherstellen und voneinander separieren. [<=]

6520 **A_14034 -Access Gateway, Übergang des ePA-Aktensystems zur TI**

6521 Die Komponente Access Gateway MUSS sicherstellen, dass der Zugriff auf Dienste der TI
6522 ausschließlich über einen Sicheren Zentralen Zugangspunkt (SZZP) erfolgt. [<=]

6523 **A_14036 -Access Gateway, Synchronisierung der Komponenten mit den** 6524 **Stratum-1-NTP-Servern der TI**

6525 Die Komponente Access Gateway MUSS alle Komponenten seines Access Gateways mit
6526 den Stratum-1-NTP-Servern der TI synchronisieren. [<=]

6527 **A_13879 -Access Gateway, Serverseitige Authentisierung**

6528 Die Komponente Access Gateway MUSS sich gegenüber dem ePA-Frontend des
6529 Versicherten beim Aufbau der TLS-Session durch sein ExtendedValidation-
6530 Zertifikat authentisieren. Die Beschaffung des Zertifikats erfolgt durch den Anbieter über
6531 eine öffentliche CA. [<=]

6532 **A_14033 -Access Gateway, TLS Verschlüsselung**

6533 Die Komponente Access Gateway MUSS sicherstellen, dass jede Kommunikation mit dem
6534 ePA-Frontend des Versicherten TLS verschlüsselt erfolgt. [<=]

6535 Die Verwendung der SoapAction ermöglicht einer Reverse-Proxy-Komponente innerhalb
6536 des Access Gateways, die Nachrichten zu verarbeiten, ohne die http-Payload zu
6537 untersuchen.

6538 **A_13876 -Access Gateway, Kein direkter Zugriff auf Dienste der zentralen TI-** 6539 **Plattform**

6540 Die Komponente Access Gateway MUSS einen direkten Zugriff aus dem Internet auf
6541 Dienste der zentralen TI-Plattform verhindern. [<=]

6542 **A_14016 -Access Gateway , Schutz vor Angriffen aus dem Internet**

6543 Die Komponente Access Gateway MUSS für alle vom Internet erreichbaren Schnittstellen
6544 Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere
6545 Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS
6546 Lösungen verhindert werden. [<=]

6547 **A_15196 -Access Gateway, Schutz vor volumetrischen DoS-Angriffen**

6548 Die Komponente Access Gateway MUSS bei Beauftragung eines qualifizierten
6549 Dienstleisters zum Schutz vor volumetrischen DoS-Angriffen Kriterien des BSI zur
6550 Auswahl qualifizierter Dienstleister umsetzen. [<=]

6551 Als Maßnahme gegen volumetrische Denial-of-Service-Angriffe wird die Verwendung von
6552 DNS- oder BGP-Routing-Diensten empfohlen. Hinweise des BSI:

6553 [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos_node.html)
6554 [und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos_node.html).

6555 3.20 Data Submission Service

6556 Die Daten der elektronischen Patientenakten sollen nach § 363 Absatz 1 SGB V für die in
6557 § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszwecke zugänglich gemacht und
6558 hierfür in pseudonymisierter Form automatisiert von den ePA-Aktensystemen an das
6559 Forschungsdatenzentrum Gesundheit (FDZ) nach § 303d SGB V übermittelt werden,
6560 sofern Versicherte dem nicht widersprochen haben.

6561 Neben dem FDZ und den ePA-Aktensystemen ist die Vertrauensstelle (VST) nach § 303c
6562 SGB V im Prozess involviert. Deren Aufgabe ist es, die von den ePA-Aktensystemen
6563 erhaltenen Lieferpseudonyme in periodenübergreifende Pseudonyme umzuwandeln und
6564 diese an das FDZ zu übermitteln.

6565 Der Data Submission Service im Aktensystem übernimmt in der Übermittlung der
6566 pseudonymisierten medizinischen Daten folgende Aufgaben:

- 6567 • Erstellung der Lieferpseudonyme (auf Basis der KVN-R) und der Arbeitsnummern
- 6568 • Registrierung der Arbeitsnummer mit dem zugehörigen Lieferpseudonym bei der
6569 Vertrauensstelle
- 6570 • Pseudonymisierung der medizinischen Daten
- 6571 • Verknüpfung der pseudonymisierten medizinischen Daten mit der Arbeitsnummer
- 6572 • Übermittlung der pseudonymisierten medizinischen Daten und der zugehörigen
6573 Arbeitsnummern an das Forschungsdatenzentrum Gesundheit

6574 Die Übermittlung der Daten erfolgt blockweise. D.h. es wird ein Paket von
6575 pseudonymisierten medizinischen Daten mit zugehörigen Arbeitsnummern aus
6576 verschiedenen Aktenkonten zusammengestellt (Datenpaket FDZ) und alle für dieses
6577 Paket benötigten Arbeitsnummern und Lieferpseudonyme mit einem Mal bei der VST
6578 registriert (Datenpaket VST). Die Datenpakete haben eine anbieterübergreifend
6579 eindeutige SubmissionID und die SubmissionID zusammengehöriger Datenpakete VST
6580 und FDZ ist identisch.

6581 Für die Übermittlung wird zwischen Aktensystem und VST, sowie Aktensystem und FDZ
6582 jeweils ein beidseitig authentisierter VAU-Kanal aufgebaut, auf dem sich die Dienste VST
6583 und FDZ mit einer Identität ID.FD.AUT mit ihren entsprechenden Rollen authentisieren.

6584 Der Versicherte kann mit Hilfe seines ePA-FdVs oder über die Ombudsstelle des
6585 Kostenträgers der Übermittlung seiner pseudonymisierten medizinischen Daten an das
6586 FDZ widersprechen oder die möglichen Sekundärnutzungszwecke seiner übermittelten
6587 pseudonymisierten medizinischen Daten im FDZ einschränken. Dies erfolgt über das
6588 Consent Decision Management im Aktensystem.

6589 3.20.1 Erstellung von Arbeitsnummern und Lieferpseudonymen

6590 Der Data Submission Service erzeugt eindeutige Arbeitsnummern und Lieferpseudonyme,
6591 um die pseudonymisierten medizinischen Daten in der Übermittlung an das FDZ eindeutig
6592 zuordnen zu können.

6593 A_26211 -Data Submission Service - Erstellung des Lieferpseudonyms

6594 Der Data Submission Service MUSS das Lieferpseudonym des Versicherten gemäß
6595 [I_VST] unter Verwendung der KVN-R des Versicherten erstellen.[<=]

6596 **A_26409 -Data Submission Service - keine Erstellung von LP für**
6597 **Validierungsaktenkonten**

6598 Der Data Submission Service DARF KEINE Lieferpseudonyme für KVNRn
6599 von Validierungsaktenkonten erstellen.[<=]

6600 **A_26212 -Data Submission Service - Erstellung der Arbeitsnummer**

6601 Der Data Submission Service MUSS für die Arbeitsnummer einen Zufallswert mit einer
6602 Mindestentropie von 120 Bit erzeugen und die Kodierung aus [I_VST] verwenden.[<=]

6603 **A_26410 -Data Submission Service - keine Erstellung von AN für**
6604 **Validierungsaktenkonten**

6605 Der Data Submission Service DARF KEINE Arbeitsnummern für Daten
6606 aus Validierungsaktenkonten erstellen.[<=]

6607 **A_26255 -Data Submission Service - Verwendungsdauer von**
6608 **Lieferpseudonymen und Arbeitsnummern**

6609 Der Data Submission Service MUSS für jedes in einem Datenpaket FDZ übermittelte
6610 pseudonymisierte medizinische Datum zu einer KVNR eine neue Arbeitsnummer und ein
6611 neues Lieferpseudonym generieren.[<=]

6612 **A_26256 -Data Submission Service - Registrierung von Arbeitsnummern**

6613 Der Data Submission Service MUSS jede Arbeitsnummer zusammen mit dem
6614 zugehörigen Lieferpseudonym in das entsprechende Datenpaket VST aufnehmen und an
6615 die Vertrauensstelle übermitteln.[<=]

6616 **3.20.2 Auswahl von medizinischen Daten**

6617 Der Data Submission Service muss bestimmte neue und geänderte FHIR-Ressourcen an
6618 den FDZ übertragen. Dies betrifft im ersten Schritt die Medikationsdaten aus der E-
6619 Medikationsliste und wird subsequent weiter ausgebaut.

6620 Der Medication Service, als Quelle der Medikationsdaten zur Übertragung an den FDZ,
6621 erlaubt flexible, datenbasierte Operationen auf einzelnen FHIR-Ressourcen. Dies erfordert
6622 entsprechende Implementierung um effizient und zuverlässig die neuen und geänderten
6623 Ressourcen identifizieren können um daraus die Auswahl für die zu übertragende FHIR-
6624 Ressourcen treffen zu können.

6625 **A_26296 -Data Submission Service - Übertragung neuer und geänderter FHIR-**
6626 **Ressourcen**

6627 Der Data Submission Service MUSS neue und geänderte FHIR-Ressourcen identifizieren
6628 können und daraus die Auswahl für die Übermittlung der Daten an FDZ treffen
6629 können.[<=]

6630 **A_26297 -Data Submission Service - Einschränkung der FHIR-Ressourcen nach**
6631 **Änderungsdatum**

6632 Der Data Submission Service MUSS den Zeitpunkt der letzten Übermittlung
6633 (lastSubmissionTimestamp) merken und in nachfolgenden Übermittlungen nur die
6634 Ressourcen, die sich seit diesem Zeitpunkt geändert haben, berücksichtigen. Hierfür ist
6635 das FHIR-Element meta.lastUpdated in der jeweiligen FHIR-Ressource zu
6636 verwenden.[<=]

6637 *Hinweis: Ressourcen, die im Rahmen eines Anbieterwechsels in ein Aktenkonto*
6638 *übernommen werden, sind nicht erneut zu übermitteln.*

6639 **A_26298 -Data Submission Service - FHIR-Ressourcen zur Übermittlung an FDZ**

6640 Der Data Submission Service MUSS die FHIR-Ressourcen gemäß der Tabelle "Auswahl
6641 der zu übertragenden FHIR-Ressourcen" an FDZ übertragen, dabei sind die Filter-
6642 Bedingungen (Spalte 'Filter Expression') und zu inkludierende referenzierte Ressourcen

zu berücksichtigen (Spalte 'Include' sowie Tabelle "Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen").[<=]

Tabelle 44: Auswahl der zu übertragenden FHIR-Ressourcen

Ressourcentyp / Profil	Filter Expression	Include
MedicationRequest \${epa-medication}/epa-medication-request	status != 'active' and identifier.where(system='https://gematik.de/fhir/epa-medication/sid/rx-prescription-process-identifier').hasValue()	MedicationRequest:medication
MedicationDispense \${epa-medication}/epa-medication-response	status != 'in-progress' and extension('https://gematik.de/fhir/epa-medication/StructureDefinition/rx-prescription-process-identifier-extension').hasValue()	MedicationDispense:medication

Tabelle 45: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen

Ressourcentyp/Profil	Anmerkung
Medication \${epa-medication}/epa-medication	Referenziert durch MedicationRequest, MedicationDispense

3.20.3 Protokollierung des Datenexports an das FDZ

Ein Datenexport erfolgt immer in Verbindung mit dem Einstellen neuer oder der Änderung existierender Daten für ein Aktenkonto. Ein Datenexport nach Auswahl der Daten gemäß A_26298 wird als Bestandteil der Protokollierung des auslösenden Ereignisses protokolliert (siehe dazu: 3.13.2.2- Medication Service)

3.20.4 Pseudonymisierung von medizinischen Daten

Bevor medizinische Daten an das FDZ übermittelt werden dürfen, müssen diese pseudonymisiert werden und Daten mit direktem Personenbezug entfernt werden.

A_26300 -Data Submission Service - Pseudonymisierung von medizinischen Daten

Der Data Submission Service MUSS an das FDZ zu übermittelnde medizinische Daten gemäß der Vorgaben aus [DataPseudonymization] pseudonymisieren.[<=]

A_26408 -Data Submission Service - keine Pseudonymisierung von Daten aus Validierungsaktenkonten

Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem. Kapitel 2.4) pseudonymisieren. [<=]

A_26315 -Data Submission Service - Randomisierung der Reihenfolge des Datenpakets FDZ

Das ePA-Aktensystem MUSS sicherstellen, dass in einem Datenpaket FDZ vor der Übermittlung die Einträge nach Arbeitsnummer (AN) aufsteigend sortiert werden. Die Arbeitsnummer (32-Byte Zufallswert, A_26212-*) wird dabei als natürliche Zahl (byteorder=big) interpretiert. [<=]

Verständnishinweis:

Die Akten werden regelmäßig nach zu übermittelnden Daten vom ePA-Aktensystem durchsucht. Dabei kann es passiert, dass in einer Akte mehrere Daten zur Übermittlung anfallen, die nach der Pseudonymisierung in einer Reihenfolge in das Datenpaket FDZ gelangen. Deshalb kann die Reihenfolge der Einträge im Datenpaket FDZ statistisch relevante Informationen über den Zusammenhang von Einträgen geben. Durch eine Randomisierung der Reihenfolge der Einträge innerhalb des Datenpakets wird dies verhindert. Die AN werden zufällig erzeugt, eine Sortierung nach AN ist deshalb eine Randomisierung der Reihenfolge.

3.20.5 Übermittlung der pseudonymisierten medizinischen Daten

Die Übermittlung von Datenpaketen an VST und FDZ erfolgt gemäß den Vorgaben des RKI (VST) und BfArM (FDZ) und deren Schnittstellenspezifikationen.

Die Übermittlung der pseudonymisierten Daten eines Aktenkontos für Sekundärnutzungszwecke erfolgt automatisch, sofern kein Widerspruch gegen Sekundärdatennutzung vorliegt. Die Voreinstellung ist dabei "kein Widerspruch erteilt" (siehe: 3.8.1- Widersprüche für Funktionen der ePA). Vor der allerersten Übermittlung solcher Daten wird dem Versicherten daher eine Frist gewährt, gegebenenfalls einen Widerspruch gegen diese Sekundärdatennutzung zu formulieren.

A_26462 -Data Submission Service - Übermittlung Datenpaket nach Ablauf der Widerspruchsfrist

Der Data Submission Service MUSS sicherstellen, dass vor der erstmaligen Übermittlung von Daten eines Aktenkontos die Widerspruchsfrist gemäß den Vorgaben des Kostenträgers abgelaufen ist. [<=]

Hinweis: Die erste Datenübermittlung ist die erste automatisiert mögliche Übermittlung (nach Aktivierung des Aktenkontos) und nicht die erste Datenübermittlung nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung.

HinweisHinweis: Für eine Übermittlung nach Ablauf dieser Widerspruchsfrist oder nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung werden immer nur ab diesem Zeitpunkt neu angefallene Daten berücksichtigt, Es erfolgt keine Übermittlung von vorhandenen Daten des Aktenkontos.

A_26214 -Data Submission Service - Erstellung der SubmissionID

Der Data Submission Service MUSS für zusammengehörige Datenpakete VST und FDZ eine gemeinsame anbieterübergreifend eindeutige SubmissionID erzeugen und diese mit den Datenpaketen übertragen. [<=]

A_26304 -Data Submission Service - Zufällige SubmissionID

Der Data Submission Service MUSS sicherstellen, dass die SubmissionID ein zufällig gewählter 256-Bit Wert mit einer Mindestentropie von 120 Bit ist. [<=]

- 6709 **A_26215 -Data Submission Service - Übermittlung Datenpaket VST**
6710 Der Data Submission Service MUSS das Datenpaket VST gemäß [I_VST] an die
6711 Vertrauensstelle übermitteln.[<=]
- 6712 **A_26407 -Data Submission Service - keine Übermittlung von Daten aus**
6713 **Validierungsaktenkonten**
6714 Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem.
6715 Kapitel 2.4) an das Forschungsdatenzentrum übermitteln.[<=]
- 6716 **A_26216 -Data Submission Service - Realisierung der Schnittstelle**
6717 **I_Data_Submission_Service**
6718 Der Data Submission Service MUSS die Operationen der Schnittstelle
6719 I_Data_Submission_Service gemäß [I_Data_Submission_Service] umsetzen.[<=]
- 6720 **A_26217 -Data Submission Service - Verbindung zur Vertrauensstelle**
6721 Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des
6722 Datenpakets VST ausschließlich über einen VAU-Kanal erfolgt in dem sich die
6723 Vertrauensstelle über ein Zertifikat C.FD.AUT mit professionOID gleich oid_epa_vst
6724 authentisiert hat.[<=]
- 6725 **A_26218 -Data Submission Service - Verbindung zum Forschungsdatenzentrum**
6726 **Gesundheit**
6727 Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des
6728 Datenpakets FDZ ausschließlich über einen VAU-Kanal erfolgt in dem sich das
6729 Forschungsdatenzentrum Gesundheit über ein Zertifikat C.FD.AUT mit professionOID
6730 gleich oid_epa_fdz authentisiert hat.[<=]
- 6731 **A_26299 -Data Submission Service - Wechsel des Verschlüsselungsschlüssels**
6732 **für Datenpakete**
6733 Falls die Datenpakete VST und FDZ außerhalb der VAU im System des
6734 Aktensystembetreibers gespeichert werden, MUSS der Data Submission Service
6735 sicherstellen, dass ein Schlüssel für die Verschlüsselung der Datenpakete VST bzw. FDZ
6736 maximal 4 Wochen genutzt werden kann und danach ein neuer
6737 Verschlüsselungsschlüssel mittels der Regel hsm-r8 mit Hilfe eines geänderten
6738 Ableitungsvektors abgeleitet wird.[<=]
- 6739 **A_26312 -Data Submission Service - Timeout in der Übermittlung**
6740 Der Data Submission Service MUSS die Übermittlung der Pakete VST und FDZ erneut
6741 starten, wenn das Datenpaket FDZ nicht innerhalb von 30 Minuten nach erfolgreicher
6742 Übermittlung des Datenpakets VST abgerufen wird.[<=]
- 6743 **A_26313 -Data Submission Service - Konfiguration der Intervalle und**
6744 **maximalen Größe eines Datenpakets**
6745 Der Data Submission Service MUSS folgende Parameter konfigurierbar gestalten:
6746
 - das Intervall in dem Datenpakete VST und FDZ übermittelt werden
 - eine maximale Größe eines Datenpakets FDZ bei deren Erreichen die Datenpakete
6747 übermittelt werden
6748
6749 [<=]
- 6750 **A_26244 -Data Submission Service - Löschen von Datenpaketen nach**
6751 **Übermittlung**
6752 Der Data Submission Service MUSS nach erfolgreicher Übermittlung des Datenpakets
6753 FDZ an das Forschungsdatenzentrum Gesundheit das übermittelte Datenpaket FDZ und
6754 das zugehörige Datenpaket VST lokal löschen.[<=]

A_26245 -Data Submission Service - Löschen von Datenpaketen bei Nicht-Übermittlung

Der Data Submission Service MUSS das Datenpaket FDZ und das zugehörige Datenpaket VST lokal löschen, wenn das Datenpaket FDZ länger als 72 Stunden nicht an das Forschungsdatenzentrum Gesundheit übermittelt werden konnte. Die enthaltenen Widersprüche MÜSSEN in die aktuell in Erstellung befindlichen Datenpakete VST und FDZ übernommen werden. [≤]

Hinweis: Wenn Widersprüche in ein neues Datenpaket übernommen werden, muss für jeden der Widersprüche eine neue Arbeitsnummer (AN) und ein Lieferpseudonym (LP) erstellt werden, da die bisherigen AN und LP im Kontext des zu löschenden Paketes stehen.

A_26246 -Data Submission Service - Aufnahme von Widersprüchen

Der Data Submission Service MUSS Widersprüche gegen die Freigabe von Daten zur Sekundärnutzung durch das FDZ oder Änderungen zu Sekundärnutzungszwecken, aus dem Consent Decision Management, in die aktuell in Erstellung befindlichen Datenpakete VST und FDZ übernehmen. Es MUSS sichergestellt werden, dass in einem Datenpaket FDZ für eine KVNR immer nur die zuletzt erklärten Widersprüche gegen die Übermittlung von Daten zur Sekundärnutzung durch das FDZ bzw. zu Sekundärnutzungszwecken enthalten sind. [≤]

Hinweis: Sollte während der Erstellung eines Datenpakets FDZ mehrfach die Widersprüche für eine KVNR geändert werden, wird immer nur der letzte Stand übermittelt.

A_26307 -Data Submission Service - Durchsetzung von Widersprüchen

Falls für ein Aktenkonto ein Widerspruch gegen die Übermittlung an das FDZ eingestellt wird, MUSS der Data Submission Service sicherstellen, dass in allen zukünftig zu übermittelnden Datenpaketen VST und FDZ außer den Daten für den Widerspruch keine Daten für dieses Aktenkonto enthalten sind. [≤]

Hinweis zu A_26307: Zum Zeitpunkt des Eingangs des Widerspruchs im Aktensystems bereits in der Übermittlung befindliche Datenpakete sind von der Anforderung ausgeschlossen. Betroffen sind jedoch auch die aktuell in Erstellung befindlichen Datenpakete VST und FDZ, bei denen die Übermittlung an die VST bzw. das FDZ noch nicht begonnen hat.

3.21 Push Notification Management

Nutzer von Anwendungen für Versicherte (ePA-FdV) können mittels Push Notifications direkt über Ereignisse in bestimmten Fachdiensten der TI oder des Kostenträgers auf ihren Endgeräten informiert werden. Diese Notifications erreichen einen Nutzer auch außerhalb aktiver Anmeldungen in diesen Fachdiensten. Die Ereignisse von Interesse zur Benachrichtigung des Nutzers sind dabei individuell abonnierbar.

Der Versand einer Push Notification erfolgt stets durch die einzelnen Fachdienste für Ereignisse ihrer Domäne. Die Übertragung in das Endgerät des Nutzers unter Einbindung der plattformspezifischen, externen Push-Dienste und betreiberspezifischen Push-Gateways wird für alle beteiligten Fachdienste gemeinsam durch ein Push Notification System realisiert. Dieses anwendungsübergreifende System und seine Komponenten für Push Notifications im Gesundheitswesen sind in [gemF_PushNotification] und [PushNotificationConcept] detailliert beschrieben.

6801 Dort sind auch die normativen Vorgaben für unterstützende Anwendungen und
6802 Fachdienste in Bezug auf Registrierung von Applikationen und Ereignissen für Push
6803 Nachrichten, Schnittstellen, sicherheitstechnische Anforderungen und notwendige
6804 Artefakte für einen interoperablen Betrieb formuliert.

6805 **3.21.1 Push Notification Management des ePA-Aktensystems**

6806 Das Push Notification Management des ePA-Aktensystems ist als ein spezifischer
6807 Fachdienst in dieses übergreifende System eingebunden und bedient die in
6808 [gemF_PushNotification] geforderten und in [PushNotificationConcept] beschriebenen
6809 Schnittstellen und Verfahren.

6810 Push Notifications der ePA können ausschließlich durch Versicherte für Ereignisse ihres
6811 eigenen Aktenkontos genutzt werden. Der Erhalt von Benachrichtigungen aus dem
6812 Aktenkonto eines vertretenen Versicherten wird nicht unterstützt.

6813 Der Nutzung des Push Notification Managements der ePA kann nicht widersprochen
6814 werden. Dieser Dienst gehört nicht zu den widerspruchsfähigen Funktionen der ePA.
6815 Versicherte, die keine Benachrichtigungen der ePA erhalten möchten, können die
6816 Benachrichtigungen durch Abwahl der Benachrichtigungskanäle oder auch generell durch
6817 den Verzicht des ePA-FdV auf eine Registrierung für Push Notifications unterbinden.

6818 Schnittstellen, die das Push Notification Management der ePA zur Nutzung durch Clients
6819 (ePA-FdV) anbietet, sind um ePA-spezifische Verfahren und Anforderungen ergänzt und
6820 als OpenApi gemäß [I_Push_Notification_Management] verfügbar.

6821 **A_27637 -Push Notification Management - Realisierung der Schnittstelle** 6822 **I_Push_Notification_Management**

6823 Das Push Notification Management MUSS die Operationen der Schnittstelle
6824 I_Push_Notification_Management gemäß [I_Push_NotificationManagement] ~~Notification~~
6825 umsetzen. [<=]

6826 **3.21.2 Registrierung eines ePA-FdV als Pusher**

6827 (siehe auch: [gemF_PushNotification]#Kapitel "Pusher registrieren")

6828 Ein Versicherter kann registrierte Geräte (im Sinne des Device Managements gemäß ~~3.12.1~~
6829 ~~Device Management~~) zur Nutzung seiner aktivierten elektronischen Patientenakte auch
6830 für den Erhalt von Push Nachrichten nutzen, sofern das übergreifende Push Notification
6831 System die technologische Infrastruktur für Benachrichtigungen an den Geräte-, bzw.
6832 Betriebssystemtyp des Versichertengeräts unterstützt. Dazu kann die ePA-FdV-
6833 Anwendung jedes dieser Geräte als ePA-FdV Instanz, bzw. 'Pusher', im eigenen
6834 Aktenkonto des Versicherten registriert werden.

6835 Die ePA-FdV Instanz Registrierung eines Gerätes als Pusher erfolgt immer durch und für
6836 das auf diesem Gerät installierte ePA-FdV und unter Nutzung der Schnittstelle
6837 [I_Push_Notification_Management]. Über diese Schnittstelle werden existierende
6838 Registrierungen auch aktualisiert und wieder entfernt.

6839 Die Daten der Registrierungen, inklusive des kryptographischen Materials der
6840 Schlüsselableitungen und der Auswahl der Benachrichtigungskanäle, sind Bestandteil des
6841 Aktenkontos und werden dort gespeichert. Pro registriertem Gerät kann jeweils nur eine
6842 ePA-FdV Instanz im Aktenkonto hinterlegt sein und eine Registrierung gilt immer nur für
6843 genau eine bestimmte ePA-FdV Instanz. Eine ePA-FdV Instanz Registrierung ist daher
6844 fest an eine Device Registration gebunden.

A_27638 -Push Notification Management- Speicherung der Daten

Das Push Notification Management MUSS alle Daten des Dienstes für einen Versicherten im SecureDataStorage des Aktenkontos des Versicherten speichern.[<=]

A_27640 -Push Notification Management - automatisches Löschen der Registrierung einer ePA-FdV Instanz

Das Push Notification Management MUSS sicherstellen, dass eine existierende Registrierung einer ePA-FdV Instanz und die dazugehörigen Daten vollständig und automatisch gelöscht werden, wenn die Device Registration des assoziierten Geräts im Device Management des Aktensystems gelöscht wird.[<=]

A_27639 -Push Notification Management - eindeutiger pushKey

Das Push Notification Management MUSS sicherstellen, dass der `pushKey` einer Registrierung einer ePA-FdV Instanz eindeutig ist und es keine zwei oder mehr Registrierungen mit gleichem `pushKey` gibt.[<=]

Bei jedem Versand einer Push Nachricht an das Push Gateway kann dieses in den Rückgabewerten der Push Operation einen Eintrag oder eine Liste veralteter, bzw. ungültiger `pushKeys` melden. Eine weitere Nutzung solcher Registrierungen, bzw. `pushKeys`, soll unterbleiben. Die assoziierten Registrierungen von ePA-FdV-Instanzen werden daher aus dem Aktenkonto entfernt.

A_27682 -Push Notification Management - Entfernen ungültiger pushKeys

Das Push Notification Management MUSS Registrierungen von ePA-FdV-Instanzen löschen, wenn `pushKeys` dieser Registrierungen durch das Push Gateway als ungültig gemeldet werden.[<=]

Hinweis: Es werden nur Registrierungen aus dem versendenden Aktenkonto entfernt. Eventuelle Rückmeldungen des Push Gateways zu pushKeys, die nicht oder nicht mehr mit dem versendenden Aktenkonto verbunden sind, werden ignoriert.

3.21.3 Push Notification Channels

(siehe auch: [gemF_PushNotification]#Kapitel "Channel/ Trigger Konfiguration")

Das ePA-Aktensystem bietet eine Auswahl an Channels zu Ereignissen, über deren Aktivität ein Versicherter durch Push-Benachrichtigungen informiert werden kann. Der jeweilige Nachrichteninhalte beschreibt dabei in Kurzform das auslösende Ereignis.

Die Grundeinstellung für den Versand von Push-Benachrichtigungen an neu erstellten Registrierungen für ePA-FdV-Instanzen lautet für jeden Channel zunächst deaktiviert ('disabled' - keine Benachrichtigung für diesen Kanal). Ein Versicherter kann diese Grundeinstellung individuell für jede seiner ePA-FdV-Instanzen jederzeit ändern und die Benachrichtigung pro Channel aktivieren ('enabled' - Benachrichtigungen für diesen Kanal), bzw. auch wieder deaktivieren.

Die Verwaltung der individuellen Channelkonfiguration des ePA-Aktenkontos für eine registrierte ePA-FdV-Instanz erfolgt über die Schnittstelle [I_Push_Notification_Management].

A_27641-01 -Push Notification Management - Push Notification Channels

Das Push Notification Management MUSS ausschließlich für die folgenden Ereignisse Push Nachrichten erstellen können, wenn das Ereignis durch einen Nutzer der definierten Nutzergruppe ausgelöst wird und die damit verbundene Operation erfolgreich (nicht

6888 durch einen Fehler abgebrochen) ist.
6889

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

6890 [**<=**]

6891 3.21.4 Push Notification Nachrichteninhalte

6892 (siehe auch: [gemF_PushNotification]#Kapitel "Operation Notify")

6893 Für jedes ausgelöste Ereignis eines Push Channels wird eine Push Notification erstellt. Die
6894 Nachrichtendaten für ein Ereignis werden strukturiert gemäß Schema angeordnet und
6895 nach den Vorgaben in [gemF_PushNotification#A_27610-*] auf konstante Länge
6896 aufgefüllt.

6897 **A_27645 -Push Notification Management - Push Notification Datenstruktur**

6898 Das Push Notification Management MUSS die Nachrichtendaten einer Push Nachricht für
6899 den Versand gemäß [Schema_PushNotifications] strukturieren. [**<=**]

6900 Es gibt eine maximal erlaubte Größe für Nachrichteninhalte, die durch das Push
6901 Notification System [gemF_PushNotification] vorgegeben wird. Es muss sichergestellt
6902 werden, dass erzeugte Nachrichteninhalte diese Größe nicht übersteigen.

6903 **A_27673 -Push Notification Management - Verkürzung der Nachrichteninhalte**

6904 Falls der erzeugte Nachrichtinhalt die maximal erlaubte Größe für Nachrichteninhalte
6905 übersteigt MUSS das Push Notification Management die Elemente `actor`, `title`, `who`,
6906 `folderTitle` so verkürzen, dass die maximal erlaubte Größe für Nachrichteninhalte
6907 gerade nicht überschritten wird. [`<=`]

6908 *Hinweis: Es müssen nicht alle aufgeführten Elemente gleichzeitig verkürzt werden.*

6909 **A_27674 -Push Notification Management - Art der Verkürzung**

6910 Falls Elemente einer Nachricht verkürzt werden, dann sollen diese so verkürzt werden,
6911 dass:

- 6912 • am Ende der Zeichenkette Zeichen entfernt werden
- 6913 • die Verkürzung mit "..." angezeigt wird.

6914 [`<=`]

6915 *Hinweis: Es kann sinnvoll sein, nur das längste kürzbare Element zu kürzen. Es wird*
6916 *empfohlen eine Mindestlänge von 50 Bytes nicht zu unterschreiten.*

6917 **3.21.5 Versenden von Push Nachrichten**

6918 (siehe auch: [gemF_PushNotification]#Kapitel "Operation Notify" und [PushNotificationConcept]#Concept:
6919 "Verschlüsselung des Benachrichtigungsinhalts")

6920 Eine erstellte Push Nachricht wird an jede ePA-FdV-Instanz mit einer Registrierung im
6921 Aktenkonto gesendet, wenn für diese der assoziierte Kanal abonniert wurde
6922 (Konfiguration `channelId == enabled`).

6923 Die längenkorrigierte Nachricht wird jeweils mit dem für den aktuellen Monat gültigen
6924 Schlüssel `AES/CGM-Schlüssel-Jahr-Monat` der Registrierung für jede adressierte ePA-
6925 FdV-Instanz verschlüsselt. Das Verschlüsselungsergebnis ist der Inhalt von `ciphertext`
6926 der `notification` für den Versand ([`I_Push_Gateway`]).

6927 **A_27651 -Push Notification Management - verpflichtende Verschlüsselung der**
6928 **Nachrichteninhalte**

6929 Das Push Notification Management MUSS sicherstellen, dass ausschließlich verschlüsselte
6930 Nachrichteninhalte als Push Nachricht versendet werden. [`<=`]

6931 Jedes einer Push Nachricht zugrundeliegenden Ereignis erzeugt auch einen
6932 Protokolleintrag im Audit Event Service. Die Menge der korrespondierenden
6933 Protokolleinträge ergibt dadurch im Aktenkonto ein Archiv der Push Ereignisse. Damit
6934 Clients ein Push Ereignis zu einem späteren Zeitpunkt, also nachdem die Push Nachricht
6935 im Client selbst schon gelöscht ist, restaurieren können, wird jeder Push Nachricht auch
6936 der Identifier des Protokolleintrags angehängt.

6937 **A_27644 -Push Notification Management - Referenz auf Protokolleintrag**

6938 Das Push Notification Management MUSS den eindeutigen Identifier `Resource.id` des zu
6939 einem Push Notification Ereignis gehörenden Protokolleintrags (AuditEvent) des
6940 Aktenkontos im Feld `notification/identifizier` einer Push Notification angeben. [`<=`]

3.21.6 Protokollierung

A_27636 -Push Notification Management- Protokollierung der ePA-FdV-Instanz-Registrierung

Das Push Notification Management MUSS für Erstellung und Änderung (CUD) von ePA-FdV-Instanz-Registrierungen jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

Tabelle 46: Constraint Management Protokollierung

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die API
	"object"		Bei intern ausgelösten Änderungen (internes Löschen einer ePA-FdV-Instanz-Registrierung nach Löschen Device Registration)
AuditEvent.action	C, U, D		
AuditEvent.entity.name	"PushNotificationManagement"		
AuditEvent.entity.detail	type	value[x]	
	"DisplayNamePusher"	<device_display_name aus der Pusher Registrierung>	
	"DisplayNameDevice"	<displayName der Device Registration>	

[<=]

Hinweis: DisplayNamePusher und DisplayNameDevice können gleich lauten.

A_27662 -Push Notification Management- Protokollierung von Änderungen der Channel Konfiguration

Das Push Notification Management MUSS für Änderungen der Channel-Konfiguration jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

6955 **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>	

6956 **[<=]**

6957 *Hinweis: Die Speicherung von Protokolleinträgen erfordert einen berechtigten Benutzer,*
 6958 *um den Zugriff auf den sicheren Datenspeicher zu gewährleisten. Daher wird die*
 6959 *Erstellung von Protokolleinträgen immer übersprungen und es wird kein Protokolleintrag*
 6960 *gespeichert, wenn diese Bedingung nicht erfüllt ist.*

6961 **3.22 Schnittstellen (OpenAPI)**

6962 Hinweis: Die Vorgaben in den beschreibenden Dateien der REST-Schnittstellen (yaml)
6963 sind normativ für den Anbieter der Schnittstellen. Die Anforderungen im vorliegenden
6964 Dokument ergänzen diese Vorgaben, insbesondere, wenn diese für sicherheitstechnische
6965 Gutachten erforderlich sind.

6966 **3.22.1 Übersicht der Schnittstellen des Aktensystems**

6967 **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.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
getUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine bestimmte LEI aus der Liste der LEIs anzuzeigen, die keinen Zugriff auf den Medication Service haben.
deleteUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI aus der Liste der LEIs zu entfernen, damit diese LEI wieder Zugriff auf den Medication Service haben kann.
I_Constraint_Management_Insurant	
Schnittstelle des Constraint Managements gemäß [I_Constraint_Management_Insurant]	
getDenyPolicyAssignments	Diese Operation gibt eine Liste aller konfigurierten Einträge der General Deny Policy aus.
setPolicyAssignment	Diese Operation fügt der General Deny Policy einen neuen Eintrag hinzu.
deletePolicyAssignment	Diese Operation löscht einen bestimmten Eintrag der General Deny Policy.
I_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.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
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 Zugriffscode 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	

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
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

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
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.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
renderEMLAsPDF	Diese Operation gibt die Medikationsliste im PDF/A-Format zurück.
I_Medication_Service_FHIR	
REST-Schnittstelle zum Abruf der Medikationsdaten im FHIR-Format	
I_Email_Management	
getEmailAddress	Diese Operation ruft die hinterlegte E-Mail-Adresse des Versicherten ab.
replaceEmailAddress	Diese Operation setzt oder ändert die E-Mail Adresse für einen Versicherten ab.
I_Tool_Convert_PDF_Insurant	
Schnittstelle des XDS Document Managements gemäß [I_Tool_Convert_PDF_Insurant]	
convertPDF	Diese Operation konvertiert ein PDF in ein PDF/A Format
I_Data_Submission_Service	
Schnittstelle des Data Submission Service gemäß [I_Data_Submission_Service]	
getSubmissionPackage	Diese Operation stellt dem FDZ ein Datenpaket für eine bestimmte SubmissionID bereit.
I_Push_Notification_Management_Insurant	
Schnittstelle des Push Notification Managements gemäß [I_Push_Notification_Management]	
getPushers	Diese Operation gibt alle Pusher Registrierungen eines Aktenkontos aus
updatePusher	Diese Operation setzt, aktualisiert oder löscht eine Pusher Registrierung
getChannelsOfPusher	Diese Operation gibt die aktuelle Konfiguration der Push Notification Channels für einen Pusher aus

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
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

6968

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 Performedaten 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

6969 Die Schnittstellen (REST) und Operationen sind funktional in den Beschreibungen der
 6970 jeweiligen Schnittstelle beschrieben. Darüber hinaus gelten die folgenden übergreifenden
 6971 Anforderungen.

6972 **3.22.2 Übergreifende Festlegungen zu den Schnittstellen**6973 **A_23918 -Schnittstellen (OpenApi) - Prüfung der Befugnis**

6974 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6975 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6976 eine vorhandene und gültige Befugnis (entitlement) für den Nutzer der Operation fordern
6977 und diese nicht vorliegt. [\leq]

6978 *Hinweis: A_23918 deckt auch die Fehlersituationen "kein VAU-Kanal" und "keine User*
6979 *Session" ab, da diese eine Vorbedingung für den Nachweis einer gültigen Befugnis sind.*

6980 **A_24365 -Schnittstellen (OpenApi) - Prüfung des Aktenkontos**

6981 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6982 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6983 die Existenz des adressierten Aktenkontos fordern und diese nicht für den
6984 Operationsaufruf verwendet wird. [\leq]

6985 *Hinweis A_24365 deckt auch die Fehlersituation "kein Health Record Context" ab, da*
6986 *dieses nur infolge eines nicht vorhandenen Aktenkontos auftritt.*

6987 **A_24538 -Schnittstellen (OpenApi) - Prüfung des Aktenkontostatus**

6988 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6989 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6990 einen vorgegebenen Status des Aktenkontos fordern und dieser nicht vorhanden ist. [\leq]

6991 **A_24366 -Schnittstellen (OpenApi) - Prüfung der Rolle**

6992 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6993 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6994 die Zulässigkeit der Operation auf bestimmte Rollen (professionOID) einschränken und
6995 der Nutzer der Operation diese nicht nachweist. [\leq]

6996 **A_24367 -Schnittstellen(OpenApi) - Prüfung des Identifiers**

6997 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
6998 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
6999 die Zulässigkeit der Operation auf bestimmte Identifier (KVNR oder Telematik-ID)
7000 einschränken und der Nutzer der Operation diese nicht nachweist. [\leq]

7001 **A_24580 -Schnittstellen (OpenApi) - Protokollierung der Operationen**

7002 Das ePA-Aktensystem MUSS nach der Ausführung der Operationen der REST-
7003 Schnittstellen eine Protokolleintrag erstellen, wenn die Protokollierung in den
7004 Nachbedingungen (Postconditions) der Operationen gefordert ist (log-entry). [\leq]

4 Informationsmodelle

7005

7006 Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten
7007 wird nicht benötigt.

7008

5 Anhang A – Verzeichnisse

7009

5.1 Abkürzungen

Kürzel	Erläuterung
AdV	Anwendungen des Versicherten
AN	Arbeitsnummer in der Übermittlung von Daten zur Sekundärnutzung
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BGP	Border Gateway Protokoll
BPPC	Basic Patient Privacy Consents
CRUD	Create Read Update Delete
DiGA	Digitale Gesundheitsanwendung
ePA-FdV	ePA-Frontend des Versicherten
ePA-FdV AdV	ePA-Frontend des Versicherten im KTR-AdV-Terminal
FDZ	Forschungsdatenzentrum Gesundheit
HL7	Health Level Seven
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IHE ITI TF	IHE IT Infrastructure Technical Framework
JWT	JSON-Web-Token
JWS	signiertes JSON-Web-Token

Kürzel	Erläuterung
KTR	Kostenträger
LP	Lieferpseudonym in der Übermittlung von Daten zur Sekundärnutzung
MIO	Medizinisches Informationsobjekt
MHD	Mobile access to Health Documents (FHIR-Service im Aktensystem u.a. für Volltextsuche)
MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
PDSG	Patientendaten-Schutz-Gesetz
PHR	Personal Health Record
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

7010 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]).

7011 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung
7012 gestellt.

7013 5.3 Abbildungsverzeichnis

7014	Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls.....47
7015	Abbildung 2 - Überblick Service-VAUs81
7016	Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung84
7017	Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer
7018	Überschlüsselung86
7019	Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP ..229
7020	Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP233
7021	Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes235
7022	Abbildung 8: Dokumente mit Anhangsbeziehungen.....278
7023	Abbildung 9: Beispiel Verweiszirkel und doppelte Eltern.....280
7024	Abbildung 10: Beispiel Anhangskette zu lang281
7025	

7026 5.4 Tabellenverzeichnis

7027	Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat18
7028	Tabelle 2: Zustandswechsel im Lebenszyklus eines Aktenkontos.....27
7029	Tabelle 3 : Health Record Relocation Service Protokollierung37
7030	Tabelle 4: Tab_AS_VAU_Token_Modul_Rules -Prüfregeln VAU Token48
7031	Tabelle 5: Überblick über die Regeln des Befugnisverifikations-Moduls54
7032	Tabelle 6: Tab_AS_Entitlement_Registration_Rules - Regeln zur Registrierung von
7033	Befugnissen56
7034	Tabelle 7: Tab_AS_SDS-Key_Rules Key Rules - Regeln zur Ableitung der
7035	versichertenindividuellen Persistierungsschlüssel66
7036	Tabelle 8: Widerspruchsfähige Funktionen der elektronischen Patientenakte89

7037	Tabelle 9: Consent Decision Management Protokollierung - Widersprüche für Funktionen	
7038	der ePA	91
7039	Tabelle 10: Consent Decision Management Protokollierung - unveränderte	
7040	Entscheidungen zu widerspruchsfähigen Funktionen der ePA.....	92
7041	Tabelle 11: Consent Decision Management Protokollierung - Widersprüche zu	
7042	Sekundärnutzungszwecken	93
7043	Tabelle 12: Consent Decision Management Protokollierung - unveränderte Widersprüche	
7044	zu Sekundärnutzungszwecken.....	94
7045	Tabelle 13: Consent Decision Management Protokollierung - User Specific Deny Policy	
7046	Medication	96
7047	Tabelle 14: Inhalt einer Befugnis	97
7048	Tabelle 15: Befugnisse für berechtigte Nutzergruppen und Nutzer	99
7049	Tabelle 16: Befugnisse EU-Zugriff für berechtigte Nutzergruppen und Nutzer	101
7050	Tabelle 17: Entitlement Management Protokollierung	103
7051	Tabelle 18: Inhalt eines Blocked User Policy Eintrags	111
7052	Tabelle 19: Legal Policy	118
7053	Tabelle 20: Legal Policy - EU-Zugriff	121
7054	Tabelle 21: Beschreibung der Kategorien.....	123
7055	Tabelle 22: Constraint Management Protokollierung.....	127
7056	Tabelle 23: Inhalt eines General Deny Policy Eintrags	130
7057	Tabelle 24: Verbergen eines Medical Service.....	130
7058	Tabelle 25: Kennzeichnung von Optionalitäten	143
7059	Tabelle 26: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den	
7060	Außerschnittstellen des XDS Document Service	144
7061	Tabelle 27: Schnittstelle I_Document_Management	166
7062	Tabelle 28: Schnittstelle I_Document_Management_Insurant	169
7063	Tabelle 29: Schnittstelle I_Document_Management_Ncpeh.....	171
7064	Tabelle 30: Festlegung Folder.entryUUIDzu statischen Ordnern	172
7065	Tabelle 31: Nutzungsvorgaben für Metadatenattribute XDS	175
7066	Tabelle 32: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language	
7067	Codes	192
7068	Tabelle 33: Einsortierung_Datenkategorien.....	198
7069	Tabelle 34: TAB_EPA_Sammlungstypen	201
7070	Tabelle 35: Auswirkungen bei Widerspruch gegen eine Funktion der ePA.....	205
7071	Tabelle 36: XDS Document Service Protokollierung.....	206
7072	Tabelle 37: Patient Service Protokollierung	210
7073	Tabelle 38: Medication Service Protokollierung	212
7074	Tabelle 39: MHD Service Protokollierung	216
7075	Tabelle 40 : Inhaltliche Definitionen eines AuditEvent	218

7076	Tabelle 41 Befüllung AuditEvent	219
7077	Tabelle 42 Audit Event Management Protokollierung - Fehler	223
7078	Tabelle 43: Audit Event Service Protokollierung	224
7079	Tabelle 44: Auswahl der zu übertragenden FHIR-Ressourcen	244
7080	Tabelle 45: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen	244
7081	Tabelle 46: Constraint Management Protokollierung	252
7082	Tabelle 47: Constraint Management Protokollierung	253
7083	Tabelle 48: Übersicht der Schnittstellen des Aktensystems	255
7084		

7085 5.5 Referenzierte Dokumente

7086 5.5.1 Dokumente der gematik

7087 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
7088 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

[Quelle]	Herausgeber: Titel
[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-3.1.3
[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

[Quelle]	Herausgeber: Titel
[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-3.1.3
[I_Constraint_Management_Insur- rant]	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.ya ml
[I_Tool_Convert_PDF_Insurant]	gematik: I_Tool_Convert_PDF_Insurant Schnittstelle für die PDF Formatkonvertierung siehe [ePA_XDS_Document] Path: src/openapi/ I_Tool_Convert_PDF_Insurant.yaml
[XDSDocumentService]	gematik: XDSDocumentService.wsdl IHE-Schnittstelle des XDSDocumentService siehe [ePA_XDS_Document] Path: src/schema
[HealthRecordMigration]	gematik: ref-ePA-HealthRecordMigration Referenzimplementierung und Vorgaben für das Exportpaket bei einem Anbieterwechsel GitHub: https://github.com/gematik/ref-ePA- HealthRecordMigration/tree/ePA-3.1
[IG_Basic]	gematik: FHIR Implementation Guide "ePA Basisfunktionalitäten" https://gematik.de/fhir/epa/1.2.0

[Quelle]	Herausgeber: Titel
[IG_Medication_Service]	gematik: FHIR Implementation Guide "ePA Medication Service" https://gematik.de/fhir/epa-medication/1.2.0
[IG_MHD_Service]	gematik: FHIR Implementation Guide "ePA MHD Service" https://gematik.de/fhir/epa-mhd/1.0.1
[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

[Quelle]	Herausgeber: Titel
[I_Push_Gateway]	gematik: Push Gateway API REST-Schnittstelle des Push Gateways zum Versand von Push Nachrichten GitHub: https://gematik.github.io/gem-push-notifications-concept/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

7089 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/

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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/

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[WSIAP]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[WSIBSP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html
[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/
[XHTML]	W3C (2010): XHTML 1.1 - Module-based XHTML - Second Edition, https://www.w3.org/TR/xhtml1/

7090

6 Anhang B – Erläuternde Informationen

7091
7092

Dieser Anhang enthält nicht normative Informationen, die dazu dienen, das Verständnis der Spezifikation zu vereinfachen.

7093

6.1 Dokumentenanhänge

7094
7095
7096

Der vorliegende Abschnitt enthält einige Abbildungen, die das Konzept der Dokumentenanhänge in der ePA für alle visuell erläutern und damit leichter verständlich machen sollen.

7097

6.1.1 Überblick

7098
7099
7100

Die folgende Abbildung zeigt fünf Dokumente (bzw. DocumentEntries), die teilweise über Anhangsbeziehungen miteinander verbunden sind:

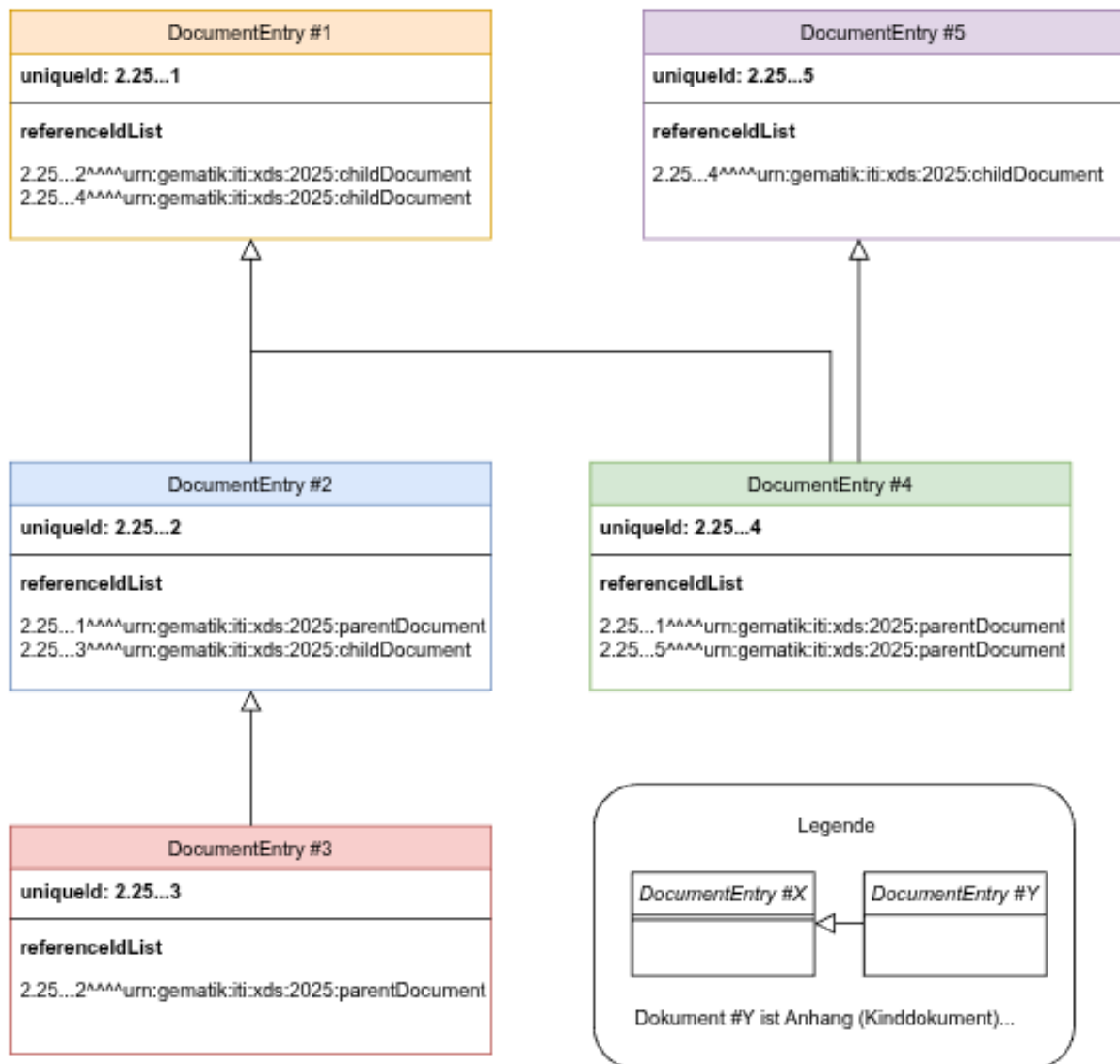


Abbildung 8: Dokumente mit Anhangsbeziehungen

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.
 - ist selbst an Dokument #2 angehängt.
- Dokument #4

- 7123 • besitzt keine Anhänge.
- 7124 • ist selbst an zwei Dokumente angehängt (Dokumente #1 und #5)
- 7125 • Dokument #5
- 7126 • besitzt einen Anhang (Dokument #4).

7127 **Notation**

7128 Jedes Dokument verweist auf Dokumentenanhänge über einen Eintrag in seiner
 7129 referenceIdList
 7130 (`<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2025:childDocument`), wobei
 7131 `DocumentEntry.uniqueId` sich auf die eindeutige Kennung des Anhangsdokuments
 7132 bezieht. In der Spezifikation wird der Anhang manchmal als Kinddokument bezeichnet,
 7133 und das Dokument, an dem es hängt als Elterndokument. In diesem Sinne ist Dokument
 7134 #3 bspw. das Kinddokument von Dokument #2.

7135 **Anzahl Anhänge**

7136 Wie aus der Abbildung hervorgeht, kann ein Dokument mehrere Anhänge besitzen; im
 7137 Beispiel verfügt Dokument über zwei Anhänge. Umgekehrt kann auch jeder Anhang an
 7138 mehr als einem Dokument hängen (im Beispiel ist Dokument #4 Anhang sowohl für
 7139 Dokument #1 also auch Dokument #5).

7140 Die Beziehung zwischen Eltern- und Kinddokumenten ist also m:n: Ein Dokument kann
 7141 beliebig viele Anhänge besitzen und ein Anhang kann an beliebig vielen Dokumenten
 7142 anhängen.

7143 **6.1.2 Ungültige Anhänge**

7144 Dieser Abschnitt illustriert einige nicht erlaubte Anhangsszenarien.

6.1.2.1 Verweiszirkel und doppelte Eltern

Die folgende Abbildung demonstriert Anhänge, wie sie nicht in den XDS Document Service eingebracht werden können:

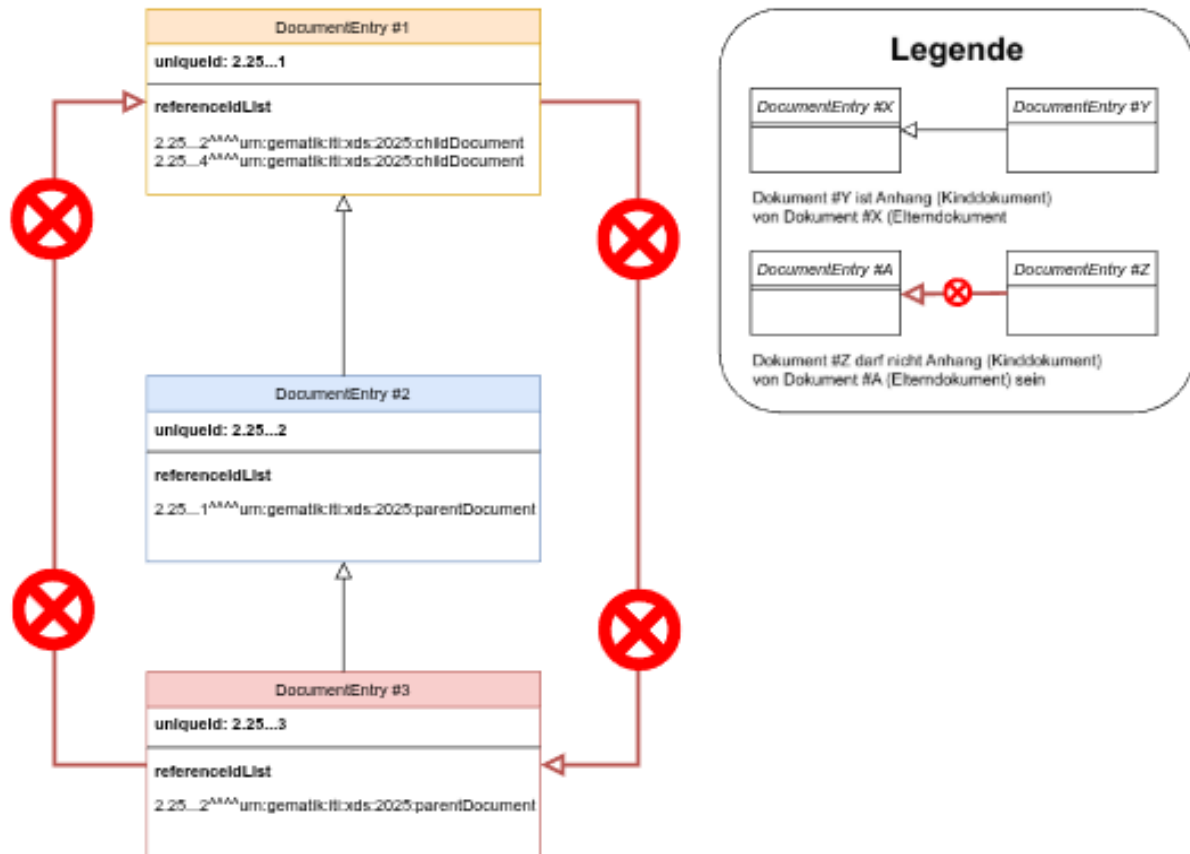


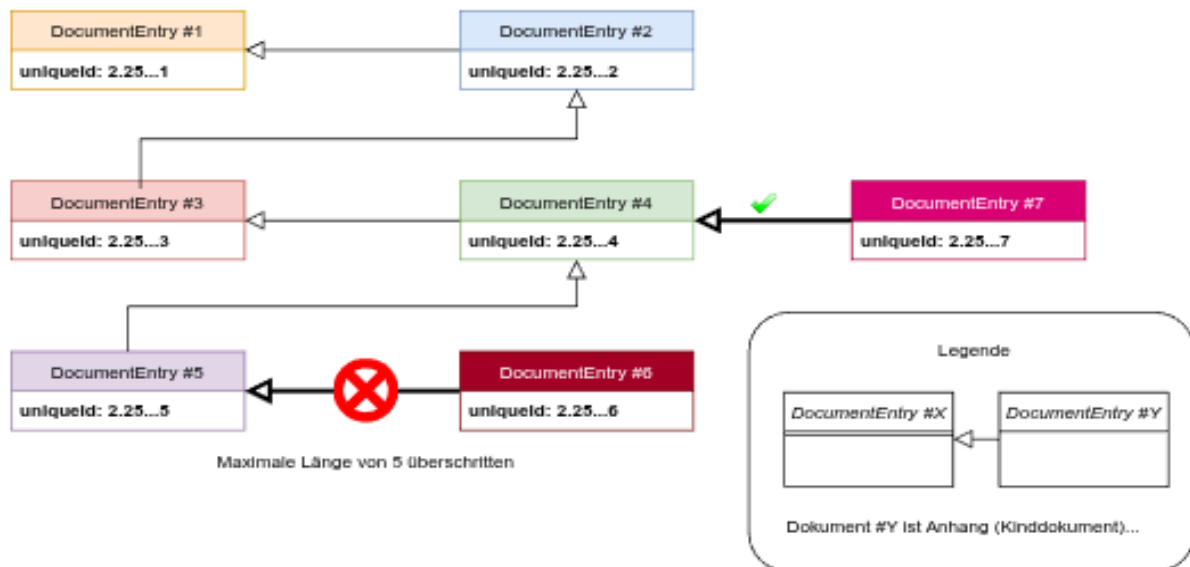
Abbildung 9: Beispiel Verweiszirkel und doppelte Eltern

- Ausgangssituation (unproblematisch):
 - Dokument #3 ist Anhang zu Dokument #2.
 - Dokument #2 ist Anhang zu Dokument #1.
- Falls nun anschließend versucht wird, Dokument #3 als Kind von Dokument #1 einzutragen (roter Pfeil auf der linken Seite), ist dies nicht erlaubt, da ein Dokument nicht Anhang zu zweien seiner "Vorfahren" in der Anhangskette sein darf (denn Dokument #3 ist bereits Anhang von Dokument #2, das wiederum an Dokument #1 hängt).
- Auch der Versuch, Dokument #1 als Anhang zu Dokument #3 zu markieren schlägt fehl, denn es würde ein Verweiszirkel entstehen, in dem ein Kinddokument gleichzeitig Elterndokument für eines seiner Vorfahren ist.

6.1.2.2 Anhangskette zu lang

Die maximale Länge der Anhangsketten ist auf fünf beschränkt. Die folgende Abbildung zeigt, in welchem Fall das Hinzufügen eines weiteren Anhangs zu Problemen führt (und

7167 wann nicht):
7168



7169
7170

Abbildung 10: Beispiel Anhangskette zu lang

- 7171 • Ausgangssituation (Dokumente #1-#5) unproblematisch. Länge der Anhangskette
7172 ist fünf.
- 7173 • Wenn versucht wird, Dokument #6 einzufügen, ist die Anhangskette zu lang.
- 7174 • Das würde auch gelten, wenn der Einstellende bspw. Dokumente #1 und #2
7175 gar nicht sehen könnte (Legal Policy, Verbergen)
- 7176 • Es würde ein Fehler zurückgegeben.
- 7177 • Das Einstellen von Dokument #7 wäre unproblematisch.
- 7178 • Die Anhangskette von Dokument #7 hätte fünf Dokumente, Dokument #6
7179 gehört also nicht mit dazu.
- 7180 • Das Dokument könnte auf diese Weise als Anhang an Dokument #4 eingestellt
7181 werden.

7182
7183
7184