

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation Aktensystem ePA für alle

Version:	1. <del>34</del> .0 <u>CC</u>
Revision:	<del>986724</del> <u>1132068</u>
Stand:	14. <del>08.2024</del> <u>02.2025</u>
Status:	<u>zur Abstimmung</u> freigegeben
Klassifizierung:	öffentlich <u>Entwurf</u>
Referenzierung:	gemSpec_Aktensystem_ePAfueralle

26

**Dokumenteninformationen**

27

**Änderungen zur Vorversion**

28

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

30

31

**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
<u>1.3.0</u>	<u>14.08.2024</u>		<u>ePA für alle -Release 3.1.0</u>	<u>gematik</u>
<u>1.34.0</u> <u>CC</u>	<u>14.08.2024</u> <u>02.2025</u>		<b>ePA für alle - Release 3.0.5</b> (Themen dgMP und Datenausleitung zur Sekundärdatennutzung für ePA für alle 3.1- <del>0</del> herausgenommen)	gematik

## Inhaltsverzeichnis

<b>1 Einführung</b>	<b>11</b>
1.1 Zielsetzung	11
1.2 Zielgruppe	11
1.3 Geltungsbereich	11
1.4 Abgrenzungen	11
1.5 Methodik	12
<b>2 Übergreifende Festlegungen</b>	<b>13</b>
2.1 Aktensystem und Service-Lokalisierung	14
2.2 Redundanz	16
2.3 Datenschutz und Sicherheit	17
2.4 Validierungsaktenkonto	22
2.5 Tracing in Nichtproduktivumgebungen	25
2.6 Benutzerführung	26
2.7 Useragent	27
2.8 Datenmigration	27
2.8.1 Herstellerspezifische Umsetzung der Datenmigration	28
2.8.2 Durchführung der Migration	29
2.8.3 Bereinigung von Registry und Repository im Zuge der Migration	29
2.8.4 Protokollierung der Migration	33
2.9 Performance aus Anwendersicht	35
<b>3 Funktionsmerkmale</b>	<b>37</b>
3.1 Aktenkonto eines Versicherten (Health Record)	37
3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte	37
3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger	37
3.1.2 Lebenszyklus und Zustände eines Aktenkontos	38
3.1.3 Anlage eines neuen Aktenkontos	40
3.1.4 Löschen eines Aktenkontos	43
3.2 Health Record Relocation Service	43
3.2.1 Ablauf eines Aktenkontoumzugs	48
3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter	48
3.2.1.2 Abfrage existierendes Aktenkonto und Anfrage zum Transfer	49
3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen Anbieter	49
3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den neuen Anbieter	50
3.2.1.5 Import des Exportpakets durch den neuen Anbieter	50
3.2.1.6 Abschluss des Transfers durch beide Anbieter	50
3.2.1.7 Fehlersituationen und Handhabung	51

72	3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich	
73	oder derzeit nicht möglich .....	51
74	3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter .....	51
75	3.2.1.7.3 Nicht-erfolgter Download oder fehlende Rückmeldung durch den neuen	
76	Anbieter .....	52
77	3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter .....	53
78	<b>3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM</b>	
79	.....	<b>54</b>
80	<b>3.4 Befugnisverifikations-Modul .....</b>	<b>57</b>
81	3.4.1 VAU-Token-Modul .....	58
82	3.4.2 Regeln des Befugnisverifikations-Moduls .....	65
83	<b>3.5 Vertrauenswürdige Ausführungsumgebung (VAU) .....</b>	<b>83</b>
84	3.5.1 Übergreifende VAU-Anforderungen .....	84
85	3.5.1.1 Schutz der Integrität der VAU .....	84
86	3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU .....	85
87	3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU .....	86
88	3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM .....	86
89	3.5.1.5 Logging und Monitoring .....	86
90	3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU .....	88
91	3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU ...	88
92	3.5.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-	
93	VAU .....	89
94	3.5.2.3 Konsistenz des Systemzustands .....	90
95	3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU .....	90
96	3.5.4 Zusätzliche Anforderungen an eine Service-VAU .....	91
97	3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU .....	93
98	<b>3.6 Umschlüsselung und Überschlüsselung .....</b>	<b>93</b>
99	<b>3.7 User Session und Health Record Context .....</b>	<b>97</b>
100	<b>3.8 Consent Decision Management .....</b>	<b>98</b>
101	3.8.1 Widersprüche für Funktionen der ePA .....	98
102	3.8.2 Einschränkung der Verwendung von Daten auf bestimmte	
103	Sekundärnutzungszwecke .....	102
104	3.8.3 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny	
105	Policy Medication) .....	104
106	<b>3.9 Entitlement Management .....</b>	<b>106</b>
107	3.9.1 Initiale Befugnisse (static Entitlements) .....	113
108	3.9.2 Erstellen einer Befugnis durch Clients .....	115
109	3.9.2.1 Befugnisvergabe durch ein ePA-FdV .....	115
110	3.9.2.2 Befugnisvergabe durch ein Primärsystem .....	117
111	3.9.3 Löschen von Befugnissen .....	119
112	3.9.4 Befugnisausschluss (Blocked User Policy) .....	120
113	<b>3.10 Legal Policy .....</b>	<b>124</b>
114	<b>3.11 Constraint Management .....</b>	<b>132</b>
115	3.11.1 Aktenkontoweites Verbergen (General Deny Policy) .....	135
116	3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes	
117	.....	137
118	<b>3.12 Device Management .....</b>	<b>137</b>

119	<b>3.13 Medical Services .....</b>	<b>141</b>
120	3.13.1 XDS Document Service .....	142
121	3.13.1.1 Formatprüfung beim Einstellen von Dokumenten .....	142
122	3.13.1.2 Anforderungen zur Validierung .....	145
123	3.13.1.3 Namensräume .....	146
124	3.13.1.4 Nutzung von IHE IT Infrastructure Profilen für Speicherung und Abruf von Dokumenten .....	147
125	3.13.1.4.1 Anforderungen an IHE ITI Akteure .....	147
126	3.13.1.4.2 Überblick über gruppierte IHE ITI Akteure und Optionen .....	150
127	3.13.1.4.3 Vorgaben zu IHE ITI Transaktionen bei mehreren Schnittstellen ...	153
128	3.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS Operationen .....	161
129	3.13.1.5 Fehlerbehandlung in Schnittstellenoperationen .....	162
130	3.13.1.6 Schnittstellen im XDS Document Service .....	163
131	3.13.1.6.1 Schnittstelle I_Document_Management .....	163
132	3.13.1.6.2 Schnittstelle I_Document_Management_Insurant .....	167
133	3.13.1.7 Statische Metadaten .....	170
134	3.13.1.8 Nutzungsvorgaben für IHE ITI XDS Metadaten .....	172
135	3.13.1.8.1 Allgemeine Metadatenvorgaben .....	172
136	3.13.1.8.2 Metadaten der Dokumente und SubmissionSets .....	192
137	3.13.1.8.3 Metadaten für Datenkategorien .....	196
138	3.13.1.9 Strukturierte Dokumente .....	198
139	3.13.1.9.1 Sammlungstypen .....	198
140	3.13.1.9.2 Konfigurierbarkeit .....	200
141	3.13.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode .....	201
142	3.13.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die Dokumente des Aktenkontos .....	202
143	3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI auf die Dokumente des Aktenkontos .....	203
144	3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service .....	203
145	3.13.1.14 Unterstützungsleistung für das ePA-FdV .....	206
146	3.13.2 FHIR Data Services .....	208
147	3.13.2.1 Patient Information Service .....	208
148	3.13.2.2 Medication Service .....	208
149	<b>3.14 Audit Event Service .....</b>	<b>215</b>
150	<b>3.15 Information Service .....</b>	<b>224</b>
151	3.15.1 Information Service .....	224
152	3.15.1.1 Informationen zu Widersprüchen (Consent Decisions) .....	225
153	3.15.1.2 Informationen zur Anwenderperformance (UX Performance) .....	225
154	3.15.2 Information Service – Account .....	225
155	<b>3.16 Email Management .....</b>	<b>226</b>
156	<b>3.17 Zusätzliche Anforderungen an den Authorization Service .....</b>	<b>227</b>
157	3.17.1 Anforderungen an den Authorization Service für die Authentisierung von Versicherten (FdV) .....	228
158	3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B .....	233
159		
160		
161		
162		
163		
164		

165	3.17.3 Anforderungen an den Authorization Service für die Authentisierung des E-	
166	Rezept-Fachdienstes .....	235
167	<b>3.18 Anbindung Verzeichnisdienst FHIR Directory .....</b>	<b>236</b>
168	<b>3.19 Access Gateway .....</b>	<b>236</b>
169	3.19.1 Paketfilter .....	236
170	3.19.1.1 Funktion .....	236
171	3.19.1.2 Redundanz .....	238
172	3.19.1.3 Konfiguration .....	238
173	3.19.1.4 Adressierung .....	238
174	3.19.1.4.1 Access Gateway zum Transportnetz Internet .....	238
175	3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz .....	239
176	3.19.2 Proxy für das VAU-Protokoll .....	239
177	3.19.3 Proxy Schlüsselgenerierungsdienst .....	239
178	3.19.4 Tracing in Nichtproduktivumgebungen .....	239
179	3.19.5 Übergreifende Festlegungen .....	241
180	<b>3.20 Data Submission Service .....</b>	<b>242</b>
181	3.20.1 Erstellung von Arbeitsnummern und Lieferpseudonymen .....	243
182	3.20.2 Auswahl von medizinischen Daten .....	243
183	3.20.3 Pseudonymisierung von medizinischen Daten .....	247
184	3.20.4 Übermittlung der pseudonymisierten medizinischen Daten .....	248
185	<b>3.21 Schnittstellen (OpenAPI) .....</b>	<b>250</b>
186	3.21.1 Übersicht der Schnittstellen des Aktensystems .....	251
187	3.21.2 Übergreifende Festlegungen zu den Schnittstellen .....	258
188	<b>4 Informationsmodelle .....</b>	<b>259</b>
189	<b>5 Anhang A Verzeichnisse .....</b>	<b>260</b>
190	5.1 Abkürzungen .....	260
191	5.2 Glossar .....	262
192	5.3 Abbildungsverzeichnis .....	262
193	5.4 Tabellenverzeichnis .....	263
194	5.5 Referenzierte Dokumente .....	266
195	5.5.1 Dokumente der gematik .....	266
196	5.5.2 Weitere Dokumente .....	269
197	<b>1 Einführung .....</b>	<b>11</b>
198	1.1 Zielsetzung .....	11
199	1.2 Zielgruppe .....	11
200	1.3 Geltungsbereich .....	11
201	1.4 Abgrenzungen .....	11
202	1.5 Methodik .....	12
203	<b>2 Übergreifende Festlegungen .....</b>	<b>13</b>
204	2.1 Aktensystem- und Service-Lokalisierung .....	14
205	2.2 Redundanz .....	16

206	<b>2.3 Datenschutz und Sicherheit .....</b>	<b>17</b>
207	<b>2.4 Validierungsaktenkonto .....</b>	<b>22</b>
208	<b>2.5 Tracing in Nichtproduktivumgebungen .....</b>	<b>25</b>
209	<b>2.6 Benutzerführung .....</b>	<b>26</b>
210	<b>2.7 Useragent .....</b>	<b>27</b>
211	<b>2.8 Datenmigration .....</b>	<b>27</b>
212	2.8.1 Herstellerspezifische Umsetzung der Datenmigration .....	28
213	2.8.2 Durchführung der Migration .....	29
214	2.8.3 Bereinigung von Registry und Repository im Zuge der Migration .....	29
215	2.8.4 Protokollierung der Migration .....	33
216	2.8.5 Weitere Datenanpassungen .....	35
217	<b>2.9 Performance aus Anwendersicht .....</b>	<b>35</b>
218	<b>3 Funktionsmerkmale .....</b>	<b>37</b>
219	<b>3.1 Aktenkonto eines Versicherten (Health Record) .....</b>	<b>37</b>
220	3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen	
221	Patientenakte .....	37
222	3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den	
223	Kostenträger .....	37
224	3.1.2 Lebenszyklus und Zustände eines Aktenkontos .....	38
225	3.1.3 Anlage eines neuen Aktenkontos .....	40
226	3.1.4 Löschen eines Aktenkontos .....	43
227	<b>3.2 Health Record Relocation Service .....</b>	<b>43</b>
228	3.2.1 Ablauf eines Aktenkontoumzugs .....	48
229	3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter .....	48
230	3.2.1.2 Start Transfer eines existierenden Aktenkontos .....	49
231	3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen Anbieter .....	49
232	3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den neuen	
233	Anbieter .....	50
234	3.2.1.5 Import des Exportpakets durch den neuen Anbieter .....	50
235	3.2.1.6 Abschluss des Transfers durch beide Anbieter .....	50
236	3.2.1.7 Fehlersituationen und Handhabung .....	51
237	3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich	
238	oder derzeit nicht möglich .....	51
239	3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter .....	51
240	3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen	
241	Anbieter .....	52
242	3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter .....	53
243	<b>3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM</b>	
244	<b>.....</b>	<b>54</b>
245	<b>3.4 Befugnisverifikations-Modul .....</b>	<b>57</b>
246	3.4.1 VAU-Token-Modul .....	58
247	3.4.2 Regeln des Befugnisverifikations-Moduls .....	65
248	<b>3.5 Vertrauenswürdige Ausführungsumgebung (VAU) .....</b>	<b>83</b>
249	3.5.1 Übergreifende VAU-Anforderungen .....	84
250	3.5.1.1 Schutz der Integrität der VAU .....	84
251	3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU .....	85

252	<u>3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU.....</u>	86
253	<u>3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM.....</u>	86
254	<u>3.5.1.5 Logging und Monitoring.....</u>	86
255	<u>3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU.....</u>	88
256	<u>3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU ...</u>	88
257	<u>3.5.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-</u>	
258	<u>VAU.....</u>	89
259	<u>3.5.2.3 Konsistenz des Systemzustands .....</u>	90
260	<u>3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU.....</u>	90
261	<u>3.5.4 Zusätzliche Anforderungen an eine Service-VAU .....</u>	91
262	<u>3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU.....</u>	93
263	<b><u>3.6 Umschlüsselung und Überschlüsselung .....</u></b>	<b>93</b>
264	<b><u>3.7 User Session und Health Record Context.....</u></b>	<b>97</b>
265	<b><u>3.8 Consent Decision Management .....</u></b>	<b>98</b>
266	<u>3.8.1 Widersprüche für Funktionen der ePA .....</u>	98
267	<u>3.8.2 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny</u>	
268	<u>Policy Medication).....</u>	104
269	<b><u>3.9 Entitlement Management.....</u></b>	<b>106</b>
270	<u>3.9.1 Initiale Befugnisse (static Entitlements) .....</u>	113
271	<u>3.9.2 Erstellen einer Befugnis durch Clients .....</u>	115
272	<u>3.9.2.1 Befugnisvergabe durch ein ePA-FdV.....</u>	115
273	<u>3.9.2.2 Befugnisvergabe durch ein Primärsystem .....</u>	117
274	<u>3.9.3 Löschen von Befugnissen .....</u>	119
275	<u>3.9.4 Befugnisausschluss (Blocked User Policy) .....</u>	120
276	<u>3.9.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting) .....</u>	122
277	<b><u>3.10 Legal Policy .....</u></b>	<b>124</b>
278	<b><u>3.11 Constraint Management.....</u></b>	<b>132</b>
279	<u>3.11.1 Aktenkontoweites Verbergen (General Deny Policy) .....</u>	135
280	<u>3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes</u>	
281	<u>.....</u>	137
282	<b><u>3.12 Device Management .....</u></b>	<b>137</b>
283	<b><u>3.13 Medical Services .....</u></b>	<b>141</b>
284	<u>3.13.1 XDS Document Service .....</u>	142
285	<u>3.13.1.1 Formatprüfung beim Einstellen von Dokumenten .....</u>	142
286	<u>3.13.1.2 Anforderungen zur Validierung .....</u>	145
287	<u>3.13.1.3 Namensräume.....</u>	146
288	<u>3.13.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von</u>	
289	<u>Dokumenten.....</u>	147
290	<u>3.13.1.4.1 Anforderungen an IHE ITI-Akteure.....</u>	147
291	<u>3.13.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen .....</u>	150
292	<u>3.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen ...</u>	153
293	<u>3.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen .....</u>	161
294	<u>3.13.1.5 Fehlerbehandlung in Schnittstellenoperationen .....</u>	162
295	<u>3.13.1.6 Schnittstellen im XDS Document Service .....</u>	163
296	<u>3.13.1.6.1 Schnittstelle I Document Management.....</u>	163
297	<u>3.13.1.6.2 Schnittstelle I Document Management Insurant .....</u>	167
298	<u>3.13.1.6.3 Schnittstelle I Document Management Ncpeh .....</u>	169



299	<u>3.13.1.7 Statische Metadaten .....</u>	<u>170</u>
300	<u>3.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten .....</u>	<u>172</u>
301	<u>3.13.1.8.1 Allgemeine Metadatenvorgaben .....</u>	<u>172</u>
302	<u>3.13.1.8.2 Metadaten der Dokumente und SubmissionSets .....</u>	<u>192</u>
303	<u>3.13.1.8.3 Metadaten für Datenkategorien .....</u>	<u>196</u>
304	<u>3.13.1.9 Strukturierte Dokumente .....</u>	<u>198</u>
305	<u>3.13.1.9.1 Sammlungstypen .....</u>	<u>198</u>
306	<u>3.13.1.9.2 Konfigurierbarkeit .....</u>	<u>200</u>
307	<u>3.13.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode .....</u>	<u>201</u>
308	<u>3.13.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die .....</u>	<u>202</u>
309	<u>Dokumente des Aktenkontos .....</u>	<u>202</u>
310	<u>3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication .....</u>	<u>203</u>
311	<u>Service durch eine spezifische LEI auf die Dokumente des Aktenkontos .....</u>	<u>203</u>
312	<u>3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service .....</u>	<u>203</u>
313	<u>3.13.1.14 Unterstützungsleistung für das ePA-FdV .....</u>	<u>206</u>
314	<u>3.13.2 FHIR Data Services .....</u>	<u>208</u>
315	<u>3.13.2.1 Patient Information Service .....</u>	<u>208</u>
316	<u>3.13.2.2 Medication Service .....</u>	<u>208</u>
317		
318	<b><u>3.14 Audit Event Service .....</u></b>	<b><u>215</u></b>
319	<b><u>3.15 Information Service .....</u></b>	<b><u>224</u></b>
320	<u>3.15.1 Information Service .....</u>	<u>224</u>
321	<u>3.15.1.1 Informationen zu Widersprüchen (Consent Decisions) .....</u>	<u>225</u>
322	<u>3.15.1.2 Informationen zur Anwenderperformance (UX Performance) .....</u>	<u>225</u>
323	<u>3.15.2 Information Service - Account .....</u>	<u>225</u>
324	<b><u>3.16 Email Management .....</u></b>	<b><u>226</u></b>
325	<b><u>3.17 Zusätzliche Anforderungen an den Authorization Service .....</u></b>	<b><u>227</u></b>
326	<u>3.17.1 Anforderungen an den Authorization Service für die Authentisierung von .....</u>	<u>228</u>
327	<u>Versicherten (FdV) .....</u>	<u>228</u>
328	<u>3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B .....</u>	<u>233</u>
329	<u>3.17.3 Anforderungen an den Authorization Service für die Authentisierung des E- .....</u>	<u>235</u>
330	<u>Rezept-Fachdienstes .....</u>	<u>235</u>
331		
332	<b><u>3.18 Anbindung Verzeichnisdienst FHIR-Directory .....</u></b>	<b><u>236</u></b>
333	<b><u>3.19 Access Gateway .....</u></b>	<b><u>236</u></b>
334	<u>3.19.1 Paketfilter .....</u>	<u>236</u>
335	<u>3.19.1.1 Funktion .....</u>	<u>236</u>
336	<u>3.19.1.2 Redundanz .....</u>	<u>238</u>
337	<u>3.19.1.3 Konfiguration .....</u>	<u>238</u>
338	<u>3.19.1.4 Adressierung .....</u>	<u>238</u>
339	<u>3.19.1.4.1 Access Gateway zum Transportnetz Internet .....</u>	<u>238</u>
340	<u>3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz .....</u>	<u>239</u>
341	<u>3.19.2 Proxy für das VAU-Protokoll .....</u>	<u>239</u>
342	<u>3.19.3 Proxy Schlüsselgenerierungsdienst .....</u>	<u>239</u>
343	<u>3.19.4 Tracing in Nichtproduktivumgebungen .....</u>	<u>239</u>
344	<u>3.19.5 Übergreifende Festlegungen .....</u>	<u>241</u>
345	<b><u>3.20 Schnittstellen (OpenAPI) .....</u></b>	<b><u>250</u></b>

346	3.20.1 Übersicht der Schnittstellen des Aktensystems .....	251
347	3.20.2 Übergreifende Festlegungen zu den Schnittstellen .....	258
348	<b>4 Informationsmodelle .....</b>	<b>259</b>
349	<b>5 Anhang A – Verzeichnisse .....</b>	<b>260</b>
350	5.1 Abkürzungen .....	260
351	5.2 Glossar .....	262
352	5.3 Abbildungsverzeichnis .....	262
353	5.4 Tabellenverzeichnis .....	263
354	5.5 Referenzierte Dokumente .....	266
355	5.5.1 Dokumente der gematik .....	266
356	5.5.2 Weitere Dokumente .....	269
357		

---

## 1 Einführung

---

### 1.1 Zielsetzung

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

### 1.2 Zielgruppe

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

### 1.3 Geltungsbereich

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

#### Schutzrechts-/Patentrechtshinweis

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

### 1.4 Abgrenzungen

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

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

## 389 1.5 Methodik

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

394  
395 **<AFO-ID> - <Titel der Afo>**  
396 Text / Beschreibung  
397 [**<=**]

398 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [**<=**]  
399 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 ~~zu User-Agent~~ zum Useragent sind in A\_22470\* definiert.

### **A\_24816-01 - Aktenkontokennung in HTTP Header innerhalb des VAU-Kanals**

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

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

Hinweis: Das betrifft die Kommunikationen 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\_27443 - Nutzung Terminologiepaket**

Das ePA-Aktensystem MUSS die relevanten Terminologien des Terminologiepakets gemäß [gemTerminology] verarbeiten und in der Kommunikation mit dem ePA-Aktensystem berücksichtigen. [≤]

Hinweis zu A\_27443:

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

## **2.1 Aktensystem- und Service-Lokalisierung**

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

Ein ePA-Client aus der TI kennt die FQDNs der ePA-Aktensysteme (diese werden hier fest definiert, vgl. A\_24592-\*). Das Vorgehen der festvorgegebenen FQDNs ist analog zum E-Rezept-Vorgehen.

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

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

#### **A\_24592-02 - Anbieter ePA-Aktensystem -Registrierung an übergreifender ePA-Domäne**

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

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

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

[≤]

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

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

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

492

### 493 Beispiele der Dienstlokalisierung

#### 494 PU :

#### 495 Aktensystem A

496

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

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

499 ...

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

501

#### 502 Aktensystem B

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

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

505

#### 506 TU :

#### 507 Aktensystem 1

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

509 ...

510

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

### 515 A\_14128-04 - Anbieter ePA-Aktensystem - Resource Records FQDN ePA

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

518 [ $\leq$ ]

### 519 A\_22688-03 - Anbieter ePA-Aktensystem, Konfiguration Schnittstellen über 520 /.well-known/

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

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

527

528

529 {  
"version" : "<Produkttypversion des Aktensystems im Format[0-

```

530 9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}>",
531     "sgd1"   : "<pfad_Schlüsselgenerierungsdienst_typ1>",
532     "sgd2"   : "<pfad_Schlüsselgenerierungsdienst_typ2>",
533     ....
534 }[<=]

```

535 **A\_22687 - Aktensystem, Konfiguration Schnittstellen über /.well-known/**  
 536 Das ePA-Aktensystem MUSS sicherstellen, dass dem Anbieter des ePA-Aktensystems die  
 537 technische Möglichkeit bereitgestellt wird A\_22688-\* umzusetzen. [**<=**]

### 538 ~~A\_17969-06 – Anbieter A\_26814 - ePA-Aktensystem -~~ 539 ~~Schnittstellenadressierung~~

540 ~~Der Anbieter des ePA-Aktensystems MUSS alle nach außen angebotenen Dienste gemäß~~  
 541 ~~der ePA-OpenAPI-Spezifikationen ([I\_Information\_Service] etc.) an seinen ePA-~~  
 542 ~~spezifischen HTTPS-Schnittstellen anbieten (insbesondere mit den in den ePA-OpenAPI-~~  
 543 ~~Spezifikationen aufgeführten Pfadnamen). Falls die Operationen innerhalb einer ePA-VAU~~  
 544 ~~liegt, so gilt der Pfadname der ePA-OpenAPI-Spezifikation für den inneren HTTP-Request~~  
 545 ~~(übertragen innerhalb eines VAU-Kanals).~~

546 ~~Ein ePA-Client verwendet, falls die Operation innerhalb einer VAU liegt gemäß~~  
 547 ~~[gemSpec\_Krypt#A\_24428-\*] den Pfadnamen /VAU für die Initiierung eines VAU-Kanals.~~  
 548 ~~Beim Aufbau des VAU-Kanals gibt das Aktensystem den für den VAU-Kanal weiter zu~~  
 549 ~~verwendenden Pfadnamen vor [gemSpec\_Krypt#A\_24608]. Innerhalb des VAU-Kanals,~~  
 550 ~~d. h. für innere HTTP-Request, MÜSSEN die Pfadnamen der ePA-OpenAPI-Spezifikationen~~  
 551 ~~umgesetzt werden. Für Schnittstellen, die außerhalb einer VAU liegen, gelten ebenfalls~~  
 552 ~~die jeweilige ePA-OpenAPI-Spezifikation mit den dort aufgeführten Pfadnamen. [**<=**]~~

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

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

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

560 Abgrenzend hierzu wird das VAU-Protokoll und die dabei verwendeten Pfade in  
 561 [gemSpec\_Krypt#7] definiert.

### 562 **A\_24801 - Aktensystem, Liste von FQDN im Internet**

563 Das ePA-Aktensystem MUSS dem ePA-FdV eine Liste aller Kostenträger und der FQDN,  
 564 unter der deren ePA-Aktensystem im Internet erreichbar ist, bereitstellen. Die Liste setzt  
 565 sich zusammen aus den selbst verwalteten Kostenträgern und den über  
 566 I\_Information\_Service\_Accounts bezogenen Teillisten der anderen ePA-  
 567 Aktensysteme. [**<=**]

## 568 **2.2 Redundanz**

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

574 Die Auswahl und der Zugriff auf Services des ePA-Aktensystems wird durch die  
 575 Primärsysteme anhand definierter FQDNs vorgenommen [siehe Kapitel 2.1]. Auf die  
 576 Auswahl der Services des ePA-Aktensystems kann der Anbieter des ePA-Aktensystems  
 577 durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die



Verfügbarkeit ist hergestellt, wenn jedes Primärsystem oder andere Fachdienste (z.B. E-Rezept-Fachdienst, ein anderes ePA-Aktensystem, ...) die Möglichkeit haben, die Services des ePA-Aktensystems zu erreichen. Von der Versichertenseite aus erfolgt der Zugriff auf die Komponenten des ePA-Aktensystems durch das ePA-Frontend des Versicherten.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen Komponenten des ePA-Aktensystems ist über grundlegende Maßnahmen wie redundante Netzteile hinaus nicht erforderlich. Es steht dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern einzusetzen, so dass jede einzelne Komponente des ePA-Aktensystems im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

#### **A\_14921 - Anbieter ePA-Aktensystem - lokale Redundanz im Standort des ePA-Aktensystems**

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

#### **A\_15245 - Anbieter ePA-Aktensystem - standortübergreifende Redundanz und Verfügbarkeit**

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

#### **A\_24862-03 - Anbieter ePA-Aktensystem – Georedundanz: Verfügbarkeit der Akten innerhalb von fünf Arbeitstagen**

Der Betreiber des ePA-Aktensystems MUSS Maßnahmen zur Verfügbarkeit der Akten ergreifen, die sicherstellen, dass bei einem Großereignis, bei dem alle Aktensysteminstanzen ausfallen, die betroffenen Akten innerhalb von fünf Arbeitstagen wieder vollumfänglich für die Versorgung genutzt werden können. Die Maßnahmen zur Erhaltung der Verfügbarkeit des Aktensystems müssen die Sicherheitsanforderungen für das ePA-Aktensystem erfüllen.[<=]

## **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.[<=]

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

627 **A\_25722 - ePA-Aktensystem - Löschen von personenbezogenen Daten von**  
628 **Vertretern nach Wegfall der Notwendigkeit**

629 Das ePA-Aktensystem MUSS die personenbezogenen Daten eines Vertreters löschen,  
630 sofern der Vertreter kein Aktenkonto im ePA-Aktensystem besitzt und der Vertreter keine  
631 Versicherten im ePA-Aktensystem mehr vertritt. [ $\leq$ ]

632 **A\_15104 - Anbieter ePA-Aktensystem - Ordnungsgemäße IT-Administration**

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

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

639 **A\_15824 - Anbieter ePA-Aktensystem - Sichere Speicherung von Daten**

640 Unabhängig davon, ob die Daten schon verschlüsselt vorliegen, MUSS der Anbieter des  
641 ePA-Aktensystems die Daten des ePA-Aktensystems bei der Speicherung  
642 verschlüsseln. [ $\leq$ ]

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

645 **A\_24774 - Anbieter ePA-Aktensystem - Zwei-Faktor-Authentisierung von**  
646 **Administratoren**

647 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass sich Administratoren  
648 mindestens mit einer Zwei-Faktor-Authentisierung anmelden. [ $\leq$ ]

649 **A\_15107-02 - Anbieter ePA-Aktensystem - Keine unzulässige Weitergabe von**  
650 **Daten**

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

657 **A\_15119 - Anbieter ePA-Aktensystem - Löschkonzept**

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

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

667 [ $\leq$ ]

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

670 **A\_15169 - ePA-Aktensystem - Verbot von Werbe- und Usability-Tracking**

671 Die Komponenten des ePA-Aktensystems DÜRFEN im Produktivbetrieb ein Werbe- und  
 672 Usability-Tracking NICHT verwenden.  
 673 Davon ausgenommen ist das Erfassen des standardmäßigen quantitativen  
 674 Nutzerverhaltens zur Ermittlung der Standard-Aktenutzung entsprechend der  
 675 Anforderung A\_15154. [≤]

676 **A\_15154 - Anbieter ePA-Aktensystem - Ermittlung von Standard-Aktenutzung**  
 677 Der Anbieter des ePA-Aktensystems MUSS mindestens einmal im Jahr Werte zu einer  
 678 Standard-Aktenutzung von LE und Versicherten durch die Profilierung anonymer  
 679 Zugriffsstatistiken auf das ePA-Aktensystem zum Zweck der Erkennung von Zugriffen  
 680 gemäß A\_15155 ermitteln. [≤]

681 **A\_15155 - Anbieter ePA-Aktensystem - Abweichung von Standard-**  
 682 **Aktenutzung**  
 683 Der Anbieter des ePA-Aktensystems MUSS Zugriffe und Zugriffsmuster, die nicht einer  
 684 Standard-Aktenutzung entsprechen, erkennen und Maßnahmen zur  
 685 Schadensreduzierung umsetzen. [≤]

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

689 **A\_24778 - Anbieter ePA-Aktensystem - Einsatz zertifizierter HSM**  
 690 Der Anbieter des ePA-Aktensystems MUSS beim Einsatz eines HSM sicherstellen, dass  
 691 dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als  
 692 Evaluierungsschemata kommen dabei Common Criteria oder Federal Information  
 693 Processing Standard (FIPS) in Frage.  
 694 Die Prüftiefe MUSS mindestens

- 695 1. FIPS 140-2 Level 3 oder
  - 696 2. FIPS 140-3 Level 3 oder
  - 697 3. Common Criteria EAL 4+ (mit AVA\_VAN.5)
- 698 entsprechen. [≤]

699 **A\_15157 - Anbieter ePA-Aktensystem - Sicherer Betrieb und Nutzung eines**  
 700 **HSMs**  
 701 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die auf dem HSM  
 702 verarbeiteten privaten Schlüssel, Konfigurationen und eingesetzte Software nicht  
 703 unautorisiert ausgelesen, unautorisiert verändert, unautorisiert ersetzt oder in anderer  
 704 Weise unautorisiert benutzt werden können. [≤]

705 **A\_15159 - Anbieter ePA-Aktensystem - Schutzmaßnahmen gegen die OWASP**  
 706 **Top 10 Risiken**  
 707 Der Anbieter des ePA-Aktensystems MUSS in allen Komponenten des ePA-Aktensystems  
 708 technische Maßnahmen zum Schutz vor den in der aktuellen Version genannten OWASP-  
 709 Top-10-Risiken umsetzen. [≤]

710 **~~AA~~ 24780-01 - Anbieter ePA-Aktensystem – Versicherte über sensible**  
 711 **Änderungen informieren**

712 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass der Versicherte ~~über~~  
 713 ~~Änderungen in den folgenden Anwendungsfällen~~ informiert wird, –

- 714 ~~• E-Mail-Adresse ändern,~~
- 715 ~~• Aktenkonto schließen~~

716 ~~und~~ wenn der Anbieter des Aktensystems eine manuelle Änderung bezüglich einer Akte  
 717 (Aktenverwaltung) im Auftrag eines Versicherten durchführt. ~~[≤]~~. [≤]

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

722 **A\_15163 - Anbieter ePA-Aktensystem - Angriffen entgegenwirken**

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

726 **A\_15167 - Anbieter ePA-Aktensystem - Social Engineering Angriffen**  
 727 **entgegenwirken**

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

730 **A\_24989 - Anbieter ePA-Aktensystem - Schutz vor Angriffen über die TI**

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

735 **A\_15168 - ePA-Aktensystem - Verbot vom dynamischen Inhalt**

736 Die Komponenten des ePA-Aktensystems DÜRFEN dynamischen Inhalt von Drittanbietern  
 737 NICHT herunterladen und verwenden.  
 738 [≤]

739 **A\_17080 - Verhindern von Session Hijacking**

740 Die Komponenten des ePA-Aktensystems MÜSSEN geeignete Schutzmaßnahmen gegen  
 741 Session-Hijacking implementieren.  
 742 [≤]

743 **A\_16323-01 - ePA-Aktensystem - Verbot von medizinisch irrelevantem Inhalt**

744 Der Anbieter des ePA-Aktensystems MUSS der Ablage von Dokumenten, die für die  
 745 medizinische Versorgung oder für die Eigenorganisation medizinischer Belange des  
 746 Versicherten oder zur Erstattung der Behandlungskosten irrelevant sind, mittels AGB auf  
 747 Anbieterseite entgegenwirken.  
 748 [≤]

749 **A\_24781 - Sicherer Betrieb des Produkts nach Handbuch**

750 Der Anbieter eines ePA-Aktensystems MUSS die im Handbuch des eingesetzten ePA-  
 751 Aktensystems beschriebenen Voraussetzungen für den sicheren Betrieb des Produktes  
 752 gewährleisten. [≤]

753 **A\_18953 - Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im**  
 754 **Handbuch**

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

759 **A\_19122-01 - Anbieter ePA-Aktensystem – Trennung zu anderen Mandanten**

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

762 **A\_21106 - Anbieter ePA-Aktensystem – Signaturschlüssel für Protokolle**

763 Das ePA-Aktensystem MUSS für die Signatur von Listen von Protokollen des Versicherten  
 764 Schlüsselmaterial der Ausstelleridentität ID.FD.SIG mit einem zugehörigen Zertifikat  
 765 C.FD.SIG mit der Rolle oid\_epa\_logging gemäß [gemSpec\_OID] besitzen. [≤]

**A\_21107 - Anbieter ePA-Aktensystem – Speicherung Signaturschlüssel für Protokolle im HSM**

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

[<=]

**A\_22409 - Anbieter ePA-Aktensystem - CA-Anbieterwechsel**

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

**A\_19118-01 - Komponenten des Aktensystems, Schutz vor XSW-Angriffen**

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

**A\_24783 - ePA-Aktensystem - Eingabevalidierung von Operationen**

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

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

**A\_24992 - ePA-Aktensystem - Zugriffe durch Versicherte übers Access Gateway**

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

**A\_24993 - ePA-Aktensystem - Zugriffe übers Access Gateway ausschließlich für Versicherte**

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

**A\_25006 - ePA-Aktensystem - User Session bei Inaktivität Beenden**

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

**A\_25022 - ePA-Aktensystem - Debug-Protokoll für Testbetrieb**

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

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

**A\_25023 - ePA-Aktensystem - Keine Echtdaten im Testbetrieb**

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

**A\_25042 - ePA-Aktensystem - Prüfung von Signaturen**

Das ePA-Aktensystem MUSS bei der Prüfung von Signaturen

- das Signaturzertifikat gemäß A\_25040-\* prüfen,
- die Signatur prüfen (i. S. v. Verify()-Funktion des kryptographischen Signaturverfahrens ergibt "valid")

[<=]

**A\_25040-01 - ePA-Aktensystem - Prüfung Signaturzertifikate**

Das ePA-Aktensystem MUSS Signaturzertifikate gemäß [gemSpec\_PKI#TUC\_PKI\_018] mit folgenden Parametern auf Gültigkeit prüfen:

**Tabelle 1: Tab\_Prüfung\_Signaturzertifikate Parameter Prüfung Signaturzertifikat**

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

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

**2.4 Validierungsaktenkonto**

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

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



Folgende Anwendungsfälle sollen mit den Validierungsaktenkonten adressiert werden:

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

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

#### **A\_18168-01 - Anbieter des ePA-Aktensystem - Validierungsaktenkonto für gematik**

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

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

[<=]

#### **A\_18169-02 - Anbieter des ePA-Aktensystem - Validierungsaktenkonto für eigene Zwecke**

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

[<=]

#### **A\_22522-01 - Anbieter des ePA-Aktensystems - Validierungskonto für Dritte**

Der Anbieter des ePA-Aktensystems MUSS auf Antrag der gematik

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

[<=]

Hinweis zu A\_22522-\*: Die Einrichtung der Validierungsaktenkonten für Dritte kann gegen Bezahlung erfolgen. Die Entscheidung *dafür obliegt dem Anbieter des ePA-Aktensystems*.

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

#### **A\_26187 - Anlage von Validierungsaktenkonten**

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

**A\_26188 - Anbieter des ePA-Aktensystems - Aktivierung von Validierungsaktenkonten**

Der Anbieter des ePA-Aktensystems MUSS den Status von Validierungsaktenkonten, welche für die gematik (gem. A\_18168-\*) oder für Dritte (gem. A\_22522-\*) angelegt wurden, nach der Anlage auf ACTIVATED setzen. [ <= ]

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

**A\_22524-01 - Anbieter des ePA-Aktensystems - Löschen von Validierungsaktenkonten nach 5 Jahren**

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

**A\_22684-01 - Validierungsaktenkonten im Store-Review der FdVs**

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

**A\_22942 - Besonderheiten bei Validierungskonten für StoreReviews**

Bei Validierungsaktenkonten, für die die Regelung gem. A\_22684-\* gilt [Validierungskonten im StoreReview der FdVs], MÜSSEN folgende Besonderheiten berücksichtigt werden:

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

[ <= ]

**A\_26209 - Prüfung auf Vertretungsberechtigung für Prüfidentität**

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

**A\_24539 - Nutzung von Validierungsaktenkonten via FdV**

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

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

**~~A\_26209 - Prüfung auf Vertretungsberechtigung für Prüfidentität~~**



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

## 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. [ <= ]

979 *Hinweis: Die Aktivier- bzw. Deaktivierbarkeit nach A\_22581-\* kann dabei auch teilweise*  
 980 *mit organisatorische Maßnahmen umgesetzt werden, d. h. es ist hier **kein***  
 981 *vollautomatisierter Mechanismus notwendig, der im Millisekunden-Bereich umschalten*  
 982 *kann.*

## 983 **2.6 Benutzerführung**

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

### 987 **A\_15842 - Anbieter ePA-Aktensystem - Ergonomie der Benutzerführung**

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

### 991 **DIN-Normen und Verordnungen zur Beachtung:**

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

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

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

- 1000 • Teil 8: Anforderungen an Farbdarstellungen
- 1001 • Teil 9: Anforderungen an Eingabegeräte – außer Tastaturen
- 1002 • Teil 110: Grundsätze der Dialoggestaltung (ersetzt den bisherigen Teil 10)
- 1003 • Teil 11: Anforderungen an die Gebrauchstauglichkeit – Leitsätze
- 1004 • Teil 12: Informationsdarstellung
- 1005 • Teil 13: Benutzerführung
- 1006 • Teil 14: Dialogführung mittels Menüs
- 1007 • Teil 15: Dialogführung mittels Kommandosprachen
- 1008 • Teil 16: Dialogführung mittels direkter Manipulation
- 1009 • Teil 17: Dialogführung mittels Bildschirmformularen
- 1010 • Teil 171: Leitlinien für die Zugänglichkeit von Software BITV 2.0

### 1011 **BITV 2.0 - Barrierefreie Informationstechnik-Verordnung**

1012 Die Umsetzung der Verordnung dient zur behindertengerechten Umsetzung  
 1013 von Webseiten und anderen grafischen Oberflächen.

1014 Insbesondere sollen deshalb neben der Übernahme der international anerkannten  
 1015 Standards für barrierefreie Webinhalte, die Web Content Accessibility Guidelines (WCAG)  
 1016 2.1, auch die Belange gehörloser, hör-, lern- und geistig behinderter Menschen  
 1017 berücksichtigt werden.

1018 Die BITV 2.0 regelt unter anderem den sachlichen Geltungsbereich, die einzubeziehenden  
 1019 Gruppen behinderter Menschen und die anzuwendenden Standards.

1020 Weitere Richtlinien und Empfehlungen zur digitalen Barrierefreiheit sind die EU-Richtlinie  
 1021 2016/2102 für öffentliche Stellen und die europäische Norm EN 301 549 V2.1.2 mit dem  
 1022 Titel "Accessibility requirements for ICT products and services".

## 1023 **A\_15846 - Anbieter ePA-Aktensystem - Schnittstellen für die Unterstützung der** 1024 **barrierefreien Bedienungsmöglichkeit**

1025 Der Anbieter des ePA-Aktensystems SOLL die Schnittstellen für die Unterstützung der  
 1026 barrierefreien Bedienungsmöglichkeit, welche vom Betriebssystem zur Verfügung gestellt  
 1027 werden, unterstützen. [=]

## 1028 **2.7 Useragent**

### 1029 **AA\_22470-0506 - Definition x-useragent**

1030 Das Produkt MUSS für das x-useragent-Element in Eingangs- oder Ausgangsparametern  
 1031 einer Operation folgende Formatvorgaben berücksichtigen:

- 1032 • der Useragent umfasst 2 Informationen, welche als 1 String - getrennt durch "/"  
 1033 (Slash) - im Header übertragen werden
- 1034 • erster Teil: ClientIDClient-ID = ein bis zu 20 Zeichen langer String (a-z A-Z 0-  
 1035 9, "-"), welcher im Rahmen der Produktregistrierung bei der gematik erzeugt  
 1036 wird,
- 1037 • zweiter Teil: Versionsnummer = bis zu 15 Zeichen langer String (a-z A-Z 0-9,  
 1038 "-", ".") welcher die aktuelle Produktversion des Clients repräsentiert.

1039 Beispiel: "CLIENTID1234567890AB/2.1.12-45"

1040 ~~[<=]~~ Hinweis: gem. RFC7231 ist im http-Header ein Useragent einzutragen. Dieser RFC-  
 1041 Useragent enthält z.B. Angaben zum Betriebssystem oder zum Browser und ist nicht zu  
 1042 verwechseln mit dem hier definierten x-useragent. Dieser (x-useragent) muss deshalb im  
 1043 x-useragent-Parameter des http-Headers eingetragen werden, NICHT im Useragent-  
 1044 Parameter gem. RFC7231. Ein Beispiel für die Verwendung bieten die OpenAPI-  
 1045 Spezifikationen der fachlichen Aktensystem-Operationen. [=]

1046 *Hinweis zum Erhalt der ClientIDClient-ID: die ClientIDClient-ID wird durch die gematik*  
 1047 *vergeben und übermittelt, sobald sich ein (Client-)Produkthersteller (z.B. FdV oder*  
 1048 *Primärsystem) unter idp-registrierung@gematik.de registriert hat. Dazu ist im Rahmen*  
 1049 *dieser Registrierung der Name des Herstellers und der Name des zu registrierenden*  
 1050 *Produktes zu übermitteln. Sollte im Rahmen einer anderen TI-Anwendung bereits eine*  
 1051 *Registrierung vorgenommen worden sein, kann die ClientIDClient-ID auch im ePA-*  
 1052 *Kontext genutzt werden (sofern es sich um das gleiche Softwareprodukt handelt).*

1053 *Hinweis für FdV-Hersteller: Bei Entwicklung eines White-Label-Clients ist der Useragent*  
 1054 *Teil des kundenspezifischen Customizings, sodass über die ClientIDClient-ID im*  
 1055 *Useragent das spezifische Kostenträger-ePA-FdV erkennbar sein muss.*

## 1056 **2.8 Datenmigration**

1057 Jeder ~~Versicherter~~Versicherte (vorbehaltlich eines Widerspruchs durch den Versicherten)  
 1058 erhält in ePA 3.0 ein neues, leeres Aktenkonto. Bei der Migration werden Daten und  
 1059 Vertreterberechtigungen aus ePA 2.6 in dieses Aktenkonto übertragen.

1060 Für die Migration eines existierenden Aktenkontos der Version ePA-2.x wird  
 1061 vorausgesetzt, dass ein migriertes Aktenkonto sowohl die Schnittstellen der ePA für alle,

1062 als auch die Schnittstellen der bisherigen ePA-Version 2.x bereitstellt und simultan  
1063 verarbeiten kann.

1064 Die Migration eines existierenden Aktenkontos der ePA-Version 2.x erfordert die  
1065 Entschlüsselung der existierenden Inhalte durch die Anwendung des  
1066 aktenkontospezifischen Akten- und Kontextschlüssels und deren Überführung in die  
1067 Verwaltungs- und Diensteeinheiten der im vorliegenden Dokument beschriebenen ePA-  
1068 Version 3.x.

1069 Aus einem existierenden Aktenkonto werden die folgenden Artefakte übernommen:

- 1070 • Kategorien und Ordner, insoweit die Kategorien nicht abgekündigt sind. Ordner  
1071 erhalten eine feste UUID.
- 1072 • Dokumente, sowie deren Metadaten
- 1073 • Protokolle

1074 Die Vertraulichkeitsstufen für die Sichtbarkeit von Dokumenten werden nicht mehr  
1075 unterstützt. Dokumente mit bisheriger Vertraulichkeitsstufe *confidential* werden bei der  
1076 Migration der GeneralDenyPolicy des Constraint Managements zugeordnet.

1077 Alle weiteren Nutzergruppen (LEI, Apotheken, usw) erhalten eine Befugnis zur Nutzung  
1078 dediziert in einer Behandlungssituation oder durch direkte Befugnisvergabe durch den  
1079 Versicherten oder einen Vertreter mittels ePA-FdV.

1080 Für Versicherte, die keine ePA-FdV nutzen möchten oder können, ist eine Migration der  
1081 Daten einer existierenden Akte nicht möglich, da die dafür notwendige Übertragung des  
1082 bisherigen individuellen Akten- und Kontextschlüssels nicht erfolgen kann. Versicherte  
1083 ohne ePA-FdV erhalten (vorbehaltlich eines Widerspruchs durch den Versicherten) ein  
1084 neues, leeres Aktenkonto ohne Inhalten, die womöglich in ePA 2.6 existierten. Eine  
1085 Befugnisvergabe für Leistungserbringerorganisationen ist in diesem Fall ausschließlich  
1086 durch die Befugnisvergabe im Behandlungskontext möglich. Dieses erfordert eine LEI mit  
1087 einem Client gemäß ePA-Version 3.x.

1088 Es resultiert ein Aktenkonto, welches direkt durch den Versicherten, befugte Vertreter,  
1089 den Kostenträger, die Ombudsstelle und den E-Rezept-Fachdienst genutzt werden kann.

1090 Zusätzlich zur Datenmigration beim Wechseln von ePA 2 nach ePA 3 kann es auch  
1091 innerhalb von ePA 3 zu notwendigen Datenanpassungen kommen, z. B. wenn das  
1092 Aktensystem Metadaten zu bestehenden Dokumenten ergänzen soll. Derartige Hinweise  
1093 finden sich im Unterabschnitt Weitere Datenanpassungen.

## 1094 2.8.1 Herstellerspezifische Umsetzung der Datenmigration

1095 Die technische Umsetzung der Datenmigration obliegt grundsätzlich dem Hersteller des  
1096 ePA-Aktensystems. Es muss jedoch sichergestellt werden, dass der Schutz der zu  
1097 migrierenden Daten durchgehend gewährleistet wird.

### 1098 **A\_24995 - Migration: Sicherheitskonzept für Datenmigration**

1099 Der Hersteller des ePA-Aktensystems MUSS ein Sicherheitskonzept zur Datenmigration  
1100 erstellen, in welchem er beschreibt, mit welchen Maßnahmen die zu migrierenden Daten  
1101 im gesamten Datenmigrationsprozess geschützt werden. [≤]

### 1102 **A\_25000 - Migration: Stärke der Sicherheitsmaßnahmen für Datenmigration**

1103 Das ePA-Aktensystem MUSS sicherstellen, dass die zu migrierenden Daten im gesamten  
1104 Datenmigrationsprozess mit technischen Maßnahmen geschützt werden, die auch gegen  
1105 einzelne Innentäter beim Betreiber des ePA-Aktensystems wirken. [≤]

### 1106 **A\_25049 - Migration: Migrationskonzept**

1107 Der Anbieter des ePA-Aktensystems MUSS ein Migrationskonzept erstellen, welches  
1108 sowohl die Aktensystemmigration, als auch die Datenmigration, mitsamt der  
1109 Bereitstellungs- und ggf. Außerbetriebnahme-Zeitpunkte der benötigten Komponenten  
1110 berücksichtigt. Das Migrationskonzept MUSS dabei auch aufzeigen, welche  
1111 Abhängigkeiten zu anderen TI-Diensten bestehen, wann und in welchem Umfang die  
1112 Migration getestet wird und wie eventuelle Roll-Back-Szenarios aussehen.  
1113 [ $\leq$ ]

## 1114 2.8.2 Durchführung der Migration

1115 Das Aktenkonto muss durch den Anbieter für die Migration der Daten vorbereitet werden.  
1116 Dabei müssen alle Maßnahmen umgesetzt werden, die im Zustand INITIALIZED eines  
1117 neuen Aktenkontos vor der Aktivierung erforderlich sind (siehe 3.1.3- Anlage eines  
1118 neuen Aktenkontos ). Abweichend von den Maßnahmen für die Erstellung eines neuen  
1119 Aktenkontos kann auf den Status INITIALIZED verzichtet werden und das Aktenkonto im  
1120 Status ACTIVATED verbleiben.

1121 Für ein zu migrierendes Aktenkonto sind alle Schritte anzuwenden, die auch für die  
1122 Erstellung eines neuen Aktenkontos vor der Aktivierung erforderlich sind, insbesondere  
1123 die Anlage der initialen Befugnisse für den Versicherten, den Kostenträger und die  
1124 Ombudsstelle, sowie den E-Rezept-Fachdienst.

1125 Im Anschluss an die Initialisierung erfolgt einmalig die Bereitstellung der Akten- und  
1126 Kontextschlüssel durch ein ePA-FdV. Existierende Daten werden übertragen.

### 1127 A\_25148 - Migration: Information des Versicherten

1128 Der Anbieter des ePA-Aktensystems MUSS den Versicherten über die Notwendigkeit und  
1129 die Folgen einer Migration vor der eigentlichen Migration informieren, insbesondere  
1130 darüber, welche Dokumentenformate und welche Berechtigungen übernommen und  
1131 welche nicht übernommen werden, über die Freiwilligkeit einer Migration. [ $\leq$ ]

1132 Die Entschlüsselung des Datenbestands für die Überführung in das vorbereitete  
1133 Aktenkonto und die Migration der Berechtigungen der Vertreter wird durch die Nutzung  
1134 eines ePA-FdV gemäß ePA-Version 3.x abgeschlossen. Bei der ersten Nutzung eines ePA-  
1135 FdV durch den Versicherten mit dem zur Migration vorbereiteten Aktenkonto erfolgt die  
1136 Migration über die vom ePA Aktensystem bereitgestellten Schnittstellen.

### 1137 A\_24922 - Migration: Schnittstellen zur Durchführung der Migration

1138 Das ePA-Aktensystem MUSS für jedes Aktenkonto eine Migration von ePA 2.6 auf ePA 3.0  
1139 durchführen und geeignete Schnittstellen zum FdV anbieten, mit denen der Versicherte  
1140 vom FdV das Entschlüsseln der verschlüsselten ePA 2.6-Akteninhalte anstoßen  
1141 kann. [ $\leq$ ]

1142 In der ePA für alle ist der Zugriff über einen Client der ePA-Version 2.x nicht mehr  
1143 möglich, da sich die grundsätzliche Architektur und die Schnittstellen und Protokolle  
1144 geändert haben.

## 1145 2.8.3 Bereinigung von Registry und Repository im Zuge der 1146 Migration

### 1147 A\_24964 - XDS Document Service - Migration: Isolation der Migration

1148 Der XDS Document Service MUSS die Verarbeitung von entschlüsselten Dokumenten, die  
1149 im Rahmen der Migration durchgeführt werden, so technisch isolieren, dass kein Schaden  
1150 für Aktenkonten oder das ePA-Aktensystem selbst entsteht. [ $\leq$ ]



**A\_25730 - XDS Document Service - Konvertierung von PDF in PDF/A bei der Datenmigration**

Der XDS Document Service MUSS die Konvertierung von entschlüsselten PDF-Dokumenten in PDF/A-Dokumente, die im Rahmen der Migration durchgeführt wird, in einer Aktenkontoverwaltungs-VAU oder in einer getrennten VAU-Instanz durchführen, wobei

- die Konvertierung innerhalb der Aktenkontoverwaltungs-VAU ausschließlich für die Datenmigration von ePA2.6 auf die ePA3.0 verwendet werden darf und
- es bei einer getrennten VAU-Instanz eine 1:1-Beziehung zur Aktenkontoverwaltungs-VAU geben muss (d.h. die getrennte VAU-Instanz zur Konvertierung ist nur mit einer (1) Aktenkontoverwaltungs-VAU verbunden und eine Aktenkontoverwaltungs-VAU nur mit einer (1) VAU-Instanz für die Konvertierung) und die getrennte VAU-Instanz für die Konvertierung ausschließlich für die Datenmigration von ePA2.6 auf die ePA3.0 verwendet werden darf.

[&lt;=]

**A\_26682 - XDS Document Service - Konvertierung von Bildformaten in PDF/A bei der Datenmigration**

Der XDS Document Service MUSS die Konvertierung von entschlüsselten Bildformaten in PDF/A-Dokumente, die im Rahmen der Migration durchgeführt wird, in einer Aktenkontoverwaltungs-VAU oder in einer getrennten VAU-Instanz durchführen, wobei

- die Konvertierung innerhalb der Aktenkontoverwaltungs-VAU ausschließlich für die Datenmigration von ePA2.6 auf die ePA3.0 verwendet werden darf und
- es bei einer getrennten VAU-Instanz eine 1:1-Beziehung zur Aktenkontoverwaltungs-VAU geben muss (d.h. die getrennte VAU-Instanz zur Konvertierung ist nur mit einer (1) Aktenkontoverwaltungs-VAU verbunden und eine Aktenkontoverwaltungs-VAU nur mit einer (1) VAU-Instanz für die Konvertierung) und die getrennte VAU-Instanz für die Konvertierung ausschließlich für die Datenmigration von ePA2.6 auf die ePA3.0 verwendet werden darf.

Bildformate sind Dokumente im Format "jpeg", "png" oder "tiff".[<=]

**A\_25002 - XDS Document Service - Migration: Umbenennung von Ordnern**

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

**A\_24562 - XDS Document Service - Migration: Auflösung abgekündigter Ordner**

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 die abgekündigten Kategorien auflösen. Dabei MÜSSEN sämtliche Dokumente gemäß der Einordnungsregeln in A\_19388-\* neu Ordnern zugeordnet werden und die Ordner der abgekündigten Kategorien gelöscht werden. [<=]

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

1198 Die Kinderuntersuchungshefte werden nicht migriert und verbleiben im Ordner  
1199 childsrecord.

1200

1201 **A\_24963 - XDS Document Service - Migration: Keine Übernahme von**  
1202 **Dokumenten mit unzulässigem Format**

1203 Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0  
1204 sämtliche Dokumente der ePA2.6 gemäß A\_24864-\* auf die zulässigen  
1205 Dokumentenformate prüfen und Dokumente in einem nicht erlaubten Format nicht in die  
1206 "ePA für alle" migrieren. [≤]

1207 *Hinweis zu A\_24963-\*: Für die Migration von Dokumenten der ePA2.6 auf ePA3.0 sind*  
1208 *bei der Prüfung auf zulässige Dokumentenformate die Hinweise zu A\_24864-\* und*  
1209 *A\_25009-\* zu berücksichtigen.*

1210 **A\_24966 - XDS Document Service - Migration: Konvertieren von PDF- in PDF/A-**  
1211 **Dokumente**

1212 Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0  
1213 Dokumente im PDF-Format in ein PDF/A-Format konvertieren und ausschließlich das  
1214 Dokument im PDF/A-Format in das Aktenkonto übernehmen. [≤]

1215 **A\_25032 - XDS Document Service - Migration: Information des Versicherten zur**  
1216 **Nichtübernahme von Dokumenten in bestimmten Formaten**

1217 Der Anbieter des ePA-Aktensystems MUSS den Versicherten darüber informieren, das  
1218 Dokumente in der ePA2.6, die ein bestimmtes Format besitzen, nicht in die "ePA für alle"  
1219 übernommen werden und informieren, um welche Formate es sich handelt. [≤]

1220 **A\_24520 - XDS Document Service - Migration: Prüfsumme Dokument erzeugen**

1221 Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 für  
1222 jedes Dokument, das im Klartext vorliegt, die kryptographische Prüfsumme des  
1223 Dokumentes berechnen und in `DocumentEntry.hash` hinterlegen. Dabei MUSS SHA-256  
1224 verwendet werden. Außerdem MUSS die Dokumentengröße für das Feld  
1225 `DocumentEntry.size` berechnet und gesetzt werden. [≤]

1226 **A\_24847 - XDS Document Service - Migration: Identifizieren und Auflösen von**  
1227 **Dokumenten-Dubletten**

1228 Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 zum  
1229 Zeitpunkt der Entschlüsselung eine Dublettenerkennung durchführen. Dabei werden  
1230 entschlüsselte Dokumente innerhalb und außerhalb von Sammlungen verglichen mit  
1231 Dokumenten, die durch eine zwischenzeitliche Nutzung von ePA für alle in die Akte  
1232 eingestellt worden sind. Dubletten werden anhand der Gleichheit des Hash-Wertes im  
1233 Feld `documentEntry.hash` identifiziert. Das Dokument mit dem älteren Einstelldatum  
1234 wird verworfen. [≤]

1235 **A\_24851 - XDS Document Service - Migration: Dokumente und Ordner mergen**

1236 Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf die ePA 3.0  
1237 zum Zeitpunkt der Entschlüsselung des Datenbestands die Ordnerinhalte einer Kategorie  
1238 vergleichen, falls es neben den migrierten ePA 2.6-Akteninhalten durch eine ePA3-  
1239 Aktennutzung ebenfalls Ordnerinhalte gibt. Unter Berücksichtigung der Dublettenprüfung  
1240 werden alle Dokumente von zwei Ordnern derselben Kategorie (in ePA 2.6 bzw. 3.0  
1241 entstanden) in einen Ordner zusammengeführt. Dokumente und RPLC-Ketten, die durch  
1242 die `documentEntry.uniqueId` erkennbar zusammen gehören, werden unter Wahrung der  
1243 Abfolge der Einstelldaten zusammengeführt und das jüngste Dokument als aktives  
1244 Dokument der Kette behandelt. Dokumente erhalten eine `rootDocumentUniqueId` gemäß  
1245 A\_24451-\*, falls noch nicht vorhanden. [≤]

#### A\_24848 - XDS Document Service - Migration: Auflösung von duplizierten dynamischen Ordnern

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf die ePA 3.0 anhand des Titels dynamischer Ordner erkennen, ob zwei dynamische Ordner zur selben Kategorie vorliegen, z.B. zur selben Schwangerschaft. In diesem Falle werden alle vorhandenen Einträge in einen der Ordner hinein gemergt und der andere Ordner gelöscht.

[<=]

#### A\_24522 - XDS Document Service - Migration: Erzeugen von Titeln für Dokumente

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

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

[<=]

#### A\_24523 - XDS Document Service - Migration: Löschen von ConfidentialityCodes

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

#### A\_24817 - XDS Document Service - Migration: Normalisieren und Validieren der URI

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 die ePA 3.0 für sämtliche Dokumente die `documentEntry.URI` gemäß A\_24524-\* und A\_23447-\* normalisieren und validieren. [<=]

#### AA\_24866-01 - Audit Event Service - Migration: Übernahme von Protokolldaten

Der Audit Event Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 sämtliche Protokolldaten des Versicherten in die migrierte Akte übernehmen. Für die Migration werden alte Protokolldaten in ein PDF/A überführt und in **die Kategorie "patient" eingestellt.** ~~[<=]~~ **den Ordner "technical" eingestellt. Für dieses Dokument sind die folgenden Metadaten für `DocumentEntry` zu verwenden:**

- `title`: "Zugriffsprotokoll (bis Anfang 2025)"**
- `classCode`: "DOK": (Dokumente ohne besondere Form (Notizen))**
- `typeCode`: "PATD": (Patienteneigene Dokumente)**
- `mimeType`: "application/pdf"**
- `formatCode`:**
  - `codeSystem` "2.25.154081344090540725127779452347992051720"**
  - `code`: "urn:gematik:ig:archivedAuditEventData:v1.0"**
  - `displayName`: "Zugriffsprotokoll (bis Anfang 2025)"; (gleicher Text wie 'title')**



1284 [<=]1285 **2.8.4 Protokollierung der Migration**1286 **AA\_25029-01 - XDS Document Service - Protokollierung der Migration der**  
1287 **medizinischen Daten**

1288 Der XDS Document Service MUSS den Vorgang der Migration der medizinischen Daten  
1289 (Dokumente, Folder, Metadaten) gemäß A\_24704\* protokollieren. Dabei ist die Migration  
1290 als atomares Ereignis zu betrachten und mit einem Protokolleintrag zu dokumentieren.  
1291 Für den Protokolleintrag ist folgende Wertebelegung zu berücksichtigen:

1292 **Tabelle 2: Protokollierung der Migration der medizinischen Daten**

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

Strukturelement	Wert		Erläuterung
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	dieses Strukturelement ist zu versorgen, wenn einzelne Dokumente nicht übernommen werden konnten
	"DocumentTitle"	<DocumentEntry.title>	Name des Dokumentes, welches nicht übernommen werden konnte
	"DocumentUniqueId"	<Document.uniqueId>	ID des Dokumentes, welches nicht übernommen werden konnte
	"DocumentFormatCode"	<DocumentEntry.formatCode>	kodiert als Datentyp „Coded String“ gemäß [IHE-IT1-TF3].
	"DocumentMimeType"	<DocumentEntry.mimeType>	

[&lt;=]

### **AA\_25031-01 - Audit Event Service - Protokollierung der Migration der Protokolldaten des Versicherten**

Der Audit Event Service MUSS den Vorgang der Migration der Protokolldaten des Versicherten gemäß A\_24704\* protokollieren.

Dabei ist die Migration als atomares Ereignis zu betrachten und mit einem Protokolleintrag zu dokumentieren.

Für den Protokolleintrag ist folgende Wertebelegung zu berücksichtigen:

**Tabelle 3: Protokollierung der Migration der Protokolldaten des Versicherten**

Strukturelement	Wert	Erläuterung
AuditEvent.type	"object"	
AuditEvent.action	E	
<u>AuditEvent.source.type.code</u>	<u>"AUDITSVC"</u>	

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

[&lt;=]

## 2.8.5 Weitere Datenanpassungen

### A 27482 - XDS Document Service – Metadatenkorrektur bei elektronischen Arztbriefen

Der XDS Document Service MUSS die Metadaten (DocumentEntry) von bestehenden Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief) gemäß [gemSpec\_IG\_ePA] derartig anpassen, dass DocumentEntry.eventCodeList zusätzlich um den KDL-Code (code: ED110104, codeSystem: 1.2.276.0.76.5.552, displayName: eArztbrief) erweitert wird, wenn dieser nicht bereits vorhanden ist.

[&lt;=]

Hinweis: Eine Protokollierung der in diesem Abschnitt beschriebenen Datenanpassungen ist nicht notwendig.

## 2.9 Performance aus Anwendersicht

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

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

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

1337 Die eingegangenen Messergebnisse werden vom Aktensystem verarbeitet und  
1338 anschließend gemäß der Vorgaben aus [gemSpec\_Perf] an die Betriebsdatenerfassung  
1339 der gematik im Rahmen der Rohdatenlieferung übermittelt.

1340

### 1341 **A\_24570-01 - Verarbeitung von UX-Messdaten**

1342 Das ~~ePA~~-Aktensystem MUSS für die im zu betrachtenden Zeitintervall der  
1343 ~~Rohdatenlieferung~~Betriebsdatenlieferung (gemäß [gemSpec\_Perf]) eingegangenen  
1344 Messdaten je UX-Usecase, je ~~ClientID~~Client-ID und je Client-Version folgende Werte  
1345 ermitteln und gemäß [gemSpec\_Perf] übermitteln:

- 1346 - Durchschnittswert der Messergebnisse
- 1347 - Anzahl der berücksichtigten Messergebnisse
- 1348 - Maximalwert
- 1349 - Minimalwert[<=]

1350 Die Versionsnummer des Useragents wird bei der Konsolidierung nicht weiter verarbeitet  
1351 und dient dem Anbieter des ePA-Aktensystems zur Identifikation von möglichen  
1352 Fehlerquellen im Rahmen des Eigenmonitorings und Troubleshootings.

1353

---

## 3 Funktionsmerkmale

---

1354

### 3.1 Aktenkonto eines Versicherten (Health Record)

1355  
1356  
1357  
1358  
1359

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.

1360  
1361

#### 3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte

1362  
1363  
1364  
1365  
1366  
  
1367  
1368  
1369  
1370  
  
1371  
1372  
1373  
1374  
  
1375

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

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

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

1376  
1377  
1378  
1379  
1380

#### 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. [ <= ]

1381  
1382  
1383

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.

1384  
1385  
1386  
1387  
1388

#### 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. [ <= ]

1389  
1390

#### 3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger

1391  
1392

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

1393 der ePA eigenständig im Rahmen der gesetzlichen Vorgaben umzusetzen und sind nicht  
1394 Bestandteil dieser Spezifikation.

### 1395 3.1.2 Lebenszyklus und Zustände eines Aktenkontos

1396 Ein Aktenkonto durchläuft in seinem Lebenszyklus diverse Zustände. Einige dieser  
1397 Zustände sind für rein administrative Vorgänge vorgesehen (Initialisierung, Umzug des  
1398 Aktenkontos zu einem anderen Anbieter), andere für die Nutzung der Akte im  
1399 Versorgungsprozess. Diese Nutzung für Versorgungsprozesse ist dabei auf den Zustand  
1400 "Activated" eingeschränkt.

1401 Eine Übersicht der unterschiedlichen Status und der Bedingungen für den  
1402 Statusübergang sind in der folgenden Tabelle dargestellt.

1403 **Tabelle 4: Zustandswechsel im Lebenszyklus eines Aktenkontos**

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



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

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

### ~~A\_24980 – Aktenkontoverwaltung – Protokollierung des Aktenkontostatus~~

~~Die Aktenkontoverwaltung MUSS bei Änderungen des Status eines Aktenkontos jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:~~

**Tabelle 5: Protokollierung von Änderungen des Aktenkontostatus**

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

~~[<=>]~~

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

### 3.1.3 Anlage eines neuen Aktenkontos

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

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

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

#### **A\_24336 - Anbieter ePA-Aktensystem - Identifizierung eines Aktenkontos**

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

#### **A\_23775 - Anbieter ePA-Aktensystem - Neues Aktenkonto anlegen**

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

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\_24302A\_27343 - Anbieter ePA-Aktensystem - verpflichtende Nutzung von startRelocationPrüfung auf Widerspruch gegen die Nutzung der ePA bei einem anderen Anbieter**~~

~~Der Anbieter des ePA-Aktensystems MUSS **bevor** der Anlage eines **neuen** Aktenkontos durch Verwendung der **Operation-startRelocation** Operationen der Schnittstelle gemäß [I\_Information\_Service\_Accounts] auf Existenz eines Aktenkontos des Versicherten bei allen anderen Anbietern prüfen. [ $\leq$ ]~~

#### ~~**A\_24790 —, ob bei einem anderen Anbieter ePA-Aktensystem — keine unbegründete Nutzung von startRelocation**~~

~~Der Anbieter ein Widerspruch des ePA-Aktensystems DARF Versicherten gegen die **Operation-startRelocation** gemäß [I\_Information\_Service\_Accounts] für Zwecke abweichend Nutzung der Vorgaben in A\_24302\* NICHT nutzende ePA vorliegt oder ein Aktenkonto des Versicherten existiert. [ $\leq$ ]~~

#### **A\_24789 - Anbieter ePA-Aktensystem - verpflichtender Import eines existierenden Aktenkontos**

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

#### **Der 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 ).

#### **AA\_24790-01 - Anbieter ePA-Aktensystem - keine unbegründeter Import eines Aktenkontos**

Der Anbieter des ePA-Aktensystems DARF den Import eines existierenden Aktenkontos von einem anderen Anbieter für Zwecke abweichend der Vorgaben in A\_24302-\* NICHT nutzen oder veranlassen. [ <= ]

#### **A\_15870-01-02 - Anbieter ePA-Aktensystem - Abbruch bei Nichtverfügbarkeit anderer Anbieter**

Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen, wenn die ~~Operation startRelocation gemäß [I Information Service Accounts]~~ 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. [ <= ]

Hinweis zu A\_27344\*: Ein Import kann beispielsweise fehlschlagen, wenn schwerwiegende Fehler bei der Exportpaketerstellung oder bei der Übertragung auftreten (siehe 3.2- Health Record Relocation Service ).

#### **~~A\_23775 - Anbieter ePA-Aktensystem - Neues Aktenkonto anlegen~~**

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

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

#### **A\_14996-01 - Anbieter ePA-Aktensystem - Manuelle Ergänzung E-Mail-Adresse**

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

#### **A\_14993-02 - Anbieter ePA-Aktensystem - Mailadresse validieren**

Der Anbieter des ePA-Aktensystems MUSS eine Mailadresse

- 1507 • bei der ersten Hinterlegung im Aktensystem,
- 1508 • bei einer Änderung der Mailadresse

1509 auf Gültigkeit hin validieren. [≤]

#### 1510 **A\_24369 - Anbieter ePA-Aktensystem - Initialisierung des Aktenkontos**

1511 Der Anbieter des ePA-Aktensystems MUSS die Initialisierung der Bestandteile

- 1512 • Consent Decision Management (initiale Entscheidungen)
- 1513 • Constraint Management (Policies)
- 1514 • Entitlement Management (initiale Befugnisse und Befugnisausschlüsse)
- 1515 • Information Service (initiale Entscheidungen "Versorgungsprozess")
- 1516 • XDS Document Service (statische Aktenkontoinhalte)
- 1517 • Device Management
- 1518 • Authorization Service
- 1519 • Audit Event Service
- 1520 • Medication Service

1521 vor der Aktivierung eines Aktenkontos durchführen. Die genannten Bestandteile MÜSSEN  
1522 nach der Aktivierung des Aktenkontos sofort nutzbar sein. [≤]

1523 Im Zustand INITIALIZED obliegt es dem Anbieter, ein Aktenkonto mittels administrativer  
1524 Eingriffe in die verschiedenen Bestandteile des Aktensystems und -kontos auf die  
1525 Aktivierung vorzubereiten bzw. zu konfigurieren.

#### 1526 **A\_26005 - ePA-Aktensystem – Optionale Schnittstelle zum Einbringen von** 1527 **initialen Befugnissen**

1528 Das ePA-Aktensystem KANN eine Schnittstelle für Kostenträger anbieten, über die  
1529 Kostenträger die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle  
1530 ins ePA-Aktensystem einbringen können. [≤]

#### 1531 **A\_26006 - ePA-Aktensystem – Nutzen der optionalen Schnittstelle zum** 1532 **Einbringen von initialen Befugnissen ausschließlich im Status INITIALIZED**

1533 Falls das ePA-Aktensystem eine Schnittstelle für Kostenträger anbietet, über die  
1534 Kostenträger die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle  
1535 für ein Aktenkonto einbringen können, MUSS das ePA-Aktensystem sicherstellen, dass  
1536 diese Schnittstelle ausschließlich genutzt werden kann, wenn sich das Aktenkonto im  
1537 Status INITIALIZED befindet.

1538 [≤]

1539 Das Aktenkonto wird nach Abschluss der Initialisierung durch den Anbieter aktiviert und  
1540 kann dann durch befugte Nutzer und Nutzergruppen verwendet werden. Eine Aktivierung  
1541 erfolgt für den Rollout der ePA Version 3 im Kontext des ePA Go-Live-Termins und zu  
1542 späteren, individuellen Zeitpunkten, wenn Versicherte als ePA-Nutzer neu dazu  
1543 gekommen (bspw. Widerspruch wird zurückgenommen und ePA wird später angelegt  
1544 oder Versicherte Person kommt erstmalig ins Gesundheitssystem im Falle eines Zuzugs  
1545 oder eines Neugeborenen).

#### 1546 **A\_24335 - Anbieter ePA-Aktensystem - Neues Aktenkonto aktivieren**

1547 Der Anbieter des ePA-Aktensystems MUSS ein neues Aktenkonto nach Abschluss der  
1548 Initialisierung aktivieren (Status ACTIVATED), wenn die gesetzliche Widerspruchsfrist  
1549 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. [ $\leq$ ]

*Hinweis: Zur Schnittstelle I\_Information\_Service\_Accounts siehe [33.15.2- Information Service - Account](#) ).*

## **A\_24821 - Health Record Relocation Service - Suspendierung des Aktenkontos**

Der Health Record Relocation Service MUSS sicherstellen, dass das Aktenkontos für die Erstellung eines Exportpakets auf den Status SUSPENDED gesetzt wird. [ $\leq$ ]

## **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. [ $\leq$ ]

## **~~AA\_25005-0102~~ - 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
- Entitlement Management (außer Befugnisse für Versicherter, E-Rezept-Fachdienst, Kostenträger und Ombudsstelle).
- 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).

**[ $\Leftarrow$ ]**

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.

**[ $\leq$ ]**

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

## **A\_25605 - 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. [ $\leq$ ]

## **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. [ $\leq$ ]



1638 *Hinweis: Der CMAC einer Befugnis wird nicht ins Export-Paket übernommen.*

1639 **A\_25719 - Health Record Relocation Service - JWT der Befugnis im Exportpaket**

1640 Der Health Record Relocation Service MUSS sicherstellen, dass die Befugnisse im  
1641 Exportpaket als gültig signierte JWT mit den dargestellten Inhalten abgelegt sind:  
1642

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

1643 **[<=]**

1644 Der Wert "ES256" (JWS-Parameters "alg") gilt auch für die Kurve "brainpoolP256r1" (also  
1645 nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu  
1646 erstellen."

1647

1648 **A\_24787-01 - Health Record Relocation Service - Verschlüsselung des**  
1649 **Exportpaketes**

1650 Der Health Record Relocation Service MUSS sicherstellen, dass Exportpakete  
1651 ausschließlich verschlüsselt für den Download zu einem anderen Betreiber zur Verfügung  
1652 stehen. Für die Verschlüsselung MUSS das kryptographische Material des ENC-Zertifikats  
1653 verwendet werden, welches mittels der Regel hsm-r7 vom VAU-HSM abgerufen  
1654 wurde.**[<=]**

**A\_24942 - Health Record Relocation Service – Prüfung Provider ENC Zertifikat**

Der Health Record Relocation Service MUSS das übergebene Provider ENC-Zertifikat mittels TUC\_PKI\_018 (OCSP-Graceperiod=12h, PolicyList= oid\_fd\_enc, professionOID = oid\_epa\_vau ) prüfen und ungültige Zertifikate mit der Fehlermeldung " CERTIFICATE\_INVALID " ablehnen. [ <= ]

**A\_21750 - Health Record Relocation Service – Integritätsschutz Exportpaket**

Der Health Record Relocation Service MUSS das erstellte Exportpaket mit einem "Digest" HTTP Response Header ( <https://tools.ietf.org/html/rfc5843> ) als Integritätsschutz versehen und dabei als Digest Algorithmus SHA-256 verwenden.  
Beispiel Digest-Header:  
Digest: SHA-256=MWVkmWQxYTRiMzk5MDQ0MzI3NGU5NDEyZTk5OWY1ZGFmNzgyZTJlODYzYjRjYzFhOTlmNTQwYzI2M2QwM2U2MQ==  
[ <= ]

**A\_15051 - Health Record Relocation Service - Authentisierung gegenüber einem neuen Aktenanbieter**

Der Health Record Relocation Service, welcher das Exportpaket zur Verfügung stellt, MUSS sich beim Abruf des Exportpakets durch ein anderes ePA-Aktensystem mit der TLS-Identität oid\_epa\_mgmt und Zertifikatsprofil C.FD.TLS-S authentisieren.  
[ <= ]

**A\_15048 - Health Record Relocation Service - Authentifizierung des neuen Aktenanbieters**

Der Health Record Relocation Service MUSS den Abruf des Exportpakets durch ein anderes ePA-Aktensystem ablehnen, wenn sich der abrufende Client nicht als ePA-Aktensystem in der Rolle oid\_epa\_mgmt in einem TLS-Zertifikat C.FD.TLS-C authentisiert. [ <= ]

**A\_17236 - Health Record Relocation Service - Prüfung der TLS-Zertifikate**

Der Health Record Relocation Service MUSS bei der Authentifizierung eines anderen Aktensystems beim Abruf des Exportpakets die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC\_PKI\_018 durchführen. Zur Prüfung des TLS-Zertifikats C.FD.TLS-S sind dabei die Parameter PolicyList=oid\_fd\_tls\_s, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-serverAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD.TLS-C sind dabei die Parameter PolicyList=oid\_fd\_tls\_c, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-clientAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden.  
[ <= ]

**A\_15703 - Health Record Relocation Service - Verfügbarkeit Export-Paket**

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

**A\_21239 - Health Record Relocation Service – Verhalten bei Nichtabholen des Exportpakets**

Der Health Record Relocation Service MUSS nach Ablauf des Bereithaltungszeitraums entsprechend A\_15703\* ein erstelltes Export-Paket löschen und den Status des Aktensystems von SUSPENDED auf ACTIVATED zurücksetzen. [ <= ]

*Hinweis: siehe dazu auch 33.2.1.7.3- Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter*

**A\_14905-04 - Health Record Relocation Service – Import des Exportpakets des vorhergehenden Aktenkontos**

1705 Der Health Record Relocation Service MUSS das vom vorhergehenden Anbieter ePA-  
1706 Aktensystem des Versicherten bezogene Exportpaket, in das neue  
1707 Aktenkonto importieren und dazu:

- 1708 • das Exportpaket mittels des privaten ENC-VAU-Schlüssels des neuen  
1709 Betreibers entschlüsseln,
- 1710 • den Digest gemäß A\_21750-\* prüfen,
- 1711 • die Befugnisse mit Regel "rr5" (siehe Tab\_AS\_Entitlement\_Registration\_Rules im  
1712 Aktensystem) registrieren und
- 1713 • falls DocumentEntry.originalURI im Exportpaket vorhanden ist, wird für jedes  
1714 Dokument eines SubmissionSet der Inhalt von DocumentEntry.URI durch den  
1715 Inhalt von DocumentEntry.originalURI ersetzt. (Hinweis:  
1716 DocumentEntry.originalURI darf nicht als eigenständiges Metadatum in die  
1717 Registry übernommen werden, da es lediglich dem Transport des Originalwertes  
1718 von DocumentEntry.URI aus dem alten Aktensystem dient.

1719 [ $\leq$ ]

#### 1720 **A\_21548-01 - Health Record Relocation Service - Information der Vertreter über** 1721 **neuen FQDN nach Abschluss des Anbieterwechsels**

1722 Der Health Record Relocation Service MUSS sicherstellen, dass alle Vertreter nach  
1723 erfolgreichem Import des Exportpakets und somit Abschluss des Anbieterwechsels über  
1724 Anbieterwechsel und den FQDN des neuen Aktensystems des Versicherten informiert  
1725 werden, so dass sie in der Lage sind, die erforderliche initiale Anmeldung und  
1726 Geräteregistrierung durchzuführen und informiert sind, welche Art von  
1727 personenbezogenen Daten vom Vertreter im Rahmen der Vertreterberechtigung im ePA-  
1728 Aktensystem verarbeitet werden, wie der Vertreter eine Vertreterberechtigung widerrufen  
1729 kann und gegenüber wem er seine datenschutzrechtlichen Betroffenenrechte  
1730 wahrnehmen kann. [ $\leq$ ]

1731 Hinweis zu A\_21548-01: Für die Benachrichtigung derjenigen Vertreter, die dem  
1732 importierenden Aktensystem nicht bekannt sind, werden die E-Mail-Adressen aus dem  
1733 Exportpaket genommen. Für die Benachrichtigung der Vertreter, die dem importierenden  
1734 Aktensystem bekannt sind, wird die im importierenden Aktensystem hinterlegte E-Mail-  
1735 Adresse des Vertreters verwendet.

#### 1736 **A\_26257 - Health Record Relocation Service - Löschen der im Exportpaket** 1737 **enthaltenen E-Mail-Adressen der Vertreter**

1738 Der Health Record Relocation Service MUSS sicherstellen, dass die im Exportpaket  
1739 enthaltenen E-Mail-Adressen von Vertretern ausschließlich zur Information der Vertreter  
1740 gemäß A\_21548-\* genutzt werden und nach Abschluss des Anbieterwechsels im  
1741 importierenden Aktensystem gelöscht werden, d.h. nicht im importierenden Aktensystem  
1742 gespeichert werden. [ $\leq$ ]

#### 1743 **A\_24788 - Health Record Relocation Service - Löschen des Exportpakets nach** 1744 **Umzug des Aktenkontos**

1745 Das Aktensystem MUSS sicherstellen, dass ein vorhandenes Exportpaket nach einem  
1746 erfolgreichen Transfer eines Aktenkontos eines Versicherten von einem Anbieter zu  
1747 einem anderen Anbieter gelöscht wird. [ $\leq$ ]

1748

#### 1749 **AA\_24982-02 - Health Record Relocation Service – Protokollierung des** 1750 **Anbieterwechsels eines Aktenkontos**

1751 Der Health Record Relocation Service des neuen (importierenden) Aktensystems MUSS  
1752 nach der erfolgreichen oder einer abgebrochenen Übertragung der Inhalte eines

1753 Aktenkontos vom bisherigen Anbieter einen Protokolleintrag gemäß A\_24704\* erzeugen.  
 1754 Dabei ist folgende Wertebelegung zu berücksichtigen:

1755 **Tabelle 5 : Health Record Relocation Service Protokollierung**

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

1756 [**<=**]

1757 ~~Hinweis: Statuswechsel des Aktenkontos im Kontext eines Wechsels des Anbieters~~  
 1758 ~~erzeugen Protokolleinträge gemäß A\_24980\*.~~

1759

1760 *Hinweis: Das Aktensystem des bisherigen Anbieters muss keinen Protokolleintrag gemäß*  
 1761 *A\_24982\* erzeugen.*

## 1762 3.2.1 Ablauf eines Aktenkontoumzugs

### 1763 3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter

1764 Der Anbieter (neu) lässt im Aktensystem (neu) ein neues Aktenkonto anlegen. Dieses  
 1765 erhält den Status INITIALIZED. Hierfür gelten die Anforderungen gemäß 3.1.3- Anlage  
 1766 eines neuen Aktenkontos.

1767 Falls der Versicherte schon einen Widerspruch gegen die Nutzung der ePA bei seinem  
 1768 bisherigen Kostenträger erklärt hat, kann die Initialisierung eines neuen Aktenkontos ggf.  
 1769 entfallen<sub>7.1</sub>. Ein Transfer, bzw. die Erstellung eines Exportpakets, ist in diesem Fall  
 1770 mangels eines existierenden Aktenkontos beim bisherigen Anbieter nicht erforderlich.

1771 Die Abfrage eines existierenden Widerspruchs des Versicherten bei einem anderen  
1772 Anbieter ePA-Aktensystem erfolgt über dessen Information Service.

Abfrage eines existierenden Widerspruchs gegen die Nutzung der ePA

#### **I\_Information\_Service\_Accounts (bisheriges Aktensystem)**

getGeneralConsentDecision

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

### ~~3.2.1.2 Abfrage existierendes Aktenkonto und Anfrage zum Start Transfer~~

#### ~~3.2.1.2 Das Aktensystem (neu) fragt im Rahmen der Initialisierung des neuen eines existierenden Aktenkontos alle Aktensysteme der weiteren Betreiber an, ob bei diesen ein Aktenkonto für den Versicherten (KVNR) existiert.~~

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

1781 Das Aktensystem (alt), bei welchem das Aktenkonto existiert, bestätigt diese Anfrage  
1782 zum Transfer mit einer Vorgangs-ID.

Starten des Transfers

#### **I\_Information\_Service\_Accounts (bisheriges Aktensystem)**

startRelocation

initiiieren der Exportpaketerstellung

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

### **3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen Anbieter**

1789 Das Aktensystem (alt) informiert den Anbieter (alt) über die Anfrage zum Transfer und  
1790 die Vorgangsnummer. Der Anbieter (alt) öffnet das existierende Aktenkonto des  
1791 Versicherten und stößt in der VAU die Erzeugung des Exportpakets an. Der Health Record  
1792 Relocation Service beantwortet diese Anfrage durch Rückgabe einer URL für den späteren  
1793 Download des Exportpakets durch den neuen Anbieter und startet die Erzeugung des  
1794 Exportpakets. Das Aktenkonto wird vor der Paketerstellung auf den Status SUSPENDED  
1795 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

1796 In dieses Exportpaket werden alle Daten des Aktenkontos gemäß A\_25005\*  
 1797 übernommen. Das fertige Exportpaket wird mittels ENC-Zertifikat, welches im VAU-HSM  
 1798 eingebracht und gespeichert wurde, verschlüsselt und am vorbereiteten Downloadpunkt  
 1799 bereitgestellt.

#### 1800 **3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den** 1801 **neuen Anbieter**

1802 Der Anbieter (alt) veranlasst nach Erhalt der Download-URL über das Aktensystem (alt)  
 1803 den Versand der Url an das Aktensystem (neu).

1804 Das Aktensystem (alt) prüft vor der Übermittlung der Download-URL an das Aktensystem  
 1805 (neu), ob das Exportpaket für den Download bereitsteht, ggf. wird auf den Abschluss der  
 1806 Paketerstellung gewartet. Ist dieses der Fall, erfolgt die Benachrichtigung des  
 1807 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
--------------------------------	-------------------------------------

#### 1808 **3.2.1.5 Import des Exportpakets durch den neuen Anbieter**

1809 Der Information Service des Aktensystems (neu) nimmt die Download-URL entgegen und  
 1810 übermittelt diese an den Kostenträger (neu). Dieser öffnet den Zugang zum Aktenkonto  
 1811 (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
--------------------	---

#### 1812 **3.2.1.6 Abschluss des Transfers durch beide Anbieter**

1813 Das Aktensystem (neu) startet den Download des Exportpakets, entschlüsselt dieses und  
 1814 übernimmt die Daten in das initialisierte Aktenkonto des Versicherten. Nach  
 1815 erfolgreichem Abschluss wird (kann) das Aktenkonto (neu) in den Status ACTIVATED  
 1816 überführt werden.

1817 Unter Verwendung des Information Service wird das Aktensystem (alt) über den  
 1818 erfolgreichen Import und den Abschluss des Transfers informiert. Das Aktenkonto (alt)  
 1819 kann daraufhin, ggf. unter Einhaltung weiterer Bedingungen des Kostenträgers bzw.  
 1820 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)
---------------------	--



### 1821 3.2.1.7 Fehlersituationen und Handhabung

1822 Der gesamte Austausch von Informationen zwischen Aktensystemen und Anbietern kann  
 1823 durch die in ~~Schritt~~Schritt 1 erzeugte Vorgangs-ID genau einem konkreten Relocation  
 1824 Vorgang zugeordnet werden. Diese Vorgangsnummer wird auch verwendet, wenn das  
 1825 jeweils andere Aktensystem über Fehler im Ablauf benachrichtigt werden muss  
 1826 (Incidents).

1827 *3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich oder*  
 1828 *derzeit nicht möglich*

1829 Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter  
 1830 (alt) das Exportpaket voraussehbar nicht importieren oder widerspricht der Versicherte  
 1831 nach der Initialisierung des Aktenkontos beim neuen Kostenträger der Nutzung der ePA,  
 1832 so kann durch Übertragung eines Incidents an das Aktensystem (alt) dieser Sachverhalt  
 1833 mitgeteilt werden, so dass der Transfervorgang abgebrochen und das Exportpaket nicht  
 1834 erzeugt oder wieder gelöscht wird.

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

1835 Das Aktenkonto wird bei Anbieter (alt) wieder in den Status ACTIVATED gesetzt, um eine  
 1836 weitere Nutzung zu ermöglichen.

1837 Für einen Transfer zu einem späteren Zeitpunkt muss der Anbieter (neu) den Vorgang  
 1838 durch Anfrage bei den weiteren Anbietern (alt) und Übermittlung eines ENC-Zertifikats  
 1839 erneut starten.

1840 *3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter*

1841 Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter  
 1842 (alt) das Exportpaket unter Verwendung der übertragenen Download-URL nicht oder  
 1843 nicht vollständig laden oder die Inhalte des Exportpaketes aufgrund fehlerhafter  
 1844 Verschlüsselung oder fehlerhafter Struktur oder Inhalte nicht erfolgreich integrieren oder

1845 der Anbieter (neu) hat keine Download-URL vom Anbieter (alt) bezogen, so kann durch  
 1846 Übertragung eines Incidents an den Anbieter (alt) dieser Sachverhalt mitgeteilt werden.

Incident Fehler bei Import		
<b>I_Information_Service_Accounts (bisheriges Aktensystem)</b>		
postExportPackageIncident	Benachrichtigung zu Problemen beim Import des Exportpakets	
	<b>Incident</b>	
	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

1847 Das Aktenkonto verbleibt beim neuen Anbieter in Status INITIALIZED. Die  
 1848 Incidentmeldung an den Anbieter (alt) kann durch Kommunikation der Anbieter und/oder  
 1849 Betreiber untereinander zum Zweck der Problemlösung ergänzt werden.

1850 Der Anbieter (alt) meldet die Korrektur durch erneuten Versand einer Download-URL an  
 1851 den Anbieter (neu) für den unterbrochenen Vorgang.

1852 Es obliegt dem Anbieter (alt), bei zeitlich aufwendigen Korrekturen das Aktenkonto  
 1853 zunächst für eine weitere Nutzung wieder zu aktivieren (Status ACTIVATED) und nach  
 1854 Abschluss der Korrektur wieder in den Status SUSPENDED zu überführen.

1855 Es obliegt dem Anbieter (alt) auch, bei zeitlich aufwendigen Korrekturen den Transfer  
 1856 durch Senden des Incidents "relocationAborted" an den Anbieter (neu) abubrechen und  
 1857 das Aktenkonto zur weiteren Nutzung wieder zu aktivieren (Status ACTIVATED). Der  
 1858 Transfer muss dann durch den Anbieter (neu) erneut gestartet werden.

1859 *3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter*

1860 Ruft ein neuer Anbieter ein bereitgestelltes Exportpaket nicht ab oder erfolgt durch den  
 1861 neuen Anbieter keine Benachrichtigung über einen erfolgreichen Abschluss des Transfers

1862 oder einen Fehler beim Import des Exportpakets, dann kann eine Benachrichtigung an  
1863 den neuen Anbieter erfolgen.

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

1864 Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei  
1865 Anbieter (alt) auf den Status ACTIVATED gesetzt, um eine weitere Nutzung zu  
1866 ermöglichen. Exportpaket und Downloadlink können gelöscht werden. Der Transfer muss  
1867 durch den Anbieter (neu) erneut gestartet werden.

#### 1868 3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter

1869 Ein Anbieter (alt) kann den Abbruch eines angeforderten Transfers an den Anbieter (neu)  
1870 signalisieren.

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

1871 Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei  
1872 Anbieter (alt) auf den Status ACTIVATED zurückgesetzt, wenn dieses schon den Status

1873 SUSPENDED hat, um eine weitere Nutzung zu ermöglichen. Exportpaket und  
 1874 Downloadlink können gelöscht werden. Der Transfer muss durch den Anbieter (neu)  
 1875 erneut gestartet werden.

### 1876 3.3 Sichere Speicherung sensibler Schlüssel und Informationen im 1877 VAU-HSM

1878 Im Folgenden wird beschrieben, welche Informationen in einem HSM (als VAU-HSM  
 1879 bezeichnet) zu speichern sind.

1880 Verständnishinweis: Die HMAC-Schlüssel (symmetrische Schlüssel) für die Prüfung der  
 1881 VSDM+-Prüfnachweise [gemSpec\_SST\_FD\_VSDM], [C\_11321] werden von den VSDM-  
 1882 Betreibern erzeugt und für die ePA-VAUs der ePA-Betreiber verschlüsselt exportiert. Die  
 1883 Schlüssel und auch die Export/Import-Vorgänge (Mehr-Augen-Prinzip) sind die gleichen  
 1884 wie sie auch für/bei der E-Rezept-VAU verwendet werden.

#### 1885 **AA\_24611-0203 - ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und** 1886 **Informationen für VAU-Betrieb**

1887 Das ePA-Aktensystem MUSS sicherstellen, dass folgende, für den Betrieb der VAU  
 1888 notwendigen Schlüssel und Informationen in einem HSM (als VAU-HSM bezeichnet)  
 1889 gespeichert werden:

- 1890 • privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU  
 1891 (u.a. genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- 1892 • ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- 1893 • ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- 1894 • privater Schlüssel der Verschlüsselungsidentität der VAU
- 1895 • privater Schlüssel der Signaturidentität der VAU
- 1896 • Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die  
 1897 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- 1898 • Masterkeys für die Ableitung der versichertenindividuellen  
 1899 Datenpersistierungsschlüssel
- 1900 • Masterkeys für die Ableitung der versichertenindividuellen  
 1901 Befugnispersistierungsschlüssel
- 1902 • Masterkeys für die Ableitung der versichertenindividuellen  
 1903 Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und  
 1904 Überschlüsselung")
- 1905 • symmetrische Schlüssel für die HMAC-Prüfung der VSDM-Prüfziffern (jeweils einen  
 1906 pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als  
 1907 gemeinsames Geheimnis bezeichnet werden.
- 1908 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- 1909 • Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für  
 1910 die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf.  
 1911 für Service-VAUs)
- 1912 • Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

1913 [<=]

**Hinweis:**

Es gelten die Anforderungen aus [gemSpec Krypt#3.18 VSDM-Prüfziffer Version 2] für ein ePA-Aktensystem in der Rolle "Prüfziffer Version 2 prüfendes System". Aus den ins HSM importierten gemeinsamen Geheimnissen erfolgt im HSM eine Schlüsselableitung (A\_27299-\*) der für die Entschlüsselung der Prüfziffer Version 2 benötigten AES/GCM-Schlüssel.

- ~~• 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).~~

**A\_26109 - ePA-Aktensystem - Unterschiedliche private****Authentisierungsschlüssel für AK-, Befugnisverifikations- und Service-VAU**

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

**A\_26110 - ePA-Aktensystem - Unterschiedliche private****Authentisierungsschlüssel für unterschiedliche Service-VAUs**

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

Hinweis zu A\_26110: Ein Typ einer Service-VAU könnte beispielsweise eine PDF-Konvertierungs-Service-VAU ~~oder eine Pseudonymisierungs-Service-VAU für Daten zur Sekundärnutzung sein.~~ Alle Instanzen einer PDF-Konvertierungs-Service-VAU nutzen denselben privaten Authentisierungsschlüssel. Die Instanzen der Pseudonymisierungs-Service-VAU dürfen den Authentisierungsschlüssel der PDF-Konvertierungs-Service-VAU jedoch nicht verwenden.

**~~AA\_24612-0304~~ - ePA-Aktensystem - Erzwingen von 4-Augen-Prinzip für Einbringen und Verwalten von Informationen ins VAU-HSM**

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

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- 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).

[<=]

- ~~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).~~

[<=>]

#### **AA\_24614-0203 - 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 policyIdentifier oid\_epa\_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- 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.

#### **AA\_24618-0203 - 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:

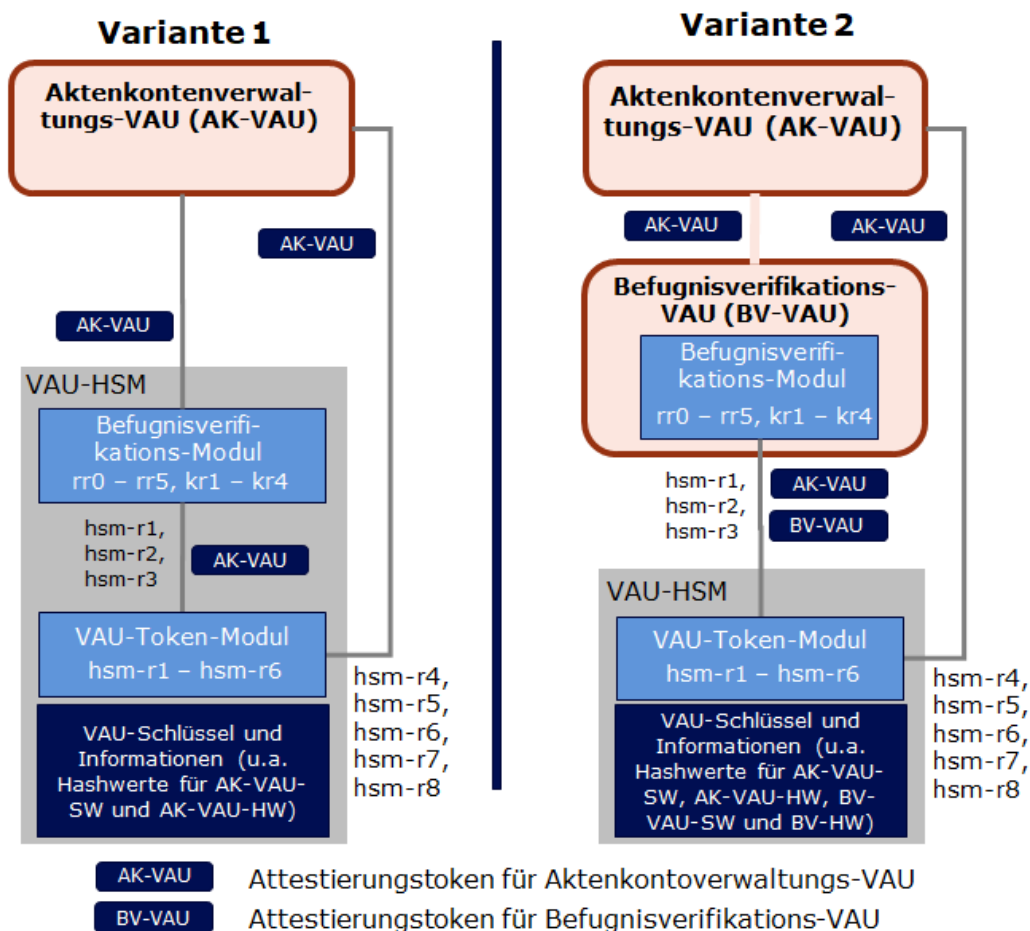
- privater Schlüssel der Authentisierungsidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU ausschließlich durch eine Befugnisverifikations-VAU-Instanz



- 2003 • privater Schlüssel der Authentisierungsidentität eines Service-VAU-Typs
- 2004 ausschließlich durch eine Service-VAU-Instanz dieses Service-VAU-Typs
- 2005 • privater Schlüssel der Verschlüsselungsidentität der VAU ausschließlich durch eine
- 2006 Aktenkontoverwaltungs-VAU-Instanz
- 2007 • privater Schlüssel der Signaturidentität der VAU ausschließlich durch eine
- 2008 Aktenkontoverwaltungs-VAU-Instanz
- 2009 • Zertifikat C.FD.ENC mit policyIdentifier oid\_epa\_vau für die
- 2010 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers ausschließlich
- 2011 durch eine Aktenkontoverwaltungs-VAU-Instanz
- 2012 • Masterkeys für die Ableitung der versichertenindividuellen
- 2013 Datenpersistierungsschlüssel ausschließlich durch eine Aktenkontoverwaltungs-
- 2014 VAU-Instanz
- 2015 • Masterkeys für die Ableitung der versichertenindividuellen
- 2016 Befugnispersistierungsschlüssel ausschließlich durch eine Aktenkontoverwaltungs-
- 2017 VAU-Instanz
- 2018 • Masterkeys für die Ableitung der versichertenindividuellen
- 2019 Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und
- 2020 Überschlüsselung") ausschließlich durch die Aktenkontoverwaltungs-VAU-Instanz
- 2021 oder durch eine dedizierte Überschlüsselungs-VAU
- 2022 • symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-
- 2023 Dienst-Betreiber)), die im Kontext der Prüfziffer Version 2 auch als gemeinsames
- 2024 Geheimnis bezeichnet werden, ausschließlich durch eine Aktenkontoverwaltungs-
- 2025 VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz
- 2026 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- 2027 ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine
- 2028 Befugnisverifikations-VAU-Instanz.
- 2029 [ $\leq$ ]

### 2030 3.4 Befugnisverifikations-Modul

- 2031 Das Befugnisverifikations-Modul enthält die Regeln zur Befugnisregistrierung (entitlement
- 2032 registration rules) und die Regeln zum Abruf der versichertenindividuellen
- 2033 Persistierungsschlüssel (key rules).
- 2034 Die folgende Abbildung zeigt die zwei möglichen Architekturvarianten für die Ausführung
- 2035 des Befugnisverifikations-Moduls. In Variante 1 wird es direkt im VAU-HSM ausgeführt. In
- 2036 Variante 2 wird es in einer Befugnisverifikations-VAU ausgeführt, die zwischen einer
- 2037 Aktenkontoverwaltungs-VAU und einem VAU-HSM vermittelt und Prüfungen für das VAU-
- 2038 HSM übernimmt (z. B. prüfen der ID-Token oder registrieren neuer Befugnisse).
- 2039 In beiden Varianten ist ein Zugriff auf die Schlüssel im VAU-HSM nur durch integrale und
- 2040 attestierte VAUs möglich. Die Prüfung der VAU-Attestierungstoken verbleibt in beiden
- 2041 Varianten im VAU-HSM (VAU-Token-Modul). Das VAU-HSM speichert in Variante 2 neben
- 2042 den Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware
- 2043 für die VAU der Aktenkontoverwaltung zusätzlich auch die Hashwertrepräsentationen der
- 2044 erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der
- 2045 Befugnisverifikations-VAU. Ein Zugriff auf das HSM ist dann nur mit einem validen
- 2046 Attestierungstoken für die Aktenkontoverwaltung-VAU und die Befugnisverifikations-VAU
- 2047 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. [≤]

**AA\_25282-0102 - ePA-Aktensystem - Regeln des VAU-Token-Moduls**

Das VAU-Token-Modul MUSS die in Tabelle *Tab\_AS\_VAU-Token\_Modul\_Rules* definierten Regeln umsetzen. [≤]

**Tabelle 6: 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><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• VAU-Attestierungstoken einer Befugnisverifikations-VAU (optional)</li> <li>• Daten</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Daten gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur(en)des(r) VAU-Attestierungstoken (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> <li>3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <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><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• KVNR</li> <li>• gewünschte Persistierungsschlüssel [Label für Datenpersistierungs-Masterkey und/oder Label für Befugnispersistierungs-Masterkey]</li> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• falls in Eingangsdaten angefordert: versichertenindividueller Befugnispersistierungsschlüssel</li> <li>• falls in Eingangsdaten angefordert: versichertenindividueller Datenpersistierungsschlüssel</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> <li>3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <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>Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfziffern <u>der Version 1 oder der Entschlüsselung der VSDM-Prüfziffern der Version 2</u></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li><del>Daten</del></li> <li><del>Bezeichner des HMAC-Schlüssels</del></li> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.)</li> <li><u>Szenario VSDM-Prüfziffer Version 1</u> <ul style="list-style-type: none"> <li><u>Daten</u></li> <li><u>Bezeichner des HMAC-Schlüssels</u></li> </ul> </li> <li><u>Szenario VSDM-Prüfziffer Version 2</u> <ul style="list-style-type: none"> <li><u>VSDM-Prüfziffer in Version 2</u></li> </ul> </li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li><u>Szenario VSDM-Prüfziffer Version 1:</u> HMAC der Daten mit dem symmetrischen Schlüssel, der zum übergebenen Bezeichner des HMAC-Schlüssels gehört</li> <li><u>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</u></li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch)</li> <li>prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> <li>(opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <p><u>Szenario VSDM-Prüfziffer Version 1:</u> Falls die Prüfungen 1) - 3) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.</p> <p><u>Szenario VSDM-Prüfziffer Version 2:</u> 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><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Challenge</li> <li>• [VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU] VAU-Attestierungstoken einer Befugnisverifikations-VAU] VAU-Attestierungstoken eines Service-VAU-Typs]</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Challenge signiert mit privatem Schlüssel der AUT-Identität</li> <li>• der Aktenkontoverwaltungs-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU übergeben wurde,</li> <li>• der Befugnisverifikations-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Befugnisverifikations-VAU übergeben wurde,</li> <li>• des Service-VAU-Typs, falls in den Eingangsdaten ein VAU-Attestierungstoken des Service-VAU-Typs übergeben wurde.</li> </ul> <p><b>Prüfschritte</b></p> <ol style="list-style-type: none"> <li>1. prüfen der <del>Signatur des</del> <u>Signaturdes</u> VAU-Attestierungstokens (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und zum VAU-Typ passt.</li> </ol> <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><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• verschlüsselte Daten</li> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• entschlüsselte Daten</li> </ul> <p><b>Prüfschritte</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind.</li> </ol> <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><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• zu signierende Daten</li> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• signierte Daten</li> </ul> <p><b>Prüfschritte</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen Daten mit dem privatem 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><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Verschlüsselungszertifikat C.FD.ENC des anderen Aktensystembetreibers</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen der <del>Signatur des</del> <u>Signaturdes</u> VAU-Attestierungstokens (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind</li> </ol> <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><del>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.</del></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder einer Service-VAU</li> <li>• Ableitungsvektor <i>dv</i></li> <li>• Label für Masterkey (opt.)</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• symmetrischer Schlüssel <i>symKey</i></li> <li>• Label für Befugnis-Masterkey</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</li> <li>2. prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und es sich um die Attestierung einer Aktenkontoverwaltungs-VAU oder Service-VAU handelt</li> <li>3. falls ein Label für einen Masterkey In den Eingangsdaten enthalten ist, prüfen, ob das Label zu einem Befugnis-Masterkey gehört</li> </ol> <p>Falls alle Prüfungen erfolgreich waren, wird <i>symKey</i> wie folgt abgeleitet:</p> <p>Fall: Eingangsdaten enthalten ein Label <i>mkey_label</i> für einen Befugnis-Masterkey:  Ableitung eines AES-Schlüssels [FIPS-197] <i>symKey</i> mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren auf Basis des Befugnis-Masterkeys mit Label <i>mkey_label</i> und dem Ableitungsvektor "eds: "+ <i>dv</i>. Ausgangsdaten sind der abgeleitete Schlüssel <i>symKey</i> und das Label <i>mkey_label</i>.</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 (<i>dv</i>) vorangestellt wird.)</p> <p>Fall: Eingangsdaten enthalten kein Label für einen Befugnis-Masterkey:  Ableitung eines AES-Schlüssels [FIPS-197] <i>symKey</i> mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#Abschnitt 2.4] zulässigen Verfahren auf Basis des aktuellen Befugnis-Masterkeys und dem Ableitungsvektor "eds: " + <i>dv</i>. Ausgangsdaten sind der abgeleitete Schlüssel <i>symKey</i> und das Label des aktuellen Befugnis-Masterkeys.</p>

2078

### 2079 **A\_24667 - ePA-Aktensystem -VAU-HSM - Prüfen des VAU-Attestierungstokens**

2080 Das VAU-HSM MUSS bei der Prüfung eines VAU-Attestierungstokens sicherstellen, dass  
 2081 dieses zeitlich gültig ist und Replay-Attacken abwehren. [≤]

### 2082 **A\_26303 - ePA-Aktensystem - Abgeleitete Verschlüsselungsschlüssel sind** 2083 **ausschließlich einer VAU zugänglich**

2084 Das ePA-Aktensystem MUSS sicherstellen, dass ein mit Regel hsm-r8 abgeleiteter  
 2085 Schlüssel ausschließlich einer VAU zugänglich ist und ausschließlich mittels AES/GCM  
 2086 analog [gemSpec\_Krypt#GS-A\_4389] verwendet wird. [≤]

## 2087 **3.4.2 Regeln des Befugnisverifikations-Moduls**

2088 Die folgende Tabelle zeigt die Regeln des Befugnisverifikations-Moduls im Überblick.

2089 **Tabelle 7: Überblick über die Regeln des Befugnisverifikations-Moduls**

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
rr0	Mit dieser Regel werden <b>ID-Token</b> im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr1	Mit dieser Regel werden vom <b>Aktenkontoinhaber</b> am ePA-FdV erstellte <b>Befugnisse</b> 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 <b>Vertreter</b> am ePA-FdV erstellte <b>Befugnisse</b> 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 <b>Befugnisse</b> im Aktensystem registriert, die sich durch <del>das Stecken</del> <u>das Stecken</u> der <b>eGK in einer Leistungserbringerumgebung</b> ergeben.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr4	Mit dieser Regel werden die <b>Befugnisse</b> für den Kostenträger und die zuständige Ombudsstelle bei der <b>Anlage eines Aktenkontos</b> im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
rr5	Mit dieser Regel werden die <b>Befugnisse</b> bei einem <b>betreiberübergreifenden Anbieterwechsel</b> im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
kr1	Diese Regel wird für die <b>Anmeldung</b> des <b>Aktenkontoinhabers</b> genutzt.	<i>Tab_AS_SDS-Key_Rules</i>
kr2	Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssels genutzt. Sie wird für die <b>Anmeldung</b> 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 <b>Anmeldung</b> von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	<i>Tab_AS_SDS-Key_Rules</i>
kr4	Diese Regel wird für die <b>Anmeldung</b> des <b>E-Rezept-Fachdienstes</b> 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>

2090

2091

2092

2093

2094

**AA\_24573-0203 - ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls**

Das Befugnisverifikations-Modul MUSS die in den Tabellen *Tab\_AS\_Entitlement\_Registration\_Rules* und *Tab\_AS\_SDS-Key\_Rules* definierten Regeln umsetzen. [ $\leq$ ]

2095  
2096

**Tabelle 8: Tab\_AS\_Entitlement\_Registration\_Rules - Regeln zur Registrierung von Befugnissen**

Regel	Beschreibung
rr0	<p>Mit dieser Regel werden <b>ID-Token</b> im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• ID-Token mit NutzerID=x signiert durch einen sektoralen Identity Provider, den IDP-Dienst oder den E-Rezept-Fachdienst</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• HSM-ID-Token mit NutzerID=x gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>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).</li> <li>2. Falls die Prüfung in 1) erfolgreich war, <ol style="list-style-type: none"> <li>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).</li> <li>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"> <li>i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> </ol> </li> <li>3. Das Befugnisverifikations-Modul liefert das mittels CMAC gesicherte HSM-ID-Token als Ergebnis des Regelaufrufs zurück.</li> </ol>

rr1	<p>Mit dieser Regel werden vom <b>Aktenkontoinhaber</b> am ePA-FdV erstellte Befugnisse im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• ID-Token oder HSM-ID-Token gesichert mit CMAC</li> <li>• Befugnis1 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) signiert vom Versicherten</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Befugnis2 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen des ID-Tokens gemäß <u>Tokensgemäß</u> A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> <li>a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist</li> <li>b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt</li> </ol> <p>oder prüfen des HSM-ID-Tokens</p> <ol style="list-style-type: none"> <li>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"> <li>i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>d. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist</li> <li>e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt.</li> </ol> </li> <li>2. prüfen der Befugnis1 <ol style="list-style-type: none"> <li>a. prüfen der Signatur gemäß A_25042-* (Zertifikatsprofil C.CH.SIG)</li> <li>b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_versicherter</code> ist</li> <li>c. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der "KVNR Aktenkonto" in der Befugnis1 übereinstimmt.</li> <li>d. prüfen, dass das JWT gemäß A_24587-* <u>nicht-abgelaufenzeitlich gültig</u> ist (<u><math>\text{Feld:iat} - 15s \leq \text{aktuelle Zeit} \leq \text{exp} + 15s</math></u>)</li> </ol> </li> <li>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:</li> </ol>
-----	--

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"><li>4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis2<ol style="list-style-type: none"><li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li></ol></li><li>5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.</li></ol>

rr2	<p><i>Mit dieser Regel werden vom <b>Vertreter</b> 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><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• ID-Token oder HSM-ID-Token gesichert mit CMAC</li> <li>• Befugnis1 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) signiert vom Vertreter</li> <li>• Befugnis2 = (KVNR Aktenkonto, KVNR Vertreter) gesichert mittels CMAC</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Befugnis3 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> <li>a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist</li> <li>b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt</li> </ol> oder prüfen des HSM-ID-Tokens <ol style="list-style-type: none"> <li>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"> <li>i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>d. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist</li> <li>e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt.</li> </ol> </li> <li>2. prüfen der Befugnis1 und Befugnis2 <ol style="list-style-type: none"> <li>a. prüfen der Signatur von Befugnis1 gemäß A_25042-* (Zertifikatsprofil C.CH.SIG)</li> <li>b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek_versicherter</code> ist</li> <li>c. prüfen des CMAC von Befugnis2</li> <li>d. prüfen, dass die Telematik-ID in Befugnis 1 keine KVNR ist (Vertreter dürfen keine weiteren Vertreter befugen)</li> <li>e. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der „KVNR Vertreter“ in der Befugnis2 übereinstimmt</li> </ol> </li> </ol>
-----	---



Regel	Beschreibung
	<ul style="list-style-type: none"> <li>f. prüfen, ob die „KVNR Aktenkonto“ in Befugnis 1 mit der „KVNR Aktenkonto“ in Befugnis2 übereinstimmt</li> <li>g. prüfen, dass das JWT gemäß A_24587-* <del>nicht-abgelaufen</del><u>zeitlich gültig</u> ist (<del>Feld: iat</del> - 15s &lt;= aktuelle Zeit &lt; <del>exp</del> + 15s)</li> <li>3. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis3 vom Befugnisverifikations-Modul erstellt. Die Inhalte werden aus Befugnis1 übernommen.</li> <li>4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis3 <ul style="list-style-type: none"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ul> </li> <li>5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis3 als Ergebnis des Regelaufrufs zurück.</li> </ul>

rr3	<p>Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das Stecken der eGK in einer Leistungserbringenumgebung ergeben.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• <u>VSDM-Prüfziffer des VSDM-Prüfungsnachweises in Version 1 oder 2</u> signiert mit AUT-Identität der SMC-B</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels <u>CMAC<sub>CMA</sub></u></li> </ul> <p><b>Prüfschritte:</b></p> <ul style="list-style-type: none"> <li>• <u>falls VSDM-Prüfziffer in Version 2, zusätzlich die innere Struktur der Prüfziffer im Klartext gemäß A 27278-* (I Feld 1, r iat 8, KVNR)</u></li> </ul> <p><b>Prüfschritte:</b>  <u>Prüfen, ob die übergebene VSDM-Prüfziffer eine Version 1 oder Version 2 ist: Führe für die VSDM-Prüfziffer die Prüfschritte 1. und 2. gemäß A 27279-* durch. Es ergibt sich die dekodierte VSD-Prüfziffer, an der man am Most-significant-Bit erkennt, ob es sich um Version 1 oder Version 2 der Prüfziffer handelt.</u></p> <p><u>Szenario VSDM-Prüfziffer in Version 1:</u></p> <ol style="list-style-type: none"> <li>1. prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A_25042-* (C.HCI.AUT)</li> <li><del>1. prüfen, dass das JWT gemäß A_24590-* nicht abgelaufen ist (Feld: exp)</del></li> <li><u>2. Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert.</u></li> <li><u>2.3. prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer nicht länger als 20 Minuten zurückliegt</u>  <u>mit <math>\text{prüfziffer.timestamp} - 30s \leq \text{aktuelle Zeit} &lt; \text{prüfziffer.timestamp} + 20 \text{ Minuten} + 15s</math></u></li> <li><u>3.4. prüfen des HMAC der VSDM-Prüfziffer mittels VAU-HSM Regel hsm-r3</u> <ol style="list-style-type: none"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li><u>4.5. Falls die Prüfungen in 1) bis 4) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:</u> <ul style="list-style-type: none"> <li>• Aktenkonto: die KVNR aus dem VSDM-Prüfziffer</li> <li>• Telematik-ID: die Telematik-ID aus der SMC-B-Signatur</li> <li>• Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur.</li> </ul> </li> <li><u>5.6. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis</u></li> </ol>
-----	---

Regel	Beschreibung
	<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><u>7.</u> Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis als Ergebnis des Regelaufrufs zurück.</p> <p><u>Szenario VSDM-Prüfziffer in Version 2:</u></p> <ol style="list-style-type: none"> <li><u>1. prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A 25042-* (C.HCI.AUT)</u></li> <li><u>2. Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert.</u></li> <li><u>3. Aufruf von VAU-HSM Regel hsm-r3 mit der dekodierten VSDM-Prüfziffer</u> <ol style="list-style-type: none"> <li><u>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</u></li> </ol> </li> <li><u>4. prüfen der inneren Struktur nach Prüfschritt 6 gemäß A 27279-* (d.h. eGK ist nicht gesperrt)</u></li> <li><u>5. prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer (prüfziffer.iat) nicht länger als 20 Minuten zurückliegt (prüfziffer.iat - 30s &lt;= aktuelle Zeit &lt; prüfziffer.iat + 20 Minuten +15s, Hinweis in der Prüfziffer gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben)</u></li> <li><u>6. prüfen des prüfziffer.hcv nach Prüfschritt 8 gemäß A 27279-* bzgl. des hcv im JWT</u></li> <li><u>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:</u> <ul style="list-style-type: none"> <li><u>• Aktenkonto: KVNR, die als Ergebnis der VAU-HSM Regel hsm-r3 zurückgeliefert wird</u></li> <li><u>• Telematik-ID: die Telematik-ID aus der SMC-B-Signatur</u></li> <li><u>• Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur.</u></li> </ul> </li> <li><u>8. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis</u> <ol style="list-style-type: none"> <li><u>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</u></li> </ol> </li> </ol> <p><u><del>1.</del>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.</u></p>

Regel	Beschreibung
rr4	<p><i>Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der <b>Anlage eines Aktenkontos</b> im Aktensystem registriert.</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• Befugnis1 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) signiert mit SMC-B des Kostenträgers bzw. der Ombudsstelle</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Befugnis2 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. Prüfen der Befugnis1 <ol style="list-style-type: none"> <li>a. prüfen der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle gemäß A_25042-* (C.HCI.OSIG)</li> <li>b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_kostentraeger</code> bzw. <code>oid_ombudsstelle</code> ist</li> <li>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</li> </ol> </li> <li>2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 erstellt. Die Inhalte der Befugnis2 sind: <ul style="list-style-type: none"> <li>• Aktenkonto: die KVNR des Aktenkontos aus Befugnis1</li> <li>• Telematik-ID: die Telematik-ID aus Befugnis1</li> </ul> </li> <li>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"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.</li> </ol>

Regel	Beschreibung
rr5	<p>Mit dieser Regel werden die <b>Befugnisse</b> bei einem <b>betreiberübergreifenden Anbieterwechsel</b> im Aktensystem registriert.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>Befugnis1 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) signiert vom alten Aktensystembetreiber</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>Befugnis2 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) gesichert mittels CMAC</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>Prüfen der Befugnis1 <ol style="list-style-type: none"> <li>prüfen der Signatur gemäß A_25042-* (C.FD.SIG)</li> <li>prüfen, ob im Signaturzertifikat C.FD.SIG der policyIdentifier <code>oid_epa_vau</code> ist</li> <li>prüfen, dass das Signaturzertifikat C.FD.SIG nicht auf das importierende Aktensystem ausgestellt ist.</li> </ol> </li> <li>Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 mit den Inhalten aus Befugnis1 erstellt.</li> <li>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"> <li>Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.</li> </ol>

2097

## 2098 **A\_24690-01 - ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen des ID-Tokens**

2099

2100 Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung eines ID-Tokens durchführen:

2101

- 2102 • das ID-Token muss gemäß A\_25042-\* valide signiert sein durch einen sektoralen Identity Provider oder den IDP-Dienst (professionOID ist `oid_idpd_sek` oder `oid_idpd`),
- 2103 • das ID-Token muss zeitlich gültig sein (Felder: `iat`, `exp`),
- 2104 • das ID-Token muss im Feld `aud` das ePA-Aktensystem eingetragen haben.

2105

2106

2107 [**<=**]

2108 **A\_24691 - ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen von übers**  
 2109 **ePA-FdV erstellten Befugnissen**

2110 Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung einer von  
 2111 einem Versicherten bzw. Vertreter über das ePA-FdV eingestellten signierten Befugnis  
 2112 durchführen:

- 2113 • die Befugnis muss gemäß A\_25042-\* valide signiert sein durch einen Versicherten  
 2114 bzw. Vertreter (C.CH.SIG, professionOID ist `oid_versicherter`),
- 2115 • das JWT für die Befugnis gemäß A\_24587-\* darf nicht abgelaufen sein (Feld:  
 2116 `exp`),
- 2117 • das Feld `insurantID` des JWT muss eine KVNR sein,
- 2118 • das Feld `actorID` des JWT muss eine KVNR oder eine Telematik-ID sein,
- 2119 • das Feld `validTO` des JWT muss ein zeitliches Datum sein.

2120 **[<=]**

2121 Die folgenden Regeln dienen zum Abruf der versichertenindividuellen Daten- und  
 2122 Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel und  
 2123 die Ableitungsvorschriften sind in [gemSpec\_Krypt] in Abschnitt 3.15.2 festgelegt.

2124 **Tabelle 9: Tab\_AS\_SDS-Key\_Rules Key Rules - Regeln zur Ableitung der**  
2125 **versichertenindividuellen Persistierungsschlüssel**



Regel	Beschreibung
kr1	<p><i>Diese Regel wird für die Anmeldung des <b>Aktenkontoinhabers</b> genutzt.</i></p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• ID-Token oder HSM-ID-Token gesichert mit CMAC</li> <li>• Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "&lt;current&gt;" für jüngsten im VAU-HSM verfügbaren).</li> <li>• Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "&lt;current&gt;" für jüngsten im VAU-HSM verfügbaren).</li> <li>• ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys</li> <li>• versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys</li> </ul> <p><b>Regelverhalten:</b></p> <ol style="list-style-type: none"> <li>1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> <li>a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist oder prüfen des HSM-ID-Tokens</li> <li>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"> <li>i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>c. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist</li> </ol> </li> <li>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"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>3. Das Befugnisverifikations-Modul liefert die abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.</li> </ol>

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><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• KVNR (Aktenkonten-ID)</li> <li>• Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> <li>• ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys</li> <li>• ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>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"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>2. Das Befugnisverifikations-Modul liefert den abgeleiteten Befugnispersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.</li> </ol>

kr3

*Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.*

**Eingangsdaten:**

- VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU
- ID-Token oder HSM-ID-Token gesichert mit CMAC
- Befugnis = (KVNR Aktenkonto, BefugtenID (TID|KVNR), Gültigkeitszeitraum (opt.)) mit CMAC gesichert
- Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll
- ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll

**Ausgangsdaten:**

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

**Prüfschritte:**

1. prüfen des ID-Tokens
  - a. gemäß A\_24690-\* (Zertifikatsprofil C.FD.SIG)  
oder prüfen des HSM-ID-Tokens
  - b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung
    - i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
2. Prüfen der Befugnis
  - a. prüfen des CMAC der Befugnis mittels VAU-HSM Regel hsm-r1
    - i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
  - b. prüfen, ob ~~die Nutzer~~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-~~Token~~Tokenbzw. im

Regel	Beschreibung
	<p>HSM-ID-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>Diese Regel wird für die Anmeldung des <b>E-Rezept-Fachdienstes</b> verwendet.</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU</li> <li>• ID-Token oder HSM-ID-Token gesichert mit CMAC</li> <li>• KVNR (Aktenkonten-ID)</li> <li>• Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> <li>• ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys</li> <li>• ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys</li> </ul> <p><b>Prüfschritte:</b></p> <ol style="list-style-type: none"> <li>1. Prüfen des ID-Tokens <ol style="list-style-type: none"> <li>a. prüfen der <del>Signatur gemäß</del> <u>Signaturgemäß</u> A_25042-* (C.FD.AUT)</li> <li>b. prüfen, ob die professionOID im Zertifikat C.FD.AUT gleich <code>oid_erp-vau</code> ist</li> <li>c. prüfen des ID-Tokens gemäß A_24658-* oder prüfen des HSM-ID-Tokens</li> <li>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"> <li>i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>e. prüfen, ob die professionOID im HSM-ID-Token <code>oid_erp-vau</code> ist</li> </ol> </li> <li>2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel <code>hsm-r2</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR aus dem ID-Token bzw. dem HSM-ID-Token und dem Label für den Datenpersistierungs-Masterkey zur Ableitung des Datenpersistierungsschlüssels aufgerufen. <ol style="list-style-type: none"> <li>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</li> </ol> </li> <li>3. Das Befugnisverifikations-Modul liefert den abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.</li> </ol>

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 <a href="#">33.6- Umschlüsselung und Überschlüsselung</a>). Dabei kann es auch zu einer Umschlüsselung einer älteren Überschlüsselung kommen.</p> <p>Sei &lt;current&gt; 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 "&lt;current&gt;" durch ein selbstgewählten Symbolnamen zu ersetzen.)</p> <p><b>Eingangsdaten:</b></p> <ul style="list-style-type: none"> <li>• VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder ggf. einer dedizierten Überschlüsselungs-VAU</li> <li>• KVNR (Aktenkonten-ID)</li> <li>• Labelliste: nicht leere Liste von Label-n von Überschlüsselungs-Masterkeys (im Regelfall enthält die Liste mindestens "&lt;current&gt;" als Element)</li> </ul> <p><b>Ausgangsdaten:</b></p> <ul style="list-style-type: none"> <li>• Liste von Paaren: versichertenindividueller Überschlüsselungsschlüssel (Secure Data Storage Key), Label für verwendeten Überschlüsselungs-Masterkey</li> </ul> <p>(Hinweis: Die Liste enthält mindestens ein Element -- im Fall der ersten Überschlüsselung in Intervall 2 (vgl. Abschnitt <a href="#">33.6</a> ))</p> <p><b>Ablauf:</b></p> <p>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 "&lt;current&gt;" durch das Label des jüngsten Überschlüsselungs-Masterkeys vor Abarbeitung ersetzt.</p> <p>In der Ergebnisse (siehe Ausgangsdaten) ist "&lt;current&gt;" ebenfalls so ersetzt. Die Reihenfolge in der Eingangsliste muss in der Ausgabeliste gleich bleiben.</p>

2126

## 2127 3.5 Vertrauenswürdige Ausführungsumgebung (VAU)

2128 Eine Vertrauenswürdige Ausführungsumgebung (VAU) gewährleistet mit technischen  
 2129 Maßnahmen, dass Daten serverseitig im ePA-Aktensystem im Klartext verarbeitet werden  
 2130 können, ohne dass einzelne Mitarbeiter des Betreibers auf diese Daten zugreifen können.

2131 Die Datenverarbeitungen der Aktenkontoverwaltung müssen in einer VAU ausgeführt  
2132 werden. Diese VAU wird im folgenden als Aktenkontoverwaltungs-VAU bezeichnet. Des  
2133 weiteren kann das Befugnisverifikations-Modul in einer VAU ausgeführt werden. Diese  
2134 VAU wird im folgenden als Befugnisverifikations-VAU bezeichnet.

#### 2135 **A\_25716-01 - ePA-Aktensystem - Services ausschließlich in der VAU**

2136 Das ePA-Aktensystem MUSS sicherstellen, dass die folgenden Services ausschließlich  
2137 innerhalb einer VAU ausgeführt werden können und ein Zugriff auf die Schnittstellen  
2138 ausschließlich über einen VAU-Kanal erfolgen kann:

- 2139 • Consent Decision Management Service
- 2140 • Entitlement Management
- 2141 • Constraint Management
- 2142 • Device Management
- 2143 • E-Mail Management
- 2144 • Audit Event Service
- 2145 • Authorization Service
- 2146 • Health Record Relocation Service
- 2147 • alle Medical Services
- 2148 • Data Submission Service.

2149 [**<=**]

2150 In den folgenden Abschnitten werden zunächst die Anforderungen an eine VAU  
2151 beschrieben, die sowohl von einer Aktenkontoverwaltungs-VAU als auch  
2152 einer Befugnisverifikations-VAU zu erfüllen sind. Die speziellen Anforderungen an eine  
2153 Aktenkontoverwaltungs-VAU bzw. an eine Befugnisverifikations-VAU folgen darauf in  
2154 separaten Abschnitten.

### 2155 **3.5.1 Übergreifende VAU-Anforderungen**

#### 2156 **3.5.1.1 Schutz der Integrität der VAU**

2157 Die folgenden Anforderungen stellen die Integrität der VAU sicher.

##### 2158 **A\_24613 - ePA-Aktensystem - Bildung Hashwertrepräsentation des VAU-** 2159 **Images**

2160 Der Hersteller des VAU-Images MUSS für seine zugelassenen VAU-Images  
2161 Hashwertrepräsentationen bilden. Diese MÜSSEN signiert und die signierten  
2162 Hashwertrepräsentationen an die gematik übermitteln. Dabei SOLLEN bezüglich der  
2163 kryptographischen Vorgaben zur Signatur die Vorgaben aus [gemSpec\_Krypt]  
2164 eingehalten werden. [**<=**]

2165 Erläuterung zu A\_24613-\*:

2166 Bei Intel-SGX sind die durch die Intel-Hardware erzeugten Signaturen RSA-3072-Bit-  
2167 Signaturen, bei denen der öffentliche Exponent 3 ist. Dies entspricht nicht den Vorgaben  
2168 in [gemSpec\_Krypt] für allgemeine RSA-Signaturen (also nicht im SGX-Kontext). Deshalb  
2169 steht in A\_24613-\* diesbezüglich nur eine SOLL-Formulierung. Im Kontext SGX ist der  
2170 öffentliche RSA-Exponent 3 zulässig.

##### 2171 **A\_24642 - ePA-Aktensystem - Ausschluss von Manipulationen an der Hardware** 2172 **der VAU**



2173 Die VAU MUSS die Integrität der eingesetzten Hardware schützen und damit  
2174 insbesondere Manipulationen an der Hardware durch den Betreiber des ePA-  
2175 Aktensystems ausschließen. [≤]

2176 **A\_24616 - ePA-Aktensystem - Attestierung des VAU-Images und der VAU-**  
2177 **Hardware beim Start**

2178 Das ePA-Aktensystem MUSS beim Start einer VAU das genutzte VAU-Image sowie die  
2179 VAU-Hardware, auf der die VAU ausgeführt werden soll, kryptographisch attestieren und  
2180 ein signiertes VAU-Attestierungstoken erzeugen, welches vom VAU-HSM geprüft werden  
2181 kann. [≤]

2182 **A\_24684 - ePA-Aktensystem - Hardwarebasierter Vertrauensanker für**  
2183 **Attestierung der VAU**

2184 Das ePA-Aktensystem MUSS sicherstellen, dass der kryptographische Vertrauensanker  
2185 für die Attestierung des VAU-Images und der VAU-Hardware in einem hardwarebasierten  
2186 sicheren Schlüsselspeicher gesichert ist. [≤]

2187 **A\_24617 - ePA-Aktensystem - Betreiberunabhängiger Vertrauensanker für**  
2188 **Attestierung der VAU**

2189 Das ePA-Aktensystem MUSS sicherstellen, dass der kryptographische Vertrauensanker  
2190 für die Attestierung des VAU-Images und der VAU-Hardware nicht in der Hoheit des  
2191 Betreibers des Aktensystems liegt. [≤]

2192 *Hinweis zu A\_24617: Mit der Anforderung soll die Bedrohung abgewehrt werden, dass*  
2193 *sich einzelne Innentäter beim Betreiber des ePA-Aktensystems eigene VAU-Software oder*  
2194 *VAU-Hardware mit Schwachstellen erstellen und sich für diese einen falschen Hashwert*  
2195 *attestieren, der dem VAU-HSM bekannt ist.*

2196 **A\_24620 - ePA-Aktensystem - Attestierung durch Systeme außerhalb der VAU**  
2197 **zur Laufzeit**

2198 Das ePA-Aktensystem MUSS technisch ermöglichen, dass Änderungen an der VAU-  
2199 Software und der VAU-Hardware während der Laufzeit durch Systeme außerhalb der VAU  
2200 automatisiert geprüft werden können. [≤]

2201 *Hinweis: Die gematik soll regelmäßig die Integrität der Aktensysteme prüfen können.*

2202 **3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU**

2203 Die folgenden Anforderungen der VAU stellen sicher, dass die innerhalb der VAU  
2204 verarbeiteten Daten technisch geschützt werden.

2205 **A\_24621 - ePA-Aktensystem - Äußere Isolation der VAU von**  
2206 **Datenverarbeitungsprozessen des Betreibers**

2207 Die VAU MUSS die in ihr ablaufenden Datenverarbeitungsprozesse von allen sonstigen  
2208 Datenverarbeitungsprozessen des Betreibers technisch trennen und damit gewährleisten,  
2209 dass der einzelne Mitarbeiter des Betreibers vom Zugriff auf die in der VAU verarbeiteten  
2210 Daten technisch ausgeschlossen ist. [≤]

2211 **A\_24638 - ePA-Aktensystem - Schutz der Daten vor physischem Zugang zu**  
2212 **Systemen der VAU**

2213 Die VAU MUSS mit technischen Mitteln sicherstellen, dass bei einem physischen Zugang  
2214 zu Hardware-Komponenten der VAU keine Daten aus der VAU extrahiert oder manipuliert  
2215 werden können. [≤]

2216 **A\_24651 - ePA-Aktensystem - Betreiber ergreift Maßnahmen gegen physische**  
2217 **Angriffe auf die VAU**

2218 Der Betreiber des ePA-Aktensystems MUSS mit technischen und/oder organisatorischen  
2219 Maßnahmen ausschließen, dass ein einzelner Innentäter beim Betreiber des ePA-  
2220 Aktensystems physische Angriffe auf eine VAU ausführen kann. [≤]

2221 **A\_24641 - ePA-Aktensystem - Löschen aller Daten beim Beenden einer VAU-**  
2222 **Instanz**

2223 Das ePA-Aktensystem MUSS sicherstellen, dass beim Beenden einer VAU-Instanz  
2224 sämtliche Daten dieser VAU-Instanz aus flüchtigen Speichern sicher gelöscht werden  
2225 oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [ <= ]

2226 **A\_25244 - ePA-Aktensystem - x-insurantId nicht außerhalb des VAU-Kanals**

2227 Das ePA-Aktensystem MUSS sicherstellen, dass das HTTP Header-Element mit dem  
2228 Namen "x-insurantId" nicht außerhalb des VAU-Kanals gesendet wird. [ <= ]

2229 **3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU**

2230 **A\_26314 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**  
2231 **gespeicherten Daten**

2232 Das ePA-Aktensystem MUSS sicherstellen, dass eine VAU-Daten, die im System des  
2233 Aktensystembetreibers gespeichert werden sollen und für die keine spezifischen  
2234 Anforderungen zum Schutz der gespeicherten Daten existieren, ausschließlich  
2235 verschlüsselt gespeichert werden und der verwendete Verschlüsselungsschlüssel mittels  
2236 der Regel hsm-r8 vom VAU-HSM abgeleitet wird. [ <= ]

2237 Hinweise zu A\_26314:

- 2238 • Spezifische Anforderungen zum Schutz der gespeicherten Daten gibt es z.B. für  
2239 die Aktenkontoverwaltungs-VAU in Abschnitt 3.5.2.2 und die durch die VAU für  
2240 den Betrieb erstellten Protokolle in Abschnitt 3.5.1.5.
- 2241 • Außerhalb der VAU verschlüsselt gespeicherte Daten der ePA3.0, die bisher nicht  
2242 mit Regel hsm-r8 verschlüsselt sein konnten, sind beim Öffnen der Akte  
2243 umzuschlüsseln und mit einem Schlüssel zu sichern, der mit Regel hsm-r8  
2244 abgeleitet wird. Eine Umschlüsselung ohne Öffnen der Akte ist nicht erforderlich.

2245 **A\_26322 - ePA-Aktensystem - Unterschiedliche Schlüssel für die**  
2246 **Verschlüsselung von außerhalb der VAU gespeicherten Daten bei**  
2247 **unterschiedlichen Verarbeitungszwecken**

2248 Falls Daten außerhalb der VAU im System des Aktensystembetreibers gespeichert  
2249 werden, MUSS das ePA-Aktensystem sicherstellen, dass für die Verschlüsselung von  
2250 Daten, die zu unterschiedlichen Zwecken verarbeitet werden, unterschiedliche  
2251 Verschlüsselungsschlüssel genutzt werden. [ <= ]

2252 Hinweis zu A\_26322: Verarbeitungszwecke für Daten ~~sind beispielsweise die~~  
2253 ~~Verarbeitung von Daten zum Zwecke der Sekundärnutzung (siehe Data Submission~~  
2254 ~~Service) oder ist beispielsweise~~ die Verarbeitung von Daten für die Nutzerverwaltung im  
2255 Aktensystem (insbesondere Geräteinformationen und E-Mail-Adressen).

2256 **3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM**

2257 **A\_24653 - ePA-Aktensystem - Sichere Verbindung zwischen VAU und VAU-HSM**

2258 Das ePA-Aktensystem MUSS technisch sicherstellen, dass zwischen einer VAU und einem  
2259 VAU-HSM eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die  
2260 vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des  
2261 Betreibers des Aktensystems schützen. [ <= ]

2262 **3.5.1.5 Logging und Monitoring**

2263 Hinweis: Die Anforderungen dieses Abschnitts könnten sich noch ändern, falls sich bei  
2264 der Umsetzung des ePA-Aktensystems herausstellt, dass weitere Protokollierungen auf  
2265 Seiten des Betreibers notwendig werden.

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

#### **A\_24910 - ePA-Aktensystem - Erlaubte Zwecke der Betreiberprotokolle**

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

#### **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 - ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen innerhalb einer VAU-Instanz**

Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus ausschließen, dass sich innerhalb einer VAU-Instanz die Verarbeitungen eines Health Record Context oder einer User Session schadhaft auf die Verarbeitungen eines anderen Health Record Context oder einer anderen User Session auswirken können. [ $\leq$ ]

Hinweis zu A\_24636-\*: Die Anforderung schließt eine Umsetzung mit Server-Threads, Worker und Ähnlichem nicht grundsätzlich aus, sofern die Sicherheitsleistung der Separation erbracht werden kann.

##### **A\_24885 - ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen unterschiedlicher VAU-Instanzen**

Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der unabhängig vom Separationsmechanismus in A\_24636-\* ist, ausschließen, dass sich Verarbeitungen in einer VAU-Instanz schadhaft auf die Verarbeitungen einer anderen VAU-Instanz auswirken können. [ $\leq$ ]

##### **A\_24637 - ePA-Aktensystem - Maximale Health Record Context in einer VAU-Instanz**

Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Health Record Context gleichzeitig in einer VAU-Instanz laufen können. [ $\leq$ ]

##### **A\_25028 - ePA-Aktensystem - Keine Kommunikation zwischen Aktenkontoverwaltungs-VAUs**

2361 Das ePA-Aktensystem MUSS sicherstellen, dass es keine direkte Kommunikation  
2362 zwischen VAU-Instanzen von Aktenkontoverwaltungs-VAUs gibt. [≤]

2363 **A\_26111 - ePA-Aktensystem - Keine Kommunikation zwischen Health Record**  
2364 **Contexts**

2365 Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer  
2366 Aktenkontoverwaltungs-VAU-Instanz keine Kommunikation zwischen Health Record  
2367 Contexts gibt. [≤]

2368 **A\_24639 - ePA-Aktensystem - Löschen aller Daten beim Beenden eines Health**  
2369 **Record Context**

2370 Die VAU MUSS sicherstellen, dass beim Beenden eines Health Record Context sämtliche  
2371 Daten dieses Health Record Context aus flüchtigen Speichern sicher gelöscht werden  
2372 oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [≤]

2373 **A\_24640 - ePA-Aktensystem - Löschen aller Daten beim Beenden einer User**  
2374 **Session**

2375 Die VAU MUSS sicherstellen, dass beim Beenden einer User Session sämtliche Daten  
2376 dieser User Session aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf  
2377 diese Daten technisch ausgeschlossen ist. [≤]

2378 *Hinweis zu A\_24639-\*, A\_24640-\* und A\_24648-\*: Eine zeitliche Verzögerung des*  
2379 *Löschens ist tolerabel, sofern ein sofortiges Löschen aufgrund der Architektur des*  
2380 *Aktensystemherstellers aus Performanzgründen nicht sinnvoll ist. In diesem Fall ist ein*  
2381 *geeigneter Kompromiss zwischen dem Löschezitpunkt und der Performanz zu wählen.*

2382 **A\_25231 - ePA-Aktensystem - Schließen des Health Record Context beim**  
2383 **Beenden einer User Session**

2384 Die VAU MUSS sicherstellen, dass beim Beenden einer User Session alle mit dieser User  
2385 Session verknüpften Health Record Context beendet werden, wenn der jeweilige Health  
2386 Record Context nicht mit mindestens einer weiteren User Session verknüpft ist. [≤]

2387 **A\_25051 - ePA-Aktensystem - VAU-Kanal endet immer in einer**  
2388 **Aktenkontoverwaltungs-VAU**

2389 Die VAU MUSS sicherstellen, dass ein VAU-Kanal von einem Client der ePA (ePA-Client  
2390 oder ePA-FdV) ausschließlich in einer Aktenkontoverwaltungs-VAU endet. [≤]

2391 Hinweis: Der VAU-Kanal darf z.B. nicht in einer Befugnisverifikations-VAU enden.

2392 **3.5.2.2 Schutz der Daten bei Speicherung außerhalb der**  
2393 **Aktenkontoverwaltungs-VAU**

2394 Die folgenden Anforderungen gewährleisten den Schutz der beim Betreiber des ePA-  
2395 Aktensystems persistierten Daten von Aktenkonten. Die Verschlüsselung der Daten eines  
2396 Versicherten erfolgt mit seinem versichertenindividuellen Daten- und  
2397 Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel sind  
2398 in [gemSpec\_Krypt#3.15.2] festgelegt.

2399 **A\_24643 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**  
2400 **gespeicherten Daten mit dem Datenpersistierungsschlüssel**

2401 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten

- 2402 1. Daten des FHIR-Data Service
- 2403 2. Daten des XDS Document Service
- 2404 3. Daten des Audit Event Service (Protokolle für den Versicherten zum Zwecke der
- 2405 Datenschutzkontrolle)
- 2406 4. Daten des Constraint Managements (Policies zu verborgenen Daten)



2407 5. Daten des Consent Managements (Widersprüche des Versicherten)  
2408 vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb  
2409 des Health Record Context mit dem zum Health Record gehörenden  
2410 versichertenindividuellen Datenpersistierungsschlüssel verschlüsselt werden.  
2411 [ $\leq$ ]

2412 **A\_24644 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**  
2413 **gespeicherten Befugnissen mit dem Befugnispersistierungsschlüssel**  
2414 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten  
2415 Daten des Entitlement Managements, d. h. Befugnisse und Befugnisverbote, vor der  
2416 Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health  
2417 Record Context mit dem zum Health Record gehörenden versichertenindividuellen  
2418 Befugnispersistierungsschlüssel verschlüsselt werden. [ $\leq$ ]

2419

### 2420 3.5.2.3 Konsistenz des Systemzustands

2421 **A\_24650 - ePA-Aktensystem - Konsistenter Systemzustand eines Health Record**  
2422 **Context**  
2423 Die VAU MUSS sicherstellen, dass ein konsistenter Zustand eines Health Record Context  
2424 auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw.  
2425 wiederhergestellt werden kann. [ $\leq$ ]

2426 **A\_24696 - ePA-Aktensystem - Konsistenz bei parallelen Zugriffen**  
2427 Die VAU MUSS auch bei parallelen Zugriffen auf dasselbe Aktenkonto durch mehrere  
2428 Nutzer immer einen konsistenten Zustand des Aktenkontos gewährleisten. [ $\leq$ ]

### 2429 3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations- 2430 VAU

2431 Eine Befugnisverifikations-VAU ist eine spezielle VAU, in der ausschließlich das  
2432 Befugnisverifikations-Modul ausgeführt wird.

2433 **A\_24646 - ePA-Aktensystem - Befugnisverifikations-VAU verarbeitet**  
2434 **ausschließlich ein Befugnisverifikations-Modul**  
2435 Das ePA-Aktensystem MUSS sicherstellen, dass in einer Befugnisverifikations-VAU  
2436 ausschließlich ein Befugnisverifikations-Modul ausgeführt wird. [ $\leq$ ]

2437 **A\_24647 - ePA-Aktensystem - Befugnisverifikations-VAU speichert keine Daten**  
2438 Eine Befugnisverifikations-VAU DARF die Daten, die sie im Rahmen der Regeln des  
2439 Befugnisverifikations-Moduls verarbeitet, NICHT außerhalb der Befugnisverifikations-VAU  
2440 speichern. [ $\leq$ ]

2441 Eine Befugnisverifikations-VAU darf insbesondere die vom VAU-HSM abgeleiteten  
2442 versichertenindividuellen Persistierungsschlüssel nicht speichern.

2443 **A\_24648 - ePA-Aktensystem - Befugnisverifikations-VAU löscht Daten nach**  
2444 **Regelbearbeitung**  
2445 Eine Befugnisverifikations-VAU MUSS sämtliche Daten, die sie im Rahmen eines  
2446 Regelaufrufs des Befugnisverifikations-Moduls verarbeitet, sofort nach Abarbeitung der  
2447 Regel sicher aus der Befugnisverifikations-VAU löschen bzw. einen Zugriff auf diese  
2448 Daten technisch ausschließen. [ $\leq$ ]

2449 **A\_24671 - ePA-Aktensystem - Sichere Verbindung zwischen VAU-Instanzen**  
2450 Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer VAU-Instanz einer  
2451 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).

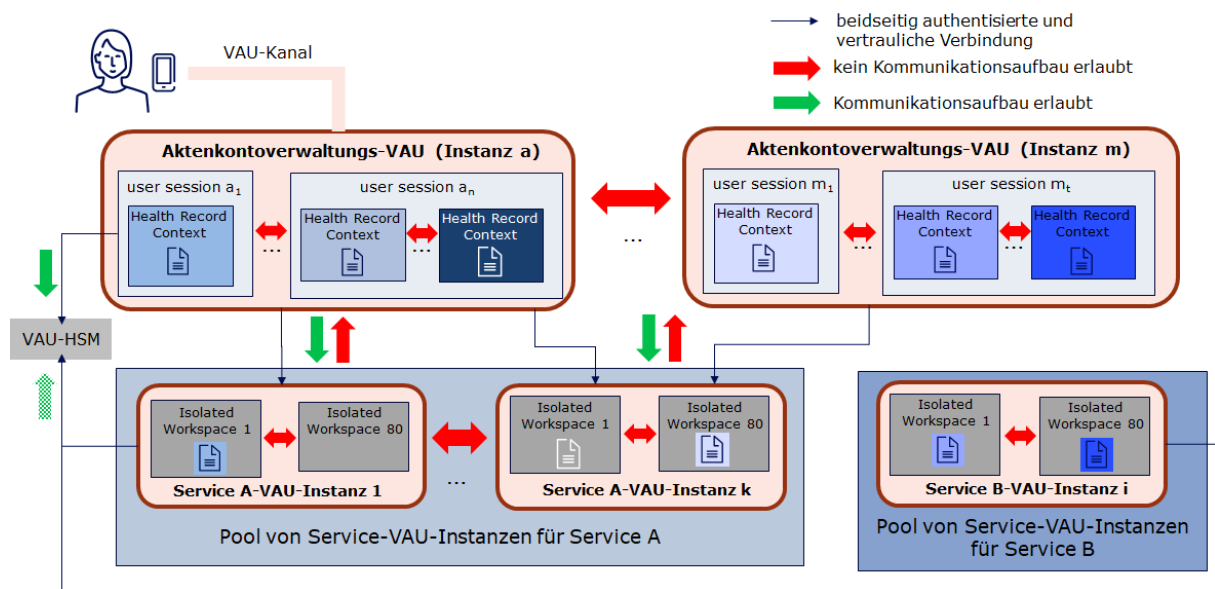


Abbildung 2 - Überblick Service-VAUs

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.



2481 **A\_26112 - ePA-Aktensystem - Maximale Isolated Workspaces in einer Service-**  
2482 **VAU-Instanz**

2483 Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Isolated Workspaces  
2484 gleichzeitig in einer Service-VAU-Instanz laufen können. [ <= ]

2485 **A\_26113 - ePA-Aktensystem - Isolation zwischen Isolated Workspaces**  
2486 **innerhalb einer Service-VAU-Instanz**

2487 Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus  
2488 ausschließen, dass sich innerhalb einer Service-VAU-Instanz die Verarbeitungen eines  
2489 Isolated Workspaces schadhaft auf die Verarbeitungen eines anderen Isolated  
2490 Workspaces auswirken können. [ <= ]

2491 **A\_26114 - ePA-Aktensystem - Isolation zwischen unterschiedlichen Service-**  
2492 **VAU-Instanzen**

2493 Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der  
2494 unabhängig vom Separationsmechanismus in A\_26113-\* ist, ausschließen, dass sich  
2495 Verarbeitungen in einer Service-VAU-Instanz schadhaft auf die Verarbeitungen einer  
2496 anderen Service-VAU-Instanz auswirken können. [ <= ]

2497 **A\_26115 - ePA-Aktensystem - Isolated Workspace verarbeitet maximal einen**  
2498 **Request einer AK-VAU**

2499 Nachdem ein Isolated-Workspace einen (1) Service-Request einer  
2500 Aktenkontoverwaltungs-VAU-Instanz verarbeitet hat, MUSS das ePA-Aktensystem  
2501 sicherstellen, dass alle Daten des Isolated-Workspaces sicher gelöscht werden, um den  
2502 Isolated-Workspace für nachfolgende Service-Requests wieder neu zu initialisieren. [ <= ]

2503 **A\_26116 - ePA-Aktensystem - In einem Isolated Workspace sind zu einem**  
2504 **Zeitpunkt nur Daten eines Versicherten**

2505 Das ePA-Aktensystem MUSS sicherstellen, dass in einem Isolated Workspace zu einem  
2506 Zeitpunkt ausschließlich Daten eines Versicherten verarbeitet werden können, sofern die  
2507 Auswahl der zu verarbeitenden Daten durch die Logik im ePA-Aktensystem bestimmt  
2508 wird. [ <= ]

2509 Hinweis zu A\_26116-\*: Falls Nutzer die Daten für die Service-VAU auswählen, ohne dass  
2510 das ePA-Aktensystem auf diese Daten Einfluss hat (z.B. Nutzer wählt zu konvertierende  
2511 PDF-Dokumente im ePA-FdV aus) kann es dazu kommen, dass zu einem Zeitpunkt auch  
2512 Daten mehrerer Versicherter in einem Isolated Workspace verarbeitet werden.

2513 **A\_26117 - ePA-Aktensystem - Keine Kommunikation zwischen Isolated**  
2514 **Workspaces**

2515 Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer Service-VAU-Instanz  
2516 keine Kommunikation zwischen Isolated Workspaces gibt. [ <= ]

2517 **A\_26118 - ePA-Aktensystem - Keine Kommunikation zwischen Service-VAU**

2518 Das ePA-Aktensystem MUSS sicherstellen, dass es keine Kommunikation zwischen  
2519 Instanzen von Service-VAUs gibt. [ <= ]

2520 **A\_26119 - ePA-Aktensystem - Service-VAUs speichern keine Daten in**  
2521 **Aktenkonten**

2522 Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine Daten in  
2523 einem Aktenkonto eines Versicherten persistieren. [ <= ]

2524 **A\_26120 - ePA-Aktensystem - Service-VAUs verarbeiten keine Identitätstoken**

2525 Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine  
2526 Identitätstoken von Nutzern verarbeiten. [ <= ]

2527 **A\_26123 - ePA-Aktensystem - Service-VAU-Instanzen haben maximale**  
2528 **Lebensdauer**

2529 Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen nach einer  
2530 definierten Lebensdauer (abhängig von der Funktionalität der Services) keine neuen  
2531 Service-Requests mehr annehmen können und, nachdem die laufenden Requests  
2532 abgearbeitet wurden, beendet und neu gestartet werden.[<=]

2533 **A\_26124 - ePA-Aktensystem - Information über neuen Service-VAU-Typ**

2534 Der Hersteller des ePA-Aktensystems MUSS die gematik über die Absicht der Einführung  
2535 eines neuen Service-VAU-Typs informieren und ggf. für diesen neuen Service-VAU-Typ zu  
2536 erfüllende Rahmenbedingungen abstimmen.[<=]

2537 Hinweis zu A\_26124-\*: Hierzu gehört z.B. auch die Festlegung der maximalen  
2538 Lebensdauer für den neuen Service-VAU-Typ (siehe A\_26123-\*).

2539 **A\_26125 - ePA-Aktensystem - Starten ausschließlich attestierter Service-VAUs**

2540 Das ePA-Aktensystem MUSS sicherstellen, dass ausschließlich attestierte Service-VAU-  
2541 Instanzen gestartet werden können.[<=]

2542 **3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU**

2543 **A\_26126 - ePA-Aktensystem - Gesicherte und authentifizierte Verbindung**  
2544 **zwischen AK-VAU- und Service-VAU-Instanzen**

2545 Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer Aktenkontoverwaltungs-  
2546 VAU-Instanz und einer Service-VAU-Instanz eine beidseitig authentifizierte und  
2547 vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe  
2548 durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen.[<=]

2549 **A\_26127 - ePA-Aktensystem - Kein Kommunikationsaufbau von Service-VAU-**  
2550 **Instanzen zu AK-VAU-Instanzen**

2551 Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine  
2552 Kommunikation zu einer AK-VAU-Instanz aufbauen kann.[<=]

2553 **A\_26128 - ePA-Aktensystem - Kein Aufruf von Schnittstellen von AK-VAU-**  
2554 **Instanzen durch Service-VAU-Instanzen**

2555 Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine  
2556 Schnittstellen/Services aufrufen kann, die in einer AK-VAU-Instanz ausgeführt  
2557 werden.[<=]

2558 **3.6 Umschlüsselung und Überschlüsselung**

2559 Das Kerckhoffs'sche Prinzip von 1883 ist ein Grundpfeiler der Kryptographie. Es besagt u.  
2560 a. dass die Sicherheit von kryptographischen Verfahren alleinig von der Geheimhaltung  
2561 der Schlüssel abhängen darf, und dass Schlüssel leicht auswechselbar sein müssen. Damit  
2562 kryptographische Schlüssel in der Praxis ihre Sicherheitseigenschaft behalten können  
2563 müssen sie einen Lebenszyklus besitzen (vgl. bspw. [NIST-SP-800-57P1]), der den  
2564 regelmäßigen Austausch (Wechsel) der Schlüssel vorsieht und umsetzt. Jährlich werden  
2565 aus diesem Grunde die Masterkey für Akten Daten und die Masterkey für Befugnisse  
2566 erneuert (vgl. A\_15745-\* und A\_20519-\* (beide aus [gemSpec\_Krypt])). Bei dieser  
2567 Erneuerung muss eine Umschlüsselung durchgeführt werden:

- 2568
- Schlüssel\_alt\_KVNR = Ableitung (MK\_alt, KVNR),
  - 2569 • Schlüssel\_neu\_KVNR = Ableitung (MK\_neu, KVNR),
  - 2570 • Umschlüsselung pro Akte: Schlüssel\_alt\_KVNR -> Schlüssel\_neu\_KVNR.

2571 Falls eine AK-VAU Zugriff auf eine Akte besitzt und zu diesem Zeitpunkt feststellt neue  
2572 Masterkeys (vgl. betreiberspezifische Schlüssel A\_15745-\*) existieren, muss sie eine

2573 Umschlüsselung durchführen (A\_20519-\*). Falls eine Akte länger nicht verwendet wird,  
2574 kann eine AK-VAU keinen Zugang zu den Klartexten der Akte erhalten, da sie nur nach  
2575 erfolgreicher Nutzerauthentisierung vom VAU-HSM die aktenspezifischen  
2576 Ableitungsschlüssel erhält. Dann kann eine AK-VAU zunächst auch keine Umschlüsselung  
2577 vornehmen. Aus diesem Grunde muss eine VAU (entweder eine AK-VAU oder eine  
2578 dedizierte Überschlüsselungs-VAU) eine Überschlüsselung der Chiffre der Akte  
2579 vornehmen. Dafür werden Überschlüsselungsschlüssel benötigt. Es gibt analog zu den  
2580 anderen betreiberspezifischen Schlüssel (A\_15745-\*) Masterkeys für eine  
2581 Schlüsselableitung für die Überschlüsselung der Chiffre einer Akte.

2582 **A\_26197 - ePA-Aktensystem - betreiberspezifische Schlüssel:**  
2583 **Überschlüsselungs-Masterkeys**

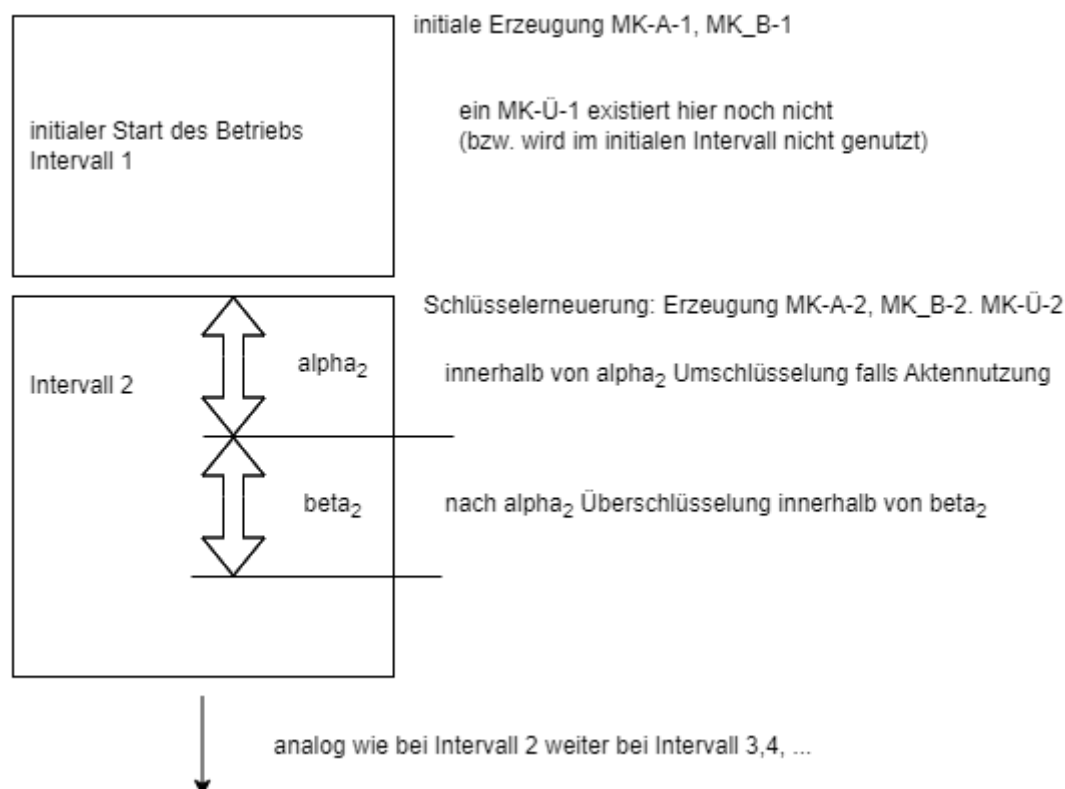
2584 Ein ePA-Aktensystem MUSS sicherstellen, dass die Menge der betreiberspezifischen  
2585 Schlüssel aus [gemSpec\_Krypt#A\_15745-\*] um die Kategorie Überschlüsselungs-  
2586 Masterkeys erweitert wird. Für die Überschlüsselungsschlüssel MÜSSEN die gleichen  
2587 Vorgaben wie für alle betreiberspezifischen Schlüssel gemäß A\_15745-\* gelten.  
2588 Die betreiberspezifischen Schlüssel werden mindestens jährlich aktualisiert (A\_20519-\*),  
2589 die alten Schlüssel MÜSSEN solange im VAU-HSM verfügbar sein, solange Chiffre im  
2590 Aktensystem existieren (bspw. Daten einer Akte), die mit diesen Schlüsseln  
2591 kryptographisch gesichert sind. [ <= ]

2592 D. h. wie in Abschnitt 3.3.3 (bspw. A\_24611-\*) definiert, gibt es bei den Masterkeys drei  
2593 Kategorien: (1) Aktenpersistierung, (2) Befugnispersistierung und (3) Überschlüsselung.  
2594 Initial startet der Betrieb eines Aktensystems mit je einem Schlüssel in den ersten zwei  
2595 Kategorien. Nach maximal einem Jahr (A\_20519-\*), oder anders formuliert im nächsten  
2596 Intervall, werden diese beiden ersten Schlüssel zufällig neu erzeugt. Dabei muss nun ein  
2597 neuer Überschlüsselungsmasterkey erzeugt werden. Die Anzahl der Schlüssel nach o. g.  
2598 Kategorie ist anschließend (1) 2, (2) 2, (3) 1.

2599 **A\_26198 - ePA-Aktensystem - neuer Überschlüsselungsschlüssel bei**  
2600 **Erneuerung betreiberspezifischen Schlüssel**

2601 Ein ePA-Aktensystem MUSS sicherstellen, dass bei jeder Erneuerung der Masterkeys zur  
2602 Aktenpersistierung ein weiterer neuer Überschlüsselungsmasterkey zufällig im VAU-HSM  
2603 erzeugt wird.  
2604 [ <= ]

2605 Bei einer Erneuerung der betreiberspezifischen Schlüssel gibt es verschiedene  
2606 Zeitabschnitte:



**Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung**

#### **A\_26204 - ePA-Aktensystem - zeitliche Vorgaben zur Durchführung der Umschlüsselung und Überschlüsselung**

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

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

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

[<=]

Die folgenden zwei Anforderung geben weitere Details zu A\_26204-\*.

#### **A\_26205 - ePA-Aktensystem - Umschlüsselung**

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

verschlüsselt sind), MÜSSEN im Aktensystem nach erfolgreicher Umschlüsselung gelöscht werden.

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

Hinweis zu A\_26205-\*: Die notwendigen aktenspezifischen Schlüssel liegen nun in der AK-VAU vor. Die Umschlüsselung muss nicht direkt sofort vor Nutzung der Akte erfolgen, sondern kann auch einige Minuten später erfolgen. Die konkrete Ausgestaltung liegt beim Hersteller.

### A\_26206 - ePA-Aktensystem - Überschüsselung

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

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

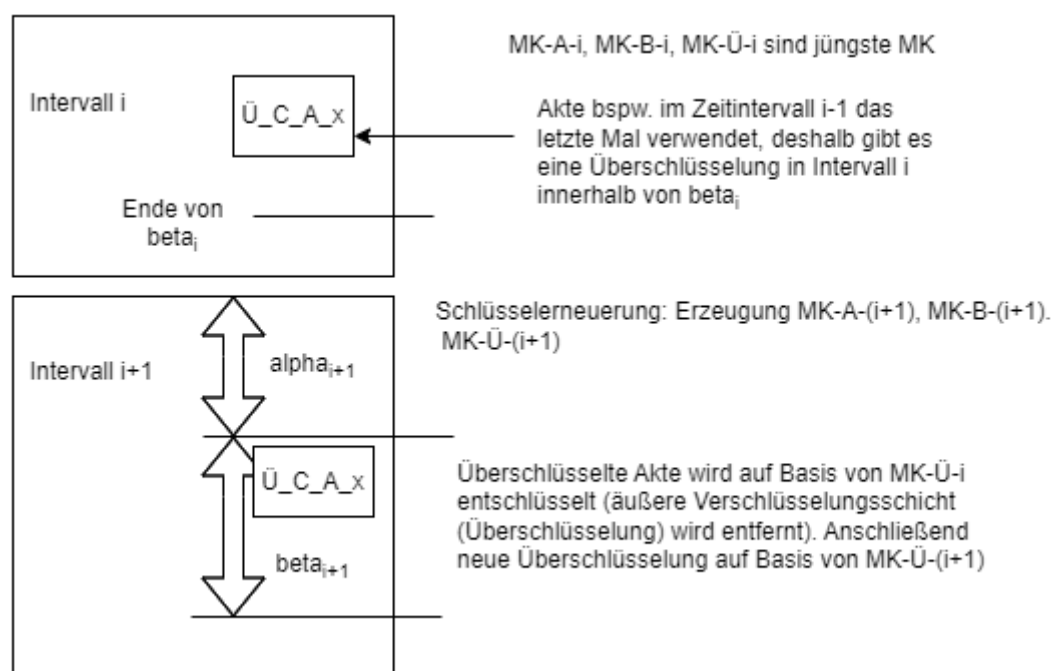


Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer Überschüsselung

2665

**2666 A\_26208 - ePA Aktensystem - Umschlüsselung einer Überschlüsselung**

2667 Ein ePA-Aktensystem MUSS sicherstellen, dass jeweils in einem Intervall innerhalb von  
2668 beta überprüft wird, ob überschlüsselte Akten existieren, deren Überschlüsselung auf  
2669 Basis eines alten Überschlüsselungs-Masterkeys (also aus einem früheren Intervall  
2670 stammend) durchgeführt wurde. Die AK-VAU (oder eine dedizierte Überschlüsselungs-  
2671 VAU) MUSS die überschlüsselten Akten umschlüsseln, d. h. die Überschlüsselung auf  
2672 Grundlage eines älteren Überschlüsselungs-Masterkeys wird aufgehoben (äußeren  
2673 Verschlüsselungsschicht innerhalb der VAU entschlüsselt) und das Ergebnis (= Chiffre  
2674 einer Akte) neu verschlüsselt auf Basis des aktuellen Überschlüsselungs-Masterkeys. Die  
2675 alten Chiffre (also vor der Umschlüsselung der Überschlüsselung) MÜSSEN gelöscht  
2676 werden. Das ePA-Aktensystem MUSS sicherstellen, dass nach Ablauf von beta keine  
2677 überschlüsselten Akten existieren, deren Überschlüsselung auf Basis eines  
2678 Überschlüsselungsschlüssel, der nicht aus dem aktuellen Intervall stammt, durchgeführt  
2679 wurde.

2680 [ $\leq$ ]

2681 Sollte durch irgendeinen Umstand die Sicherheitseigenschaft der Betreiberschlüssel  
2682 (A\_15745-\*) in Frage stehen, so muss ein Aktensystembetreiber die Umschlüsselung  
2683 bzw. die Überschlüsselung aktivieren/starten können.

**2684 A\_26199 - ePA-Aktensystem - Notfall-Aktivierung****2685 Umschlüsselung/Überschlüsselung**

2686 Ein ePA-Aktensystem MUSS sicherstellen, dass das ePA-Aktensystem es einem ePA-  
2687 Betreiber ermöglicht eine Erneuerung der betreiberspezifischen Schlüssel zu  
2688 starten/aktivieren. Es MUSS also dem ePA-Betreiber möglich sein neben der  
2689 regelmäßigen Erneuerung der betreiberspezifischen Schlüssel (A\_205019-\*) eine  
2690 Erneuerung zu initiieren.

2691 [ $\leq$ ]

2692 Nach A\_20519-\* muss es mindestens jährlich eine Schlüsselerneuerung geben. Mit  
2693 26199-\* kann ein ePA-Betreiber im Notfall sozusagen den Zyklus "beschleunigen" -- ein  
2694 neues Intervall sofort einleiten/erzeugen.

2695 Da die Chiffre in einem ePA-Aktensystem mit Verschlüsselungsschlüsseln, die aus  
2696 unterschiedlichen Masterkeys (aus unterschiedlichen Intervallen) abgeleitet werden,  
2697 erzeugt werden können, muss an den äußeren Meta-Daten eines Chiffres ersichtlich sein  
2698 auf welchem Masterkeys sie basieren (vom welchem Masterkey sind sie abgeleitet sind).

**2699 A\_26223 - ePA-Aktensystem - Metadaten von ePA-spezifischen Chiffren**

2700 Ein ePA-Aktensystem MUSS sicherstellen, dass bei ePA-spezifischen Daten  
2701 (Datenpersistierung von Akten, überschlüsselte Aktenchiffre, verschlüsselte Befugnisse  
2702 etc.) an den äußeren (also unverschlüsselten) Meta-Daten des Chiffres erkennbar ist  
2703 mithilfe welches (oder welcher) Masterkeys die Chiffre entschlüsselbar sind. [ $\leq$ ]

**2704 3.7 User Session und Health Record Context**

2705 Die Verarbeitungen innerhalb einer VAU werden über User Sessions und Health Record  
2706 Contexts voneinander getrennt.

2707 Wenn ein ePA-Client einen VAU-Kanal zum Aktensystem aufbaut, wird dieser einer  
2708 bestimmten VAU-Instanz zugeordnet, in welcher dann eine User Session für den Nutzer  
2709 des ePA-Clients erzeugt wird. Nach erfolgreicher Authentifizierung des Nutzers unter  
2710 Verwendung des sektoralen IDPs (Versicherte) oder des IDP-Dienstes (LEI) ist die User  
2711 Session etabliert und kann durch den ePA-Client genutzt werden. Alle Verbindungen für



2712 diesen VAU-Kanal werden immer an dieselbe VAU-Instanz geleitet, die die User Session  
2713 verwaltet. Eine VAU-Instanz kann mehrere User Sessions verwalten.

2714 Wird durch den ePA-Client eine Operation für eine bestimmte Akte aufgerufen (Parameter  
2715 x-insurantid) der Operation, wird in der User Session geprüft, ob diese Akte schon  
2716 verwendet wird (ein anderer Nutzer gerade mit der Akte arbeitet) oder nicht. Sollte die  
2717 Akte noch nicht verwendet werden, wird die Akte in einem Health Record Context  
2718 geöffnet und kann durch den ePA-Client in dessen User Session verwendet werden.  
2719 Existiert für die Akte schon ein geöffneter Health Record Context, darf es durch den  
2720 parallelen Zugriff zu keinen Inkonsistenzen in der Akte kommen.

2721 Innerhalb einer VAU-Instanz dürfen nur eine maximale Anzahl von Health Record  
2722 Contexts gleichzeitig aufgebaut sein. Sollte diese Anzahl überschritten werden, wird der  
2723 am längsten nicht genutzte Health Record Context geschlossen, um einen neuen Health  
2724 Record Context öffnen zu können.

### 2725 3.8 Consent Decision Management

2726 Das Consent Decision Management des Aktensystems verwaltet die Entscheidungen eines  
2727 Versicherten oder eines Vertreters für oder gegen die Nutzung von definiert  
2728 widerspruchsfähigen Funktionen gemäß gesetzlicher Vorgaben.

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

Der Widerspruch gegen die grundsätzliche Nutzung der ePA wird nicht im Consent Decision Management berücksichtigt. Die Existenz eines Aktenkontos für einen Versicherten impliziert, dass kein Widerspruch gegen die Nutzung der ePA erteilt wurde. Der Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger wird ebenfalls nicht hier verwaltet (siehe zu beiden Widersprüchen auch 33.1.1- Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte).

### 2740 3.8.1 Widersprüche für Funktionen der ePA

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

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

Die aktuell erteilten Widersprüche können durch einen Versicherten oder einen Vertreter jederzeit über ein ePA-FdV eingesehen und geändert werden. Versicherte und Vertreter, die ein ePA-FdV nicht nutzen möchten, können eine Auskunft über die aktuell erteilten Widersprüche über die Ombudsstelle erhalten und dort auch Änderungen an den Entscheidungen im Aktenkonto veranlassen. Die Ansicht oder Änderung der



- 2756 Widersprüche erfolgt im Aktenkonto stets gesichert innerhalb der VAU, die aktuellen  
 2757 Entscheidungen zu den widerspruchsfähigen Funktionen der ePA sind  
 2758 versichertenindividuell mit dem SecureDataStorageKey verschlüsselt abgelegt.
- 2759 Die Information über relevante erteilte oder nicht erteilte Widersprüche können Clients  
 2760 auf einfache Weise (ohne Authentisierung oder Etablierung eines VAU-Kanals) im Vorfeld  
 2761 einer Operation über den Information Service abfragen (siehe auch [33.15- Information](#)  
 2762 [Service](#) ).
- 2763 Das Consent Decision Management des Aktenkontos spiegelt ("cached") die  
 2764 Entscheidungen zu den Widersprüchen für die schnelle Abfrage über den Information  
 2765 Service in einen Bereich, der ohne den Aufbau eines VAU-Kanals und Verwendung des  
 2766 versichertenindividuellen SecureDataStorageKey nutzbar ist.
- 2767 Das Aktenkonto unterstützt die Durchsetzung eines erteilten Widerspruchs überall dort,  
 2768 wo Aktivitäten dediziert als Teil einer widerspruchsfähigen Funktion zugeordnet werden  
 2769 können. Beispielsweise wird das Einstellen neuer Verordnungs- und Dispensierdaten in  
 2770 die Ordner der Kategorie "medication" immer verhindert, wenn der Teilnahme am digital  
 2771 gestützten Medikationsprozess widersprochen wurde. Die konkreten Auswirkungen eines  
 2772 Widerspruchs sind in den jeweiligen Kapiteln zur Handhabung von Dokumenten und  
 2773 Daten des Aktenkontos dargestellt (siehe [33.13.1- XDS Document Service](#) und [33.13.2-](#)  
 2774 [FHIR Data Services](#) ) .
- 2775 Die jeweils berücksichtigten widerspruchsfähigen Funktionen sind wie folgt definiert.  
 2776 Diese Liste kann in folgenden Versionen der ePA ergänzt oder verändert werden.
- 2777 **AA\_23874-01 - Consent Decision Management - Definition der**  
 2778 **widerspruchsfähigen Funktionen der ePA**  
 2779 Das Consent Decision Management MUSS die Attribute zu widerspruchsfähigen  
 2780 Funktionen der ePA gemäß der folgenden Tabelle verwenden.
- 2781 **Tabelle 10: 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"

2782 **[<=]**

- 2783 *Hinweis: Die Bezeichnungen in () sind die Bezeichnungen in den Schnittstellen für den*  
 2784 *Abruf und die Verwaltung der Widersprüche. Eine widerspruchsfähige Funktion wird durch*  
 2785 *die ID der Funktion eindeutig identifiziert.*

2786 *Hinweis: Die Verwaltung der Widersprüche gegen die Nutzung des Aktenkontos durch*  
2787 *eine spezifische Leistungserbringerinstitution erfolgt über die Befugnisverwaltung (siehe*  
2788 *3.9.4- Befugnisausschluss (Blocked User Policy) ).*

2789 Die Entscheidungen zu den widerspruchsfähigen Funktionen "medication" und "erp-  
2790 submission" sind durch das Aktensystem dabei abhängig assoziiert:

2791 **A\_25300 - Consent Decision Management - Untereinander abhängige**  
2792 **Entscheidungen zu Widersprüchen**

2793 Das Consent Decision Management MUSS durch interne Maßnahmen sicherstellen, dass  
2794 bei Erteilung eines Widerspruchs gegen die Nutzung der Funktion der elektronischen  
2795 Patientenakte 'erp-submission' ('deny') auch der Widerspruch gegen die Nutzung der  
2796 Funktion 'medication' gesetzt wird ('deny') und dass bei der Rücknahme ('permit') des  
2797 Widerspruchs gegen die Nutzung der Funktion 'medication' auch der Widerspruch gegen  
2798 die Nutzung der Funktion 'erp-submission' zurückgenommen wird. [ <= ]

2799 *Hinweis zu A\_25300\*: Die Änderung der Entscheidung zur Nutzung der "führenden"*  
2800 *Funktion hat automatisch eine Entscheidung zur Nutzung der "abhängigen" Funktion zur*  
2801 *Folge. Dieses gilt nur für die aufgeführten Entscheidungsänderungen. Alle weiteren, nicht*  
2802 *aufgeführten, Änderungen zu Entscheidungen haben keine "abhängige" Auswirkung auf*  
2803 *weitere Entscheidungen zu Funktionen. Beispiel: Wird die Entscheidung für 'medication'*  
2804 *von 'permit' auf 'deny' gesetzt, so hat dieses keine weiteren Änderungen an*  
2805 *Entscheidungen zur Folge.*

2806 **A\_23766 - Consent Decision Management - Initialisierung der**  
2807 **Widerspruchsinformation zur Nutzung von Funktionen der ePA**

2808 Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen  
2809 bezüglich der Nutzung von Funktionen der elektronischen Patientenakte bei Erstellung  
2810 eines neuen Aktenkontos oder bei Übernahme eines existierenden Aktenkontos einer  
2811 älteren ePA-Version für alle Funktionen, gegen die der Versicherte nicht widersprochen  
2812 hat mit der Entscheidung "kein Widerspruch erklärt" ("permit") initialisieren sowie alle  
2813 Funktionen, gegen die der Versicherte widersprochen hat, mit "deny" initialisieren.  
2814 [ <= ]

2815 **A\_24343 - Consent Decision Management - Speichern der Inhalte**

2816 Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen  
2817 bezüglich der Nutzung von Funktionen der elektronischen Patientenakte unter  
2818 Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen. [ <= ]

2819 **A\_23712 - Consent Decision Management - Übertrag der**  
2820 **Widerspruchsinformation zur Nutzung von Funktionen der ePA für den**  
2821 **Informationsdienst**

2822 Das Consent Decision Management MUSS die aktuellen Entscheidungen  
2823 zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen  
2824 Patientenakte der Funktionsklassen

2825 

- Versorgungsprozess ("healthCareProcess")

2826 sofort im Anschluss an eine Änderung der Entscheidung im Consent Decision  
2827 Management für die Abfrage durch den Information Service des Aktensystems ohne  
2828 Nutzung der VAU und des SecureAdminStorageKeys verfügbar machen.  
2829 [ <= ]

2830 **A\_24040 - Consent Decision Management - Periodischer Übertrag der**  
2831 **Widerspruchsinformation zur Nutzung von Funktionen der ePA für den**  
2832 **Informationsdienst**

2833 Das Consent Decision Management MUSS die aktuellen Entscheidungen  
2834 zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen  
2835 Patientenakte der Funktionsklassen

- Versorgungsprozess ("healthCareProcess")

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

Clients der Ombudsstelle und aus der Umgebung des Versicherten nutzen das Consent Decision Management über die Operationen der Schnittstelle

I\_Consent\_Decision\_Management. Clients aus der Umgebung der LEI und der E-Rezept-Fachdienst nutzen für die schnelle Abfrage die Operation der **Schnittstelle** **±Schnittstelle** I\_Information\_Service.

#### **A\_23824 - Aktensystem - Realisierung der Schnittstelle**

##### **I\_Consent\_Decision\_Management**

Das **ePA**-Aktensystem MUSS die Operationen der Schnittstelle

I\_Consent\_Decision\_Management gemäß [I\_Consent\_Decision\_Management] umsetzen. [≤]

#### **A\_23919 - Consent Decision Management - unveränderte Übernahme der Widerspruchsentscheidung**

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

#### **A\_24844 - Consent Decision Management - Information über Änderungen der Widerspruchsinformation**

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

#### **A\_24055 - Consent Decision Management – Protokollierung geänderter Entscheidungen zu Widersprüchen**

Das Consent Decision Management MUSS Bei Änderungen von Entscheidungen zu den widerspruchsfähigen Funktionen der ePA jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen. Für die Wertebelegung ist A\_23874\* zu berücksichtigen und die Protokollstruktur entsprechend zu belegen:

**Tabelle 11: Consent Decision Management Protokollierung - Widersprüche für Funktionen der ePA**

Strukturelement	Wert		Erläuterung
AuditEvent.action	U		Update
AuditEvent.entity.name	"ConsentDecision"		Eintrag protokolliert eine Widerspruchsentscheidung
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	

Strukturelement	Wert		Erläuterung
	"ConsentClass"	<consent class"	z.b. "healthcareProcess"
	"ConsentClassId"	<consent class Id>	z.b. "medication"
	"ConsentDecision"	<consent decision>	"deny" oder "permit"

[<=]

*Hinweis: Die initiale Entscheidung zu den Widersprüchen bei Anlage eines Aktenkontos wird nicht protokolliert, ~~dieses ist implizit mit der Protokollierung der Aktivierung bzw. Migration abgedeckt.~~ Die spezifische Protokollierung erfolgt für Folgeänderungen.*

### **~~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 die Sekundärdatennutzung durch das FDZ über den Data Submission Service an das FDZ weiterleiten. [<=]~~

### **~~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\_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**

~~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—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 13: 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	<b>type</b>	<b>value{x}</b>
	"Purpose"	<purposeId>
	"ConsentDecision"	<consentdecision>

[<=]

### 3.8.33.8.2 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 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. 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 ~~ConstraintConsent Decision Management~~ ~~Insurant~~ gemäß

[I\_ ~~ConstraintConsent Decision Management~~ ~~Insurant~~] 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



2977 Policy Medication vorgenommen wurden, wann die Änderung erfolgte und darauf  
2978 hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind. [ <= ]

2979 **A\_26406 - Consent Decision Management - Policy für berechnigte**  
2980 **Nutzergruppen und Nutzer**

2981 Das Consent Decision Management MUSS die Konfiguration der User Specific Deny Policy  
2982 Medication auf die folgenden Nutzergruppen einschränken:  
2983

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

2984  
2985  
2986 [ <= ]

2987  
2988 **A\_26405 - Consent Decision Management – Protokollierung geänderter**  
2989 **Entscheidungen der User Specific Deny Policy Medication**  
2990 Das Consent Decision Management MUSS für jede Änderung der User Specific Deny  
2991 Policy Medication einen Protokolleintrag gemäß A\_24704\* erzeugen:



2992 **Tabelle 12: Consent Decision Management Protokollierung - User Specific Deny Policy**  
 2993 **Medication**

Strukturelement	Wert		Erläuterung
AuditEvent.action	C, D		Update
AuditEvent.entity.name	"UdpMedication"		Eintrag protokolliert eine Änderung der User Specific Deny Policy für Medication Service
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"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

2994 [**<=**]

### 2996 3.9 Entitlement Management

2997 Befugnisse (Entitlements) werden individuell für jeden Nutzer des Aktenkontos erstellt  
 2998 (Versicherter, Vertreter, Leistungserbringerinstitutionen, Kostenträger, Ombudsstelle und  
 2999 Fachdienste). Eine erteilte Befugnis ist notwendige Voraussetzung für die Nutzung des  
 3000 Aktenkontos und zum internen Bezug des Datenpersistierungsschlüssels  
 3001 (SecureDataStorageKey) für den Zugriff auf die Dokumenten- und Datenverwaltung.

3002 Eine Befugnis enthält folgende Informationen:

#### 3003 **A\_23734-01 - Entitlement Management - Definition einer Befugnis**

3004 Das Entitlement Management MUSS für eine individuelle Befugnis die folgenden Daten  
 3005 nutzen und verwalten:

3006 **Tabelle 13: Inhalt einer Befugnis**

Element	Inhalt	Anmerkung	signiertes Element (*)
Identifizier des Aktenkontos (insurantId)	KVNR des Aktenkontos, für welches die Befugnis ausgestellt ist		ja

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

3007 [ $\leq$ ]

3008 *Hinweis: Ein Nutzer ist der Adressat, für den die Befugnis ausgestellt wird. Der Ersteller*  
 3009 *ist der Nutzer, welcher die Befugnisausstellung veranlasst hat. Die Bezeichner in () sind*  
 3010 *die Bezeichner in den Schnittstellenbeschreibungen.*

3011 *Hinweis (\*): A\_23734 definiert eine "vollständige" Befugnis, welche auch Daten enthält,*  
 3012 *die für eine Prüfung einer gültigen Befugnis im Kontext einer Schnittstellenoperation*  
 3013 *nicht notwendig sind. Für diesen Zweck wird nur der (HSM-) signierte Anteil als Ergebnis*  
 3014 *einer Befugnisverifikation verwendet (signiertes Element = ja). Eine gespeicherte*  
 3015 *Befugnis enthält jedoch alle Elemente für eine qualifizierte Verwaltung der Befugnisse*  
 3016 *durch einen Versicherten oder Vertreter.*

3017 *Hinweis: Befugnisse können durch das Aktensystem selbst (initiale Befugnisse), durch*  
 3018 *den Versicherten oder einen befugten Vertreter unter Verwendung eines ePA-FdV oder*  
 3019 *durch eine Leistungserbringerinstitution in einer Behandlungssituation erstellt werden.*

3020 Eine Befugnis kann nur für Nutzer und Nutzergruppen mit bestimmter Rolle erteilt  
 3021 werden. Nutzergruppen mit abweichenden Rollen können nicht befugt werden und  
 3022 erhalten keinen Zugriff auf das Aktenkonto.

3023 Erfolgt die Befugniserteilung durch eine Leistungserbringerinstitution in einer  
 3024 Behandlungssituation, wird eine vorgegebene Gültigkeitsdauer der Rolle des Befugten  
 3025 entsprechend durch das Entitlement Management vergeben. Ein Versicherter oder ein  
 3026 befugter Vertreter kann den Gültigkeitszeitraum frei wählen (ausgenommen  
 3027 Vertreterbefugnisse).

3028

### 3029 **A\_23941-01 - Entitlement Management - Erteilung von Befugnissen für** 3030 **berechtigte Nutzergruppen und Nutzer**

3031 Das Entitlement Management MUSS die Erteilung von Befugnissen in der jeweiligen  
 3032 Umgebung auf die folgenden Nutzergruppen und Nutzer einschränken:

3033 **Tabelle 14: 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

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_psychotherapeut	x	x	-	90	var
oid_institution-pflege	x	x	-	90	var
oid_institution-geburtshilfe	x	x	-	90	var
oid_praxis-physiotherapeut	x	x	-	90	var
oid_praxis-ergotherapeut	x	x	-	90	var
oid_praxis-logopaede	x	x	-	90	var
oid_praxis-podologe	x	x	-	90	var
oid_praxis-ernaehrungstherapeut	x	x	-	90	var
oid_institution-oegd	x	x	-	3	var
oid_institution-arbeitsmedizin	x	x	-	3	var
oid_kostentraeger	-	-	x (statisch)	-	-
oid_ombudsstelle	-	-	x (statisch)	-	-
oid_erp-vau (E-Rezept vertrauenswürdige Ausführungsumgebung)	-	-	x (statisch)	-	-
oid_versicherter (Versicherter)	-	-	x (statisch)	-	-

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_versicherter (Vertreter)	-	x	-	-	dauerhaft
oid_diga	-	x	-	-	dauerhaft

Hinweis:

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

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

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

FdV = Versicherter oder Vertreter,

KTR = Kostenträger

AS = Aktensystem (systemseitig erteilte Befugnisse)

Tage = Gültigkeit in Tagen: angegebener Wert ist einschließlich aktuellem Datum, z. B. 90 Tage bedeutet aktuelles Datum + 89 Tage.

dauerhaft = Befugnis unbegrenzt gültig (Enddatum = 9999-12-31)

statisch = Gültigkeit analog 'dauerhaft', Befugnis ist implizit vorhanden.

var = Gültigkeitsdauer von 1 Tag bis dauerhaft in jeweils ganzen Tagen[<=]

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

Einzelne Nutzer können durch den Versicherten, einen befugten Vertreter oder die Ombudsstelle explizit von der Befugnisvergabe ausgeschlossen sein (siehe 3.9.4. Befugnisausschluss (Blocked User Policy) ). Eine Befugniserstellung ist dann weder für Leistungserbringerinstitutionen in einer Behandlungssituation, noch durch den Versicherten oder einen Vertreter möglich.

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

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

### **A\_26167 - Entitlement Management (EU) - Erteilung der Befugnis EU-Zugriff**

Das Entitlement Management MUSS die Erteilung einer Befugnis EU-Zugriff in der jeweiligen Umgebung zusätzlich zu A\_23941-\* auf die folgenden Nutzergruppen und Nutzer einschränken:

3068 **Tabelle 15: Befugnisse EU-Zugriff für berechtigte Nutzergruppen und Nutzer**

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

3069 Hinweis:

3070 'x' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung befugt  
3071 werden3072 '-' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung nicht  
3073 befugt werden3074 LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-  
3075 Prüfungsnachweis (Prüfziffer),

3076 FdV = Versicherter oder Vertreter,

3077 AS = Aktensystem (systemseitig erteilte Befugnisse)[&lt;=]

3079 **A\_24371 - Entitlement Management - Verschlüsselung der Befugnisse**3080 Das Entitlement Management MUSS Befugnisse mit dem versichertenindividuellen  
3081 SecureAdminStorageKey verschlüsseln und im Aktenkonto persistieren.[<=]3082 **A\_24372 - Entitlement Management - Keine persistente Ablage**  
3083 **unverschlüsselter Befugnisse**3084 Das Entitlement Management MUSS sicherstellen, dass Befugnisse ausschließlich  
3085 verschlüsselt unter Verwendung des versichertenindividuellen SecureAdminStorageKey  
3086 im Aktenkonto gespeichert werden.[<=]3087 **A\_24687 - Entitlement Management - Keine Speicherung oder Verwendung**  
3088 **nicht verifizierter Befugnisse**3089 Das Entitlement Management MUSS sicherstellen, dass ausschließlich Befugnisse  
3090 persistiert oder für eine Befugnisprüfung verwendet werden, die erfolgreich durch das  
3091 HSM unter Verwendung der adäquaten Regeln 'rr1 - rr4' gemäß A\_24573\*  
3092 befugnisverifiziert sind.[<=]3093 **A\_23842 - Entitlement Management - Eindeutigkeit der Befugnisse im**  
3094 **Befugniskontext**3095 Das Entitlement Management MUSS sicherstellen, dass im Befugniskontext keine zwei  
3096 oder mehr Befugnisse existieren, die als Identifier des befugten Nutzers die gleiche  
3097 Identifikation (actorId) aufweisen.[<=]3098 **A\_24785 - Entitlement Management - VSDM-Prüfungsnachweis kann höchstens**  
3099 **einmal genutzt werden**3100 Das Entitlement Management MUSS sicherstellen, dass ein VSDM-Prüfungsnachweis  
3101 (Prüfziffer) höchstens einmal zur Registrierung einer Befugnis genutzt werden kann.[<=]

3102 ePA-Clients nutzen zur Befugnisvergabe die Operationen der  
 3103 Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`.  
 3104 Die initialen Befugnisse des Aktenkontos werden auf organisatorischem Weg direkt im  
 3105 Aktenkonto erstellt.

3106 **A\_24506 - Entitlement Management- Realisierung der Schnittstelle**  
 3107 **I\_Entitlement\_Management**

3108 Das Entitlement Management MUSS die Operationen der Schnittstelle  
 3109 `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` umsetzen. [`<=`]

3110 **A\_26168 - Entitlement Management (EU)- Realisierung der Schnittstelle**  
 3111 **I\_Entitlement\_Management\_EU**

3112 Das Entitlement Management MUSS die Operationen der Schnittstelle  
 3113 `I_Entitlement_Management_EU` gemäß `[I_Entitlement_Management_EU]`  
 3114 umsetzen. [`<=`]

3115 **A\_24987-01 - Entitlement Management - Protokolleinträge für Zugriffe auf das**  
 3116 **Entitlement Management**

3117 Das Entitlement Management MUSS für das Erteilen und Entziehen von Befugnissen und  
 3118 das Setzen und Löschen von Befugnisausschlüssen jeweils einen Protokolleintrag gemäß  
 3119 A\_24704 erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

3120 **Tabelle 16: Entitlement Management Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		
AuditEvent.action	C, D, U		ein Code aus den genannten, je nach Operation
AuditEvent.entity.name	"UserBlocking"		Setzen und Löschen von Befugnisausschlüssen
	"EntitlementManagement"		Erteilen oder Entziehen von Befugnissen
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"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



Strukturelement	Wert		Erläuterung
	"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

3121

3122 [**<=**]

3123 *Hinweis: Ein Update ("U") eines Entitlements liegt vor, wenn ein existierendes*  
 3124 *Entitlement aufgrund des längeren Gültigkeitszeitraums eines neuen Entitlements*  
 3125 *überschrieben wird.*

### 3126 3.9.1 Initiale Befugnisse (static Entitlements)

3127 Einige grundsätzlich notwendige Befugnisse sind zum Zeitpunkt der Aktivierung eines  
 3128 Aktenkontos verfügbar.

3129 Zu diesen initialen Befugnissen gehören die Befugnisse für den Versicherten, den E-  
 3130 Rezept-Fachdienst, den Kostenträger und die Ombudsstelle. Diese Befugnisse müssen in  
 3131 der Phase der Initialisierung eines Aktenkontos durch das Aktensystem erstellt werden.

3132 Diese Befugnisse sind dauerhaft gültig und unveränderbar und können nicht gelöscht  
 3133 werden.

#### 3134 **A\_24145 - Entitlement Management – Implizite initiale (statische) Befugnisse**

3135 Das Entitlement Management MUSS sicherstellen, dass der Versicherte (KVNR des  
 3136 Akteninhabers, oid\_versicherter), und der E-Rezept-Fachdienst (registrierte Telematik-  
 3137 ID, oid\_erp-vau) dauerhaft den versichertenindividuellen SecureDataStorageKey  
 3138 beziehen können und Zugriff auf die Dokumenten- und Datenverwaltung erhalten. Die  
 3139 Befugnisse MÜSSEN den Vorgaben der folgenden Tabelle entsprechen:

3140

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

Element	Versicherter	E-Rezept-Fachdienst
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

3141 [**<=**]3142 **A\_24374 - Entitlement Management – Signierte initiale (statische) Befugnisse**

3143 Das Entitlement Management MUSS sicherstellen, dass für den Kostenträger und die  
 3144 Ombudsstelle gültige Befugnisse mit unbegrenzter Gültigkeitsdauer zum Zeitpunkt der  
 3145 Aktivierung des Aktenkontos gemäß der Vorgaben der folgenden Tabelle vorliegen:

3146

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

3147 [**<=**]3148 **A\_24688-01 - Entitlement Management – Befugnisverifikation signierter initialer Befugnisse**

3149 Das Entitlement Management MUSS sicherstellen, dass die initialen, signierten  
 3150 Befugnisse des Kostenträgers und der Ombudsstelle spätestens beim ersten Zugriff auf  
 3151 das Aktenkonto durch das HSM unter Verwendung der Regel 'rr4' gemäß A\_24573\*  
 3152 befugnisverifiziert sind. [**<=**]

3154 **A\_24533 - Entitlement Management - Keine Änderung statischer Befugnisse**

3155 Das Entitlement Management MUSS sicherstellen, dass die dauerhaften Befugnisse des  
 3156 Versicherten, des E-Rezept-Fachdienstes, des Kostenträgers und der Ombudsstelle nicht  
 3157 verändert oder gelöscht werden können. [**<=**]

3158 **A\_24784 - Entitlement Management - Höchstens eine Befugnis für KTR und**  
 3159 **Ombudsstelle pro Aktenkonto**

3160 Das Entitlement Management MUSS sicherstellen, dass in einem Aktenkonto höchstens  
 3161 eine Befugnis für einen Kostenträger und höchstens eine Befugnis für eine Ombudsstelle  
 3162 hinterlegt ist. [≤]

3163 **A\_24955 - Entitlement Management - Befugnis für KTR und Ombudsstelle nur**  
 3164 **bei Anlage und betreiberinterner Anbieterwechsel**

3165 Das Entitlement Management MUSS sicherstellen, dass eine signierte Befugnis des  
 3166 Kostenträgers und eine signierte Befugnis der Ombudsstelle ausschließlich bei einer  
 3167 Anlage eines Aktenkontos (Initialisierung) oder bei einem betreiberinternen  
 3168 Anbieterwechsel in die Befugnisse des Aktenkontos aufgenommen werden.  
 3169 [≤]

3170 **3.9.2 Erstellen einer Befugnis durch Clients**

3171 Die Anforderung zur Vergabe einer neuen Befugnis erfolgt durch die Clients der ePA. Bei  
 3172 einer Befugnisvergabe aus der Umgebung der Leistungserbringer ist dieses das  
 3173 Primärsystem (PS), aus der Umgebung des Versicherten ist es das ePA-FdV.

3174 Clients verwenden zur Befugnisvergabe signierte JSON Web Token (JWS). Das Token  
 3175 wird zur Verifikation an das HSM übergeben. Als Ergebnis der HSM Verarbeitung liegt  
 3176 eine bestätigte, CMAC gesicherte Befugnis mit den Elementen `actorId` (Identifizier des zu  
 3177 befugnenden Nutzers), `kvnur` (AktenkontoId) und `validTo` (Gültigkeitszeitraum) für die  
 3178 spätere Befugnisprüfung vor. Das HSM Ergebnis wird mit den weiteren Daten gemäß  
 3179 A\_23734\* (`oid`, `displayName`, `issued`-\*) ergänzt und gemäß A\_24371\* mit dem  
 3180 `SecureAdminStorageKey` gesichert im Aktenkonto abgelegt.

3181 **3.9.2.1 Befugnisvergabe durch ein ePA-FdV**

3182 Ein ePA-FdV muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

3183 **A\_24587-01 - Entitlement Management - Befugnis durch ein ePA-FdV**

3184 Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ePA-  
 3185 FdV über die Schnittstelle `I_Entitlement_Management` durch Verwendung eines gültig  
 3186 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

Befugnis	Claim Name	Claim	Beispiel
	"actorId"	Identifizier (Telematik-id oder KVN-R)	3-883110000092471
	"oid"	professionOid	1.2.276.0.76.4.54
	"displayName"	Name des Befugten	Test-Apotheke
	"validTo"	Ende der Gültigkeit, (Bei unbegrenzter Gültigkeit ist 9999-12-31T00:00:00Z zu verwenden.)	gemäß [RFC3339], z.B. 2025-06-30T21:59:59Z oder 2025-06-30T23:59:59+02:00

3187 [ $\leq$ ]

3188 Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve  
 3189 "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext  
 3190 der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur  
 3191 und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

3192 *Hinweis zu A\_24587\*: Im Falle der Befugnisvergabe für einen NCPeH (EU-Zugriff, "oid"*  
 3193 *== "oid\_ncpeh") wird durch das Aktensystem sichergestellt, dass die vorgeschriebene*  
 3194 *Gültigkeitsdauer für derartige Befugnisse angewendet wird. Dieses erfolgt durch die*  
 3195 *Befugnisverifikation gemäß Regel "rr1" im HSM. Die Angabe eines Gültigkeitsendes im*  
 3196 *"validTo"-Element des JWT wird daher für diesen Fall ignoriert, das Element selbst muss*  
 3197 *jedoch vorhanden sein.*

3198

#### 3199 **A\_24689 - Entitlement Management - Befugnisverifikation einer Befugnis durch** 3200 **ein ePA-FdV**

3201 Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein  
 3202 ePA-FdV unter Verwendung der Regeln 'rr1' (Befugnisvergabe durch den Versicherten)  
 3203 bzw. 'rr2' (Befugnisvergabe durch einen Vertreter) des HSM eine Befugnisverifikation  
 3204 durchführen. [ $\leq$ ]

#### 3205 **A\_24535 - Entitlement Management - Befugnisse für Vertreter**

3206 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (actorId  
 3207 = KVN-R) ausschließlich durch den Versicherten erstellt oder gelöscht werden  
 3208 können. [ $\leq$ ]

#### 3209 **A\_26698 - Entitlement Management - maximale Anzahl Befugnisse für Vertreter** 3210 Das Entitlement Management MUSS sicherstellen, dass maximal fünf gültige Befugnisse 3211 für Vertreter gleichzeitig in einem Aktenkonto vorhanden sind. [ $\leq$ ]

#### 3212 **A\_24536 - Entitlement Management - Gültigkeitsdauer der Befugnisse für** 3213 **Vertreter**

3214 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (actorId  
 3215 = KVN-R) ausschließlich mit einer unbegrenzten Gültigkeit erstellt werden. [ $\leq$ ]

#### 3216 **A\_24754 - Entitlement Management - E-Mail-Adresse des Vertreters**

3217 Das Entitlement Management MUSS sicherstellen, dass bei Befugnissen für Vertreter  
 3218 (`actorId` = KVNR) eine E-Mail-Adresse des Vertreters für dessen Benachrichtigung  
 3219 angegeben wird. [`<=`]

3220 Die in A\_24754 angegebene E-Mail-Adresse wird ausschließlich zur Benachrichtigung des  
 3221 Vertreters über die eingestellte Befugnis verwendet (vgl. A\_24755-\*), jedoch nicht für  
 3222 die Geräteregistrierung. Um eine Vertretung wahrnehmen zu können und hierfür Geräte  
 3223 zu registrieren, muss der Vertreter in seinem Home-AS eine E-Mail-Adresse hinterlegt  
 3224 haben.

### 3225 **A\_24755-01 - Entitlement Management - Benachrichtigung des Vertreters bei** 3226 **Befugniserstellung**

3227 Das Entitlement Management MUSS im Anschluss an die erfolgreiche, neue  
 3228 Befugniserstellung für einen Vertreter eine E-Mail an die E-Mail-Adresse des Vertreters  
 3229 senden, die diesen über die Befugniserstellung für das Aktenkonto des Versicherten  
 3230 geeignet informiert. In der Nachricht MUSS der Name des Versicherten enthalten sein  
 3231 und welche Art von personenbezogenen Daten vom Vertreter im Rahmen der  
 3232 Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine  
 3233 Vertreterberechtigung widerrufen kann und gegenüber wem er seine  
 3234 datenschutzrechtlichen Betroffenenrechte wahrnehmen kann. [`<=`]

3235 Hinweis: Unter Art der personenbezogenen Daten ist z.B. „Krankenversichertennummer,  
 3236 Name und E-Mail-Adresse“ gemeint, aber nicht die tatsächliche KVNR des Vertreters, der  
 3237 tatsächliche Name oder die tatsächliche E-Mail-Adresse.

3238

### 3239 **3.9.2.2 Befugnisvergabe durch ein Primärsystem**

#### 3240 **A\_27288 - Entitlement Management – Abgleich der KVNR bei Erstellen einer** 3241 **Befugnis über VSDM-Prüfziffer**

3242 Das Entitlement Management MUSS sicherstellen, dass für die in `setEntitlementPs` vom  
 3243 Primärsystem in `x-insurantid` übergebene KVNR und die übergebene Befugnis  
 3244 (signiertes JWT) folgendes gilt: die KVNR in `x-insurantid` stimmt mit der KVNR überein,  
 3245 die in der CMAC-gesicherten Befugnis enthalten ist, die als Ergebnis des Aufrufs der  
 3246 Regel `rr3` mit der vom Primärsystem erhaltenen Befugnis (signiertes JWT) vom HSM  
 3247 zurückgegeben wird.  
 3248 [`<=`]

3249 Ein Primärsystem muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe  
 3250 erstellen.

3251 Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve  
 3252 "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext  
 3253 der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur  
 3254 und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

#### 3255 **AA\_27321 - Entitlement Management – Abgleich hcv bei Erstellen einer** 3256 **Befugnis über VSDM-Prüfziffer in Version 2**

3257 Falls vom Primärsystem in `setEntitlementPs` eine Befugnis (signiertes JWT) mit einer  
 3258 Prüfziffer in Version 2 übergeben wird und das Ergebnis des Aufrufs der Regel `rr3` eine  
 3259 interne Datenstruktur der VSDM-Prüfziffer zurückliefert, MUSS das Entitlement  
 3260 Management sicherstellen, dass

- 3261 • bei einem JWT mit Attribut "hcv" der Wert von "hcv" mit dem Wert von hcv aus  
 3262 der VSDM-Prüfziffer übereinstimmt und ansonsten die Operation `setEntitlementPs`  
 3263 abbricht,

- bei einem JWT ohne Attribut "hcv" die Operation `setEntitlementPs` abbricht, falls der Konfigurationsparameter `enforce_hcv_check` (vgl. A\_27342-\*) auf `true` gesetzt ist.

[<=]

#### **A\_27289 - Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer**

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

#### **A\_27322 - Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche der VSD-Update-Zeit bei Erstellen einer Befugnis über VSDM-Prüfziffer in Version 2**

Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer Stunde maximal fünfmal eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2 über `setEntitlementPs` übermitteln kann, bei der die Operation `setEntitlementPs` gemäß A\_27321-\* abbricht. [≤]

#### **A\_24590-02 - Entitlement Management - Befugnis durch ein Primärsystem**

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

Befugnis	Claim Name	Claim
Protected Header		
	"typ"	"JWT"
	"alg"	"ES256" oder "PS256"
	"x5c"	Signaturzertifikat C.HCI.AUT
Payload		
	"iat"	Zeitstempel Ausgabezeitpunkt
	"exp"	Verfalldatum, = "iat" + 20 min
	"auditEvidence"	VSDM-Prüfziffer aus dem VSDM-Prüfungsnachweis, <u>base64-kodiert.</u>

Befugnis	Claim Name	Claim
	<u>"hcv"</u>	<u>optional solange enforce hcv_check = FALSE; Hash check value der als Ergebnis der Operation ReadVSD gemäß A_27352-* berechnet wird. Der berechnete hcv-Wert MUSS base64 kodiert werden.</u>

3288 [ $\leq$ ]

3289 ~~Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve~~  
 3290 ~~"brainpoolP256r1" basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext~~  
 3291 ~~der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur~~  
 3292 ~~und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.~~

### 3294 **A\_25249 - Entitlement Management - Befugnisverifikation einer Befugnis durch** 3295 **ein Primärsystem**

3296 Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein  
 3297 Primärsystem unter Verwendung der Regeln 'rr3' (Stecken der eGK in einer  
 3298 Leistungserbringerumgebung) des HSM eine Befugnisverifikation durchführen. [ $\leq$ ]

### 3300 **A\_24537 - Entitlement Management - Standardgültigkeitsdauer für Befugnisse**

3301 Das Entitlement Management MUSS sicherstellen, dass neue Befugnisse, die unter  
 3302 Verwendung der Schnittstelle `I_Entitlement_Management` gemäß  
 3303 `[I_Entitlement_Management]` erstellt werden, eine vorgegebene, rollenspezifische  
 3304 Befugnisdauer gemäß A\_23941-\* erhalten. [ $\leq$ ]

## 3305 **3.9.3 Löschen von Befugnissen**

3306 Erteilte Befugnisse werden grundsätzlich nach Erreichen des Endzeitpunkts ihrer  
 3307 Gültigkeit durch das Aktensystem gelöscht.

### 3308 **A\_24504 - Entitlement Management - Löschen ungültiger Befugnisse**

3309 Das Entitlement Management MUSS vorhandene Befugnisse, deren Enddatum der  
 3310 Gültigkeit überschritten ist, unverzüglich aus dem Befugnis Kontext des Aktenkontos  
 3311 vollständig löschen. [ $\leq$ ]

3312 Das explizite Löschen von Befugnissen innerhalb ihres Gültigkeitszeitraums kann  
 3313 ausschließlich durch den Versicherten oder einen Vertreter mittels eines ePA-FdV  
 3314 erfolgen. Es können alle erteilten Befugnisse gelöscht werden, ausgenommen die initialen  
 3315 Befugnisse gemäß 3.9.1- Initiale Befugnisse (static Entitlements) .

3316 Für das Löschen von Befugnissen durch einen Vertreter gilt darüber hinaus folgende  
 3317 Einschränkung:

### 3318 **A\_25246 - Entitlement Management - Löschen von Befugnissen durch einen** 3319 **Vertreter**

3320 Das Entitlement Management MUSS sicherstellen, dass eine erteilte Befugnis für einen  
 3321 Vertreter (`actorId` der Befugnis == KVNR) durch einen Vertreter nur dann gelöscht  
 3322 werden kann, wenn die KVNR des löschenden Vertreters der KVNR der `actorId` der zu  
 3323 löschenden Befugnis entspricht. [ $\leq$ ]

3324 *Hinweis: Ein Vertreter darf nur seine eigene Befugnis löschen, nicht aber die Befugnis*  
 3325 *weiterer Vertreter.*



### **A\_25269 - Entitlement Management - Benachrichtigung des Versicherten bei Löschen einer Vertreterbefugnis durch Vertreter**

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

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

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

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

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

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

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

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

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

### **A\_24463-01 - Entitlement Management - zulässige Rollen für den Widerspruch gegen die Nutzung durch eine Leistungserbringerinstitution**

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

professionOID / Nutzergruppe
oid_praxis_arzt
oid_krankenhaus
oid_institution-vorsorge-reha
oid_zahnarztpraxis

professionOID / Nutzergruppe
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

3361 **[<=]**

3362 Ein Eintrag der Blocked User Policy enthält Angaben gemäß der folgenden Tabelle:  
 3363 (Beispiel)

3364 **Tabelle 17: Inhalt eines Blocked User Policy Eintrags**

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

3365 **A\_25135 - Entitlement Management - Initialisierung der Blocked User Policy**

3366 Das Entitlement Management MUSS für ein Aktenkonto eine Blocked User Policy ohne  
 3367 initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policies über die  
 3368 Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`  
 3369 ermöglichen. **[<=]**

**A\_24514 - Entitlement Management - Keine Befugnis für von einer Befugnis ausgeschlossene Nutzer**

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

**A\_24515 - Entitlement Management- Verschlüsselung der Einträge der Blocked User Policy**

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

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

**A\_24965 - Entitlement Management - Information über Änderungen der Blocked User Policy**

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

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

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

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

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

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

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

**A\_27311 - Entitlement Management – RateLimit-oid-List**

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

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

gespeichert werden. [ $\leq$ ]

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

**A 27290 - Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Stunde**

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

- oid praxis arzt maximal 200 Befugnisse
- oid krankenhaus maximal 1.000 Befugnisse
- oid institution-vorsorge-reha maximal 1.000 Befugnisse
- oid zahnarztpraxis maximal 200 Befugnisse
- oid öffentliche apotheke maximal 200 Befugnisse
- oid praxis psychotherapeut maximal 100 Befugnisse
- oid institution-pflege maximal 100 Befugnisse
- oid institution-geburtshilfe maximal 100 Befugnisse
- oid praxis-physiotherapeut maximal 100 Befugnisse
- oid institution-oegd maximal 100 Befugnisse
- oid institution-arbeitsmedizin maximal 100 Befugnisse

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

**A 27291 - Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Monat**

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

- oid praxis arzt maximal 10.000 Befugnisse
- oid krankenhaus maximal 200.000 Befugnisse
- oid institution-vorsorge-reha maximal 200.000 Befugnisse
- oid zahnarztpraxis maximal 10.000 Befugnisse
- oid öffentliche apotheke maximal 25.000 Befugnisse
- oid praxis psychotherapeut maximal 10000 Befugnisse
- oid institution-pflege maximal 10000 Befugnisse
- oid institution-geburtshilfe maximal 10000 Befugnisse
- oid praxis-physiotherapeut maximal 10000 Befugnisse
- oid institution-oegd maximal 10000 Befugnisse
- oid institution-arbeitsmedizin maximal 10000 Befugnisse

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

Hinweis zu A 27290-\* und A 27291-\*: Die Stunde bzw. der Tag müssen sich nicht auf die aktuelle Stunde bzw. Kalendertag beziehen, sondern können auch je Leistungserbringerinstitution auf Requestzeitpunkte bezogen werden. Dann gilt für einen Monat 30 Tage.

#### **A 27318 - ePA-Aktensystem - RateLimit-oid-List: Maßnahmen zum Schutz der Konfiguration**

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

#### **A 27312 - ePA-Aktensystem - RateLimit-oid-List: Konfiguration durch Betreiber**

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

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

#### **A 27313 - Entitlement Management - Prüfen der RateLimit-oid-List beim Einstellen von Befugnissen**

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

#### **A 27310 - ePA-Aktensystem - Erfassung der Nutzer zur Prüfung RateLimit-oid-List**

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

### **3.10 Legal Policy**

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

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

Beispiele sind:

- Apotheker haben keinen Zugriff auf das Zahnbonusheft zahnärztliche Dokumentation in der Datenkategorie "dental").".

- 3501 • Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen  
3502 noch löschen.

3503 Die Legal Policy wird durch das Aktensystem durchgesetzt und ist jederzeit vorhanden.  
3504 Die Konfiguration kann durch Clients oder Bestandteile des Aktensystems nicht verändert  
3505 werden.

3506 **A\_19303-20 - Legal Policy – gesetzlich vorgegebene Zugriffsrechte**

3507 Das ePA-Aktensystem MUSS alle in der folgenden Tabelle aufgeführten Regeln der Legal  
3508 Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

3509 **Tabelle 18: Legal Policy**

Kategorie	Nutzergruppe										
Technischer Identifier	Med	Apo	Pflege	GH	HM E	AM	KT R	O M	DiG A	eR P	Ver
<b>Medical Services (XDS Document Service)</b>	<b>Zugriffsrecht gemäß § 352 SGB V</b>										
reports	CRUD	R	R	R	R	R	-	-	-	-	RD
emp	CRUD	CRUD	R	R	R	R	-	-	-	-	RD
emergency	CRUD	R	R	R	R	R	-	-	-	-	RD
eab	CRUD	R	R	R	R	R	-	-	-	-	RD
dental	CRUD	-	R	-	-	R	-	-	-	-	RD
childsrecord	RD	R	R	RD	R	R	-	-	-	-	RD
child	CRUD	R	R	CRUD	R	R	-	-	-	-	RD (CU (*))
pregnancy_childbirth	CRUD	R	R	CRUD	R	R	-	-	-	-	RD
vaccination	CRUD	CRUD	R	R	-	CRUD	-	-	-	-	RD
patient	RD	R	R	R	R	R	C	-	-	-	CRUD

Kategorie	Nutzergruppe										
receipt	RD	RD	-	R	R	R	CU	-	-	-	RD
<u>health risk analysis</u>	-	-	-	-	-	-	<u>C</u>	-	-	-	<u>RD</u>
diga	R	R	R	R	R	R	-	-	CU	-	RD
care	CRUD	R	CRUD	R	R	R	-	-	-	-	RD
eau	CRUD	-	-	-	-	R	-	-	-	-	RD
rehab	CRUD	-	-	-	-	-	-	-	-	-	RD
transcripts	CRUD	-	-	-	-	-	-	-	-	-	RD
other	CRUD	-	-	-	-	R	-	-	-	-	RD
<b>Medical Services (FHIR Data Service)</b>	<b>Zugriffsrecht</b>										
medication	CRUD	CRUD	R	R	R	R	-	-	-	CU	R
<b>Basic Services</b>	<b>Zugriffsrecht</b>										
Consent Decisions	-	-	-	-	-	-	-	X	-	-	X
Constraints	-	-	-	-	-	-	-	-	-	-	X
Entitlements	X	X	X	X	X	X	-	-	-	-	X
Entitlements.Blocked User	-	-	-	-	-	-	-	X	-	-	X
Audit Events	-	-	-	-	-	-	-	X	-	-	X
Information	X	X	X	X	X	X	X	X	<del>X</del>	X	-
Devices	-	-	-	-	-	-	-	-	-	-	X

Nutzergruppen:



- 3512 • Med = Arztpraxis, Zahnarztpraxis, Krankenhaus, Psychotherapeut, Vorsorge- und  
3513 Rehabilitation, Öffentlicher Gesundheitsdienst
- 3514 • (oid\_praxis\_arzt,, oid\_krankenhaus, oid\_institution-vorsorge-reha,  
3515 oid\_zahnarztpraxis, oid\_praxis\_psychotherapeut oid\_institution-oegd)
- 3516 • Apo = Öffentliche Apotheke
- 3517 • (oid\_öffentliche\_apotheke)
- 3518 • Pflege = Gesundheits-, Kranken- und Altenpflege
- 3519 • (oid\_institution-pflege)
- 3520 • GH = Geburtshilfe
- 3521 • (oid\_institution-geburtshilfe)
- 3522 • HME = Heilmittelerbringer
- 3523 • (oid\_praxis-physiotherapeut, oid\_praxis-ergotherapeut, oid\_praxis-logopaede,  
3524 oid\_praxis-podologe, oid\_praxis-ernaehrungstherapeut)
- 3525 • AM = Arbeitsmedizin
- 3526 • (oid\_institution-arbeitsmedizin)
- 3527 • KTR = Kostenträger
- 3528 • (oid\_kostentraeger)
- 3529 • OM = Ombudsstelle
- 3530 • (oid\_ombudsstelle)
- 3531 • DiGA = Digitale Gesundheitsanwendung
- 3532 • (oid\_diga)
- 3533 • eRP = E-Rezept vertrauenswürdige Ausführungsumgebung
- 3534 • (oid\_erp-vau)
- 3535 • Ver = Versicherter / Vertreter
- 3536 • (oid\_versicherter)

## 3537 Legende:

- 3538 • CRUD = create, read, update, delete; update: Aktualisierung von Metadaten,  
3539 Aktualisierung eines Dokuments
- 3540 • "-" = keine Zugriffsrechte;
- 3541 • "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den  
3542 Dienst (Service) definiert)
- 3543 • "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- 3544 • "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung  
3545 in einer zukünftigen Version der ePA vorgesehen.

## 3546 Hinweise:

- 3547 • (\*) Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann der  
3548 Versicherte bzw. sein Vertreter oder eine Leistungserbringerinstitution gemäß der  
3549 zuvor genannten Liste definierter professionOIDs sein. Sofern ein  
3550 Versicherter/Vertreter der Einsteller der Elternnotiz ist, darf er abweichend von

3551 den oben aufgeführten Zugriffsunterbindungsregeln in die Datenkategorie mit  
 3552 dem technischen Identifier 'child' schreiben.

3553 [ $\leq$ ]

3554 **AA\_26166-0102 - Legal Policy (EU) – EU-Zugriff: gesetzlich vorgegebene**  
 3555 **Zugriffsrechte**

3556 Das ePA-Aktensystem MUSS zusätzlich zu den Regeln aus A\_19303-\* alle in der  
 3557 folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten  
 3558 und Dienste des Aktenkontos durchsetzen.

3559 **Tabelle 19: Legal Policy - EU-Zugriff**

Kategorie	Nutzergruppe
Technischer Identifier	NCPeH
Medical Services (XDS Document Service)	Zugriffsrecht gemäß § 352 SGB V
reports	-
emp	-
emergency	R
eab	-
dental	-
child	-
childsrecord	-
pregnancy_childbirth	-
vaccination	-
patient	-
receipt	-
<u>health_risk_analysis</u>	-
diga	-
care	-
eau	-

Kategorie	Nutzergruppe
rehab	-
transcripts	-
other	-
<b>Medical Services (FHIR Data Service)</b>	<b>Zugriffsrecht</b>
medication	-
<b>Basic Services</b>	<b>Zugriffsrecht</b>
Consent Decisions	-
Constraints	-
Entitlements	-
Entitlements.Blocked User	-
Audit Events	-
Information	x
Devices	-

3560  
3561

Nutzergruppen:

- 3562
- NCPeH = NCPeH-Fachdienst (oid\_ncpeh)

3563

Legende:

- 3564
- CRUD = create, read, update, delete; update: Aktualisierung von Metadaten, Aktualisierung eines Dokuments
- 3565
- "-" = keine Zugriffsrechte;
- 3566
- "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den Dienst (Service) definiert)
- 3567
- "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- 3568
- "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung in einer zukünftigen Version der ePA vorgesehen.
- 3569
- 3570
- 3571
- 3572

3573 [**<=**]

3574 Die folgende Tabelle erläutert die Kategorien aus A\_19303-\* und A\_26166-\*:

3575 **Tabelle 20: Beschreibung der Kategorien**

Technischer Identifier	Beschreibung
<b>Medical Services</b>	<b>XDS Document Service</b>
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	<del>Daten zum Nachweis der regelmäßigen Inanspruchnahme zahnärztlicher Vorsorgeuntersuchungen gemäß § 55 Absatz 1 in Verbindung mit § 92 Absatz 1 Satz 2 Nummer 2 (elektronisches Zahnbonusheft)</del> <u>Daten aus der zahnärztlichen Dokumentation</u>
child	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
childsrecord	Archiv aus ePA 2.x: Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
pregnancy_childbirth	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass) sowie Daten, die sich aus der Versorgung der Versicherten mit Hebammenhilfe ergeben
vaccination	Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation)

Technischer Identifier	Beschreibung
patient	Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden
receipt	Bei Kostenträgern gespeicherte Daten über die in Anspruch genommenen Leistungen des Versicherten
<u>health risk analysis</u>	<u>Ergebnisse datengestützter Auswertungen der Krankenkassen zu individuellen Gesundheitsrisiken gemäß SGB V § 25b.</u>
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
<b>Medical Services</b>	<b>Medication Service</b>
medication	Verordnungs-, Dispensier- und Medikationsdaten in einer elektronischen Medikationsliste (eML) <u>und einem elektronischen Medikationsplan (eMP)</u>
<b>Basic Services</b>	<b>Account Management</b>
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

Technischer Identifier	Beschreibung
Information	Informationen für nicht befugte Nutzer
Devices	Management der registrierten Geräte eines Nutzers

3576

### 3577 **A\_21211-01 - Legal Policy - Änderungen der Legal Policy nicht erlauben**

3578 Das **ePA**-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass  
 3579 Änderungen der Konfiguration der Legal Policy gemäß A\_19303-\* ausgeschlossen  
 3580 sind. [ $\leq$ ]

### 3581 **A\_24548 - Legal Policy - Durchsetzung der Zugriffsrechte der Legal Policy**

3582 Das **ePA**-Aktensystem MUSS sicherstellen, dass Operationen auf Daten und Operationen  
 3583 der Dienste eines Aktenkontos abgebrochen und mit einer Fehlermeldung beendet  
 3584 werden, wenn diese Operation durch die Vorgaben der Legal Policy gemäß A\_19303-\* für  
 3585 die Nutzergruppe des Aufrufers der Operation nicht zulässig ist. [ $\leq$ ]

## 3586 **3.11 Constraint Management**

3587 Das Constraint Management des Aktenkontos stellt sicher, dass nur Zugriffe auf Daten in  
 3588 Ordnern des XDS Document Service über die Vorgaben der Legal Policy hinaus  
 3589 zugelassen werden, welche nicht vom Versicherten oder einem Vertreter unterbunden  
 3590 (verborgen) wurden.

3591 Die Umsetzung dieser Beschränkungen erfolgt anhand der **General Deny Policy** für  
 3592 jeden befugten Nutzer der betroffenen Nutzergruppen des Aktenkontos.

3593 Die General Deny Policy adressiert Nutzergruppen (professionOID) und Metadaten  
 3594 der Daten. Es können einzelne Dokumente, Kategorien oder Ordner verborgen werden.  
 3595 Bei jedem Zugriff auf Daten in Ordnern wird diese Policy bezüglich der Rolle eines  
 3596 Nutzers und der betroffenen Dokumente ausgewertet und durchgesetzt.

3597 Die folgende Anforderung zeigt eine Übersicht der Nutzergruppen, für welche Dokumente  
 3598 durch Einträge in der General Deny Policy vor einem Zugriff verborgen werden können.

### 3599 **A\_24306-02 - Constraint Management - Policy für berechnigte Nutzergruppen und Nutzer**

3600 Das Constraint Management MUSS die Konfiguration der General Deny Policy auf die  
 3601 folgenden Nutzergruppen einschränken:  
 3602  
 3603

Nutzergruppe [professionOID] der General Deny Policy
oid_praxis_arzt
oid_krankenhaus
oid_institution-vorsorge-reha
oid_zahnarztpraxis

Nutzergruppe [professionOID] der General Deny Policy
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

3604  
3605  
3606

[<=]

3607

#### **A\_24390-01 - Constraint Management- Anwendung der General Deny Policy**

3608 Das Constraint Management MUSS bei jedem Zugriff auf Daten durch den XDS Document  
3609 Service durch befugte Nutzer oder Nutzergruppen die General Deny Policy anwenden und  
3610 den Zugriff verhindern, wenn ein Dokument oder dessen assoziierter Ordner oder dessen  
3611 assoziierte Datenkategorie in der Policy konfiguriert ist.

3612  
3613

[<=]

3614 Dienste des Aktenkontos (Basic Services) können nicht verborgen werden. Hier gelten die  
3615 Zugriffsregelungen gemäß Legal Policy und die Beschränkungen der Schnittstellen.

3616 Datendienste (Medication Service) können nicht auf Daten- oder Ordner Ebene verborgen  
3617 werden. Hier gelten die Regelungen bezüglich des Widerspruchs gegen die Nutzung von  
3618 widerspruchsfähigen Funktionen der ePA (siehe 3.8- Consent Decision Management ).

3619 Die Kategorie "emp", bzw. einzelne Dokumente dieser Kategorie, des XDS Document  
3620 Service dürfen nicht verborgen werden. Die Nutzung der Dokumente der Kategorie "emp"  
3621 wird über das Consent Decision Management, bzw. einen erteilten Widerspruch gegen die  
3622 widerspruchsfähige Funktion "medication" der ePA verhindert (siehe 3.8- Consent  
3623 Decision Management).

3624 Die Operationen der Schnittstelle des Constraint Managements erlauben die  
3625 Konfiguration der General Deny Policy durch den Versicherten oder einen befugten  
3626 Vertreter.



3627 **A\_24395 - Constraint Management - Realisierung der Schnittstelle**

3628 **I\_Constraint\_Management\_Insurant**

3629 Das Constraint Management MUSS die Operationen der Schnittstelle

3630 I\_Constraint\_Management\_Insurant gemäß [I\_Constraint\_Management\_Insurant]

3631 umsetzen.[<=]

3632 **A\_24887-01 - Constraint Management - Protokolleinträge für Zugriffe auf das**  
 3633 **Constraint Management**

3634 Das Constraint Management MUSS für das Aufnehmen und Löschen von Einträgen in die  
 3635 General Deny Policy jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen. Dabei ist  
 3636 folgende Wertbelegung zu berücksichtigen:

3637 **Tabelle 21: 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 Ordern)
AuditEvent.action	C, D		
AuditEvent.entity.name	"GeneralDenyPolicy"		Eintrag für das Aufnehmen(Create) von Einträgen in die oder Löschen (Delete) von Einträgen aus der General Deny Policy
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"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

Strukturelement	Wert		Erläuterung
	"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

[<=]

Für die Policy gelten folgende Vorgaben.

#### **A\_24393-01 - Constraint Management - Initialisierung der General Deny Policy**

Das Constraint Management MUSS für ein Aktenkonto eine General Deny Policy ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policy über die Schnittstelle `I_Constraint_Management_Insurant` gemäß `[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.

- 3666 Die Konfiguration der General Deny Policy erfolgt durch den Versicherten oder einen  
3667 befugten Vertreter mittels ePA-FdV. Einträge können hinzugefügt oder entfernt werden.  
3668 Zum Zeitpunkt der Erstellung des Aktenkontos enthält die General Deny Policy keine  
3669 Einträge.
- 3670 Ein Eintrag in der General Deny Policy referenziert entweder ein bestimmtes Dokument,  
3671 einen dynamischen Ordner oder eine Datenkategorie. Die Menge der Einträge ist nicht  
3672 limitiert.
- 3673 Jeder Eintrag der General Deny Policy verbirgt die betroffenen Daten und verhindert  
3674 deren Nutzung - durch Nutzergruppen gemäß A\_24306-\*. Enthält ein Eintrag der Policy  
3675 einen dynamischen Ordner oder eine Kategorie, so werden alle in diesem Ordner bzw.  
3676 Kategorie enthaltenen Daten verborgen und von der Nutzung ausgeschlossen. Ein  
3677 dynamischer Ordner selbst wird ebenfalls verborgen und von der Nutzung  
3678 ausgeschlossen, eine Kategorie selbst wird nicht verborgen. Verborgene Daten schränken  
3679 die Anwendung der Datenoperationen ein, die konkreten Auswirkungen sind bei den  
3680 jeweiligen Operationen definiert.
- 3681 Beim kategorienbasierten Verbergen von dynamischen Ordnern kann ein einzelner  
3682 Ordner oder die Datenkategorie an sich verborgen werden. In letzterem Fall werden alle  
3683 assoziierten Ordner verborgen.
- 3684 Bei Kategorien und Ordnern, die zusammengesetzte MIOs oder strukturierte Dokumente  
3685 enthalten (MIOs oder strukturierte Dokumente, deren Inhalt über mehrere XDS  
3686 Dokumente mit Zusammenhang verteilt ist - "Passdokumente") ist das Verbergen  
3687 einzelner XDS Dokumente des MIOs nicht sinnvoll und daher nicht zulässig. In diesen  
3688 Fällen erfolgt das Verbergen der Daten durch das Verbergen der Kategorie bzw. des  
3689 dynamischen Ordners. Diese Einschränkung betrifft die Sammlungstypen "mixed" und  
3690 "uniform".
- 3691 Für das erfolgreiche Verbergen von Daten durch Einträge der General Deny Policy muss  
3692 das adressierte XDS Dokument, der Ordner oder die Kategorie im Aktensystem  
3693 vorhanden sein. Wird im Verlauf von Operationen ein XDS Dokument oder ein Ordner  
3694 gelöscht, so werden auch die referenzierenden Policy-Einträge automatisch entfernt  
3695 (siehe A\_24461-\* und A\_24662-\*).
- 3696 Ein Eintrag der General Deny Policy enthält Angaben gemäß der folgenden Tabelle:  
3697 **Tabelle 22: Inhalt eines General Deny Policy Eintrags**

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

Element		Inhalt	Erläuterung
[choice]	folderUUID	folder.entryUUID	Identifiziert des zu verbergenden dynamischen Ordners
	categoryId	categoryId	technischer Identifizier der zu verbergenden Kategorie

3698

3699 Beispiel:

3700 **Tabelle 23: Verbergen eines Medical Service**

**General Deny Policy - Verbergen der Datenkategorie "Zahnbonusheft"dental"  
(Daten aus der zahnärztlichen Dokumentation)**

denyType		"category"
parameters:		
	categoryId	"dental"

### 3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes

Das Verbergen über den confidentialityCode ist im Kontext der Operationen des XDS Document Service definiert und in 3.13.1.10- Verbergen von Dokumenten durch Verwendung des confidentialityCode beschrieben.

3706

## 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

- 3721 Schnittstelle, über die die durch das Home-AS signierte Geräteinformationen abgerufen  
3722 werden können.
- 3723 Bei erstmaliger Nutzung des Gerätes initiiert das ePA-FdV die Geräteregistrierung und  
3724 erhält dadurch eine DeviceID (bestehend aus deviceIdentifier und deviceToken), welche  
3725 bei folgenden Verwendungen des ePA-FdV zur Identifizierung des Geräts verwendet wird.  
3726 Eine neue Geräteregistrierung muss durch den Nutzer bestätigt werden. Der Zugriff auf  
3727 ein Aktenkonto kann nur mit einem Gerät mit bestätigter Geräteregistrierung erfolgen.
- 3728 Das Device Management ermittelt dazu die für den Nutzer im ePA-Aktensystem  
3729 hinterlegte E-Mail-Adresse und versendet bei der Geräteregistrierung eine E-Mail an den  
3730 Nutzer mit einem generierten Geräteregistrierungscode (confirmationCode). Der Nutzer  
3731 sendet den Geräteregistrierungscode unter Verwendung des ePA-FdV zurück an das  
3732 Device Management und bestätigt dadurch die Registrierung des neuen Geräts. Das  
3733 Gerät kann nach der Bestätigung uneingeschränkt mit einem Aktenkonto genutzt  
3734 werden.
- 3735 **A\_24828 - Device Management - Realisierung der Schnittstelle**  
3736 **I\_Device\_Management\_Insurant**  
3737 Das Device Management MUSS die Operationen der Schnittstelle  
3738 I\_Device\_Management\_Insurant gemäß [I\_Device\_Management\_Insurant]  
3739 umsetzen.[<=]
- 3740 **A\_25164 - Device Management - Beschränkung der Schnittstellenoperationen**  
3741 **auf Geräte des Nutzers**  
3742 Das Device Management MUSS die Operationen der Schnittstelle  
3743 I\_Device\_Management\_Insurant gemäß [I\_Device\_Management\_Insurant] auf die  
3744 Geräte des aufrufenden Nutzers einschränken.[<=]
- 3745 **A\_26153 - Device Management - Nutzen von Device Management auch bei**  
3746 **Widerspruch gegen Aktenkonto**  
3747 Das Device Management MUSS sicherstellen, dass das Device Management auch von  
3748 Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben.[<=]
- 3749 **A\_26154 - ePA-Aktensystem - Ausschließlich Nutzen von Email Management**  
3750 **und Device Management bei Widerspruch**  
3751 Das ePA-Aktensystem MUSS sicherstellen, dass Versicherte, die einem Aktenkonto  
3752 widersprochen haben, ausschließlich das Email Management und das Device Management  
3753 nutzen können.[<=]
- 3754 **A\_26155 - Device Management - Versicherte nutzen Device Management**  
3755 **ausschließlich im Home-AS**  
3756 Das Device Management des ePA-Aktensystems MUSS sicherstellen, dass das Device  
3757 Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-  
3758 Aktensystem das Home-AS ist.[<=]
- 3759 **A\_24979 - Device Management - Sicheres Löschen von Geräten**  
3760 Das Device Management MUSS beim Entfernen eines Gerätes sicherstellen, dass das  
3761 Gerät gelöscht ist und dass das Gerät nicht mehr als verifiziertes Gerät genutzt werden  
3762 kann. [<=]
- 3763 **A\_17947-03 - Device Management - Gültigkeitszeitraum und Löschung der**  
3764 **Devicekennung**  
3765 Das Device Management MUSS jede generierte und zu einem Nutzer gespeicherte  
3766 Geräteregistrierung nach 2 Jahren löschen und darf Nutzeranfragen mit dieser Device-  
3767 Kennung nach diesem Zeitpunkt nicht mehr akzeptieren.  
3768 [<=]

3769 Hinweis zu A\_17947-\*: Der Hersteller des ePA-FdVs kann die Nutzerführung seines ePA-  
3770 FdVs so gestalten, dass der Versicherte auf ein baldiges Auslaufen der Registrierung  
3771 hingewiesen wird und automatisch eine neue Registrierung vom ePA-FdV am  
3772 Aktensystem ausgelöst wird.  
3773

#### 3774 **A\_14595-02 - Device Management - Pflegeprozess Geräteverwaltung**

3775 Das Device Management MUSS die interne Liste aller bekannten Geräte derart pflegen,  
3776 dass ein Gerät nach spätestens 1 Jahr nach der letzten Nutzung des Gerätes automatisch  
3777 aus der Liste der registrierten Geräte gelöscht wird. [ $\leq$ ]

3778 Hinweis zu A\_14595-\*: Der Abruf einer Device Attestation durch ein registriertes Gerät  
3779 gilt ebenfalls als eine Nutzung dieses Geräts.

#### 3780 **A\_25270 - Device Management - Erzeugung von Geräteinformationen und** 3781 **Geräteregistrierungscode bei der Geräteregistrierung**

3782 Das Device Management MUSS bei der Geräteregistrierung für das zu registrierende  
3783 Gerät eines Nutzers

- 3784 • einen deviceIdentifizier als aktensystemweit eindeutigen Gerätebezeichner (uuid),
- 3785 • ein deviceToken als eine Zufallszahl als String mit 64 Zeichen mit einer  
3786 Mindestentropie von 120 Bit gemäß [gemSpec\_Krypt#GS-A\_4367] und
- 3787 • eine zufällige sechsstellige natürliche Zahl als Geräteregistrierungscode

3788 erzeugen. [ $\leq$ ]

#### 3789 **A\_25271-01 - Device Management - Speicherung der Geräteinformationen**

3790 Das Device Management MUSS bei einer Geräteregistrierung eines Geräts eines Nutzers  
3791 folgende Inhalte für den Nutzer verschlüsselt persistieren:

- 3792 • deviceIdentifizier
- 3793 • deviceToken
- 3794 • createdAt (Zeitpunkt der Erzeugung des deviceTokens)
- 3795 • lastUse
- 3796 • status
- 3797 • displayName
- 3798 • Geräteregistrierungscode,
- 3799 • Fehlerzähler.

3800 [ $\leq$ ]

3801 Hinweis zu A\_25271-\*: Für die verschlüsselte Speicherung der Geräteinformationen sind  
3802 die Anforderungen aus Abschnitt 3.5.1.3 zu berücksichtigen.

#### 3803 **A\_25272 - Device Management - Pseudonyme Speicherung der** 3804 **Geräteinformationen**

3805 Das Device Management MUSS sicherstellen, dass die Zuordnung der außerhalb der VAU  
3806 persistierten verschlüsselten Geräteinformationen zum Nutzer eindeutig ist und durch ein  
3807 Pseudonym erfolgt. [ $\leq$ ]

3808 Hinweis: Aus A\_25272 folgt, dass die Zuordnung der Speicherung der verschlüsselten  
3809 Geräteinformationen nicht über die KVN-R des Nutzers erfolgen darf.

#### 3810 **A\_25273 - Device Management - Gültigkeitsdauer des** 3811 **Geräteregistrierungscodes**

3812 Das Device Management MUSS sicherstellen, dass der bei der Geräteregistrierung  
3813 erzeugte Geräteregistrierungscode maximal 6 Stunden nach Erzeugung der DeviceID  
3814 (createdAt) für die Verifikation eines Gerätes genutzt werden kann. [≤]

3815 **A\_25274 - Device Management - Löschen nach Gültigkeitsdauer des**  
3816 **Geräteregistrierungscodes**

3817 Das Device Management MUSS sicherstellen, dass die Geräteinformationen für eine nicht  
3818 bestätigte Geräteregistrierung nach Ende der Gültigkeitsdauer des  
3819 Geräteregistrierungscodes gelöscht werden. [≤]

3820 **A\_25275 - Device Management - Versenden des Geräteregistrierungscodes per**  
3821 **E-Mail**

3822 Das Device Management MUSS bei der Geräteregistrierung für den Nutzer, für den das  
3823 Gerät registriert werden soll, alle im Aktensystem hinterlegten E-Mail-Adressen ermitteln  
3824 und an alle ermittelten E-Mail-Adressen eine E-Mail in einer für den Nutzer verständlichen  
3825 Form mit folgenden Informationen versenden:

- 3826 • Zweck der E-Mail,
- 3827 • Geräteregistrierungscode,
- 3828 • Gültigkeitsdauer des Geräteregistrierungscodes.

3829 [≤]

3830 **A\_25276 - Device Management - Bestätigung mittels**  
3831 **Geräteregistrierungscodes**

3832 Das Device Management MUSS für einen übergebenen Geräteregistrierungscode und eine  
3833 übergebene DeviceID (deviceIdentifier und deviceToken) prüfen, ob der vom Device  
3834 Management bei der Geräteregistrierung erzeugte Geräteregistrierungscode für das  
3835 angegebene Gerät (deviceIdentifier, deviceToken) mit dem übergebenen  
3836 Geräteregistrierungscode übereinstimmt sowie der Geräteregistrierungscode zeitlich  
3837 gültig ist und

- 3838 1. bei Gleichheit und
  - 3839 a. zeitlicher Gültigkeit
    - 3840 • den Status für die Geräteregistrierung wechseln, so dass die erfolgreiche
    - 3841 Bestätigung des Geräts aus dem Status hervorgeht,
    - 3842 • den Geräteregistrierungscode und den Fehlerzähler aus den
    - 3843 Geräteinformationen löschen und
    - 3844 • den Zeitpunkt der erfolgreichen Bestätigung in lastUsed erfassen,
  - 3845 b. zeitlicher Ungültigkeit
    - 3846 • alle Geräteinformationen zu diesem deviceIdentifier löschen,
- 3847 2. bei Ungleichheit den Fehlerzähler der Geräteinformation um eins erhöhen und
  - 3848 • falls der Fehlerzähler größer oder gleich fünf ist,
  - 3849 • alle Geräteinformationen zu diesem Gerät löschen.

3850 [≤]

3851 **A\_25277 - Device Management - Sperrung bei vermehrter Anzahl von**  
3852 **abgebrochenen Geräteregistrierungen**

3853 Falls für einen Nutzer innerhalb von 8 Stunden drei Geräteregistrierungen abgebrochen  
3854 werden mussten, MUSS das Device Management sicherstellen, dass dieser Nutzer für 8  
3855 Stunden ab dem Zeitpunkt der dritten abgebrochenen Geräteregistrierung keine Geräte  
3856 mehr registrieren darf. [≤]



**A\_25291 - ePA-Aktensystem - Health Record Context nur mit verifizierten Gerät**

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

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

**A\_26157 - Device Management - Device Attestation kann nur mit verifiziertem Gerät abgerufen werden**

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

**A\_26156 - Device Management - Inhalte der Device Attestation**

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

Attribut	Inhalt
actorId	KVNR aus dem ID-Token des angemeldeten Nutzers (bzw. der User Session)
iat	Zeitstempel Ausgabezeitpunkt
exp	Verfalldatum, = "iat" + 2 Stunden

[<=]

**A\_26158 - Device Management - Signatur der Device Attestation**

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

**3.13 Medical Services****A\_25830-02 - Medical Services - Reihenfolge der Auswertung Legal Policy, Consent Decisions und Constraints**

Die Medical Services MÜSSEN bei der Ausführung von Operationen der Schnittstellen der Medical Services sicherstellen, dass die Prüfung zu Bedingungen

1. der Einschränkung der Rolle des Aufrufenden (oid),
2. der Existenz des Aktenkontos (Status UNKNOWN oder INITIALIZED),
3. des Zustands des Aktenkontos (Status ACTIVATED),
4. der Befugnis des Aufrufenden,
5. der Legal Policy,
6. der Entscheidungen zu widerspruchsfähigen Funktionen der ePA,

- 3892 7. der Einträge der General Deny Policy
- 3893 8. des Entscheidungen zum nutzerspezifischen Ausschluss von der Teilnahme am
- 3894 digital gestützten Medikationsprozess

3895 in der dargestellten Reihenfolge erfolgt. Diese Reihenfolge MUSS auch eingehalten

3896 werden, wenn einzelne Prüfungen für eine Operation nicht anwendbar, bzw. nicht

3897 relevant, sind. [ $\leq$ ]

3898 *Hinweis: Eine Operation kann nicht erfolgreich ausgeführt werden, weil dieses der Legal*

3899 *Policy widerspricht und weil ein Eintrag der General Deny Policy die Ausführung*

3900 *verhindert. Die Fehlermeldung zum Abbruch der Operation resultiert dann aus der*

3901 *Prüfung der Legal Policy, da die Bedingungen dieser gemäß der definierten Reihenfolge*

3902 *vor den Bedingungen der General Deny Policy geprüft werden müssen.*

### 3903 3.13.1 XDS Document Service

3904 Die gesetzlichen Vorgaben schränken den Zugriff Dritter auf Dokumente

3905 über berufsgruppenspezifische Vorgaben gemäß § 341 Absatz 2 SGB V ein. Dazu

3906 verwendet der XDS Document Service festgelegte Datenkategorien, welche mit

3907 spezifischen Zugriffsrechten der grundlegenden Zugriffsoperationen (CRUD - create,

3908 read, update, delete) wirken.

3909 Jedes eingestellte Dokument wird vom XDS Document Service mit einer automatischen

3910 Zuordnung zu einem statischen Ordner, welcher die Datenkategorie repräsentiert,

3911 erweitert. Diese statischen Ordner sind initial bei jedem Aktenkonto eines Versicherten

3912 existent. Die serverseitige Zuordnung in diese Ordner erfolgt anhand der XDS-Metadaten

3913 in Kombination mit der Nutzergruppe des Einstellers.

3914 Das bedeutet weiterhin, dass das Anlegen von statischen Ordnern durch ePA-Clients nicht

3915 erlaubt ist, um eine zweifelsfreie Anwendung der Zugriffsregeln auf Grundlage der

3916 Datenkategorien zu gewährleisten.

3917 Eine Ausnahme bilden bestimmte medizinische Informationsobjekte (MIOs), die eine

3918 weitere Gruppierung innerhalb der zugeordneten Datenkategorie erfordern. Ein Beispiel

3919 dafür ist der Mutterpass. Die Dokumente eines Mutterpasses müssen für die konkrete

3920 Schwangerschaft innerhalb der Kategorie separiert werden. Für die betroffenen

3921 Kategorien wird daher kein statischer Ordner vorbereitet, sondern der separierende,

3922 dynamische Ordner muss zeitgleich mit einer Dokumentenregistrierung durch den ePA-

3923 Client angelegt werden,

3924 ePA-Clients, die Dokumente für MIOs einstellen, können die dem MIO zugeordnete

3925 Kategorie und die Art des Ordners (statisch, dynamisch) aus den Metadatenvorgaben für

3926 MIOs gemäß [Implementation-Guidelines] entnehmen.

3927 Die Durchsetzung der Zugriffskontrolle auf die Kategorien, Ordner und Dokumente

3928 gemäß der gesetzlichen Vorgaben und ggf. weiterer Beschränkungen durch den

3929 Versicherten oder einen Vertreter erfolgt durch das Constraint Management (siehe 3.11.-

3930 Constraint Management ).

#### 3931 3.13.1.1 Formatprüfung beim Einstellen von Dokumenten

##### 3932 A\_25233 - XDS Document Service - erlaubte Formate für PDF-Dokumente

3933 Der XDS Document Service MUSS sicherstellen, dass ausschließlich die folgenden PDF/A-

3934 Formate unterstützt werden:

- 3935 • PDF/A-1a
- 3936 • PDF/A-1b

- 3937 • PDF/A-2a
- 3938 • PDF/A-2u
- 3939 • PDF/A-2b

3940 [~~<=~~]

#### 3941 **AA\_24864-0204 - XDS Document Service - Prüfen auf zulässiges Format beim** 3942 **Einstellen von Dokumenten**

3943 Der XDS Document Service MUSS beim Einstellen eines Dokumentes prüfen, dass das  
 3944 Dokument eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und den  
 3945 in Klammern angegebenen Dateiendungen (DocumentEntry.URI) besitzt

- 3946 • application/pdf nur PDF/A gemäß A\_25233 (pdf)
- 3947 ~~• image/jpeg (jpeg oder jpg)~~
- 3948 ~~• image/png (png)~~
- 3949 ~~• image/tiff (tiff)~~
- 3950 • text/plain (txt)
- 3951 • application/xml (xml)
- 3952 • application/hl7-v3 (xml)
- 3953 • application/pkcs7-mime (~~p7s~~ oder p7)
- 3954 • application/fhir+xml (xml)
- 3955 • application/fhir+json (json)
- 3956 • application/json (json)

3957 sowie der tatsächliche Inhalt des Dokuments konform mit dem behaupteten MIME-Type  
 3958 ist. Falls die Prüfung nicht erfolgreich ist, muss das Einstellen des Dokumentes abgelehnt  
 3959 werden-

3960 ~~{<=}~~. [~~<=~~]

3961 ~~Hinweis~~*Hinweise* zu A\_24864-~~--~~\*:

- 3962 • *Dokumente im PDF-Format werden vom XDS Document Service abgelehnt, da sie*  
 3963 *ausführbaren Code enthalten können. Daher müssen die Clients, falls sie*  
 3964 *Dokumente im PDF-Format einstellen wollen, diese zunächst in ein PDF/A*  
 3965 *konvertieren.*
- 3966 • *p7s ist die Default-Dateiendung für Dokumente des mimetypes application/pkcs7-*  
 3967 *mime in der ePA und für Dokumente dieses mimetypes gemäß*  
 3968 *[gemSpec IG ePA] und für automatisierte Anpassungen von filename extensions*  
 3969 *bei Dokumentenupload (A\_23447-\*, A\_24451-\*) zu berücksichtigen.*

3970

#### 3971 **AA\_25009-0203 - XDS Document Service - Prüfen auf zulässiges Format beim** 3972 **Einstellen von Dokumenten durch Versicherte**

3973 Der XDS Document Service MUSS sicherstellen, dass Versicherte ausschließlich  
 3974 Dokumente eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und  
 3975 den in Klammern angegebenen Dateiendungen (DocumentEntry.URI) einstellen können:

- 3976 • application/pdf nur PDF/A gemäß A\_25233 (pdf)
- 3977 ~~• image/jpeg (jpeg oder jpg)~~
- 3978 ~~• image/png (png)~~

~~image/tiff (tiff)~~

- 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.

[<=]

Hinweis zu A\_24867-\*:

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

Der in A\_24636-\* geforderte technische Separationsmechanismus zur Isolation von Health Record Contexten innerhalb einer VAU-Instanz kann ebenfalls zur Isolation der Formatprüfung in A\_24867-\* genutzt werden.

Findet eine Dokumentenformatprüfung innerhalb eines Health Record Context statt, wird durch den Isolationsmechanismus aus A\_24636-\* verhindert, dass sich die Dokumentenformatprüfung schadhaft auf andere Health Record Contexte auswirkt. Es verbleibt dann zur Umsetzung der A\_24867-\* noch zu gewährleisten, dass sich die Dokumentenformatprüfung nicht schadhaft auf den Health Record Context auswirkt, in dem die Dokumentenformatprüfung erfolgt.

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

Ein Ausschluss einer schadhaften Auswirkung auf den Health Record Context ist bei folgenden Prüfungen des Dokumentenformats denkbar, so dass diese innerhalb des Health Record Contexts ohne zusätzliche Isolationsmaßnahmen durchgeführt werden können und kein Verstoß gegen die Anforderung A\_24867-\* vorliegt:

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

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

#### **A\_25285 - XDS Document Service - Sicheres Löschen von Dokumenten mit unzulässigem Format**

Falls der XDS Document Service bei der Prüfung des Dateiformats (siehe A\_24864-\*) beim Einstellen eines Dokuments ein unzulässiges Format erkennt, MUSS der XDS Document Service das Dokument sicher löschen.

[<=]

#### **A\_24943 - XDS Document Service - Formatprüfung exponiert keine Daten aus der VAU heraus**

Der XDS Document Service MUSS sicherstellen, dass bei der Formatprüfung (siehe A\_24864-\*) keine innerhalb der VAU verarbeiteten Daten die VAU verlassen.[<=]

### **3.13.1.2 Anforderungen zur Validierung**

#### **A\_15035 - XDS Document Service – Verwendung von SOAP Message Security 1.1**

Der XDS Document Service MUSS die Sicherheitsanforderungen aus SOAP Message Security 1.1 [WSS] für die Verarbeitung von SOAP 1.2-Nachrichten umsetzen.[<=]

#### **A\_15034 - XDS Document Service – Unterstützung von Profilen der Web Services Interoperability Organization (WS-I)**

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

#### **A\_15186 - XDS Document Service – Prüfung der Kombination von WS-Addressing Action und SOAP Body**

4071 Der XDS Document Service MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-  
 4072 Eingangsnachrichten dahingehend prüfen, ob die angegebene WS-Addressing Action zum  
 4073 SOAP Body passt. Ist diese Kombination nicht passend, MUSS der XDS Document Service  
 4074 die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und die  
 4075 Verarbeitung der Nachricht abbrechen. [≤]

#### 4076 **A\_15585 - XDS Document Service – Gleichheit von SOAP Action und WS- 4077 Addressing Action**

4078 Der XDS Document Service MUSS SOAP 1.2-Eingangsnachrichten mit einem HTTP-  
 4079 Statuscode 400 gemäß [RFC7231] quittieren und die Verarbeitung der Nachricht  
 4080 abbrechen, falls die Werte aus SOAP Action (HTTP Header) und des `Action`-Elements  
 4081 [WSA] des SOAP Headers nicht übereinstimmen. [≤]

#### 4082 **A\_14465-01 - XDS Document Service – XML Schema-Validierung für SOAP- 4083 Eingangsnachrichten**

4084 Der XDS Document Service MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-  
 4085 Eingangsnachrichten einer XML Schema-Validierung auf Basis ausschließlich intern  
 4086 vorliegender XML Schema-Definitionen unterziehen und gemäß [SOAP] verarbeiten. Sind  
 4087 Nachrichten nicht wohlgeformt oder ungültig, MUSS der XDS Document Service die  
 4088 Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren. [≤]

#### 4089 **A\_14809 - XDS Document Service – Keine Verwendung des 4090 "xsi:schemaLocation"-Attributs**

4091 Der XDS Document Service MUSS SOAP 1.2-Eingangsnachrichten mit einem HTTP-  
 4092 Statuscode 400 gemäß [RFC7231] quittieren, falls ein `xsi:schemaLocation`-Attribut  
 4093 gemäß [XMLSchema#2.6.3] enthalten ist. [≤]

4094

#### 4095 **A\_14811-01 - XDS Document Service – Ablehnung von SOAP 1.2-Nachrichten 4096 ohne UTF-8 Kodierung**

4097 Der XDS Document Service MUSS SOAP 1.2-Nachrichten dahingehend prüfen, dass diese  
 4098 der Zeichenkodierung UTF-8 entsprechen, und andernfalls die Operation einem  
 4099 geeigneten HTTP-Statuscode gemäß [RFC7231] ablehnen. [≤]

#### 4100 **A\_21200 - XDS Document Service und Clients – UTF-8 Kodierung von SOAP 1.2- 4101 Nachrichten**

4102 Der XDS Document Service und Clients des XDS Document Service MÜSSEN  
 4103 sicherstellen, dass die XML-Inhalte der SOAP 1.2-Nachrichten, die sie senden, der  
 4104 Zeichenkodierung UTF-8 entsprechen. [≤]

4105 Es ist zu beachten, dass sich die Anzeige der verwendeten Kodierung in der Nachricht  
 4106 unterscheiden kann, z. B. in Nachrichten, in denen MTOM verwendet wird.

### 4107 **3.13.1.3 Namensräume**

4108 Für die Spezifikation der Schnittstellen des XDS Document Service werden die folgenden  
 4109 XML-Präfixe verwendet, um den Namensraum bzw. das Vokabular des XML-Dokuments  
 4110 zu kennzeichnen.

Präfix	Namensraum
lcm	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0



Präfix	Namensraum
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

#### 4111 **3.13.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und** 4112 **Abruf von Dokumenten**

##### 4113 3.13.1.4.1 Anforderungen an IHE ITI-Akteure

4114 In diesem Abschnitt werden Anforderungen und Einschränkungen an relevante IHE ITI-  
4115 Akteure und -Transaktionen des XDS Document Service gestellt, um die geforderte IHE  
4116 ITI-Semantik zum ePA-Aktensystem zu bewahren. Werden IHE ITI-Akteure mit weiteren  
4117 Sub-Akteuren gruppiert, so werden die Anforderungen der Sub-Akteure zum gruppierten  
4118 Akteur übernommen. Eine Übersicht und Herleitung der IHE ITI-Akteure ist 3.13.1.4.2-  
4119 Überblick über gruppierte IHE ITI-Akteure und Optionen zu entnehmen.

4120 *Hinweis: Alle spezifizierten Anforderungen der IHE ITI-Akteure definieren das zu*  
4121 *implementierende Verhalten an den*  
4122 *Außenschnittstellen I\_Document\_Management sowie I\_Document\_Management\_Insurant.*  
4123

#### 4124 **A\_17826-01 - XDS Document Service – Außenverhalten der IHE ITI-** 4125 **Implementierung**

4126 Der XDS Document Service DARF NICHT vom Verhalten der definierten  
4127 Außenschnittstellen

4128 I\_Document\_Management, sowie I\_Document\_Management\_Insurant aus Abschnitt  
4129 3.13.1.6 abweichen. Dies schließt über die Anforderungslage  
4130 hinausgehende Implementierungen von IHE ITI-Akteuren und Optionen innerhalb  
4131 des XDS Document Service mit ein, sodass zusätzlich implementierte IHE-  
4132 Funktionalitäten keine Auswirkungen an den definierten Außenschnittstellen aufweisen  
4133 dürfen. [≤]



- 4134 **A\_13806 - XDS Document Service – Implementierung des IHE ITI-Akteurs XDS**  
4135 **Document Registry**  
4136 Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Registry"  
4137 gemäß [IHE-ITI-TF1] implementieren. [≤]
- 4138 **A\_14727 - XDS Document Service – Implementierung des IHE ITI-Akteurs XDS**  
4139 **Document Repository**  
4140 Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Repository"  
4141 gemäß [IHE-ITI-TF1] implementieren. [≤]
- 4142 Die § 291a-konforme Protokollierung von Zugriffen erfolgt mit Mechanismen außerhalb  
4143 des IHE ITI-TF. Eine technische Protokollierung via ATNA kann gemäß der Anforderung  
4144 A\_17826 dennoch erfolgen.
- 4145 **A\_13809 - XDS Document Service – Keine Implementierung des IHE ITI-**  
4146 **Akteurs ATNA Audit Record Repository**  
4147 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "ATNA Audit Record  
4148 Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]
- 4149 Die Mechanismen der IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure  
4150 Application" zur Node Authentication werden über das Konzept "Vertrauenswürdige  
4151 Ausführungsumgebung" (siehe 3.5- Vertrauenswürdige Ausführungsumgebung (VAU))  
4152 umgesetzt, sodass die Nutzung des Integrationsprofils ATNA diesbzgl. eingeschränkt  
4153 wird.
- 4154 **A\_17166 - XDS Document Service – Keine Implementierung der IHE ITI-**  
4155 **Akteure ATNA Secure Node sowie ATNA Secure Application für Node**  
4156 **Authentication**  
4157 Der XDS Document Service DARF zur Node Authentication die IHE ITI-Akteure "ATNA  
4158 Secure Node" sowie "ATNA Secure Application" gemäß [IHE-ITI-TF1] NICHT  
4159 implementieren. [≤]
- 4160 Der Zeitdienst der Telematikinfrastruktur unterstützt das Network Time Protocol in  
4161 Version 4. Das IHE ITI-TF verlangt hingegen, das Zeitsynchronisierungsprotokoll in  
4162 Version 3.
- 4163 **A\_14654 - XDS Document Service – Keine Implementierung des IHE ITI-**  
4164 **Akteurs CT Time Client**  
4165 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "CT Time Client"  
4166 gemäß [IHE-ITI-TF1] implementieren. [≤]
- 4167 **A\_14665 - XDS Document Service – Keine Implementierung des IHE ITI-**  
4168 **Akteurs XDS Document Source**  
4169 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XSDocument Source"  
4170 gemäß [IHE-ITI-TF1] implementieren. [≤]
- 4171 **A\_14667 - XDS Document Service – Keine Implementierung des IHE ITI-**  
4172 **Akteurs XDS Integrated Document Source/Repository**  
4173 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Integrated Document  
4174 Source/Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]
- 4175 **A\_14668 - XDS Document Service – Keine Implementierung des IHE ITI-**  
4176 **Akteurs XDS Document Consumer**  
4177 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Consumer"  
4178 gemäß [IHE-ITI-TF1] implementieren. [≤]
- 4179 **A\_14666 - XDS Document Service – Keine Implementierung des IHE ITI-**  
4180 **Akteurs XDS Patient Identity Source**

- 4181 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Patient Identity  
4182 Source" gemäß [IHE-ITI-TF1] implementieren.  
4183 [ $\leq$ ]
- 4184 **A\_14669 - XDS Document Service – Keine Implementierung des IHE ITI-  
4185 Akteurs XDS On-Demand Document Source**  
4186 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS On-Demand Document  
4187 Source" gemäß [IHE-ITI-TF1] implementieren.[ $\leq$ ]
- 4188 **A\_14950 - XDS Document Service – Keine Angabe einer Fehlerlokalisierung im  
4189 RegistryError-Element**  
4190 Der XDS Document Service DARF NICHT das location-Attribut im rs:RegistryError-  
4191 Element in der IHE ITI-Ausgangsnachricht verwenden, sofern ein Fehler bei der  
4192 Verarbeitung einer IHE ITI-Eingangsnachricht auftritt. Diese Einschränkung gilt nur für  
4193 Error Stack Traces bzw. der Offenbarung von Programmierdetails.[ $\leq$ ]
- 4194 **A\_15081 - XDS Document Service – Implementierung des IHE ITI-Akteurs RMU  
4195 Update Responder**  
4196 Der XDS Document Service MUSS den IHE ITI-Akteur "RMU Update Responder"  
4197 gemäß [IHE-ITI-RMU] implementieren.[ $\leq$ ]
- 4198 3.13.1.4.1.1 Gruppierungen mit anderen IHE ITI-Akteuren  
4199 **A\_15093-02 - XDS Document Service – Gruppierung RMU Update Responder mit  
4200 Document Registry**  
4201 Der XDS Document Service als RMU-Akteur "Update Responder" MUSS mit dem XDS-  
4202 Akteur "Document Registry" gemäß [IHE-ITI-RMU] gruppiert sein.[ $\leq$ ]
- 4203 3.13.1.4.1.2 Optionen des IHE ITI-Akteurs  
4204 **A\_15094 - XDS Document Service – RMU Update Responder ohne "Forward  
4205 Update"-Option**  
4206 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option  
4207 "Forward Update" unterstützen.  
4208 [ $\leq$ ]
- 4209 **A\_15095-02 - XDS Document Service – RMU Update Responder ohne "XCA  
4210 Persistence"-Option**  
4211 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option  
4212 "XCA Persistence" unterstützen.[ $\leq$ ]
- 4213 **A\_15096-02 - XDS Document Service – RMU Update Responder mit "XDS  
4214 Persistence"-Option**  
4215 Der XDS Document Service als RMU-Akteur "Update Responder" MUSS die Option "XDS  
4216 Persistence" unterstützen.[ $\leq$ ]
- 4217 **A\_15097 - XDS Document Service – RMU Update Responder ohne "XDS Version  
4218 Persistence"-Option**  
4219 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option  
4220 "XDS Version Persistence" unterstützen.[ $\leq$ ]
- 4221 3.13.1.4.1.3 Gruppierungen mit anderen IHE ITI-Akteuren  
4222 3.13.1.4.1.4 Optionen des IHE ITI-Akteurs  
4223 **A\_14637 - XDS Document Service – XDS Document Registry ohne  
4224 "Asynchronous Web Services Exchange"-Option**  
4225 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option  
4226 "Asynchronous Web Services Exchange" unterstützen.[ $\leq$ ]
- 4227 **A\_14638 - XDS Document Service – XDS Document Registry mit "Reference  
4228 ID"-Option**

- 4229 Der XDS Document Service als XDS-Akteur "Document Registry" MUSS die  
 4230 Option "Reference ID" unterstützen.[<=]
- 4231 **A\_14639 - XDS Document Service – XDS Document Registry ohne "Patient  
 4232 Identity Feed"-Option**  
 4233 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option  
 4234 "Patient Identity Feed" unterstützen.  
 4235 [<=]
- 4236 **A\_14640 - XDS Document Service – XDS Document Registry ohne "Patient  
 4237 Identity Feed HL7v3"-Option**  
 4238 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option  
 4239 "Patient Identity Feed HL7v3" unterstützen.[<=]
- 4240 **A\_14641 - XDS Document Service – XDS Document Registry ohne "On-Demand  
 4241 Documents"-Option**  
 4242 Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option  
 4243 "On-Demand Documents" unterstützen.[<=]
- 4244 3.13.1.4.1.5 Optionen des IHE ITI-Akteurs  
 4245 **A\_14636 - XDS Document Service – XDS Document Repository ohne  
 4246 "Asynchronous Web Services Exchange"-Option**  
 4247 Der XDS Document Service als XDS-Akteur "Document Repository" DARF NICHT die  
 4248 Option "Asynchronous Web Services Exchange" unterstützen.[<=]
- 4249

4250 *3.13.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen*

- 4251 Die folgende Tabelle fasst die oben definierten Anforderungen zu Gruppierungen und  
 4252 Optionen zusammen. Dabei wird die folgende Notation für Optionalitäten (Opt.)  
 4253 verwendet:

4254 **Tabelle 24: 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.

4255

4256  
4257

**Tabelle 25: 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				

4258

4259 3.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen

4260 **A\_17832 - XDS Document Service – Unterstützung MTOM/XOP**

4261 Der XDS Document Service MUSS gemäß den Anforderungen von [IHE-ITI-  
4262 TF2x#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP  
4263 [MTOM] verwenden.[<=]

4264 **A\_24524 - XDS Document Service - Migration, Upload: Normalisieren des URI**

4265 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten  
4266 den `DocumentEntry.URI` normalisieren. Dies gilt für `FileURI`, z. B. "  
4267 <file:///C:/path/to/file.html#anchor>" oder `"/C:/path/to/file.html#anchor"`. Die URI MUSS auf  
4268 den reinen Dateinamen mit Extension (d. h. ohne Pfadangaben) reduziert werden, z. B.  
4269 "file.html". Nach der Normalisierung MUSS eine Validierung der Extension  
4270 gemäß A\_23447-\* erfolgen.[<=]

4271 **A\_23447-01 - XDS Document Service - DocumentEntry.URI extension entspricht**  
4272 **mimetype**

4273 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten  
4274 das Metadatum `DocumentEntry.URI` daraufhin prüfen, ob `DocumentEntry.URI` eine  
4275 filename extension aufweist, die nicht dem `DocumentEntry.mimetype` entspricht. Zuvor  
4276 muss die URI mittels A\_24524-\* normalisiert worden sein. Danach MUSS der XDS  
4277 Document Service sicherstellen, dass in `Document.URI` die filename extension dem  
4278 `DocumentEntry.mimeType` entspricht. Im Falle einer Abweichung MUSS an die  
4279 ursprüngliche `DocumentEntry.URI` die filename extension gemäß A\_24864\*~~,-\*~~, bzw.  
4280 A\_25009\*~~,-\*~~ angehängt werden, die dem `mimeType` entspricht. Die Groß-  
4281 /Kleinschreibung der filename extension ist bei der Prüfung nicht relevant.[<=]

4282 **A\_24451-01 - XDS Document Service - Automatisches initiales Erzeugen einer**  
4283 **versionsübergreifenden ID für Dokumente**

4284 Der XDS Document Service MUSS beim initialen Einstellen eines Dokumentes die  
4285 `DocumentEntry.uniqueId` als Eintrag einer `ReferenceID` in die `ReferenceIDList` in  
4286 folgendem Format einstellen:

4287 `<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2023:rootDocumentUniqueId`

4288 Beim Upload einer neuen Version des Dokumentes DARF dieser Eintrag in der  
4289 `ReferenceIDList`, d.h. die `rootDocumentUniqueId`, NICHT verändert werden. Er bleibt  
4290 über alle Versionen des Dokumentes hinweg unverändert erhalten. Der Versuch eines  
4291 Clients, die `rootDocumentUniqueId` durch ein Metadata-Update oder im Zuge des  
4292 Einstellens einer neuen Dokumentenversion zu verändern, MUSS mit einem IHE-Error  
4293 `XDSRegistryMetadataError` abgebrochen werden. Es MUSS im `codeContext`-Attribut  
4294 des zurückgegebenen `XDSRegistryMetadataError`-Elements der  
4295 Text „rootDocumentUniqueId must not be changed“ zurückgegeben werden.[<=]

4296 **A\_14926-03 - XDS Document Service – Automatisiertes Löschen oder Verbergen**  
4297 **von Dokumenten**

4298 Der XDS Document Service MUSS bei zu löschenden oder zu verbergenden Dokumenten  
4299 und `DocumentEntry`-Einträgen im selben Zuge auch alle assoziierten `DocumentEntry`-  
4300 Einträge und Dokumente löschen bzw. verbergen.[<=]

4301 3.13.1.4.3.1 Provide and Register Document Set-b [ITI-41]

4302 **A\_13715 - XDS Document Service – Ablauflogik für**  
4303 **ProvideAndRegisterDocumentSet-b**

4304 Der XDS Document Service MUSS die Umsetzung der  
4305 Operation `ProvideAndRegisterDocumentSet-b` gemäß den definierten Ablauflogiken  
4306 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  
4307 3.41.4.2.3 ] implementieren.[<=]

#### **A\_15162-05 - XDS Document Service – Keine Registrierung bei Angabe von Document Entry Relationships in Metadaten**

Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem XDSRepositoryMetadataError-Fehlercode quittieren, sofern die Metadaten andere Association Types nach [IHE-ITI-TF3#4.2.2.2] als die Folgenden enthalten:

- urn:ihe:iti:2007:AssociationType:RPLC (Replace)
- urn:ihe:iti:2007:AssociationType:APND (Append).

[<=]

#### **A\_14938-02 - XDS Document Service – Validierung der Metadaten aus ITI Document Sharing-Profilen**

Der XDS Document Service MUSS die SubmissionSet- sowie die DocumentEntry-Metadaten der eingehenden Nachricht vor einer Zugriffskontrolle gemäß Konformität zu den Nutzungsvorgaben in [A\_14760-\*] prüfen. Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem XDSRepositoryMetadataError quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht. [<=]

#### ~~**A\_23538-01 – XDS Document Service – vereinfachte Prüfung der Metadaten in DocumentEntry.eventCodeList**~~

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

- ~~• ICD10gm (urn:oid:1.2.276.0.76.5.518)~~
- ~~• OPS (urn:oid:1.2.276.0.76.5.519)~~
- ~~• KDL (urn:oid:1.2.276.0.76.5.552).~~

~~[<=]~~

#### **A\_23123 - XDS Document Service – APND-Assoziation mit existierenden Dokument oder Dokument aus SubmissionSet**

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

#### **A\_23124 - XDS Document Service – Addendum nur mit einem Dokument verknüpfen**

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

Das heißt, ein Addendum-Dokument kann sich gemäß IHE immer nur auf ein einzelnes Vorgängerdokument (IHE: "parent document") beziehen.

#### **A\_23125 - XDS Document Service – Kein automatisches "Deprecated" des Addendums**

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

#### **A\_24521 - XDS Document Service - Erzeugen von Prüfsummen für Dokumente**

Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes Dokument seine kryptographische Prüfsumme berechnen und in DocumentEntry.hash



- 4355 hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die  
4356 Dokumentengröße in `DocumentEntry.size` berechnet und gesetzt werden. [`<=`]
- 4357 **A\_24988 - XDS Document Service - Dublettenprüfung für Dokumente**  
4358 Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes  
4359 Dokument den hash-Wert vergleichen mit allen bereits in dieser Akte existierenden hash-  
4360 Werten der Dokumente und bei einer Übereinstimmung das Einstellen mit dem  
4361 Fehlercode `XDSDuplicateDocument` ablehnen. Es MUSS im `codeContext`-Attribut  
4362 des zurückgegebenen `rs:RegistryError`-Elements die Liste der UUIDs  
4363 (DocumentEntry.entryUUID) der identifizierten Dokumente angegeben werden. [`<=`]
- 4364 **A\_24990 - XDS Document Service - Dublettenprüfung für dynamische Ordner**  
4365 Der XDS Document Service MUSS beim Anlegen dynamischer Folder prüfen, ob ein  
4366 Ordner bereits existiert, der gemäß vom Titel her identisch ist mit demjenigen, den der  
4367 Client einzustellen versucht. Im Falle eines identischen Titels MUSS der Einstellversuch  
4368 mit dem Fehlercode `XDSDuplicateFolder` abgelehnt werden. [`<=`]
- 4369 **A\_14937 - XDS Document Service – Dokumentengröße prüfen**  
4370 Der XDS Document Service MUSS die Dateigröße jedes übergebenen Dokuments  
4371 ermitteln, bevor das SubmissionSet verarbeitet wird. Der XDS Document Service  
4372 MUSS die Verarbeitung ablehnen und mit einem `MaxDocSizeExceeded`- bzw.  
4373 `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren, wenn die  
4374 Gesamtgröße aller übermittelten Dokumente 25 MByte übersteigt oder die Größe  
4375 mindestens eines einzelnen Dokuments 25 MByte übersteigt.  
4376 [`<=`]
- 4377 Das bedeutet, dass Dokumente bis zu einer Größe von 25 MB =  $25 * (1024)^2$  Byte in  
4378 die ePA hochgeladen werden. Grundlage für die Berechnung der Dokumentengröße ist  
4379 das Dokument ohne Transportcodierung. Größere Dokumente können nicht hochgeladen  
4380 werden.
- 4381 **A\_23098-01 - XDS Document Service – Keine Registrierung bei zeitlicher**  
4382 **Ungültigkeit von strukturierten Dokumenten**  
4383 Der XDS Document Service MUSS beim Einstellen eines strukturierten  
4384 Dokuments sicherstellen, dass die Vorgaben gemäß [gemSpec\_IG\_ePA] hinsichtlich der  
4385 zeitlichen Gültigkeit erfüllt werden und andernfalls das Registrieren und Speichern von  
4386 Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`  
4387 quittieren. Es MUSS im `codeContext`-Attribut  
4388 des zurückgegebenen `XDSRepositoryMetadataError`-Elements der Text „Version of  
4389 submitted structured document is not supported“ zurückgegeben werden. [`<=`]
- 4390 **A\_21610-03 - Sonderfälle Anlegen von Foldern durch Clientsysteme**  
4391 Der XDS Document Service MUSS sicherstellen, dass ausschließlich dynamische Ordner  
4392 vom Typ "Schwangerschaft und Geburt" (Folder.Code = pregnancy\_childbirth) durch  
4393 Clients angelegt werden können. [`<=`]
- 4394 **A\_22400-01 - XDS Document Service - Ablehnung Upload bei abweichenden**  
4395 **confidentialityCode**  
4396 Der XDS Document Service MUSS Uploads, die als Resultat einen uneinheitlichen  
4397 `documentEntry.confidentialityCode` über alle Dokumente in einer mixed- oder uniform-  
4398 Sammlung haben, mit einem `XDSRegistryMetadataError` ablehnen. [`<=`]
- 4399 Die Anforderung bezieht sich auf Einträge in `documentEntry.confidentialityCode` die nicht  
4400 aus dem ValueSet zum Verbergen (`confidentialityCode=CON`), resultieren.
- 4401 **AA\_24797-0204 - XDS Document Service - Ablehnung Upload bei veränderten**  
4402 **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 die Metadatenattribute creationTime, entryUUID sowie uniqueId und confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491). [ $\leq$ ]~~

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).

[ $\leq$ ]

#### **AA\_24531-0304 - Constraint Management - Verbergen von Dokumenten durch confidentialityCode**

Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) durch eine Nutzergruppe der Rolle ~~gemäß A\_24306\* oder~~ oid\_versicherter eingestellt wird, nicht Bestandteil einer Sammlung, also eines Ordners der Ausprägung "mixed" oder "uniform" ist, und kein Dokument der Kategorie "emp" ist, dann MUSS der XDS Document Service sicherstellen, dass das Dokument durch einen Eintrag in der General Deny Policy verborgen wird. Es MUSS ein Eintrag mit denyType = "document" für die General Deny Policy erzeugt werden. [ $\leq$ ]

#### **AA\_25856-0102 - XDS Document Service - Fehlerhaftes Verbergen von Dokumenten durch confidentialityCode**

Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) nicht durch eine Nutzergruppe der Rolle ~~gemäß A\_24306\* oder~~ oid\_versicherter eingestellt wird, oder Bestandteil einer Sammlung, also eines Ordners der Ausprägung "mixed" oder "uniform" ist, dann MUSS der XDS Document Service die Operation abbrechen und mit einem Fehlercode ConstraintViolation beenden. [ $\leq$ ]

Das Verbergen von Dokumenten ist in Kapitel ~~3.13.1.10: Verbergen von Dokumenten durch Verwendung des confidentialityCode~~ beschrieben.

#### 3.13.1.4.3.2 Registry Stored Query [ITI-18]

##### **A\_14913 - XDS Document Service – Ablauflogik für Registry Stored Query**

Der XDS Document Service MUSS die Umsetzung der Operation RegistryStoredQuery gemäß der definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3 ] implementieren. [ $\leq$ ]

##### **A\_24761 - XDS Document Service – Ermitteln verknüpfter Approved Documents für Registry Stored Query**

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "GetRelatedApprovedDocuments" mit der Query-ID "urn:uuid:1c1f1cea-ad3a-11ed-afa1-0242ac120002" mit denselben Parameternutzungsvorgaben der Registry Stored Query „GetDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.5] mit der Multiplizität 1 unterstützen. Das resultierende DocumentEntry Objekt MUSS

- mit dem Ergebnis von GetDocuments übereinstimmen, falls dieses sich im Zustand approved befindet;
- andernfalls über Associations ermittelt werden. Dabei wird jeweils ausgehend von der übergebenen DocumentEntry.EntryUUID oder DocumentEntry.UniqueId über

4451 die Replace- Associations dasjenige DocumentEntry Objekt ermittelt, das sich im  
4452 Zustand approved befindet.

4453 Das wsa:Action-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery"  
4454 besitzen.  
4455 [ $\leq$ ]

4456 **A\_24762 - XDS Document Service – Suchanfragen über das Metadatenattribut**  
4457 **DocumentEntry.title**

4458 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "FindDocumentsByTitle"  
4459 mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben  
4460 Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-  
4461 ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter  
4462 \$XDSDocumentEntryTitle unterstützen, sodass eine Suchergebnismenge über das  
4463 Attribut XDSDocumentEntry.title eingeschränkt werden kann. Weiterhin MUSS dieselbe  
4464 Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den  
4465 Parameter \$XDSDocumentEntryAuthorPerson. Das wsa:Action-Element MUSS den Wert  
4466 "urn:ihe:iti:2007:RegistryStoredQuery" besitzen.[ $\leq$ ]

4467 **A\_25183 - XDS Document Service – Suchanfragen über das Metadatenattribut**  
4468 **DocumentEntry.comment**

4469 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp  
4470 "FindDocumentsByComment" mit der Query-ID "urn:uuid:2609dda5-2b97-44d5-a795-  
4471 3e999c24ca99" und denselben Parameternutzungsvorgaben der Registry Stored Query  
4472 "FindDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren  
4473 verpflichtenden Suchparameter \$XDSDocumentEntryComment unterstützen, sodass eine  
4474 Suchergebnismenge über das Attribut XDSDocumentEntry.comment eingeschränkt  
4475 werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert  
4476 sein, wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson.  
4477 Das wsa:Action-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery"  
4478 besitzen.[ $\leq$ ]

4479

4480 **A\_24763 - XDS Document Service – Suche über Author Institution bei Registry**  
4481 **Stored Query**

4482 Der XDS Document Service MUSS für den Anfragetyp "FindDocumentsByTitle" den  
4483 weiteren optionalen Parameter \$XDSDocumentEntryAuthorInstitution verarbeiten  
4484 können, sodass eine Suchergebnismenge über den authorInstitution-Slot der  
4485 XDSDocumentEntry.author-Classification (Wertemenge des authorInstitution-Sub-  
4486 Attributs) eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels  
4487 Platzhalter implementiert sein, wie für Suchanfragen über den Parameter  
4488 \$XDSDocumentEntryAuthorPerson.[ $\leq$ ]

4489 **A\_24764 - XDS Document Service – Rückgabe unscharfer Suchergebnisse für**  
4490 **Registry Stored Query**

4491 Der XDS Document Service MUSS bei der Ermittlung der Ergebnisse einer Registry  
4492 Stored Query bei Auswertung der folgenden Queries und deren Suchparametern beim  
4493 Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d. h. bezogen auf das  
4494 jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht  
4495 abweichende Ergebnisse zurück liefern können:

- 4496 • Query "FindDocuments" und Query "FindDocumentsByTitle" und Query  
4497 "FindDocumentsByComment"
- 4498 • \$XDSDocumentEntryTitle
- 4499 • \$XDSDocumentEntryAuthorInstitution

- 4500 • \$XDSDocumentEntryAuthorPerson
- 4501 • \$XDSDocumentEntry.comment
- 4502 • Query "FindSubmissionSets"
- 4503 • \$XDSSubmissionSetAuthorPerson

4504 Dabei MUSS der XDS Document Service mindestens unscharfe Ergebnisse bezüglich  
4505 Groß/Kleinschreibung unterstützen, also Groß/Kleinschreibung für die angegebenen  
4506 Parameter der ausgewählten Query-Typen ignorieren.  
4507 [ $\leq$ ]

4508 Das zur Ermittlung weiterer unscharfer Ergebnisse vom XDS Document Service  
4509 einzusetzende Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu  
4510 liefern, die ihm möglicherweise sonst wegen beispielsweise falscher Schreibweise eines  
4511 Namens (z. B. "Meyer" vs. "Maier") vorenthalten worden wäre. Dabei sind Verfahren wie  
4512 die Kölner Phonetik aber auch andere Mechanismen denkbar.

4513 3.13.1.4.3.3 Remove Metadata [ITI-62]

#### 4514 **A\_14908-02 - XDS Document Service – Ablauflogik für Remove Metadata**

4515 Der XDS Document Service MUSS die Umsetzung der Operation RemoveMetadata gemäß  
4516 der definierten Ablauflogik in [IHE-ITI-RMD#3.62.4.1.2 und 3.62.4.1.3 ]  
4517 implementieren.[ $\leq$ ]

#### 4518 **A\_20701 - XDS Document Service – Unwiderrufliches Löschen bei Remove 4519 Metadata**

4520 Der XDS Document Service MUSS sicherstellen, dass einmal gelöschte Dokumente und  
4521 Metadatenobjekte nicht wiederhergestellt werden können.[ $\leq$ ]

#### 4522 **A\_21715 - XDS Document Service – Kein Löschen von "replaced"-Dokumenten 4523 im Status "Deprecated"**

4524 Der XDS Document Service MUSS sicherstellen, dass keine Löschanfrage eines ePA-Client  
4525 auf Dokumenten mit dem availabilityStatus = Deprecated ausgeführt werden darf.[ $\leq$ ]

#### 4526 **A\_21714-03 - XDS Document Service – Löschen von strukturierten Dokumenten 4527 durch ein ePA-FdV**

4528 Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein  
4529 ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete  
4530 Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert  
4531 aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie  
4532 zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die  
4533 Nachricht mit dem XDSRegistryError-Fehlercode zurückgegeben werden. Es MUSS im  
4534 codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert  
4535 "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt  
4536 werden.[ $\leq$ ]

#### 4537 **A\_21817-02 - XDS Document Service – Löschen von strukturierten Dokumenten 4538 durch ein Primärsystem**

4539 Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein  
4540 Primärsystem ablehnen, wenn zugehörige Submission Sets, Associations oder  
4541 zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners  
4542 impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets,  
4543 Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben  
4544 vor, MUSS die Nachricht mit XDSRegistryError-Fehlercode zurückgegeben werden. Es MUSS  
4545 im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der  
4546 Wert "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt  
4547 werden.[ $\leq$ ]

#### 4548 **A\_24663-01 - XDS Document Service – Bereinigung der General Deny Policy**

4549 Der XDS Document Service MUSS als Folge von erfolgreichen Löschanfragen alle Einträge  
 4550 der General Deny Policy entfernen, welche die betroffenen Dokumente oder dynamischen  
 4551 Ordner referenzieren. [`<=`]

4552 **A\_24765 - XDS Document Service – Kein Löschen von statischen Ordnern und**  
 4553 **Associations**

4554 Der XDS Document Service MUSS sicherstellen, dass eine Löschanfrage keine statischen  
 4555 Ordner und Assoziationen löschen darf. Dies gilt nicht für dynamische Ordner. Der XDS  
 4556 Document Service MUSS bei Löschung eines Dokumentes die Assoziation zum Folder  
 4557 löschen. [`<=`]

4558 Dynamische Ordner sind beispielsweise Mutterpass (folderCode = pregnancy\_childbirth)  
 4559 oder DiGA (folderCode = diga).

4560 **A\_20579-01 - XDS Document Service – Löschen von Ordnern**

4561 Der XDS Document Service MUSS Requests, die darauf abzielen, einen statischen Folder  
 4562 direkt zu löschen, mit einem XDSRegistryMetadataError ablehnen. [`<=`]

4563

4564 3.13.1.4.3.4 RetrieveDocumentSet [ITI-43]

4565 **A\_14914 - XDS Document Service – Ablauflogik für Retrieve Document Set**

4566 Der XDS Document Service MUSS die Umsetzung der Operation RetrieveDocumentSet  
 4567 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3 ] und  
 4568 [IHE-ITI-TF2b#3.43.4.2.2 und 3.43.4.2.3 ] implementieren. [`<=`]

4569 **A\_16201 - XDS Document Service – Prüfung der zurückgegebenen Paketgröße**

4570 Der XDS Document Service MUSS anhand der übergebenen DocumentUniqueIDs die  
 4571 Gesamtgröße ermitteln und bei Überschreitung von 250 MByte die Verarbeitung ablehnen  
 4572 und die Nachricht mit einem MaxPkgSizeExceeded-Fehlercode gemäß [IHE-ITI-  
 4573 TF3#4.2.4] quittieren. [`<=`]

4574

4575 3.13.1.4.3.5 Restricted Update Document Set [ITI-92]

4576 **~~AA\_15061-0507~~ - XDS Document Service – Ablauflogik für Restricted Update**  
 4577 **Document Set**

4578 Der XDS Document Service MUSS die Umsetzung der  
 4579 Operation RestrictedUpdateDocumentSet gemäß der definierten Ablauflogik in [IHE-ITI-  
 4580 RMU#3.92.4.1.2 und 3.92.4.1.3] implementieren und sicherstellen, dass (nur) die  
 4581 folgenden Metadatenobjekte gesendet werden:

- 4582 • ein neues SubmissionSet,
- 4583 • einen DocumentEntry inklusive der ~~entryUUID~~ entryUUID des zu ändernden  
 4584 DocumentEntry-Objekts. Das übermittelte DocumentEntry-Objekt kann sowohl  
 4585 alle vollständigen Metadatenattribute als auch nur zu ändernde  
 4586 Metadatenattribute enthalten. In jedem Fall dürfen Änderungen ausschließlich  
 4587 gemäß A\_15083-\* angenommen und durchgeführt werden.
- 4588 • für das Hinzufügen, Ändern oder Löschen eines einzelnen oder mehrerer Werte  
 4589 in DocumentEntry.author, DocumentEntry.confidentialityCode und  
 4590 DocumentEntry.eventCodeList gilt darüber hinaus:
- 4591 • es MÜSSEN alle und nicht nur die zu ändernden Werte (z. B. Autoren) über  
 4592 ihre jeweiligen <classification classificationScheme="urn:uuid:...>-XML-  
 4593 Elemente im gewünschten Soll-Zustand gesendet werden.



- das Löschen aller Werte (z. B. Autoren) MUSS durch Übertragung ein einzelnen, komplett leeren <classification="urn:uuid:...>-XML-Elements signalisiert werden.

- eine SS-DE HasMember-Association, die das SubmissionSet mit dem geschickten DocumentEntry verbindet.
- die „lid“ (logicalID) DARF NICHT gesendet werden.
- der Slot "PreviousVersion" MUSS immer mit dem Wert "1" gesendet werden.
- der Slot „AssociationPropagation“ MUSS auf „no“ gesetzt werden. Zusätzlich MUSS der alternative Slot-Name "associationPropagation" akzeptiert werden.

Der XDS Document Service DARF die gesendete Association und das neue SubmissionSet NICHT dauerhaft speichern. [≤]

Der alternative Slot-Name "associationPropagation" wird unterstützt, da alte Versionen von ePA fälschlicherweise, abweichend von [IHE-ITI-RMU] diesen Wert gefordert haben.

#### **A\_15082-02 - XDS Document Service – Validierung der Metadaten aus ITI Document Sharing-Profilen**

Der XDS Document Service MUSS die übermittelten DocumentEntry-Metadaten der Operation RestrictedUpdateDocumentSet dahingehend prüfen, dass gegenüber den Bestandsdaten die geänderten Metadaten konform zu den Nutzungsvorgaben in [A\_14760-\*] geändert werden. Der XDS Document Service MUSS das Aktualisieren der Metadatenattribute ablehnen und mit einem XDSRepositoryMetadataError quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht. [≤]

#### **~~AA\_15083-0708~~ - XDS Document Service – Prüfung auf ausschließliche Aktualisierung der erlaubten Metadaten**

Der XDS Document Service MUSS die übermittelten DocumentEntry-Metadaten der Operation RestrictedUpdateDocumentSet dahingehend prüfen, dass gegenüber den Bestandsdaten ausschließlich die folgenden Metadaten geändert werden:

- DocumentEntry.author
- DocumentEntry.classCode
- DocumentEntry.comments
- DocumentEntry.confidentialityCode (confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) ist nicht erlaubt)
- DocumentEntry.creationTime
- DocumentEntry.eventCodeList
- DocumentEntry.formatCode
- DocumentEntry.healthcareFacilityTypeCode
- DocumentEntry.languageCode
- DocumentEntry.legalAuthenticator
- DocumentEntry.practiceSettingCode
- DocumentEntry.referenceIdList
- DocumentEntry.serviceStartTime

- 4636 • DocumentEntry.serviceStopTime
- 4637 • DocumentEntry.title
- 4638 • DocumentEntry.typeCode
- 4639 • DocumentEntry.URI

4640 Wenn das Metadatum DocumentEntry.referenceIdList ohne rootDocumentUniqueId  
 4641 gesendet wird, MUSS der XDS Document Service den Wert automatisch setzen (identisch  
 4642 zu rootDocumentId in DocumentEntry.referenceIdList des ersetzten Dokuments). Wenn  
 4643 die rootDocumentUniqueId gesendet wird, MUSS der XDS Document Service  
 4644 sicherstellen, dass der Wert dem ansonsten automatisch gesetzten Wert entspricht.

4645  
 4646 Werden unerlaubte Metadatenänderungen geschickt, muss die Operation mit  
 4647 einem LocalPolicyRestrictionError-Fehlercode abgebrochen werden. Werden  
 4648 Metadatenattribute mit leeren Werten übermittelt, signalisiert dies ein Löschen  
 4649 des Metadatums (z.B. DocumentEntry.comments). Es müssen die Kardinalitäten  
 4650 in A\_14760-\* berücksichtigt bzw. dürfen nicht verletzt werden. Das  
 4651 Metadatum DocumentEntry.referenceIdList MUSS dabei mindestens die  
 4652 rootDocumentUniqueId enthalten.

4653 Wenn in der Eingangsnachricht keine Aktualisierung für die erlaubten Metadaten  
 4654 enthalten ist, ist die Weiterverarbeitung abubrechen und die Nachricht mit einem  
 4655 LocalPolicyRestrictionError-Fehlercode zu quittieren. [ <= ]. [ <= ]

4656

#### 4657 **A\_21533 - XDS Document Service – Kein Anlegen von Versionen für Restricted** 4658 **Update Document Set**

4659 Der XDS Document Service DARF eine echte Versionierung NICHT umsetzen, d. h. er  
 4660 DARF den alten DocumentEntry NICHT speichern. Insbesondere DARF der XDS Document  
 4661 Service DocumentEntry.version NICHT anlegen und verwalten. [ <= ]

#### 4662 **A\_21783-03 - XDS Document Service - Vererbung der geänderten Metadaten für** 4663 **Restricted Update Document Set**

4664 Der XDS Document Service MUSS die neu gesetzten Metadaten ebenfalls auf alle mit  
 4665 dem geänderten Dokument assoziierten Dokumente setzen. Als assoziierte Dokumente  
 4666 sind im Sinne dieser Anforderung Dokumente einer RPLC-Kette zu betrachten. [ <= ]

4667 Metadaten von Dokumenten einer mixed- oder uniform-Sammlung dürfen nicht geändert  
 4668 werden.

#### 4669 **A\_25173 - XDS Document Service - Restricted Update Document Set nicht für** 4670 **MIOs**

4671 Falls die Operation RestrictedUpdateDocumentSet für Dokumente einer mixed- oder  
 4672 uniform-Sammlung aufgerufen wird MUSS der XDS Document Service das Aktualisieren  
 4673 der Metadatenattribute ablehnen, mit einem XDSRepositoryMetadataError quittieren  
 4674 und im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements den  
 4675 Text "Metadata Update for MIOs not allowed" angeben.  
 4676 [ <= ]

#### 4677 *3.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen*

#### 4678 **A\_24508-01 - XDS Document Service – Prüfung der Policies bei Suchanfrage**

4679 Der XDS Document Service MUSS bei einer Suchanfrage für einen angemeldeten Nutzer  
 4680 die Suchergebnismenge entsprechend der Legal Policy und der General Deny Policy  
 4681 filtern, d. h. die Suchergebnismenge enthält ausschließlich XDS-Metadaten, die für einen  
 4682 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. [≤]

**~~AA\_24510-01~~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 XDSRepositoryMetadataError**

Der XDS Document Service KANN alternativ zum Fehler "XDSRepositoryMetadataError" den Fehler "XDSRegistryMetadataError" verwenden. [≤]

**A\_23148-01 - XDS Document Service – Festlegung zu http-Statuscode bei IHE-Responses**

4730 Der XDS Document Service MUSS für den Fall, dass eine IHE-Response in der HTTP-  
4731 Response enthalten ist, den http-Statuscode 200 zurückgeben. Das gilt auch, wenn die  
4732 IHE-Response einen IHE-Fehler überträgt. [ <= ]

4733 **A\_26324-01 - XDS Document Service - Aktenkonto im Umzug**

4734 Falls sich ein Aktenkonto im Zustand SUSPENDED befindet MUSS der XDS Document  
4735 Service die Verarbeitung ablehnen und mit einem `StatusMismatch`-Fehlercode gemäß  
4736 [IHE-ITI-TF3#4.2.4] quittieren. <= [ <= ]

4737 **A\_26325-01 - XDS Document Service - Aktenkonto unbekannt oder im Zustand**  
4738 **INITIALIZED**

4739 Falls sich ein Aktenkonto im Zustand UNKNOWN oder INITIALIZED befindet MUSS der  
4740 XDS Document Service die Verarbeitung ablehnen und mit einem `NoHealthRecord`-  
4741 Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. <= [ <= ]

4742 **A\_25683-01 - XDS Document Service - Prüfung auf Befugnis**

4743 Falls keine gültige Befugnis für den aufrufenden Nutzer vorliegt MUSS der XDS Document  
4744 Service die Verarbeitung ablehnen und mit einem `NotEntitled`-Fehlercode gemäß [IHE-  
4745 ITI-TF3#4.2.4] quittieren. [ <= ]

4746 **A\_26459 - XDS Document Service - keine Authentisierung des Nutzers**

4747 Falls keine erfolgreiche Authentifizierung des Nutzers vorliegt MUSS der XDS Document  
4748 Service die Verarbeitung ablehnen und mit einem `InvalidAuth`-Fehlercode gemäß [IHE-  
4749 ITI-TF3#4.2.4] quittieren. <= [ <= ]

4750 **3.13.1.6 Schnittstellen im XDS Document Service**

4751 In diesem Abschnitt wird die Außenschnittstelle des XDS Document Service festgelegt.  
4752 Einzelne Umsetzungsanforderungen suggerieren eine vermischte Verarbeitung von  
4753 Funktionalitäten, welche bei IHE ITI originär getrennt von einer Document Registry und  
4754 einem Document Repository (bzw. den Responding Gateways) durchgeführt werden. Da  
4755 die Außenschnittstelle des XDS Document Service nicht zwischen Document Registry und  
4756 Document Repository unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit  
4757 differenzierten Pfaden, siehe A\_17969,26814-\*, werden sonst bei IHE ITI explizite  
4758 Operationen zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne  
4759 Umsetzung angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-  
4760 Nachricht kann an IHE ITI-konforme Akteure ausgerichtet werden.

4761 **3.13.1.6.1 Schnittstelle I\_Document\_Management**

4762 Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3: Vorgaben zu IHE ITI-  
4763 Transaktionen bei mehreren Schnittstellen .

4764 **A\_14152-02 - XDS Document Service – Implementierung der Schnittstelle**  
4765 **I\_Document\_Management**

4766 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-  
4767 Service-Schnittstelle für den Zugriff von ePA-Clients, die über das zentrale Netz zugreifen  
4768 implementieren.

4769 **Tabelle 26: Schnittstelle I\_Document\_Management**

Schnittstelle	I_Document_Management
<b>Version</b>	2.0.0
<b>Namensraum</b>	urn:ihe:iti:xds-b:2007

Schnittstelle	I_Document_Management	
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"> <li>• PRPA_IN201301UV02.xsd</li> <li>• PRPA_IN201302UV02.xsd</li> <li>• PRPA_IN201304UV02.xsd</li> <li>• MCCI_IN000002UV01.xsd</li> <li>• query.xsd</li> <li>• rs.xsd</li> <li>• lcm.xsd</li> <li>• rim.xsd</li> <li>• XDS.b_DocumentRepository.xsd</li> </ul>	

4770 [**<=**]

4771 Durch die Legal Policy ist geregelt, welche Clients (professionOID) letztendlich zugreifen  
4772 dürfen.

4773 3.13.1.6.1.1 Operation I\_Document\_Management::ProvideAndRegisterDocumentSet-b  
4774 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
4775 Transaktion "ProvideAndRegisterDocumentSet-b" [ITI-41] sind [IHE-ITI-TF2x] sowie  
4776 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4777 ~~**A\_14941-06—XDS Document Service—Keine Registrierung bei Angabe von**~~  
4778 ~~**Document Entry Relationships in Metadaten**~~  
4779 ~~Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und~~  
4780 ~~Dokument(en) ablehnen und mit einem XDSRepositoryMetadataError Fehlercode~~  
4781 ~~quittieren, sofern die Metadaten die folgenden Association Types nach [IHE-ITI-~~  
4782 ~~TF3#4.2.2] enthalten:~~

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

**[<=>]**

Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner gesammelt. Das Anlegen eines DiGA-Ordners erfolgt durch den XDS Document Service unter der Voraussetzung, dass es eine gültige Befugnis für die DiGA gibt. Der DiGA-Ordner wird vom XDS Document Service mit der Telematik-ID der DiGA verknüpft. Die Zuordnung von DiGA-Dokumenten beim Schreiben erfolgt implizit über die TelematikID aus dem IDToken des Nutzers. Da ein DiGA-Ordner im Titel immer den Namen der DiGA enthält kann ein Client (z.B. LEI) darüber die relevante DiGA auswählen und auf die Dokumente der DiGA, sofern eine Befugnis für den Nutzer vorliegt, lesend zugreifen.

Ein Update eines bestehenden Dokuments mit der bekannten DocumentEntry.entryUUID kann durch einen DiGA-Client erfolgen. Hierzu ist es erforderlich, dass ein DiGA-Client die DocumentEntry.entryUUID persistiert und keine symbolischen IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] verwendet.

#### **A\_21512-04 - XDS Document Service – dynamisches Anlegen von DiGA-Ordern**

Falls eine gültige Befugnis für eine konkrete DiGA vorliegt, MUSS der XDS Document Service beim erstmaligen Einstellen eines Dokumentes für diese DiGA in die Akte des Versicherten (Operation `I_Document_Management::ProvideAndRegisterDocumentSet-b()`) sicherstellen, dass genau ein Ordner für den Versicherten mit den folgenden Eigenschaften angelegt ist:

- DiGA-Ordner der Kategorie `diga` gemäß A\_19388 (Belegung `Folder.codeList`) unter Berücksichtigung allgemeiner Vorgaben für `Folder`-Metadaten in A\_14760 (Belegung der restlichen Metadatenfelder).
- `Folder.title` wird entsprechend des Attributs "organizationName" aus dem IDToken der zugreifenden DiGA belegt.
- `Folder.comment` wird belegt mit "urn:gematik:diga:<Telematik-ID>", wobei die Telematik-ID dem Attribut "idNummer" des ID-Token entspricht.
- `Folder.EntryUUID` wird mit einer aus der TelematikID abgeleiteten UUID belegt.

Die `folder.EntryUUID` MUSS wie folgend dargestellt aus der TelematikID der DiGA erzeugt werden:

- Algorithmus: Name-Based UUID gemäß [RFC4122#4.3], Version 3 (MD5)
- Namensraum-UUID: "e2310a38-0b62-415e-8b44-994dc8312965"
- Name: "<TelematikId>"

Eine konkrete DiGA wird identifiziert durch die TelematikID und ist als DiGA durch die `professionOID` gekennzeichnet.

**[<=]**

#### **A\_22994-01 - XDS Document Service - automatische Folder-Zuordnung für DiGA**

Der XDS Document Service MUSS beim Einstellen eines DiGA-Dokumentes in die Akte des Versicherten (Operation

`I_Document_Management::ProvideAndRegisterDocumentSet-b()`) sicherstellen, dass das DiGA-Dokument in den durch die TelematikID referenzierten DiGA-Ordner abgelegt wird.

4829 Die TelematikID des zu adressierenden Ordners entspricht dem Attribut "idNummer" des  
4830 ID-Token .[<=]

#### 4831 **A\_21713-03 - XDS Document Service – Kein Einstellen von Ordnern**

4832 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und  
4833 Dokument(en) über die

4834 Schnittstelle `I_Document_Management::ProvideAndRegisterDocumentSet-b` ablehnen  
4835 und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der  
4836 Eingangsnachricht ein oder mehrere neu anzulegende Folder enthalten sind. Ausnahme:  
4837 Folder der Kategorie `pregnancy_childbirth` in `Folder.codeList`. [≤]

4838

#### 4839 **A\_24497 - XDS Document Service - Verwendung der korrekten Telematik-ID 4840 beim Einstellen**

4841 Der XDS Document Service MUSS die Telematik-ID aus dem ID-Token der aktuellen User  
4842 Session abgleichen mit der Telematik-ID aus `SubmissionSet.authorInstitution` und  
4843 das Abweichen der Telematik-Ids mit einem `XDSRepositoryMetadataError`-Fehlercode  
4844 quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError-`  
4845 Elements den Text "Telematik-ID does not match" angeben.[≤]

#### 4846 **A\_24456 - XDS Document Service - Durchsetzung von Uniqueness beim 4847 Einstellen von Notfalldaten**

4848 Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien  
4849 "emergency" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein  
4850 einzelnes NFD- und ein einzelnes DPE-Dokument im Status "approved" gibt. Der Versuch,  
4851 innerhalb dieses Ordners ein zweites NFD- oder DPE-Dokument einzustellen, MUSS mit  
4852 dem `IHE-ErrorInvalidDocumentContent` abgebrochen werden. Es MUSS im  
4853 `codeContext`-Attribut des zurückgegebenen `InvalidDocumentContent`-Elements der Text  
4854 "Medical information object has to be unique" zurückgegeben werden.[≤]

#### 4855 **A\_25137 - XDS Document Service - Durchsetzung von Uniqueness beim 4856 Einstellen vom Medikationsplan**

4857 Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien  
4858 "emp" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein einzelnes  
4859 eMP-Dokument im Status "approved" gibt. Der Versuch, innerhalb dieses Ordners ein  
4860 zweites eMP-Dokument einzustellen, MUSS mit dem `IHE-`  
4861 `ErrorInvalidDocumentContent` abgebrochen werden. Es MUSS im `codeContext`-Attribut  
4862 des zurückgegebenen `InvalidDocumentContent`-Elements der Text "Medical information  
4863 object has to be unique" zurückgegeben werden.[≤]

4864

4865

#### 4866 3.13.1.6.1.2 Operation `I_Document_Management::RegistryStoredQuery`

4867 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
4868 Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie  
4869 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

#### 4870 3.13.1.6.1.3 Operation `I_Document_Management::RemoveMetadata`

4871 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
4872 Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-  
4873 ITI-TF2x] zu entnehmen.

#### 4874 3.13.1.6.1.4 Operation `I_Document_Management::RetrieveDocumentSet`

4875 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
4876 Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie  
4877 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4878 3.13.1.6.1.5 Operation I\_Document\_Management::RestrictedUpdateDocumentSet  
 4879 Weitere Details zur Ausgestaltung dieser Operation finden sich bezüglich der  
 4880 dazugehörigen IHE ITI-Transaktion "RestrictedUpdateDocumentSet" [ITI-92] in [IHE-ITI-  
 4881 RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x].

4882 Weitere Anforderungen zur Umsetzung der Operation RestrictedUpdateDocumentSet  
 4883 befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92] .

4884 3.13.1.6.2 Schnittstelle I\_Document\_Management\_Insurant

4885 Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-  
 4886 Transaktionen bei mehreren Schnittstellen .

4887 **A\_14478-01 - XDS Document Service – Implementierung der Schnittstelle**  
 4888 **I\_Document\_Management\_Insurant**

4889 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-  
 4890 Service-Schnittstelle für den Zugriff des ePA-FdV implementieren .

4891 **Tabelle 27: 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]	



Schnittstelle	I_Document_Management_Insurant
XML Schema	<ul style="list-style-type: none"> <li>• PRPA_IN201301UV02.xsd</li> <li>• PRPA_IN201302UV02.xsd</li> <li>• PRPA_IN201304UV02.xsd</li> <li>• MCCI_IN000002UV01.xsd</li> <li>• query.xsd</li> <li>• rs.xsd</li> <li>• lcm.xsd</li> <li>• rim.xsd</li> <li>• XDS.b_DocumentRepository.xsd</li> </ul>

4892

4893 [ $\leq$ ]4894 **A\_26460 - XDS Document Service - Zugriff über**4895 **I\_Document\_Management\_Insurant mit nicht registriertem Gerät**

4896 Falls Operationen von I\_Document\_Management\_Insurant ohne registriertes Gerät  
 4897 aufgerufen werden MUSS der XDS Document Service die Verarbeitung ablehnen und mit  
 4898 einem UnregisteredDevice-Fehlercode gemäß ~~[IHE-ITI-TF3#4.2.4]~~ quittieren. [ $\leq$ ]

4899 3.13.1.6.2.1 Operation

4900 I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b

4901 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
 4902 Transaktion "Provide And Register Document Set-b" [ITI-41] sind [IHE-ITI-TF2x] sowie  
 4903 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4904 **A\_21481-04 - XDS Document Service – Kein Einstellen von Ordnern und**  
 4905 **Associations**

4906 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und  
 4907 Dokument(en) über die Schnittstelle

4908 I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b() ablehnen und  
 4909 mit einem XDSRegistryMetadataError-Fehlercode quittieren, wenn in der  
 4910 Eingangsnachricht ein oder mehrere neu anzulegende Folder oder andere als die  
 4911 folgenden Assoziationen

4912 • SS-DE

4913 • SS-HM

4914 • FD-DE

4915 • RPLC

4916 • APND

4917 enthalten sind. [ $\leq$ ]

4918 Das Referenzieren bestehender Ordner ist davon nicht berührt, wie dies z. B. beim  
 4919 Einstellen von Dokumenten in Sammlungen der Fall ist (z. B. Einstellen eines Dokuments  
 4920 in einen Mutterpass).

4921 **A\_23144 - XDS Document Service - Automatische Ablage von Dokumenten im**  
 4922 **Ordner "technical"**



4923 Der XDS Document Service MUSS sicherstellen, dass Dokumente mit einem formatCode  
 4924 mit der codeSystem OID "2.25.154081344090540725127779452347992051720",  
 4925 unabhängig von weiteren Metadaten, im statischen Ordner "technical" abgelegt  
 4926 werden. [≤]

4927 3.13.1.6.2.2 Operation I\_Document\_Management\_Insurant::RegistryStoredQuery  
 4928 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
 4929 Transaktion "Registry Stored Query" [ITI-18] sind [IHE-ITI-TF2a], [IHE-ITI-TF2x] sowie  
 4930 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4931 3.13.1.6.2.3 Operation I\_Document\_Management\_Insurant::RemoveMetadata  
 4932 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
 4933 Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-  
 4934 ITI-TF2x] zu entnehmen.

4935 3.13.1.6.2.4 Operation I\_Document\_Management\_Insurant::RetrieveDocumentSet  
 4936 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
 4937 Transaktion "RetrieveDocumentSet" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie  
 4938 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4939 3.13.1.6.2.5 Operation  
 4940 I\_Document\_Management\_Insurant::RestrictedUpdateDocumentSet  
 4941 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
 4942 Transaktion "RestrictedUpdateDocumentSet" [ITI-92] sind [IHE-ITI-RMU], [IHE-ITI-  
 4943 TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4944 Weitere Anforderungen zur Umsetzung der Operation RestrictedUpdateDocumentSet  
 4945 befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92].

### 4946 3.13.1.6.3 Schnittstelle I Document Management Ncpeh

4947 Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-  
 4948 Transaktionen bei mehreren Schnittstellen .

### 4949 A 27300 - XDS Document Service (EU) – Implementierung der Schnittstelle 4950 I Document Management Ncpeh

4951 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-  
 4952 Service-Schnittstelle für den Zugriff des ePA-FdV implementieren.

4953 **Tabelle 28: Schnittstelle I Document Management Ncpeh**

<u>Schnittstelle</u>	<u>I Document Management Ncpeh</u>	
<u>Version</u>	<u>2.0.0</u>	
<u>Namensraum</u>	<u>urn:ihe:iti:xds-b:2007</u>	
<u>Namensraumkürzel</u>	<u>tns</u>	
<u>Operationen</u>	<u>Name</u>	<u>Beschreibung</u>
	<u>Registry Stored Query</u>	<u>Abfrage von Metadaten zu registrierten Dokumenten</u>
	<u>Retrieve Document Set</u>	<u>Anfrage von registrierten Dokumenten</u>

<u>Schnittstelle</u>	<u>I Document Management Ncpeh</u>
<u>WSDL</u>	<u>[XSDDocumentService]</u>
<u>XML Schema</u>	<ul style="list-style-type: none"> <li>• <u>PRPA_IN201301UV02.xsd</u></li> <li>• <u>PRPA_IN201302UV02.xsd</u></li> <li>• <u>PRPA_IN201304UV02.xsd</u></li> <li>• <u>MCCI_IN000002UV01.xsd</u></li> <li>• <u>query.xsd</u></li> <li>• <u>rs.xsd</u></li> <li>• <u>lcm.xsd</u></li> <li>• <u>rim.xsd</u></li> <li>• <u>XDS.b_DocumentRepository.xsd</u></li> </ul>

#### [<=]

3.13.1.6.3.1 Operation I Document Management Ncpeh::RegistryStoredQuery  
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie  
Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.3.2 Operation I Document Management Ncpeh::RetrieveDocumentSet  
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-  
Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie  
Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

### **3.13.1.7 Statische Metadaten**

Statische Inhalte werden vor der ersten Nutzung des XDS Document Service angelegt, d. h. bevor auf XDS Metadaten zugegriffen wird. Sie sind unveränderlich.

#### **AA\_24491-0102 - XDS Document Service – Anlegen von statischen Ordnern**

Der XDS Document Service MUSS nach der erfolgreichen Anlage der Akte des Versicherten die Kategorienordner unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A\_14760\* (Belegung der restlichen Metadatenfelder) für den Versicherten gemäß der folgenden Tabelle anlegen. Alle statischen Kategorienordner werden mit jeweils einem Ordner pro Kategorie angelegt. Alle statischen Ordner sind nach dem Anlegen initial leer.

Das Anlegen von Submission Sets und zugehöriger Associations zu den statischen Ordnern ist nicht vorgegeben. Das XDS-Informationsmodell MUSS allerdings hinsichtlich der Folder-DocumentEntry- sowie SubmissionSet-HasMember-Associations bei einer Verarbeitung durch die Document Consumer (z. B. Querying) erfüllt werden.

**Tabelle 29: Festlegung Folder.entryUUID zu statischen Ordnern**

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
reports	b878db05-49e4-4f74-a329-b3bcdd8082c4

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
emp	7c1054ea-a4df-4a1b-8e10-209f6d8812ee
emergency	a7bb6be7-d756-46dd-90d4-4020ed55b777
eab	2ed345b1-35a3-49e1-a4af-d71ca4f23e57
dental	af547321-b8e8-4e1d-b9af-51bb4a990bda
child	2c898452-4667-40e3-9d3e-c09d7385b527
vaccination	9c3edaf3-a978-46fe-8e6e-021ff4aca60b
patient	d236c9a2-ab01-4902-a00a-1e1dff439fe7
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d
<a href="#">health_risk_analysis</a>	<a href="#">840a59c7-61d4-4caa-80a7-1857af2f166f</a>
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

4979

4980

[&lt;=]

4981 *Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner vom Typ*  
4982 *"pregnancy\_childbirth", mit dem Folder.title für den Namen des Kindes bzw. ein*  
4983 *Kennzeichen der Schwangerschaft (A\_22515-\*).*

#### 4984 **A\_20216-03 - XDS Document Service – Unveränderlichkeit von statischen** 4985 **Akteninhalten**

4986 Der XDS Document Service DARF die Metadaten eines statischen Aktenobjekts gemäß  
4987 A\_24491 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen.  
4988 Dabei gelten folgende Ausnahmen:

- 4989 • Folder.lastUpdateTime - Folder.lastUpdateTime wird automatisch vom XDS  
4990 Document Service aktualisiert, sobald Dokumente in den Ordner eingestellt oder  
4991 daraus gelöscht werden, siehe auch [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-  
4992 TF3#4.2.3.4.6].

4993 [**<=**]

### 4994 **3.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten**

4995 Für den XDS Document Service werden Vorgaben bezüglich zu verwendender IHE XDS-  
4996 Metadatenattribute auf Ebene von Submission Set, Document Entry sowie Folder  
4997 vorgenommen. Diese Nutzungsvorgaben referenzieren größtenteils Value Sets der IHE  
4998 Deutschland Arbeitsgruppe "XDS Value Sets" [IHE-ITI-VS] und sind für die ePA-  
4999 Fachanwendung verbindlich. Diese XDS-Value Sets sind teilweise von IHE-Deutschland  
5000 als "offen" gekennzeichnet, um Erweiterungen flexibel einbringen zu können. Für  
5001 die ePA-Fachanwendung gelten jedoch definierte Vorgaben, wie neue Codes und Value  
5002 Sets sicher über eine Konfigurationsschnittstelle eingebracht werden können. Daher sind  
5003 die in dieser Spezifikation beschriebenen Nutzungsvorgaben für Value Sets als fest  
5004 anzusehen bzw. die Offenheit der XDS Value Sets wird nicht unterstützt.

#### 5005 **3.13.1.8.1 Allgemeine Metadatenvorgaben**

5006 Die Spalten der unten dargestellten, tabellarischen Übersichten für die Metadaten von  
5007 Dokumenten (IHE XDS.b Document Entry) und Übertragungspaketen (IHE XDS.b  
5008 Submission Set) haben die folgenden Bedeutungen:

- 5009 • Die Spalte "Metadatenattribut XDS.b" listet alle aus dem IHE ITI TF vorgesehenen  
5010 Metadaten für Document Entry- und Submission Set-Elemente auf.
- 5011 • Die Spalten "Mult. PS" (Multiplizität Primärsystem; alle Primärsysteme außer PS-  
5012 KTR), "Mult. KTR" (Multiplizität "PS-KTR"), "Mult. DS" (Multiplizität "Document  
5013 Service"), "Mult. FV" (Multiplizität "ePA-Frontend des Versicherten") kennzeichnen  
5014 die Multiplizität des Metadatenattributs beim Erzeugen oder Verarbeiten durch das  
5015 jeweilige System.  
5016 Die Angabe der jeweiligen Spalte entspricht einem Wertebereich. Die Zeichen [...] für Wertebereich wurden zum Zwecke der besseren Darstellbarkeit weggelassen.
- 5018 • Die Spalte "Kurzbeschreibung" beschreibt kurz die Bedeutung des  
5019 Metadatenattributs.
- 5020 • Die Spalte "Nutzungsvorgabe" macht Bedingungen für die Verwendung eines  
5021 Metadatenattributs (z. B. erlaubte Wertebereiche und Formatangaben), welche  
5022 über die im IHE ITI TF definierten Vorgaben hinausgehen.
- 5023 • Die Spalte "FV Edit" beschreibt, ob ein bestimmtes Metadatenattribut beim  
5024 Einstellen eines Dokuments über das ePA-FdV durch den Versicherten veränderbar  
5025 gestaltet werden muss. Es sollten dabei immer nur die für den aktuellen Workflow  
5026 relevanten Metadatenattribute angezeigt werden, um die Komplexität für den

5027 Versicherten gering zu halten. Veränderbar gestaltete Metadatenattribute müssen  
5028 mit sinnvollen Default-Werten vorbelegt werden.

5029 **AA\_14760-2425 - Nutzungsvorgaben für die Verwendung von XDS-Metadaten**

5030 Der XDS Document Service MUSS sicherstellen, dass Primärsysteme und das ePA-  
5031 Frontend des Versicherten zur Registrierung von Dokumenten die nachstehenden  
5032 Nutzungsvorgaben für Metadaten berücksichtigen. Der XDS Document Service MUSS  
5033 diese Metadaten verarbeiten können und diese Metadaten ggf. während des  
5034 Registriervorgangs ergänzen. Metadaten können über die Operationen

5035 • I\_Document\_Management::ProvideAndRegisterDocumentSet-b sowie

5036 • I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b

5037 registriert oder über die Operationen

5038 • I\_Document\_Management::RestrictedUpdateDocumentSet

5039 • I\_Document\_Management\_Insurant::RestrictedUpdateDocumentSet

5040 geändert werden.

5041 Für den Produkttyp DiGA gelten die gleichen Vorgaben wie für die Primärsysteme sofern  
5042 unter Nutzungsvorgaben keine abweichenden Bedingungen definiert werden.

5043 **Tabelle 30: Nutzungsvorgaben für Metadatenattribute XDS**

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd 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 <u>33.13.1.8.2- 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 <u>33.13.1.8.2- Metadaten der Dokumente und SubmissionSets</u> (A_21209) genügen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
authorRole	0. .n	0. .n	0. .0	0. .n	Rolle des Autors	Der Wert MUSS einem Code des <del>in [gemSpec_Voc_ePA] definierten</del> Value Sets für <del>DocumentEntry.authorRole_EPAXD</del> SAuthorRoleVS aus <del>[gemTerminology]</del> entsprechen.	X
authorSpeci alty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung des Autors	Der Wert MUSS einem Code des <del>in [gemSpec_Voc_ePA] definierten</del> Value Sets für <del>DocumentEntry.authorSpecialty_E</del> PAXDSAAuthorSpecialtyVS aus <del>[gemTerminology]</del> entsprechen.	X
authorTelec ommunicati on	0. .n	0. .0	0. .0	0. .n	Telekommunika tionsdaten des Autors	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.1.4.5] genügen.	X
availabilityStat us	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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
classCode	1. .1	1. .1	0. .0	1. .1	Grobe Klassifizierung des Dokuments	<p>Der Wert MUSS einem Code des <del>in [gemSpec_Voc_ePA] definierten</del> Value Sets für <del>DocumentEntry.classCodeEPAXDS</del> <u>ClassCodeVS</u> aus <u>[gemTerminology]</u> entsprechen.</p> <p>Sofern das Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt <del>33.13.1.9-</del> <u>Strukturierte Dokumente</u> genügen.</p> <p>PS-KTR MUSS für Dokumente</p> <ul style="list-style-type: none"> <li><u>der Kategorie receipt</u> ausschließlich den Code "ADM" (Administratives Dokument) <del>aus dem in [gemSpec_Voc_ePA] definierten Value Set</del> <u>verwenden</u></li> <li><u>und</u> für <u>DocumentEntry.classCodes</u> <u>olche der Kategorie</u> <u>health risk analysis den</u> <u>Code "ASM" (Assessment)</u> verwenden.</li> </ul>	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
	PS	KT R	D S	Fd V			
confidentiality Code	0. .n	0. .n	0. .1	0. .n	Vertraulichkeits kennzeichnung des Dokuments	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3# 4.2.3.2.5] genügen und <del>den Codes der in [gemSpec_Voc_ePA] definierten</del> einem Code des Value Sets für <del>DocumentEntry.confidentialityCode</del> <u>ePAXDSConfidentialityCodeVS</u> aus [gemTerminology] entsprechen.</p> <p>Für ProvideAndRegisterDocumentSet -b MUSS für das Verbergen des Dokumentes der Code</p> <ul style="list-style-type: none"> <li>Code = "CON", Display Name = "constraint"</li> </ul> <p>aus dem Code System 1.2.276.0.76.5.491 (siehe auch [gemSpec_Voc_ePA Value Set <u>EPAXDSConfidentialityCodeVS</u> aus [gemTerminology]]) gesetzt werden.</p>	X
creationTime	1. .1	1. .1	0. .0	1. .1	Erstellungszeitp unkt 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
	PS	KT R	D S	Fd V			
eventCodeList	0. .n	0. .0	0. .0	0. .n	Ereignisse, die zur Erstellung des Dokuments geführt haben.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.8] genügen und einem Code des <del>in</del> <u>[gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.eventCodeEPAXDSEventCodeVS aus [gemTerminology]</u> entsprechen.	X
formatCode	1. .1	1. .1	0. .0	1. .1	Global eindeutiger Code für das Dokumentenformat.  Zusammen mit dem DocumentEntry.typeCode eines Dokuments soll es einem potentiellen zugreifenden System erlauben, im Vorfeld festzustellen, ob das Dokument verarbeitet werden kann.	Der Wert MUSS einem Code des <del>in [gemSpec_Voc_ePA] definierten Value Sets für DocumentEntry.formatCode oder EPAXDSFormatCode aus der Tabelle in der Anforderung A-14761-*</del> <u>[gemTerminology]</u> entsprechen. Der Wert KANN "urn:ihe:iti:xds:2017:mimeTypeSufficient" (siehe [IHE-ITI-TF3#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 <del>33.13.1.9- Strukturierte Dokumente</del> genügen.	
hash	0. .0	0. .0	1. .1	0. .0	Kryptographische Prüfsumme des Dokuments	Der Wert wird vom XDS Document Service beim Einstellen des Dokuments in die Akte berechnet.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
healthcareFacilityTypeCode	1. .1	1. .1	0. .0	1. .1	Art der Einrichtung, in der das dokumentierte Ereignis stattgefunden hat.	Der Wert MUSS einem Code des in <del>[gemSpec_Voc_ePA]</del> definierten Value Sets für <del>DocumentEntry.healthcareFacilityTypeCode</del> <u>EPAXDSHealthcareFacilityTypeCodeVS</u> aus <u>[gemTerminology]</u> entsprechen. Das PS-KTR MUSS <u>healthcareFacilityTypeCode</u> ausschließlich <del>den Codem</del> mit dem Wert "VER" (Versicherungsträger) aus dem in <del>[gemSpec_Voc_ePA]</del> definierten Value Set für <del>DocumentEntry.healthcareFacilityTypeCode</del> verwenden. <u>belegen</u> . Die DiGA MUSS healthcareFacilityTypeCode mit dem Wert "PAT" belegen.	X
homeCommunityId	0. .1	0. .1	0. .0	0. .1		n/a Eine optional übertragene homeCommunityId wird nicht gespeichert.	
languageCode	1. .1	1. .1	0. .0	1. .1	Sprache, in der das Dokument abgefasst ist.	Der Wert MUSS einem Code des in <del>[gemSpec_Voc_ePA]</del> definierten Value Sets für <del>DocumentEntry.languageCode</del> <u>EPAXDSLlanguageCodeVS</u> aus <u>[gemTerminology]</u> entsprechen. Es MÜSSEN mindestens die in der Tabelle Tab_LanguageCodes angegebenen Codes unterstützt werden, alle weiteren Codes KÖNNEN unterstützt werden.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
legalAuthenticator	0. .1	0. .0	0. .0	0. .1	Rechtlich Verantwortliche r für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.14] genügen.  Das Attribut DARF NICHT gesetzt werden, falls es sich um ein automatisch erstelltes und nicht durch eine natürliche Person freigegebenes Dokument handelt.	
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierungsattribut, dass das Metadatenelement DocumentEntry nicht den vollständigen Satz an Metadaten enthält.		

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd 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><u>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</u></p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt <u>33.13.1.9- Strukturierte Dokumente</u> 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>	
patientId	1. .1	1. .1	0. .0	1. .1	Systemweit eindeutige Kennung des Patienten	<p>Der Wert MUSS den Inhalts- und Formatvorgaben aus A_14974* genügen.</p> <p>Außerdem MUSS der Wert der Identität des Akteninhabers entsprechen und MUSS vom XDS Document Service dahingehend bei Registrierung der Metadaten geprüft werden.</p>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
practiceSetting Code	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 in <del>[gemSpec_Voc_ePA]</del> definierten Value Sets für <del>DocumentEntry.practiceSettingCode</del> <u>de-EPAXDSPracticeSettingCodeVS</u> aus <u>[gemTerminology]</u> entsprechen. Die DiGA MUSS practiceSettingCode mit dem Wert "PAT" belegen.	X
referenceIdList	0. .n	0. <del>.0</del> <u>1</u>	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.  <u>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.</u>	
repositoryUniq ueId	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.	
serviceStartTi me	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
serviceStopTi me	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

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
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
	PS	KT R	D S	Fd V			
typeCode	1. .1	1. .1	0. .0	1. .1	Art des Dokuments	<p>Der Wert MUSS einem Code des in <del>[gemSpec_Voc_ePA]</del> definierten Value Sets für <del>DocumentEntry.typeCodeEPAXDS</del> <u>TypeCodeVS</u> aus <u>[gemTerminology]</u> entsprechen.</p> <p><u>PS-KTR MUSS für Dokumente der Kategorie health risk analysis ausschließlich den Code "GRIS" verwenden</u></p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Inhalts- und Formatvorgaben aus Abschnitt <del>33.13.1.9- Strukturierte Dokumente</del> 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.	
<b>Metadaten für SubmissionSet</b>							
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
	PS	KT R	D S	Fd V			
authorPerson	0. .1	0. .1	0. .0	<del>±0</del> .. 1	Name der einstellenden P erson oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus Abschnitt <del>33</del> 13.1.8.2- Metadaten der Dokumente und SubmissionSets genügen. <u>ePA-FdV</u> : 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. <u>Ist authorPerson nicht gesetzt, MUSS das ePA Aktensystem das Metadatenattribut authorPerson für Versicherte entsprechend der Vorgaben aus A_14762-* unter Verwendung der entsprechenden Informationen aus der User Session (KVNR, family_name und given_name) setzen. Das ePA Aktensystem KANN in einer übergebenen authorPerson den Nachnamen und Vornamen mit Informationen aus der User Session überschreiben.</u> PS/DiGAs können hier im Bedarfsfall Einträge für Software- Komponente bzw. Gerät als Autor entsprechend A_14762-* vornehmen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
authorInstitution	<del>1</del> 0 .. 1	<del>1</del> 0 .. 1	0. .0	0. .0	Institution, welcher die einstellende Person oder das einstellende System zugeordnet ist.	Der Wert MUSS den Formatvorgaben aus Abschnitt <del>33</del> 13.1.8.2- Metadaten der Dokumente und SubmissionSets (A_21209*) genügen. Das ePA-Aktensystem MUSS die Identität von TelematikID-basierten Identitäten mit den Inhalten aus authorInstitution prüfen. Eine Gleichheit liegt vor, wenn Telematik-ID aus der XCN-Struktur des Autors nach den Vorgaben von A_14763-* bzw. A_21511-* mit dem entsprechenden Wert aus der User Session übereinstimmt. <u>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.</u>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
authorRole	1. .n	1. .n	0. .0	1. .1	Rolle der einstellenden P erson oder des einstellenden Systems	Der Wert MUSS einem Code des <del>in [gemSpec_Voc_ePA] definierten</del> Value Sets für <del>DocumentEntry.authorRoleEPAXD</del> <u>SAuthorRoleVS</u> aus <u>[gemTerminology]</u> entsprechen. Das PS-KTR MUSS den Code "105" (Kostenträgervertreter) <del>aus dem in [gemSpec_Voc_ePA] definierten Value Set</del> für <del>DocumentEntry.authorRole</del> verwenden. Das ePA-Frontend des Versicherten MUSS den Code "102" (der Patient selbst) <del>aus dem in [gemSpec_Voc_ePA] definierten Value Set</del> für <del>DocumentEntry.authorRole</del> verwenden. Die DiGA MUSS authorRole mit dem Code "12" (dokumentierendes Gerät) <del>belegen</del> <u>verwenden</u> .	
authorSpecialty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung der einstellenden P erson oder des einstellenden Systems	Der Wert MUSS einem Code des <del>in [gemSpec_Voc_ePA] definierten</del> Value Sets für <del>DocumentEntry.authorSpecialtyEP</del> <u>AXDSAAuthorSpecialtyVS</u> aus <u>[gemTerminology]</u> entsprechen.	
authorTelecommunication	0. .n	0. .0	0. .0	0. .n	Telekommunikationsdaten der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	
availabilityStatus	0. .0	0. .0	1. .1	0. .0	Status des Submission Sets ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approved" entsprechen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise zum Submission Set in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.3.3] genügen.	X
contentTypeCode	0. .1	0. .1	0. .0	0. .1	Klinische Aktivität, die zum Einstellen des Submission Set geführt hat.	Der Wert MUSS einem Code des <del>in</del> <del>[gemSpec_Voc_ePA] definierten</del> Value Sets <del>für</del> <u>SubmissionSet.contentTypeCodeE</u> <u>PAXDScontentTypeCodeVS aus</u> <u>[gemTerminology]</u> 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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
sourceId	0. .0	0. .0	0. .0	0. .0	Weltweit eindeutige, unveränderlich e Kennung des einstellenden Systems		
submissionTime	1. .1	1. .1	0. .0	1. .1	Zeit, zu der das Submission Set zusammengest ellt 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.	
<b>Metadaten für dynamische Folder</b>							
availabilityStatus	1. .1	n/ a	0. .0	n/ a	Status des Ordnern ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approved" entsprechen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
codeList	1. .1	n/ a	0. .0	n/ a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] und <del>[ValueSet-Speciality-Oth]</del> <u>genügen einem Code des Value Sets EPaDataCategoryOtherVS aus [gemTerminology] entsprechen.</u> Bei Folder.codeList=pregnancy_childbirth MUSS das Primärsystem diese Codes angeben.	
comments	0. .1	n/ a	0. .0	n/ a	Freitextkommentar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen.	
entryUUID	1. .1	n/ a	1. .1	n/ a	Intern verwendete, aktenweit eindeutige Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
lastUpdateTime	0. .0	n/ a	1. .1	n/ a	Zeitstempel, an dem der Ordner das letzte mal geändert wurde	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.6] genügen. Der XDS Document Service MUSS den Wert automatisch gemäß [IHE-ITI-TF2b#3.42.4.1.3.6] aktuell halten.	
limitedMetadata	Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden.						
patientId	1. .1	n/ a	0. .0	n/ a	Patienten ID, zu der der Ordner gehört.	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	



Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd V			
title	1. .1	n/ a	0. .0	n/ a	Titel des Ordnern	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.8] genügen.	
uniqueId	1. .1	n/ a	0. .0	n/ a	Eindeutige, aktenweite Kennung des Ordnern	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.9] genügen.	
<b>Metadaten für statische Folder</b>							
availabilityStat us	n/ a	n/ a	1. .1	n/ a	Status des Ordnern ("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 <del>[ValueSet-Speciality-Oth]</del> <u>einem Code des Value Sets</u> <u>EPADDataCategoryOtherVS</u> und <del>[ValueSet-Speciality-Med]</del> <u>genügen.</u> <u>EPADDataCategoryMedicalVS aus</u> <u>[gemTerminology] entsprechen.</u> Der XDS Document Service MUSS codeList gemäß A_19388* setzen.	
comments	n/ a	n/ a	0. .1	n/ a	Freitextkomme ntar 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 Ordnern	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.	
homeCommun ityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	PS	KT R	D S	Fd 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.	
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.	

5044  
5045**Tabelle 31: Tab\_LanguageCodes - Mindestanforderung an zu unterstützende Language Codes**

Language / Country Code Kombination	Language / Country Code Kombination
bg-BG (bulgarisch, Bulgarien)	it-IT (italienisch, Italien) it-CH (italienisch, Schweiz)
cs-CZ (tschechisch, Tschechien)	lt-LT (litauisch, Litauen)
da-DK (dänisch, Dänemark)	lb-LU (luxemburgisch, Luxemburg)

Language / Country Code Kombination	Language / Country Code Kombination
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)	n1-NL (niederländisch, Niederlande) n1-BE (niederländisch, Belgien)
es-ES (spanisch, Spanien)	no-NO (norwegisch, Norwegen)
et-EE (estnisch, Estland)	pl-PL (polnisch, Polen)
fi-FI (finnisch, Finnland)	pt-PT (portugiesisch, Portugal)
fr-FR (französisch, Frankreich) fr-CH (französisch, Schweiz) fr-LU (französisch, Luxemburg) fr-BE (französisch, Belgien)	rm-CH (rätoromanisch, Schweiz)
ga-IE (irisch, Irland)	ro-RO (rumänisch, Rumänien)
hr-HR (kroatisch, Kroatien)	sk-SK (slowakisch, Slowakei)
hu-HU (ungarisch, Ungarn)	sl-SI (slowenisch, Slowenien)
is-IS (isländisch, Island)	sv-SE (schwedisch, Schweden)

5046

5047 [**<=**]5048 *3.13.1.8.2 Metadaten der Dokumente und SubmissionSets*5049 **A\_23369-02 - XDS Document Service – Verpflichtender Dokumententitel in DocumentEntry.title**

5050 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von  
 5051 Dokumenten und dem Ändern von Metadaten an Dokumenten `DocumentEntry.title`  
 5052 befüllen. Der Titel des Dokumentes soll eine fachliche Beschreibung des Dokumentes  
 5053 enthalten. Bei `DocumentEntry.title` MÜSSEN führende und endende Leerzeichen  
 5054 entfernt werden. In `DocumentEntry.title` DARF NICHT leer sein (`!= ""`) (insbesondere  
 5055 auch nicht nach etwaigen Entfernen von Leerzeichen vorne und hinten). In  
 5056 `Document.title` DÜRFEN keine nicht-druckbaren Zeichen enthalten sein. [**<=**]  
 5057

5058 **A\_25188 - XDS Document Service - Input Sanitization**

5059 Der XDS Document Service MUSS sicherstellen, dass bei Anlage und Aktualisierung  
 5060 (Ändern) von Metadaten:

- 5061 1. führende (leading) und endende (trailing) Whitespace von den Attributen
- 5062 automatisch entfernt werden.
- 5063 2. die notwendigen Attribute nichtleer sind (insbesondere auch noch Whitespace-
- 5064 Entfernung aus 1.). und
- 5065 3. Die Attribute nur druckbare Zeichen enthalten.

5066 [`<=`]

5067 **A\_14762-05 - XDS Document Service – Nutzungsvorgabe für `authorPerson` als**  
 5068 **Teil von `DocumentEntry.author` und `SubmissionSet.author`**

5069 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von  
 5070 Dokumenten und dem Ändern von Dokumenten-Metadaten an `authorPerson` unterhalb  
 5071 von `DocumentEntry.author` und `SubmissionSet.author` neben [IHE-ITI-  
 5072 TF3#4.2.3.1.4.2] auch die folgenden Vorgaben beachten.

5073

5074 **Bei Leistungserbringer als Autor:**

- 5075 1. Lebenslange Identifikationsnummer eines Arztes (Lebenslange Arztnummer -
- 5076 LANR 9 Stellen) oder im Falle eines Zahnarztes die Zentrale Zahnarzt Nummer
- 5077 (ZANR)- sofern die ZANR bekannt ist
- 5078 2. `"^"`
- 5079 3. Nachname
- 5080 4. `"^"`
- 5081 5. Vorname
- 5082 6. `"^"`
- 5083 7. Weiterer Vorname
- 5084 8. `"^"`
- 5085 9. Namenszusatz
- 5086 10. `"^"`
- 5087 11. Titel
- 5088 12. `"^^^&"` - sofern LANR oder ZANR angegeben, ansonsten `"^^^"`
- 5089 13. `"1.2.276.0.76.4.16"` - sofern LANR angegeben oder `"1.2.276.0.76.4.296"`, falls
- 5090 ZANR angegeben
- 5091 14. `"&ISO"` - sofern LANR oder ZANR angegeben

5092 **Beispiele:**

5093 `165746304^Weber^Thilo^^^Dr.^^^&1.2.276.0.76.4.16&ISO`  
 5094 `^Zahnschmerz^Eberhard^^^Dr.^^^`

5095

5096 **Bei Versichertem als Autor:**

- 5097 1. Der unveränderbare Teil der KVNR (10 Stellen)
- 5098 2. `"^"`
- 5099 3. Nachname
- 5100 4. `"^"`
- 5101 5. Vorname

- 5102 6. "^"
- 5103 7. Weiterer Vorname
- 5104 8. "^"
- 5105 9. Namenszusatz
- 5106 10. "^"
- 5107 11. Titel
- 5108 12. "^^^&"
- 5109 13. "1.2.276.0.76.4.8"
- 5110 14. "&ISO"
- 5111 Beispiel: G995030566^Gundlach^Monika^^^^^&1.2.276.0.76.4.8&ISO
- 5112 Sowohl beim LE als auch beim Versicherten müssen Vorname und Nachname belegt
- 5113 werden.
- 5114
- 5115 **Software-Komponente bzw. Gerät als Autor**
- 5116 Beim (automatisierten) Einstellen von Dokumenten MUSS der max. 256-Zeichen lange
- 5117 Name der Software-Komponente bzw. des Geräts als Nachname und ggf. als Vorname(n)
- 5118 eingetragen werden.
- 5119 Beispiel: ^PHR-Gerät-XY^PHR-Software-XY
- 5120 Im Falle einer DiGA MUSS das Feld Autor folgendermaßen aufgebaut sein:
- 5121 1. Telematik-ID der DiGA
- 5122 2. "A"
- 5123 3. Name der DiGA (Name der Verordnungseinheit)
- 5124 4. "A"
- 5125 5. Name des DiGA-Herstellers
- 5126 6. "A"
- 5127 7. optionale Ergänzung der Bezeichnung der SW
- 5128 8. "A"
- 5129 9. optionale Ergänzung der Bezeichnung der SW
- 5130 10. "A"
- 5131 11. optionale Ergänzung der Bezeichnung der SW
- 5132 12. "^^^&"
- 5133 13. <OID für DiGAs, wie in professionOID>
- 5134 14. "&ISO"
- 5135
- 5136 Für alle drei Arten von Autoren (Versicherter, LE, Gerät) MUSS jeweils Vorname und
- 5137 Nachname angegeben sein. [ <= ]
- 5138 **A\_14763-03 - XDS Document Service - Nutzungsvorgabe für**
- 5139 **SubmissionSet.authorInstitution**
- 5140 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
- 5141 Dokumenten und dem Ändern von Dokumenten-Metadaten an

5142 SubmissionSet.authorInstitution neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die  
5143 folgenden Vorgaben beachten.

- 5144 1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
- 5145 2. "^^^^^&"
- 5146 3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine  
5147 Telematik-ID)
- 5148 4. "&ISO^^^^"
- 5149 5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

5150 Beispiele:

- 5151 • Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-  
5152 e518
- 5153 • gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^8-  
5154 34923902a

5155 [**<=**]

#### 5156 **A\_21511-01 - Nutzungsvorgabe SubmissionSet.authorInstitution für DIGAs**

5157 Der XDS Document Service MUSS sicherstellen, dass DiGAs beim Upload von  
5158 Dokumenten, die folgenden Nutzungsvorgaben für das Metadatenattribut  
5159 DocumentEntry.authorInstitution sowie SubmissionSet.authorInstitution berücksichtigen.  
5160 Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.1.4.1] genügen und ist inhaltlich  
5161 nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen.

- 5162 1. Name des Anbieters der DiGA
- 5163 2. "^^^^^&"
- 5164 3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine  
5165 Telematik-ID)
- 5166 4. "&ISO^^^^"
- 5167 5. Telematik-ID der DiGA

5168 [**<=**]

5169

#### 5170 **A\_21209-02 - XDS Document Service - Nutzungsvorgabe für** 5171 **DocumentEntry.authorInstitution**

5172 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von  
5173 Dokumenten und dem Ändern von Dokumenten-Metadaten an  
5174 DocumentEntry.authorInstitution neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die  
5175 folgenden Vorgaben beachten.

- 5176 1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
- 5177 2. "^^^^^&"
- 5178 3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine  
5179 Telematik-ID)
- 5180 4. "&ISO^^^^"
- 5181 5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

5182 Die Komponenten 2.-5. sind nur anzugeben, wenn die Telematik ID (5.) der  
5183 Autoreninstitution bekannt ist oder ad-hoc ermittelt werden kann, bspw. über den

Verzeichnisdienst der TI-Plattform (VZD). Ansonsten wird ausschließlich der Name gesetzt.

Beispiele:

- Arztpraxis Dr. Thilo Weber^^^^^1.2.276.0.76.4.188&ISO^^^^1-2c47sd-e518
- gematik Betriebskrankenkasse^^^^^1.2.276.0.76.4.188&ISO^^^^8-34923902a
- Arztpraxis Dr. Wiebke Werner

[<=]

### A\_22408-02 - XDS Document Service - DocumentEntry.authorInstitution ohne Telematik-ID

Der XDS Document Service MUSS Nachrichten zum Registrieren von Dokumenten bei fehlender Telematik-ID in DocumentEntry.authorInstitution akzeptieren und daraufhin alle Zeichen hinter dem Namen der authorInstitution abschneiden und verwerfen.[<=]

### A\_14974-02 - XDS Document Service - Nutzungsvorgabe für DocumentEntry.patientId und SubmissionSet.patientId

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten die folgenden Nutzungsvorgaben für DocumentEntry.patientId und SubmissionSet.patientId berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.2.16] bzw. [IHE-ITI-TF3#4.2.3.3.8] genügen und ist inhaltlich nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen:

1. Der unveränderbare Teil der KVNR des Akteninhabers (10 Stellen)
2. "^^^&"
3. "1.2.276.0.76.4.8" (OID zur Kennzeichnung einer unveränderbaren KVNR)
4. "&ISO"

Beispiel: G995030566^^^&1.2.276.0.76.4.8&ISO[<=]

### 3.13.1.8.3 Metadaten für Datenkategorien

#### AA\_19388-2021 - Nutzungsvorgaben für die Verwendung von Datenkategorien

Der XDS Document Service MUSS beim Einstellen eines Dokuments und beim Ändern von Metadaten die folgende Zuordnung zu einer Datenkategorie (d. h. Assoziierung mit einem bestimmten Folder) vornehmen. Dabei haben Auswertungs- und Zuordnungsregeln, die sich aus A\_14761-\* und damit verbunden aus [gemSpec\_IG\_ePA] ableiten, immer den Vorrang gegenüber anderen Auswertungsregeln. Ferner MUSS der XDS Document Service sicherstellen, dass bei einer Aktualisierung eines Dokuments derselbe Ordner des zu ersetzenden Dokuments zugeordnet wird.

Für eine eindeutige Zuordnung zu einer Datenkategorie MUSS die Auswertung der Metadatenvorgaben in der Reihenfolge der folgend dargestellten Einsortierungskriterien erfolgen:



5225 **Tabelle 32: 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
<u>health_risk_analysis</u>	<u>healthcareFacilityTypeCode = VER und</u> <u>typeCode = GRIS und</u> <u>DocumentEntry.authorRole=105 und</u> <u>Submissionset.authorRole = 105</u>
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"> <li>• ED110102 (KDL-Code Notfalldatenmanagement (NFD))</li> <li>• AU190104 (KDL-Code Notfalldatensatz)</li> <li>• AD020105 (KDL-Code Notfall-/Vertretungsschein)</li> </ul>
transcripts	eventCodeList = <ul style="list-style-type: none"> <li>• UB999997 (KDL-Code Gesamtdokumentation stationäre Versorgung) oder</li> <li>• UB999998 (KDL-Code Gesamtdokumentation ambulante Versorgung)</li> </ul>

Datenkategorie/Technischer Identifier/Foldercode	Einsortierkriterium (anzuwenden auf DocumentEntry, wenn nicht anders angegeben. Oder-Verknüpfungen, wenn nicht "und" angegeben)
reports	classCode = ANF, ASM, BEF, BIL, DOK, DUR, LAB oder PLA
other	Alle Dokumente, die in keine andere Kategorien eingeordnet werden können

5226 \*Falls Basiskonzepte angegeben werden, dann gelten automatisch alle Subkonzepte, z.B.  
 5227 gilt für die Kategorie "care" die Einsortierregel bei PracticeSettingCode = PFL wie auch für  
 5228 die Sub-Konzepte ALT (Altenpflege) und KIN (Kinderpflege).[<=]

### 5229 3.13.1.9 Strukturierte Dokumente

5230 Die elektronische Patientenakte unterstützt unterschiedliche sogenannte "strukturierte  
 5231 Dokumente", deren Aufbau über Implementation Guides genau vorgegeben ist. Der  
 5232 Umfang der unterstützten strukturierten Dokumente wird durch den Umfang der  
 5233 veröffentlichten Implementation Guides festgelegt (3.13.1.9.2- Konfigurierbarkeit ). Für  
 5234 alle strukturierten Dokumente gelten spezifische Metadatenvorgaben, um sie eindeutig zu  
 5235 identifizieren und gezielt verarbeiten zu können.

#### 5236 A\_14761-08 - Nutzungsvorgaben für die Verwendung von IHE ITI XDS- 5237 Metadaten bei strukturierten Dokumenten

5238 Der XDS Document Service MUSS die Nutzungsvorgaben für strukturierte Dokumente  
 5239 unter [gemSpec\_IG\_ePA] berücksichtigen. Dabei ist das Format des Dokuments, welches  
 5240 über einen Code des Metadatenattributs `formatCode` ausgedrückt wird, führend. Das  
 5241 bedeutet, bei Registrierung eines strukturierten Dokuments mit einem `formatCode`  
 5242 MÜSSEN die weiteren Metadatenattribute `classCode`, `typeCode`, `mimeType` sowie  
 5243 `eventCodeList` entsprechend belegt werden. Der XDS Document Service MUSS eine  
 5244 solche Registrierung diesbzgl. prüfen und im Fehlerfall analog zu A\_14938-\* antworten.  
 5245 [<=]

#### 5246 3.13.1.9.1 Sammlungstypen

5247 Je nach Art ihrer Zusammensetzung und ihrer Handhabung existieren unterschiedliche  
 5248 Typen strukturierter Dokumente, sogenannte medizinische Informationsobjekte. Ein  
 5249 medizinisches Informationsobjekt (MIO) ist eine **Sammlung** von Informationen zu  
 5250 medizinischen, strukturellen oder administrativen Sachverhalten, die in sich geschlossen  
 5251 oder entsprechend verschachtelt vorliegt. Zudem ist ein MIO eine klar definierte Vorgabe,  
 5252 wie diese Informationssammlung in der elektronischen Patientenakte gespeichert wird,  
 5253 damit semantische und syntaktische Interoperabilität gewährleistet werden. Die  
 5254 Festlegung dieser Vorgaben ist gemäß SGB V Aufgabe der KBV. Beispiele für  
 5255 medizinische Informationsobjekte sind der Impfpass, das Kinderuntersuchungsheft, der  
 5256 Mutterpass, das zahnärztliche Bonusheft, oder DiGA. MIOs werden über Sammlungen  
 5257 und Sammlungstypen umgesetzt.

5258 Einige strukturierte Dokumente sind für sich genommen vollständig und schlüssig wie z.  
 5259 B. ein Elektronischer Arztbrief. Sie sind ohne Zuhilfenahme weiterer Dokumente in der  
 5260 ePA für einen Benutzer sinnvoll zu verwenden. Andere Typen strukturierter Dokumente  
 5261 müssen hingegen fast immer in Kombination betrachtet werden, z. B.  
 5262 Impfpassdokumente. Bei letzteren spiegelt jedes Impfpassdokument ein oder mehrere  
 5263 Impfungen wieder. Ein Impfpass, wie er in der analogen Welt geläufig und als logisches

5264 Konstrukt sinnvoll ist, besteht immer aus der gemeinsamen Betrachtung  
 5265 aller Impfpassdokumente und somit aller vorhandenen Impfeinträge. Die Kombination ein  
 5266 oder mehrerer strukturierter Dokumente ergeben eine Sammlung.

5267 Eine Sammlungsinstanz (z. B. der Mutterpass der ersten Schwangerschaft der Patientin  
 5268 Martha Mustermann) ist eine konkrete Ausprägung der Information, die zwischen den  
 5269 beteiligten Akteuren ausgetauscht wird. Nicht jede Sammlung besteht zwangsläufig aus  
 5270 Dokumenten desselben Formats: Ein Kinderuntersuchungsheft beispielsweise besteht aus  
 5271 Dokumenten mit drei verschiedenen strukturierten Dokumenttypen. Zentral für alle  
 5272 Sammlungstypen ist immer mindestens ein strukturiertes Dokument mit einem  
 5273 festgelegten Dokumentenformat. Für eine technische Umsetzung sind die  
 5274 Sammlungstypen "mixed" und "uniform" zu unterscheiden, die technisch unterschiedlich  
 5275 umgesetzt werden und zum Teil unterschiedliche Operationen erlauben.

5276 Der Sammlungstyp "mixed" fasst semantisch zusammengehörige, strukturierte  
 5277 Dokumente unterschiedlicher Struktur mittels Ordner zu einer Sammlung zusammen. Der  
 5278 Sammlungstyp "uniform" wird ebenfalls intern über Ordner abgebildet. Dies stellt sicher,  
 5279 dass zukünftige Versionen dieser strukturierten Dokumente/Pässe oder DiGA verlässlich  
 5280 verarbeitet werden können. Ordner gelten als "statische Ordner", bis auf Sammlungen  
 5281 der Kategorie Mutterpass und DiGA ("dynamische Ordner"). Der dynamische Ordner für  
 5282 einen konkreten Mutterpass wird durch den Client angelegt, weil es aus Gründen, die nur  
 5283 der Client kennt (Anzahl der Schwangerschaften), mehrere Ordner dieses Typs geben  
 5284 kann ("nicht-statische Ordner", vgl. A\_21610-\*). Die Version der Struktur eines  
 5285 Dokuments ist am Format Code erkennbar.

5286 Passdokumente

#### 5287 **A\_20577-06 - Definition und Zuweisung von Sammlungstypen**

5288 Der XDS Document Service MUSS jeder Sammlung einen von zwei Sammlungstypen  
 5289 zuweisen:

#### 5290 **Tabelle 33: 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.

5291 Es gelten die Metadaten für strukturierte Dokumente gemäß [gemSpec\_IG\_ePA]. In den  
 5292 unter [gemSpec\_IG\_ePA] gemachten Vorgaben werden auch Ordner-Kardinalitäten für  
 5293 spezifische Sammlungen festgelegt. Diese Angaben sagen aus, wie viele Instanzen einer  
 5294 Sammlung (d. h. minimal und maximal) registriert werden können. [ $\leq$ ]

#### 5296 **A\_20707-04 - XDS Document Service – Keine unpassenden Dokumente in nicht-** 5297 **statische Ordner**

5298 Falls das Dokument nicht den Vorgaben der Metadaten für strukturierte Dokumente  
 5299 gemäß [gemSpec\_IG\_ePA] entspricht, MUSS der XDS Document Service das Registrieren  
 5300 und Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-

5301 Fehlercode `BadFolderAssociation` quittieren. Es MUSS im `codeContext`-Attribut  
5302 des zurückgegebenen `rs:RegistryError`-Elements die  
5303 UUID (`DocumentEntry.entryUUID`) des identifizierten Dokuments angegeben  
5304 werden. [`<=`]

5305 **AA\_20581-0506 - XDS Document Service – Löschen von Dokumenten aus**  
5306 **Sammlungen der Typen "mixed" und "uniform" durch ein ePA-FdV**

5307 Der XDS Document Service MUSS beim Löschen eines Dokuments der Sammlungstypen  
5308 "mixed" und "uniform" durch das ePA-FdV sicherstellen, dass die Operation mit dem  
5309 Fehler ~~`ReferencesExistsException`~~`ReferencesExistException` abgebrochen wird,  
5310 wenn die Löschanfrage nicht alle Dokumente der Sammlung enthält. Es besteht folgende  
5311 Ausnahme: Das Löschen einer Elternnotiz im Kinderuntersuchungsheft ist erlaubt. [`<=`]

5312 Nur Leistungserbringern ist es erlaubt, einzelne Dokumente aus Sammlungen der Typen  
5313 "mixed" und "uniform" zu löschen, um die medizinische Interpretation der gesamten  
5314 Sammlungsinstanz nicht zu gefährden.

5315 *Hinweis: Die zeitliche Gültigkeit ergibt sich aus den Attributen "validFrom" und (optional)*  
5316 *"clientReadOnlyFromDate" der Vorgaben in [gemSpec\_IG\_ePA].*

5317 **3.13.1.9.2 Konfigurierbarkeit**

5318 **A\_17546-02 - Konfigurierbarkeit von strukturierten Dokumenten**

5319 Der XDS Document Service MUSS die Liste strukturierter Dokumente konfigurierbar  
5320 machen, indem dieser die Unterstützung strukturierter Dokumente unter Angabe  
5321 folgender Eigenschaften ermöglicht:

- 5322     • Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec\_IG\_ePA]  
5323     konfigurativ hinzufügen bzw. entfernen,
- 5324     • Sammlungen zu `TAB_EPA_Sammlungstypen`  
5325     gemäß [gemSpec\_IG\_ePA] konfigurativ hinzufügen bzw. entfernen.

5326 [`<=`]

5327 Das Entfernen der Unterstützung von strukturierten Dokumenten oder  
5328 Sammlungen bedeutet, dass diese zu einem früheren Zeitpunkt in das Aktensystem  
5329 geschrieben werden konnten, aber durch Erreichen von "clientReadOnlyFromDate" nicht  
5330 mehr geschrieben werden dürfen. Das Schreiben umfasst das Aktualisieren oder neu  
5331 Anlegen. Das Lesen ist weiterhin erlaubt.

5332 **A\_17551-01 - Prüfanforderungen zur Konfigurierbarkeit von Value Sets**

5333 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die zu konfigurierenden  
5334 Value Sets des XDS Document Service gemäß der Anforderung A\_17546-\* den  
5335 folgenden Prüfkriterien unterliegen, bevor bestehende, im XDS Document Service  
5336 verarbeitete Value Sets verändert werden:

- 5337     • Es DÜRFEN KEINE Codes der Value Sets gelöscht werden, lediglich das Hinzufügen  
5338     von Codes zu existierenden Value Sets ist aus Kompatibilitätsgründen erlaubt.
- 5339     • Neue Codes MÜSSEN den Formatvorgaben gemäß Tabelle 4.2.3.1.7-2 in [IHE-ITI-  
5340     TF3#4.2.3.1.7] entsprechen und gegenüber einer internen Referenzliste validiert  
5341     werden. Dies schließt auch Prüfungen zur Zeichenkodierung, der Datentypen als  
5342     auch zu den Längenbeschränkungen ein.

5343 [`<=`]

5344 **A\_21212-01 - Restriktionen zur Konfigurierbarkeit von Metadaten für**  
5345 **strukturierte Dokumente und Sammlungen**

5346 Der XDS Document Service MUSS durch technische Maßnahmen sicherstellen, dass  
 5347 Änderungen an den in den Implementierungsvorgaben in [gemSpec\_IG\_ePA]  
 5348 spezifizierten Codes ausgeschlossen sind. [≤]

### 5349 **A\_21214-03 - Konfiguration strukturierter Dokumente im Rahmen der** 5350 **Veröffentlichung durch die gematik**

5351 Der Anbieter des ePA-Aktensystems MUSS durch organisatorische Maßnahmen  
 5352 sicherstellen, dass die Konfiguration im Aktensystem zur Unterstützung strukturierter  
 5353 Dokumente aus [gemSpec\_IG\_ePA] ausschließlich im Rahmen der Veröffentlichung der  
 5354 Implementation Guides durch die gematik erfolgt. [≤]

5355 Bei Einführung neuer strukturierter Dokumente werden die beschriebenen  
 5356 Konfigurationsmöglichkeiten so verwendet, dass eine Erweiterung der Spezifikation und  
 5357 daraus resultierend eine Änderung des ePA-Aktensystems mit erneuter Zulassung nicht  
 5358 erforderlich sind.

### 5359 **3.13.1.10 Verbergen von Dokumenten durch Verwendung des** 5360 **confidentialityCode**

5361 Der Versicherte oder ein Vertreter kann vorhandene Dokumente des Aktenkontos durch  
 5362 die Verwendung der General Deny Policy des Constraint Managements verbergen oder  
 5363 sichtbar machen.

5364 Der Versicherte oder ein Vertreter kann ein neues Dokument ~~kann auch~~ direkt beim  
 5365 Einstellen ~~des Dokuments verbergen werden in das Aktenkonto verbergen~~. Dazu wird  
 5366 durch den XDS Document Service beim Einstellen bzw. Aktualisieren (Replace) eines  
 5367 Dokuments der DocumentEntry.confidentialityCode der Dokumentmetadaten  
 5368 ausgewertet. Enthält der confidentialityCode beim Einstellen bzw. Aktualisieren den Wert  
 5369 "CON" (constraint), wird durch das Aktensystem ein Eintrag in der General Deny Policy  
 5370 erzeugt und das Dokument verbergen.

5371 ~~Dieses Verbergen von Dokumenten kann Diese zusätzliche Art des direkten Verbergens~~  
 5372 ~~ist dabei grundsätzlich nur auf Anweisung Dokumententypen anwendbar, welche~~ durch  
 5373 ~~deneinen~~ Versicherten oder einen Vertreter ~~auch aus der Umgebung der~~  
 5374 ~~Leistungserbringer erfolgen. Aus der Umgebung der Leistungserbringer über ein ePA-FdV~~  
 5375 ~~eingestellt werden können auf diesem Weg Dokumente lediglich verbergen werden.~~  
 5376 ~~Verborgene Inhalte können aus der Umgebung der Leistungserbringer nicht sichtbar~~  
 5377 ~~gemacht werden.~~

5378 ~~Diese Art des Verbergens ist nicht auf Dokumente anwendbar, die Bestandteil eines~~  
 5379 ~~Ordners des Typs "mixed" oder "uniform" sind. Die dort enthaltenen (keine MIOs oder~~  
 5380 ~~strukturierter Dokumente können nur durch ein ePA-FdV kategorie- oder ordnerbasiert~~  
 5381 ~~verbergen werden.-).~~

5382 Das Metadatum DocumentEntry.confidentialityCode = "CON" (codeSystem =  
 5383 urn:oid:1.2.276.0.76.5.491:

- 5384 1. Führt beim Einstellen und Replace eines Dokuments zum Verbergen des  
 5385 Dokuments, d.h. das Dokument wird auf die General Deny Policy des Aktenkontos  
 5386 gesetzt.
- 5387 2. Wird im Aktensystem nicht persistiert sondern über dort intern über eine General  
 5388 Deny Policy umgesetzt.
- 5389 3. Wird im ePA-FdV nicht zur Anzeige gebracht und kann dort auch nicht geändert  
 5390 werden.

4. Ein PS darf DocumentEntry.confidentialityCode = "CON" nicht ~~aus den gespeicherten Daten zum Einstellen bzw. Replace verwenden. Der aktuelle Wille des Versicherten entscheidet über das Verbergen verwenden.~~

~~Für ein verborgenes Dokument gelten für eine LEI folgende Einschränkungen:~~

- ~~1. Löschen ist nicht erlaubt~~
- ~~2. Aktualisieren von Metadaten ist nicht erlaubt~~
- ~~3. Herunterladen ist nicht erlaubt~~
- ~~4. Suchen: die Suchergebnismenge enthält ausschließlich XDS-Metadaten nicht verborgener Dokumente~~

### 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:

**Tabelle 34: Auswirkungen bei Widerspruch gegen eine Funktion der ePA**

widerspruchsfähige Funktion	Auswirkung bei erteiltem Widerspruch
Teilnahme am digital gestützten Medikationsprozess ("medication")	Das Einstellen, Verändern, Lesen oder Suchen von Dokumenten des Ordners "emp" (elektronischer Medikationsplan) wird durch den XDS Document Service abgelehnt. Ausgenommen hiervon sind der Versicherte und befugte Vertreter.
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst ("erp-submission")	Alle vorhandenen Dokumente des Ordners "emp" (elektronischer Medikationsplan) werden gelöscht.

*Hinweis zum Medikationsprozess: Dadurch wird verhindert, dass Leistungserbringer im Versorgungsprozess veraltete oder unvollständige Daten verwenden.*

#### **A\_23860 - XDS Document Service - Löschen der Dokumente des Medikationsprozesses**

Der XDS Document Service des Aktensystems MUSS alle Dokumente aus dem Ordner elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") löschen, wenn der Status der widerspruchsfähigen Funktion "Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst" (Id = "erp-submission") auf "Widerspruch erklärt" ("deny") geändert wird. [ $\leq$ ]

#### **A\_23895-02 - XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch**

Falls ein Widerspruch zur widerspruchsfähigen Funktion "Teilnahme am Medikationsprozess" (Id = "medication" und status = "deny") vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem =



5423 "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für alle Nutzer, ausgenommen der  
 5424 Versicherte oder befugte Vertreter (oid\_versicherter), ablehnen und die Operation mit  
 5425 dem Fehlercode ConsentDecisionViolation abbrechen.  
 5426 [ $\leq$ ]

#### 5427 **A\_25151-01 - XDS Document Service – Prüfung der Widersprüche bei** 5428 **Suchanfrage**

5429 Der XDS Document Service MUSS bei einer Suchanfrage die Suchergebnismenge für alle  
 5430 Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid\_versicherter), filtern  
 5431 und sicherstellen, dass diese keinerlei XDS-Metadaten von Dokumenten des Ordners  
 5432 elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code =  
 5433 "eMP") enthält, wenn ein Widerspruch gegen die widerspruchsfähige Funktion "Teilnahme  
 5434 am digital gestützten Medikationsprozess" (Id = "medication" und status = "deny")  
 5435 vorliegt.  
 5436 [ $\leq$ ]

### 5437 **3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des** 5438 **Medication Service durch eine spezifische LEI auf die Dokumente des** 5439 **Aktenkontos**

5440 Wird ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische  
 5441 LEI erklärt, verhindert der XDS Document Service, dass auf die Dokumente der Kategorie  
 5442 "emp" zugegriffen werden kann.

#### 5443 **A\_26429 - XDS Document Service - Keine Operationen mit Dokumenten des** 5444 **Medikationsprozesses bei Widerspruch gegen die Nutzung des Medication** 5445 **Service durch eine spezifische LEI**

5446 Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische  
 5447 LEI vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und  
 5448 Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan  
 5449 (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für diese LEI, ablehnen und  
 5450 die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.  
 5451 [ $\leq$ ]

#### 5452 **A\_26430 - XDS Document Service – Prüfung des Widerspruchs gegen die** 5453 **Nutzung des Medication Service durch eine spezifische LEI bei Suchanfrage**

5454 Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische  
 5455 LEI vorliegt, MUSS der XDS Document Service bei einer Suchanfrage die  
 5456 Suchergebnismenge für diese LEI filtern und sicherstellen, dass die  
 5457 Suchergebnismenge keinerlei XDS-Metadaten von Dokumenten des Ordners  
 5458 elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code =  
 5459 "eMP") enthält.  
 5460 [ $\leq$ ]

5461

5462

### 5463 **3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service**

#### 5464 **A\_24715-01 - XDS Document Service - Protokolleinträge für Zugriffe auf den** 5465 **XDS Document Service**

5466 Der XDS Document Service MUSS für die Operationen

- 5467 • ProvideAndRegisterDocumentSet-b,
- 5468 • RetrieveDocumentSet,



- 5469      • RemoveMetadata,
- 5470      • RestrictedUpdateDocumentSet,
- 5471      • RegistryStoredQuery (entfällt, wenn Nutzung durch den Versicherten erfolgt)

5472 Protokolleinträge gemäß A\_24704\* erzeugen und dabei folgende Wertebelegung

5473 berücksichtigen:

5474 **Tabelle 35: XDS Document Service Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"document"		
AuditEvent.action	C		Für ProvideAndRegisterDocumentSet-b ohne Replace Option
	U		Für ProvideAndRegisterDocumentSet-b mit Replace Option
	U		Für RestrictedUpdateDocumentSet
	R		Für RegistryStoredQuery
	R		Für RetrieveDocumentSet
	D		Für Zugriffe mit RemoveMetadata
AuditEvent.entity.description	<Operation>		ein Wert aus {ProvideAndRegisterDocumentSet-b, RetrieveDocumentSet, RemoveMetadata, RestrictedUpdateDocumentSet, RegistryStoredQuery}
Parameterwerte für die Operationen ProvideAndRegisterDocumentSet-b, RetrieveDocumentSet und RemoveMetadata			
AuditEvent.entity.name	<DocumentEntry.title>		wenn in der entity Struktur ein XDSDocument beschrieben wird
	<Folder.title>		wenn in der entity Struktur ein XDSFolder beschrieben wird
	type	value[x]	

Strukturelement	Wert		Erläuterung
AuditEvent.entity.detail	"DocumentFormatCode"	<DocumentEntry.formatCode>	wenn in der entity Struktur ein XSDDocument 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 XSDDocument 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
<b>Parameterwerte für die Operation RegistryStoredQuery der Schnittstellen I_Document_Management und I_Document_Management_Insurant (nur Vertreter)</b>			
AuditEvent.entity.name	"AdhocQuery"		fester Wert
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	"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.
<b>Parameterwerte für die Operation RestrictedUpdateDocumentSet</b>			

Strukturelement	Wert	Erläuterung
<p>Alle Metadaten, die <b>geändert</b> wurden, sind mit altem und neuem Wert mit den Parameternamen AuditEvent.entity.detail.<b>type</b> und <b>.value[x]</b> 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 -&gt; Parameter value<b>type</b>: DocumentFormatCode und prevDocumentFormatCode.  Attributunterstrukturen werden ebenfalls in gemischter Groß/Kleinschreibung zusammengesetzt (z.B. author.Person -&gt; AuthorPerson).</p>		

5475 [**<=**]

5476 *Hinweis: In der AuditEvent.entity Struktur sind Dokumente und/oder Folder zu*  
5477 *berücksichtigen, die in der zu protokollierenden Operation referenziert werden.*

#### 5478 **A\_24925 - XDS Document Service - Protokolleinträge für Zugriffe gleicher Art**

5479 Werden mehrere XDS Dokumente bzw Folder in der zu protokollierenden Operation  
5480 referenziert und die Zugriffe sind gleicher Art (AuditEvent.action) KANN der XDS  
5481 Document Service einen Protokolleintrag erzeugen, der mehreren AuditEvent.entity  
5482 Strukturen enthält. [**<=**]

5483 Das bedeutet, wenn in einer ProvideAndRegisterDocumentSet-b Operation zehn  
5484 Dokumente eingestellt werden, kann für diesen Zugriff ein AuditEvent mit zehn Entity  
5485 Strukturen erzeugt werden. Werden zehn Dokumente eingestellt und das zehnte  
5486 Dokument ersetzt ein bereits vorhandenes, kann in einem Protokolleintrag das Einstellen  
5487 (Create) mit neun Entity Strukturen dokumentiert und muss in einem weiteren  
5488 Protokolleintrag ein Ersetzen (Update) (zehnte Dokument) protokolliert werden.

#### 5489 **A\_25007 - XDS Document Service - Nicht zu protokollierende Zugriffe**

5490 Werden mit der Operation RestrictedUpdateDocumentSet keine geänderten Metadaten  
5491 eines referenzierten DocumentEntry gesendet, d.h. die gesendeten Metadateninhalte  
5492 unterscheiden sich nicht von bereits persistierten Werten, DARF der XDS Document  
5493 Service diesen Zugriff NICHT protokollieren. [**<=**]

#### 5494 **A\_27253 - XDS Document Service - Nicht zu protokollierende Zugriffe auf** 5495 **Ordner "technical"**

5496 Der XDS Document Service DARF Zugriffe auf den statischen Ordner "technical" oder  
5497 dessen Inhalte NICHT protokollieren. Ausgenommen hiervon sind Zugriffe auf Dokumente  
5498 mit Daten der Protokollierung gemäß A\_24866-\* (Protokolle aus der Migration eines ePA-  
5499 2.6 Aktenkontos) [**<=**]

#### 5500 **A\_27254 - XDS Document Service - Protokollierung von Nutzerzugriffen auf den** 5501 **Ordner "technical"**

5502 Der XDS Document Service MUSS Nutzerzugriffe auf den Ordner "technical" dann  
5503 protokollieren, wenn durch den Zugriff Dokumente gemäß A\_24466-\*  
5504 (Protokolldokumente einer ePA-2.6 Aktenkontomigration) betroffen sind. Diese  
5505 Protokollierung MUSS gemäß der Vorgaben in A\_24715-\* erfolgen. [**<=**]

### 5506 **3.13.1.14 Unterstützungsleistung für das ePA-FdV**

5507 Der XDS Document Service akzeptiert aus Sicherheitsgründen nur bestimmte  
5508 Dokumentenformate. Das schränkt auch das Format PDF auf bestimmte PDF/A-Varianten  
5509 ein (siehe auch A\_25233\*). Daher müssen PDF-Dokumente des Versicherten unter  
5510 Umständen vor dem Einstellen in die ePA konvertiert werden.  
5511 Um das ePA-FdV dabei zu entlasten und Komplexität aus dem ePA-FdV zu nehmen, wird

5512 eine Funktion angeboten, durch die ein PDF in ein PDF/A konvertiert werden kann. Das  
5513 ePA-FdV muss aber berücksichtigen, dass die Konvertierung ggf. technisch nicht  
5514 durchgeführt werden kann oder das Ergebnis der Konvertierung durch ein geändertes  
5515 Layout ggf. nicht verwendbar ist.

5516 **A\_25456 - XDS Document Service - Keine negativen Auswirkungen auf**  
5517 **Folgekonvertierungen von PDF zu PDF/A**

5518 Der XDS Document Service MUSS sicherstellen, dass eine Konvertierung eines PDF-  
5519 Dokuments sich nicht schädlich auf folgende Konvertierungen auswirken kann. [ <= ]

5520 Hinweis zu A\_25456\*: Die Anforderung soll erreichen, dass ein potentiell über ein PDF-  
5521 Dokument eingebrachter Schadcode nach der Konvertierung gelöscht wird, z.B. durch  
5522 Zurücksetzen der Sandbox oder der VAU-Instanz

5523 **A\_25455 - XDS Document Service - Isolation der Konvertierung von PDF zu**  
5524 **PDF/A**

5525 Der XDS Document Service MUSS die Verarbeitung von PDF-Dokumenten, die im  
5526 Rahmen der Konvertierung in ein PDF/A durchgeführt wird, in einer separaten VAU-  
5527 Instanz durchführen, die ausschließlich eine Verbindung zu einem ePA-FdV besitzen  
5528 darf. [ <= ]

5529 **A\_25454 - XDS Document Service - Realisierung der Schnittstelle**  
5530 **I\_Tool\_Convert\_PDF\_Insurant**

5531 Der XDS Document Service MUSS die Operationen der Schnittstelle  
5532 I\_Tool\_Convert\_PDF\_Insurant gemäß [I\_Tool\_Convert\_PDF\_Insurant] umsetzen [ <= ]

5533 **A\_26129 - ePA-Aktensystem - Rahmenbedingungen bei Nutzung einer Service-**  
5534 **VAU für PDF-Konvertierung**

5535 Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV  
5536 für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU  
5537 verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die vom ePA-  
5538 FdV übermittelten PDF-Dokumente in der Aktenkontoverwaltungs-VAU ausschließlich  
5539 weitergeleitet aber ansonsten nicht verarbeitet werden. Gleiches gilt für die von der  
5540 Service-VAU an das ePA-FdV übermittelten konvertierten PDF/A-Dokumente. [ <= ]

5541 **A\_26130 - ePA-Aktensystem - maximale Lebensdauer einer Service-VAU für**  
5542 **PDF-Konvertierung**

5543 Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV  
5544 für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU  
5545 verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die Lebensdauer  
5546 einer solchen Service-VAU-Instanz maximal 12 Stunden beträgt. [ <= ]

5547 **A\_26131 - ePA-Aktensystem - Keine Speicherung von in der Service-VAU für**  
5548 **PDF-Konvertierung verarbeiteten Daten**

5549 Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV  
5550 für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU  
5551 verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass weder die vom  
5552 ePA-FdV übermittelten und zu konvertierenden PDF-Dokumente noch die daraus  
5553 konvertierten PDF/A-Dokumente von der "PDF-VAU" im ePA-Aktensystem gespeichert  
5554 werden. [ <= ]

5555 **A\_26121 - ePA-Aktensystem - Keine Verarbeitung von Geräteinformationen**

5556 Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV  
5557 für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU  
5558 verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass keine  
5559 Geräteinformationen (Device Management) von Nutzern verarbeitet werden. [ <= ]

### 3.13.2 FHIR Data Services

#### 3.13.2.1 Patient Information Service

##### **~~AA\_26252~~—Anbieter ePA-Aktensystem-01 - Patient Information Service -**

##### **Realisierung der Schnittstelle des FHIR IG Patient Information Service**

Der ~~Anbieter des ePA-Aktensystems~~Patient Information Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide für den Patient Information Service [IG\_Patient\_Information\_Service] umsetzen.

[<=]

##### **A\_26254 - Patient Information Service - Protokolleinträge für Zugriffe auf den Patient Information Service**

Der Patient Information Service MUSS einen Protokolleintrag gemäß A\_24704\* erzeugen und dabei folgende Wertebelegung berücksichtigen:

**Tabelle 36: Patient Information Service Protokollierung**

Strukturelement	Wert	Erläuterung
AuditEvent.type	"rest"	
AuditEvent.action	U	Update
AuditEvent.entity.name	Patient	
AuditEvent.entity.description	operation:upsertPatient	

[<=]

#### 3.13.2.2 Medication Service

##### **~~AA\_26253~~—Anbieter ePA-Aktensystem-01 - Medication Service - Realisierung der Schnittstellen des FHIR IG Medication Service**

Der ~~Anbieter des ePA-Aktensystems~~Medication Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide für den Medication Service [IG\_Medication\_Service] umsetzen. [<=]

##### **A\_26317 - Medication Service - Erzeugung eines xHTML-Exports**

Der Medication Service MUSS gemäß den Vorgaben von [IG\_Medication\_Service] für die Generierung der Medikationsliste im xHTML-Format nach [XHTML] sicherstellen, dass kein ausführbarer Code im Export enthalten ist. [<=]

##### **A\_24820 - Medication Service - Ablehnung von Request bei vorliegendem Widerspruch**

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID != oid\_erp-vau, oid\_versicherter mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("medication") die Entscheidung ("deny") gesetzt ist. [<=]

##### **A\_25152 - Medication Service - Ablehnung neuer Daten bei vorliegendem Widerspruch**

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID == oid\_erp-vau mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent

5594 Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion  
5595 ("erp-submission") die Entscheidung ("deny") gesetzt ist. [ <= ]

5596 **A\_25153 - Medication Service - Löschen der Daten des Medication Service**

5597 Der Medication Service MUSS alle vorhandenen fachlichen Daten des Medication Service  
5598 löschen, wenn im Consent Decision Management in der Funktionsklasse  
5599 ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny")  
5600 gesetzt wird. [ <= ]

5601 **A\_26399 - Medication Service - Ablehnung von Request bei vorliegendem**  
5602 **Widerspruch**

5603 Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID  
5604 gemäß A\_26406-\* mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im  
5605 Consent Decision Management die LEI der User Session in der User Specific Deny Policy  
5606 des Medication Service enthalten ist. [ <= ]

5607 **A\_24841-02 - Medication Service - Schemavalidierung**

5608 Der Medication Service MUSS die im Body der HTTP-POST-Operation übertragenen  
5609 Parameter gegen das jeweilige Schema der Operationsdefinition aus

- 5610 • [https://gematik.de/fhir/epa-medication/OperationDefinition/add-amts-allergies-](https://gematik.de/fhir/epa-medication/OperationDefinition/add-amts-allergies-OP)  
5611 [OP](https://gematik.de/fhir/epa-medication/OperationDefinition/add-amts-allergies-OP)
- 5612 • [https://gematik.de/fhir/epa-medication/OperationDefinition/add-amts-](https://gematik.de/fhir/epa-medication/OperationDefinition/add-amts-observation-OP)  
5613 [observation-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/add-amts-observation-OP)
- 5614 • [https://gematik.de/fhir/epa-medication/OperationDefinition/add-medication-](https://gematik.de/fhir/epa-medication/OperationDefinition/add-medication-information-OP)  
5615 [information-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/add-medication-information-OP)
- 5616 • [https://gematik.de/fhir/epa-medication/OperationDefinition/amts-observation-](https://gematik.de/fhir/epa-medication/OperationDefinition/amts-observation-entered-in-error-OP)  
5617 [entered-in-error-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/amts-observation-entered-in-error-OP)
- 5618 • [https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-dispensation-](https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-dispensation-OP)  
5619 [OP](https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-dispensation-OP)
- 5620 • [https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-dispensation-](https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-dispensation-erp-OP)  
5621 [erp-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-dispensation-erp-OP)
- 5622 • [https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-prescription-](https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-prescription-erp-OP)  
5623 [erp-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-prescription-erp-OP)
- 5624 • [https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-list-](https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-list-OP)  
5625 [OP](https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-list-OP)
- 5626 • [https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-plan-](https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-plan-OP)  
5627 [OP](https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-plan-OP)
- 5628 • [https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-plan-](https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-plan-history-OP)  
5629 [history-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-plan-history-OP)
- 5630 • [https://gematik.de/fhir/epa-medication/OperationDefinition/link-prescription-](https://gematik.de/fhir/epa-medication/OperationDefinition/link-prescription-process-OP)  
5631 [process-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/link-prescription-process-OP)
- 5632 • [https://gematik.de/fhir/epa-medication/OperationDefinition/manage-amts-](https://gematik.de/fhir/epa-medication/OperationDefinition/manage-amts-allergies-OP)  
5633 [allergies-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/manage-amts-allergies-OP)
- 5634 • [https://gematik.de/fhir/epa-medication/OperationDefinition/manage-](https://gematik.de/fhir/epa-medication/OperationDefinition/manage-medicationstatement-OP)  
5635 [medicationstatement-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/manage-medicationstatement-OP)
- 5636 • [https://gematik.de/fhir/epa-medication/OperationDefinition/manage-note-amts-](https://gematik.de/fhir/epa-medication/OperationDefinition/manage-note-amts-observation-OP)  
5637 [observation-OP](https://gematik.de/fhir/epa-medication/OperationDefinition/manage-note-amts-observation-OP)

- <https://gematik.de/fhir/epa-medication/OperationDefinition/manage-medication-plan-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/medication-entered-in-error-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-dispensation-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-dispensation-erp-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-medication-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-medication-plan-note-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-prescription-erp-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/remove-medication-plan-note-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/replace-medication-information-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/verify-medication-plan-OP>

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

#### **AA\_24849-0102 - Medication Service - Protokolleinträge für Zugriffe auf den Medication Service**

Der Medication Service MUSS einen Protokolleintrag gemäß A\_24704\* erzeugen und dabei folgende Wertebelegung berücksichtigen:

**Tabelle 37: Medication Service Protokollierung**

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
type		"rest"	
action	OperationId: providePrescription_MedicationSvc	"C"	Einstellen von Verschreibungsdaten



Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
	OperationId: provideDispensation_MedicationSvc	"C"	Einstellen einer Medikamentenabgabe
	OperationId: cancelPrescription_MedicationSvc	"U"	Stornieren von Verschreibungsdaten
	OperationId: cancelDispensation_MedicationSvc	"U"	Stornieren einer Medikamentenabgabe
	OperationId: addAMTSAllergyIntolerance_MedicationSvc	"C"	Einstellen von Allergie- oder Intoleranzinformationen im Rahmen von arzneimittelsicherheitsrelevanten Zusatzinformationen
	OperationId: addAMTSObservation_MedicationSvc	"C"	Einstellen von arzneimittelsicherheitsrelevanten Zusatzinformationen
	OperationId: createMedicationStatement_MedicationSvc	"C"	Einstellen von Medikamentenzusatzinformationen
	OperationId: enteredInErrorMedication_MedicationSvc	"U"	Markieren von Medikamentenzusatzinformationen als fehlerhaft
	OperationId: cancelDispensationPS_MedicationSvc	"U"	Stornieren einer Medikamentenabgabe
	OperationId: getMedicationList_MedicationSvc	"R"	Abruf der Medikationsliste

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
	OperationId: getMedicationPlan_MedicationSvc	"R"	Abruf des Medikationsplans
	OperationId: getMedicationPlanHistory_MedicationSvc	"R"	Medikationsplanshistorie
	OperationId: linkPrescriptionProcess_MedicationSvc	"U"	Verknüpfen von Verschreibungs- und Medikamentenabgabedaten
	OperationId: manageAllergyIntolerance_MedicationSvc	"U"	Aktualisieren von Allergie- und Intoleranzinformationen
	OperationId: updateMedicationStatement_MedicationSvc	"U"	Aktualisieren von Medikamentenzusatzinformationen
	OperationId: manageNoteAMTSObservation_MedicationSvc	"U"	Aktualisierung von Beobachtungsdaten im Rahmen von arzneimittelsicherheitsrelevanten Zusatzinformationen
	OperationId: manageMedicationPlan_MedicationSvc	"U"	Aktualisierung des Medikationsplans
	OperationId: enteredInErrorMedication_MedicationSvc	"U"	Kennzeichnen eines hinterlegten Medikaments als fehlerhaft eingestellt
	OperationId: provideDispensationPS_MedicationSvc	"C"	Einstellen von Medikamentenabgabe ohne Verschreibung

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
	OperationId: provideMedication_MedicationSvc	"C"	Einstellen eines Medikaments
	OperationId: provideMedicationPlanNote_MedicationSvc	"C"	Einstellen eines Medikationsplan-übergreifenden Hinweises
	OperationId: removeMedicationPlanNote_MedicationSvc	"D"	Löschen eines Medikationsplan-übergreifenden Hinweises
	OperationId: replaceMedicationInformation_MedicationSvc	"U"	Medikaments und ggf. dazugehöriger Medikamentenzusatzinformationen
	OperationId: verifyMedicationPlan_MedicationSvc	"U"	Verifizieren des aktuellen Medikationsplans
	OperationId: renderMedicationListToHTML_MedicationSvc	"R"	Abruf der Medikationsliste im HTML-Format
	OperationId: renderMedicationListToPDF_MedicationSvc	"R"	Abruf der Medikationsliste im PDF-Format
	OperationId: renderMedicationPlanToPDF_MedicationSvc	"R"	Abruf des Medikationsplans im PDF-Format
	OperationId: listAllergyIntolerances_MedicationSvc	"R"	Abruf von Allergie- und Intoleranzinformationen
	OperationId: listMedications_MedicationSvc	"R"	Abruf von Medikamenteninformationen

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
	OperationId: listMedicationDispenses_MedicationSvc	"R"	Abruf von Medikamentenabgabeformationen
	OperationId: listMedicationRequests_MedicationSvc	"R"	Abruf von Verschreibungsinformationen
	OperationId: listMedicationStatements_MedicationSvc	"R"	Abruf von Medikamentenzusatzinformationen
	OperationId: listObservations_MedicationSvc	"R"	Abruf von Beobachtungsdaten im Rahmen von arzneimittelsicherheitsrelevanten Zusatzinformationen
	OperationId: listOrganizations_MedicationSvc	"R"	Abruf von Organisationsinformationen
	OperationId: listPractitioners_MedicationSvc	"R"	Abruf von Leistungserbringerinformationen
	<u>OperationId: getMedicationList_MedicationSvc</u>	<u>"R"</u>	<u>Abruf der Medikationsliste</u>
	OperationId: listPractitionerRoles_MedicationSvc	"R"	Abruf von Leistungserbringerinformationen
	FHIR Query API:	"R"	Suche über die FHIR Query API
entity.name		<ul style="list-style-type: none"> <li>"Medical Service" bei Operationen</li> <li>&lt;FHIR Resource Name&gt; bei FHIR Query API</li> </ul>	
<b>Nur, wenn nicht FHIR Query API:</b>			

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
entity.description		OperationId der ausgeführten Operation, z. B. "provideMedication_MedicationSvc"	
entity.detail.type		"display-text"	
entity.detail.value[x]		Text der oben für die jeweilige OperationId angegebenen Erklärungsspalte, z. B. "Einstellen eines Medikaments"	
<b>Nur bei FHIR Query API:</b>			
entity.detail.type		"search-parameters"	
entity.detail.value[x]		<ResourceName>?parameter1=<value>&parameter2=<value>&...mehr	Suchkriterien in URL-Query-Notation

Sofern ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF der Medication Service keinen Protokolleintrag erzeugen.  
[<=]

### 3.14 Audit Event Service

Ereignisse und Zugriffe auf die ePA eines Versicherten werden im ePA Aktensystem protokolliert. Die Protokollierung dient der Datenschutzkontrolle für den Versicherten. Der Audit Event Service ist ein FHIR Data Service und ermöglicht dem Versicherten, befugten Vertretern bzw. der Ombudsstelle den Zugriff auf diese Protokollinformationen.

#### **A\_24704 - Audit Event Service - FHIR-Ressource AuditEvent**

Der Audit Event Service MUSS die FHIR-Ressource AuditEvent gemäß der FHIR-Profilierung [[gemSpec\\_ePAAuditEvent-IG Audit Event Service](#)] unterstützen.[<=]

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

5681 **Tabelle 38 : Inhaltliche Definitionen eines AuditEvent**

Information	Strukturelement
Wann ist der Zugriff erfolgt bzw. hat das Ereignis stattgefunden?	AuditEvent.recorded
Wer war der Akteur/Auslöser?	AuditEvent.agent
Welcher Art Service wurde angefragt?	AuditEvent.type
Worauf wurde zugegriffen?	AuditEvent.source
Welcher Art war der Zugriff?	AuditEvent.action
War der Zugriff erfolgreich?	AuditEvent.outcome
Informationen zu Daten/Dokumente/Objekte	AuditEvent.entity

5682

5683 Die spezifische Befüllung eines Audit Events gemäß A\_24704\* wird durch die jeweiligen  
5684 Services vorgegeben. Allgemeine Elemente sind wie folgt zu befüllen:

5685

5686 **AA\_25154-0203 - ePA-Aktensystem - Befüllung der Elemente recorded,**  
5687 **agent und source eines Audit Events**

5688 Das ePA-Aktensystem MUSS die Audit Event Elemente AuditEvent.recorded,  
5689 AuditEvent.agent und AuditEvent.source wie folgt befüllen.

5690

5691

**Tabelle 39 Befüllung AuditEvent**

Element [AuditEvent.]		Beschreibung	Beispiel
recorded		Systemzeit bei Erstellung des AuditEvents im Format YYYY-MM-DDThh:mm:ssZ	"2025-01-15T14:52:04.928Z"
purposeOfEvent		<del>Zweck(e) des protokollierten Ereignisses gemäß des zulässigen Value-Sets aus [gemSpec_EPAAuditEvent]. Nur zu belegen, wenn explizit bei entsprechender Protokollierungsanforderung gefordert.</del>	
	system	<del>Das verwendete Codesystem</del>	<del>"<a href="https://gematik.de/fhir/epa/ValueSet/epa-auditevent-purpose-of-event-vs">https://gematik.de/fhir/epa/ValueSet/epa-auditevent-purpose-of-event-vs</a>"</del>
	code	<del>Der verwendete Code aus dem Codesystem</del>	<del>"EXPORTFDZ"</del>
	display	<del>Der Bezeichner zur Anzeige aus dem Codesystem</del>	<del>"Export für das Forschungsdatenzentrum Gesundheit"</del>
agent[client].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets <del>aus [gemSpec_EPAAuditEvent].</del>	



Element [AuditEvent.]		Beschreibung	Beispiel
	system	Das verwendete Codesystem; Fest vorgegebener Wert: "http://dicom.nema.org/resources/ontology/DCM"	"http://dicom.nema.org/resources/ontology/DCM"
	code	Der verwendete Code aus dem Codesystem; Fest vorgegebener Wert: "110150"	"110150"
	display	Der Bezeichner zur Anzeige aus dem Codesystem; Fest vorgegebener Wert: "Application"	"Application"
agent[client].who.identifizier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets <del>aus [gemSpec_EPAAuditEvent]</del>	
	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"> <li>&lt;display_name&gt; des auslösenden Akteurs aus dem ID-Token der UserSession</li> <li>"Elektronische Patientenakte Fachdienst" für intern ausgelöste AuditEvents</li> </ul>	1) "E-Rezept-Fachdienst" 2) "Elektronische Patientenakte Fachdienst" 3) "Portugal" (Beispiel EU-Zugriff)

Element [AuditEvent.]		Beschreibung	Beispiel
agent[client].	requestor	Fest vorgegebener Wert "false"	"false"
agent[user].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets <del>aus [gemSpec_EPAAuditEvent].</del>	
	system	Das verwendete Codesystem	" <a href="http://terminology.hl7.org/CodeSystem/v3-RoleClass">http://terminology.hl7.org/CodeSystem/v3-RoleClass</a> "
	code	Der verwendete Code aus dem Codesystem	"PROV"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"healthcare provider"
agent[user].who.identifier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets <del>aus [gemSpec_EPAAuditEvent]</del>	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/sid/telematik-id"
	value	<Telematik-Id> oder <KVNR>	1) "2-121212121212121" 2) "Z123456789"
agent[user].	altId	<value> aus agent.who.identifier	1) "2-121212121212121" 2) "Z123456789"
agent[user].role.coding		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthProfessionalRole.	

Element [AuditEvent.]		Beschreibung	Beispiel
	system	Das verwendete Codesystem	"urn:oid:1.3.6.1.4.1.12559.11.10.1.3.2.2.2"
	code	Der verwendete Code aus dem Codesystem	"Resident Physician"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Resident Physician"
agent[user].extension		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthcareFacilityType; extension mit url="https://gematik.de/fhir/dev-epa/StructureDefinition/epa-healthcare-facility-type-extension">	
	system	Das verwendete Codesystem	"urn:oid:2.16.840.1.113883.2.9.6.2.7"
	code	Der verwendete Code aus dem Codesystem	"221"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Medical Doctors"
agent[user].	name	Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: <leiName> / <healthProfessionalName> Andernfalls: <display_name> des auslösenden Akteurs aus dem ID-Token der UserSession	EU-Zugriff: "Dr. Manuel Dos Santos / Clínica de Dos Santos" Andernfalls: "John Doe"
agent[user].	requestor	Fest vorgegebener Wert "false"	false

Element [AuditEvent.]		Beschreibung	Beispiel
agent[internal].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets <del>aus</del> <del>[gemSpec_EPAAuditEvent].</del>	
	system	Das verwendete Codesystem	"http://dicom.nema.org/resources/ontology/DCM"
	code	Der verwendete Code aus dem Codesystem	"110150"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Application"
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 <del>aus</del> <del>[gemSpec_EPAAuditEvent].</del>	
	system	Das verwendete Codesystem	" <a href="https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs">https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs</a> "

Element [AuditEvent.]		Beschreibung	Beispiel
	code	Der verwendete Code aus dem Codesystem	"CDMGMT"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Consent Decision Management"

Hinweis:

agent[client]: Angaben zur Applikation, z. B. eRezept-Fachdienst, NCPeH

agent [user]: Angaben zu LEI oder Vertreter oder Versicherter

agent[internal]: Angaben zu systemeigenen Prozessen, z. B. Datenexport für das FDZ

[<=]

5699

5700

#### 5701 **A\_24503 - ePA-Aktensystem - Aufbewahrungsdauer der Protokolleinträge**

5702 Das ePA-Aktensystem MUSS die zum Zwecke der Datenschutzkontrolle für den  
5703 Versicherten erstellten

5704 Protokolleinträge für drei Jahre aufbewahren. Danach sind sie vom Aktensystem  
5705 automatisch zu löschen. [ $\leq$ ]

5706 Die Protokolleinträge können durch den Versicherten oder durch einen befugten Vertreter  
5707 mittels ePA-FdV eingesehen werden. Versicherte ohne ePA-FdV können bei ihrer  
5708 zuständigen Ombudsstelle beantragen, die Protokolldaten zur Verfügung gestellt zu  
5709 bekommen.

5710 Für eine Abfrage der Protokolleinträge als strukturierte Einträge nutzen ein ePA-FdV und  
5711 die Ombudsstelle den Audit Event Service [IG\_Audit\_Event\_Service].

#### 5712 **A\_24714-01 - Audit Event Service - Realisierung der Query API: AuditEvent**

5713 Der Audit Event Service MUSS die "Query API: AuditEvent" des FHIR Implementation  
5714 Guide für den Audit Event Service [IG\_Audit\_Event\_Service] umsetzen. [ $\leq$ ]

#### 5715 **A\_24750-02 - Audit Event Service - Realisierung der Render API: PDF Audit**

5716 Der Audit Event Service MUSS die "Render API: PDF Audit" des FHIR Implementation  
5717 Guide für den Audit Event Service [IG\_Audit\_Event\_Service] umsetzen. [ $\leq$ ]

#### 5718 **A\_25172 - Audit Event Service - Speicherung der Protokolldaten**

5719 Der Audit Event Service MUSS die Daten der Protokolleinträge ~~im~~-verschlüsselt im  
5720 SecureDataStorage persistieren. [ $\leq$ ]

5721 Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A\_25172\* entfällt, wenn ein  
5722 Protokolleintrag mangels eines befugten Nutzers (kein Bezug des  
5723 SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann.

#### 5724 **A\_25018 - Audit Event Service - PAdES-Signatur in renderAuditEventsToPDF**

5725 Der Audit Event Service MUSS bei der Operation `renderAuditEventsToPDF` beim  
5726 Signieren eines Protokolls im PDF/A-Format eine PAdES-Signatur gemäß [PAdES-3] und  
5727 [PAdES Baseline Profile] erstellen. Bei der Signaturerstellung ist das Attribut `signing`  
5728 `certificate reference` gemäß den Vorgaben aus [PAdES-3] Kapitel 4.4.3 „Signing  
5729 Certificate Reference Attribute“ anzulegen. [ $\leq$ ]

5730 Durch die Baseline-Profilierung [PAdES Baseline Profile] wird festgelegt, wie der  
5731 Signaturzeitpunkt, gemessen als Systemzeit des ePA-Aktensystems, in die Signatur  
5732 eingebracht wird.

#### 5733 **A\_24991 - Audit Event Service – Protokollierung von Zugriffen auf die** 5734 **Protokolldaten**

5735 Der Audit Event Service MUSS für die Zugriffe der Ombudsstelle oder eines Vertreters auf  
5736 die protokollierten Daten jeweils einen Protokolleintrag gemäß A\_24704\* erzeugen.

#### 5737 **Tabelle 40: Audit Event Service Protokollierung**

Strukturelement	Wert	Erläuterung
AuditEvent.type	"rest"	
AuditEvent.action	R	Read

Strukturelement	Wert		Erläuterung
AuditEvent.entity.name	"AuditEvent"		
AuditEvent.entity.description	Passend zur ausgeführten Operation ein Wert aus folgender Liste: <ul style="list-style-type: none"> <li>• listAuditEvents</li> <li>• getAuditEventById</li> <li>• renderAuditEventsToPDF</li> </ul>		
AuditEvent.entity.detail	<b>type</b>	<b>value[x]</b>	
	parameters	parameter1=<value>¶parameter2=<value>& ...mehr	Nur bei getAuditEventList
	identifizier	<id> des AuditEvents	Nur bei getAuditEvent

5738 [**<=**]

5739 *Hinweis: Zugriffe des Versicherten auf die Protokolle des Aktenkontos werden nicht*  
 5740 *protokolliert.*

5741

## 5742 3.15 Information Service

### 5743 3.15.1 Information Service

5744 Der Information Service ist ohne die Nutzung eines VAU-Kanals nutzbar. Die über den  
 5745 Information Service genutzten Daten sind ausschließlich persistierte Daten des  
 5746 Aktenkontos, die weder mit dem SecureAdminStorageKey noch mit dem  
 5747 SecureDataStorageKey gesichert sind.

5748 Der Zugang erfolgt durch Nutzung der Schnittstelle `I_Information_Service`.

#### 5749 **A\_24344 - Information Service - Realisierung der Schnittstelle**

##### 5750 **`I_Information_Service`**

5751 Der Information Service MUSS die Operationen der Schnittstelle `I_Information_Service`  
 5752 gemäß [`I_Information_Service`] umsetzen. [**<=**]

#### 5753 **A\_24345 - Information Service - Kein Zugriff auf verschlüsselte Daten des** 5754 **Aktenkontos**

5755 Der Information Service DARF NICHT auf Daten zugreifen, die nicht explizit für die  
 5756 Verwendung durch den Informationsdienst bereitgestellt wurden. Dazu gehören  
 5757 insbesondere alle Daten des Aktenkontos, die mit den versichertenindividuellen



5758 Schlüsseln zur Daten- oder Befugnispersistierung (SecureDataStorageKey oder  
5759 SecureAdminStorageKey) gesichert sind.[<=]

### 5760 **3.15.1.1 Informationen zu Widersprüchen (Consent Decisions)**

5761 Die Widersprüche eines Versicherten gegen die Nutzung von Funktionen der  
5762 elektronischen Patientenakte werden durch das Consent Decision Management gesichert  
5763 administriert. Änderungen an den Widersprüchen erfolgen dort.

5764 Der Information Service bietet für die Nutzergruppen der ePA eine einfache  
5765 Abfragemöglichkeit der aktuell erteilten oder nicht erteilten Widersprüche auch ohne die  
5766 Nutzung des Consent Decision Managements an. Liegt ein Widerspruch gegen die  
5767 Nutzung einer Funktion vor, kann auf die Ausführung der zur Nutzung dieser Funktion  
5768 notwendigen Aktionen mit der ePA eines Versicherten durch den Client verzichtet  
5769 werden.

5770 Für diese vereinfachte Abfragemöglichkeit der aktuellen Widersprüche verwendet der  
5771 Information Service den durch das Consent Decision Management persistent  
5772 übertragenen Zustand der Widersprüche ("Cache" des Zustands der Widersprüche).  
5773 Berücksichtigt wird dabei die Widerspruchsinformation, für die eine vereinfachte Abfrage  
5774 vorgesehen ist (Widersprüche der Klasse "Versorgungsprozess").

### 5775 **3.15.1.2 Informationen zur Anwenderperformance (UX Performance)**

5776 Der Information Service stellt für die Umgebung der Leistungserbringer die Operation zur  
5777 Sammlung der Messwerte zu den Anwendungsfällen der Nutzererfahrung zur Verfügung.  
5778 Die Weiterverarbeitung der gesammelten Daten ist in 22.9- Performance aus  
5779 Anwendersicht definiert und vorgegeben.

## 5780 **3.15.2 Information Service - Account**

5781 Die Operationen der Information Service - Account werden für den Umzug eines  
5782 existierenden Aktenkontos zu einem neuen Anbieter verwendet. Die Nutzung der  
5783 Operationen erfolgt exklusiv durch die Aktensystembetreiber.

5784 Die Verwendung der einzelnen Operationen erfolgt im Verbund mit den Operationen der  
5785 Schnittstelle I\_Health\_Record\_Relocation\_Service für die Umsetzung der  
5786 Anwendungsfälle eines automatischen Aktenkontoumzugs und sind in 33.2- Health  
5787 Record Relocation Service erläutert.

### 5788 **A\_24424 - Information Service Account - Realisierung der Schnittstelle** 5789 **I\_Information\_Service\_Accounts**

5790 Der Information Service MUSS die Operationen der Schnittstelle  
5791 I\_Information\_Service\_Accounts gemäß [I\_Information\_Service\_Accounts]  
5792 umsetzen.[<=]

### 5793 **A\_24665 - Information Service Account - Nutzung beidseitig authentisiertes TLS**

5794 Der Information Service MUSS sicherstellen, dass die Operationen der Schnittstelle  
5795 I\_Information\_Service\_Accounts ausschließlich unter Verwendung einer beidseitig  
5796 authentisierten TLS-Verbindung zwischen den beteiligten Aktensystemen genutzt werden  
5797 und die Operationen ansonsten abgebrochen und mit einer Fehlermeldung gemäß  
5798 Vorgaben in [I\_Information\_Service\_Accounts] beantwortet werden.[<=]

### 5799 **A\_25054 - Information Service Account - Gegenseitige Authentisierung** 5800 **Aktensysteme**

5801 Die Information Service Account Dienste der Aktensysteme MÜSSEN sich mit der TLS-  
5802 Identität mit professionOID oid\_epa\_mgmt mittels des Zertifikats C.FD-TLS-S gegenseitig

5803 authentisieren.  
5804 [ $\leq$ ]

5805 **A\_25053 - Information Service Account - Prüfung der TLS-Zertifikate**

5806 Der Information Service Account MUSS bei der Authentifizierung eines jeweils anderen  
5807 Aktensystems die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC\_PKI\_018  
5808 durchführen. Zur Prüfung des TLS-Zertifikats C.FD-TLS-S sind dabei die  
5809 Parameter PolicyList=oid\_fd\_tls\_s, IntendedKeyUsage=digitalSignature,  
5810 intendedExtendedKeyUsage=id-kp-serverAuth, OCSP-Graceperiod=60 Minuten, Offline-  
5811 Modus=nein zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD-TLS-C sind dabei die  
5812 Parameter PolicyList=oid\_fd\_tls\_c, IntendedKeyUsage=digitalSignature,  
5813 intendedExtendedKeyUsage=id-kp-clientAuth, OCSP-Graceperiod=60 Minuten, Offline-  
5814 Modus=nein zu verwenden.  
5815 [ $\leq$ ]

5816 **3.16 Email Management**

5817 Das Email Management ermöglicht einem FdV-Nutzer die Verwaltung seiner E-Mail-  
5818 Adresse und einem Kostenträger die Verwaltung von E-Mail-Adressen von Versicherten,  
5819 die bei diesem Kostenträger versichert sind.

5820 Die Schnittstelle zum Verwalten der E-Mail-Adressen durch den Kostenträger dient dem  
5821 ausschließlichen Zweck des Einstellens, Lesens und der Änderung von E-Mail-Adressen  
5822 auf Verlangen des Versicherten. Dies ermöglicht dem Kostenträger, seinen Versicherten  
5823 die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte auf Berichtigung und  
5824 Auskunft bzgl. der im Aktensystem verarbeiteten E-Mail-Adresse zu gewährleisten.

5825 Für einen Versicherten kann nur genau eine E-Mail Adresse hinterlegt werden.

5826 **A\_25435 - Email Management - Realisierung der Schnittstelle**

5827 **I\_Email\_Management**

5828 Das Email Management MUSS die Operationen der Schnittstelle  
5829 I\_Email\_Management gemäß [I\_Email\_Management] umsetzen. [ $\leq$ ]

5830 **A\_25438 - Email Management - Beschränkung der Schnittstellenoperationen auf**  
5831 **E-Mail-Adressen des FdV-Nutzers**

5832 Das Email Management MUSS die Operationen der Schnittstelle  
5833 I\_Email\_Management gemäß [I\_Email\_Management] auf die E-Mail-Adresse des  
5834 aufrufenden Nutzers einschränken, sofern der Nutzer ein FdV-Nutzer ist. [ $\leq$ ]

5835 **A\_26161 - Email Management - Nutzen von Email Management auch bei**  
5836 **Widerpruch**

5837 Das Email Management MUSS sicherstellen, dass das Email Management auch von  
5838 Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben. [ $\leq$ ]

5839 **A\_26162 - Email Management - Versicherte nutzen Email Management**  
5840 **ausschließlich im Home-AS**

5841 Das Email Management des ePA-Aktensystems MUSS sicherstellen, dass das Email  
5842 Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-  
5843 Aktensystem das Home-AS ist. [ $\leq$ ]

5844 Hinweis: Für das Email Management ist auch Anforderung A\_26154 umzusetzen.

5845 **A\_25439 - Email Management - Kostenträger kann ausschließlich E-Mail-**  
5846 **Adressen der eigenen Versicherten verwalten**

5847 Das Email Management MUSS sicherstellen, dass ein Kostenträger mittels der  
5848 Operationen der Schnittstelle I\_Email\_Management gemäß [I\_Email\_Management]

5849 ausschließlich E-Mail-Adressen von Versicherten verwalten kann, die beim Kostenträger  
5850 versichert sind. [ <= ]

5851 **A\_25440-01 - Email Management - Benachrichtigung bei Änderung der E-Mail-**  
5852 **Adresse**

5853 Falls eine E-Mail-Adresse a) ersetzt oder b) ergänzt wird, MUSS das Device Management  
5854 bei a) eine E-Mail an die alte und die neue E-Mail-Adresse senden und bei b) eine E-Mail  
5855 an die neue E-Mail-Adresse senden, in der bei a) über die Ersetzung bzw. bei b) die  
5856 Ergänzung einer E-Mail-Adresse informiert wird. In der E-Mail MUSS darüber informiert  
5857 werden, wann und ob der FdV-Nutzer selbst oder der Kostenträger die E-Mail ersetzt  
5858 bzw. ergänzt hat. [ <= ]

5859 **A\_25441 - Email Management - Information bzgl. der Ergänzung bei E-Mail-**  
5860 **Adressen**

5861 Das Email Management MUSS sicherstellen, dass der FdV-Nutzer für eine im Email  
5862 Management hinterlegte E-Mail-Adresse erkennen kann, wann und von wem diese E-  
5863 Mail-Adresse ergänzt wurde. [ <= ]

5864 **A\_25968-01 - Email Management - Maximale Anzahl E-Mail-Adressen**

5865 Das Email Management MUSS sicherstellen, dass für einen Nutzer maximal eine E-Mail-  
5866 Adresse hinterlegt werden kann. [ <= ]

5867

5868 **A\_26163 - Email Management - Keine Persistierung einer im Rahmen der**  
5869 **Vertretereinrichtung übergebenen E-Mail-Adresse**

5870 Das Email Management MUSS sicherstellen, dass eine im Rahmen des Anwendungsfalls  
5871 der Vertretereinrichtung vom Nutzer übermittelte E-Mail-Adresse nicht persistiert und  
5872 spätestens bei Beendigung der User Session gelöscht wird. [ <= ]

5873 **A\_26164 - Email Management - Keine Geräteregistrierung mit der im Rahmen**  
5874 **der Vertretereinrichtung übergebenen E-Mail-Adresse**

5875 Das Email Management MUSS sicherstellen, dass keine E-Mail-Adressen zur Übermittlung  
5876 eines Geräteregistrierungscodes genutzt werden, die dem ePA-Aktensystem im Rahmen  
5877 des Anwendungsfalls der Vertretereinrichtung übermittelt wurden. [ <= ]

5878 Hinweis zu A\_26163 und A\_26164: Die im Rahmen des Anwendungsfalls der  
5879 Vertretereinrichtung übermittelte E-Mail-Adresse wird ausschließlich zur Information des  
5880 Vertreters über die Einrichtung der Vertretung genutzt (vgl. A\_24755-\*).

5881 **3.17 Zusätzliche Anforderungen an den Authorization Service**

5882 Der ePA Authorization Service wird sowohl für die Authentisierung der Versicherten über  
5883 das FdV als auch für die Authentisierung von Leistungserbringern und Kostenträgern über  
5884 deren Primärsystem benötigt. Ebenso muss die Zugriffsautorisierung für andere  
5885 Fachdienste wie z.B. E-Rezept geprüft werden. Die Festlegungen für den Authorization  
5886 Server finden sich in [gemSpec\_IDP\_FD]. Dieser Abschnitt des vorliegenden Dokuments  
5887 enthält spezifische Anforderungen, die vom Authorization Service des Aktensystems  
5888 zusätzlich umzusetzen sind.

5889 **A\_24923 - Authorization Service - I\_Authorization\_Service**

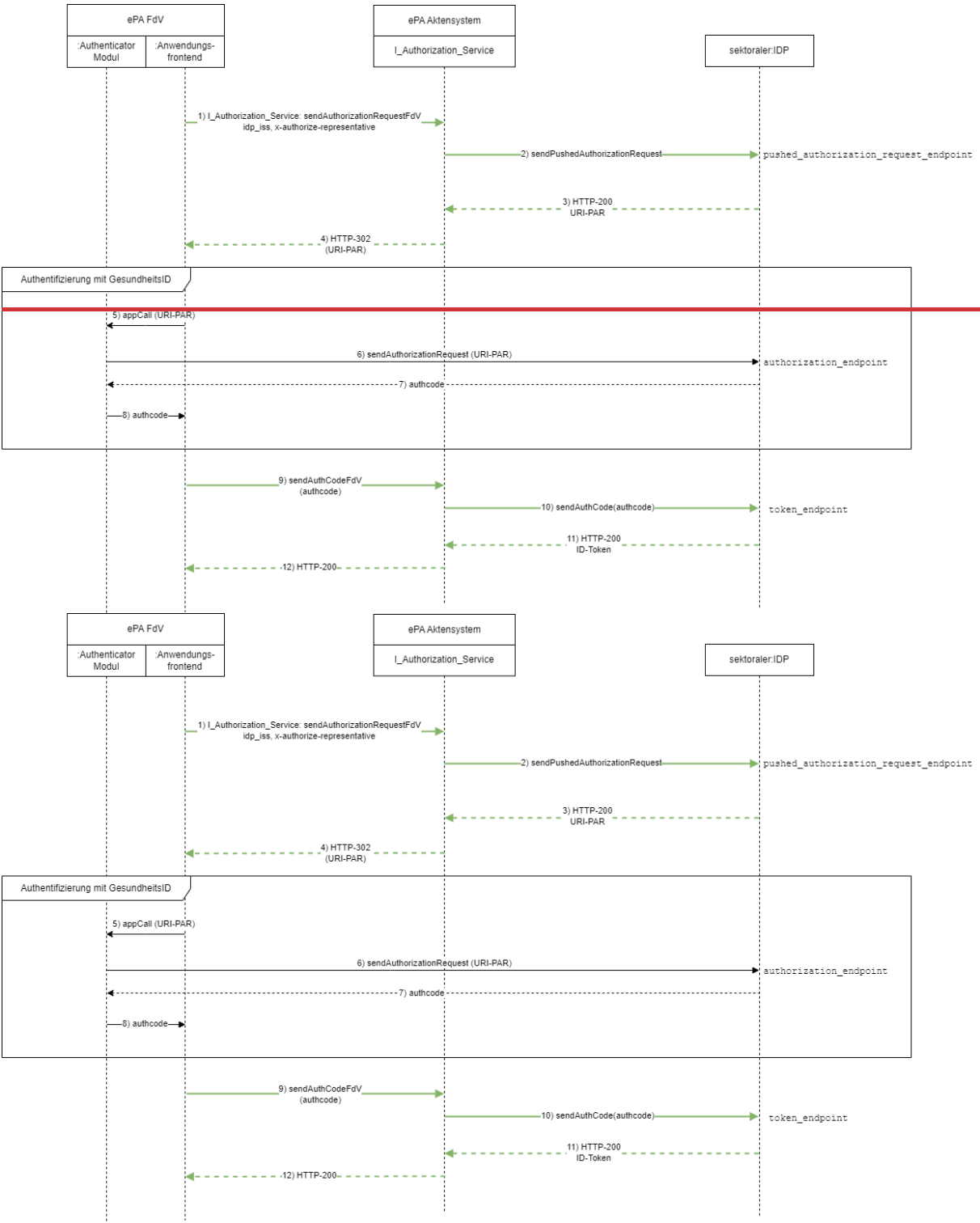
5890 Der Authorization Service MUSS die Operationen der  
5891 Schnittstelle I\_Authorization\_Service implementieren gemäß  
5892 [I\_Authorization\_Service]. [ <= ]

5893 **A\_25283 - Authorization Service - Konvertieren von ID-Token**

5894 Der Authorization Service MUSS sicherstellen, dass für ein nach erfolgreicher  
 5895 Authentifizierung des Nutzers vorliegendes ID-Token mittels Regel *rr0* gemäß  
 5896 *Tab\_AS\_Entitlement\_Registration\_Rules* ein HSM-ID-Token erstellt wird, bevor das ID-  
 5897 Token zeitlich ungültig ist. [ $\leq$ ]

### 5898 **3.17.1 Anforderungen an den Authorization Service für die** 5899 **Authentisierung von Versicherten (FdV)**

5900 Im Rahmen der Authentisierung des Versicherten erfolgt die Prüfung der  
 5901 Geräteregistrierung (Verifikation) direkt. Das Gerät muss dafür die Geräteparameter  
 5902 eines zuvor ausgeführten und bestätigten Registrierungsprozesses verwenden  
 5903 Bisher nicht registrierte Geräte, bzw. Geräteparameter einer bisher nicht bestätigten  
 5904 Geräteregistrierung, können unter Verwendung des Device Management registriert, bzw.  
 5905 bestätigt werden (siehe Kapitel [33.12- Device Management](#)).  
 5906



**Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP**  
**AA\_25717-01-03 - Authorization Service - Pushed Authorization-Request des IDP-Dienstes**  
**Authorization Service an sektorale Identity Provider**

Der ePA Authorization Service MUSS den Pushed Authorization Request (PAR) am durch den vom ePA-FdV übergebenen Parameter idp-iss adressierten sektoralen IDP gemäß [gemSpec\_IDP\_FD#AF\_10117] mit folgenden Parametern aufrufen:

Parameter	Wert	Anmerkung
scope	"openid urn:telematik:display_name urn:telematik:versicherter <u>urn:telematik:family_name</u> <u>urn:telematik:given_name</u> "	Notwendige Scopes für den Zugriff für die Autorisierung von Nutzern am ePA-Aktensystem
acr_values	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung
redirect_uri	<del>&lt;Location Authorization Service&gt;/epa/authz/&lt;version&gt;/send_authcode_fdv</del> <u>Inhalt des Parameters x-redirecturi [sendAuthorizationRequestFdV in I Authorization Service], andernfalls eine herstellerspezifische Standard-redirect uri.</u>	Diese URI muss unter dem claim redirect_uris im Entity Statement des Authorization Service enthalten sein. <u>Mandanten, welche eine eigene redirect uri verwenden [sendAuthorizationRequestFdV in I Authorization Service], müssen diese im Rahmen des Registrierungsprozesses beim Authorization Service bekannt geben.</u>

5915 **[<=]**

5916 Hinweis 1: An die redirect\_uri im Pushed Authorization Request sendet der sektorale IDP  
5917 den ausgestellten Authorization Code (siehe [gemSpec\_IDP\_Sek])

5918 Hinweis 2: Der Redirectaufruf, der vom Authenticator Modul an die redirect\_uri  
5919 ausgeführt wird, wird vom ePA-FdV über Plattformmechanismen (deeplink/universallink)  
5920 gefangen und stellt selbst einen POST-Request an den Endpunkt des Authorization  
5921 Service.

#### 5922 **A 26584 - Authorization Service - Liste der redirect uris im Entity Statement**

5923 Der Authorization Service MUSS in seinem Entity Statement im claim  
5924 redirect\_uris die redirect\_uris aller Mandanten auflisten, welche bei der  
5925 Registrierung an einem beliebigen ePA Authorization Service eine eigene redirect uri  
5926 angegeben haben. Über Änderungen des claim redirect\_uris MUSS der Anbieter des  
5927 Federation Master vor produktiver Verwendung informiert werden[<=]

5928 Hinweis: Im Registrierungsprozess eines Mandanten mit eigener redirect uri muss  
5929 sichergestellt sein,

- 5930 • dass alle Anbieter von ePA Authorization Servern (ePA Aktensystem Anbieter)  
5931 entsprechend informiert sind und das Entity Statement anpassen
- 5932 • dem Hersteller des Federation Master über ein ITSM Change bekannt gemacht  
5933 wird, dass sich die Entity Statements aller ePA Authorization Server ändern

#### **A\_27145 - Synchronisation "redirect URI" mit Marktteilnehmer - E-Mail-Adresse**

Der Anbieter ePA-Aktensystem MUSS der gematik eine E-Mail-Adresse mitteilen, über welche er die eigenverantwortliche Registrierung (von redirect-URIs im Entity-Statement) durchführt und über die der Anbieter bei Änderungen erreichbar ist.

Hinweis: Diese E-Mail-Adressen werden durch das Provider Management der gematik anschließend unter den relevanten Anbietern verteilt bzw. können dort erfragt werden. Die Änderung der E-Mail-Adressen ist ebenfalls zu kommunizieren.

Hintergrund: Für Stellvertretung via ePA-FdV ist eine Synchronisierung der redirect URIs notwendig. [ <= ]

#### **A\_27186 - Synchronisation "redirect URI" mit Marktteilnehmer - Information**

Der Anbieter ePA-Aktensystem MUSS bei Änderungen der redirect URIs im eigenen Entity Statement allen anderen Marktteilnehmern des gleichen Fachdiensttyps diese Änderung innerhalb 24 Stunden mitteilen. [ <= ]

#### **A\_27187 - Synchronisation "redirect URI" mit Marktteilnehmer - Aktualisierung**

Der Anbieter ePA-Aktensystem MUSS nach dem Empfang der Mitteilungen über Änderungen der Redirect URIs in einem externen Entity Statement diese Änderung binnen 24 Stunden in den Redirect URIs des eigenen Entity Statement synchronisieren.

Hinweis: Diese Änderung erfordert anschließend keine Information nach A\_27186. [ <= ]

#### **A\_24878-01 - Authorization Service - Authentifizierung eines Versicherten am ePA-FdV des Vertreters**

Falls der Eingangsparameter x-authorize-representative=True der Operation I\_Authorization\_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der Authorization Service im PAR als Parameter amr mit den Werten urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [ <= ]

#### **A\_26189-01 - Authorization Service - Authentifizierung eines Versicherten im Gastmodus mit eGK und PIN**

Falls der Eingangsparameter x-authorize-egk=True der Operation I\_Authorization\_Service::sendAuthorizationRequestFdV gesetzt ist, MUSS der Authorization Service im PAR als Parameter amr mit den Werten urn:telematik:auth:guest:eGK belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [ <= ]

#### **A\_24937-01 - Authorization Service - Einschränkung bei Authentifizierung eines Versicherten am ePA-FdV des Vertreters**

Der Authorization Service MUSS sicherstellen, dass ein mit x-authorize-representative=True authentisierter Nutzer ausschließlich Zugriff auf das Entitlement Management erhält. [ <= ]

#### **A\_26159 - Authorization Service - Prüfen der Device Attestation**

Der Authorization Service MUSS sicherstellen, dass von einem anderen ePA-Aktensystem signierte Device Attestations ausschließlich akzeptiert werden, wenn

- die Device Attestation gemäß A\_25042-\* valide von einer Signaturidentität der VAU eines anderen ePA-Aktensystems signiert wurde,



5982 • die KVN-R in der Device Attestation mit der KVN-R im ID-Token des angemeldeten  
5983 Nutzers übereinstimmt,

5984 • die Device Attestation zeitlich gültig ist.

5985 [ $\leq$ ]

5986 **A\_26160 - Authorization Service - Keine Persistierung der Device Attestation**

5987 Der Authorization Service MUSS sicherstellen, dass die von einem anderen ePA-  
5988 Aktensystem signierte Device Attestation und deren Inhalte spätestens bei Beendigung  
5989 der User Session gelöscht und nicht persistiert werden. [ $\leq$ ]

5990 **A\_25310-01 - Authorization Service - Einschränkung bei Authentifizierung mit**  
5991 **einem unregistrierten Gerät**

5992 Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wird und der Nutzer  
5993 nicht mit x-authorize-representative=True authentisiert wurde, MUSS der  
5994 Authorization Service sicherstellen, dass der Nutzer ausschließlich Zugriff auf das Device  
5995 Management erhält. [ $\leq$ ]

5996 Hinweis:

5997 Ein vollständiger Zugriff eines authentisierten Nutzers auf alle Dienste des Aktensystems  
5998 kann nur mit einem Gerät erfolgen, dessen Geräteregistrierung bei der Authentifizierung  
5999 des Nutzers erfolgreich verifiziert wurde.

6000 Ein Nachweis einer Geräteregistrierung ist entweder DeviceID (deviceIdentifizier und  
6001 deviceToken), die für den Nutzer im Aktensystem bekannt sind oder die vom Client  
6002 übergebene Device Attestation (deviceAttestation), die zuvor am Device Management des  
6003 Home Aktensystems durch den Client abgerufen wurde.

6004 **A\_24804-01 - Authorization Service - Prüfung auf registriertes Gerät**

6005 Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des  
6006 Vertreters handelt und im Operationsaufruf  
6007 `I_Authorization_Service::sendAuthCodeFdV` eine DeviceID (deviceIdentifizier und  
6008 deviceToken) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung  
6009 eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer  
6010 registriert und bestätigt ist und übereinstimmt. [ $\leq$ ]

6011 **A\_24914-03 - Authorization Service - Prüfung auf registriertes Gerät - kein**  
6012 **registriertes Gerät**

6013 Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wurde, MUSS  
6014 der Authorization Service die Operation `sendAuthCodeFdV` mit einer Fehlermeldung  
6015 abbrechen und die User Session beenden. [ $\leq$ ]

6016

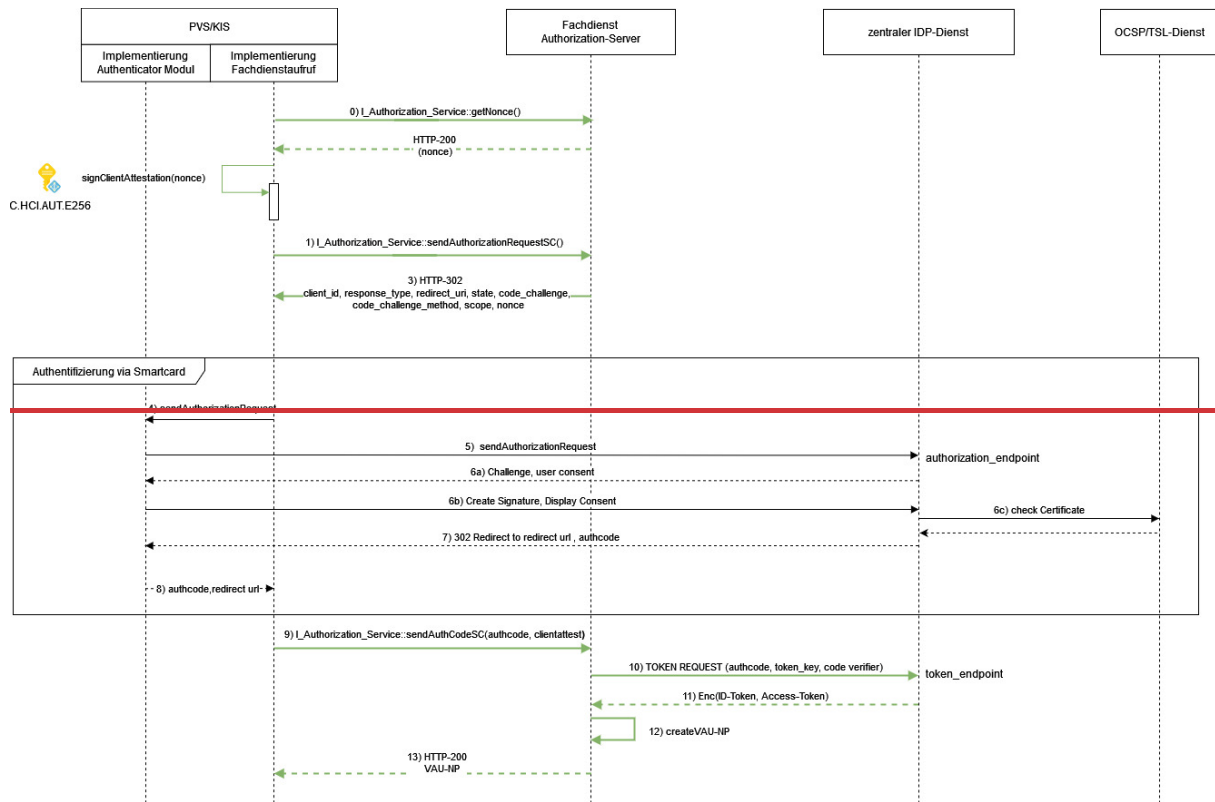
6017 **A\_24915-01 - Authorization Service - Prüfung auf registriertes Gerät -**  
6018 **registriertes Gerät nicht bestätigt**

6019 Falls als Nachweis einer Geräteregistrierung eine DeviceID (deviceIdentifizier und  
6020 deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status ==  
6021 'pending'), MUSS der Authorization Service die Operation `sendAuthCodeFdV` mit einer  
6022 Fehlermeldung abbrechen und die User Session beenden. [ $\leq$ ]

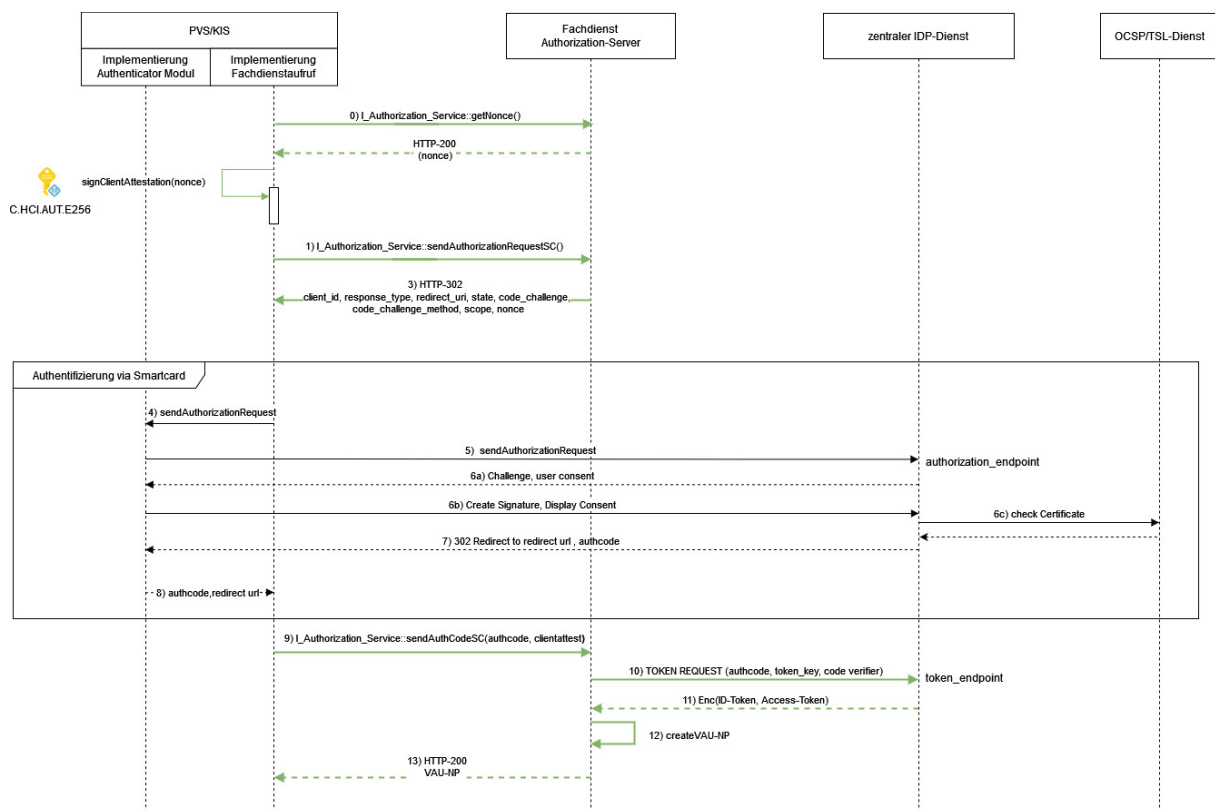
6023

6024  
6025

### 3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B



6026



6027

**Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP**

**A\_24717 - Authorization Service: IDToken vom IDP-Dienst nur mit Client-Attestation nutzbar**

Der Authorization Service MUSS sicherstellen, dass ein vom IDP-Dienst abgerufenes ID-Token für Nutzer "TelematikID\_X" nur dann akzeptiert wird, falls im Authorization Service auch eine Client-Attestation vom Nutzer "TelematikID\_X" vorliegt. [ $\leq$ ]

**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. [ $\leq$ ]

**A\_25444-01 - Authorization Service - JWT Client Attestation**

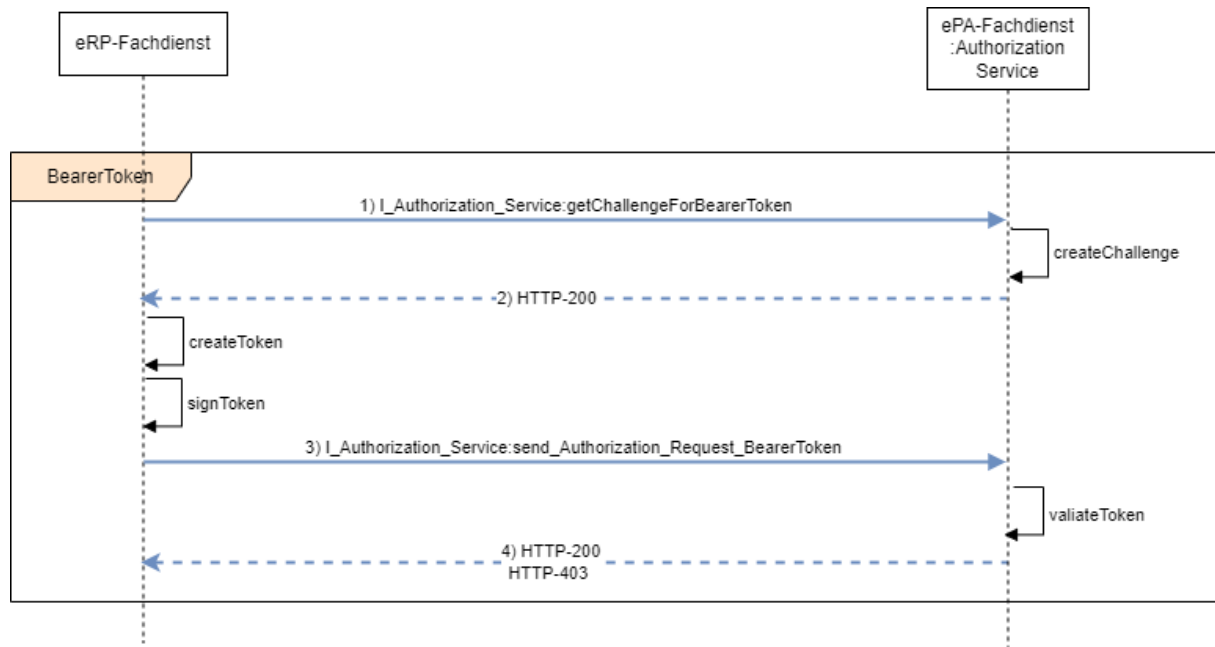
Der Authorization Service MUSS bei der Authentifizierung einer Leistungserbringerinstitution prüfen, dass das übermittelte JWT der Client Attestierung mindestens die folgenden Inhalte aufweist.

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256" oder "PS256"	
	"x5c"	Signaturzertifikat C.HCI.AUT	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"exp"	Verfalldatum, = "iat" + 20 min	Beispiel: "1705675744"
	"nonce"	Nonce aus einer <code>getNonce</code> Operation	siehe [I_Authorization_Service]

[ $\leq$ ]

Für das Signaturzertifikat zu "x5c" (AUT-Zertifikat der SMC-B) gilt: Basiert der öffentlichen Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

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



**Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes**

#### A\_25165-03 - Authorization Service: JWT Bearer-Token des E-Rezept-Fachdienstes

Das Authorization Service MUSS sicherstellen, dass die Authentifizierung des E-Rezept-Fachdienstes über die Schnittstelle `I_Authorization_Service` durch Verwendung eines gültig signierten JWT Bearer Token mit den dargestellten Mindest-Inhalten und Prüfung durch Regel 'rr0' des Befugnisverifikations-Moduls erfolgt. Die Claims in 'Payload' MÜSSEN dazu die Vorgaben aus [gemSpec\_Krypt], A\_24658\* befolgen.

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert

Part	Claim Name	Claim	Anmerkung
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Krypt]
	"sub"	Telematik-ID des E-Rezept-Fachdienstes	

6067 [**<=**]

6068 Das Signaturzertifikat zu "x5c" (AUT-Zertifikat der E-Rezept-VAU) kommt aus der  
 6069 Komponenten-PKI der TI. Basiert der öffentlichen Schlüssel auf der ECC-Kurve  
 6070 brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve  
 6071 und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß  
 6072 [RFC7515] zu erstellen.

## 6073 **3.18 Anbindung Verzeichnisdienst FHIR-Directory**

### 6074 **A\_25176 - ePA-Aktensystem - Anbindung Verzeichnisdienst FHIR-Directory**

6075 Das ePA-Aktensystem MUSS bei der Suche des Versicherten nach Einträgen  
 6076 im Verzeichnisdienst FHIR-Directory und bei der initialen Anlage einer Akte den  
 6077 Anwendungsfall "AF\_10219\* - Versicherter sucht Einträge im FHIR-Directory" gemäß  
 6078 [gemSpec\_VZD\_FHIR\_Directory] als Fachdienst unterstützen und dabei für die Client  
 6079 Anfrage von search-access\_token die Operation getFHIRVZDtoken gemäß  
 6080 [I\_Authorization\_Service.yaml] bereitstellen. [**<=**]

## 6081 **3.19 Access Gateway**

6082 Das Access Gateway ermöglicht den Versicherten bzw. deren berechtigten Vertretern den  
 6083 Zugang zum zugehörigen Aktensystem über das Internet. Auf der einen Seite dient es  
 6084 der Abschottung des ePA-Aktensystems in Richtung Internet, auf der anderen Seite  
 6085 regelt es den kontrollierten Zugriff der Versicherten auf das Aktensystem mit seinen  
 6086 funktionalen Komponenten.

### 6087 **3.19.1 Paketfilter**

#### 6088 **3.19.1.1 Funktion**

6089 Der Paketfilter stellt die Anbindung des ePA-Aktensystems an das Internet her und  
 6090 gewährleistet die Abschottung des ePA-Aktensystems in Richtung Internet.

#### 6091 **A\_14017 - Access Gateway, Sicherung zum Transportnetz Internet durch Paketfilter**

6092 Das ePA-Aktensystem MUSS zum Transportnetz Internet durch einen Paketfilter (ACL)  
 6093 gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der  
 6094 Paketfilter der Komponente Access Gateway MUSS frei konfigurierbar sein auf der  
 6095

6096 Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse,  
6097 IP-Protokoll sowie Quell- und Zielport.[<=]

6098 **A\_14018 - Access Gateway, Platzierung des Paketfilters Internet**

6099 Der Paketfilter der Komponente Access Gateway, zum Schutz in Richtung Transportnetz  
6100 Internet, DARF NICHT auf den anderen, zum Access Gateway gehörenden, physischen  
6101 Komponenten implementiert werden.[<=]

6102 **A\_14019-02 - Access Gateway, Richtlinien für den Paketfilter zum Internet**

6103 Der Paketfilter der Komponente Access Gateway MUSS die Weiterleitung von IP-Paketen  
6104 an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

- 6105 1. HTTPS, und  
6106 2. OCSP-Zugriffe für das OCSP-Stapling (vgl. Hinweis nach A\_14019-02), ggf.  
6107 notwendige DNS Anfragen (und Antworten).

6108 Ein Verbindungsaufbau aus dem ePA-Aktensystem über das Access Gateway in Richtung  
6109 Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 .[<=]

6110 *Hinweis zu A\_14019-02: Der Aktensystem-Anbieter muss für seine HTTPS-Schnittstelle*  
6111 *ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-*  
6112 *Zertifikate also über einen aktuellen Webbrowser prüfbar ist, vgl. A\_14776). Für dieses*  
6113 *TLS-Zertifikat fragt das Access Gateway (die HTTPS-Schnittstelle ist Teil davon)*  
6114 *regelmäßig für das OCSP-Stapling (vgl. [gemSpec\_Krypt#A\_24913-\*]) den OCSP-*  
6115 *Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält*  
6116 *das Access Gateway eine OCSP-Response. Diese wird nach A\_19126 geprüft und*  
6117 *anschließend von der HTTPS-Schnittstelle verwendet*  
6118 *(vgl. <https://tools.ietf.org/html/rfc6066#section-8> und*  
6119 *bspw. [http://nginx.org/en/docs/http/ngx\\_http\\_ssl\\_module.html#ssl\\_stapling](http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling) ).*

6120 Um dies zu ermöglichen, muss der Paketfilter entsprechende stateful-Firewall-Regeln  
6121 gemäß A\_14019-\* und A\_19126 definieren.

6122 **A\_19126-02 - Access Gateway, OCSP-Status für das OCSP-Stapling**

6123 Der Paketfilter der Komponente Access Gateway MUSS bezüglich des OCSP-Stapling  
6124 (vgl. A\_24913-\*) folgende Vorgaben umsetzen:

- 6125 1. Für das vom Aktensystem-Anbieter erworbene TLS-Zertifikat (vgl. Hinweis zu  
6126 A\_14019-01) MUSS die Komponente initial die IP-Adresse (ggf. die IP-Adressen)  
6127 des entsprechenden OCSP-Responser ermitteln.
- 6128 2. Diese IP-Adresse(n) MÜSSEN gemäß A\_14019-01 per stateful-Firewalling  
6129 Verbindungen von der HTTPS-Schnittstelle an den OCSP-Responder erlaubt  
6130 werden.
- 6131 3. Gemäß OCSP-Stapling ( <https://tools.ietf.org/html/rfc6066#section-8> ) MUSS die  
6132 Komponente regelmäßig eine OCSP-Response vom entsprechenden OCSP-  
6133 Responder beziehen (Die Regelmäßigkeit wird vom zertifikatsausgebenden TSP  
6134 und der Gültigkeitsdauer dessen OCSP-Responses bestimmt).
- 6135 4. Die OCSP-Responses MÜSSEN von der Komponente geprüft werden  
6136 (Signaturprüfung, CertID in der OCSP-Response passt zum angefragten  
6137 Zertifikat). Falls eine der Prüfung ein nicht-positives Ergebnis liefert, so MUSS die  
6138 erhaltene OCSP-Response verworfen werden.
- 6139 5. Sollte die letzte in der Komponente vorhandene OCSP-Response zeitlich nicht  
6140 mehr gültig sein (bspw. der OCSP-Responder im Internet war länger nicht  
6141 erreichbar), so MUSS diese OCSP-Response verworfen werden und ein von einem  
6142 Klienten (ePA FdV) initiiertes TLS-Verbindungsaufbau der HTTPS-Schnittstelle  
6143 ohne OCSP-Stapling durchgeführt werden.

6144 [ $\leq$ ]

6145 **A\_14776 - Access Gateway, Richtlinien zum TLS-Verbindungsaufbau**

6146 Die Komponente Access Gateway MUSS sich beim TLS-Verbindungsaufbau gegenüber  
6147 dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB  
6148 Forum] authentisieren. Das Zertifikat MUSS an die Schnittstelle der Proxy-Komponente  
6149 gebunden werden.[ $\leq$ ]

6150 **3.19.1.2 Redundanz**

6151 Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec\_Perf#3.18.1.3]. Die  
6152 Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Access  
6153 Gateways.

6154 Die Auswahl der Access Gateways wird durch das ePA-Frontend des Versicherten aus  
6155 einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des Access  
6156 Gateways kann der Anbieter des ePA-Aktensystems durch die Konfiguration und  
6157 Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn  
6158 jeder Versicherte mit existierendem Konto beim Anbieter des ePA-Aktensystems oder  
6159 dessen berechtigter Vertreter die Möglichkeit zum Verbindungsaufbau hat.

6160 Eine hardwaretechnische Hochverfügbarkeit der einzelnen Access Gateways ist über  
6161 grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht  
6162 dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische  
6163 Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern  
6164 einzusetzen, so dass jedes einzelne Access Gateway im Ergebnis eine höhere  
6165 Verfügbarkeit oder Leistungsfähigkeit besitzt.

6166 **A\_14026 - Access Gateway, Redundanz der Paketfilter im Access Gateway**

6167 Die Komponente Access Gateway MUSS sicherstellen, dass bei Ausfall eines von  
6168 mehreren Paketfiltern die verbleibenden Paketfilter in dem-selben Standort den  
6169 Datenverkehr aller Mandanten des ausgefallenen Paketfilters zusätzlich übernehmen  
6170 können.[ $\leq$ ]

6171 **3.19.1.3 Konfiguration**

6172 **A\_14030 - Access Gateway, Verhalten des Access Gateways bei Vollauslastung**

6173 Die Komponente Access Gateway MUSS den Paketfilter Internet so konfigurieren, dass  
6174 bei Vollauslastung der Systemressourcen im ePA-Aktensystem keine weiteren  
6175 Verbindungen angenommen werden.[ $\leq$ ]

6176 Durch die Zurückweisung von Verbindungen wird sichergestellt, dass das ePA-Frontend  
6177 des Versicherten einen Verbindungsaufbau mit einem anderen Access Gateway des  
6178 jeweiligen ePA-Aktensystems versucht, bei dem die erforderlichen Ressourcen zur  
6179 Verfügung stehen.

6180 **3.19.1.4 Adressierung**

6181 *3.19.1.4.1 Access Gateway zum Transportnetz Internet*

6182 **A\_14031 - Access Gateway, IPv4-Adressierung der Internetschnittstellen des**  
6183 **Access Gateways**

6184 Der Anbieter des ePA-Aktensystems MUSS jedem Access Gateway genau eine öffentliche  
6185 IPv4-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum  
6186 Internet konfiguriert werden. Die öffentlichen IP-Adressen des Access Gateways MÜSSEN  
6187 vom Anbieter des ePA-Aktensystems zur Verfügung gestellt werden.[ $\leq$ ]



**A\_14032 - Access Gateway, IPv6-Adressierung der Internetschnittstellen des Access Gateways**

Der Anbieter des ePA-Aktensystems SOLL jedem Access Gateway eine IPv6-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentliche IPv6-Adresse MUSS vom Anbieter des Access Gateways zur Verfügung gestellt werden. [≤]

**3.19.1.4.2 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. [≤]

**3.19.3 Proxy Schlüsselgenerierungsdienst**

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

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

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

**A\_17495 - Access Gateway, Zugriff auf den Schlüsselgenerierungsdienst**

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

**3.19.4 Tracing in Nichtproduktivumgebungen**

Für die Fehlersuche - insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase - hat es sich als notwendig erwiesen, dass ein Fehlersuchender den Klartext der Kommunikation zwischen ePA-Client und VAU-Instanz mitlesen kann. (vgl. auch 22.5: 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-

6229 Punkte vor DoS-Angriffen zu schützen, erlaubt das Access Gateway im Fall der Fälle die  
6230 TCP-Ports auf IP-Layer über Firewall-Regeln abzusichern.

### 6231 **A\_21890-01 - Access Gateway, Sensorpunkt für Nichtproduktivumgebungen**

6232 Die Komponente Access Gateway MUSS genau in Nichtproduktivumgebungen:

- 6233 • die Daten der Sensorpunkte des Aktensystems auf TCP-Ports (bspw. ab Port  
6234 8000) öffentlich (ggf. auch ohne TLS-Sicherung) im Internet zur Verfügung  
6235 stellen, indem die aktuell an den Sensorpunkten auflaufenden Daten auf dem  
6236 TCP-Port am Access Gateway öffentlich gestreamt werden.
- 6237 • die Möglichkeit bieten, den Zugriff auf diese TCP-Ports durch Firewall-  
6238 Einstellungen auf IP-Layer zu beschränken.

6239 Weiterhin MUSS das Access Gateway über die URL /tracingpoints Informationen über die  
6240 aktuell im AS verfügbaren und damit auch im Access Gateway öffentlich exponierten  
6241 Sensorpunkt-Daten als JSON-Array (=> Response-Type 'application/json') der folgenden  
6242 Form bereitstellen:

```
6243 [  
6244 {"name" : "zentraler Tigerproxy",  
6245  "port" : 8001,  
6246  "DoS-protection-type" : „secret_url“  
6247  "DoS-protection-port" : „udp/46789“  
6248 },  
6249 {"name" : "Extra Sensor VAU RZ2/B1/R1",  
6250  "port" : 8002,  
6251  "DoS-protection-type" : „ssh_tunnel“  
6252  "DoS-protection-port" : „tcp/46790“  
6253 }, ...  
6254 ]
```

6255 Sollten keine Sensorpunkte aktuell im AS aktiviert sein (bspw. bei Lasttests) so ist das  
6256 Array leer: [ ].

6257 Sollte es keinen optionalen DoS-Schutzmechanismus gemäß A\_22582-\* geben, so fallen  
6258 die DoS-\* Attribute in der o. g. Datenstruktur weg (sind nicht existent).

6259 Die einzelnen Felder des Arrays sind associative array (oder auch maps oder dictionaries  
6260 genannt). Diese KÖNNEN neben "name" und "port" beliebige vom AS definierbare,  
6261 weitere key-value-Paare enthalten. Der Eintrag "port" gibt an, an welchem öffentlich  
6262 erreichbaren TCP-Port des Access Gateway die Sensordaten des entsprechenden Sensors  
6263 abrufbar sind (gestreamt werden).

6264 [**<=**]

6265 *Hinweis zu A\_21890-\*: Die semistatische JSON-Datei, welche ein Client unter dem Pfad*  
6266 *„/tracingpoints“ erhalten kann, ist eine einfache Form von Service-Discovery. Damit kann*  
6267 *ein Client (Fehlersuchende(r)) erfahren, welche Tracing-Quellen es aktuell im AS gibt i.*  
6268 *S. v. welche Tracing-Quellen ein Client zur Fehlersuche aktuell verwenden kann.*

### 6269 **A\_22582 - Tracing in Nichtproduktivumgebungen, DoS-Schutz**

6270 Die Komponente Access Gateway KANN Sicherheitsmechanismen bereitstellen und  
6271 aktivieren, die es genau in Nichtproduktivumgebungen ermöglichen, temporär,  
6272 automatisiert und nur nach erfolgreicher Authentifizierung die TCP-Ports für das  
6273 Streaming der Sensorpunkte für Clients nach A\_21890-\* freizuschalten. [**<=**]

6274 *Hinweis zu A\_22582-\*: In den Nichtproduktivumgebungen darf es keine Echtdaten*  
6275 *geben. Es dürfen sich dort nur Daten befinden, deren Schutzbedarf bezüglich*  
6276 *Vertraulichkeit niedrig ist. Der optionale Schutzmechanismus nach A\_22582-\* braucht*  
6277 *nur einen einfachen DoS-Schutz leisten gegen einen Angreifer mit niedrigen*  
6278 *Angriffspotential. Der Anbieter ist, sofern er einen solchen Mechanismus einsetzen*  
6279 *möchte, frei, dafür den Mechanismus selbst zu wählen. Er wählt dann bei "DoS-*

6280 *protection-type" (vgl. A\_21890-\*) einen selbstdefinierten (möglichst sprechenden)*  
6281 *Namen.*

6282 Beispiele für Umsetzungsmöglichkeiten:

- 6283 1. Es gibt im Access Gateway eine geheime URL (bspw.  
6284 /tracing/964b059de83d20581f43dd1b867d740c). Ein Client kennt das Geheimnis  
6285 und ruft diese URL auf. Daraufhin wird im Access Gateway für die IP-Adresse des  
6286 Clients die Tracing-Quelle im Access Gateway frei geschaltet (TCP-Port 8000, ... ).
- 6287 2. Die gematik stellt eine Beispielimplementierung zur Verfügung. Dort gibt es einen  
6288 UDP-Server (Access Gateway) und einen UDP-Client (Fehlersuchende), die beide  
6289 ein gemeinsames HMAC-Geheimnis teilen. Wenn der Client die aktuelle Zeit und  
6290 dessen IP-Adresse per HMAC authentisiert dem UDP-Server sendet, so schaltet  
6291 der UDP-Server nach erfolgreicher Prüfung des HMACs den entsprechenden TCP-  
6292 Port für die authentifizierte IP-Adresse des Clients frei.
- 6293 3. Auf dem Access Gateway läuft ein SSH-Daemon. Der öffentliche  
6294 Authentisierungsschlüssel eines Clients ist dort als gültiger Nutzer konfiguriert  
6295 (Login-Shell: /bin/false). Die Tracing-Quellen im Access Gateway sind so  
6296 konfiguriert, dass sie nur mittels authentisierten SSH-Port-Forwarding (  
6297 <https://www.ssh.com/academy/ssh/tunneling/example>) erreichbar sind.

### 6298 3.19.5 Übergreifende Festlegungen

#### 6299 **A\_14249 - Komponente Access Gateway - Separierung der Schnittstellen für** 6300 **verschiedene Umgebungen**

6301 Die Komponente Access Gateway MUSS die Bereitstellung von Schnittstellen für die  
6302 Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen  
6303 Umgebungen der TI (RU/TU, PU) sicherstellen und voneinander separieren. [ <= ]

#### 6304 **A\_14034 - Access Gateway, Übergang des ePA-Aktensystems zur TI**

6305 Die Komponente Access Gateway MUSS sicherstellen, dass der Zugriff auf Dienste der TI  
6306 ausschließlich über einen Sicheren Zentralen Zugangspunkt (SZZP) erfolgt. [ <= ]

#### 6307 **A\_14036 - Access Gateway, Synchronisierung der Komponenten mit den** 6308 **Stratum-1-NTP-Servern der TI**

6309 Die Komponente Access Gateway MUSS alle Komponenten seines Access Gateways mit  
6310 den Stratum-1-NTP-Servern der TI synchronisieren. [ <= ]

6311

#### 6312 **A\_13879 - Access Gateway, Serverseitige Authentisierung**

6313 Die Komponente Access Gateway MUSS sich gegenüber dem ePA-Frontend des  
6314 Versicherten beim Aufbau der TLS-Session durch sein ExtendedValidation-  
6315 Zertifikat authentisieren. Die Beschaffung des Zertifikats erfolgt durch den Anbieter über  
6316 eine öffentliche CA. [ <= ]

#### 6317 **A\_14033 - Access Gateway, TLS Verschlüsselung**

6318 Die Komponente Access Gateway MUSS sicherstellen, dass jede Kommunikation mit dem  
6319 ePA-Frontend des Versicherten TLS verschlüsselt erfolgt. [ <= ]

6320 Die Verwendung der SoapAction ermöglicht einer Reverse-Proxy-Komponente innerhalb  
6321 des Access Gateways, die Nachrichten zu verarbeiten, ohne die http-Payload zu  
6322 untersuchen.

#### 6323 **A\_13876 - Access Gateway, Kein direkter Zugriff auf Dienste der zentralen TI-** 6324 **Plattform**

6325 Die Komponente Access Gateway MUSS einen direkten Zugriff aus dem Internet auf  
6326 Dienste der zentralen TI-Plattform verhindern. [ <= ]

#### 6327 **A\_14016 - Access Gateway , Schutz vor Angriffen aus dem Internet**

6328 Die Komponente Access Gateway MUSS für alle vom Internet erreichbaren Schnittstellen  
6329 Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere  
6330 Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS  
6331 Lösungen verhindert werden. [ <= ]

#### 6332 **A\_15196 - Access Gateway, Schutz vor volumetrischen DoS-Angriffen**

6333 Die Komponente Access Gateway MUSS bei Beauftragung eines qualifizierten  
6334 Dienstleisters zum Schutz vor volumetrischen DoS-Angriffen Kriterien des BSI zur  
6335 Auswahl qualifizierter Dienstleister umsetzen. [ <= ]

6336 Als Maßnahme gegen volumetrische Denial-of-Service-Angriffe wird die Verwendung von  
6337 DNS- oder BGP-Routing-Diensten empfohlen. Hinweise des BSI:

6338 [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)  
6339 [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).

### 6340 **~~3.20 Data Submission Service~~**

6341 ~~Die Daten der elektronischen Patientenakten sollen nach § 363 Absatz 1 SGB V für die in~~  
6342 ~~§ 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszwecke zugänglich gemacht und~~  
6343 ~~hierfür in pseudonymisierter Form automatisiert von den ePA-Aktensystemen an das~~  
6344 ~~Forschungsdatenzentrum Gesundheit (FDZ) nach § 303d SGB V übermittelt werden,~~  
6345 ~~sofern Versicherte dem nicht widersprochen haben.~~

6346 ~~Neben dem FDZ und den ePA-Aktensystemen ist die Vertrauensstelle (VST) nach § 303c~~  
6347 ~~SGB V im Prozess involviert. Deren Aufgabe ist es, die von den ePA-Aktensystemen~~  
6348 ~~erhaltenen Lieferpseudonyme in periodenübergreifende Pseudonyme umzuwandeln und~~  
6349 ~~diese an das FDZ zu übermitteln.~~

6350 ~~Der Data Submission Service im Aktensystem übernimmt in der Übermittlung der~~  
6351 ~~pseudonymisierten medizinischen Daten folgende Aufgaben:~~

- 6352 ~~• Erstellung der Lieferpseudonyme (auf Basis der KVNR) und der Arbeitsnummern~~
- 6353 ~~• Registrierung der Arbeitsnummer mit dem zugehörigen Lieferpseudonym bei der~~  
6354 ~~Vertrauensstellen~~
- 6355 ~~• Pseudonymisierung der medizinischen Daten~~
- 6356 ~~• Verknüpfung der pseudonymisierten medizinischen Daten mit der Arbeitsnummer~~
- 6357 ~~• Übermittlung der pseudonymisierten medizinischen Daten und der zugehörigen~~  
6358 ~~Arbeitsnummern an das Forschungsdatenzentrum Gesundheit~~

6359 ~~Die Übermittlung der Daten erfolgt blockweise. D.h. es wird ein Paket von~~  
6360 ~~pseudonymisierten medizinischen Daten mit zugehörigen Arbeitsnummern aus~~  
6361 ~~verschiedenen Aktenkonten zusammengestellt (Datenpaket FDZ) und alle für dieses~~  
6362 ~~Paket benötigten Arbeitsnummern und Lieferpseudonyme mit einem Mal bei der VST~~  
6363 ~~registriert (Datenpaket VST). Die Datenpakete haben eine anbieterübergreifend~~  
6364 ~~eindeutige SubmissionID und die SubmissionID zusammengehöriger Datenpakete VST~~  
6365 ~~und FDZ ist identisch.~~

6366 ~~Für die Übermittlung wird zwischen Aktensystem und VST, sowie Aktensystem und FDZ~~  
6367 ~~jeweils ein beidseitig authentisierter VAU-Kanal aufgebaut, auf dem sich die Dienste VST~~  
6368 ~~und FDZ mit einer Identität ID.FD.AUT mit ihren entsprechenden Rollen authentisieren.~~

Der Versicherte kann mit Hilfe seines ePA-FdVs oder über die Ombudsstelle des Kostenträgers der Übermittlung seiner pseudonymisierten medizinischen Daten an das FDZ widersprechen oder die möglichen Sekundärnutzungszwecke seiner übermittelten pseudonymisierten medizinischen Daten im FDZ einschränken. Dies erfolgt über das Consent Decision Management im Aktensystem.

### 3.20.1 Erstellung von Arbeitsnummern und Lieferpseudonymen

Der Data Submission Service erzeugt eindeutige Arbeitsnummern und Lieferpseudonyme, um die pseudonymisierten medizinischen Daten in der Übermittlung an das FDZ eindeutig zuordnen zu können.

#### ~~A\_26211—Data Submission Service—Erstellung des Lieferpseudonyms~~

Der Data Submission Service MUSS das Lieferpseudonym des Versicherten gemäß [I\_VST] unter Verwendung der KVNR des Versicherten erstellen. [ $\leq$ ]

#### ~~A\_26409—Data Submission Service—keine Erstellung von LP für Validierungsaktenkonten~~

Der Data Submission Service DARF KEINE Lieferpseudonyme für KVNRn von Validierungsaktenkonten erstellen. [ $\leq$ ]

#### ~~A\_26212—Data Submission Service—Erstellung der Arbeitsnummer~~

Der Data Submission Service MUSS für die Arbeitsnummer einen Zufallswert mit einer Mindestentropie von 120 Bit erzeugen und die Kodierung aus [I\_VST] verwenden. [ $\leq$ ]

#### ~~A\_26410—Data Submission Service—keine Erstellung von AN für Validierungsaktenkonten~~

Der Data Submission Service DARF KEINE Arbeitsnummern für Daten aus Validierungsaktenkonten erstellen. [ $\leq$ ]

#### ~~A\_26255—Data Submission Service—Verwendungsdauer von Lieferpseudonymen und Arbeitsnummern~~

Der Data Submission Service MUSS für jedes in einem Datenpaket FDZ übermittelte pseudonymisierte medizinische Datum zu einer KVNR eine neue Arbeitsnummer und ein neues Lieferpseudonym generieren. [ $\leq$ ]

#### ~~A\_26256—Data Submission Service—Registrierung von Arbeitsnummern~~

Der Data Submission Service MUSS jede Arbeitsnummer zusammen mit dem zugehörigen Lieferpseudonym in das entsprechende Datenpaket VST aufnehmen und an die Vertrauensstelle übermitteln. [ $\leq$ ]

### 3.20.2 Auswahl von medizinischen Daten

Der Data Submission Service muss bestimmte neue und geänderte FHIR-Ressourcen an den FDZ übertragen. Dies betrifft im ersten Schritt die Medikationsdaten aus der E-Medikationsliste und wird subsequent weiter ausgebaut.

Der Medication Service, als Quelle der Medikationsdaten zur Übertragung an den FDZ, erlaubt flexible, datenbasierte Operationen auf einzelnen FHIR-Ressourcen. Dies erfordert entsprechende Implementierung um effizient und zuverlässig die neuen und geänderten Ressourcen identifizieren können um daraus die Auswahl für die zu übertragende FHIR-Ressourcen treffen zu können.

### ~~A\_26296—Data Submission Service—Übertragung neuer und geänderter FHIR-Ressourcen~~

~~Der Data Submission Service MUSS neue und geänderte FHIR-Ressourcen identifizieren können und daraus die Auswahl für die Übermittlung der Daten an FDZ treffen können. [≤]~~

### ~~A\_26297—Data Submission Service—Einschränkung der FHIR-Ressourcen nach Änderungsdatum~~

~~Der Data Submission Service MUSS den Zeitpunkt der letzten Übermittlung (lastSubmissionTimestamp) merken und in nachfolgenden Übermittlungen nur die Ressourcen, die sich seit diesem Zeitpunkt geändert haben, berücksichtigen. Hierfür ist das FHIR-Element meta.lastUpdated in der jeweiligen FHIR-Ressource zu verwenden. [≤]~~

~~Hinweis: Ressourcen, die im Rahmen eines Anbieterwechsels in ein Aktenkonto übernommen werden, sind nicht erneut zu übermitteln.~~

### ~~A\_26298—Data Submission Service—FHIR-Ressourcen zur Übermittlung an FDZ~~

~~Der Data Submission Service MUSS die FHIR-Ressourcen gemäß der Tabelle "Auswahl der zu übertragenden FHIR-Ressourcen" an FDZ übertragen, dabei sind die Filter-Bedingungen (Spalte 'Filter Expression') und zu inkludierende referenzierte Ressourcen zu berücksichtigen (Spalte 'Include' sowie Tabelle "Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen"). [≤]~~

~~Table 1 Auswahl der zu übertragenden FHIR-Ressourcen~~

<del>Ressourcentyp/Profil</del>	<del>Filter Expression</del>	<del>Include</del>
<del>MedicationRequest \${epa-medication}/epa-medication-request</del>	<del>status != 'active' and identifier.where(system='https://gematik.de/fhir/epa-medication/sid/rx-prescription-process-identifier').hasValue()</del>	<del>MedicationRequest: :medication</del>
<del>MedicationDispense \${epa-medication}/epa-medication-response</del>	<del>status != 'in-progress' and extension('https://gematik.de/fhir/epa-medication/StructureDefinition/rx-prescription-process-identifier-extension').hasValue()</del>	<del>MedicationDispense: :medication</del>

~~Table 2 Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen~~

<del>Ressourcentyp/Profil</del>	<del>Anmerkung</del>
<del>Medication \${epa-medication}/epa-medication</del>	<del>Referenziert durch MedicationRequest, MedicationDispense</del>

### ~~A\_26461—Data Submission Service—Protokollierung eines Datenexports für das FDZ~~



Der Data Submission Service MUSS nach dem Zugriff auf zu exportierende Daten des Medication Service (gemäß A\_26298\*) den folgenden Protokolleintrag gemäß A\_24704\* erzeugen und dabei folgende zusätzliche Vorgaben zur Wertebelegung berücksichtigen:

**Tabelle 42 Vorgaben AuditEvent für Datenexport an FDZ**

Element [AuditEvent]		Beschreibung	Zu verwendender Wert
type:		Art des Ereignisses, das protokolliert wird	
	system	Das verwendete Codesystem	" <a href="http://dicom.nema.org/resources/ontology/DCM">http://dicom.nema.org/resources/ontology/DCM</a> "
	code	Der verwendete Code aus dem Codesystem	"110106"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Export"
purposeOfEvent:		Hält den Zweck des Datenexports fest (hier Export für das FDZ).	
	system	Das verwendete Codesystem	" <a href="https://gematik.de/fhir/epa/ValueSet/epa-auditevent-purpose-of-event-vs">https://gematik.de/fhir/epa/ValueSet/epa-auditevent-purpose-of-event-vs</a> "
	code	Der verwendete Code aus dem Codesystem	"EXPORTFDZ"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Export für das Forschungsdatenzentrum Gesundheit"
agent[internal]:		Information zum Auslöser des Audit Events	
	type.system	Das verwendete Codesystem	" <a href="https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs">https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs</a> "
	type.code	Der verwendete Code aus dem Codesystem	"DATASUBSVC"



Element [AuditEvent-]		Beschreibung	Zu-verwendender-Wert
	type.display	Der Bezeichner zur Anzeige aus dem Codesystem	"Data-Submission-Service"
source-		Informationen zum auslösenden Service des Aktensystems	
source.observer-	display	Fester Wert "Elektronische Patientenakte Fachdienst"	"Elektronische Patientenakte Fachdienst"
source.type-		Der auslösende Service gemäß des zulässigen Value-Sets aus [gemSpec_EPAAuditEvent]-	
	system	Das verwendete Codesystem	" <a href="https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs">https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs</a> "
	code	Der verwendete Code aus dem Codesystem	"DATASUBSVC"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Data-Submission-Service"
entity-			
	detail.type	"data-min-date"	

Element [AuditEvent-]		Beschreibung	Zu-verwendender-Wert
	d etail.valu e[*]	Frühester Erstellungs- oder— Änderungszeitpunkt der Daten, die für den Export relevant sind; d.h., Daten die nach diesem Zeitpunkt erstellt oder verändert wurden, wurden exportiert.  Der Zeitstempel MUSS im Format YYYY-MM- DDThh:mm:ssZ angegeben werden.	

Ein erfolgloser Export der Daten aus dem Medication Service DARF NICHT protokolliert werden.

[<=]

### 3.20.3 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 passieren, 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.

### **3.20.4 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 oder Migration einer vorherigen Version der ePA) und nicht die erste Datenübermittlung nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung.

Hinweis: Für eine Übermittlung nach Ablauf dieser Widerspruchsfrist oder nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung werden immer nur ab diesem Zeitpunkt neu angefallene Daten berücksichtigt. Es erfolgt keine Übermittlung von vorhandenen Daten des Aktenkontos.

#### **A\_26214—Data Submission Service—Erstellung der SubmissionID**

Der Data Submission Service MUSS für zusammengehörige Datenpakete VST und FDZ eine gemeinsame anbieterübergreifend eindeutige SubmissionID erzeugen und diese mit den Datenpaketen übertragen. [<=]

#### **A\_26304—Data Submission Service—Zufällige SubmissionID**

Der Data Submission Service MUSS sicherstellen, dass die SubmissionID ein zufällig gewählter 256-Bit Wert mit einer Mindestentropie von 120 Bit ist. [<=]

#### **A\_26215—Data Submission Service—Übermittlung Datenpaket VST**

Der Data Submission Service MUSS das Datenpaket VST gemäß [I\_VST] an die Vertrauensstelle übermitteln. [<=]

#### **A\_26407—Data Submission Service—keine Übermittlung von Daten aus Validierungsaktenkonten**

Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem. Kapitel 2.4) an das Forschungsdatenzentrum übermitteln. [<=]

#### **A\_26216—Data Submission Service—Realisierung der Schnittstelle**

##### **I\_Data\_Submission\_Service**

Der Data Submission Service MUSS die Operationen der Schnittstelle I\_Data\_Submission\_Service gemäß [I\_Data\_Submission\_Service] umsetzen. [<=]

#### **A\_26217—Data Submission Service—Verbindung zur Vertrauensstelle**

Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des Datenpakets VST ausschließlich über einen VAU-Kanal erfolgt in dem sich die Vertrauensstelle über ein Zertifikat C.FD.AUT mit professionOID gleich oid\_epa\_vst authentisiert hat. [<=]

#### **~~A\_26218—Data Submission Service—Verbindung zum Forschungsdatenzentrum Gesundheit~~**

Der Data Submission Service MUSS sicher stellen, dass die Übermittlung des Datenpakets FDZ ausschließlich über einen VAU-Kanal erfolgt in dem sich das Forschungsdatenzentrum Gesundheit über ein Zertifikat C.FD.AUT mit professionOID gleich oid\_epa\_fdz authentisiert hat. [<=]

#### **~~A\_26299—Data Submission Service—Wechsel des Verschlüsselungsschlüssels für Datenpakete~~**

Falls die Datenpakete VST und FDZ außerhalb der VAU im System des Aktensystembetreibers gespeichert werden, MUSS der Data Submission Service sicherstellen, dass ein Schlüssel für die Verschlüsselung der Datenpakete VST bzw. FDZ maximal 4 Wochen genutzt werden kann und danach ein neuer Verschlüsselungsschlüssel mittels der Regel hsm-r8 mit Hilfe eines geänderten Ableitungsvektors abgeleitet wird. [<=]

#### **~~A\_26312—Data Submission Service—Timeout in der Übermittlung~~**

Der Data Submission Service MUSS die Übermittlung der Pakete VST und FDZ erneut starten, wenn das Datenpaket FDZ nicht innerhalb von 30 Minuten nach erfolgreicher Übermittlung des Datenpakets VST abgerufen wird. [<=]

#### **~~A\_26313—Data Submission Service—Konfiguration der Intervalle und maximalen Größe eines Datenpakets~~**

Der Data Submission Service MUSS folgende Parameter konfigurierbar gestalten:

- das Intervall in dem Datenpakete VST und FDZ übermittelt werden
- eine maximale Größe eines Datenpakets FDZ bei deren Erreichen die Datenpakete übermittelt werden

[<=]

#### **~~A\_26244—Data Submission Service—Löschen von Datenpaketen nach Übermittlung~~**

Der Data Submission Service MUSS nach erfolgreicher Übermittlung des Datenpakets FDZ an das Forschungsdatenzentrum Gesundheit das übermittelte Datenpaket FDZ und das zugehörige Datenpaket VST lokal löschen. [<=]

#### **~~A\_26245—Data Submission Service—Löschen von Datenpaketen bei Nicht-Übermittlung~~**

Der Data Submission Service MUSS das Datenpaket FDZ und das zugehörige Datenpaket VST lokal löschen, wenn das Datenpaket FDZ länger als 72 Stunden nicht an das Forschungsdatenzentrum Gesundheit übermittelt werden konnte. Die enthaltenen Widersprüche MÜSSEN in die aktuell in Erstellung befindlichen Datenpakete VST und FDZ übernommen werden. [<=]

*Hinweis: Wenn Widersprüche in ein neues Datenpaket übernommen werden, muss für jeden der Widersprüche eine neue Arbeitsnummer (AN) und ein Lieferpseudonym (LP) erstellt werden, da die bisherigen AN und LP im Kontext des zu löschenden Paketes stehen.*

#### **~~A\_26246—Data Submission Service—Aufnahme von Widersprüchen~~**

Der Data Submission Service MUSS Widersprüche gegen die Freigabe von Daten zur Sekundärnutzung durch das FDZ oder Änderungen zu Sekundärnutzungszwecken, aus dem Consent Decision Management, in die aktuell in Erstellung befindlichen Datenpakete

~~VST und FDZ übernehmen. Es MUSS sichergestellt werden, dass in einem Datenpaket FDZ für eine 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.*~~

### **3.213.20 Schnittstellen (OpenAPI)**

Hinweis: Die Vorgaben in den beschreibenden Dateien der REST-Schnittstellen (yaml) sind normativ für den Anbieter der Schnittstellen. Die Anforderungen im vorliegenden Dokument ergänzen diese Vorgaben, insbesondere, wenn diese für sicherheitstechnische Gutachten erforderlich sind.

6590 **3-21-13.20.1 Übersicht der Schnittstellen des Aktensystems**

6591 **Tabelle 41: Übersicht der Schnittstellen des Aktensystems**

<b>Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)</b>	
<b>I_Consent_Decision_Management</b>	
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.
<del>updateDataUsagePurposes</del>	<del>Diese Operation erlaubt dem FdV und der Ombudsstelle die Änderung der Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden.</del>
<del>getDataUsagePurposes</del>	<del>Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht der aktuellen Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden bzw. wurden.</del>

getUserSpecificMedicationDenyList	Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht, welche LEI keinen Zugriff auf den Medication Service haben.
setUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI in die Liste der LEIs aufzunehmen, die keinen Zugriff auf den Medication Service haben.
getUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine bestimmte LEI aus der Liste der LEIs anzuzeigen, die keinen Zugriff auf den Medication Service haben.
deleteUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI aus der Liste der LEIs zu entfernen, damit diese LEI wieder Zugriff auf den Medication Service haben kann.
<b>I_Constraint_Management_Insurant</b>	
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.
<b>I_Entitlement_Management</b>	
Schnittstelle des Entitlement Management gemäß [I_Entitlement_Management] zur Vergabe von Befugnissen und Befugnisausschlüssen	
setEntitlementPs	Diese Operation fügt eine Befugnis für eine Leistungserbringerinstitution in einer Behandlungssituation hinzu.
getEntitlements	Diese Operation erlaubt dem FdV den Abruf aller aktuellen Befugnisse.



getEntitlement	Diese Operation erlaubt dem FdV den Abruf einer bestimmten Befugnis.
setEntitlement	Diese Operation erlaubt dem FdV das Setzen einer Befugnis für einen Nutzer.
deleteEntitlement	Diese Operation erlaubt dem FdV den Abruf das Löschen einer existierenden Befugnis.
getBlockedUserPolicyAssignments	Diese Operation erlaubt dem FdV den Abruf der aktuell vorhandenen Befugnisausschlüsse.
setBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Befugnisausschluss für einen Nutzer.
getBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Abruf eines bestimmten Befugnisausschlusses.
deleteBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV die Aufhebung eines Befugnisausschlusses.
<b>I_Entitlement_Management_EU</b>	
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.
<b>Render API: PDF Audit</b>	
Schnittstelle des Audit Event Service gemäß [IG_Audit_Event_Service] zum Abruf der Protokolldaten in lesbarer Form	
renderAuditEventsToPDF	Diese Operation erlaubt FdV und Ombudsstelle den Abruf der Protokolldaten als PDF.
<b>Query API: AuditEvent</b>	

Schnittstelle des Audit Event Service gemäß [IG_Audit_Event_Service] 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.
<b>I_Health_Record_Relocation_Service</b>	
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.
<b>I_Device_Management_Insurant</b>	
Schnittstelle zur Geräteverwaltung aus der Umgebung des Versicherten	
getDevice	Diese Operation ruft eine bestimmte Geräteregistrierung ab.
getDevices	Diese Operation ruft alle Geräteregistrierungen ab.
updateDevice	Diese Operation ändert den Displayname einer Geräteregistrierung.
deleteDevice	Diese Operation löscht eine bestimmte Geräteregistrierung.
registerDevice	Diese Operation erzeugt eine neue Geräteregistrierung und neue Geräteparameter
confirmPendingDevice	Diese Operation bestätigt eine neue Geräteregistrierung mit einem Geräteregistrierungscode
getDeviceAttestation	Diese Operation ruft die Bestätigung einer Geräteregistrierung am Home-AS ab.

<b>I_Authorization_Service</b>	
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
<b>I_Medication_Service_eML_Render</b>	
renderEMLasHTML	Diese Operation gibt die Medikationsliste im html-Format zurück.
renderEMLasPDF	Diese Operation gibt die Medikationsliste im PDF/A-Format zurück.
<b>I_Medication_Service_FHIR</b>	
REST-Schnittstelle zum Abruf der Medikationsdaten im FHIR-Format	

<b>I_Email_Management</b>	
<del>setEmailAddress</del>	<del>Diese Operation registriert eine neue E-Mail-Adresse für einen FdV-Nutzer/Versicherten.</del>
getEmailAddress	Diese Operation ruft die <u>hinterlegte</u> E-Mail-Adresse <del>für einen FdV-Nutzer/des</del> Versicherten ab.
replaceEmailAddress	Diese Operation <u>setzt oder</u> ändert die E-Mail Adresse für einen <del>FdV-Nutzer/</del> Versicherten ab.
<b>I_Tool_Convert_PDF_Insurant</b>	
Schnittstelle des XDS Document Managements gemäß [I_Tool_Convert_PDF_Insurant]	
convertPDF	Diese Operation konvertiert ein PDF in ein PDF/A Format
<b>I_Data_Submission_Service</b>	
Schnittstelle des Data Submission Service gemäß [I_Data_Submission_Service]	
getSubmissionPackage	Diese Operation stellt dem FDZ ein Datenpaket für eine bestimmte SubmissionID bereit.

6592

Schnittstellen des Aktensystems (Nutzung ohne VAU-Kanal)	
<b>I_Information_Service</b>	
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.
<b>I_Information_Service_Accounts</b>	
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

6593 Die Schnittstellen (REST) und Operationen sind funktional in den Beschreibungen der  
 6594 jeweiligen Schnittstelle beschrieben. Darüber hinaus gelten die folgenden übergreifenden  
 6595 Anforderungen.

6596 **3-21-23.20.2 Übergreifende Festlegungen zu den Schnittstellen**6597 **A\_23918 - Schnittstellen (OpenApi) - Prüfung der Befugnis**

6598 Das **ePA**-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen  
6599 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)  
6600 eine vorhandene und gültige Befugnis (entitlement) für den Nutzer der Operation fordern  
6601 und diese nicht vorliegt. [ $\leq$ ]

6602 *Hinweis: A\_23918 deckt auch die Fehlersituationen "kein VAU-Kanal" und "keine User*  
6603 *Session" ab, da diese eine Vorbedingung für den Nachweis einer gültigen Befugnis sind.*

6604 **A\_24365 - Schnittstellen (OpenApi) - Prüfung des Aktenkontos**

6605 Das **ePA**-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen  
6606 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)  
6607 die Existenz des adressierten Aktenkontos fordern und diese nicht für den  
6608 Operationsaufruf verwendet wird. [ $\leq$ ]

6609 *Hinweis A\_24365 deckt auch die Fehlersituation "kein Health Record Context" ab, da*  
6610 *dieses nur infolge eines nicht vorhandenen Aktenkontos auftritt.*

6611 **A\_24538 - Schnittstellen (OpenApi) - Prüfung des Aktenkontostatus**

6612 Das **ePA**-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen  
6613 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)  
6614 einen vorgegebenen Status des Aktenkontos fordern und dieser nicht vorhanden ist. [ $\leq$ ]

6615 **A\_24366 - Schnittstellen (OpenApi) - Prüfung der Rolle**

6616 Das **ePA**-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen  
6617 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)  
6618 die Zulässigkeit der Operation auf bestimmte Rollen (professionOID) einschränken und  
6619 der Nutzer der Operation diese nicht nachweist. [ $\leq$ ]

6620 **A\_24367 - Schnittstellen(OpenApi) - Prüfung des Identifiers**

6621 Das **ePA**-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen  
6622 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)  
6623 die Zulässigkeit der Operation auf bestimmte Identifier (KVNR oder Telematik-ID)  
6624 einschränken und der Nutzer der Operation diese nicht nachweist. [ $\leq$ ]

6625 **A\_24580 - Schnittstellen (OpenApi) - Protokollierung der Operationen**

6626 Das **ePA**-Aktensystem MUSS nach der Ausführung der Operationen der REST-  
6627 Schnittstellen eine Protokolleintrag erstellen, wenn die Protokollierung in den  
6628 Nachbedingungen (Postconditions) der Operationen gefordert ist (log-entry). [ $\leq$ ]

---

## 4 Informationsmodelle

---

6629

6630 Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten  
6631 wird nicht benötigt.



6632

## 5 Anhang A – Verzeichnisse

6633

### 5.1 Abkürzungen

Kürzel	Erläuterung
AdV	Anwendungen des Versicherten
<del>AN</del>	<del>Arbeitsnummer in der Übermittlung von Daten zur Sekundärnutzung</del>
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
<del>FDZ</del>	<del>Forschungsdatenzentrum Gesundheit</del>
HL7	Health Level Seven
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IHE ITI TF	IHE IT Infrastructure Technical Framework
JWT	JSON-Web-Token
JWS	signiertes JSON-Web-Token

KTR	Kostenträger
<del>LP</del>	<del>Lieferpseudonym in der Übermittlung von Daten zur Sekundärnutzung</del>
MIO	Medizinisches Informationsobjekt
MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
PDSG	Patientendaten-Schutz-Gesetz
PHR	Personal Health Record
RMU	Restricted Metadata Update Profile
SAML	Security Assertion Markup Language
TLS	Transport Layer Security
UUID	Universally Unique Identifier
VAU	Vertrauenswürdige Ausführungsumgebung
<del>VST</del>	<del>Vertrauensstelle Elektronische Patientenakte</del>
W3C	World Wide Web Consortium
WS-I	Web-Services Interoperability Consortium
XCA	Cross-Community Access Profile
XDS	Cross-Enterprise Document Sharing Profile
XDW	Cross-Enterprise Document Workflow Profile
XOP	XML-binary Optimized Packaging
XSPA	Cross-Enterprise Security and Privacy Authorization Profile

5.2 Glossar

Begriff	Erläuterung
Authenticator-Modul	Das Authenticator-Modul ist die Client-Komponente zum sektoralen Identity Provider. Über die das Authenticator-Modul authentifiziert sich der Versicherte gegenüber des sektoralen IDP. Das Authenticator-Modul kann in ein App (z.B. Service-App einer Krankenkasse oder ePA-FdV) integriert oder als eigenständige App implementiert werden (siehe auch [gemSpec_IDP_Sek]).

Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.

5.3 Abbildungsverzeichnis

Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls.....	58
Abbildung 2: Überblick Service VAUs .....	91
Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung .....	95
Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer Überschlüsselung .....	96

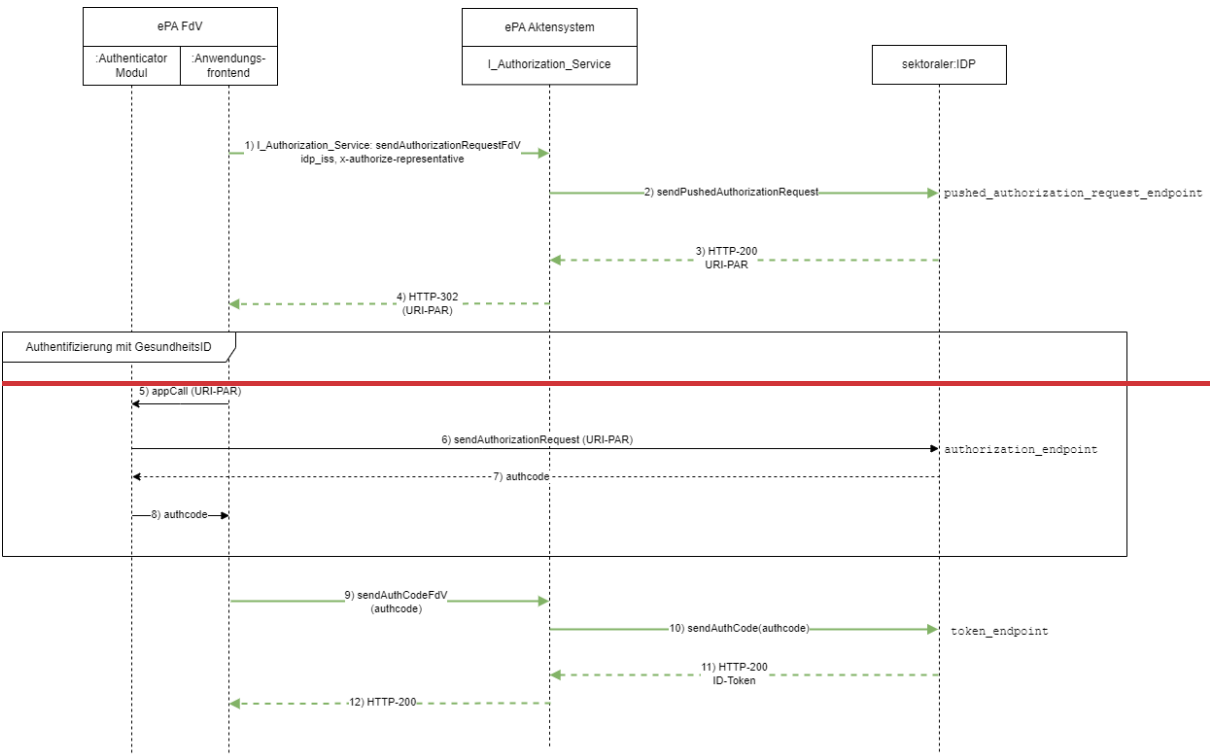


Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP .....	229
Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP .....	234
Abbildung 7: Ablauf der Authentisierung des E-Rezept Fachdienstes .....	235

6648	<u>Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls .....</u>	58
6649	<u>Abbildung 2 - Überblick Service-VAUs .....</u>	91
6650	<u>Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung .....</u>	95
6651	<u>Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer</u>	
6652	<u>Überschlüsselung .....</u>	96
6653	<u>Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP ..</u>	229
6654	<u>Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP .....</u>	234
6655	<u>Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes .....</u>	235
6656		

## 6657 5.4 Tabellenverzeichnis

6658	<u>Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat .....</u>	22
6659	<u>Tabelle 2: Protokollierung der Migration der medizinischen Daten .....</u>	33
6660	<u>Tabelle 3: Protokollierung der Migration der Protokolldaten des Versicherten .....</u>	34
6661	<u>Tabelle 4: Zustandswechsel im Lebenszyklus eines Aktenkontos .....</u>	38
6662	<u>Tabelle 5: Protokollierung von Änderungen des Aktenkontostatus .....</u>	39
6663	<u>Tabelle 6 : Health Record Relocation Service Protokollierung .....</u>	48
6664	<u>Tabelle 7: Tab_AS_VAU-Token_Modul_Rules-Prüfregeln VAU-Token .....</u>	59
6665	<u>Tabelle 8: Überblick über die Regeln des Befugnisverifikations-Moduls .....</u>	65
6666	<u>Tabelle 9: Tab_AS_Entitlement_Registration_Rules-Regeln zur Registrierung von</u>	
6667	<u>Befugnissen .....</u>	67
6668	<u>Tabelle 10: Tab_AS_SDS-Key_Rules-Key Rules-Regeln zur Ableitung der</u>	
6669	<u>versichertenindividuellen Persistierungsschlüssel .....</u>	77
6670	<u>Tabelle 11: Widerspruchsfähige Funktionen der elektronischen Patientenakte .....</u>	99
6671	<u>Tabelle 12: Consent Decision Management Protokollierung-Widersprüche für Funktionen</u>	
6672	<u>der ePA .....</u>	101
6673	<u>Tabelle 13: Consent Decision Management Protokollierung-Widersprüche zu</u>	
6674	<u>Sekundärnutzungszwecken .....</u>	103
6675	<u>Tabelle 14: Consent Decision Management Protokollierung-User Specific Deny Policy</u>	
6676	<u>Medication .....</u>	106
6677	<u>Tabelle 15: Inhalt einer Befugnis .....</u>	106
6678	<u>Tabelle 16: Befugnisse für berechtigte Nutzergruppen und Nutzer .....</u>	108
6679	<u>Tabelle 17: Befugnisse EU-Zugriff für berechtigte Nutzergruppen und Nutzer .....</u>	111
6680	<u>Tabelle 18: Entitlement Management Protokollierung .....</u>	112
6681	<u>Tabelle 19: Inhalt eines Blocked User Policy Eintrags .....</u>	121
6682	<u>Tabelle 20: Legal Policy .....</u>	125
6683	<u>Tabelle 21: Legal Policy-EU-Zugriff .....</u>	128
6684	<u>Tabelle 22: Beschreibung der Kategorien .....</u>	130

6685	<u>Tabelle 23: Constraint Management Protokollierung.....</u>	134
6686	<u>Tabelle 24: Inhalt eines General-Deny-Policy-Eintrags .....</u>	136
6687	<u>Tabelle 25: Verbergen eines Medical-Service.....</u>	137
6688	<u>Tabelle 26: Kennzeichnung von Optionalitäten .....</u>	150
6689	<u>Tabelle 27: Übersicht über gruppierte IHE-ITI-Akteure und Optionen an den</u>	
6690	<u>Außenschnittstellen des XDS-Document-Service .....</u>	151
6691	<u>Tabelle 28: Schnittstelle I-Document-Management .....</u>	163
6692	<u>Tabelle 29: Schnittstelle I-Document-Management-Insurant .....</u>	167
6693	<u>Tabelle 30: Festlegung Folder.entryUUID zu statischen Ordnern.....</u>	170
6694	<u>Tabelle 31: Nutzungsvorgaben für Metadatenattribute XDS .....</u>	173
6695	<u>Tabelle 32: Tab-LanguageCodes – Mindestanforderung an zu unterstützende Language</u>	
6696	<u>Codes .....</u>	191
6697	<u>Tabelle 33: Einsortierung Datenkategorien.....</u>	197
6698	<u>Tabelle 34: TAB-EPA-Sammlungstypen .....</u>	199
6699	<u>Tabelle 35: Auswirkungen bei Widerspruch gegen eine Funktion der ePA .....</u>	202
6700	<u>Tabelle 36: XDS-Document-Service-Protokollierung.....</u>	204
6701	<u>Tabelle 37: Patient-Information-Service-Protokollierung.....</u>	208
6702	<u>Tabelle 38: Medication-Service-Protokollierung .....</u>	210
6703	<u>Tabelle 39 : Inhaltliche Definitionen eines AuditEvent .....</u>	216
6704	<u>Tabelle 40 Befüllung AuditEvent .....</u>	217
6705	<u>Tabelle 41: Audit-Event-Service-Protokollierung.....</u>	223
6706	<u>Tabelle 42 Vorgaben AuditEvent für Datenexport an FDZ.....</u>	245
6707	<u>Tabelle 43: Übersicht der Schnittstellen des Aktensystems .....</u>	251
6708	<u>Tabelle 1: Tab Prüfung Signaturzertifikate Parameter Prüfung Signaturzertifikat .....</u>	22
6709	<u>Tabelle 2: Protokollierung der Migration der medizinischen Daten .....</u>	33
6710	<u>Tabelle 3: Protokollierung der Migration der Protokolldaten des Versicherten .....</u>	34
6711	<u>Tabelle 4: Zustandswechsel im Lebenszyklus eines Aktenkontos.....</u>	38
6712	<u>Tabelle 5 : Health Record Relocation Service Protokollierung.....</u>	48
6713	<u>Tabelle 6: Tab AS VAU Token Modul Rules -Prüfregeln VAU Token .....</u>	59
6714	<u>Tabelle 7: Überblick über die Regeln des Befugnisverifikations-Moduls .....</u>	65
6715	<u>Tabelle 8: Tab AS Entitlement Registration Rules - Regeln zur Registrierung von</u>	
6716	<u>Befugnissen.....</u>	67
6717	<u>Tabelle 9: Tab AS SDS-Key Rules Key Rules - Regeln zur Ableitung der</u>	
6718	<u>versichertenindividuellen Persistierungsschlüssel .....</u>	77
6719	<u>Tabelle 10: Widerspruchsfähige Funktionen der elektronischen Patientenakte .....</u>	99
6720	<u>Tabelle 11: Consent Decision Management Protokollierung - Widersprüche für Funktionen</u>	
6721	<u>der ePA .....</u>	101

6722	<u>Tabelle 12: Consent Decision Management Protokollierung - User Specific Deny Policy</u>	
6723	<u>Medication .....</u>	106
6724	<u>Tabelle 13: Inhalt einer Befugnis .....</u>	106
6725	<u>Tabelle 14: Befugnisse für berechnigte Nutzergruppen und Nutzer .....</u>	108
6726	<u>Tabelle 15: Befugnisse EU-Zugriff für berechnigte Nutzergruppen und Nutzer .....</u>	111
6727	<u>Tabelle 16: Entitlement Management Protokollierung .....</u>	112
6728	<u>Tabelle 17: Inhalt eines Blocked User Policy Eintrags .....</u>	121
6729	<u>Tabelle 18: Legal Policy .....</u>	125
6730	<u>Tabelle 19: Legal Policy - EU-Zugriff .....</u>	128
6731	<u>Tabelle 20: Beschreibung der Kategorien .....</u>	130
6732	<u>Tabelle 21: Constraint Management Protokollierung .....</u>	134
6733	<u>Tabelle 22: Inhalt eines General Deny Policy Eintrags .....</u>	136
6734	<u>Tabelle 23: Verbergen eines Medical Service .....</u>	137
6735	<u>Tabelle 24: Kennzeichnung von Optionalitäten .....</u>	150
6736	<u>Tabelle 25: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den</u>	
6737	<u>Außenschnittstellen des XDS Document Service .....</u>	151
6738	<u>Tabelle 26: Schnittstelle I Document Management .....</u>	163
6739	<u>Tabelle 27: Schnittstelle I Document Management Insurant .....</u>	167
6740	<u>Tabelle 28: Schnittstelle I Document Management Ncpeh .....</u>	169
6741	<u>Tabelle 29: Festlegung Folder.entryUUID zu statischen Ordnern .....</u>	170
6742	<u>Tabelle 30: Nutzungsvorgaben für Metadatenattribute XDS .....</u>	173
6743	<u>Tabelle 31: Tab LanguageCodes - Mindestanforderung an zu unterstützende Language</u>	
6744	<u>Codes .....</u>	191
6745	<u>Tabelle 32: Einsortierung Datenkategorien .....</u>	197
6746	<u>Tabelle 33: TAB EPA Sammlungstypen .....</u>	199
6747	<u>Tabelle 34: Auswirkungen bei Widerspruch gegen eine Funktion der ePA .....</u>	202
6748	<u>Tabelle 35: XDS Document Service Protokollierung .....</u>	204
6749	<u>Tabelle 36: Patient Information Service Protokollierung .....</u>	208
6750	<u>Tabelle 37: Medication Service Protokollierung .....</u>	210
6751	<u>Tabelle 38 : Inhaltliche Definitionen eines AuditEvent .....</u>	216
6752	<u>Tabelle 39 Befüllung AuditEvent .....</u>	217
6753	<u>Tabelle 40: Audit Event Service Protokollierung .....</u>	223
6754	<u>Tabelle 41: Übersicht der Schnittstellen des Aktensystems .....</u>	251
6755		

6756 **5.5 Referenzierte Dokumente**6757 **5.5.1 Dokumente der gematik**

6758 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument  
 6759 referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemKPT_ePAfuerAlle]	gematik: Grobkonzept der "ePA für alle"
[gemSpec_FdV_ePA]	gematik: Spezifikation ePA-Frontend des Versicherten
[gemSpec_IDP_Sek]	gematik: Spezifikation des sektoralen IDP (GesundheitsID)
[gemSpec_IDP_FD]	gematik: Spezifikation der Fachdienste der TI-Föderation
[gemSpec_IDP_Frontend]	gematik: Spezifikation der Frontendkomponenten für Fachdienste der TI-Föderation
[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform
[gemSpec_IG_ePA]	gematik: Implementation Guides für strukturierte Dokumente GitHub: GitHub: <a href="https://github.com/gematik/ePA-XDS-Document">https://github.com/gematik/ePA-XDS-Document</a> Path: src/implementation_guides
<del>[gemSpec_Voc_ePA]</del>	<del>gematik: Vocabulary ePA GitHub: <a href="https://github.com/gematik/ePA-XDS-Document">https://github.com/gematik/ePA-XDS-Document</a> Path: src/vocabulary</del>
<del>[gemSpec_EPAAuditEvent]</del>	<del>gematik: Datenstruktur für Audit-Protokolle im ePA-Aktensystem <a href="https://gematik.de/fhir/epa/StructureDefinition/epa-auditevent">https://gematik.de/fhir/epa/StructureDefinition/epa-auditevent</a></del>
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory



<del>{ValueSet-Speciality-Øth}[gemTerminology]</del>	<del>gematik: Value-Set für Berechtigungskategorien-Øth-codes</del> <del>GitHub: <a href="https://github.com/gematik/ePA-XDS-Document">https://github.com/gematik/ePA-XDS-Document</a></del> <del>Path: src/vocabulary/value-sets/vs-speciality-Øth.xml</del> <del>gematik: Terminologies for Telematics Infrastructure (TI)</del> <del>Simplifier: <a href="https://simplifier.net/packages/de.gematik.terminology/1.0.5">https://simplifier.net/packages/de.gematik.terminology/1.0.5</a></del>
<del>{ValueSet-Speciality-Med}</del>	<del>gematik: Value-Set für Berechtigungskategorien-med-codes</del> <del>GitHub: <a href="https://github.com/gematik/ePA-XDS-Document">https://github.com/gematik/ePA-XDS-Document</a></del> <del>Path: src/vocabulary/value-sets/vs-speciality-med.xml</del>
[I_Consent_Decision_Management]	gematik: I_Consent_Decision_Management REST-Schnittstell zum Management der Widersprüche zu Versorgungsprozessen GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Consent_Decision_Management.yaml
[I_Constraint_Management_Insurant]	gematik: I_Constraint_Management_Insurant.yaml REST-Schnittstelle zum Verbergen und Sichtbarmachen von Dokumenten GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Constraint_Management_Insurant.yaml
[I_Entitlement_Management]	gematik: I_Entitlement_Management REST-Schnittstelle zur Verwaltung von Befugnissen und Befugnisausschlüssen GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Entitlement_Management.yaml
[I_Entitlement_Management_EU]	gematik: I_Entitlement_Management_EU REST-Schnittstelle zur Verwaltung von Befugnissen EU-Zugriff GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Entitlement_Management_EU.yaml

[I_Device_Management_Insurant]	gematik: I_Device_Management_Insurant.yaml REST-Schnittstelle zur Geräteverwaltung GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Device_Management_Insurant.yaml
[I_Health_Record_Relocation_Service]	gematik: I_Health_Record_Relocation_Service REST-Schnittstelle zum Aktenumzug GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Health_Record_Relocation_Service.yaml
[I_Information_Service_Accounts]	Schnittstellenspezifikation Information Service für Betreiber GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Information_Service_Accounts.yaml
[I_Information_Service]	Schnittstellenspezifikation Information Service GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Information_Service.yaml
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung und impliziten Geräteregistrierung GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Authorization_Service.yaml
[IG_Audit_Event_Service]	gematik: FHIR Implementation Guide "Audit Event Service" Simplifier: <a href="https://simplifier.net/guide/audit-event-service?version=1.0.0">https://simplifier.net/guide/audit-event-service?version=1.0.0</a>
[I_Email_Management]	gematik: I_Email_Management REST-Schnittstelle zum Management von E-Mail-Adressen eines Versicherten GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Email_Management.yaml
[I_Tool_Convert_PDF_Insurant]	gematik: I_Tool_Convert_PDF_Insurant Schnittstelle für die PDF Formatkonvertierung GitHub: <a href="https://github.com/gematik/ePA-XDS-Document">https://github.com/gematik/ePA-XDS-Document</a> Path: src/openapi/I_Tool_Convert_PDF_Insurant.yaml

[XSDDocumentService]	gematik: XSDDocumentService.wsdl IHE-Schnittstelle des XSDDocumentService GitHub: <a href="https://github.com/gematik/ePA-XSD-Document">https://github.com/gematik/ePA-XSD-Document</a> Path: src/schema
[HealthRecordMigration]	gematik: ref-ePA-HealthRecordMigration Referenzimplementierung und Vorgaben für das Exportpaket bei einem Anbieterwechsel GitHub: <a href="https://github.com/gematik/ref-ePA-HealthRecordMigration">https://github.com/gematik/ref-ePA-HealthRecordMigration</a> Branch: ePA-3.1
[IG_Patient_Information_Service]	gematik: FHIR Implementation Guide "Patient Information Service" Simplifier: <a href="https://simplifier.net/guide/patient-information-service?version=1.0.0">https://simplifier.net/guide/patient-information-service?version=1.0.0</a>
[IG_Medication_Service]	gematik: FHIR Implementation Guide "Medication Service" Simplifier: <a href="https://simplifier.net/guide/medication-service?version=1.1.0">https://simplifier.net/guide/medication-service?version=1.1.0</a>
<del>[DataPseudonymization]</del>	<del>gematik: ePA-research Vorgaben zur Pseudonymisierung von Daten zur Sekundärnutzung GitHub: <a href="https://github.com/gematik/ePA-research">https://github.com/gematik/ePA-research</a> Path: docs/leitfaden_pseudonymisierung.md Branch: ePA-3.1</del>
<del>[I_Data_Submission_Service]</del>	<del>gematik: I_Data_Submission_Service Schnittstelle für den Abruf eines Datenpaketes FDZ GitHub: <a href="https://github.com/gematik/ePA-Basic">https://github.com/gematik/ePA-Basic</a> Path: src/openapi/I_Data_Submission_Service.yaml</del>

## 6760 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, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf</a>

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-RMU]	IHE International (2021): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.3 – Trial Implementation, <a href="https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf">https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf</a>
[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, <a href="https://profiles.ihe.net/ITI/TF/Volume1/">https://profiles.ihe.net/ITI/TF/Volume1/</a>
[IHE-ITI-TF2]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.0, <a href="https://profiles.ihe.net/ITI/TF/Volume2/">https://profiles.ihe.net/ITI/TF/Volume2/</a>
[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, <a href="https://profiles.ihe.net/ITI/TF/Volume3/">https://profiles.ihe.net/ITI/TF/Volume3/</a>
[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, <a href="https://mio.kbv.de/display/UH1X0X1">https://mio.kbv.de/display/UH1X0X1</a>
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, <a href="https://www.w3.org/TR/soap12-mtom/">https://www.w3.org/TR/soap12-mtom/</a>
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, <a href="https://datatracker.ietf.org/doc/html/rfc2119">https://datatracker.ietf.org/doc/html/rfc2119</a>
[RFC3339]	IETF (2002): Date and Time on the Internet: Timestamps, RFC 3339, <a href="https://datatracker.ietf.org/doc/html/rfc3339">https://datatracker.ietf.org/doc/html/rfc3339</a>
[RFC4122]	IETF (2005) A Universally Unique Identifier (UUID) URN Namespace, RFC 4122 <a href="https://datatracker.ietf.org/doc/html/rfc4122">https://datatracker.ietf.org/doc/html/rfc4122</a>

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC5246]	IETF (2008): The Transport Layer Security (TLS) Protocol Version 1.2 <a href="https://datatracker.ietf.org/doc/html/rfc5246">https://datatracker.ietf.org/doc/html/rfc5246</a>
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231, <a href="https://datatracker.ietf.org/doc/html/rfc7231">https://datatracker.ietf.org/doc/html/rfc7231</a>
[RFC7515]	IETF (2015): JSON Web Signature (JWS), RFC-7515 <a href="https://datatracker.ietf.org/doc/html/rfc7515">https://datatracker.ietf.org/doc/html/rfc7515</a>
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), <a href="https://www.w3.org/TR/soap12-part1/">https://www.w3.org/TR/soap12-part1/</a>
[WSA]	OASIS (2004): Web Services Addressing (WS-Addressing), <a href="https://www.w3.org/Submission/ws-addressing/">https://www.w3.org/Submission/ws-addressing/</a>
[WSIAP]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, <a href="http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html">http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html</a>
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), <a href="http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html">http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html</a>
[WSIBSP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, <a href="http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html">http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html</a>
[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), <a href="http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf">http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf</a>
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, <a href="http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/">http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/</a>
[XHTML]	W3C (2010): XHTML 1.1 - Module-based XHTML - Second Edition, <a href="https://www.w3.org/TR/xhtml1/">https://www.w3.org/TR/xhtml1/</a>

6761