

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Aktensystem ePA für alle

Version: 1.45.0 CC
Revision: 11777251183342
Stand: 28-0231.03.2025
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich Entwurf
Referenzierung: gemSpec_Aktensystem_ePAfueralle

Dokumenteninformationen

29

Dokumentinformationen

30

Änderungen zur Vorversion

31

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

32

33

34

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.01.2024		ePA für alle	gematik
1.1.0	28.03.2024		ePA für alle - Release 3.0.1	gematik
1.2.0	12.07.2024		ePA für alle - Release 3.0.2, Zuordnungen für Release E- Rezept 1.6.5	gematik
1.3.0	14.08.2024		ePA für alle - Release 3.1.0	gematik
1.4.0	28.02.2025		ePA für alle - Release 3.0.5	gematik
<u>1.5.0</u> <u>CC</u>	<u>31.03.2025</u>		<u>ePA für alle - Release 3.1.2</u>	<u>gematik</u>

Inhaltsverzeichnis

1 Einführung	199
1.1 Zielsetzung	205
1.2 Zielgruppe	208
1.3 Geltungsbereich	211
1.4 Abgrenzungen	212
1.5 Methodik	216
2 Übergreifende Festlegungen	218
2.1 Aktensystem und Service-Lokalisierung	221
2.2 Redundanz	222
2.3 Datenschutz und Sicherheit	222
2.4 Validierungsaktenkonto	227
2.5 Tracing in Nichtproduktivumgebungen	228
2.6 Benutzerführung	249
2.7 Useragent	249
2.8 Datenmigration	257
2.8.1 Herstellerspezifische Umsetzung der Datenmigration	257
2.8.2 Durchführung der Migration	259
2.8.3 Bereinigung von Registry und Repository im Zuge der Migration	31
2.8.4 Protokollierung der Migration	34
2.8.5 Weitere Datenanpassungen	36
2.9 Performance aus Anwendersicht	36
3 Funktionsmerkmale	38
3.1 Aktenkonto eines Versicherten (Health Record)	38
3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte	38
3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger	38
3.1.2 Lebenszyklus und Zustände eines Aktenkontos	39
3.1.3 Anlage eines neuen Aktenkontos	40
3.1.4 Löschen eines Aktenkontos	42
3.2 Health Record Relocation Service	43
3.2.1 Ablauf eines Aktenkontoumzugs	49
3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter	49
3.2.1.2 Start Transfer eines existierenden Aktenkontos	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

76	3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich	
77	oder derzeit nicht möglich	51
78	3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter	51
79	3.2.1.7.3 Nicht-erfolgter Download oder fehlende Rückmeldung durch den neuen	
80	Anbieter	52
81	3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter	53
82	3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM	
83	54
84	3.4 Befugnisverifikations-Modul	57
85	3.4.1 VAU-Token-Modul	59
86	3.4.2 Regeln des Befugnisverifikations-Moduls	66
87	3.5 Vertrauenswürdige Ausführungsumgebung (VAU)	85
88	3.5.1 Übergreifende VAU-Anforderungen	86
89	3.5.1.1 Schutz der Integrität der VAU	86
90	3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU	87
91	3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU	88
92	3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM	88
93	3.5.1.5 Logging und Monitoring	89
94	3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU	90
95	3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU ...	90
96	3.5.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-	
97	VAU	92
98	3.5.2.3 Konsistenz des Systemzustands	92
99	3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU	92
100	3.5.4 Zusätzliche Anforderungen an eine Service-VAU	93
101	3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU	96
102	3.6 User Session und Health Record Context	100
103	3.7 Consent Decision Management	101
104	3.7.1 Widersprüche für Funktionen der ePA	101
105	3.7.2 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny	
106	Policy Medication)	107
107	3.8 Entitlement Management	109
108	3.8.1 Initiale Befugnisse (static Entitlements)	116
109	3.8.2 Erstellen einer Befugnis durch Clients	118
110	3.8.2.1 Befugnisvergabe durch ein ePA-FdV	118
111	3.8.2.2 Befugnisvergabe durch ein Primärsystem	120
112	3.8.3 Löschen von Befugnissen	123
113	3.8.4 Befugnisausschluss (Blocked User Policy)	124
114	3.8.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)	126
115	3.9 Legal Policy	129
116	3.10 Constraint Management	136
117	3.10.1 Aktenkontoweites Verbergen (General Deny Policy)	140
118	3.10.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes	
119	141
120	3.11 Device Management	142
121	3.12 Medical Services	146
122	3.12.1 XDS Document Service	146
123	3.12.1.1 Formatprüfung beim Einstellen von Dokumenten	147

124	3.12.1.2 Anforderungen zur Validierung	150
125	3.12.1.3 Namensräume.....	151
126	3.12.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von	
127	Dokumenten.....	151
128	3.12.1.4.1 Anforderungen an IHE ITI-Akteure.....	151
129	3.12.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen	154
130	3.12.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen...	157
131	3.12.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen	169
132	3.12.1.5 Fehlerbehandlung in Schnittstellenoperationen.....	170
133	3.12.1.6 Schnittstellen im XDS Document Service	170
134	3.12.1.6.1 Schnittstelle I_Document_Management.....	171
135	3.12.1.6.2 Schnittstelle I_Document_Management_Insurant	174
136	3.12.1.6.3 Schnittstelle I_Document_Management_Ncpeh	176
137	3.12.1.7 Statische Metadaten	177
138	3.12.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten	179
139	3.12.1.8.1 Allgemeine Metadatenvorgaben	179
140	3.12.1.8.2 Metadaten der Dokumente und SubmissionSets	200
141	3.12.1.8.3 Metadaten für Datenkategorien	204
142	3.12.1.9 Strukturierte Dokumente.....	207
143	3.12.1.9.1 Sammlungstypen.....	207
144	3.12.1.9.2 Konfigurierbarkeit.....	209
145	3.12.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode	
146	210
147	3.12.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die	
148	Dokumente des Aktenkontos	211
149	3.12.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication	
150	Service durch eine spezifische LEI auf die Dokumente des Aktenkontos.....	212
151	3.12.1.13 Protokollierung von Zugriffen auf den XDS Document Service	212
152	3.12.1.14 Unterstützungsleistung für das ePA-FdV	215
153	3.12.2 FHIR Data Services.....	216
154	3.12.2.1 Medication Service.....	217
155	3.13 Audit Event Service	221
156	3.14 Information Service.....	229
157	3.14.1 Information Service	229
158	3.14.1.1 Informationen zu Widersprüchen (Consent Decisions)	229
159	3.14.1.2 Informationen zur Anwenderperformance (UX Performance)	229
160	3.14.2 Information Service – Account.....	230
161	3.15 Email Management	230
162	3.16 Zusätzliche Anforderungen an den Authorization Service.....	232
163	3.16.1 Anforderungen an den Authorization Service für die Authentisierung von	
164	Versicherten (FdV)	232
165	3.16.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B	
166	237
167	3.16.3 Anforderungen an den Authorization Service für die Authentisierung des E-	
168	Rezept-Fachdienstes.....	239
169	3.17 Anbindung Verzeichnisdienst FHIR-Directory.....	240

170	3.18 Access Gateway	240
171	3.18.1 Paketfilter	241
172	3.18.1.1 Funktion	241
173	3.18.1.2 Redundanz	242
174	3.18.1.3 Konfiguration	243
175	3.18.1.4 Adressierung	243
176	3.18.1.4.1 Access Gateway zum Transportnetz Internet	243
177	3.18.1.4.2 ePA Aktensystem zum Zentralen Netz	243
178	3.18.2 Proxy für das VAU-Protokoll	243
179	3.18.3 Proxy Schlüsselgenerierungsdienst	243
180	3.18.4 Tracing in Nichtproduktivumgebungen	244
181	3.18.5 Übergreifende Festlegungen	245
182	3.19 Schnittstellen (OpenAPI)	258
183	3.19.1 Übersicht der Schnittstellen des Aktensystems	259
184	3.19.2 Übergreifende Festlegungen zu den Schnittstellen	267
185	4 Informationsmodelle	268
186	5 Anhang A Verzeichnisse	269
187	5.1 Abkürzungen	269
188	5.2 Glossar	271
189	5.3 Abbildungsverzeichnis	271
190	5.4 Tabellenverzeichnis	271
191	5.5 Referenzierte Dokumente	274
192	5.5.1 Dokumente der gematik	274
193	5.5.2 Weitere Dokumente	278
194	1 Einführung	12
195	1.1 Zielsetzung	12
196	1.2 Zielgruppe	12
197	1.3 Geltungsbereich	12
198	1.4 Abgrenzungen	12
199	1.5 Methodik	13
200	2 Übergreifende Festlegungen	14
201	2.1 Aktensystem- und Service-Lokalisierung	15
202	2.2 Redundanz	17
203	2.3 Datenschutz und Sicherheit	18
204	2.4 Validierungsaktenkonto	23
205	2.5 Tracing in Nichtproduktivumgebungen	26
206	2.6 Benutzerführung	27
207	2.7 Useragent	28
208	2.8 Performance aus Anwendersicht	36

3 Funktionsmerkmale	38
3.1 Aktenkonto eines Versicherten (Health Record)	38
3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte.....	38
3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger.....	38
3.1.2 Lebenszyklus und Zustände eines Aktenkontos	39
3.1.3 Anlage eines neuen Aktenkontos	40
3.1.4 Löschen eines Aktenkontos	42
3.2 Health Record Relocation Service	43
3.2.1 Ablauf eines Aktenkontoumzugs.....	49
3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter.....	49
3.2.1.2 Start Transfer eines existierenden Aktenkontos.....	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
3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich oder derzeit nicht möglich	51
3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter.....	51
3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter.....	52
3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter	53
3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM	54
3.4 Befugnisverifikations-Modul	57
3.4.1 VAU-Token-Modul	59
3.4.2 Regeln des Befugnisverifikations-Moduls	66
3.5 Vertrauenswürdige Ausführungsumgebung (VAU)	85
3.5.1 Übergreifende VAU-Anforderungen	86
3.5.1.1 Schutz der Integrität der VAU	86
3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU	87
3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU.....	88
3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM.....	88
3.5.1.5 Logging und Monitoring.....	89
3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU.....	90
3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU ...	90
3.5.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-VAU.....	92
3.5.2.3 Konsistenz des Systemzustands	92
3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU.....	92
3.5.4 Zusätzliche Anforderungen an eine Service-VAU	93
3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU.....	96
3.6 Umschlüsselung und Überschlüsselung	96
3.7 User Session und Health Record Context.....	100
3.8 Consent Decision Management.....	101
3.8.1 Widersprüche für Funktionen der ePA	101

258	<u>3.8.2 Einschränkung der Verwendung von Daten auf bestimmte</u>	
259	<u>Sekundärnutzungszwecke</u>	105
260	<u>3.8.3 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny</u>	
261	<u>Policy Medication).....</u>	107
262	<u>3.9 Entitlement Management.....</u>	109
263	<u>3.9.1 Initiale Befugnisse (static Entitlements)</u>	116
264	<u>3.9.2 Erstellen einer Befugnis durch Clients</u>	118
265	<u>3.9.2.1 Befugnisvergabe durch ein ePA-FdV.....</u>	118
266	<u>3.9.2.2 Befugnisvergabe durch ein Primärsystem</u>	120
267	<u>3.9.3 Löschen von Befugnissen</u>	123
268	<u>3.9.4 Befugnisausschluss (Blocked User Policy)</u>	124
269	<u>3.9.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)</u>	126
270	<u>3.10 Legal Policy</u>	129
271	<u>3.11 Constraint Management.....</u>	136
272	<u>3.11.1 Aktenkontoweites Verbergen (General Deny Policy)</u>	140
273	<u>3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes</u>	
274	<u>.....</u>	141
275	<u>3.12 Device Management</u>	142
276	<u>3.13 Medical Services</u>	146
277	<u>3.13.1 XDS Document Service</u>	146
278	<u>3.13.1.1 Formatprüfung beim Einstellen von Dokumenten</u>	147
279	<u>3.13.1.2 Anforderungen zur Validierung</u>	150
280	<u>3.13.1.3 Namensräume.....</u>	151
281	<u>3.13.1.4 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von</u>	
282	<u>Dokumenten.....</u>	151
283	<u>3.13.1.4.1 Anforderungen an IHE ITI-Akteure.....</u>	151
284	<u>3.13.1.4.2 Überblick über gruppierte IHE ITI-Akteure und Optionen</u>	154
285	<u>3.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen ...</u>	157
286	<u>3.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen</u>	169
287	<u>3.13.1.5 Fehlerbehandlung in Schnittstellenoperationen.....</u>	170
288	<u>3.13.1.6 Schnittstellen im XDS Document Service</u>	170
289	<u>3.13.1.6.1 Schnittstelle I Document Management.....</u>	171
290	<u>3.13.1.6.2 Schnittstelle I Document Management Insurant</u>	174
291	<u>3.13.1.6.3 Schnittstelle I Document Management Ncpeh</u>	176
292	<u>3.13.1.7 Statische Metadaten</u>	177
293	<u>3.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten.....</u>	179
294	<u>3.13.1.8.1 Allgemeine Metadatenvorgaben</u>	179
295	<u>3.13.1.8.2 Metadaten der Dokumente und SubmissionSets</u>	200
296	<u>3.13.1.8.3 Metadaten für Datenkategorien</u>	204
297	<u>3.13.1.8.4 Datenmigration</u>	206
298	<u>3.13.1.9 Strukturierte Dokumente.....</u>	207
299	<u>3.13.1.9.1 Sammlungstypen.....</u>	207
300	<u>3.13.1.9.2 Konfigurierbarkeit.....</u>	209
301	<u>3.13.1.9.3 Verarbeitungsvorgaben für spezifische Dokumente</u>	210

302	<u>3.13.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode</u>	
303	210
304	<u>3.13.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die</u>	
305	<u>Dokumente des Aktenkontos</u>	211
306	<u>3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication</u>	
307	<u>Service durch eine spezifische LEI auf die Dokumente des Aktenkontos.....</u>	212
308	<u>3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service</u>	212
309	<u>3.13.1.14 Unterstützungsleistung für das ePA-FdV</u>	215
310	<u>3.13.2 FHIR Data Services.....</u>	216
311	<u>3.13.2.1 Patient Service.....</u>	216
312	<u>3.13.2.2 Medication Service.....</u>	217
313	<u>3.13.2.3 MHD Service</u>	220
314	<u>3.14 Audit Event Service</u>	221
315	<u>3.15 Information Service.....</u>	229
316	<u>3.15.1 Information Service</u>	229
317	<u>3.15.1.1 Informationen zu Widersprüchen (Consent Decisions)</u>	229
318	<u>3.15.1.2 Informationen zur Anwenderperformance (UX Performance)</u>	229
319	<u>3.15.2 Information Service - Account.....</u>	230
320	<u>3.16 Email Management</u>	230
321	<u>3.17 Zusätzliche Anforderungen an den Authorization Service.....</u>	232
322	<u>3.17.1 Anforderungen an den Authorization Service für die Authentisierung von</u>	
323	<u>Versicherten (FdV)</u>	232
324	<u>3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B</u>	
325	<u>.....</u>	237
326	<u>3.17.3 Anforderungen an den Authorization Service für die Authentisierung des E-</u>	
327	<u>Rezept-Fachdienstes</u>	239
328	<u>3.18 Anbindung Verzeichnisdienst FHIR-Directory</u>	240
329	<u>3.19 Access Gateway</u>	240
330	<u>3.19.1 Paketfilter</u>	241
331	<u>3.19.1.1 Funktion.....</u>	241
332	<u>3.19.1.2 Redundanz</u>	242
333	<u>3.19.1.3 Konfiguration</u>	243
334	<u>3.19.1.4 Adressierung.....</u>	243
335	<u>3.19.1.4.1 Access Gateway zum Transportnetz Internet.....</u>	243
336	<u>3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz.....</u>	243
337	<u>3.19.2 Proxy für das VAU-Protokoll.....</u>	243
338	<u>3.19.3 Proxy Schlüsselgenerierungsdienst</u>	243
339	<u>3.19.4 Tracing in Nichtproduktivumgebungen</u>	244
340	<u>3.19.5 Übergreifende Festlegungen</u>	245
341	<u>3.20 Data Submission Service</u>	246
342	<u>3.20.1 Erstellung von Arbeitsnummern und Lieferpseudonymen</u>	247
343	<u>3.20.2 Auswahl von medizinischen Daten</u>	248
344	<u>3.20.3 Protokollierung des Datenexports an das FDZ</u>	249
345	<u>3.20.4 Pseudonymisierung von medizinischen Daten.....</u>	249
346	<u>3.20.5 Übermittlung der pseudonymisierten medizinischen Daten</u>	250
347	<u>3.21 Push Notification Management</u>	252
348	<u>3.21.1 Push Notification Management des ePA-Aktensystems</u>	253
349	<u>3.21.2 Registrierung eines ePA-FdV als Pusher.....</u>	253
350	<u>3.21.3 Push Notification Channels</u>	254

351	3.21.4 Push Notification Nachrichteninhalte	255
352	3.21.5 Versenden von Push Nachrichten.....	256
353	3.21.6 Protokollierung.....	256
354	3.22 Schnittstellen (OpenAPI).....	258
355	3.22.1 Übersicht der Schnittstellen des Aktensystems	259
356	3.22.2 Übergreifende Festlegungen zu den Schnittstellen	267
357	4 Informationsmodelle	268
358	5 Anhang A – Verzeichnisse	269
359	5.1 Abkürzungen	269
360	5.2 Glossar	271
361	5.3 Abbildungsverzeichnis.....	271
362	5.4 Tabellenverzeichnis	271
363	5.5 Referenzierte Dokumente.....	274
364	5.5.1 Dokumente der gematik.....	274
365	5.5.2 Weitere Dokumente.....	278
366	6 Anhang B – Erläuternde Informationen	281
367	6.1 Dokumentenanhänge.....	281
368	6.2 Überblick	281
369	6.3 Löschen und Verbergen in Anhangsketten.....	282
370	6.4 Ungültige Anhänge	284
371	6.4.1 Verweiszirkel und doppelte Eltern.....	284
372	6.4.2 Anhangskette zu lang	285
373		

1 Einführung

1.1 Zielsetzung

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

1.2 Zielgruppe

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

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

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

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

405 1.5 Methodik

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

410
411 **<AFO-ID> - <Titel der Afo>**
412 Text / Beschreibung
413 [**<=**]

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

2 Übergreifende Festlegungen

416

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

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

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

427 **A_25149-01 - ePA-Aktensystem - Rollentrennung ePA-Aktensystem und** 428 **sektoraler IDP**

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

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

436 Das ePA-Aktensystem MUSS die Systemzeit über den Zeitdienst in der TI
437 gemäß [gemSpec_Net#6.2] synchronisieren
438 [\leq]

439 **A_25612 - ePA-Aktensystem - Authentisierung gegenüber einem Client** 440 **innerhalb der TI**

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

443

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

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

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

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

454 Die Formatvorgaben zum Useragent sind in A_22470* definiert.

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

456 Das ePA-Aktensystem MUSS sicherstellen, dass ePA-Clients in der Kommunikation mit
457 den Medical Services der ePA innerhalb des VAU-Kanals ein HTTP Header Element mit
458 dem Namen "x-insurantId" gesendet wird und andernfalls den Request mit HTTP-Fehler
459 400 ablehnen. [\leq]

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

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

467 **A_27443 - Nutzung Terminologiepaket**

468 Das ePA-Aktensystem MUSS die relevanten Terminologien des Terminologiepakets
 469 gemäß [\[gemTerminologyIG TI Terminology\]](#) verarbeiten und in der Kommunikation mit
 470 dem ePA-Aktensystem berücksichtigen. [**<=**]

471 Hinweis zu A_27443:

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

474 **2.1 Aktensystem- und Service-Lokalisierung**

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

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

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

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

491 **A_24592-02 - Anbieter ePA-Aktensystem -Registrierung an übergreifender ePA- 492 Domäne**

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

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

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

503 [**<=**]

504

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

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

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

508

509 Beispiele der Dienstlokalisierung

510 PU :

511 Aktensystem A

512

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

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

515 ...

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

517

518 Aktensystem B

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

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

521

522 TU :

523 Aktensystem 1

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

525 ...

526

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

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

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

534 [\leq]

535 A_22688-03 - Anbieter ePA-Aktensystem, Konfiguration Schnittstellen über 536 /.well-known/

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

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

543

544

545 {
"version" : "<Produkttypversion des Aktensystems im Format[0-


```

546 9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}>",
547     "sgd1"   : "<pfad_Schlüsselgenerierungsdienst_typ1>",
548     "sgd2"   : "<pfad_Schlüsselgenerierungsdienst_typ2>",
549     ....
550 }[<=]

```

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

554 **A_26814 - ePA-Aktensystem - Schnittstellenadressierung**
 555 Das ePA-Aktensystem MUSS die Schnittstellenadressierung (relative Pfade) gemäß der
 556 Schnittstellenspezifikationen umsetzen. [\leq]

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

563 **A_24801 - Aktensystem, Liste von FQDN im Internet**
 564 Das ePA-Aktensystem MUSS dem ePA-FdV eine Liste aller Kostenträger und der FQDN,
 565 unter der deren ePA-Aktensystem im Internet erreichbar ist, bereitstellen. Die Liste setzt
 566 sich zusammen aus den selbst verwalteten Kostenträgern und den über
 567 I_Information_Service_Accounts bezogenen Teillisten der anderen ePA-
 568 Aktensysteme. [\leq]

569 2.2 Redundanz

~~570 Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf]. Die~~
~~571 Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der~~
~~572 Komponenten des ePA-Aktensystems. In diesem Dokument werden zusätzliche~~
~~573 Redundanzanforderungen spezifiziert, wenn die Anforderungen in [gemSpec_Perf] zur~~
~~574 Verfügbarkeit nicht ausreichen.~~

~~575 Die Auswahl und der Zugriff auf Services des ePA-Aktensystems wird durch die~~
~~576 Primärsysteme anhand definierter FQDNs vorgenommen [siehe Kapitel 2.1]. Auf die~~
~~577 Auswahl der Services des ePA-Aktensystems kann der Anbieter des ePA-Aktensystems~~
~~578 durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die~~
~~579 Verfügbarkeit ist hergestellt, wenn jedes Primärsystem oder andere Fachdienste (z.B. E-~~
~~580 Rezept-Fachdienst, ein anderes ePA-Aktensystem, ...) die Möglichkeit haben, die Services~~
~~581 des ePA-Aktensystems zu erreichen. Von der Versichertenseite aus erfolgt der Zugriff auf~~
~~582 die Komponenten des ePA-Aktensystems durch das ePA-Frontend des Versicherten.~~

~~583 Eine hardwaretechnische Hochverfügbarkeit der einzelnen Komponenten des ePA-~~
~~584 Aktensystems ist über grundlegende Maßnahmen wie redundante Netzteile hinaus nicht~~
~~585 erforderlich. Es steht dem Anbieter jedoch frei, zur Sicherstellung der~~
~~586 Verfügbarkeitsanforderungen technische Lösungen, wie z. B. Load-Balancer und Stateful~~
~~587 Failover innerhalb von Clustern einzusetzen, so dass jede einzelne Komponente des ePA-~~
~~588 Aktensystems im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.~~

~~589 **A_14921—Anbieter ePA-Aktensystem—lokale Redundanz im Standort des ePA-**~~
~~590 **Aktensystems**~~

~~591 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass bei Ausfall einer oder~~
~~592 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. [≤]~~

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

2.3 Datenschutz und Sicherheit

A_15128 - Anbieter ePA-Aktensystem - Schutz der transportierten Daten im ePA-Aktensystem

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

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

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

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

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

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

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

A_15104 - Anbieter ePA-Aktensystem - Ordnungsgemäße IT-Administration

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

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

A_15824 - Anbieter ePA-Aktensystem - Sichere Speicherung von Daten

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

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

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

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

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

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

A_15119 - Anbieter ePA-Aktensystem - Löschkonzept

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

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

[\leq]

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

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

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

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

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

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

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

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

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

A_24778 - Anbieter ePA-Aktensystem - Einsatz zertifizierter HSM

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

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

entsprechen. [\leq]

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

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

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

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

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

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

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

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

A_15163 - Anbieter ePA-Aktensystem - Angriffen entgegenwirken

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

729 **A_15167 - Anbieter ePA-Aktensystem - Social Engineering Angriffen**
730 **entgegenwirken**

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

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

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

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

739 Die Komponenten des ePA-Aktensystems DÜRFEN dynamischen Inhalt von Drittanbietern
740 NICHT herunterladen und verwenden.
741 [≤]

742 **A_17080 - Verhindern von Session Hijacking**

743 Die Komponenten des ePA-Aktensystems MÜSSEN geeignete Schutzmaßnahmen gegen
744 Session-Hijacking implementieren.
745 [≤]

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

747 Der Anbieter des ePA-Aktensystems MUSS der Ablage von Dokumenten, die für die
748 medizinische Versorgung oder für die Eigenorganisation medizinischer Belange des
749 Versicherten oder zur Erstattung der Behandlungskosten irrelevant sind, mittels AGB auf
750 Anbieterseite entgegenwirken.
751 [≤]

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

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

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

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

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

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

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

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

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

771 Das ePA-Aktensystem MUSS das private Schlüsselmaterial der Ausstelleridentität
772 ID.FD.SIG für die Signatur von Listen von Protokollen des Versicherten in einem HSM
773 speichern.
774 [≤]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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

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

A_25006 - ePA-Aktensystem - User Session bei Inaktivität Beenden

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

A_25022 - ePA-Aktensystem - Debug-Protokoll für Testbetrieb

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

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

A_25023 - ePA-Aktensystem - Keine Echtdaten im Testbetrieb

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

A_25042 - ePA-Aktensystem - Prüfung von Signaturen

Das ePA-Aktensystem MUSS bei der Prüfung von Signaturen

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

[\leq]

A_25040-01 - ePA-Aktensystem - Prüfung Signaturzertifikate

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

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

Parameter	C.FD.SIG	C.CH.SIG	C.HCI.OSIG	C.HCI.AUT
PolicyList	oid_fd_sig	oid_egk_sig	oid_smc_b_osig	oid_smc_b_aut
intendedKeyUsage	digitalSignatur e	nonRepudiati on	nonRepudiatio n	digitalSignatu re
intendedExtendedKeyUs age	(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

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

824 **A 27498 - Anbieter ePA-Aktensystem - Offline-Datensicherung**

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

827 **A 27497 - Anbieter ePA-Aktensystem - Rollenkonzept zum Schutz der** 828 **permanenten Verfügbarkeit von Aktenkonten**

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

835 **A 27499 - Anbieter ePA-Aktensystem - HSM-Backups im 4-Augen-Prinzip**

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

839 **A 27500 - Anbieter ePA-Aktensystem - Rollentrennung Administratoren für** 840 **Backup- und Produktionsdaten**

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

845 **2.4 Validierungsaktenkonto**

846 Die Architektur des ePA-Aktensystems verhindert eine Einsichtnahme des Betreibers in
 847 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 Validierungskonten, für die die Regelung gem. A_22684-* gilt [Validierungskonten im StoreReview der FdVs], MÜSSEN folgende Besonderheiten berücksichtigt werden:

- die entsprechenden Validierungskonten dürfen nur für den Zeitpunkt des Reviews aktiviert und erreichbar sein,
- die entsprechenden Validierungskonten sind unmittelbar nach dem Review zu leeren,

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

[<=]

A_26209 - Prüfung auf Vertretungsberechtigung für Prüfidentität

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

A_24539 - Nutzung von Validierungsaktenkonten via FdV

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

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

2.5 Tracing in Nichtproduktivumgebungen

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

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

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

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

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

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

987 diesem TCP-Port verbindet, MUSS er die aktuell auf dem Interface durchlaufenden Daten
988 gestreamt lesen können.
989 [\leq]

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

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

994 **A_22581 - Tracing, Abschaltbarkeit**

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

998 *Hinweis: Die Aktivier- bzw. Deaktivierbarkeit nach A_22581-* kann dabei auch teilweise*
999 *mit organisatorische Maßnahmen umgesetzt werden, d. h. es ist hier **kein***
1000 *vollautomatisierter Mechanismus notwendig, der im Millisekunden-Bereich umschalten*
1001 *kann.*

1002 **2.6 Benutzerführung**

1003 Bietet der Anbieter des ePA-Aktensystems dem Versicherten die Aktenkontoeröffnung,
1004 die Änderung von Vertragsdaten und die Aktenkontoschließung auf einem elektronischen
1005 Weg an, dann muss die Bedienung für den Nutzer intuitiv gestaltet werden.

1006 **A_15842 - Anbieter ePA-Aktensystem - Ergonomie der Benutzerführung**

1007 Der Anbieter des ePA-Aktensystems MUSS eine ergonomisch
1008 gestaltete Benutzerführung nach den Vorgaben zur Ergonomie in [DIN EN ISO 9241-171]
1009 anbieten. [\leq]

1010 **DIN-Normen und Verordnungen zur Beachtung:**

1011 Zusätzlich zu den in diesem Kapitel aufgeführten Anforderungen zur Benutzerführung
1012 sollen auch die in der ISO 9241 aufgeführten Qualitätsrichtlinien zur Sicherstellung der
1013 Ergonomie interaktiver Systeme und Anforderungen aus der Verordnung zur Schaffung
1014 barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz
1015 (Barrierefreie-Informationstechnik-Verordnung – BITV 2.0) beachtet werden.

1016 Insbesondere soll der Fokus auf die nachfolgend aufgeführten Teile der ISO 9241
1017 gerichtet sein:

1018 **DIN EN ISO 9241 – Teile mit Bezug zur Software-Ergonomie**

- 1019 • Teil 8: Anforderungen an Farbdarstellungen
- 1020 • Teil 9: Anforderungen an Eingabegeräte – außer Tastaturen
- 1021 • Teil 110: Grundsätze der Dialoggestaltung (ersetzt den bisherigen Teil 10)
- 1022 • Teil 11: Anforderungen an die Gebrauchstauglichkeit – Leitsätze
- 1023 • Teil 12: Informationsdarstellung
- 1024 • Teil 13: Benutzerführung
- 1025 • Teil 14: Dialogführung mittels Menüs
- 1026 • Teil 15: Dialogführung mittels Kommandosprachen
- 1027 • Teil 16: Dialogführung mittels direkter Manipulation
- 1028 • Teil 17: Dialogführung mittels Bildschirmformularen

- Teil 171: Leitlinien für die Zugänglichkeit von Software BITV 2.0

1030 **BITV 2.0 - Barrierefreie Informationstechnik-Verordnung**

1031 Die Umsetzung der Verordnung dient zur behindertengerechten Umsetzung
1032 von Webseiten und anderen grafischen Oberflächen.

1033 Insbesondere sollen deshalb neben der Übernahme der international anerkannten
1034 Standards für barrierefreie Webinhalte, die Web Content Accessibility Guidelines (WCAG)
1035 2.1, auch die Belange gehörloser, hör-, lern- und geistig behinderter Menschen
1036 berücksichtigt werden.

1037 Die BITV 2.0 regelt unter anderem den sachlichen Geltungsbereich, die einzubeziehenden
1038 Gruppen behinderter Menschen und die anzuwendenden Standards.

1039 Weitere Richtlinien und Empfehlungen zur digitalen Barrierefreiheit sind die EU-Richtlinie
1040 2016/2102 für öffentliche Stellen und die europäische Norm EN 301 549 V2.1.2 mit dem
1041 Titel "Accessibility requirements for ICT products and services".

1042 **A_15846 - Anbieter ePA-Aktensystem - Schnittstellen für die Unterstützung der 1043 barrierefreien Bedienungsmöglichkeit**

1044 Der Anbieter des ePA-Aktensystems SOLL die Schnittstellen für die Unterstützung der
1045 barrierefreien Bedienungsmöglichkeit, welche vom Betriebssystem zur Verfügung gestellt
1046 werden, unterstützen.[<=]

1047 **2.7 Useragent**

1048 **A_22470-06 - Definition x-useragent**

1049 Das Produkt MUSS für das x-useragent-Element in Eingangs- oder Ausgangsparametern
1050 einer Operation folgende Formatvorgaben berücksichtigen:

- der Useragent umfasst 2 Informationen, welche als 1 String - getrennt durch "/"
1052 (Slash) - im Header übertragen werden
- erster Teil: Client-ID = ein bis zu 20 Zeichen langer String (a-z A-Z 0-9, "-"),
1054 welcher im Rahmen der Produktregistrierung bei der gematik erzeugt wird,
- zweiter Teil: Versionsnummer = bis zu 15 Zeichen langer String (a-z A-Z 0-9,
1056 "-", ".") welcher die aktuelle Produktversion des Clients repräsentiert.

1057 Beispiel: "CLIENTID1234567890AB/2.1.12-45"

1058 Hinweis: gem. RFC7231 ist im http-Header ein Useragent einzutragen. Dieser RFC-
1059 Useragent enthält z.B. Angaben zum Betriebssystem oder zum Browser und ist nicht zu
1060 verwechseln mit dem hier definierten x-useragent. Dieser (x-useragent) muss deshalb im
1061 x-useragent-Parameter des http-Headers eingetragen werden, NICHT im Useragent-
1062 Parameter gem. RFC7231. Ein Beispiel für die Verwendung bieten die OpenAPI-
1063 Spezifikationen der fachlichen Aktensystem-Operationen.[<=]

1064 *Hinweis zum Erhalt der Client-ID: die Client-ID wird durch die gematik vergeben und*
1065 *übermittelt, sobald sich ein (Client-)Produkthersteller (z.B. FdV oder Primärsystem) unter*
1066 *idp-registrierung@gematik.de registriert hat. Dazu ist im Rahmen dieser Registrierung*
1067 *der Name des Herstellers und der Name des zu registrierenden Produktes zu übermitteln.*
1068 *Sollte im Rahmen einer anderen TI-Anwendung bereits eine Registrierung vorgenommen*
1069 *worden sein, kann die Client-ID auch im ePA-Kontext genutzt werden (sofern es sich um*
1070 *das gleiche Softwareprodukt handelt).*

1071 *Hinweis für FdV-Hersteller: Bei Entwicklung eines White-Label-Clients ist der Useragent*
1072 *Teil des kundenspezifischen Customizings, sodass über die Client-ID im Useragent das*
1073 *spezifische Kostenträger-ePA-FdV erkennbar sein muss.*

2.8 Datenmigration

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

Für die Migration eines existierenden Aktenkontos der Version ePA 2.x wird vorausgesetzt, dass ein migriertes Aktenkonto sowohl die Schnittstellen der ePA für alle, als auch die Schnittstellen der bisherigen ePA-Version 2.x bereitstellt und simultan verarbeiten kann.

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

Aus einem existierenden Aktenkonto werden die folgenden Artefakte übernommen:

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

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

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

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

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

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

2.8.1 Herstellerspezifische Umsetzung der Datenmigration

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

~~A_24995—Migration: Sicherheitskonzept für Datenmigration~~

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

~~A_25000—Migration: Stärke der Sicherheitsmaßnahmen für Datenmigration~~

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

~~A_25049—Migration: Migrationskonzept~~

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

~~2.8.2 Durchführung der Migration~~

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

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

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

~~A_25148—Migration: Information des Versicherten~~

~~Der Anbieter des ePA-Aktensystems MUSS den Versicherten über die Notwendigkeit und die Folgen einer Migration vor der eigentlichen Migration informieren, insbesondere darüber, welche Dokumentenformate und welche Berechtigungen übernommen und welche nicht übernommen werden, über die Freiwilligkeit einer Migration. [<=]~~

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

~~A_24922—Migration: Schnittstellen zur Durchführung der Migration~~

~~Das ePA-Aktensystem MUSS für jedes Aktenkonto eine Migration von ePA 2.6 auf ePA 3.0 durchführen und geeignete Schnittstellen zum FdV anbieten, mit denen der Versicherte vom FdV das Entschlüsseln der verschlüsselten ePA 2.6-Akteninhalte anstoßen kann. [<=]~~

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

2.8.3 Bereinigung von Registry und Repository im Zuge der Migration

~~A_24964—XDS Document Service—Migration: Isolation der Migration~~

~~Der XDS Document Service MUSS die Verarbeitung von entschlüsselten Dokumenten, die im Rahmen der Migration durchgeführt werden, so technisch isolieren, dass kein Schaden für Aktenkonten oder das ePA-Aktensystem selbst entsteht. [<=]~~

~~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.~~

~~[<=]~~

~~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".

Die Kinderuntersuchungshefte werden nicht migriert und verbleiben im Ordner `childsrecord`.

A_24963—XDS Document Service—Migration: Keine Übernahme von Dokumenten mit unzulässigem Format

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 sämtliche Dokumente der ePA2.6 gemäß A_24864 * auf die zulässigen Dokumentenformate prüfen und Dokumente in einem nicht erlaubten Format nicht in die "ePA für alle" migrieren. [\leq]

*Hinweis zu A_24963 *: Für die Migration von Dokumenten der ePA2.6 auf ePA3.0 sind bei der Prüfung auf zulässige Dokumentenformate die Hinweise zu A_24864 * und A_25009 * zu berücksichtigen.*

A_24966—XDS Document Service—Migration: Konvertieren von PDF in PDF/A-Dokumente

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

A_25032—XDS Document Service—Migration: Information des Versicherten zur Nichtübernahme von Dokumenten in bestimmten Formaten

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

A_24520—XDS Document Service—Migration: Prüfsumme Dokument erzeugen

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

A_24847—XDS Document Service—Migration: Identifizieren und Auflösen von Dokumenten-Dubletten

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

A_24851—XDS Document Service—Migration: Dokumente und Ordner mergen

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf die ePA 3.0 zum Zeitpunkt der Entschlüsselung des Datenbestands die Ordnerinhalte einer Kategorie vergleichen, falls es neben den migrierten ePA 2.6-Akteninhalten durch eine ePA3-Aktenutzung ebenfalls Ordnerinhalte gibt. Unter Berücksichtigung der Dublettenprüfung werden alle Dokumente von zwei Ordnern derselben Kategorie (in ePA 2.6 bzw. 3.0 entstanden) in einen Ordner zusammengeführt. Dokumente und RPLC-Ketten, die durch

die `documentEntry.uniqueId` erkennbar zusammen gehören, werden unter Wahrung der Abfolge der Einstelldaten zusammengeführt und das jüngste Dokument als aktives Dokument der Kette behandelt. Dokumente erhalten eine `rootDocumentUniqueId` gemäß A_24451*, falls noch nicht vorhanden. [\leq]

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.

[\leq]

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> ohne Extension

[\leq]

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. [\leq]

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. [\leq]

A_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 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')~~
~~[<=]~~

2.8.4 Protokollierung der Migration

A_25029-01 XDS Document Service Protokollierung der Migration der medizinischen Daten

Der XDS Document Service MUSS den Vorgang der Migration der medizinischen Daten (Dokumente, Folder, Metadaten) 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 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"	

Strukturelement	Wert		Erläuterung
AuditEvent.entity.description	<Hinweistext>		
AuditEvent.source.type.code	"XDSSVC"		
AuditEvent.entity.detail	type	value[x]	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-ITI-TF3].
	"DocumentMimeType"	<DocumentEntry.mimeType>	

[<=]

A_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"	

Strukturelement	Wert	Erläuterung
<code>AuditEvent.action</code>	E	
<code>AuditEvent.source.type.code</code>	"AUDITSVC"	
<code>AuditEvent.entity.name</code>	"MigrationProtocol"	
<code>AuditEvent.entity.description</code>	<Hinweistext>	dieses Strukturelement ist nur zu versorgen, wenn bei der Migration Fehler aufgetreten sind

[<=]

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.~~

~~[<=]~~

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

2.92.8 Performance aus Anwendersicht

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

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

1350 Die Übermittlung der Messdaten erfolgt im Anschluss an den erfolgreichen Abschluss des
 1351 Anwendungsfalles an das gleiche Aktensystem (unter Verwendung der Schnittstelle
 1352 InformationService.setUserExperienceResult), bei dem auch der Anwendungsfall
 1353 stattgefunden hat. Hierbei ist die Schnittstelle zur Lieferung der Messdaten an der
 1354 Komponente "Information Service" nur für Primärsysteme normiert. Es steht dem
 1355 Hersteller des Aktensystems frei, die Lieferschnittstelle für Messdaten von FdVs selbst
 1356 oder nach dem Vorbild der PS-Schnittstelle zu implementieren.

1357 Die eingegangenen Messergebnisse werden vom Aktensystem verarbeitet und
 1358 anschließend gemäß der Vorgaben aus [gemSpec_Perf] an die Betriebsdatenerfassung
 1359 der gematik im Rahmen der Rohdatenlieferung übermittelt.

1360

1361 **A_24570-01 - Verarbeitung von UX-Messdaten**

1362 Das ePA-Aktensystem MUSS für die im zu betrachtenden Zeitintervall der
 1363 Betriebsdatenlieferung (gemäß [gemSpec_Perf]) eingegangenen Messdaten je UX-
 1364 Usecase, je Client-ID und je Client-Version folgende Werte ermitteln und gemäß
 1365 [gemSpec_Perf] übermitteln:

- 1366 - Durchschnittswert der Messergebnisse
- 1367 - Anzahl der berücksichtigten Messergebnisse
- 1368 - Maximalwert
- 1369 - Minimalwert[<=]

1370 Die Versionsnummer des Useragents wird bei der Konsolidierung nicht weiter verarbeitet
 1371 und dient dem Anbieter des ePA-Aktensystems zur Identifikation von möglichen
 1372 Fehlerquellen im Rahmen des Eigenmonitorings und Troubleshootings.

1373

3 Funktionsmerkmale

1374

3.1 Aktenkonto eines Versicherten (Health Record)

1375
1376
1377
1378
1379

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.

1380
1381

3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte

1382
1383
1384
1385
1386

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.

1387
1388
1389
1390

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.

1391
1392
1393
1394

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.

1395

1396
1397

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

1398
1399
1400

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. [<=]

1401
1402
1403

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.

1404
1405

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

1406
1407
1408

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. [<=]

1409
1410

3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger

1411
1412

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

1413 der ePA eigenständig im Rahmen der gesetzlichen Vorgaben umzusetzen und sind nicht
1414 Bestandteil dieser Spezifikation.

1415 3.1.2 Lebenszyklus und Zustände eines Aktenkontos

1416 Ein Aktenkonto durchläuft in seinem Lebenszyklus diverse Zustände. Einige dieser
1417 Zustände sind für rein administrative Vorgänge vorgesehen (Initialisierung, Umzug des
1418 Aktenkontos zu einem anderen Anbieter), andere für die Nutzung der Akte im
1419 Versorgungsprozess. Diese Nutzung für Versorgungsprozesse ist dabei auf den Zustand
1420 "Activated" eingeschränkt.

1421 Eine Übersicht der unterschiedlichen Status und der Bedingungen für den
1422 Statusübergang sind in der folgenden Tabelle dargestellt.

1423 **Tabelle 2: Zustandswechsel im Lebenszyklus eines Aktenkontos**

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

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

1424 Die Anforderungen in den folgenden Kapiteln legen die zulässigen Zustandswechsel eines
1425 Kontos fest.

1426

1427

1428 3.1.3 Anlage eines neuen Aktenkontos

1429 Ein neues Aktenkonto wird für einen Versicherten bei seinem Anbieter automatisch
1430 angelegt, wenn der Versicherte der grundsätzlichen Nutzung der ePA nicht widerspricht
1431 oder einen zuvor gegebenen Widerspruch zurücknimmt und bei einem anderen Anbieter
1432 kein Aktenkonto für den Versicherten existiert.

1433 Die Anlage eines neuen Aktenkontos erfolgt in zwei Stufen: der Initialisierung und der
1434 darauffolgenden Aktivierung.

1435 Bei der Initialisierung wird ein neues Aktenkonto bei einem Betreiber eines ePA-
1436 Aktensystems für den Versicherten angelegt und die Dienste des Aktenkontos für die
1437 Nutzung vorbereitet. Die Identifikation eines Aktenkontos erfolgt dabei über die KVNR
1438 des Versicherten (unveränderlicher Anteil der Versichertennummer) im Aktensystem und
1439 gegenüber Clients bei Nutzung der ePA.

1440 **A_24336 - Anbieter ePA-Aktensystem - Identifizierung eines Aktenkontos**

1441 Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos die
1442 KVNR des Versicherten zur Identifikation des Aktenkontos im Aktensystem verwenden
1443 und sicherstellen, dass diese Identifikation eines Aktenkontos nicht verändert werden
1444 kann.[<=]

1445 **A_23775 - Anbieter ePA-Aktensystem - Neues Aktenkonto anlegen**

1446 Der Anbieter des ePA-Aktensystems MUSS für Versicherte jeweils ein Aktenkonto
1447 anlegen, wenn kein Widerspruch des Versicherten gegen die Nutzung der ePA vorliegt,
1448 und dabei die KVNR des Versicherten zur Identifikation eines Aktenkontos im Aktenkonto
1449 registrieren. Das initialisierte Aktenkonto MUSS den Status INITIALIZED erhalten.[<=]

1450 Wechselt der Versicherte den Anbieter, so kann ein Widerspruch des Versicherten gegen
1451 die Nutzung der ePA auch bei diesem bisherigen schon vorliegen. In diesem Fall kann die
1452 Anlage eines Aktenkontos bei einem neuen Anbieter entfallen. Andernfalls kann bei dem
1453 bisherigen Anbieter ein Aktenkonto existieren, dessen Daten im Rahmen der Anlage eines
1454 Aktenkontos beim neuen Anbieter importiert werden müssen.

1455 **A_27343 - Anbieter ePA-Aktensystem - verpflichtende Prüfung auf Widerspruch gegen die Nutzung der ePA bei einem anderen Anbieter**

1456 Der Anbieter des ePA-Aktensystems MUSS vor der Anlage eines Aktenkontos durch
1457 Verwendung der Operationen der Schnittstelle gemäß [I_Information_Service_Accounts]
1458

1459 prüfen, ob bei einem anderen Anbieter ein Widerspruch des Versicherten gegen die
1460 Nutzung der ePA vorliegt oder ein Aktenkonto des Versicherten existiert. [\leq]

1461 **A_24789 - Anbieter ePA-Aktensystem - verpflichtender Import eines**
1462 **existierenden Aktenkontos**

1463 Der Anbieter des ePA-Aktensystems MUSS die Inhalte eines existierenden Aktenkontos in
1464 ein neues, initialisiertes Aktenkonto vor dessen Aktivierung übernehmen. [\leq]

1465 **A_24302-01 - Anbieter ePA-Aktensystem - verpflichtende Nutzung der**
1466 **Schnittstelle des Information Service Accounts**

1467 Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos einen
1468 Import der Inhalte eines existierenden Aktenkontos von einem anderen Anbieter durch
1469 Verwendung der Operationen der Schnittstelle gemäß [I_Information_Service_Accounts]
1470 veranlassen. [\leq]

1471 Der weitere Import eines existierenden Aktenkontos vor dessen Aktivierung erfolgt unter
1472 Verwendung des Health Record Relocation Service (3.2- Health Record Relocation
1473 Service).

1474 **A_24790-01 - Anbieter ePA-Aktensystem - keine unbegründeter Import eines**
1475 **Aktenkontos**

1476 Der Anbieter des ePA-Aktensystems DARF den Import eines existierenden Aktenkontos
1477 von einem anderen Anbieter für Zwecke abweichend der Vorgaben in A_24302-* NICHT
1478 nutzen oder veranlassen. [\leq]

1479 **A_15870-02 - Anbieter ePA-Aktensystem - Abbruch bei Nichtverfügbarkeit**
1480 **anderer Anbieter**

1481 Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen,
1482 wenn die Prüfung gemäß A_27343-* mindestens bei einem anderen Anbieters eines ePA-
1483 Aktensystems eine technische Fehlermeldung liefert oder dieser nicht erreichbar ist. [\leq]

1484 **A_27344 - Anbieter ePA-Aktensystem - Abbruch bei fehlgeschlagenem Import**

1485 Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen,
1486 wenn ein Import von Daten eines Aktenkontos von einem bisherigen Anbieter erforderlich
1487 ist und dieser nicht erfolgreich abgeschlossen werden kann. [\leq]

1488 Hinweis zu A_23744*: Ein Import kann beispielsweise fehlschlagen, wenn
1489 schwerwiegende Fehler bei der Exportpaketerstellung oder bei der Übertragung auftreten
1490 (siehe [3.2- Health Record Relocation Service](#)3.2- Health Record Relocation Service).

1491 Für die Geräteregistrierung bei Nutzung eines ePA-FdV durch den Versicherten ist eine E-
1492 Mail-Adresse des Versicherten für Bestätigung der Geräteregistrierung erforderlich. Falls
1493 vorhanden, kann diese E-Mail-Adresse bei der Anlage eines Aktenkontos im Device
1494 Management hinterlegt werden. Ansonsten muss eine E-Mail-Adresse bei der ersten
1495 Einrichtung eines ePA-FdV zur Nutzung des Aktenkontos hinterlegt werden. Eine E-Mail-
1496 Adresse muss vor der Übernahme in das Aktensystem validiert sein, beispielsweise durch
1497 Versand eines Bestätigungslink an diese E-Mail-Adresse.

1498 **A_14996-01 - Anbieter ePA-Aktensystem - Manuelle Ergänzung E-Mail-Adresse**

1499 Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten auf geeignetem Weg
1500 ermöglichen, die Registrierung einer E-Mail-Adresse für die Geräteverwaltung auch
1501 nachträglich vorzunehmen. [\leq]

1502 **A_14993-02 - Anbieter ePA-Aktensystem - Mailadresse validieren**

1503 Der Anbieter des ePA-Aktensystems MUSS eine Mailadresse

- 1504 • bei der ersten Hinterlegung im Aktensystem,
- 1505 • bei einer Änderung der Mailadresse

1506 auf Gültigkeit hin validieren. [\leq]

A_24369 - Anbieter ePA-Aktensystem - Initialisierung des Aktenkontos

Der Anbieter des ePA-Aktensystems MUSS die Initialisierung der Bestandteile

- Consent Decision Management (initiale Entscheidungen)
- Constraint Management (Policies)
- Entitlement Management (initiale Befugnisse und Befugnisausschlüsse)
- Information Service (initiale Entscheidungen "Versorgungsprozess")
- XDS Document Service (statische Aktenkontoinhalte)
- Device Management
- Authorization Service
- Audit Event Service
- Medication Service

vor der Aktivierung eines Aktenkontos durchführen. Die genannten Bestandteile MÜSSEN nach der Aktivierung des Aktenkontos sofort nutzbar sein. [\leq]

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

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

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

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

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

[\leq]

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

A_24335 - Anbieter ePA-Aktensystem - Neues Aktenkonto aktivieren

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

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,

- 1551 • nach erfolgreichem Wechsel des Anbieters durch den Versicherten und
- 1552 abgeschlossener Datenübernahme aus dem bisherigen Aktenkonto,
- 1553 • nach Beendigung des Versicherungsverhältnisses des Versicherten bei seinem
- 1554 Kostenträger.
- 1555 Ein Versicherter kann nach der Anlage eines Aktenkontos der grundsätzlichen Nutzung
- 1556 der ePA widersprechen. Liegt dieser erklärte Widerspruch vor, werden das Aktenkonto
- 1557 des Versicherten und sämtliche Inhalte durch den Anbieter des Aktenkontos gelöscht.
- 1558 Bei einem Anbieterwechsel erfolgt die Übernahme der Daten des bisherigen Aktenkontos
- 1559 zu dem neuen Anbieter. Nach erfolgreichem Abschluss der Datenübernahme in das
- 1560 Aktenkonto des neuen Anbieters löscht der bisherige Anbieter das Aktenkonto des
- 1561 Versicherten und alle darin enthaltenen Daten.
- 1562 Kündigt ein Versicherter das Vertragsverhältnis ohne Übernahme der Daten zu einem
- 1563 neuen Anbieter, löscht der Anbieter des Aktenkontos des Versicherten nach einer
- 1564 angemessenen Wartezeit, bzw. nach Ablauf von vorgeschriebenen Bereitstellungs- und
- 1565 Aufbewahrungszeiträumen, das Aktenkonto und alle darin enthaltenen Daten.
- 1566 Vor der Ausführung der endgültigen Löschung des Aktenkontos muss es dem
- 1567 Versicherten ermöglicht werden, die Protokolldaten (auch unter Einbindung der
- 1568 Ombudsstelle) für seinen eigenen Gebrauch außerhalb des Aktenkontos zu sichern.
- 1569 Dieses ist nicht erforderlich, wenn das Aktenkonto in Folge eines erfolgreichen Umzugs zu
- 1570 einem anderen Anbieter geschlossen wird.

1571

1572 **A_25289 - Anbieter ePA-Aktensystem - Löschen des Aktenkontos durch den**

1573 **Kostenträger**

1574 Der Anbieter des ePA-Aktensystems MUSS das Aktenkonto eines Versicherten inklusive

1575 aller enthaltenen Daten löschen (sämtliche Dokumente, Schlüsselmaterial, Protokolle,

1576 Widerspruchsinformation, Befugnisse und Beschränkungen), wenn dies durch den

1577 zuständigen Kostenträger beauftragt wird. [<=]

1578 **3.2 Health Record Relocation Service**

- 1579 Transfer eines Aktenkontos zu einem neuen Anbieter (Aktenkontoumzug).
- 1580 Wechselt der Versicherte den Kostenträger bzw. den Anbieter seines Aktenkontos, so
- 1581 erfolgt der Umzug der Inhalte seines bestehenden Aktenkontos vom bisherigen Anbieter
- 1582 zu einem neuen Anbieter weitestgehend automatisiert.
- 1583 Seitens der Aktensysteme werden für einen Aktenkontoumzug zwei Schnittstellen
- 1584 angeboten: `I_Health_Record_Relocation_Service` zur Nutzung durch die Anbieter (alt und
- 1585 neu) für den Zugriff auf das Aktenkonto des Versicherten und
- 1586 `I_Information_Service_Accounts` für die Interaktion der Aktensysteme (alt und neu)
- 1587 untereinander. Die notwendige Kommunikation der Kassen-Backends mit ihren
- 1588 Aktensystemen außerhalb der VAU erfolgt dabei in Absprache der Beteiligten und ist nicht
- 1589 Bestandteil der genannten Schnittstellen.

1590 **A_24786 - Health Record Relocation Service - Realisierung der Schnittstelle**

1591 **`I_Health_Record_Relocation_Service`**

1592 Der Health Record Relocation Service MUSS die Operationen der Schnittstelle

1593 `I_Health_Record_Relocation_Service` gemäß [`I_Health_Record_Relocation_Service`]

1594 umsetzen. [<=]

1595 *Hinweis: Zur Schnittstelle I_Information_Service_Accounts siehe [3.15-14.2- Information](#)*
1596 *Service - Account*).

1597 **A_24821 - Health Record Relocation Service - Suspendierung des Aktenkontos**

1598 Der Health Record Relocation Service MUSS sicherstellen, dass das Aktenkontos für die
1599 Erstellung eines Exportpakets auf den Status SUSPENDED gesetzt wird. [<=]

1600

1601 **A_24827 - Health Record Relocation Service - Reaktivierung des Aktenkontos**

1602 Der Health Record Relocation Service MUSS sicherstellen, dass ein Aktenkonto im Status
1603 SUSPENDED nach einem Abbruch eines Transfers von einem Anbieter zu einem anderen
1604 Anbieter aufgrund eines Fehlers (Datenübertrag ist nicht erfolgt) in den Status
1605 ACTIVATED gesetzt wird. [<=]

1606 **A_25005-03A_25005-02 - Health Record Relocation Service - Daten des**
1607 **Exportpakets**

1608 Der Health Record Relocation Service MUSS sicherstellen, dass alle Daten des
1609 Aktenkontos in das Exportpaket übernommen werden aus:

- 1610 • XDS Document Service
- 1611 • Medication Service
- 1612 • Consent Management
- 1613 • Constraint Management
- 1614 • Audit Event Service
- 1615 • Entitlement Management (außer Befugnisse für Versicherten, E-Rezept-Fachdienst,
1616 Kostenträger und Ombudsstelle).
- 1617 • E-Mail Management (die E-Mail-Adresse des Aktenkontoinhabers (falls vorhanden)
1618 sowie für alle Vertreter die E-Mail-Adressen, sofern sie die dem exportierenden
1619 Aktensystem bekannt sind).

1620 Bei FHIR Data Services MUSS der Health Record Relocation Service sicherstellen, dass
1621 die jeweilige Resource.id aller FHIR-Instanzen ebenso in das Exportpaket einfließen,
1622 sodass nach einem Import die Identitäten der FHIR-Daten stabil bleiben.

1623 [<=]

1624 *Hinweis: Die Geräteregistrierungen des Versicherten oder der Vertreter werden nicht*
1625 *exportiert. Bei einem neuen Anbieter ist für den Versicherten eine erneute*
1626 *Geräteregistrierung erforderlich.*

1627 **A_25605 - Health_Record_Relocation_Service - Erstellung des Exportpakets**

1628 Der Health Record Relocation Service MUSS sicherstellen, dass das Exportpaket gemäß
1629 der Vorgaben in [HealthRecordMigration] bezüglich der Struktur, der Formate für die
1630 enthaltenen Daten und die Verschlüsselung erfolgt. [<=]

1631 **A_25012 - Health Record Relocation Service - Signatur der Befugnisse**

1632 Der Health Record Relocation Service MUSS sicherstellen, dass die gemäß A_23734-*
1633 signierten Anteile einer Befugnis mit der Signaturidentität ID.FD.SIG (Rolle `oid_epa_vau`)
1634 signiert werden. [<=]

1635 *Hinweis: Der CMAC einer Befugnis wird nicht ins Export-Paket übernommen.*

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

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

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

[<=]

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

A_24787-01 - Health Record Relocation Service - Verschlüsselung des Exportpaketes

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

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==

[\leq]

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.

[\leq]

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. [\leq]

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.

[\leq]

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. [\leq]

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. [\leq]

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

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

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

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

[<=]

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

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

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

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

A_21548-01 - Health Record Relocation Service - Information der Vertreter über neuen FQDN nach Abschluss des Anbieterwechsels

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

Hinweis zu A_21548-01: Für die Benachrichtigung derjenigen Vertreter, die dem importierenden Aktensystem nicht bekannt sind, werden die E-Mail-Adressen aus dem Exportpaket genommen. Für die Benachrichtigung der Vertreter, die dem importierenden Aktensystem bekannt sind, wird die im importierenden Aktensystem hinterlegte E-Mail-Adresse des Vertreters verwendet.

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

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

1749 gemäß A_21548-* genutzt werden und nach Abschluss des Anbieterwechsels im
 1750 importierenden Aktensystem gelöscht werden, d.h. nicht im importierenden Aktensystem
 1751 gespeichert werden. [<=]

1752 **A_24788 - Health Record Relocation Service - Löschen des Exportpakets nach**
 1753 **Umzug des Aktenkontos**

1754 Das Aktensystem MUSS sicherstellen, dass ein vorhandenes Exportpaket nach einem
 1755 erfolgreichen Transfer eines Aktenkontos eines Versicherten von einem Anbieter zu
 1756 einem anderen Anbieter gelöscht wird. [<=]

1757 **A_24982-02 - Health Record Relocation Service – Protokollierung des**
 1758 **Anbieterwechsels eines Aktenkontos**

1759 Der Health Record Relocation Service des neuen (importierenden) Aktensystems MUSS
 1760 nach der erfolgreichen oder einer abgebrochenen Übertragung der Inhalte eines
 1761 Aktenkontos vom bisherigen Anbieter einen Protokolleintrag gemäß A_24704* erzeugen.
 1762 Dabei ist folgende Wertebelegung zu berücksichtigen:

1763 **Tabelle 3 : Health Record Relocation Service Protokollierung**

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

1764 [<=]

1765

1766 *Hinweis: Das Aktensystem des bisherigen Anbieters muss keinen Protokolleintrag gemäß*
 1767 *A_24982* erzeugen.*

1768 **3.2.1 Ablauf eines Aktenkontoumzugs**1769 **3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter**

1770 Der Anbieter (neu) lässt im Aktensystem (neu) ein neues Aktenkonto anlegen. Dieses
1771 erhält den Status INITIALIZED. Hierfür gelten die Anforderungen gemäß ~~3.1.3- Anlage~~
1772 ~~eines neuen Aktenkontos~~ 3.1.3- Anlage eines neuen Aktenkontos.

1773 Falls der Versicherte schon einen Widerspruch gegen die Nutzung der ePA bei seinem
1774 bisherigen Kostenträger erklärt hat, kann die Initialisierung eines neuen Aktenkontos ggf.
1775 entfallen. Ein Transfer, bzw. die Erstellung eines Exportpakets, ist in diesem Fall mangels
1776 eines existierenden Aktenkontos beim bisherigen Anbieter nicht erforderlich.

1777 Die Abfrage eines existierenden Widerspruchs des Versicherten bei einem anderen
1778 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

1779 **3.2.1.2 Start Transfer eines existierenden Aktenkontos**

1780 Hat der Versicherte bei keinem Anbieter einen Widerspruch gegen die Nutzung der ePA
1781 erklärt und existiert bei einem bisherigen Anbieter (alt) ein Aktenkonto, wird der Transfer
1782 der Daten durch das Aktensystem (neu) initiiert.

1783 Das Aktensystem (alt), bei welchem das Aktenkonto existiert, bestätigt diese Anfrage
1784 zum Transfer mit einer Vorgangs-ID.

Starten des Transfers

I_Information_Service_Accounts (bisheriges Aktensystem)

startRelocation

initiiieren der Exportpaketerstellung

1785

1786 **3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen**
1787 **Anbieter**

1788 Das Aktensystem (alt) informiert den Anbieter (alt) über die Anfrage zum Transfer und
1789 die Vorgangsnummer. Der Anbieter (alt) öffnet das existierende Aktenkonto des
1790 Versicherten und stößt in der VAU die Erzeugung des Exportpakets an. Der Health Record
1791 Relocation Service beantwortet diese Anfrage durch Rückgabe einer URL für den späteren
1792 Download des Exportpakets durch den neuen Anbieter und startet die Erzeugung des

1793 Exportpakets. Das Aktenkonto wird vor der Paketerstellung auf den Status SUSPENDED
1794 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

1795 In dieses Exportpaket werden alle Daten des Aktenkontos gemäß A_25005*
1796 übernommen. Das fertige Exportpaket wird mittels ENC-Zertifikat, welches im VAU-HSM
1797 eingebracht und gespeichert wurde, verschlüsselt und am vorbereiteten Downloadpunkt
1798 bereitgestellt.

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

1801 Der Anbieter (alt) veranlasst nach Erhalt der Download-URL über das Aktensystem (alt)
1802 den Versand der URL an das Aktensystem (neu).

1803 Das Aktensystem (alt) prüft vor der Übermittlung der Download-URL an das Aktensystem
1804 (neu), ob das Exportpaket für den Download bereitsteht, ggf. wird auf den Abschluss der
1805 Paketerstellung gewartet. Ist dieses der Fall, erfolgt die Benachrichtigung des
1806 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

3.2.1.5 Import des Exportpakets durch den neuen Anbieter

1807 Der Information Service des Aktensystems (neu) nimmt die Download-URL entgegen und
1808 übermittelt diese an den Kostenträger (neu). Dieser öffnet den Zugang zum Aktenkonto
1809 (neu) des Versicherten und veranlasst in der VAU den Import des Exportpakets.
1810

Import und Integration des Exportpakets

I_Health_Record_Relocation_Service (neuer Anbieter)

startPackageImport

Starten des Imports der vorhandenen Daten

3.2.1.6 Abschluss des Transfers durch beide Anbieter

1812 Das Aktensystem (neu) startet den Download des Exportpakets, entschlüsselt dieses und
1813 übernimmt die Daten in das initialisierte Aktenkonto des Versicherten. Nach
1814 erfolgreichem Abschluss wird (kann) das Aktenkonto (neu) in den Status ACTIVATED
1815 überführt werden.

1816 Unter Verwendung des Information Service wird das Aktensystem (alt) über den
1817 erfolgreichen Import und den Abschluss des Transfers informiert. Das Aktenkonto (alt)

1818 kann daraufhin, ggf. unter Einhaltung weiterer Bedingungen des Kostenträgers bzw.
1819 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)

1820 3.2.1.7 Fehlersituationen und Handhabung

1821 Der gesamte Austausch von Informationen zwischen Aktensystemen und Anbietern kann
1822 durch die in Schritt 1 erzeugte Vorgangs-ID genau einem konkreten Relocation Vorgang
1823 zugeordnet werden. Diese Vorgangsnummer wird auch verwendet, wenn das jeweils
1824 andere Aktensystem über Fehler im Ablauf benachrichtigt werden muss (Incidents).

1825 *3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich oder*
1826 *derzeit nicht möglich*

1827 Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter
1828 (alt) das Exportpaket voraussehbar nicht importieren oder widerspricht der Versicherte
1829 nach der Initialisierung des Aktenkontos beim neuen Kostenträger der Nutzung der ePA,
1830 so kann durch Übertragung eines Incidents an das Aktensystem (alt) dieser Sachverhalt
1831 mitgeteilt werden, so dass der Transfervorgang abgebrochen und das Exportpaket nicht
1832 erzeugt oder wieder gelöscht wird.

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

1833 Das Aktenkonto wird bei Anbieter (alt) wieder in den Status ACTIVATED gesetzt, um eine
1834 weitere Nutzung zu ermöglichen.

1835 Für einen Transfer zu einem späteren Zeitpunkt muss der Anbieter (neu) den Vorgang
1836 durch Anfrage bei den weiteren Anbietern (alt) und Übermittlung eines ENC-Zertifikats
1837 erneut starten.

1838 3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter

1839 Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter
1840 (alt) das Exportpaket unter Verwendung der übertragenen Download-URL nicht oder

- 1841 nicht vollständig laden oder die Inhalte des Exportpaketes aufgrund fehlerhafter
 1842 Verschlüsselung oder fehlerhafter Struktur oder Inhalte nicht erfolgreich integrieren oder
 1843 der Anbieter (neu) hat keine Download-URL vom Anbieter (alt) bezogen, so kann durch
 1844 Übertragung eines Incidents an den Anbieter (alt) dieser Sachverhalt mitgeteilt werden.

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

- 1845 Das Aktenkonto verbleibt beim neuen Anbieter in Status INITIALIZED. Die
 1846 Incidentmeldung an den Anbieter (alt) kann durch Kommunikation der Anbieter und/oder
 1847 Betreiber untereinander zum Zweck der Problemlösung ergänzt werden.
- 1848 Der Anbieter (alt) meldet die Korrektur durch erneuten Versand einer Download-URL an
 1849 den Anbieter (neu) für den unterbrochenen Vorgang.
- 1850 Es obliegt dem Anbieter (alt), bei zeitlich aufwendigen Korrekturen das Aktenkonto
 1851 zunächst für eine weitere Nutzung wieder zu aktivieren (Status ACTIVATED) und nach
 1852 Abschluss der Korrektur wieder in den Status SUSPENDED zu überführen.
- 1853 Es obliegt dem Anbieter (alt) auch, bei zeitlich aufwendigen Korrekturen den Transfer
 1854 durch Senden des Incidents "relocationAborted" an den Anbieter (neu) abubrechen und
 1855 das Aktenkonto zur weiteren Nutzung wieder zu aktivieren (Status ACTIVATED). Der
 1856 Transfer muss dann durch den Anbieter (neu) erneut gestartet werden.
- 1857 *3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter*
- 1858 Ruft ein neuer Anbieter ein bereitgestelltes Exportpaket nicht ab oder erfolgt durch den
 1859 neuen Anbieter keine Benachrichtigung über einen erfolgreichen Abschluss des Transfers

1860 oder einen Fehler beim Import des Exportpakets, dann kann eine Benachrichtigung an
1861 den neuen Anbieter erfolgen.

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

1862 Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei
1863 Anbieter (alt) auf den Status ACTIVATED gesetzt, um eine weitere Nutzung zu
1864 ermöglichen. Exportpaket und Downloadlink können gelöscht werden. Der Transfer muss
1865 durch den Anbieter (neu) erneut gestartet werden.

1866 *3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter*

1867 Ein Anbieter (alt) kann den Abbruch eines angeforderten Transfers an den Anbieter (neu)
1868 signalisieren.

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

1869 Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei
1870 Anbieter (alt) auf den Status ACTIVATED zurückgesetzt, wenn dieses schon den Status

1871 SUSPENDED hat, um eine weitere Nutzung zu ermöglichen. Exportpaket und
 1872 Downloadlink können gelöscht werden. Der Transfer muss durch den Anbieter (neu)
 1873 erneut gestartet werden.

1874 3.3 Sichere Speicherung sensibler Schlüssel und Informationen im 1875 VAU-HSM

1876 Im Folgenden wird beschrieben, welche Informationen in einem HSM (als VAU-HSM
 1877 bezeichnet) zu speichern sind.

1878 Verständnishinweis: Die HMAC-Schlüssel (symmetrische Schlüssel) für die Prüfung der
 1879 VSDM+-Prüfnachweise [gemSpec_SST_FD_VSDM], [C_11321] werden von den VSDM-
 1880 Betreibern erzeugt und für die ePA-VAUs der ePA-Betreiber verschlüsselt exportiert. Die
 1881 Schlüssel und auch die Export/Import-Vorgänge (Mehr-Augen-Prinzip) sind die gleichen
 1882 wie sie auch für/bei der E-Rezept-VAU verwendet werden.

1883 A_24611-06A_24611-04 - ePA-Aktensystem - Im VAU-HSM gespeicherte 1884 Schlüssel und Informationen für VAU-Betrieb

1885 Das ePA-Aktensystem MUSS sicherstellen, dass folgende, für den Betrieb der VAU
 1886 notwendigen Schlüssel und Informationen in einem HSM (als VAU-HSM bezeichnet)
 1887 gespeichert werden:

- 1888 • privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
 1889 (u.a. genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- 1890 • ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- 1891 • ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- 1892 • privater Schlüssel der Verschlüsselungsidentität der VAU
- 1893 • privater Schlüssel der Signaturidentität der VAU
- 1894 • Zertifikat C.FD.ENC mit policyIdentifier professionOID oid_epa_vau für die
 1895 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- 1896 • Zertifikat C.ZD.SIG mit professionOID oid_popp-token für die Token-Signatur-
 1897 Identität des PoPP-Services
- 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 [\leq]

1914 Hinweis:

1915 Es gelten die Anforderungen aus [gemSpec_Krypt#3.18 VSDM-Prüfziffer Version 2] für
 1916 ein ePA-Aktensystem in der Rolle "Prüfziffer Version 2 prüfendes System". Aus den ins
 1917 HSM importierten gemeinsamen Geheimnissen erfolgt im HSM eine Schlüsselableitung
 1918 (A_27299-*) der für die Entschlüsselung der Prüfziffer Version 2 benötigten AES/GCM-
 1919 Schlüssel.

1920 **A_26109 - ePA-Aktensystem - Unterschiedliche private**

1921 **Authentisierungsschlüssel für AK-, Befugnisverifikations- und Service-VAU**

1922 Das ePA-Aktensystem MUSS sicherstellen, dass für die Authentisierungsidentitäten für
 1923 Aktenkontoverwaltungs-VAUs, Befugnisverifikations-VAUs und Service-VAUs
 1924 unterschiedliche private Schlüssel verwendet werden. [\leq]

1925 **A_26110 - ePA-Aktensystem - Unterschiedliche private**

1926 **Authentisierungsschlüssel für unterschiedliche Service-VAUs**

1927 Das ePA-Aktensystem MUSS sicherstellen, dass für unterschiedliche Typen von Service-
 1928 VAUs unterschiedliche private Schlüssel für die Authentisierung genutzt werden. [\leq]

1929 Hinweis zu A_26110: Ein Typ einer Service-VAU könnte beispielsweise eine PDF-
 1930 Konvertierungs-Service-VAU sein oder eine Pseudonymisierungs-Service-VAU für Daten
 1931 zur Sekundärnutzung sein. Alle Instanzen einer PDF-Konvertierungs-Service-VAU nutzen
 1932 denselben privaten Authentisierungsschlüssel. Die Instanzen der Pseudonymisierungs-
 1933 Service-VAU dürfen den Authentisierungsschlüssel der PDF-Konvertierungs-Service-VAU
 1934 jedoch nicht verwenden.

1935 **~~A_24612-05A_24612-04~~ - ePA-Aktensystem - Erzwingen von 4-Augen-Prinzip**
 1936 **für Einbringen und Verwalten von Informationen ins VAU-HSM**

1937 Das ePA-Aktensystem MUSS technisch erzwingen, dass die folgenden, für den Betrieb der
 1938 VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip in das
 1939 VAU-HSM eingebracht und verwaltet werden können:

- 1940 • privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- 1941 • ggf. privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- 1942 • ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- 1943 • privater Schlüssel der Verschlüsselungsidentität der VAU
- 1944 • privater Schlüssel der Signaturidentität der VAU
- 1945 • Zertifikat C.FD.ENC mit policyIdentifier professionOID oid_epa_vau für die
 1946 Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- 1947 • Zertifikat C.ZD.SIG mit professionOID oid_popp-token für die Token-Signatur-
 1948 Identität des PoPP-Services
- 1949 • symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-
 1950 Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames
 1951 Geheimnis bezeichnet werden.
- 1952 • symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- 1953 • Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für
 1954 die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf.
 1955 für Service-VAUs)
- 1956 • Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

1957 [\leq]

~~A 24614-05A-24614-03~~ - 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~~professionOID oid_epa_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Zertifikat C.ZD.SIG mit professionOID oid_popp-token für die Token-Signatur-Identität des PoPP-Services
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

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

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

~~A 24618-05A-24618-04~~ - ePA-Aktensystem - Zugriff auf Schlüssel und Informationen im VAU-HSM

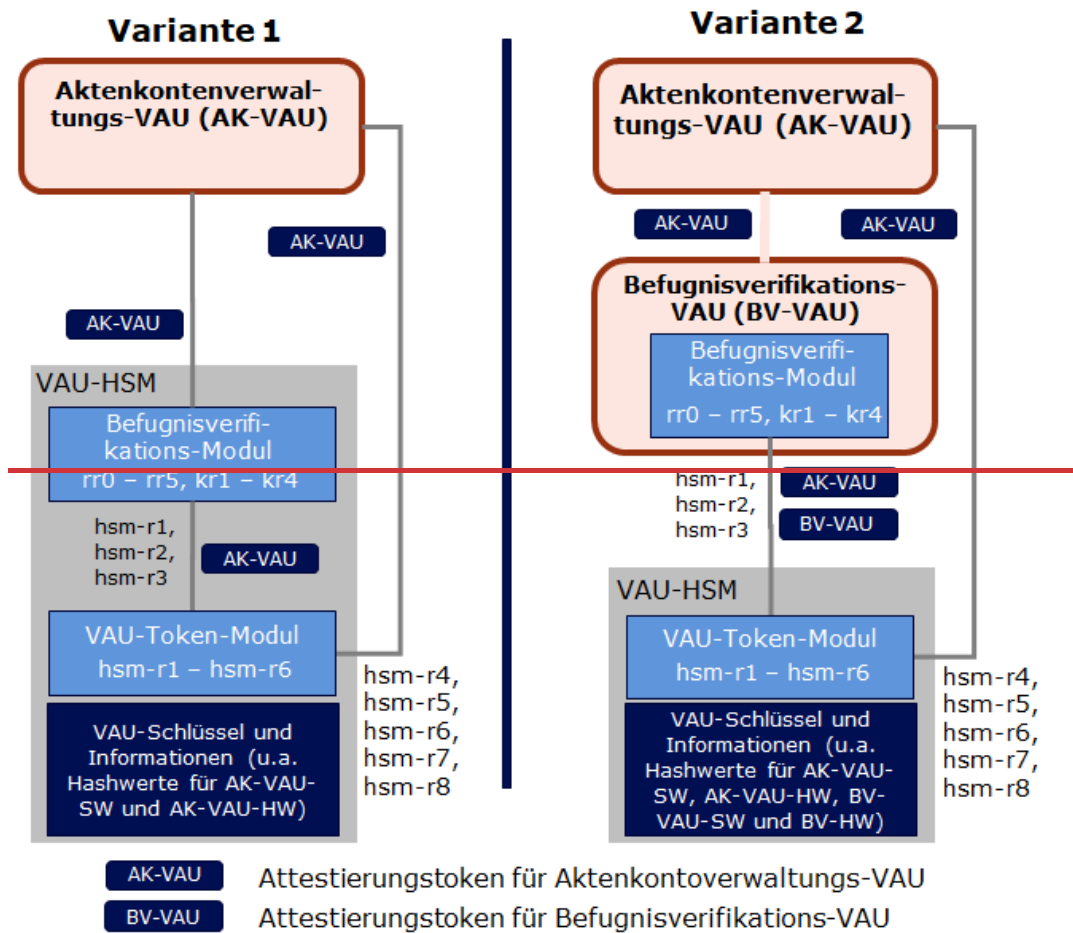
Das ePA-Aktensystem MUSS sicherstellen, dass auf die folgenden, für den Betrieb der VAU notwendigen und im VAU-HSM gespeicherten Schlüssel und Informationen ausschließlich über attestierte VAU-Instanzen zugegriffen werden kann:

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

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

2028 3.4 Befugnisverifikations-Modul

- 2029 Das Befugnisverifikations-Modul enthält die Regeln zur Befugnisregistrierung (entitlement
- 2030 registration rules) und die Regeln zum Abruf der versichertenindividuellen
- 2031 Persistierungsschlüssel (key rules).
- 2032 Die folgende Abbildung zeigt die zwei möglichen Architekturvarianten für die Ausführung
- 2033 des Befugnisverifikations-Moduls. In Variante 1 wird es direkt im VAU-HSM ausgeführt. In
- 2034 Variante 2 wird es in einer Befugnisverifikations-VAU ausgeführt, die zwischen einer
- 2035 Aktenkontoverwaltungs-VAU und einem VAU-HSM vermittelt und Prüfungen für das VAU-
- 2036 HSM übernimmt (z. B. prüfen der ID-Token oder registrieren neuer Befugnisse).
- 2037 In beiden Varianten ist ein Zugriff auf die Schlüssel im VAU-HSM nur durch integrale und
- 2038 attestierte VAUs möglich. Die Prüfung der VAU-Attestierungstoken verbleibt in beiden
- 2039 Varianten im VAU-HSM (VAU-Token-Modul). Das VAU-HSM speichert in Variante 2 neben
- 2040 den Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware
- 2041 für die VAU der Aktenkontoverwaltung zusätzlich auch die Hashwertrepräsentationen der
- 2042 erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der
- 2043 Befugnisverifikations-VAU. Ein Zugriff auf das HSM ist dann nur mit einem validen
- 2044 Attestierungstoken für die Aktenkontoverwaltung-VAU und die Befugnisverifikations-VAU
- 2045 möglich.



2046

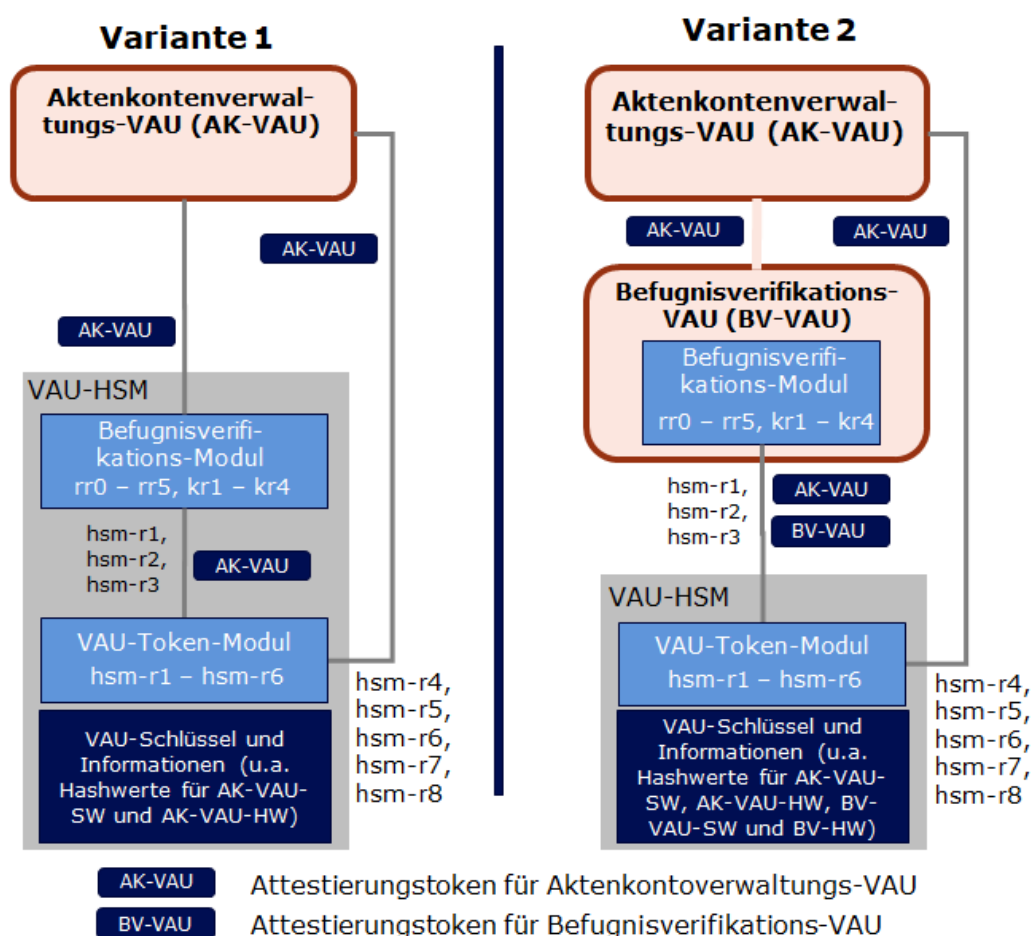


Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls

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. [≤]

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

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

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

Regel	Beschreibung
hsm-r1	<p><i>Diese Regel dient zur Sicherung von Befugnissen und HSM-ID-Token mittels CMAC.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (optional) • Daten <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Daten gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen der Signatur(en)des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Falls die Prüfungen 1) - 3) erfolgreich waren, werden die übergebenen Daten mittels CMAC gesichert.</p>

Regel	Beschreibung
hsm-r2	<p><i>Diese Regel dient zur Ableitung der versichertenindividuellen Persistierungsschlüssel</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • KVNR • gewünschte Persistierungsschlüssel [Label für Datenpersistierungs-Masterkey und/oder Label für Befugnispersistierungs-Masterkey] • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • falls in Eingangsdaten angefordert: versichertenindividueller Befugnispersistierungsschlüssel • falls in Eingangsdaten angefordert: versichertenindividueller Datenpersistierungsschlüssel <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Falls die Prüfungen 1) - 3) erfolgreich waren, wird der angeforderte versichertenindividuelle Befugnispersistierungsschlüssel und/oder versichertenindividuelle Datenpersistierungsschlüssel für die übergebene KVNR von den durch die Label identifizierten Masterkeys abgeleitet.</p>

Regel	Beschreibung
hsm-r3	<p><i>Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfziffern der Version 1 oder der Entschlüsselung der VSDM-Prüfziffern der Version 2</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) • Szenario VSDM-Prüfziffer Version 1 <ul style="list-style-type: none"> • Daten • Bezeichner des HMAC-Schlüssels • Szenario VSDM-Prüfziffer Version 2 <ul style="list-style-type: none"> • VSDM-Prüfziffer in Version 2 <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Szenario VSDM-Prüfziffer Version 1: HMAC der Daten mit dem symmetrischen Schlüssel, der zum übergebenen Bezeichner des HMAC-Schlüssels gehört • Szenario VSDM-Prüfziffer Version 2: innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) bei erfolgreicher Entschlüsselung <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. (opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Szenario VSDM-Prüfziffer Version 1: Falls die Prüfungen 1) - 3) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.</p> <p>Szenario VSDM-Prüfziffer Version 2: Falls die Prüfungen 1) - 3) erfolgreich waren, wird die VSDM-Prüfziffer gemäß den Prüfschritten 4. und 5. aus A_27279-* geprüft und entschlüsselt. Bei erfolgreicher Entschlüsselung der VSDM-Prüfziffer wird die innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) zurückgeliefert, ansonsten ein Fehler.</p>

Regel	Beschreibung
hsm-r4	<p><i>Diese Regel dient zur Nutzung der privaten Schlüssel der AUT-Identitäten der VAU</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • Challenge • [VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU] VAU-Attestierungstoken einer Befugnisverifikations-VAU] VAU-Attestierungstoken eines Service-VAU-Typs] <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Challenge signiert mit privatem Schlüssel der AUT-Identität • der Aktenkontoverwaltungs-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU übergeben wurde, • der Befugnisverifikations-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Befugnisverifikations-VAU übergeben wurde, • des Service-VAU-Typs, falls in den Eingangsdaten ein VAU-Attestierungstoken des Service-VAU-Typs übergeben wurde. <p>Prüfschritte</p> <ol style="list-style-type: none"> 1. prüfen der Signatur des <u>Signaturdes</u> VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und zum VAU-Typ passt. <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, wird die übergebene Challenge mit dem privatem Schlüssel der zum VAU-Attestierungstoken gehörenden AUT-Identität signiert.</p>
hsm-r5	<p><i>Diese Regel dient zur Nutzung des privaten Schlüssels der ENC-Identität der VAU</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • verschlüsselte Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • entschlüsselte Daten <p>Prüfschritte</p> <ol style="list-style-type: none"> 1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind. <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen verschlüsselten Daten mit dem privatem Schlüssel der ENC-Identität der VAU entschlüsselt.</p>

Regel	Beschreibung
hsm-r6	<p><i>Diese Regel dient zur Nutzung des privaten Schlüssels der Signaturidentität der VAU</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • zu signierende Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • signierte Daten <p>Prüfschritte</p> <ol style="list-style-type: none"> 1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen Daten mit dem 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>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Verschlüsselungszertifikat C.FD.ENC des anderen Aktensystembetreibers <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen der Signatur des <u>Signaturdes</u> VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Falls die Prüfungen 1) - 2) erfolgreich waren, wird das ENC-Zertifikat des anderen Aktensystembetreibers zurückgeliefert.</p>

Regel	Beschreibung
hsm-r8	<p>Diese Regel dient zum Ableiten von symmetrischen Schlüsseln für die Ver- bzw. Entschlüsselung von Daten</p> <p><u>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.</u></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder einer Service-VAU • Ableitungsvektor <i>dv</i> • Label für Masterkey (opt.) <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • symmetrischer Schlüssel <i>symKey</i> • Label für Befugnis-Masterkey <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und es sich um die Attestierung einer Aktenkontoverwaltungs-VAU oder Service-VAU handelt 3. falls ein Label für einen Masterkey In den Eingangsdaten enthalten ist, prüfen, ob das Label zu einem Befugnis-Masterkey gehört <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>

2076

2077 **A_24667 - ePA-Aktensystem -VAU-HSM - Prüfen des VAU-Attestierungstokens**

2078 Das VAU-HSM MUSS bei der Prüfung eines VAU-Attestierungstokens sicherstellen, dass
 2079 dieses zeitlich gültig ist und Replay-Attacken abwehren. [≤]

2080 **A_26303 - ePA-Aktensystem - Abgeleitete Verschlüsselungsschlüssel sind** 2081 **ausschließlich einer VAU zugänglich**

2082 Das ePA-Aktensystem MUSS sicherstellen, dass ein mit Regel hsm-r8 abgeleiteter
 2083 Schlüssel ausschließlich einer VAU zugänglich ist und ausschließlich mittels AES/GCM
 2084 analog [gemSpec_Krypt#GS-A_4389] verwendet wird. [≤]

2085 **3.4.2 Regeln des Befugnisverifikations-Moduls**

2086 Die folgende Tabelle zeigt die Regeln des Befugnisverifikations-Moduls im Überblick.

2087 **Tabelle 5: Überblick über die Regeln des Befugnisverifikations-Moduls**

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

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
rr5	Mit dieser Regel werden die Befugnisse bei einem betreiberübergreifenden Anbieterwechsel im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
kr1	Diese Regel wird für die Anmeldung des Aktenkontoinhabers genutzt.	<i>Tab_AS_SDS-Key_Rules</i>
kr2	Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	<i>Tab_AS_SDS-Key_Rules</i>
kr3	Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	<i>Tab_AS_SDS-Key_Rules</i>
kr4	Diese Regel wird für die Anmeldung des E-Rezept-Fachdienstes verwendet.	<i>Tab_AS_SDS-Key_Rules</i>
<u>kr5</u>	<u>Diese Regel wird für die Überschlüsselung (ggf. mit Umschlüsselung einer Überschlüsselung) verwendet.</u>	<u><i>Tab_AS_SDS-Key_Rules</i></u>

2088

2089

2090

2091

2092

A_24573-03 - 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]

2093
2094**Tabelle 6: Tab_AS_Entitlement_Registration_Rules - Regeln zur Registrierung von Befugnissen**

Regel	Beschreibung
rr0	<p>Mit dieser Regel werden ID-Token im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token mit NutzerID=x signiert durch einen sektoralen Identity Provider, den IDP-Dienst oder den E-Rezept-Fachdienst <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • HSM-ID-Token mit NutzerID=x gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (C.FD.SIG) bei Token eines IDPs bzw. gemäß A_24658-* bei Token des E-Rezept-Fachdiensts (C.FD.AUT). 2. Falls die Prüfung in 1) erfolgreich war, <ol style="list-style-type: none"> a. erstellt das Befugnisverifikations-Modul ein HSM-ID-Token mit der NutzerID=x, einer Gültigkeitsdauer von 24 Stunden und der professionOID aus dem Signaturzertifikat (oid_idpd_sek, oid_idpd oder oid_erp-vau). b. ruft das Befugnisverifikations-Modul die VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und dem HSM-ID-Token auf. <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert das mittels CMAC gesicherte HSM-ID-Token als Ergebnis des Regelaufrufs zurück.

rr1	<p>Mit dieser Regel werden vom Aktenkontoinhaber am ePA-FdV erstellte Befugnisse im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Befugnis1 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) signiert vom Versicherten <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis2 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß <u>Tokensgemäß</u> A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt <p>oder prüfen des HSM-ID-Tokens</p> <ol style="list-style-type: none"> c. Aufruf der VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. d. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt. 2. prüfen der Befugnis1 <ol style="list-style-type: none"> a. prüfen der Signatur gemäß A_25042-* (Zertifikatsprofil C.CH.SIG) b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_versicherter</code> ist c. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der "KVNR Aktenkonto" in der Befugnis1 übereinstimmt. d. prüfen, dass das JWT gemäß A_24587-* zeitlich gültig ist ($iat - 15s \leq \text{aktuelle Zeit} \leq exp + 15s$) 3. Falls die Prüfungen in 1) bis 2) erfolgreich waren, erstellt das Befugnisverifikations-Modul die Befugnis2. Die Inhalte werden aus Befugnis1 übernommen mit folgender Ausnahme:
-----	---

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

rr2	<p><i>Mit dieser Regel werden vom Vertreter am ePA-FdV erstellte Befugnisse für das Aktenkonto des Versicherten im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Vertreter mittels Signaturdienst signiert.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Befugnis1 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) signiert vom Vertreter • Befugnis2 = (KVNR Aktenkonto, KVNR Vertreter) gesichert mittels CMAC <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis3 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt oder prüfen des HSM-ID-Tokens <ol style="list-style-type: none"> c. Aufruf der VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. d. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt. 2. prüfen der Befugnis1 und Befugnis2 <ol style="list-style-type: none"> a. prüfen der Signatur von Befugnis1 gemäß A_25042-* (Zertifikatsprofil C.CH.SIG) b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_versicherter</code> ist c. prüfen des CMAC von Befugnis2 d. prüfen, dass die Telematik-ID in Befugnis 1 keine KVNR ist (Vertreter dürfen keine weiteren Vertreter befugen) e. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der „KVNR Vertreter“ in der Befugnis2 übereinstimmt
-----	--

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

rr3	<p>Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das Stecken der eGK in einer Leistungserbringenumgebung ergeben.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VSDM-Prüfziffer in Version 1 oder 2 signiert mit AUT-Identität der SMC-B oder signiertes PoPP-Token <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMACMAC • falls VSDM-Prüfziffer in Version 2, zusätzlich die innere Struktur der Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) <p>Prüfschritte:</p> <p>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.</p> <p><u>Szenario VSDM-Prüfziffer in Version 1:</u></p> <ol style="list-style-type: none"> 1. prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A_25042-* (C.HCI.AUT) 2. Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert. 3. prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer nicht länger als 20 Minuten zurückliegt mit prüfziffer.timestamp - 30s <= aktuelle Zeit < prüfziffer.timestamp + 20 Minuten + 15s) 4. prüfen des HMAC der VSDM-Prüfziffer mittels VAU-HSM-Regel hsm-r3 <ol style="list-style-type: none"> 2: <p>Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> 5. Falls die Prüfungen in 1) bis 4) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit <code>enforce popp only = true</code>, dann FAIL, ansonsten führe die folgenden Inhalte erstellt: <ul style="list-style-type: none"> • Aktenkonto: die KVNR aus dem VSDM-Prüfziffer • Telematik-ID: die Telematik-ID aus der SMC-B-Signatur • Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur. <p>1. Aufruf der VAU-HSM-Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis</p>
-----	--

~~a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.~~

~~1. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis als Ergebnis des Regelaufrufs zurück.~~

Szenario VSDM-Prüfziffer in Version 2 Prüfschritte durch:

1. prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A_25042-* (C.HCI.AUT)
2. Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert.
3. Aufruf von VAU-HSM Regel hsm-r3 mit der dekodierten VSDM-Prüfziffer
 - a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
4. prüfen der inneren Struktur nach Prüfschritt 6 gemäß A_27279-* (d.h. eGK ist nicht gesperrt)
5. prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer (prüfziffer.iat) nicht länger als 20 Minuten zurückliegt ($\text{prüfziffer.iat} - 30s \leq \text{aktuelle Zeit} < \text{prüfziffer.iat} + 20 \text{ Minuten} + 15s$, Hinweis in der Prüfziffer gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben)
6. prüfen des prüfziffer.hcv nach Prüfschritt 8 gemäß A_27279-* bzgl. des hcv im JWT
7. Falls die Prüfungen in 1) bis 6) erfolgreich waren, und die VAU-HSM Regel hsm-r3 den Klartext der inneren Struktur der Prüfziffer zurückgeliefert hat, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:
 - Aktenkonto: KVNR, die als Ergebnis der VAU-HSM Regel hsm-r3 zurückgeliefert wird
 - Telematik-ID: die Telematik-ID aus der SMC-B-Signatur
 - Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur.
8. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis
 - a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
9. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis sowie die entschlüsselte innere Struktur der Prüfziffer im Klartext gemäß A_27278-* als Ergebnis des Regelaufrufs zurück.

Szenario PoPP-Token:

Regel	Beschreibung
	<ol style="list-style-type: none"> 1. <u>prüfen des PoPP-Tokens via TI-PKI gemäß Abschnitt "PoPP-Token Prüfung" in [gemSpec PoPP Service], wobei im HSMbis auf den OCSP-Sperrstatus keine Prüfung des Signaturzertifikats des PoPP-Tokens erfolgt, da das Signaturzertifikat kontrolliert im 4-Augenprinzip in das HSM eingebracht wird. Da das in das HSM eingebrachte TI-PKI-Signaturzertifikat genutzt wird, ist auch kein Bezug und keine Verarbeitung von Entity Statements im HSM erforderlich. Der Claim <code>iss</code> im PoPP-Token muss nicht geprüft werden.</u> 2. <u>prüfen, dass der Ausstellungszeitpunkt des PoPP-Tokens (PoPP-Token.iat) nicht länger als 20 Minuten zurückliegt (PoPP-Token.iat - 30s <= aktuelle Zeit < PoPP-Token.iat + 20 Minuten + 15s, Hinweis: im PoPP-Token gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben)</u> 3. <u>Falls die Prüfungen in 1) bis 2) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt:</u> <ul style="list-style-type: none"> • <u>Aktenkonto: KVNR aus PoPP-Token.patientId</u> • <u>Telematik-ID: Telematik-ID aus PoPP-Token.actorID</u> • <u>Gültigkeitszeitraum: ergibt sich aus PoPP-Token.actorProfessionOid.</u> 4. <u>Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis</u> <ol style="list-style-type: none"> a. <u>Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</u> 2.5. <u>Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis zurück.</u>

Regel	Beschreibung
rr4	<p><i>Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der Anlage eines Aktenkontos im Aktensystem registriert.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Befugnis1 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) signiert mit SMC-B des Kostenträgers bzw. der Ombudsstelle <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis2 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Prüfen der Befugnis1 <ol style="list-style-type: none"> a. prüfen der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle gemäß A_25042-* (C.HCI.OSIG) b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_kostentraeger</code> bzw. <code>oid_ombudsstelle</code> ist c. prüfen, ob die Telematik-ID im Signaturzertifikat C.HCI.OSIG der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle mit der Telematik-ID in der Befugnis1 übereinstimmt 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 erstellt. Die Inhalte der Befugnis2 sind: <ul style="list-style-type: none"> • Aktenkonto: die KVNR des Aktenkontos aus Befugnis1 • Telematik-ID: die Telematik-ID aus Befugnis1 3. Aufruf der VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

Regel	Beschreibung
rr5	<p>Mit dieser Regel werden die Befugnisse bei einem betreiberübergreifenden Anbieterwechsel im Aktensystem registriert.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU Befugnis1 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) signiert vom alten Aktensystembetreiber <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> Befugnis2 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> Prüfen der Befugnis1 <ol style="list-style-type: none"> prüfen der Signatur gemäß A_25042-* (C.FD.SIG) prüfen, ob im Signaturzertifikat C.FD.SIG der <u>policyIdentifierprofessionOID</u> oid_epa_vau ist prüfen, dass das Signaturzertifikat C.FD.SIG nicht auf das importierende Aktensystem ausgestellt ist. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 mit den Inhalten aus Befugnis1 erstellt. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 <ol style="list-style-type: none"> Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

2095

2096

2097

2098

2099

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

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

2100

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 **A_24691 - ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen von übers**
2107 **ePA-FdV erstellten Befugnissen**

2108 Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung einer von
2109 einem Versicherten bzw. Vertreter über das ePA-FdV eingestellten signierten Befugnis
2110 durchführen:

- 2111 • die Befugnis muss gemäß A_25042-* valide signiert sein durch einen Versicherten
2112 bzw. Vertreter (C.CH.SIG, professionOID ist `oid_versicherter`),
- 2113 • das JWT für die Befugnis gemäß A_24587-* darf nicht abgelaufen sein (Feld:
2114 `exp`),
- 2115 • das Feld `insurantID` des JWT muss eine KVN-R sein,
- 2116 • das Feld `actorID` des JWT muss eine KVN-R oder eine Telematik-ID sein,
- 2117 • das Feld `validTO` des JWT muss ein zeitliches Datum sein.

2118 **[<=]**

2119 Die folgenden Regeln dienen zum Abruf der versichertenindividuellen Daten- und
2120 Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel und
2121 die Ableitungsvorschriften sind in [gemSpec_Krypt] in Abschnitt 3.15.2 festgelegt.

2122 **Tabelle 7: Tab_AS_SDS-Key_Rules Key Rules - Regeln zur Ableitung der**
2123 **versichertenindividuellen Persistierungsschlüssel**

Regel	Beschreibung
kr1	<p><i>Diese Regel wird für die Anmeldung des Aktenkontoinhabers genutzt.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren). • Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren). • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys • versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys <p>Regelverhalten:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist oder prüfen des HSM-ID-Tokens b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. c. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel <code>hsm-r2</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVN-R aus dem ID-Token und den Labeln der zu verwendenden Befugnispersistierungs- und Datenpersistierungs-Masterkeys zur Ableitung von Befugnis- und Datenpersistierungsschlüssel aufgerufen. <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert die abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.

Regel	Beschreibung
kr2	<p><i>Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssel genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • KVNR (Aktenkonten-ID) • Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys • ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Aufruf der VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR und dem Label des Befugnispersistierungs-Masterkeys zur Ableitung des Befugnispersistierungsschlüssels <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 2. Das Befugnisverifikations-Modul liefert den abgeleiteten Befugnispersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.

kr3

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><i>Diese Regel wird für die Anmeldung des E-Rezept-Fachdienstes verwendet.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • KVNR (Aktenkonten-ID) • Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys • ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Prüfen des ID-Tokens <ol style="list-style-type: none"> a. prüfen der Signatur gemäß <u>Signaturgemäß</u> A_25042-* (C.FD.AUT) b. prüfen, ob die professionOID im Zertifikat C.FD.AUT gleich <code>oid_erp-vau</code> ist c. prüfen des ID-Tokens gemäß A_24658-* oder prüfen des HSM-ID-Tokens d. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. e. prüfen, ob die professionOID im HSM-ID-Token <code>oid_erp-vau</code> ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel <code>hsm-r2</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR aus dem ID-Token bzw. dem HSM-ID-Token und dem Label für den Datenpersistierungs-Masterkey zur Ableitung des Datenpersistierungsschlüssels aufgerufen. <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert den abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.

Regel	Beschreibung
kr5	<p><u>Diese Regel wird für die Überschlüsselung verwendet (ggf. mit Umschlüsselung einer Überschlüsselung).</u></p> <p><u>Diese Regel kann von einer VAU (AK-VAU oder dedizierte Überschlüsselungs-VAU) verwendet werden um verschlüsselte Akten zu überschlüsseln (vgl. Abschnitt 3.6- Umschlüsselung und Überschlüsselung). Dabei kann es auch zu einer Umschlüsselung einer älteren Überschlüsselung kommen.</u></p> <p><u>Sei <current> ein spezielles Symbol was im VAU-HSM durch das Label des jüngsten Überschlüsselungsschlüssel ersetzt wird. Ein Aufruf braucht so das tatsächliche Label nicht zu kennen. (Der Hersteller ist frei "<current>" durch ein selbstgewählten Symbolnamen zu ersetzen.)</u></p> <p><u>Eingangsdaten:</u></p> <ul style="list-style-type: none"> <u>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder ggf. einer dedizierten Überschlüsselungs-VAU</u> <u>KVNR (Aktenkonten-ID)</u> <u>Labelliste: nicht leere Liste von Label-n von Überschlüsselungs-Masterkeys</u> (im Regelfall enthält die Liste mindestens "<current>" als Element) <p><u>Ausgangsdaten:</u></p> <ul style="list-style-type: none"> <u>Liste von Paaren:</u> <u>versichertenindividueller Überschlüsselungsschlüssel (Secure Data Storage Key),</u> <u>Label für verwendeten Überschlüsselungs-Masterkey</u> <p><u>(Hinweis: Die Liste enthält mindestens ein Element -- im Fall der ersten Überschlüsselung in Intervall 2 (vgl. Abschnitt 3.6))</u></p> <p><u>Ablauf:</u></p> <p><u>Das VAU-HSM muss des VAU-Attestierungstoken prüfen, ob es sich um eine AK-VAU oder dedizierte Überschlüsselungs-VAU handelt. Falls nein, Abbruch.</u></p> <p><u>Das VAU-HSM durchläuft die Label-Liste und führt mit dem entsprechenden Label verbundenen Überschlüsselungs-Masterkey und der KVNR eine Schlüsselableitung durch. Dabei wird im VAU-HSM das spezielle Symbol "<current>" durch das Label des jüngsten Überschlüsselungs-Masterkeys vor Abarbeitung ersetzt.</u></p> <p><u>In der Ergebnisse (siehe Ausgangsdaten) ist "<current>" ebenfalls so ersetzt. Die Reihenfolge in der Eingangsliste muss in der Ausgabeliste gleich bleiben.</u></p>

2124

2125 3.5 Vertrauenswürdige Ausführungsumgebung (VAU)

2126 Eine Vertrauenswürdige Ausführungsumgebung (VAU) gewährleistet mit technischen
 2127 Maßnahmen, dass Daten serverseitig im ePA-Aktensystem im Klartext verarbeitet werden
 2128 können, ohne dass einzelne Mitarbeiter des Betreibers auf diese Daten zugreifen können.

2129 Die Datenverarbeitungen der Aktenkontoverwaltung müssen in einer VAU ausgeführt
2130 werden. Diese VAU wird im folgenden als Aktenkontoverwaltungs-VAU bezeichnet. Des
2131 weiteren kann das Befugnisverifikations-Modul in einer VAU ausgeführt werden. Diese
2132 VAU wird im folgenden als Befugnisverifikations-VAU bezeichnet.

2133 **A_25716-01 - ePA-Aktensystem - Services ausschließlich in der VAU**

2134 Das ePA-Aktensystem MUSS sicherstellen, dass die folgenden Services ausschließlich
2135 innerhalb einer VAU ausgeführt werden können und ein Zugriff auf die Schnittstellen
2136 ausschließlich über einen VAU-Kanal erfolgen kann:

- 2137 • Consent Decision Management Service
- 2138 • Entitlement Management
- 2139 • Constraint Management
- 2140 • Device Management
- 2141 • E-Mail Management
- 2142 • Audit Event Service
- 2143 • Authorization Service
- 2144 • Health Record Relocation Service
- 2145 • alle Medical Services
- 2146 • Data Submission Service.

2147 [**<=**]

2148 In den folgenden Abschnitten werden zunächst die Anforderungen an eine VAU
2149 beschrieben, die sowohl von einer Aktenkontoverwaltungs-VAU als auch
2150 einer Befugnisverifikations-VAU zu erfüllen sind. Die speziellen Anforderungen an eine
2151 Aktenkontoverwaltungs-VAU bzw. an eine Befugnisverifikations-VAU folgen darauf in
2152 separaten Abschnitten.

2153 **3.5.1 Übergreifende VAU-Anforderungen**

2154 **3.5.1.1 Schutz der Integrität der VAU**

2155 Die folgenden Anforderungen stellen die Integrität der VAU sicher.

2156 **A_24613 - ePA-Aktensystem - Bildung Hashwertrepräsentation des VAU-Images**

2157 Der Hersteller des VAU-Images MUSS für seine zugelassenen VAU-Images
2158 Hashwertrepräsentationen bilden. Diese MÜSSEN signiert und die signierten
2159 Hashwertrepräsentationen an die gematik übermitteln. Dabei SOLLEN bezüglich der
2160 kryptographischen Vorgaben zur Signatur die Vorgaben aus [gemSpec_Krypt]
2161 eingehalten werden.
2162 [**<=**]

2163 Erläuterung zu A_24613-*:

2164 Bei Intel-SGX sind die durch die Intel-Hardware erzeugten Signaturen RSA-3072-Bit-
2165 Signaturen, bei denen der öffentliche Exponent 3 ist. Dies entspricht nicht den Vorgaben
2166 in [gemSpec_Krypt] für allgemeine RSA-Signaturen (also nicht im SGX-Kontext). Deshalb
2167 steht in A_24613-* diesbezüglich nur eine SOLL-Formulierung. Im Kontext SGX ist der
2168 öffentliche RSA-Exponent 3 zulässig.

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

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

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

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

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

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

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

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

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

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

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

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

3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU

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

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

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

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

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

2214 **A_24651 - ePA-Aktensystem - Betreiber ergreift Maßnahmen gegen physische**
 2215 **Angriffe auf die VAU**

2216 Der Betreiber des ePA-Aktensystems MUSS mit technischen und/oder organisatorischen
 2217 Maßnahmen ausschließen, dass ein einzelner Innentäter beim Betreiber des ePA-
 2218 Aktensystems physische Angriffe auf eine VAU ausführen kann. [\leq]

2219 **A_24641 - ePA-Aktensystem - Löschen aller Daten beim Beenden einer VAU-**
 2220 **Instanz**

2221 Das ePA-Aktensystem MUSS sicherstellen, dass beim Beenden einer VAU-Instanz
 2222 sämtliche Daten dieser VAU-Instanz aus flüchtigen Speichern sicher gelöscht werden
 2223 oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [\leq]

2224 **A_25244 - ePA-Aktensystem - x-insurantId nicht außerhalb des VAU-Kanals**

2225 Das ePA-Aktensystem MUSS sicherstellen, dass das HTTP Header-Element mit dem
 2226 Namen "x-insurantId" nicht außerhalb des VAU-Kanals gesendet wird. [\leq]

2227 **3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU**

2228 **A_26314 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU**
 2229 **gespeicherten Daten**

2230 Das ePA-Aktensystem MUSS sicherstellen, dass eine VAU-Daten, die im System des
 2231 Aktensystembetreibers gespeichert werden sollen und für die keine spezifischen
 2232 Anforderungen zum Schutz der gespeicherten Daten existieren, ausschließlich
 2233 verschlüsselt gespeichert werden und der verwendete Verschlüsselungsschlüssel mittels
 2234 der Regel hsm-r8 vom VAU-HSM abgeleitet wird. [\leq]

2235 Hinweise zu A_26314:

- 2236 • Spezifische Anforderungen zum Schutz der gespeicherten Daten gibt es z.B. für
 2237 die Aktenkontoverwaltungs-VAU in Abschnitt 3.5.2.2 und die durch die VAU für
 2238 den Betrieb erstellten Protokolle in Abschnitt 3.5.1.5.
- 2239 • Außerhalb der VAU verschlüsselt gespeicherte Daten der ePA3.0, die bisher nicht
 2240 mit Regel hsm-r8 verschlüsselt sein konnten, sind beim Öffnen der Akte
 2241 umzuschlüsseln und mit einem Schlüssel zu sichern, der mit Regel hsm-r8
 2242 abgeleitet wird. Eine Umschlüsselung ohne Öffnen der Akte ist nicht erforderlich.

2243 **A_26322 - ePA-Aktensystem - Unterschiedliche Schlüssel für die**
 2244 **Verschlüsselung von außerhalb der VAU gespeicherten Daten bei**
 2245 **unterschiedlichen Verarbeitungszwecken**

2246 Falls Daten außerhalb der VAU im System des Aktensystembetreibers gespeichert
 2247 werden, MUSS das ePA-Aktensystem sicherstellen, dass für die Verschlüsselung von
 2248 Daten, die zu unterschiedlichen Zwecken verarbeitet werden, unterschiedliche
 2249 Verschlüsselungsschlüssel genutzt werden. [\leq]

2250 Hinweis zu A_26322: Verarbeitungszwecke für Daten ist beispielsweise sind beispielsweise
 2251 die Verarbeitung von Daten zum Zwecke der Sekundärnutzung (siehe Data Submission
 2252 Service) oder die Verarbeitung von Daten für die Nutzerverwaltung im Aktensystem
 2253 (insbesondere Geräteinformationen und E-Mail-Adressen).

2254 **3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM**

2255 **A_24653 - ePA-Aktensystem - Sichere Verbindung zwischen VAU und VAU-HSM**

2256 Das ePA-Aktensystem MUSS technisch sicherstellen, dass zwischen einer VAU und einem
 2257 VAU-HSM eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die
 2258 vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des
 2259 Betreibers des Aktensystems schützen. [\leq]

3.5.1.5 Logging und Monitoring

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

A_24910 - ePA-Aktensystem - Erlaubte Zwecke der Betreiberprotokolle

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

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

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

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

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

[\leq]

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

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

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

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

A_24911 - Löschfristen Protokolle

Das ePA-Aktensystem MUSS sicherstellen, dass die

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

[\leq]

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

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

gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik

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

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

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

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

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

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

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

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

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

3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU

3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU

A_24636-01A_24636 - ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen innerhalb einer VAU-Instanz

Das ePA-Aktensystem MUSS durch ~~einen technischen Separationsmechanismus~~ ausschließend technische Maßnahmen sicherstellen, dass ~~sich~~ innerhalb einer VAU-Instanz zwischen Health Record Contexten bzw. User Sessions keine Informationsflüsse auftreten können. [\leq]

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

Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass innerhalb einer VAU-Instanz ~~von einem die Verarbeitungen eines Health Record Context oder einer User Session~~ schadhaft auf die Verarbeitungen eines anderen Health Record Context oder einer anderen bzw. einer User Sessions nicht auf den Speicher anderer Health Record Contexte bzw. User Sessions zugegriffen werden kann. [\leq ~~Session auswirken können.~~]

~~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_27535 - ePA-Aktensystem – Maximale Lebensdauer von VAU-Instanzen

Das ePA-Aktensystem MUSS sicherstellen, dass VAU-Instanzen einer Aktenkontoverwaltungs-VAU, die länger als 4 Stunden laufen, keine neuen Verbindungen von Clients zulassen dürfen. [\leq]

A_27536 - ePA-Aktensystem – Beenden von leeren und nicht mehr nutzbaren VAU-Instanzen

Das ePA-Aktensystem MUSS leere VAU-Instanzen einer Aktenkontoverwaltungs-VAU beenden, die keine neuen Verbindungen von Clients gemäß A_27535-* mehr zulassen dürfen.

[<=]

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

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

[<=]

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

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

[<=]

A_25028 - ePA-Aktensystem - Keine Kommunikation zwischen Aktenkontoverwaltungs-VAUs

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

A_26111 - ePA-Aktensystem - Keine Kommunikation zwischen Health Record Contexts

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

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

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

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

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

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

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

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

A_25051 - ePA-Aktensystem - VAU-Kanal endet immer in einer Aktenkontoverwaltungs-VAU

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

2405 Hinweis: Der VAU-Kanal darf z.B. nicht in einer Befugnisverifikations-VAU enden.

2406 **3.5.2.2 Schutz der Daten bei Speicherung außerhalb der** 2407 **Aktenkontoverwaltungs-VAU**

2408 Die folgenden Anforderungen gewährleisten den Schutz der beim Betreiber des ePA-
2409 Aktensystems persistierten Daten von Aktenkonten. Die Verschlüsselung der Daten eines
2410 Versicherten erfolgt mit seinem versichertenindividuellen Daten- und
2411 Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel sind
2412 in [gemSpec_Krypt#3.15.2] festgelegt.

2413 **A_24643 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU** 2414 **gespeicherten Daten mit dem Datenpersistierungsschlüssel**

2415 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten

- 2416 1. Daten des FHIR-Data Service
- 2417 2. Daten des XDS Document Service
- 2418 3. Daten des Audit Event Service (Protokolle für den Versicherten zum Zwecke der
2419 Datenschutzkontrolle)
- 2420 4. Daten des Constraint Managements (Policies zu verborgenen Daten)
- 2421 5. Daten des Consent Managements (Widersprüche des Versicherten)

2422 vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb
2423 des Health Record Context mit dem zum Health Record gehörenden
2424 versichertenindividuellen Datenpersistierungsschlüssel verschlüsselt werden.
2425 [\leq]

2426 **A_24644 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU** 2427 **gespeicherten Befugnissen mit dem Befugnispersistierungsschlüssel**

2428 Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten
2429 Daten des Entitlement Managements, d. h. Befugnisse und Befugnisverbote, vor der
2430 Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health
2431 Record Context mit dem zum Health Record gehörenden versichertenindividuellen
2432 Befugnispersistierungsschlüssel verschlüsselt werden. [\leq]

2433 **3.5.2.3 Konsistenz des Systemzustands**

2434 **A_24650 - ePA-Aktensystem - Konsistenter Systemzustand eines Health Record** 2435 **Context**

2436 Die VAU MUSS sicherstellen, dass ein konsistenter Zustand eines Health Record Context
2437 auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw.
2438 wiederhergestellt werden kann. [\leq]

2439 **A_24696 - ePA-Aktensystem - Konsistenz bei parallelen Zugriffen**

2440 Die VAU MUSS auch bei parallelen Zugriffen auf dasselbe Aktenkonto durch mehrere
2441 Nutzer immer einen konsistenten Zustand des Aktenkontos gewährleisten. [\leq]

2442 **3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-** 2443 **VAU**

2444 Eine Befugnisverifikations-VAU ist eine spezielle VAU, in der ausschließlich das
2445 Befugnisverifikations-Modul ausgeführt wird.

2446 **A_24646 - ePA-Aktensystem - Befugnisverifikations-VAU verarbeitet**
2447 **ausschließlich ein Befugnisverifikations-Modul**

2448 Das ePA-Aktensystem MUSS sicherstellen, dass in einer Befugnisverifikations-VAU
2449 ausschließlich ein Befugnisverifikations-Modul ausgeführt wird. [<=]

2450 **A_24647 - ePA-Aktensystem - Befugnisverifikations-VAU speichert keine Daten**

2451 Eine Befugnisverifikations-VAU DARF die Daten, die sie im Rahmen der Regeln des
2452 Befugnisverifikations-Moduls verarbeitet, NICHT außerhalb der Befugnisverifikations-VAU
2453 speichern. [<=]

2454 Eine Befugnisverifikations-VAU darf insbesondere die vom VAU-HSM abgeleiteten
2455 versichertenindividuellen Persistierungsschlüssel nicht speichern.

2456 **A_24648 - ePA-Aktensystem - Befugnisverifikations-VAU löscht Daten nach**
2457 **Regelbearbeitung**

2458 Eine Befugnisverifikations-VAU MUSS sämtliche Daten, die sie im Rahmen eines
2459 Regelaufrufs des Befugnisverifikations-Moduls verarbeitet, sofort nach Abarbeitung der
2460 Regel sicher aus der Befugnisverifikations-VAU löschen bzw. einen Zugriff auf diese
2461 Daten technisch ausschließen. [<=]

2462 **A_24671 - ePA-Aktensystem - Sichere Verbindung zwischen VAU-Instanzen**

2463 Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer VAU-Instanz einer
2464 Befugnisverifikations-VAU und einer VAU-Instanz einer Aktenkontoverwaltungs-VAU eine
2465 beidseitig authentifizierte und vertrauliche Verbindung besteht. Die vertrauliche
2466 Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des
2467 Aktensystems schützen. [<=]

2468 **A_24856 - ePA-Aktensystem - Private Authentisierungsschlüssel für sichere**
2469 **Verbindung zwischen VAU-Instanzen**

2470 Das ePA-Aktensystem MUSS sicherstellen, dass sich die VAU-Instanzen bei einer
2471 Verbindung zwischen einer VAU-Instanz einer Befugnisverifikations-VAU und einer VAU-
2472 Instanz einer Aktenkontoverwaltungs-VAU mit privaten Schlüsseln authentisieren, die
2473 ausschließlich über die jeweilige VAU-Instanz nutzbar sind. [<=]

2474 **3.5.4 Zusätzliche Anforderungen an eine Service-VAU**

2475 Spezielle Funktionen der "ePA für alle" können in eigenen, von den
2476 Aktenkontoverwaltungs-VAUs (AK-VAU) getrennten, VAUs ausgelagert und ausgeführt
2477 werden. Diese VAUs werden als **Service-VAUs** bezeichnet. Es kann Service-VAUs für
2478 unterschiedliche Funktionen geben, so dass es dementsprechend unterschiedliche **Typen**
2479 **von Service-VAUs** geben kann.

2480 Service-VAU-Instanzen können durch den Betreiber des Aktensystems gestartet und in
2481 einem Pool verwaltet werden. AK-VAU-Instanzen können bei Bedarf auf Service-VAU-
2482 Instanzen zugreifen, wenn sie den Service nutzen möchten (in Abbildung 2 mit Service A
2483 dargestellt), Ein Kommunikationsaufbau von Service-VAU-Instanzen zu AK-VAU-
2484 Instanzen ist nicht möglich.

2485 Eine Service-VAU-Instanz kann von mehreren AK-VAU-Instanzen gleichzeitig genutzt
2486 werden (die Service-VAU-Instanz zu AK-VAU-Instanz-Beziehung ist eine n:m-Beziehung).

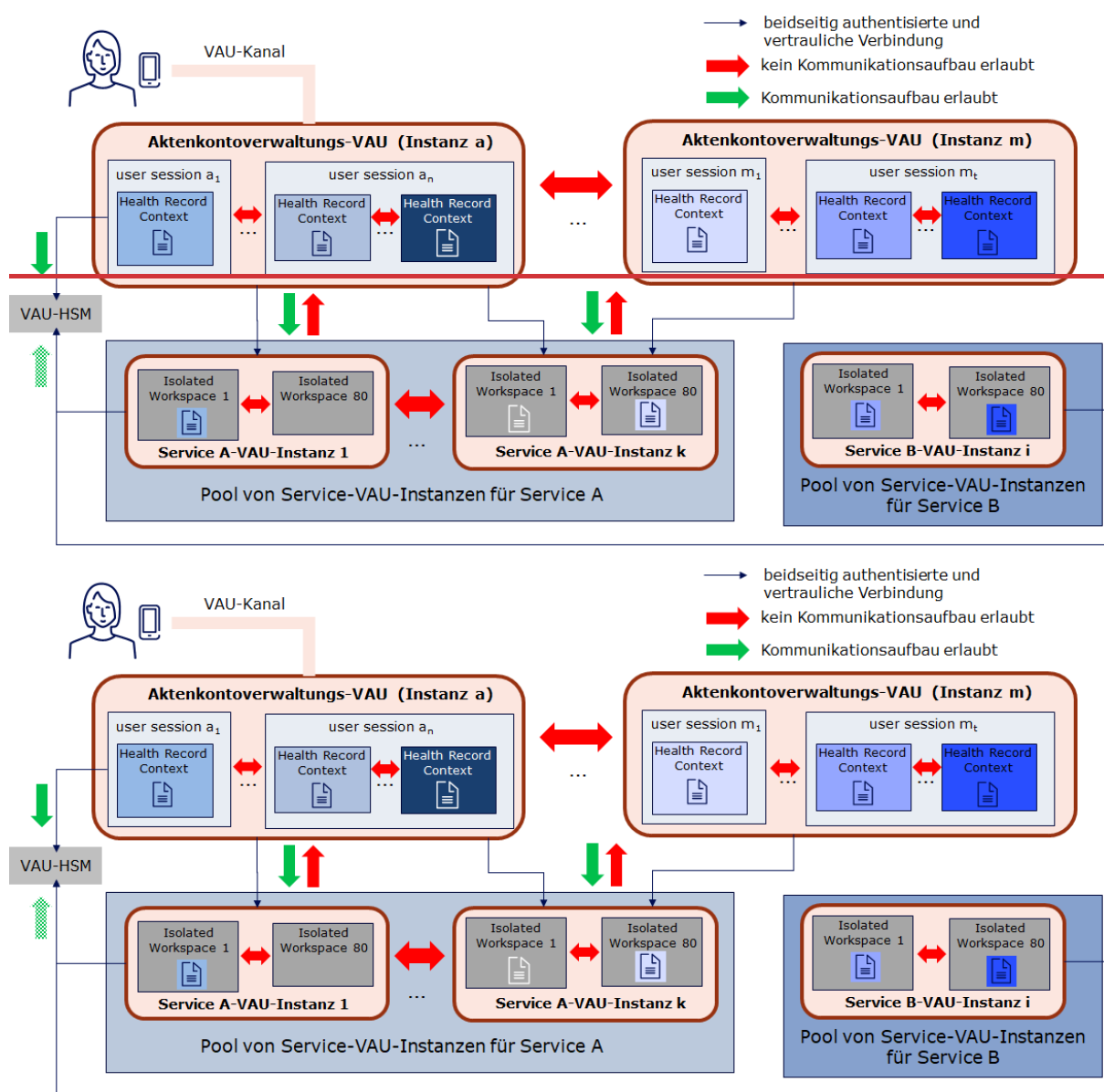


Abbildung 2 - Überblick Service-VAUs

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

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

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

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

Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus ausschließen technische Maßnahmen sicherstellen, dass sich innerhalb einer Service-VAU-Instanz die Verarbeitungen eines zwischen Isolated Workspaces schadhaft auf die Verarbeitungen eines anderen Isolated Workspaces auswirken keine Informationsflüsse

auftreten können.

[<=]

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

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

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

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

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

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

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

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

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

A_26117 - ePA-Aktensystem - Keine Kommunikation zwischen Isolated Workspaces

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.6 Umschlüsselung und Überschlüsselung

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

- Schlüssel alt KVNR = Ableitung (MK alt, KVNR),
- Schlüssel neu KVNR = Ableitung (MK neu, KVNR),
- Umschlüsselung pro Akte: Schlüssel alt KVNR -> Schlüssel neu KVNR.

Falls eine AK-VAU Zugriff auf eine Akte besitzt und zu diesem Zeitpunkt feststellt neue Masterkeys (vgl. betreiberspezifische Schlüssel A_15745-*) existieren, muss sie eine Umschlüsselung durchführen (A_20519-*). Falls eine Akte länger nicht verwendet wird, kann eine AK-VAU keinen Zugang zu den Klartexten der Akte erhalten, da sie nur nach erfolgreicher Nutzerauthentisierung vom VAU-HSM die aktenspezifischen

Ableitungsschlüssel erhält. Dann kann eine AK-VAU zunächst auch keine Umschlüsselung vornehmen. Aus diesem Grunde muss eine VAU (entweder eine AK-VAU oder eine dedizierte Überschlüsselungs-VAU) eine Überschlüsselung der Chiffre der Akte vornehmen. Dafür werden Überschlüsselungsschlüssel benötigt. Es gibt analog zu den anderen betreiberspezifischen Schlüssel (A 15745-*) Masterkeys für eine Schlüsselableitung für die Überschlüsselung der Chiffre einer Akte.

A 26197 - ePA-Aktensystem - betreiberspezifische Schlüssel: Überschlüsselungs-Masterkeys

Ein ePA-Aktensystem MUSS sicherstellen, dass die Menge der betreiberspezifischen Schlüssel aus [gemSpec Krypt#A 15745-*] um die Kategorie Überschlüsselungs-Masterkeys erweitert wird. Für die Überschlüsselungsschlüssel MÜSSEN die gleichen Vorgaben wie für alle betreiberspezifischen Schlüssel gemäß A 15745-* gelten. Die betreiberspezifischen Schlüssel werden mindestens jährlich aktualisiert (A 20519-*), die alten Schlüssel MÜSSEN solange im VAU-HSM verfügbar sein, solange Chiffre im Aktensystem existieren (bspw. Daten einer Akte), die mit diesen Schlüsseln kryptographisch gesichert sind. [≤]

D. h. wie in Abschnitt 3.3 (bspw. A 24611-*) definiert, gibt es bei den Masterkeys drei Kategorien: (1) Aktenpersistierung, (2) Befugnispersistierung und (3) Überschlüsselung. Initial startet der Betrieb eines Aktensystems mit je einem Schlüssel in den ersten zwei Kategorien. Nach maximal einem Jahr (A 20519-*), oder anders formuliert im nächsten Intervall, werden diese beiden ersten Schlüssel zufällig neu erzeugt. Dabei muss nun ein neuer Überschlüsselungsmasterkey erzeugt werden. Die Anzahl der Schlüssel nach o. g. Kategorie ist anschließend (1) 2, (2) 2, (3) 1.

A 26198 - ePA-Aktensystem - neuer Überschlüsselungsschlüssel bei Erneuerung betreiberspezifischen Schlüssel

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

Bei einer Erneuerung der betreiberspezifischen Schlüssel gibt es verschiedene Zeitabschnitte:

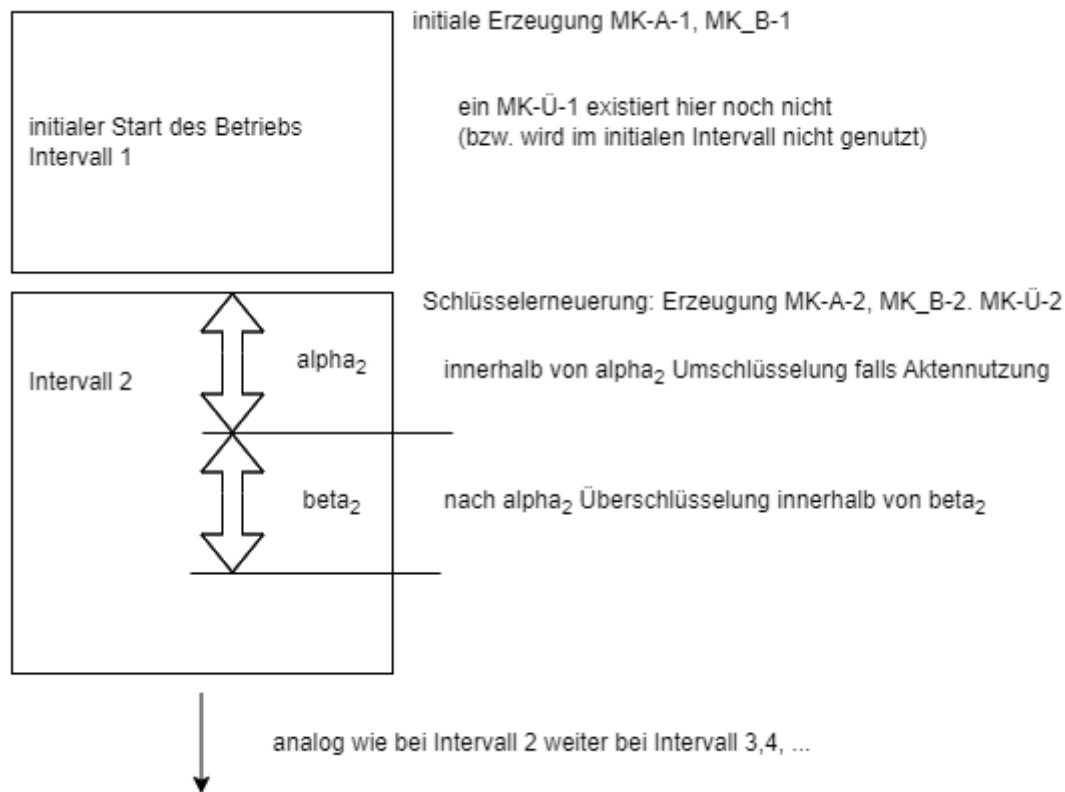


Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung

A 26204 - ePA-Aktensystem - zeitliche Vorgaben zur Durchführung der Umschlüsselung und Überschlüsselung

Ein ePA-Aktensystem MUSS sicherstellen, dass es ein konfigurierbares Zeitintervall α gibt, so dass nach einer Schlüsselerneuerung der betreiberspezifischen Schlüssel innerhalb von α bei einer Aktennutzung eine Umschlüsselung in einer AK-VAU vorgenommen wird, falls die Verschlüsselung der Akte auf einem älteren Masterkey basiert. Das Zeitintervall α startet jeweils direkt mit jedem neuen Intervall (Schlüsselerneuerung der betreiberspezifischen Schlüssel). Weiter MUSS es sicherstellen, dass es ein konfigurierbares Zeitintervall β gibt beginnend direkt nach α , so dass nach ablaufen von α eine Überschlüsselung von Chiffren von Akten, bei denen keine Umschlüsselung (wegen Nichtaktennutzung innerhalb von α) durchgeführt werden konnte, vorgenommen wird.

Der Default-Wert für die Länge von α MUSS 100 Tage und für die Länge von β 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 Überschlüsselung entschlüsseln und die nun verfügbare 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. [\leq]

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. [\leq]

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.

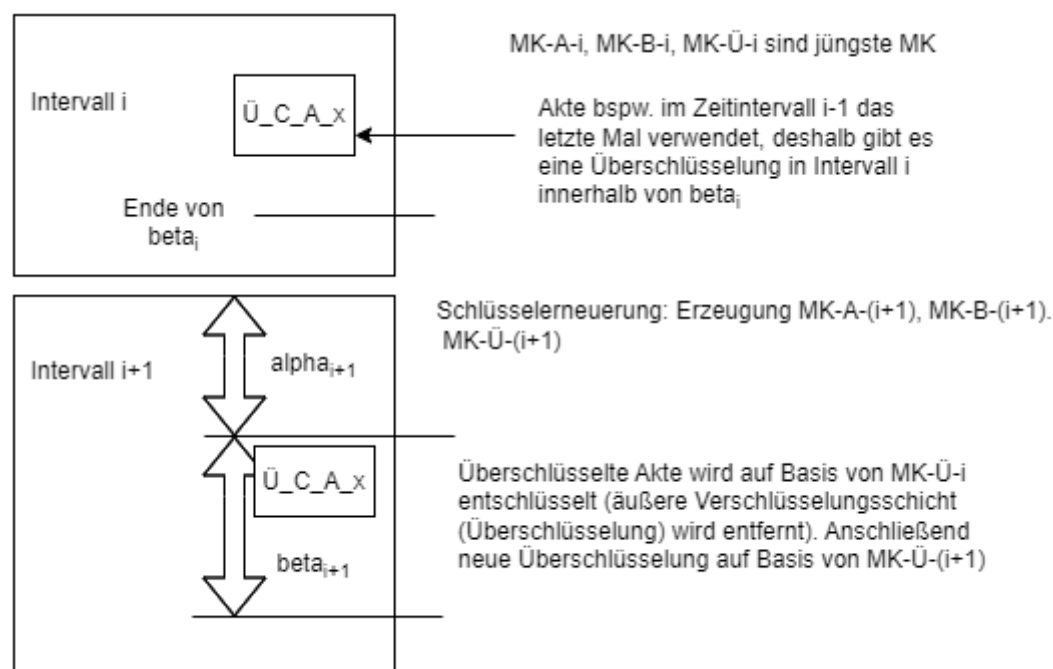


Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer Überschüsselung

A 26208 - ePA Aktensystem - Umschlüsselung einer Überschlüsselung

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

[<=]

Sollte durch irgendeinen Umstand die Sicherheitseigenschaft der Betreiberschlüssel (A 15745-*) in Frage stehen, so muss ein Aktensystembetreiber die Umschlüsselung bzw. die Überschlüsselung aktivieren/starten können.

A 26199 - ePA-Aktensystem - Notfall-Aktivierung Umschlüsselung/Überschlüsselung

Ein ePA-Aktensystem MUSS sicherstellen, dass das ePA-Aktensystem es einem ePA-Betreiber ermöglicht eine Erneuerung der betreiberspezifischen Schlüssel zu starten/aktivieren. Es MUSS also dem ePA-Betreiber möglich sein neben der regelmäßigen Erneuerung der betreiberspezifischen Schlüssel (A 205019-*) eine Erneuerung zu initiieren.

[<=]

Nach A 20519-* muss es mindestens jährlich eine Schlüsselerneuerung geben. Mit 26199-* kann ein ePA-Betreiber im Notfall sozusagen den Zyklus "beschleunigen" -- ein neues Intervall sofort einleiten/erzeugen.

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

A 26223 - ePA-Aktensystem - Metadaten von ePA-spezifischen Chiffren

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

3-63.7 User Session und Health Record Context

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

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

2733 Wird durch den ePA-Client eine Operation für eine bestimmte Akte aufgerufen (Parameter
 2734 x-insurantid) der Operation, wird in der User Session geprüft, ob diese Akte schon
 2735 verwendet wird (ein anderer Nutzer gerade mit der Akte arbeitet) oder nicht. Sollte die
 2736 Akte noch nicht verwendet werden, wird die Akte in einem Health Record Context
 2737 geöffnet und kann durch den ePA-Client in dessen User Session verwendet werden.
 2738 Existiert für die Akte schon ein geöffneter Health Record Context, darf es durch den
 2739 parallelen Zugriff zu keinen Inkonsistenzen in der Akte kommen.

2740 Innerhalb einer VAU-Instanz dürfen nur eine maximale Anzahl von Health Record
 2741 Contexts gleichzeitig aufgebaut sein. Sollte diese Anzahl überschritten werden, wird der
 2742 am längsten nicht genutzte Health Record Context geschlossen, um einen neuen Health
 2743 Record Context öffnen zu können.

2744 **3.7.3.8 Consent Decision Management**

2745 Das Consent Decision Management des Aktensystems verwaltet die Entscheidungen eines
 2746 Versicherten oder eines Vertreters für oder gegen die Nutzung von definiert
 2747 widerspruchsfähigen Funktionen gemäß gesetzlicher Vorgaben.

2748

2749 Außerdem werden im Consent Decision Management die Einschränkungen der
 2750 Verwendung von Daten auf bestimmte Sekundärnutzungszwecke durch das
 2751 Forschungsdatenzentrum Gesundheit verwaltet (siehe 3.8.2- Einschränkung der
 2752 Verwendung von Daten auf bestimmte Sekundärnutzungszwecke).

2753 Der Widerspruch gegen die grundsätzliche Nutzung der ePA wird nicht im Consent
 2754 Decision Management berücksichtigt. Die Existenz eines Aktenkontos für einen
 2755 Versicherten impliziert, dass kein Widerspruch gegen die Nutzung der ePA erteilt wurde.
 2756 Der Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger
 2757 wird ebenfalls nicht hier verwaltet (siehe zu beiden Widersprüchen auch 3.1.1-
 2758 Widerspruch des Versicherten gegen die Nutzung der elektronischen
 2759 Patientenakte).3.1.1- Widerspruch des Versicherten gegen die Nutzung der
 2760 elektronischen Patientenakte).

2761 **3.7.13.8.1 Widersprüche für Funktionen der ePA**

2762 Die vorgehaltenen Entscheidungen zu einer Funktion umfassen dabei den Zustand "kein
 2763 Widerspruch erklärt" ("permit") oder "Widerspruch erklärt" ("deny") und den Kontext
 2764 einer Funktion. Der Kontext ordnet dabei die einzelnen widerspruchsfähigen Funktionen
 2765 einem für die Umsetzung des Widerspruchs betroffenen Nutzerkreis zu und wird bei den
 2766 zugreifenden Schnittstellen zur Filterung der Ausgabe verwendet.

2767 Initial, also bei der Erstellung eines neuen Aktenkontos oder bei Übernahme eines
 2768 existierenden ePA 2.x Aktenkontos, ist für keine widerspruchsfähige Funktion ein
 2769 Widerspruch gegen die Nutzung erklärt. Ein Versicherter oder ein Vertreter kann im
 2770 Verlauf der Nutzung des Aktenkontos aktiv der Verwendung von widerspruchsfähigen
 2771 Funktionen widersprechen oder einen erteilten Widerspruch zurücknehmen.

2772 Die aktuell erteilten Widersprüche können durch einen Versicherten oder einen Vertreter
 2773 jederzeit über ein ePA-FdV eingesehen und geändert werden. Versicherte und Vertreter,
 2774 die ein ePA-FdV nicht nutzen möchten, können eine Auskunft über die aktuell erteilten
 2775 Widersprüche über die Ombudsstelle erhalten und dort auch Änderungen an den
 2776 Entscheidungen im Aktenkonto veranlassen. Die Ansicht oder Änderung der
 2777 Widersprüche erfolgt im Aktenkonto stets gesichert innerhalb der VAU, die aktuellen

Entscheidungen zu den widerspruchsfähigen Funktionen der ePA sind versichertenindividuell mit dem SecureDataStorageKey verschlüsselt abgelegt.

Die Information über relevante erteilte oder nicht erteilte Widersprüche können Clients auf einfache Weise (ohne Authentisierung oder Etablierung eines VAU-Kanals) im Vorfeld einer Operation über den Information Service abfragen (siehe auch [3.14.15- Information Service](#)).

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

Das Aktenkonto unterstützt die Durchsetzung eines erteilten Widerspruchs überall dort, wo Aktivitäten dediziert als Teil einer widerspruchsfähigen Funktion zugeordnet werden können. Beispielsweise wird das Einstellen neuer Verordnungs- und Dispensierdaten in die Ordner der Kategorie "medication" immer verhindert, wenn der Teilnahme am digital gestützten Medikationsprozess widersprochen wurde. Die konkreten Auswirkungen eines Widerspruchs sind in den jeweiligen Kapiteln zur Handhabung von Dokumenten und Daten des Aktenkontos dargestellt (siehe [3.12.1- XDS Document Service](#) und [3.12.2- FHIR Data Services](#)) - [3.13.1- XDS Document Service](#) und [3.13.2- FHIR Data Services](#))

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

A 23874-01A-23874 - Consent Decision Management - Definition der widerspruchsfähigen Funktionen der ePA

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

Tabelle 8: Widerspruchsfähige Funktionen der elektronischen Patientenakte

Funktion (name)	Funktionsklasse (consent class)	Id der Funktion (id)	Entscheidung (consent decision)
Teilnahme am digital gestützten Medikationsprozess	Versorgungsprozess ("healthcareProcess")	"medication"	"deny"/"permit"
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst	Versorgungsprozess ("healthcareProcess")	"erp-submission"	"deny"/"permit"
Sekundärdatennutzung durch das Forschungsdatenzentrum Gesundheit	Sekundärdatennutzung ("secondaryDataUsage")	"data-submission"	"deny"/"permit"

[<=]

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

Hinweis: Die Verwaltung der Widersprüche gegen die Nutzung des Aktenkontos durch eine spezifische Leistungserbringerinstitution erfolgt über die Befugnisverwaltung (siehe ~~3.8.4- Befugnisausschluss (Blocked User Policy)~~ 3.9.4- Befugnisausschluss (Blocked User Policy)).

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

A_25300 - Consent Decision Management - Untereinander abhängige Entscheidungen zu Widersprüchen

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

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

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

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

A_24343 - Consent Decision Management - Speichern der Inhalte

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

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

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

- Versorgungsprozess ("healthCareProcess")

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

[\leq]

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

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

- Versorgungsprozess ("healthCareProcess")

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

[<=]

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** `±SchnittstelleI_Information_Service`.

A_23824 - Aktensystem - Realisierung der Schnittstelle

I_Consent_Decision_Management

Das ePA-Aktensystem MUSS die Operationen der Schnittstelle

`I_Consent_Decision_Management` gemäß `[I_Consent_Decision_Management]` umsetzen. [≤]

A_23919 - Consent Decision Management - unveränderte Übernahme der Widerspruchsentscheidung

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

A_24844 - Consent Decision Management - Information über Änderungen der Widerspruchsinformation

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

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 9: Consent Decision Management Protokollierung - Widersprüche für Funktionen der ePA

Strukturelement	Wert	Erläuterung
AuditEvent.action	U	Update

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

[<=]

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

A 26293 - 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 10: Consent Decision Management Protokollierung - Widersprüche zu Sekundärnutzungszwecken

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

[<=]

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

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

Die User Specific Deny Policy Medication wird durch das Aktensystem für die in A_26406-
* aufgeführten Nutzergruppen angewendet und durchgesetzt.

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

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

Das Consent Decision Management MUSS für ein Aktenkonto eine User Specific Deny Policy Medication ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policy über die Schnittstelle I Consent Decision Management gemäß

[I Consent Decision Management] ermöglichen.[<=]

2990 **A_26401 - Consent Decision Management - Speichern der Inhalte der User**
 2991 **Specific Deny Policy Medication**

2992 Das Consent Decision Management MUSS Einträge aus der User Specific Deny Policy
 2993 Medication unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto
 2994 ablegen. [<=]

2995 **A_26403 - Consent Decision Management - Information über Änderungen der**
 2996 **User Specific Deny Policy Medication**

2997 Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung der
 2998 Entscheidungen zu der User Specific Deny Policy Medication , sofern eine E-Mail-Adresse
 2999 vorliegt, mit einer E-Mail darüber informieren, welche Änderungen der User Specific Deny
 3000 Policy Medication vorgenommen wurden, wann die Änderung erfolgte und darauf
 3001 hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind. [<=]

3002 **A_26406 - Consent Decision Management - Policy für berechnigte**
 3003 **Nutzergruppen und Nutzer**

3004 Das Consent Decision Management MUSS die Konfiguration der User Specific Deny Policy
 3005 Medication auf die folgenden Nutzergruppen einschränken:
 3006

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

Nutzergruppe [professionOID] der User Specific Deny Policy Medication

oid_praxis-ernaehrungstherapeut

[<=]

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

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

Tabelle 11: Consent Decision Management Protokollierung - User Specific Deny Policy Medication

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

[<=]

3-83.9 Entitlement Management

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

Eine Befugnis enthält folgende Informationen:

3026 **A_23734-01 - Entitlement Management - Definition einer Befugnis**
3027 Das Entitlement Management MUSS für eine individuelle Befugnis die folgenden Daten
3028 nutzen und verwalten:

3029 **Tabelle 12: Inhalt einer Befugnis**

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

Element	Inhalt	Anmerkung	signiertes Element (*)
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

3030 **[<=]**

3031 *Hinweis: Ein Nutzer ist der Adressat, für den die Befugnis ausgestellt wird. Der Ersteller*
 3032 *ist der Nutzer, welcher die Befugnisausstellung veranlasst hat. Die Bezeichner in () sind*
 3033 *die Bezeichner in den Schnittstellenbeschreibungen.*

3034 *Hinweis (*): A_23734 definiert eine "vollständige" Befugnis, welche auch Daten enthält,*
 3035 *die für eine Prüfung einer gültigen Befugnis im Kontext einer Schnittstellenoperation*
 3036 *nicht notwendig sind. Für diesen Zweck wird nur der (HSM-) signierte Anteil als Ergebnis*
 3037 *einer Befugnisverifikation verwendet (signiertes Element = ja). Eine gespeicherte*
 3038 *Befugnis enthält jedoch alle Elemente für eine qualifizierte Verwaltung der Befugnisse*
 3039 *durch einen Versicherten oder Vertreter.*

3040 *Hinweis: Befugnisse können durch das Aktensystem selbst (initiale Befugnisse), durch*
 3041 *den Versicherten oder einen befugten Vertreter unter Verwendung eines ePA-FdV oder*
 3042 *durch eine Leistungserbringerinstitution in einer Behandlungssituation erstellt werden.*

3043 Eine Befugnis kann nur für Nutzer und Nutzergruppen mit bestimmter Rolle erteilt
 3044 werden. Nutzergruppen mit abweichenden Rollen können nicht befugt werden und
 3045 erhalten keinen Zugriff auf das Aktenkonto.

3046 Erfolgt die Befugniserteilung durch eine Leistungserbringerinstitution in einer
 3047 Behandlungssituation, wird eine vorgegebene Gültigkeitsdauer der Rolle des Befugten
 3048 entsprechend durch das Entitlement Management vergeben. Ein Versicherter oder ein
 3049 befugter Vertreter kann den Gültigkeitszeitraum frei wählen (ausgenommen
 3050 Vertreterbefugnisse).

3051 **A_23941-01 - Entitlement Management - Erteilung von Befugnissen für** 3052 **berechtigte Nutzergruppen und Nutzer**

3053 Das Entitlement Management MUSS die Erteilung von Befugnissen in der jeweiligen
 3054 Umgebung auf die folgenden Nutzergruppen und Nutzer einschränken:

3055 **Tabelle 13: Befugnisse für berechtigte Nutzergruppen und Nutzer**

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

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_ombudsstelle	-	-	x (statisch)	-	-
oid_erp-vau (E-Rezept vertrauenswürdige Ausführungsumgebung)	-	-	x (statisch)	-	-
oid_versicherter (Versicherter)	-	-	x (statisch)	-	-
oid_versicherter (Vertreter)	-	x	-	-	dauerhaft
oid_diga	-	x	-	-	dauerhaft

Hinweis:

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

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

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

FdV = Versicherter oder Vertreter,

KTR = Kostenträger

AS = Aktensystem (systemseitig erteilte Befugnisse)

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

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

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

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

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

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

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

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

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

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

Tabelle 14: Befugnisse EU-Zugriff für berechnigte Nutzergruppen und Nutzer

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

Hinweis:

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

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

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

FdV = Versicherter oder Vertreter,

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

A_24371 - Entitlement Management - Verschlüsselung der Befugnisse

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

A_24372 - Entitlement Management - Keine persistente Ablage unverschlüsselter Befugnisse

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

A_24687 - Entitlement Management - Keine Speicherung oder Verwendung nicht verifizierter Befugnisse

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

A_23842 - Entitlement Management - Eindeutigkeit der Befugnisse im Befugniskontext

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

A_24785 - Entitlement Management - VSDM-Prüfungsnachweis kann höchstens einmal genutzt werden

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

A_27671 - Entitlement Management - PoPP-Token kann höchstens einmal genutzt werden

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

A_27681 - Entitlement Management - Konfigurationsvariable `enforce_popp_only`

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

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

A_24506 - Entitlement Management- Realisierung der Schnittstelle `I_Entitlement_Management`

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

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

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

A_24987-01 - Entitlement Management - Protokolleinträge für Zugriffe auf das Entitlement Management

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

Tabelle 15: Entitlement Management Protokollierung

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

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

3151

3152 [**<=**]

3153 *Hinweis: Ein Update ("U") eines Entitlements liegt vor, wenn ein existierendes*
 3154 *Entitlement aufgrund des längeren Gültigkeitszeitraums eines neuen Entitlements*
 3155 *überschrieben wird.*

3156 **3-8-13.9.1 Initiale Befugnisse (static Entitlements)**

3157 Einige grundsätzlich notwendige Befugnisse sind zum Zeitpunkt der Aktivierung eines
 3158 Aktenkontos verfügbar.

3159 Zu diesen initialen Befugnissen gehören die Befugnisse für den Versicherten, den E-
 3160 Rezept-Fachdienst, den Kostenträger und die Ombudsstelle. Diese Befugnisse müssen in
 3161 der Phase der Initialisierung eines Aktenkontos durch das Aktensystem erstellt werden.

3162 Diese Befugnisse sind dauerhaft gültig und unveränderbar und können nicht gelöscht
 3163 werden.

3164 **A_24145 - Entitlement Management – Implizite initiale (statische) Befugnisse**

3165 Das Entitlement Management MUSS sicherstellen, dass der Versicherte (KVNR des
 3166 Akteninhabers, oid_versicherter), und der E-Rezept-Fachdienst (registrierte Telematik-
 3167 ID, oid_erp-vau) dauerhaft den versichertenindividuellen SecureDataStorageKey
 3168 beziehen können und Zugriff auf die Dokumenten- und Datenverwaltung erhalten. Die
 3169 Befugnisse MÜSSEN den Vorgaben der folgenden Tabelle entsprechen:

3170

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

3171 [\leq]

3172 **A_24374 - Entitlement Management – Signierte initiale (statische) Befugnisse**

3173 Das Entitlement Management MUSS sicherstellen, dass für den Kostenträger und die
 3174 Ombudsstelle gültige Befugnisse mit unbegrenzter Gültigkeitsdauer zum Zeitpunkt der
 3175 Aktivierung des Aktenkontos gemäß der Vorgaben der folgenden Tabelle vorliegen:

3176

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

Element	Kostenträger	Ombudsstelle
Ende der Gültigkeit (validTo)	9999-12-31	9999-12-31

3177 [\leq]

3178 **A_24688-01 - Entitlement Management – Befugnisverifikation signierter**
 3179 **initialer Befugnisse**

3180 Das Entitlement Management MUSS sicherstellen, dass die initialen, signierten
 3181 Befugnisse des Kostenträgers und der Ombudsstelle spätestens beim ersten Zugriff auf
 3182 das Aktenkonto durch das HSM unter Verwendung der Regel 'rr4' gemäß A_24573*
 3183 befugnisverifiziert sind. [\leq]

3184 **A_24533 - Entitlement Management - Keine Änderung statischer Befugnisse**

3185 Das Entitlement Management MUSS sicherstellen, dass die dauerhaften Befugnisse des
 3186 Versicherten, des E-Rezept-Fachdiensts, des Kostenträgers und der Ombudsstelle nicht
 3187 verändert oder gelöscht werden können. [\leq]

3188 **A_24784 - Entitlement Management - Höchstens eine Befugnis für KTR und**
 3189 **Ombudsstelle pro Aktenkonto**

3190 Das Entitlement Management MUSS sicherstellen, dass in einem Aktenkonto höchstens
 3191 eine Befugnis für einen Kostenträger und höchstens eine Befugnis für eine Ombudsstelle
 3192 hinterlegt ist. [\leq]

3193 **A_24955 - Entitlement Management - Befugnis für KTR und Ombudsstelle nur**
 3194 **bei Anlage und betreiberinterner Anbieterwechsel**

3195 Das Entitlement Management MUSS sicherstellen, dass eine signierte Befugnis des
 3196 Kostenträgers und eine signierte Befugnis der Ombudsstelle ausschließlich bei einer
 3197 Anlage eines Aktenkontos (Initialisierung) oder bei einem betreiberinternen
 3198 Anbieterwechsel in die Befugnisse des Aktenkontos aufgenommen werden.
 3199 [\leq]

3200 **3-8-23.9.2 Erstellen einer Befugnis durch Clients**

3201 Die Anforderung zur Vergabe einer neuen Befugnis erfolgt durch die Clients der ePA. Bei
 3202 einer Befugnisvergabe aus der Umgebung der Leistungserbringer ist dieses das
 3203 Primärsystem (PS), aus der Umgebung des Versicherten ist es das ePA-FdV.

3204 Clients verwenden zur Befugnisvergabe signierte JSON Web Token (JWS). Das Token
 3205 wird zur Verifikation an das HSM übergeben. Als Ergebnis der HSM Verarbeitung liegt
 3206 eine bestätigte, CMAC gesicherte Befugnis mit den Elementen `actorId` (Identifiziert des zu
 3207 befugnenden Nutzers), `kvnr` (AktenkontoId) und `validTo` (Gültigkeitszeitraum) für die
 3208 spätere Befugnisprüfung vor. Das HSM Ergebnis wird mit den weiteren Daten gemäß
 3209 A_23734* (`oid`, `displayName`, `issued`-*) ergänzt und gemäß A_24371* mit dem
 3210 SecureAdminStorageKey gesichert im Aktenkonto abgelegt.

3211 **3-8-2-13.9.2.1 Befugnisvergabe durch ein ePA-FdV**

3212 Ein ePA-FdV muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

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

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

Befugnis	Claim Name	Claim	Beispiel
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.CH.SIG	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	
	"exp"	Verfalldatum, = "iat" + 20 min	
	"insurantId"	KVNR des Aktenkontos	A123456789
	"actorId"	Identifizier (Telematik-id oder KVNR)	3-883110000092471
	"oid"	professionOid	1.2.276.0.76.4.54
	"displayName"	Name des Befugten	Test-Apotheke
	"validTo"	Ende der Gültigkeit, (Bei unbegrenzter Gültigkeit ist 9999-12-31T00:00:00Z zu verwenden.)	gemäß [RFC3339], z.B. 2025-06-30T21:59:59Z oder 2025-06-30T23:59:59+02:00

3217 [<=]

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

Hinweis zu A_24587: Im Falle der Befugnisvergabe für einen NCPeH (EU-Zugriff, "oid" == "oid_ncpeh") wird durch das Aktensystem sichergestellt, dass die vorgeschriebene Gültigkeitsdauer für derartige Befugnisse angewendet wird. Dieses erfolgt durch die Befugnisverifikation gemäß Regel "rr1" im HSM. Die Angabe eines Gültigkeitsendes im*

3226 "validTo"-Element des JWT wird daher für diesen Fall ignoriert, das Element selbst muss
3227 jedoch vorhanden sein.

3228
3229 **A_24689 - Entitlement Management - Befugnisverifikation einer Befugnis durch**
3230 **ein ePA-FdV**

3231 Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein
3232 ePA-FdV unter Verwendung der Regeln 'rr1' (Befugnisvergabe durch den Versicherten)
3233 bzw. 'rr2' (Befugnisvergabe durch einen Vertreter) des HSM eine Befugnisverifikation
3234 durchführen. [\leq]

3235 **A_24535 - Entitlement Management - Befugnisse für Vertreter**

3236 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId`
3237 = KVNR) ausschließlich durch den Versicherten erstellt oder gelöscht werden können.
3238 [\leq]

3239 **A_26698 - Entitlement Management - maximale Anzahl Befugnisse für Vertreter**

3240 Das Entitlement Management MUSS sicherstellen, dass maximal fünf gültige Befugnisse
3241 für Vertreter gleichzeitig in einem Aktenkonto vorhanden sind. [\leq]

3242 **A_24536 - Entitlement Management - Gültigkeitsdauer der Befugnisse für**
3243 **Vertreter**

3244 Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId`
3245 = KVNR) ausschließlich mit einer unbegrenzten Gültigkeit erstellt werden. [\leq]

3246 **A_24754 - Entitlement Management - E-Mail-Adresse des Vertreters**

3247 Das Entitlement Management MUSS sicherstellen, dass bei Befugnissen für Vertreter
3248 (`actorId` = KVNR) eine E-Mail-Adresse des Vertreters für dessen Benachrichtigung
3249 angegeben wird. [\leq]

3250 Die in A_24754 angegebene E-Mail-Adresse wird ausschließlich zur Benachrichtigung des
3251 Vertreters über die eingestellte Befugnis verwendet (vgl. A_24755-*), jedoch nicht für
3252 die Geräteregistrierung. Um eine Vertretung wahrnehmen zu können und hierfür Geräte
3253 zu registrieren, muss der Vertreter in seinem Home-AS eine E-Mail-Adresse hinterlegt
3254 haben.

3255 **A_24755-01 - Entitlement Management - Benachrichtigung des Vertreters bei**
3256 **Befugniserstellung**

3257 Das Entitlement Management MUSS im Anschluss an die erfolgreiche, neue
3258 Befugniserstellung für einen Vertreter eine E-Mail an die E-Mail-Adresse des Vertreters
3259 senden, die diesen über die Befugniserstellung für das Aktenkonto des Versicherten
3260 geeignet informiert. In der Nachricht MUSS der Name des Versicherten enthalten sein
3261 und welche Art von personenbezogenen Daten vom Vertreter im Rahmen der
3262 Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine
3263 Vertreterberechtigung widerrufen kann und gegenüber wem er seine
3264 datenschutzrechtlichen Betroffenenrechte wahrnehmen kann. [\leq]

3265 Hinweis: Unter Art der personenbezogenen Daten ist z.B. „Krankenversichertennummer,
3266 Name und E-Mail-Adresse“ gemeint, aber nicht die tatsächliche KVNR des Vertreters, der
3267 tatsächliche Name oder die tatsächliche E-Mail-Adresse.

3268

3269 **3.8.2.23.9.2.2 Befugnisvergabe durch ein Primärsystem**

3270 **A_27288 - Entitlement Management – Abgleich der KVNR bei Erstellen einer**
3271 **Befugnis über VSDM-Prüfziffer**

3272 Das Entitlement Management MUSS sicherstellen, dass für die in `setEntitlementPs` vom
3273 Primärsystem in `x-insurantid` übergebene KVNR und die übergebene Befugnis

(signiertes JWT) folgendes gilt: die KVNR in `x-insurantid` stimmt mit der KVNR überein, die in der CMAC-gesicherten Befugnis enthalten ist, die als Ergebnis des Aufrufs der Regel `rr3` mit der vom Primärsystem erhaltenen Befugnis (signiertes JWT) vom HSM zurückgegeben wird.

[<=]

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

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:

<u>Befugnis</u>	<u>Claim Name</u>	<u>Claim</u>
<u>Protected Header</u>		
	<u>"typ"</u>	<u>"JWT"</u>
	<u>"alg"</u>	<u>"ES256" oder "PS256"</u>
	<u>"x5c"</u>	<u>Signaturzertifikat C.HCI.AUT</u>
<u>Payload</u>		
	<u>"iat"</u>	<u>Zeitstempel Ausgabezeitpunkt</u>
	<u>"exp"</u>	<u>Verfalldatum, = "iat" + 20 min</u>
	<u>"auditEvidence"</u>	<u>VSDM-Prüfziffer aus dem VSDM-Prüfungsnachweis, base64-kodiert.</u>
	<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>

[<=]

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

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

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

- bei einem JWT mit Attribut "hcv" der Wert von "hcv" mit dem Wert von hcv aus der VSDM-Prüfziffer übereinstimmt und ansonsten die Operation `setEntitlementPs` abbricht,
- bei einem JWT ohne Attribut "hcv" die Operation `setEntitlementPs` abbricht, falls der Konfigurationsparameter `enforce_hcv_check` (vgl. A_27342-*) auf `true` gesetzt ist.

3303 [`<=`]

3304 **A_27289 - Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche**

3305 **der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer**

3306 Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer
 3307 Stunde maximal fünfmal eine Befugnis (signiertes JWT) über `setEntitlementPs`
 3308 übermitteln kann, bei der die mitgelieferte KVNR in `x-insurantId` von der KVNR
 3309 abweicht, die in der Prüfziffer der übermittelten Befugnis (signiertes JWT) enthalten ist,
 3310 andernfalls für den Nutzer für diesen Zeitraum die Operation `setEntitlementPs`
 3311 abbrechen. [`<=`]

3312 **A_27322 - Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche**

3313 **der VSD-Update-Zeit bei Erstellen einer Befugnis über VSDM-Prüfziffer in**

3314 **Version 2**

3315 Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer
 3316 Stunde maximal fünfmal eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2
 3317 über `setEntitlementPs` übermitteln kann, bei der die Operation `setEntitlementPs`
 3318 gemäß A_27321-* abbricht. [`<=`]

~~3319 **A_24590-02 – Entitlement Management – Befugnis durch ein Primärsystem**~~
 3320 ~~Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ein~~
 3321 ~~Primärsystem über die Schnittstelle I_Entitlement_Management durch Verwendung eines~~
 3322 ~~gültig-signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:~~
 3323

Befugnis	Claim-Name	Claim
Protected Header		
	"typ"	"JWT"
	"alg"	"ES256" oder "PS256"
	"x5c"	Signaturzertifikat C.HCI.AUT
Payload		
	"iat"	Zeitstempel Ausgabezeitpunkt
	"exp"	Verfalldatum, = "iat" + 20 min
	"auditEvidence"	VSDM-Prüfziffer aus dem VSDM-Prüfungsnachweis, base64-kodiert.

Befugnis	Claim-Name	Claim
	"hev"	optional solange enforce_hev_check = FALSE; Hash-check-value der als Ergebnis der Operation ReadVSD gemäß A_27352-* berechnet wird. Der berechnete hev-Wert MUSS base64-kodiert werden.

[<=]

A_25249 - Entitlement Management - Befugnisverifikation einer Befugnis durch ein Primärsystem

Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein Primärsystem unter Verwendung der Regeln 'rr3' (Stecken der eGK in einer Leistungserbringenumgebung) des HSM eine Befugnisverifikation durchführen. [**<=**]

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

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

A_24537 - Entitlement Management - Standardgültigkeitsdauer für Befugnisse

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

3.8.33.9.3 Löschen von Befugnissen

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

A_24504 - Entitlement Management - Löschen ungültiger Befugnisse

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

Das explizite Löschen von Befugnissen innerhalb ihres Gültigkeitszeitraums kann ausschließlich durch den Versicherten oder einen Vertreter mittels eines ePA-FdV erfolgen. Es können alle erteilten Befugnisse gelöscht werden, ausgenommen die initialen Befugnisse gemäß ~~3.8.1-Initiale Befugnisse (static Entitlements)~~ 3.9.1-Initiale Befugnisse (static Entitlements) .

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

A_25246 - Entitlement Management - Löschen von Befugnissen durch einen Vertreter

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

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

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

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

3.8.43.9.4 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

3397 **[<=]**

3398 Ein Eintrag der Blocked User Policy enthält Angaben gemäß der folgenden Tabelle:
 3399 (Beispiel)

3400 **Tabelle 16: 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

3401 **A_25135 - Entitlement Management - Initialisierung der Blocked User Policy**

3402 Das Entitlement Management MUSS für ein Aktenkonto eine Blocked User Policy ohne
 3403 initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policies über die
 3404 Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`
 3405 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. [\leq]

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. [\leq]

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. [\leq]

~~3-8-53.9.5~~ Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)

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

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

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

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

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

A_27311 - Entitlement Management – RateLimit-oid-List

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

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

gespeichert werden. [\leq]

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

~~A_27290-01A_27290~~ A_27291-01A_27291 - Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Stunde

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

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

innerhalb einer Stunde durch das Primärsystem im Aktensystem registrieren kann.

[\leq]

~~A_27291-01A_27291~~ A_27291-01A_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

- 3491 • oid_institution-pflege maximal 10000 Befugnisse
- 3492 • oid_institution-geburtshilfe maximal 10000 Befugnisse
- 3493 • oid_praxis-physiotherapeut maximal 10000 Befugnisse
- 3494 • oid_praxis-ergotherapeut maximal 10000 Befugnisse
- 3495 • oid_praxis-logopaede maximal 10000 Befugnisse
- 3496 • oid_praxis-podologe maximal 10000 Befugnisse
- 3497 • oid_praxis-ernaehrungstherapeut maximal 10000 Befugnisse
- 3498 • oid_institution-oegd maximal 10000 Befugnisse
- 3499 • oid_institution-arbeitsmedizin maximal 10000 Befugnisse

3500 innerhalb eines Monats durch das Primärsystem im Aktensystem registrieren kann.
 3501 [\leq]

3502 Hinweis zu A_27290-* und A_27291-*: Die Stunde bzw. der Tag müssen sich nicht auf
 3503 die aktuelle Stunde bzw. Kalendertag beziehen, sondern können auch je
 3504 Leistungserbringerinstitution auf Requestzeitpunkte bezogen werden. Dann gilt für einen
 3505 Monat 30 Tage.

3506 **A_27318 - ePA-Aktensystem - RateLimit-oid-List: Maßnahmen zum Schutz der** 3507 **Konfiguration**

3508 Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen
 3509 umsetzen, die eine unautorisierte Änderung der *RateLimit-oid-List* verhindern. [\leq]

3510 **A_27312 - ePA-Aktensystem - RateLimit-oid-List: Konfiguration durch** 3511 **Betreiber**

3512 Der Betreiber des ePA-Aktensystem MUSS sicherstellen, dass die Werte für die Anzahl
 3513 der maximalen Befugnisse in der *RateLimit-oid-List* durch den Betreiber des ePA-
 3514 Aktensystems ausschließlich im Vier-Augen-Prinzip konfigurierbar sind. [\leq]

3515 Stellen LEI Befugnisse mittels der Operation *setEntitlementsPs* über das Primärsystem
 3516 in das ePA-Aktensystem ein, wird für diese LEI geprüft, ob diese bereits das zulässige
 3517 Limit erreicht hat. Nur falls dies nicht der Fall ist, kann die Befugnis eingestellt werden.
 3518 Hierzu erfasst das ePA-Aktensystem außerhalb der VAU wann ein Nutzer mit welcher
 3519 Rolle eine Befugnis registriert hat. Für den Nutzer wird außerhalb der VAU ein
 3520 Nutzerpseudonym geführt.

3521 **~~A_27313-01A_27313~~ - Entitlement Management - Prüfen der RateLimit-oid-List** 3522 **beim Einstellen von Befugnissen**

3523 Das Entitlement Management MUSS bei Aufruf der Operation *setEntitlementsPs* oder
 3524 *setEntitlementPsV2* prüfen, ob für das zur LEI gehörende Nutzerpseudonym und die oid
 3525 der LEI bereits das in der *RateLimit-oid-List* vorgegebene maximale Limit pro Stunde
 3526 oder Monat erreicht wurde. Falls ein Limit erreicht wurde, wird die Operation
 3527 *setEntitlementsPs*, bzw. *setEntitlementPsV2*, mit einem Fehler abgebrochen. Falls
 3528 kein Limit erreicht wurde, ist die Registrierung für das zur LEI gehörende
 3529 Nutzerpseudonym zu vermerken. [\leq]

3530 **A_27310 - ePA-Aktensystem - Erfassung der Nutzer zur Prüfung RateLimit-oid-** 3531 **List**

3532 Das ePA-Aktensystem MUSS sicherstellen dass bei der Erfassung der Nutzerdaten
 3533 außerhalb der VAU zur Prüfung der *RateLimit-oid-List* eine Profilierung über die Nutzer
 3534 nicht möglich ist und zu diesem Zweck aus der TelematikId eines Nutzers ein
 3535 Nutzerpseudonym abgeleitet wird, gemäß gemSpec_Krypt#7.5 Routing auf VAU-
 3536 Instanzen.
 3537 [\leq]

3538 **3-93.10 Legal Policy**

3539 Die Legal Policy enthält die gesetzlich verbindlichen Regelungen der Zugriffsrechte bzgl.
3540 der Berufsgruppen und Datenkategorien gemäß § 341 Absatz 2 SGB V.

3541 Für die Datenkategorien sind die grundsätzlichen Zugriffsrechte der Zugriffsoperationen
3542 (CRUD - create, read, update, delete) vorgegeben. Diese Zugriffsrechte wirken
3543 ausnahmslos für jeden befugten Nutzer.

3544 Beispiele sind:

- 3545 • Apotheker haben keinen Zugriff auf das zahnärztliche Dokumentation in der
3546 Datenkategorie "dental".
- 3547 • Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen
3548 noch löschen.

3549 Die Legal Policy wird durch das Aktensystem durchgesetzt und ist jederzeit vorhanden.

3550 Die Konfiguration kann durch Clients oder Bestandteile des Aktensystems nicht verändert
3551 werden.

3552 **A 19303-22A-19303-21 - Legal Policy – gesetzlich vorgegebene Zugriffsrechte**

3553 Das ePA-Aktensystem MUSS alle in der folgenden Tabelle aufgeführten Regeln der Legal
3554 Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

3555 **Tabelle 17: Legal Policy**

Kategorie	Nutzergruppe										
Technischer Identifier	Med	Apo	Pflege	GH	HME	AM	KT R	O M	DiG A	eR P	Ver
Medical Services (XDS Document Service)	Zugriffsrecht gemäß § 352 SGB V										
reports	CRUD	R	R	R	RCRU D	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

Kategorie	Nutzergruppe										
child	CRU D	R	R	CRU D	R	R	-	-	-	-	RD (CU (*))
pregnancy_childbirth	CRU D	R	R	CRU D	R	R	-	-	-	-	RD
vaccination	CRU D	CRU D	R	R	-	CRU D	-	-	-	-	RD
patient	RD	R	R	R	R	R	C	-	-	-	CRU D
receipt	RD	RD	-	R	R	R	CU	-	-	-	RD
health_risk_analysis	-	-	-	-	-	-	C	-	-	-	RD
diga	R	R	R	R	R	R	-	-	CU	-	RD
care	CRU D	R	CRUD	R	R	R	-	-	-	-	RD
eau	CRU D	-	-	-	-	R	-	-	-	-	RD
rehab	CRU D	-	-	-	-	-	-	-	-	-	RD
transcripts	CRU D	-	-	-	-	-	-	-	-	-	RD
other	CRU D	-	-	-	-	R	-	-	-	-	RD
Medical Services (FHIR Data Service)	Zugriffsrecht										
medication	R	R	R	R	R	R	-	-	-	CU	R
Basic Services	Zugriffsrecht										
Consent Decisions	-	-	-	-	-	-	-	X	-	-	X
Constraints	-	-	-	-	-	-	-	-	-	-	X
Entitlements	X	X	X	X	X	X	-	-	-	-	X

Kategorie	Nutzergruppe										
Entitlements.Blocked User	-	-	-	-	-	-	-	x	-	-	x
Audit Events	-	-	-	-	-	-	-	x	-	-	x
Information	x	x	x	x	x	x	x	x	x	x	-
Devices	-	-	-	-	-	-	-	-	-	-	x

3556

3557

Nutzergruppen:

3558

3559

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

3560

3561

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

3562

3563

- Apo = Öffentliche Apotheke

- (oid_öffentliche_apotheke)

3564

3565

- Pflege = Gesundheits-, Kranken- und Altenpflege

- (oid_institution-pflege)

3566

3567

- GH = Geburtshilfe

- (oid_institution-geburtshilfe)

3568

3569

3570

- HME = Heilmittelerbringer

- (oid_praxis-physiotherapeut, oid_praxis-ergotherapeut, oid_praxis-logopaede, oid_praxis-podologe, oid_praxis-ernaehrungstherapeut)

3571

3572

- AM = Arbeitsmedizin

- (oid_institution-arbeitsmedizin)

3573

3574

- KTR = Kostenträger

- (oid_kostentraeger)

3575

3576

- OM = Ombudsstelle

- (oid_ombudsstelle)

3577

3578

- DiGA = Digitale Gesundheitsanwendung

- (oid_diga)

3579

3580

- eRP = E-Rezept vertrauenswürdige Ausführungsumgebung

- (oid_erp-vau)

3581

3582

- Ver = Versicherter / Vertreter

- (oid_versicherter)

3583

Legende:

3584

3585

- CRUD = create, read, update, delete; update: Aktualisierung von Metadaten, Aktualisierung eines Dokuments

- 3586 • "-" = keine Zugriffsrechte;
- 3587 • "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den
- 3588 Dienst (Service) definiert)
- 3589 • "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- 3590 • "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung
- 3591 in einer zukünftigen Version der ePA vorgesehen.

3592 Hinweise:

- 3593 • (*) Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann der
- 3594 Versicherte bzw. sein Vertreter oder eine Leistungserbringerinstitution gemäß der
- 3595 zuvor genannten Liste definierter professionOIDs sein. Sofern ein
- 3596 Versicherter/Vertreter der Einsteller der Elternnotiz ist, darf er abweichend von
- 3597 den oben aufgeführten Zugriffsunterbindungsregeln in die Datenkategorie mit
- 3598 dem technischen Identifier 'child' schreiben.

3599 [\leq]

3600

3601 **A_26166-02 - Legal Policy (EU) – EU-Zugriff: gesetzlich vorgegebene**

3602 **Zugriffsrechte**

3603 Das ePA-Aktensystem MUSS zusätzlich zu den Regeln aus A_19303-* alle in der

3604 folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und

3605 Dienste des Aktenkontos durchsetzen.

3606 **Tabelle 18: 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	-

Kategorie	Nutzergruppe
patient	-
receipt	-
health_risk_analysis	-
diga	-
care	-
eau	-
rehab	-
transcripts	-
other	-
Medical Services (FHIR Data Service)	Zugriffsrecht
medication	-
Basic Services	Zugriffsrecht
Consent Decisions	-
Constraints	-
Entitlements	-
Entitlements.Blocked User	-
Audit Events	-
Information	x
Devices	-

3607

3608

Nutzergruppen:

3609

- NCPeH = NCPeH-Fachdienst (oid_ncpeh)

3610

Legende:

3611

- CRUD = create, read, update, delete; update: Aktualisierung von Metadaten, Aktualisierung eines Dokuments

3612

- 3613 • "-" = keine Zugriffsrechte;
- 3614 • "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den
- 3615 Dienst (Service) definiert)
- 3616 • "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- 3617 • "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung
- 3618 in einer zukünftigen Version der ePA vorgesehen.

3619 [**<=**]

3620 Die folgende Tabelle erläutert die Kategorien aus A_19303-* und A_26166-*:

3621 **Tabelle 19: Beschreibung der Kategorien**

Technischer Identifier	Beschreibung
Medical Services	XDS Document Service
reports	Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen
emp	Elektronischer Medikationsplan
emergency	Daten der elektronischen Notfalldaten nach § 334 Absatz 1 Satz 2 Nummer 5 und 7
eab	Daten in elektronischen Briefen zwischen den an der Versorgung der Versicherten teilnehmenden Ärzten und Einrichtungen (elektronische Arztbriefe)
dental	Daten aus der zahnärztlichen Dokumentation
child	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
childsrecord	Archiv aus ePA 2.x: Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)

Technischer Identifier	Beschreibung
pregnancy_childbirth	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass) sowie Daten, die sich aus der Versorgung der Versicherten mit Hebammenhilfe ergeben
vaccination	Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation)
patient	Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden
receipt	Bei Kostenträgern gespeicherte Daten über die in Anspruch genommenen Leistungen des Versicherten
health_risk_analysis	Ergebnisse datengestützter Auswertungen der Krankenkassen zu individuellen Gesundheitsrisiken gemäß SGB V § 25b.
diga	Daten des Versicherten aus digitalen Gesundheitsanwendungen des Versicherten nach § 33a.
care	Daten zur pflegerischen Versorgung des Versicherten nach den §§ 24g, 37, 37b, 37c, 39a und 39c und der Haus- oder Heimpflege nach § 44 des Siebten Buches und nach dem Elften Buch
eau	Daten nach § 73 Absatz 2 Satz 1 Nummer 9 ausgestellte Bescheinigung über eine Arbeitsunfähigkeit
rehab	Daten der Heilbehandlung und Rehabilitation nach § 27 Absatz 1 des Siebten Buches
transcripts	Elektronische Abschriften von der Patientenakte eines Primärsystems gemäß §630g Abs. 2 BGB
other	Sonstige von Leistungserbringern für Versicherten bereitgestellte Daten, insbesondere Daten, die sich aus der Teilnahme des Versicherten an strukturierten Behandlungsprogrammen bei chronischen Krankheiten gemäß § 137f ergeben
Medical Services	Medication Service
medication	Verordnungs-, Dispensier- und Medikationsdaten in einer elektronischen Medikationsliste (eML) <u>und einem elektronischen Medikationsplan (eMP)</u>

Technischer Identifier	Beschreibung
Basic Services	Account Management
Consent Decisions	Management der Entscheidungen zu widerspruchsfähigen Funktionen der ePA
Constraints	Management der Konfiguration der General Deny Policy
Entitlements	Management der Befugnisse für Nutzer und Nutzergruppen
Audit Events	Abruf der Protokolleinträge eines Aktenkontos
Information	Informationen für nicht befugte Nutzer
Devices	Management der registrierten Geräte eines Nutzers

3622

3623 **A_21211-01 - Legal Policy - Änderungen der Legal Policy nicht erlauben**

3624 Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass
 3625 Änderungen der Konfiguration der Legal Policy gemäß A_19303-* ausgeschlossen sind.
 3626 [\leq]

3627 **A_24548 - Legal Policy - Durchsetzung der Zugriffsrechte der Legal Policy**

3628 Das ePA-Aktensystem MUSS sicherstellen, dass Operationen auf Daten und Operationen
 3629 der Dienste eines Aktenkontos abgebrochen und mit einer Fehlermeldung beendet
 3630 werden, wenn diese Operation durch die Vorgaben der Legal Policy gemäß A_19303-* für
 3631 die Nutzergruppe des Aufrufers der Operation nicht zulässig ist. [\leq]

3632 **~~3.103.11~~ 3.103.11 Constraint Management**

3633 Das Constraint Management des Aktenkontos stellt sicher, dass nur Zugriffe auf Daten in
 3634 Ordnern des XDS Document Service über die Vorgaben der Legal Policy hinaus
 3635 zugelassen werden, welche nicht vom Versicherten oder einem Vertreter unterbunden
 3636 (verborgen) wurden.

3637 Die Umsetzung dieser Beschränkungen erfolgt anhand der **General Deny Policy** für
 3638 jeden befugten Nutzer der betroffenen Nutzergruppen des Aktenkontos.

3639 Die General Deny Policy adressiert Nutzergruppen (professionOID) und Metadaten
 3640 der Daten. Es können einzelne Dokumente, Kategorien oder Ordner verborgen werden.
 3641 Bei jedem Zugriff auf Daten in Ordnern wird diese Policy bezüglich der Rolle eines
 3642 Nutzers und der betroffenen Dokumente ausgewertet und durchgesetzt.

3643 Die folgende Anforderung zeigt eine Übersicht der Nutzergruppen, für welche Dokumente
 3644 durch Einträge in der General Deny Policy vor einem Zugriff verborgen werden können.

A_24306-02 - Constraint Management - Policy für berechtigte Nutzergruppen und Nutzer

Das Constraint Management MUSS die Konfiguration der General Deny Policy auf die folgenden Nutzergruppen einschränken:

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

[<=]**A_24390-01 - Constraint Management- Anwendung der General Deny Policy**

Das Constraint Management MUSS bei jedem Zugriff auf Daten durch den XDS Document Service durch befugte Nutzer oder Nutzergruppen die General Deny Policy anwenden und den Zugriff verhindern, wenn ein Dokument oder dessen assoziierter Ordner oder dessen assoziierte Datenkategorie in der Policy konfiguriert ist.

[<=]

3659 Dienste des Aktenkontos (Basic Services) können nicht verborgen werden. Hier gelten die
3660 Zugriffsregelungen gemäß Legal Policy und die Beschränkungen der Schnittstellen.

3661 Datendienste (Medication Service) können nicht auf Daten- oder Ordnerbene verborgen
3662 werden. Hier gelten die Regelungen bezüglich des Widerspruchs gegen die Nutzung von
3663 widerspruchsfähigen Funktionen der ePA (siehe ~~3.7-Consent Decision Management~~3.8-
3664 Consent Decision Management).

3665 Die Kategorie "emp", bzw. einzelne Dokumente dieser Kategorie, des XDS Document
3666 Service dürfen nicht verborgen werden. Die Nutzung der Dokumente der Kategorie "emp"
3667 wird über das Consent Decision Management, bzw. einen erteilten Widerspruch gegen die
3668 widerspruchsfähige Funktion "medication" der ePA verhindert (siehe ~~3.7-Consent~~
3669 Decision Management)-3.8- Consent Decision Management).

3670 Die Operationen der Schnittstelle des Constraint Managements erlauben die
3671 Konfiguration der General Deny Policy durch den Versicherten oder einen befugten
3672 Vertreter.

3673 **A_24395 - Constraint Management - Realisierung der Schnittstelle** 3674 **I_Constraint_Management_Insurant**

3675 Das Constraint Management MUSS die Operationen der Schnittstelle
3676 I_Constraint_Management_Insurant gemäß [I_Constraint_Management_Insurant]
3677 umsetzen.[<=]

3678 **A_24887-01 - Constraint Management - Protokolleinträge für Zugriffe auf das** 3679 **Constraint Management**

3680 Das Constraint Management MUSS für das Aufnehmen und Löschen von Einträgen in die
3681 General Deny Policy jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist
3682 folgende Wertbelegung zu berücksichtigen:

3683 **Tabelle 20: Constraint Management Protokollierung**

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die API
	"object"		Bei intern ausgelösten Änderungen (XDS Document Service confidentiality code ("CON"), Löschen von Dokumenten oder Ordnern)
AuditEvent.action	C, D		
AuditEvent.entity.name	"GeneralDenyPolicy"		Eintrag für das Aufnehmen(Create) von Einträgen in die oder Löschen (Delete) von Einträgen aus der General Deny Policy

Strukturelement	Wert		Erläuterung
AuditEvent.entity.detail	type	value[x]	
	"DocumentTitle"	<XSDDocumentEntry.title>	wenn sich der Eintrag (Create oder Delete) der Policy auf ein Dokument bezieht
	"RootDocumentId"	<rootDocumentId>	wenn sich der Eintrag (Create oder Delete) der Policy auf ein Dokument bezieht
	"FolderTitle"	<XDSFolder.title>	wenn sich der Eintrag (Create oder Delete) der Policy auf einen Folder bezieht
	"FolderEntryUUID"	<Folder.entryUUID>	wenn sich der Eintrag (Create oder Delete) der Policy auf einen Folder bezieht
	"CategoryId"	<categoryId>	wenn sich der Eintrag (Create oder Delete) der Policy auf eine Kategorie bezieht

[<=]

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. [\leq]

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. [\leq]

~~3.10.13.11.1~~ Aktenkontoweites Verbergen (General Deny Policy)

Die General Deny Policy wird durch das Aktensystem für die in A_24306-* unter "General Deny Policy" aufgeführten Nutzergruppen angewendet und durchgesetzt. Einträge der General Deny Policy gelten dabei immer für alle aufgeführten Nutzergruppen gemeinsam.

Die Konfiguration der General Deny Policy erfolgt durch den Versicherten oder einen befugten Vertreter mittels ePA-FdV. Einträge können hinzugefügt oder entfernt werden. Zum Zeitpunkt der Erstellung des Aktenkontos enthält die General Deny Policy keine Einträge.

Ein Eintrag in der General Deny Policy referenziert entweder ein bestimmtes Dokument, einen dynamischen Ordner oder eine Datenkategorie. Die Menge der Einträge ist nicht limitiert.

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

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

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

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

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

3743 **Tabelle 21: Inhalt eines General Deny Policy Eintrags**

Element		Inhalt	Erläuterung
denyType		"document" oder "folder" oder "category"	Art des zu verbergenden Inhalts,
parameter:			eine technische Referenz passend zu "denyType"
[choice]	rootDocumentId	documentEntry.referenceIdList, Item "rootDocumentUniqueId"	Identifiziert das zu verbergende XDS Dokument
	folderUUID	folder.entryUUID	Identifiziert das zu verbergende dynamische Ordner
	categoryId	categoryId	technischer Identifizierer der zu verbergenden Kategorie

3744

3745 Beispiel:

3746 **Tabelle 22: Verbergen eines Medical Service**

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

3747 **3.10.1.13.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes**

3748

3749 Das Verbergen über den confidentialityCode ist im Kontext der Operationen des XDS
 3750 Document Service definiert und in ~~3.12.1.10- Verbergen von Dokumenten durch~~
 3751 ~~Verwendung des confidentialityCode~~ 3.13.1.10- Verbergen von Dokumenten durch
 3752 Verwendung des confidentialityCode beschrieben.

3753

3754 ~~3.11~~3.12 Device Management

3755 Die Geräteverwaltung ermöglicht ePA-FdVs die Registrierung und Verwaltung der vom
3756 Nutzer verwendeten Geräte. Das Device Management stellt das API zum ePA-FdV für die
3757 Geräteverwaltung bereit und ist nur in einer VAU/authentisierten User Session
3758 erreichbar.

3759 Im Folgenden wird als **Home-AS** eines Versicherten das ePA-Aktensystem desjenigen
3760 Betreibers bezeichnet, der vom Kostenträger des Versicherten beauftragt wurde. Falls
3761 der Versicherte der Anlage eines Aktenkontos nicht widersprochen hat, wird sein
3762 Aktenkonto im Home-AS verwaltet. Im Falle von Vertretern kann es vorkommen, dass
3763 das Home-AS des zu vertretenden Versicherten nicht das Home-AS des Vertreters ist.

3764 Die E-Mail-Adressen und die Geräte eines Versicherten werden ausschließlich im Home-
3765 AS des Versicherten verwaltet. Für Vertreter, deren Home-AS nicht das Home-AS des
3766 Versicherten ist, können im Home-AS des Versicherten die im Home-AS des Vertreters
3767 registrierten Geräte nachgenutzt werden. Das ePA-Aktensystem bietet dem ePA-FdV eine
3768 Schnittstelle, über die die durch das Home-AS signierte Geräteinformationen abgerufen
3769 werden können.

3770 Bei erstmaliger Nutzung des Gerätes initiiert das ePA-FdV die Geräteregistrierung und
3771 erhält dadurch eine DeviceID (bestehend aus deviceIdentifizier und deviceToken), welche
3772 bei folgenden Verwendungen des ePA-FdV zur Identifizierung des Geräts verwendet wird.
3773 Eine neue Geräteregistrierung muss durch den Nutzer bestätigt werden. Der Zugriff auf
3774 ein Aktenkonto kann nur mit einem Gerät mit bestätigter Geräteregistrierung erfolgen.

3775 Das Device Management ermittelt dazu die für den Nutzer im ePA-Aktensystem
3776 hinterlegte E-Mail-Adresse und versendet bei der Geräteregistrierung eine E-Mail an den
3777 Nutzer mit einem generierten Geräteregistrierungscode (confirmationCode). Der Nutzer
3778 sendet den Geräteregistrierungscode unter Verwendung des ePA-FdV zurück an das
3779 Device Management und bestätigt dadurch die Registrierung des neuen Geräts. Das
3780 Gerät kann nach der Bestätigung uneingeschränkt mit einem Aktenkonto genutzt
3781 werden.

3782 **A_24828 - Device Management - Realisierung der Schnittstelle**

3783 **I_Device_Management_Insurant**

3784 Das Device Management MUSS die Operationen der Schnittstelle
3785 `I_Device_Management_Insurant` gemäß `[I_Device_Management_Insurant]`
3786 umsetzen.[<=]

3787 **A_25164 - Device Management - Beschränkung der Schnittstellenoperationen** 3788 **auf Geräte des Nutzers**

3789 Das Device Management MUSS die Operationen der Schnittstelle
3790 `I_Device_Management_Insurant` gemäß `[I_Device_Management_Insurant]` auf die
3791 Geräte des aufrufenden Nutzers einschränken.[<=]

3792 **A_26153 - Device Management - Nutzen von Device Management auch bei** 3793 **Widerspruch gegen Aktenkonto**

3794 Das Device Management MUSS sicherstellen, dass das Device Management auch von
3795 Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben.[<=]

3796 **A_26154 - ePA-Aktensystem - Ausschließlich Nutzen von Email Management** 3797 **und Device Management bei Widerspruch**

3798 Das ePA-Aktensystem MUSS sicherstellen, dass Versicherte, die einem Aktenkonto
3799 widersprochen haben, ausschließlich das Email Management und das Device Management
3800 nutzen können.[<=]

A_26155 - Device Management - Versicherte nutzen Device Management ausschließlich im Home-AS

Das Device Management des ePA-Aktensystems MUSS sicherstellen, dass das Device Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-Aktensystem das Home-AS ist. [\leq]

A_24979 - Device Management - Sicheres Löschen von Geräten

Das Device Management MUSS beim Entfernen eines Gerätes sicherstellen, dass das Gerät gelöscht ist und dass das Gerät nicht mehr als verifiziertes Gerät genutzt werden kann. [\leq]

A_17947-03 - Device Management - Gültigkeitszeitraum und Löschung der Devicekennung

Das Device Management MUSS jede generierte und zu einem Nutzer gespeicherte Geräteregistrierung nach 2 Jahren löschen und darf Nutzeranfragen mit dieser Device-Kennung nach diesem Zeitpunkt nicht mehr akzeptieren. [\leq]

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

A_14595-02 - Device Management - Pflegeprozess Geräteverwaltung

Das Device Management MUSS die interne Liste aller bekannten Geräte derart pflegen, dass ein Gerät nach spätestens 1 Jahr nach der letzten Nutzung des Gerätes automatisch aus der Liste der registrierten Geräte gelöscht wird. [\leq]

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

A_25270 - Device Management - Erzeugung von Geräteinformationen und Geräteregistrierungscode bei der Geräteregistrierung

Das Device Management MUSS bei der Geräteregistrierung für das zu registrierende Gerät eines Nutzers

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

erzeugen. [\leq]

A_25271-01 - Device Management - Speicherung der Geräteinformationen

Das Device Management MUSS bei einer Geräteregistrierung eines Geräts eines Nutzers folgende Inhalte für den Nutzer verschlüsselt persistieren:

- deviceIdentifier
- deviceToken
- createdAt (Zeitpunkt der Erzeugung des deviceTokens)
- lastUse
- status
- displayName
- Geräteregistrierungscode,

- 3846 • Fehlerzähler.

3847 [<=]

3848 Hinweis zu A_25271-*: Für die verschlüsselte Speicherung der Geräteinformationen sind
3849 die Anforderungen aus Abschnitt 3.5.1.3 zu berücksichtigen.

3850 **A_25272 - Device Management - Pseudonyme Speicherung der**
3851 **Geräteinformationen**

3852 Das Device Management MUSS sicherstellen, dass die Zuordnung der außerhalb der VAU
3853 persistierten verschlüsselten Geräteinformationen zum Nutzer eindeutig ist und durch ein
3854 Pseudonym erfolgt.[<=]

3855 Hinweis: Aus A_25272 folgt, dass die Zuordnung der Speicherung der verschlüsselten
3856 Geräteinformationen nicht über die KVN-R des Nutzers erfolgen darf.

3857 **A_25273 - Device Management - Gültigkeitsdauer des**
3858 **Geräteregistrierungscodes**

3859 Das Device Management MUSS sicherstellen, dass der bei der Geräteregistrierung
3860 erzeugte Geräteregistrierungsscode maximal 6 Stunden nach Erzeugung der DeviceID
3861 (createdAt) für die Verifikation eines Gerätes genutzt werden kann.[<=]

3862 **A_25274 - Device Management - Löschen nach Gültigkeitsdauer des**
3863 **Geräteregistrierungscodes**

3864 Das Device Management MUSS sicherstellen, dass die Geräteinformationen für eine nicht
3865 bestätigte Geräteregistrierung nach Ende der Gültigkeitsdauer des
3866 Geräteregistrierungscodes gelöscht werden.[<=]

3867 **A_25275 - Device Management - Versenden des Geräteregistrierungscodes per**
3868 **E-Mail**

3869 Das Device Management MUSS bei der Geräteregistrierung für den Nutzer, für den das
3870 Gerät registriert werden soll, alle im Aktensystem hinterlegten E-Mail-Adressen ermitteln
3871 und an alle ermittelten E-Mail-Adressen eine E-Mail in einer für den Nutzer verständlichen
3872 Form mit folgenden Informationen versenden:

- 3873 • Zweck der E-Mail,
3874 • Geräteregistrierungsscode,
3875 • Gültigkeitsdauer des Geräteregistrierungscodes.

3876 [<=]

3877 **A_25276 - Device Management - Bestätigung mittels**
3878 **Geräteregistrierungscodes**

3879 Das Device Management MUSS für einen übergebenen Geräteregistrierungsscode und eine
3880 übergebene DeviceID (deviceIdentifier und deviceToken) prüfen, ob der vom Device
3881 Management bei der Geräteregistrierung erzeugte Geräteregistrierungsscode für das
3882 angegebene Gerät (deviceIdentifier, deviceToken) mit dem übergebenen
3883 Geräteregistrierungsscode übereinstimmt sowie der Geräteregistrierungsscode zeitlich
3884 gültig ist und

3885 1. bei Gleichheit und

3886 a. zeitlicher Gültigkeit

- 3887 • den Status für die Geräteregistrierung wechseln, so dass die erfolgreiche
3888 Bestätigung des Geräts aus dem Status hervorgeht,
3889 • den Geräteregistrierungsscode und den Fehlerzähler aus den
3890 Geräteinformationen löschen und
3891 • den Zeitpunkt der erfolgreichen Bestätigung in lastUsed erfassen,

- 3892 b. zeitlicher Ungültigkeit
- 3893 • alle Geräteinformationen zu diesem deviceIdentifier löschen,
- 3894 2. bei Ungleichheit den Fehlerzähler der Geräteinformation um eins erhöhen und
- 3895 • falls der Fehlerzähler größer oder gleich fünf ist,
- 3896 • alle Geräteinformationen zu diesem Gerät löschen.

3897 [**<=**]

3898 **A_25277 - Device Management - Sperrung bei vermehrter Anzahl von**

3899 **abgebrochenen Geräteregistrierungen**

3900 Falls für einen Nutzer innerhalb von 8 Stunden drei Geräteregistrierungen abgebrochen

3901 werden mussten, MUSS das Device Management sicherstellen, dass dieser Nutzer für 8

3902 Stunden ab dem Zeitpunkt der dritten abgebrochenen Geräteregistrierung keine Geräte

3903 mehr registrieren darf. [**<=**]

3904 **A_25291 - ePA-Aktensystem - Health Record Context nur mit verifizierten Gerät**

3905 Das ePA-Aktensystem MUSS sicherstellen, dass ein Versicherter (auch wenn er als

3906 Vertreter agiert) einen Health Record Context ausschließlich mit einem verifizierten Gerät

3907 öffnen kann, außer für den Fall, dass sich der Versicherte am ePA-FdV des Vertreters

3908 anmeldet (d.h. `x-authorize-representative=True` bei der

3909 Operation `I_Authorization_Service::sendAuthorizationRequestFdV`). [**<=**]

3910 Eine Geräteregistrierung im Home-AS kann in einem anderen Aktensystem nachgenutzt

3911 werden. Hierzu kann ein ePA-FdV mittels `getDeviceAttestation` eine Device Attestation

3912 vom Home-AS abrufen, welche beim anderen Aktensystem genutzt werden kann.

3913 **A_26157 - Device Management - Device Attestation kann nur mit verifiziertem**

3914 **Gerät abgerufen werden**

3915 Das Device Management MUSS sicherstellen, dass die Operation `getDeviceAttestation`

3916 ausschließlich nach erfolgreicher Authentifizierung des Nutzers und mit einem auf den

3917 Nutzer registrierten und verifizierten Gerät erfolgt.

3918 [**<=**]

3919 **A_26156 - Device Management - Inhalte der Device Attestation**

3920 Das Device Management MUSS sicherstellen, dass eine von einem ePA-FdV über die

3921 Operation `getDeviceAttestation` abgerufene Device Attestation folgende Inhalte

3922 enthält:

Attribut	Inhalt
actorId	KVNR aus dem ID-Token des angemeldeten Nutzers (bzw. der User Session)
iat	Zeitstempel Ausgabezeitpunkt
exp	Verfalldatum, = "iat" + 2 Stunden

3923 [**<=**]

3924 **A_26158 - Device Management - Signatur der Device Attestation**

3925 Das Device Management MUSS sicherstellen, dass die über `getDeviceAttestation`

3926 abgerufene Device Attestation mit dem privaten Schlüssel der Signaturidentität der VAU

3927 des Home-AS signiert wird. [**<=**]

3928 **3-123.13 Medical Services**3929 **A_25830-02 - Medical Services - Reihenfolge der Auswertung Legal Policy,**
3930 **Consent Decisions und Constraints**

3931 Die Medical Services MÜSSEN bei der Ausführung von Operationen der Schnittstellen der
3932 Medical Services sicherstellen, dass die Prüfung zu Bedingungen

- 3933 1. der Einschränkung der Rolle des Aufrufenden (oid),
- 3934 2. der Existenz des Aktenkontos (Status UNKNOWN oder INITIALIZED),
- 3935 3. des Zustands des Aktenkontos (Status ACTIVATED),
- 3936 4. der Befugnis des Aufrufenden,
- 3937 5. der Legal Policy,
- 3938 6. der Entscheidungen zu widerspruchsfähigen Funktionen der ePA,
- 3939 7. der Einträge der General Deny Policy
- 3940 8. des Entscheidungen zum nutzerspezifischen Ausschluss von der Teilnahme am
3941 digital gestützten Medikationsprozess

3942 in der dargestellten Reihenfolge erfolgt. Diese Reihenfolge MUSS auch eingehalten
3943 werden, wenn einzelne Prüfungen für eine Operation nicht anwendbar, bzw. nicht
3944 relevant, sind. [\leq]

3945 *Hinweis: Eine Operation kann nicht erfolgreich ausgeführt werden, weil dieses der Legal*
3946 *Policy widerspricht und weil ein Eintrag der General Deny Policy die Ausführung*
3947 *verhindert. Die Fehlermeldung zum Abbruch der Operation resultiert dann aus der*
3948 *Prüfung der Legal Policy, da die Bedingungen dieser gemäß der definierten Reihenfolge*
3949 *vor den Bedingungen der General Deny Policy geprüft werden müssen.*

3950 **3-12-13.13.1 XDS Document Service**

3951 Die gesetzlichen Vorgaben schränken den Zugriff Dritter auf Dokumente
3952 über berufsgruppenspezifische Vorgaben gemäß § 341 Absatz 2 SGB V ein. Dazu
3953 verwendet der XDS Document Service festgelegte Datenkategorien, welche mit
3954 spezifischen Zugriffsrechten der grundlegenden Zugriffsoperationen (CRUD - create,
3955 read, update, delete) wirken.

3956 Jedes eingestellte Dokument wird vom XDS Document Service mit einer automatischen
3957 Zuordnung zu einem statischen Ordner, welcher die Datenkategorie repräsentiert,
3958 erweitert. Diese statischen Ordner sind initial bei jedem Aktenkonto eines Versicherten
3959 existent. Die serverseitige Zuordnung in diese Ordner erfolgt anhand der XDS-Metadaten
3960 in Kombination mit der Nutzergruppe des Einstellers.
3961 Das bedeutet weiterhin, dass das Anlegen von statischen Ordnern durch ePA-Clients nicht
3962 erlaubt ist, um eine zweifelsfreie Anwendung der Zugriffsregeln auf Grundlage der
3963 Datenkategorien zu gewährleisten.

3964 Eine Ausnahme bilden bestimmte medizinische Informationsobjekte (MIOs), die eine
3965 weitere Gruppierung innerhalb der zugeordneten Datenkategorie erfordern. Ein Beispiel
3966 dafür ist der Mutterpass. Die Dokumente eines Mutterpasses müssen für die konkrete
3967 Schwangerschaft innerhalb der Kategorie separiert werden. Für die betroffenen
3968 Kategorien wird daher kein statischer Ordner vorbereitet, sondern der separierende,
3969 dynamische Ordner muss zeitgleich mit einer Dokumentenregistrierung durch den ePA-
3970 Client angelegt werden,

3971 ePA-Clients, die Dokumente für MIOs einstellen, können die dem MIO zugeordnete
 3972 Kategorie und die Art des Ordners (statisch, dynamisch) aus den Metadatenvorgaben für
 3973 MIOs gemäß [Implementation-Guidelines] entnehmen.

3974 Die Durchsetzung der Zugriffskontrolle auf die Kategorien, Ordner und Dokumente
 3975 gemäß der gesetzlichen Vorgaben und ggf. weiterer Beschränkungen durch den
 3976 Versicherten oder einen Vertreter erfolgt durch das Constraint Management (siehe ~~3.10-~~
 3977 ~~Constraint Management~~[3.11- Constraint Management](#)).

3978 ~~3.12.1.1~~[3.13.1.1](#) **Formatprüfung beim Einstellen von Dokumenten**

3979 **A_25233 - XDS Document Service - erlaubte Formate für PDF-Dokumente**

3980 Der XDS Document Service MUSS sicherstellen, dass ausschließlich die folgenden PDF/A-
 3981 Formate unterstützt werden:

- 3982 • PDF/A-1a
- 3983 • PDF/A-1b
- 3984 • PDF/A-2a
- 3985 • PDF/A-2u
- 3986 • PDF/A-2b

3987 [\leq]

3988 **A_24864-04 - XDS Document Service - Prüfen auf zulässiges Format beim** 3989 **Einstellen von Dokumenten**

3990 Der XDS Document Service MUSS beim Einstellen eines Dokumentes prüfen, dass das
 3991 Dokument eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und den
 3992 in Klammern angegebenen Dateiendungen (DocumentEntry.URI) besitzt

- 3993 • application/pdf nur PDF/A gemäß A_25233 (pdf)
- 3994 • text/plain (txt)
- 3995 • application/xml (xml)
- 3996 • application/hl7-v3 (xml)
- 3997 • application/pkcs7-mime (p7s oder p7)
- 3998 • application/fhir+xml (xml)
- 3999 • application/fhir+json (json)
- 4000 • application/json (json)

4001 sowie der tatsächliche Inhalt des Dokuments konform mit dem behaupteten MIME-Type
 4002 ist. Falls die Prüfung nicht erfolgreich ist, muss das Einstellen des Dokumentes abgelehnt
 4003 werden. \leq

4004 *Hinweise zu A_24864-**:

- 4005 • *Dokumente im PDF-Format werden vom XDS Document Service abgelehnt, da sie*
 4006 *ausführbaren Code enthalten können. Daher müssen die Clients, falls sie*
 4007 *Dokumente im PDF-Format einstellen wollen, diese zunächst in ein PDF/A*
 4008 *konvertieren.*
- 4009 • *p7s ist die Default-Dateiendung für Dokumente des mimetypes application/pkcs7-*
 4010 *mime in der ePA und für Dokumente dieses mimetypes gemäß*
 4011 *[gemSpec_IG_ePA] und für automatisierte Anpassungen von filename extensions*
 4012 *bei Dokumentenupload (A_23447-*, A_24451-*) zu berücksichtigen.*

4013

A_25009-03 - XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten durch Versicherte

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

- application/pdf nur PDF/A gemäß A_25233 (pdf)
- text/plain (txt)
- application/fhir+xml (xml)
- application/json (json)

Ferner MUSS der XDS Document Service sicherstellen, dass ausschließlich die Elternnotiz des Kinderuntersuchungshefts als FHIR Document mit dem MIME-Type "application/fhir+xml" registriert werden kann - andere FHIR Documents sind nicht zulässig.

[<=]

Hinweise zu A_24864- und A_25009-*: Die Prüfung des zulässigen Dokumentenformats muss mindestens*

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

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

Für XML-Dokumente muss eine Schema-Validierung ausschließlich auf Basis bekannter, intern vorliegender XML Schema-Definitionen durchführen. Gegen nicht intern vorliegende XML Schema-Definitionen wird nicht validiert. Die Schema-Validierung kann innerhalb des Health Record Contexts ohne zusätzliche Isolation erfolgen.

4047

A_24867 - XDS Document Service - Isolation der Formatprüfung

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

[<=]

Hinweise zu A_24867-:*

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

4056 *Der in A_24636-* geforderte technische Separationsmechanismus zur Isolation von*
 4057 *Health Record Contexten innerhalb einer VAU-Instanz kann ebenfalls zur Isolation der*
 4058 *Formatprüfung in A_24867-* genutzt werden.*

4059 *Findet eine Dokumentenformatprüfung innerhalb eines Health Record Context statt, wird*
 4060 *durch den Isolationsmechanismus aus A_24636-* verhindert, dass sich die*
 4061 *Dokumentenformatprüfung schadhaft auf andere Health Record Contexte auswirkt. Es*
 4062 *verbleibt dann zur Umsetzung der A_24867-* noch zu gewährleisten, dass sich die*
 4063 *Dokumentenformatprüfung nicht schadhaft auf den Health Record Context auswirkt, in*
 4064 *dem die Dokumentenformatprüfung erfolgt.*

4065 *Wenn Dokumentenprüfungen innerhalb eines Health Record Contexts ohne Isolation*
 4066 *erfolgen, muss sichergestellt werden, dass sich diese Prüfungen nicht schadhaft auf den*
 4067 *Health Record Context (oder andere) auswirken können. Dies ist vom Produktgutachter*
 4068 *zu prüfen und im Produktgutachten zu dokumentieren.*

4069 *Ein Ausschluss einer schadhaften Auswirkung auf den Health Record Context ist bei*
 4070 *folgenden Prüfungen des Dokumentenformats denkbar, so dass diese innerhalb des*
 4071 *Health Record Contexts ohne zusätzliche Isolationsmaßnahmen durchgeführt werden*
 4072 *können und kein Verstoß gegen die Anforderung A_24867-* vorliegt:*

- 4073 • *Prüfung der Magic Bytes des Dokuments (wo technisch möglich)*
- 4074 • *bei txt-, XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es*
 4075 *bei XML-Dokumenten kein valides UTF8 ist, eine Prüfung auf "restriktives" ISO-*
 4076 *8859-15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09,*
 4077 *0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind."*
- 4078 • *bei XML- und JSON-Dokumenten: Parsen der Dokumente auf valides XML bzw.*
 4079 *JSON mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert*
 4080 *und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu*
 4081 *bestätigen.*
- 4082 • *bei pkcs7-Dokumenten: Parsen der Dokumente mit Parsern, die entsprechend den*
 4083 *Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser*
 4084 *ist durch den Produktgutachter zu bestätigen.*

4085 *Der Produktgutachter muss bei der Umsetzung der oben genannten Prüfungen*
 4086 *bestätigen, dass der Ausschluss einer schadhaften Auswirkung auf den Health Record*
 4087 *Context (oder andere) durch die Umsetzung im Produkt tatsächlich gegeben ist.*

4088

4089 **A_25285 - XDS Document Service - Sicheres Löschen von Dokumenten mit** 4090 **unzulässigem Format**

4091 *Falls der XDS Document Service bei der Prüfung des Dateiformats (siehe A_24864-*)*
 4092 *beim Einstellen eines Dokuments ein unzulässiges Format erkennt, MUSS der XDS*
 4093 *Document Service das Dokument sicher löschen.*

4094 **[<=]**

4095 **A_24943 - XDS Document Service - Formatprüfung exponiert keine Daten aus** 4096 **der VAU heraus**

4097 *Der XDS Document Service MUSS sicherstellen, dass bei der Formatprüfung (siehe*
 4098 *A_24864-*) keine innerhalb der VAU verarbeiteten Daten die VAU verlassen.[<=]*

3.12.1.23.13.1.2 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

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

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

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

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

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

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

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

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

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

A_21200 - XDS Document Service und Clients – UTF-8 Kodierung von SOAP 1.2-Nachrichten

Der XDS Document Service und Clients des XDS Document Service MÜSSEN sicherstellen, dass die XML-Inhalte der SOAP 1.2-Nachrichten, die sie senden, der Zeichenkodierung UTF-8 entsprechen. [≤]

Es ist zu beachten, dass sich die Anzeige der verwendeten Kodierung in der Nachricht unterscheiden kann, z. B. in Nachrichten, in denen MTOM verwendet wird.

4147 ~~3.12.1.3~~ 3.13.1.3 Namensräume

4148 Für die Spezifikation der Schnittstellen des XDS Document Service werden die folgenden
 4149 XML-Präfixe verwendet, um den Namensraum bzw. das Vokabular des XML-Dokuments
 4150 zu kennzeichnen.

Präfix	Namensraum
lcm	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0
rmd	urn:ihe:iti:rmd:2017
rs	urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0
wsa	http://schemas.xmlsoap.org/ws/2004/08/addressing
wss	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
xdsb	urn:ihe:iti:xds-b:2007
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

4151 ~~3.12.1.4~~ 3.13.1.4 Nutzung von IHE IT Infrastructure-Profilen für 4152 Speicherung und Abruf von Dokumenten

4153 ~~3.12.1.4.1~~ 3.13.1.4.1 Anforderungen an IHE ITI-Akteure

4154 In diesem Abschnitt werden Anforderungen und Einschränkungen an relevante IHE ITI-
 4155 Akteure und -Transaktionen des XDS Document Service gestellt, um die geforderte IHE
 4156 ITI-Semantik zum ePA-Aktensystem zu bewahren. Werden IHE ITI-Akteure mit weiteren
 4157 Sub-Akteuren gruppiert, so werden die Anforderungen der Sub-Akteure zum gruppierten
 4158 Akteur übernommen. Eine Übersicht und Herleitung der IHE ITI-Akteure ist ~~3.12.1.4.2-~~
 4159 ~~Überblick über gruppierte IHE ITI-Akteure und Optionen~~ 3.13.1.4.2- Überblick über
 4160 ~~gruppierte IHE ITI-Akteure und Optionen~~ zu entnehmen.

4161 *Hinweis: Alle spezifizierten Anforderungen der IHE ITI-Akteure definieren das zu*
 4162 *implementierende Verhalten an den*
 4163 *Außenschnittstellen I_Document_Management sowie I_Document_Management_Insurant.*
 4164

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

Der XDS Document Service DARF NICHT vom Verhalten der definierten Außenschnittstellen

I_Document_Management, sowie I_Document_Management_Insurant aus Abschnitt ~~3.12.1.6 abweichen~~ 3.13.1.6 abweichen. Dies schließt über die Anforderungslage hinausgehende Implementierungen von IHE ITI-Akteuren und Optionen innerhalb des XDS Document Service mit ein, sodass zusätzlich implementierte IHE-Funktionalitäten keine Auswirkungen an den definierten Außenschnittstellen aufweisen dürfen. [≤]

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

Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Registry" gemäß [IHE-ITI-TF1] implementieren. [≤]

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

Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]

Die § 291a-konforme Protokollierung von Zugriffen erfolgt mit Mechanismen außerhalb des IHE ITI-TF. Eine technische Protokollierung via ATNA kann gemäß der Anforderung A_17826 dennoch erfolgen.

A_13809 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs ATNA Audit Record Repository

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "ATNA Audit Record Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]

Die Mechanismen der IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure Application" zur Node Authentication werden über das Konzept "Vertrauenswürdige Ausführungsumgebung" (siehe ~~3.5-Vertrauenswürdige Ausführungsumgebung (VAU)~~ 3.5-Vertrauenswürdige Ausführungsumgebung (VAU)) umgesetzt, sodass die Nutzung des Integrationsprofils ATNA diesbzgl. eingeschränkt wird.

A_17166 - XDS Document Service – Keine Implementierung der IHE ITI-Akteure ATNA Secure Node sowie ATNA Secure Application für Node Authentication

Der XDS Document Service DARF zur Node Authentication die IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure Application" gemäß [IHE-ITI-TF1] NICHT implementieren. [≤]

Der Zeitdienst der Telematikinfrastruktur unterstützt das Network Time Protocol in Version 4. Das IHE ITI-TF verlangt hingegen, das Zeitsynchronisierungsprotokoll in Version 3.

A_14654 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs CT Time Client

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "CT Time Client" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14665 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs XDS Document Source

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Source" gemäß [IHE-ITI-TF1] implementieren. [≤]

- 4212 **A_14667 - XDS Document Service – Keine Implementierung des IHE ITI-**
4213 **Akteurs XDS Integrated Document Source/Repository**
4214 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Integrated Document
4215 Source/Repository" gemäß [IHE-ITI-TF1] implementieren. [\leq]
- 4216 **A_14668 - XDS Document Service – Keine Implementierung des IHE ITI-**
4217 **Akteurs XDS Document Consumer**
4218 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Consumer"
4219 gemäß [IHE-ITI-TF1] implementieren. [\leq]
- 4220 **A_14666 - XDS Document Service – Keine Implementierung des IHE ITI-**
4221 **Akteurs XDS Patient Identity Source**
4222 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Patient Identity
4223 Source" gemäß [IHE-ITI-TF1] implementieren.
4224 [\leq]
- 4225 **A_14669 - XDS Document Service – Keine Implementierung des IHE ITI-**
4226 **Akteurs XDS On-Demand Document Source**
4227 Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS On-Demand Document
4228 Source" gemäß [IHE-ITI-TF1] implementieren. [\leq]
- 4229 **A_14950 - XDS Document Service – Keine Angabe einer Fehlerlokalisierung im**
4230 **RegistryError-Element**
4231 Der XDS Document Service DARF NICHT das `location`-Attribut im `rs:RegistryError`-
4232 Element in der IHE ITI-Ausgangsnachricht verwenden, sofern ein Fehler bei der
4233 Verarbeitung einer IHE ITI-Eingangsnachricht auftritt. Diese Einschränkung gilt nur für
4234 Error Stack Traces bzw. der Offenbarung von Programmierdetails. [\leq]
- 4235 **A_15081 - XDS Document Service – Implementierung des IHE ITI-Akteurs RMU**
4236 **Update Responder**
4237 Der XDS Document Service MUSS den IHE ITI-Akteur "RMU Update Responder"
4238 gemäß [IHE-ITI-RMU] implementieren. [\leq]
- 4239 [3.12.1.4.1.13.13.1.4.1.1](#) Gruppierungen mit anderen IHE ITI-Akteuren
4240 **A_15093-02 - XDS Document Service – Gruppierung RMU Update Responder mit**
4241 **Document Registry**
4242 Der XDS Document Service als RMU-Akteur "Update Responder" MUSS mit dem XDS-
4243 Akteur "Document Registry" gemäß [IHE-ITI-RMU] gruppiert sein. [\leq]
- 4244 [3.12.1.4.1.23.13.1.4.1.2](#) Optionen des IHE ITI-Akteurs
4245 **A_15094 - XDS Document Service – RMU Update Responder ohne "Forward**
4246 **Update"-Option**
4247 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option
4248 "Forward Update" unterstützen.
4249 [\leq]
- 4250 **A_15095-02 - XDS Document Service – RMU Update Responder ohne "XCA**
4251 **Persistence"-Option**
4252 Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option
4253 "XCA Persistence" unterstützen. [\leq]
- 4254 **A_15096-02 - XDS Document Service – RMU Update Responder mit "XDS**
4255 **Persistence"-Option**
4256 Der XDS Document Service als RMU-Akteur "Update Responder" MUSS die Option "XDS
4257 Persistence" unterstützen. [\leq]

A_15097 - XDS Document Service – RMU Update Responder ohne "XDS Version Persistence"-Option

Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option "XDS Version Persistence" unterstützen. [\leq]

[3.12.1.4.1.33.13.1.4.1.3](#) Gruppierungen mit anderen IHE ITI-Akteuren

[3.12.1.4.1.43.13.1.4.1.4](#) Optionen des IHE ITI-Akteurs

A_14637 - XDS Document Service – XDS Document Registry ohne "Asynchronous Web Services Exchange"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "Asynchronous Web Services Exchange" unterstützen. [\leq]

A_14638 - XDS Document Service – XDS Document Registry mit "Reference ID"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" MUSS die Option "Reference ID" unterstützen. [\leq]

A_14639 - XDS Document Service – XDS Document Registry ohne "Patient Identity Feed"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "Patient Identity Feed" unterstützen. [\leq]

A_14640 - XDS Document Service – XDS Document Registry ohne "Patient Identity Feed HL7v3"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "Patient Identity Feed HL7v3" unterstützen. [\leq]

A_14641 - XDS Document Service – XDS Document Registry ohne "On-Demand Documents"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "On-Demand Documents" unterstützen. [\leq]

[3.12.1.4.1.53.13.1.4.1.5](#) Optionen des IHE ITI-Akteurs

A_14636 - XDS Document Service – XDS Document Repository ohne "Asynchronous Web Services Exchange"-Option

Der XDS Document Service als XDS-Akteur "Document Repository" DARF NICHT die Option "Asynchronous Web Services Exchange" unterstützen. [\leq]

[3.12.1.4.23.13.1.4.2](#) Überblick über gruppierte IHE ITI-Akteure und Optionen

Die folgende Tabelle fasst die oben definierten Anforderungen zu Gruppierungen und Optionen zusammen. Dabei wird die folgende Notation für Optionalitäten (Opt.) verwendet:

Tabelle 23: 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.

4297
4298

Tabelle 24: 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				

4299

4300 3.12.1.4.33.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen

4301 **A_17832 - XDS Document Service – Unterstützung MTOM/XOP**

4302 Der XDS Document Service MUSS gemäß den Anforderungen von [IHE-ITI-
4303 TF2x#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP
4304 [MTOM] verwenden. [≤=]

4305 **A_24524 - XDS Document Service - Migration, Upload: Normalisieren des URI**

4306 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten
4307 den `DocumentEntry.URI` normalisieren. Dies gilt für `FileURI`, z. B. "
4308 `file:///C:/path/to/file.html#anchor`" "`file:///C:/path/to/file.html#anchor`" oder
4309 `"/C/path/to/file.html#anchor"`. Die URI MUSS auf den reinen Dateinamen mit Extension
4310 (d. h. ohne Pfadangaben) reduziert werden, z. B. "file.html". Nach der Normalisierung
4311 MUSS eine Validierung der Extension gemäß A_23447-* erfolgen. [≤=]

4312 **A_23447-01 - XDS Document Service - DocumentEntry.URI extension entspricht**
4313 **mimetype**

4314 Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten
4315 das Metadatum `DocumentEntry.URI` daraufhin prüfen, ob `DocumentEntry.URI` eine
4316 filename extension aufweist, die nicht dem `DocumentEntry.mimetype` entspricht. Zuvor
4317 muss die URI mittels A_24524-* normalisiert worden sein. Danach MUSS der XDS
4318 Document Service sicherstellen, dass in `Document.URI` die filename extension dem
4319 `DocumentEntry.mimeType` entspricht. Im Falle einer Abweichung MUSS an die
4320 ursprüngliche `DocumentEntry.URI` die filename extension gemäß A_24864-*, bzw.
4321 A_25009-*, angehängt werden, die dem `mimeType` entspricht. Die Groß-
4322 /Kleinschreibung der filename extension ist bei der Prüfung nicht relevant. [≤=]

4323 **A_24451-01 - XDS Document Service - Automatisches initiales Erzeugen einer**
4324 **versionsübergreifenden ID für Dokumente**

4325 Der XDS Document Service MUSS beim initialen Einstellen eines Dokumentes die
4326 `DocumentEntry.uniqueId` als Eintrag einer `ReferenceID` in die `ReferenceIDList` in
4327 folgendem Format einstellen:

4328 `<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2023:rootDocumentUniqueId`

4329 Beim Upload einer neuen Version des Dokumentes DARF dieser Eintrag in der
4330 `ReferenceIDList`, d.h. die `rootDocumentUniqueId`, NICHT verändert werden. Er bleibt
4331 über alle Versionen des Dokumentes hinweg unverändert erhalten. Der Versuch eines
4332 Clients, die `rootDocumentUniqueId` durch ein Metadata-Update oder im Zuge des
4333 Einstellens einer neuen Dokumentenversion zu verändern, MUSS mit einem IHE-Error
4334 `XDSRegistryMetadataError` abgebrochen werden. Es MUSS im `codeContext`-Attribut
4335 des zurückgegebenen `XDSRegistryMetadataError`-Elements der
4336 Text „rootDocumentUniqueId must not be changed“ zurückgegeben werden. [≤=]

4337 **A_14926-04 - XDS Document Service – Automatisiertes Löschen oder Verbergen**
4338 **von Dokumenten in RPLC-Ketten**

4339 **A_14926-03 – XDS Document Service – Automatisiertes Löschen oder Verbergen**
4340 **von Dokumenten**

4341 Der XDS Document Service MUSS bei zu löschenden oder zu verbergenden Dokumenten und `DocumentEntry`-Einträgen im selben Zuge auch alle
4342 mittels `urn:ihe:iti:2007:AssociationType:RPLC` assoziierten `DocumentEntry`-Einträge und
4343 Dokumente löschen bzw. verbergen. [≤=]

4344 **A_27653 - XDS Document Service – Automatisches Löschen oder Verbergen von**
4345 **Dokumenten in Anhangsketten**

4346 Der XDS Document Service MUSS bei zu löschenden oder zu verbergenden Dokumenten
4347 und DocumentEntry-Einträgen im selben Zuge auch die folgenden Schritte ausführen,
4348 sofern DocumentEntry.referenceIdList mindestens einen Wert enthält, der
4349 mit `urn:gematik:iti:xds:2025:parentDocument` oder `urn:gematik:iti:xds:2025:childDocument`
4350 ausgezeichnet ist. Für jedes zu löschende oder verbergende Dokument D:

1. Löschen/Verbergen der Elternkette:

Löschen/Verbergen jedes für den Anfragenden sichtbaren Elterndokuments E, dessen DocumentEntry.uniqueId über den Wert `urn:gematik:iti:xds:2025:parentDocument` in `D.referenceIdList` referenziert wird, sofern `E.referenceIdList` keinen per `urn:gematik:iti:xds:2025:childDocument`-ausgezeichneten Wert enthält, der nicht auf `D.uniqueId` referenziert. Wenn kein solcher Wert gefunden wird, Schritt 1. für Elterndokument E (d.h. rekursiv als neues "D") wiederholen, ansonsten ist das Löschen/Verbergen der Elternkette vollständig.

2. Löschen/Verbergen der Kindkette:

Löschen/Verbergen jedes für den Anfragenden sichtbaren Kinddokuments K, dessen DocumentEntry.uniqueId über den Wert `urn:gematik:iti:xds:2025:childDocument` in `D.referenceIdList` referenziert wird, sofern `K.referenceIdList` keinen per `urn:gematik:iti:xds:2025:parentDocument`-ausgezeichneten Wert enthält, der nicht auf `D.uniqueId` referenziert. Wenn kein solcher Wert gefunden wird, Schritt 2. für Kinddokument K (d.h. rekursiv als neues "D") wiederholen, ansonsten ist das Löschen/Verbergen der Kindkette vollständig.

3. Löschen des eigentlichen Dokuments:

Löschen/Verbergen des Dokuments D.

[<=]

Hinweis: A 27653 stellt sicher, dass nur Dokumente automatisch mitverborgen oder mitgelöscht werden, die für den Anfragenden sichtbar sind und nicht auch Teil anderer Anhangsketten sind. Nicht sichtbare Teilketten (vormals Kinder- und Elterndokumente des gelöschten Dokuments) bleiben intakt.

A 27683 - XDS Document Service – Maximale Länge von Anhangsketten

Der XDS Document Service MUSS sicherstellen, dass beim Einstellen (über die Schnittstelle Provide and Register Document Set-b [ITI-41]) oder Kennzeichnen (über die Schnittstelle Restricted Update Document Set [ITI-92]) von neuen Anhängen die gesamte Anhangskette inklusive des neuen Anhangdokuments nicht mehr als fünf Dokumente enthält und ansonsten die Operation mit dem Fehler `XDSMaxAttachmentsExceeded` abbrechen.

[<=]

Der Abschnitt 6.1- Dokumentenanhänge enthält eine Illustration für diese Anforderung.

3.12.1.4.3-13.13.1.4.3.1 Provide and Register Document Set-b [ITI-41]

A_13715 - XDS Document Service – Ablauflogik für ProvideAndRegisterDocumentSet-b

Der XDS Document Service MUSS die Umsetzung der Operation ProvideAndRegisterDocumentSet-b gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3] und [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3] implementieren.[<=]

A 15162-06A-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_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 = Deprecated` 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` hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die Dokumentengröße in `DocumentEntry.size` berechnet und gesetzt werden. [`<=`]

A_24988 - XDS Document Service - Dublettenprüfung für Dokumente

Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes Dokument den hash-Wert vergleichen mit allen bereits in dieser Akte existierenden hash-Werten der Dokumente und bei einer Übereinstimmung das Einstellen mit dem Fehlercode `XSDuplicateDocument` ablehnen. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die Liste der UUIDs (`DocumentEntry.entryUUID`) der identifizierten Dokumente angegeben werden. [`<=`]

A_24990 - XDS Document Service - Dublettenprüfung für dynamische Ordner

Der XDS Document Service MUSS beim Anlegen dynamischer Folder prüfen, ob ein Ordner bereits existiert, der gemäß vom Titel her identisch ist mit demjenigen, den der Client einzustellen versucht. Im Falle eines identischen Titels MUSS der Einstellversuch mit dem Fehlercode `XSDuplicateFolder` abgelehnt werden. [`<=`]

A_14937 - XDS Document Service – Dokumentengröße prüfen

Der XDS Document Service MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das SubmissionSet verarbeitet wird. Der XDS Document Service MUSS die Verarbeitung ablehnen und mit einem `MaxDocSizeExceeded`- bzw. `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren, wenn die

4449 Gesamtgröße aller übermittelten Dokumente 250 MByte übersteigt oder die Größe
4450 mindestens eines einzelnen Dokuments 25 MByte übersteigt.
4451 [`<=`]

4452 Das bedeutet, dass Dokumente bis zu einer Größe von $25 \text{ MB} = 25 * (1024)^2 \text{ Byte}$ in
4453 die ePA hochgeladen werden. Grundlage für die Berechnung der Dokumentengröße ist
4454 das Dokument ohne Transportcodierung. Größere Dokumente können nicht hochgeladen
4455 werden.

4456 **A_23098-01 - XDS Document Service – Keine Registrierung bei zeitlicher**
4457 **Ungültigkeit von strukturierten Dokumenten**
4458 Der XDS Document Service MUSS beim Einstellen eines strukturierten
4459 Dokuments sicherstellen, dass die Vorgaben gemäß [gemSpec_IG_ePA] hinsichtlich der
4460 zeitlichen Gültigkeit erfüllt werden und andernfalls das Registrieren und Speichern von
4461 Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`
4462 quittieren. Es MUSS im `codeContext`-Attribut
4463 des zurückgegebenen `XDSRepositoryMetadataError`-Elements der Text „Version of
4464 submitted structured document is not supported“ zurückgegeben werden. [`<=`]

4465 **A_21610-03 - Sonderfälle Anlegen von Foldern durch Clientsysteme**
4466 Der XDS Document Service MUSS sicherstellen, dass ausschließlich dynamische Ordner
4467 vom Typ "Schwangerschaft und Geburt" (Folder.Code = `pregnancy_childbirth`) durch
4468 Clients angelegt werden können. [`<=`]

4469 **A_22400-01 - XDS Document Service - Ablehnung Upload bei abweichenden**
4470 **confidentialityCode**
4471 Der XDS Document Service MUSS Uploads, die als Resultat einen uneinheitlichen
4472 `documentEntry.confidentialityCode` über alle Dokumente in einer mixed- oder uniform-
4473 Sammlung haben, mit einem `XDSRegistryMetadataError` ablehnen. [`<=`]

4474 Die Anforderung bezieht sich auf Einträge in `documentEntry.confidentialityCode` die nicht
4475 aus dem ValueSet zum Verbergen (`confidentialityCode=CON`), resultieren.

4476 **A_24797-04 - XDS Document Service - Ablehnung Upload bei veränderten**
4477 **Metadaten bei einer RPLC Assoziation**
4478 Der XDS Document Service MUSS Uploads, die als Resultat ein zum Vorgängerdokument
4479 verändertes Metadatum enthalten, mit einem `XDSRegistryMetadataError` ablehnen.
4480 Einzige Ausnahmen sind:

- 4481 • Metadatenattribute `creationTime`, `entryUUID` sowie `uniqueId` und
4482 `confidentialityCode = "CON"` (`codeSystem = urn:oid:1.2.276.0.76.5.491`).
- 4483 • Das Metadatenattribut `DocumentEntry.referenceIdList` DARF ohne die
4484 `rootDocumentUniqueId` gesendet werden; in dem Fall wird die
4485 `rootDocumentUniqueId` automatisch vom XDS Document Service gesetzt (Wert
4486 identisch zu dem des ersetzten Dokuments).

4487 [`<=`]

4488 **A_24531-04 - Constraint Management - Verbergen von Dokumenten durch**
4489 **confidentialityCode**
4490 Falls das Dokument, welches mit `confidentialityCode = "CON"` (`codeSystem =`
4491 `urn:oid:1.2.276.0.76.5.491`) durch eine Nutzergruppe der
4492 Rolle `oid_versicherter` eingestellt wird, nicht Bestandteil einer Sammlung, also eines
4493 Ordners der Ausprägung "mixed" oder "uniform" ist, und kein Dokument der Kategorie
4494 "emp" ist, dann MUSS der XDS Document Service sicherstellen, dass das Dokument
4495 durch einen Eintrag in der General Deny Policy verborgen wird. Es MUSS ein Eintrag mit
4496 `denyType = "document"` für die General Deny Policy erzeugt werden. [`<=`]

A_25856-02 - XDS Document Service - Fehlerhaftes Verbergen von Dokumenten durch confidentialityCode

Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) nicht durch eine Nutzergruppe der Rolle oid_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.

3.13.1.4.3.1.1 Dokumentenanhänge

Für die Verwaltung von Anhängen wird ein Mechanismus basierend auf DocumentEntry.referenceIdList verwendet. Zwei Dokumente werden verknüpft, indem in beiden dazugehörigen DocumentEntrys das jeweils andere Dokument als "Elterndokument" bzw. "Kinddokument" (=Anhang) eingetragen wird. Dies geschieht über die Auszeichnung der Referenzen mit den qualifizierenden Codes urn:gematik:iti:xds:2025:childDocument (Verweis auf ein Kinddokument) und urn:gematik:iti:xds:2025:parentDocument (Verweis auf ein Elterndokument).

Ein Verweis auf ein Elternformat hat also das

Format: <DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2025:parentDocument

Dabei muss das Dokument, auf das per Kind- oder Elternreferenz verwiesen wird, zusammen mit oder nach dem referenzierten Dokument eingestellt werden. Wenn z. B. das Elterndokument bereits im Aktensystem gespeichert ist und ein Kinddokument (Anhang) dazu hochgeladen wird, muss der DocumentEntry des Kinddokuments das Elterndokument in der referenceIdList referenzieren. Die Markierung des Elterndokuments (mit dem Verweis auf das Kinddokument) wird dann vom Aktensystem automatisch vorgenommen. Damit wird vermieden, dass zwei Aufrufe notwendig sind (Einstellen gefolgt vom Aktualisieren der Metadaten), was zu inkonsistenten Zuständen im Aktensystem führen kann. Werden Eltern- und Kinddokument gemeinsam eingestellt, ist der Verweis auf das Elterndokument verpflichtend, während die Referenz auf das Kinddokument im Elterndokument nur optional angegeben wird (da sie vom Aktensystem automatisch ergänzt werden kann).

A_27654 - XDS Document Service – Einstellen von neuen Anhängen oder Anhängen an neue Dokumente

Der XDS Document Service MUSS beim Registrieren und Speichern von Metadaten und Dokument(en) über die Schnittstelle

I Document Management Insurant::ProvideAndRegisterDocumentSet-b() die folgenden zusätzlichen Schritte durchführen, wenn das Feld DocumentEntry.referenceIdList einen Wert mit Identifier Type Code

urn:gematik:iti:xds:2025:parentDocument (oder urn:gematik:iti:xds:2025:childDocument) enthält; im Folgenden ist der Fall

für urn:gematik:iti:xds:2025:parentDocument beschrieben, der Fall childDocument ist analog zu behandeln und jeweils in Klammern angegeben)

1. Prüfung, ob das dort als parentDocument (childDocument) adressierte Dokument (mit entsprechender DocumentEntry.uniqueId) entweder Teil des SubmissionRequests oder bereits im XDS Document Service vorhanden (und im zweiten Fall für den Anfragenden sichtbar ist), und wenn beides nicht zutrifft, die Verarbeitung mit dem Fehler XDSNoSuchParent (XDSNoSuchChild) abbrechen.

2. Prüfung, ob durch das Einstellen des Dokuments kein Verweiszirkel entsteht und ansonsten die Verarbeitung mit dem Fehler `XDSAttachmentCycle` abbrechen.

3. Prüfung, ob durch das Einstellen des Dokuments der zusätzliche Verweis nicht auf ein Elterndokument (Kinddokument) gemacht wird, das bereits Teil der Elternketten (Kindkette) ist und ansonsten die Verarbeitung mit dem Fehler `XDSInvalidAttachmentHierarchy` abbrechen.

4. Der XDS Document Service MUSS im referenzierten Dokument die `DocumentEntry.uniqueId` des einzustellenden Dokuments in die `referenceIdList` mit Identifier Code `urn:gematik:iti:xds:2025:childDocument` (`urn:gematik:iti:xds:2025:parentDocument`) eintragen, wenn dies nicht bereits geschehen ist.

[<=]

Hinweis 1: Ein Verweiszirkel kann entstehen, wenn ein Kinddokument direkt oder indirekt (d.h. ggf. über eine Kette von Kinddokumenten hinweg) gegenüber seinem Elterndokument gleichzeitig auch selbst als Elterndokument auftritt.

Hinweis 2: Der Fehler `XDSInvalidAttachmentHierarchy` spiegelt die Situation wider, dass in einer Kette von Anhängen (wie 1<-2<-3) versucht wird, ein Kind (3) zusätzlich als Kind eines Vorfahren seines Elterndokuments (1) einzuführen.

Hinweis 3: Punkt 4 stellt sicher, dass das referenzierte Dokument passend markiert wird, egal ob es in der Anfrage enthalten ist oder bereits im Aktensystem hinterlegt ist.

Siehe auch entsprechende Illustrationen im Anhang.

[3.12.1.4.3-23.13.1.4.3.2](#) 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. [<=]

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 die `Replace-Associations` dasjenige `DocumentEntry` Objekt ermittelt, das sich im Zustand `approved` befindet.

Das `wsa:Action-Element` MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery" besitzen.

[<=]

A_24762 - XDS Document Service – Suchanfragen über das Metadatenattribut `DocumentEntry.title`

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-

4593 ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter
4594 \$XDSDocumentEntryTitle unterstützen, sodass eine Suchergebnismenge über das
4595 Attribut XDSDocumentEntry.title eingeschränkt werden kann. Weiterhin MUSS dieselbe
4596 Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den
4597 Parameter \$XDSDocumentEntryAuthorPerson. Das `wsa:Action`-Element MUSS den Wert
4598 "urn:ihe:iti:2007:RegistryStoredQuery" besitzen. [`<=`]

4599 **A_25183 - XDS Document Service – Suchanfragen über das Metadatenattribut** 4600 **DocumentEntry.comment**

4601 Der XDS Document Service MUSS einen zusätzlichen Anfragetyp
4602 "FindDocumentsByComment" mit der Query-ID "urn:uuid:2609dda5-2b97-44d5-a795-
4603 3e999c24ca99" und denselben Parameternutzungsvorgaben der Registry Stored Query
4604 "FindDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren
4605 verpflichtenden Suchparameter \$XDSDocumentEntryComment unterstützen, sodass eine
4606 Suchergebnismenge über das Attribut XDSDocumentEntry.comment eingeschränkt
4607 werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert
4608 sein, wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson.
4609 Das `wsa:Action`-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery"
4610 besitzen. [`<=`]

4611 **A_24763 - XDS Document Service – Suche über Author Institution bei Registry** 4612 **Stored Query**

4613 Der XDS Document Service MUSS für den Anfragetyp "FindDocumentsByTitle" den
4614 weiteren optionalen Parameter \$XDSDocumentEntryAuthorInstitution verarbeiten
4615 können, sodass eine Suchergebnismenge über den authorInstitution-Slot der
4616 XDSDocumentEntry.author-Classification (Wertemenge des authorInstitution-Sub-
4617 Attributs) eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels
4618 Platzhalter implementiert sein, wie für Suchanfragen über den Parameter
4619 \$XDSDocumentEntryAuthorPerson. [`<=`]

4620 **A_24764 - XDS Document Service – Rückgabe unscharfer Suchergebnisse für** 4621 **Registry Stored Query**

4622 Der XDS Document Service MUSS bei der Ermittlung der Ergebnisse einer Registry
4623 Stored Query bei Auswertung der folgenden Queries und deren Suchparametern beim
4624 Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d. h. bezogen auf das
4625 jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht
4626 abweichende Ergebnisse zurück liefern können:

- 4627 • Query "FindDocuments" und Query "FindDocumentsByTitle" und Query
4628 "FindDocumentsByComment"
- 4629 • \$XDSDocumentEntryTitle
- 4630 • \$XDSDocumentEntryAuthorInstitution
- 4631 • \$XDSDocumentEntryAuthorPerson
- 4632 • \$XDSDocumentEntry.comment
- 4633 • Query "FindSubmissionSets"
- 4634 • \$XDSSubmissionSetAuthorPerson

4635 Dabei MUSS der XDS Document Service mindestens unscharfe Ergebnisse bezüglich
4636 Groß/Kleinschreibung unterstützen, also Groß/Kleinschreibung für die angegebenen
4637 Parameter der ausgewählten Query-Typen ignorieren.
4638 [`<=`]

4639 Das zur Ermittlung weiterer unscharfer Ergebnisse vom XDS Document Service
4640 einzusetzende Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu

liefern, die ihm möglicherweise sonst wegen beispielsweise falscher Schreibweise eines Namens (z. B. "Meyer" vs. "Maier") vorenthalten worden wäre. Dabei sind Verfahren wie die Kölner Phonetik aber auch andere Mechanismen denkbar.

A_27655 - XDS Document Service – Suche nach Anhangsketten

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "GetDocumentAppendices" mit der Query-ID "urn:uuid:2a6b3197-8ea8-4245-a6de-daf71b469116" und denselben Parameternutzungsvorgaben der Registry Stored Query "GetDocumentsAndAssociations" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.8] unterstützen. Die Suchergebnismenge muss für jedes über \$XDSDocumentEntryEntryUUID oder \$XDSDocumentEntryUniqueId referenzierte Dokument die Ergebnismenge wie folgt ermitteln:

1. Alle DocumentEntrys der Ergebnismenge hinzufügen, welche auf die uniqueId des Dokuments aus dem Eingangsparameter in der DocumentEntry.referenceIdList verweisen (ausgezeichnet als urn:gematik:iti:xds:2025:childDocument oder urn:gematik:iti:xds:2025:parentDocument).
2. Für jeden im vorher durchgeführten Schritt identifizierten DocumentEntry D, der über den Eintrag urn:gematik:iti:xds:2025:childDocument identifiziert wurde, alle DocumentEntries der Ergebnismenge hinzufügen, welche die uniqueId von D wiederum als urn:gematik:iti:xds:2025:childDocument in der referenceIdList enthalten.
3. Für jeden im vorher durchgeführten Schritt identifizierten DocumentEntry E, der über den Eintrag urn:gematik:iti:xds:2025:parentDocument identifiziert wurde, alle DocumentEntries der Ergebnismenge hinzufügen, welche die uniqueId von E wiederum als urn:gematik:iti:xds:2025:parentDocument in der referenceIdList enthalten.
4. Schritte 2 und 3 jeweils wiederholen, bis keine weiteren DocumentEntries mehr gefunden werden können.

[<=]

Hinweis: Wenn als Eingabe eine entryUUID gegeben wird, muss der XDS Document Service die dazugehörige uniqueID ggf. intern selbst ermitteln

3.12.1.4.3.33.13.1.4.3.3 Remove Metadata [ITI-62]

A_14908-02 - XDS Document Service – Ablauflogik für Remove Metadata

Der XDS Document Service MUSS die Umsetzung der Operation RemoveMetadata gemäß der definierten Ablauflogik in [IHE-ITI-RMD#3.62.4.1.2 und 3.62.4.1.3] implementieren.[<=]

A_20701 - XDS Document Service – Unwiderrufliches Löschen bei Remove Metadata

Der XDS Document Service MUSS sicherstellen, dass einmal gelöschte Dokumente und Metadatenobjekte nicht wiederhergestellt werden können.[<=]

A_21715 - XDS Document Service – Kein Löschen von "replaced"-Dokumenten im Status "Deprecated"

Der XDS Document Service MUSS sicherstellen, dass keine Löschanfrage eines ePA-Client auf Dokumenten mit dem availabilityStatus = Deprecated ausgeführt werden darf.[<=]

A_21714-03 - XDS Document Service – Löschen von strukturierten Dokumenten durch ein ePA-FdV

Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert

4689 aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie
 4690 zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die
 4691 Nachricht mit dem XDSRegistryError-Fehlercode zurückgegeben werden. Es MUSS im
 4692 codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert
 4693 "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt
 4694 werden.[<=]

4695 **A_21817-02 - XDS Document Service – Löschen von strukturierten Dokumenten** 4696 **durch ein Primärsystem**

4697 Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein
 4698 Primärsystem ablehnen, wenn zugehörige Submission Sets, Associations oder
 4699 zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners
 4700 impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets,
 4701 Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben
 4702 vor, MUSS die Nachricht mit XDSRegistryError-Fehlercode zurückgegeben werden. Es MUSS
 4703 im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der
 4704 Wert "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt
 4705 werden.[<=]

4706 **A_24663-01 - XDS Document Service – Bereinigung der General Deny Policy**

4707 Der XDS Document Service MUSS als Folge von erfolgreichen Löschanfragen alle Einträge
 4708 der General Deny Policy entfernen, welche die betroffenen Dokumente oder dynamischen
 4709 Ordner referenzieren.[<=]

4710 **A_24765 - XDS Document Service – Kein Löschen von statischen Ordnern und** 4711 **Associations**

4712 Der XDS Document Service MUSS sicherstellen, dass eine Löschanfrage keine statischen
 4713 Ordner und Assoziationen löschen darf. Dies gilt nicht für dynamische Ordner. Der XDS
 4714 Document Service MUSS bei Löschung eines Dokumentes die Assoziation zum Folder
 4715 löschen.[<=]

4716 Dynamische Ordner sind beispielsweise Mutterpass (folderCode = pregnancy_childbirth)
 4717 oder DiGA (folderCode = diga).

4718 **A_20579-01 - XDS Document Service – Löschen von Ordnern**

4719 Der XDS Document Service MUSS Requests, die darauf abzielen, einen statischen Folder
 4720 direkt zu löschen, mit einem XDSRegistryMetadataError ablehnen.[<=]

4721

4722 **A_27656 - XDS Document Service – Löschen von Anhängen oder Dokumenten** 4723 **mit Anhängen**

4724 Der XDS Document Service MUSS beim Löschen eines Dokuments D, das in der
 4725 DocumentEntry.referenceIdList ein Dokument E via
 4726 urn:gematik:iti:xds:2025:childDocument oder
 4727 urn:gematik:iti:xds:2025:parentDocument referenziert, im Dokument E die dazu
 4728 passende rückwärtige Referenz auf D aus E's referenceIdList entfernen.
 4729 Dies gilt auch, falls E für das anfragende System nicht sichtbar ist.
 4730 **[<=]**

4731 Die Anforderung stellt sicher, dass keine "toten" Eltern- und Kindreferenzen im XDS
 4732 Document Service verbleiben.

4733 3.12.1.4.3.4.3.13.1.4.3.4 RetrieveDocumentSet [ITI-43]

4734 **A_14914 - XDS Document Service – Ablauflogik für Retrieve Document Set**

4735 Der XDS Document Service MUSS die Umsetzung der Operation RetrieveDocumentSet
 4736 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3] und
 4737 [IHE-ITI-TF2b#3.43.4.2.2 und 3.43.4.2.3] implementieren.[<=]

A_16201 - XDS Document Service – Prüfung der zurückgegebenen Paketgröße

Der XDS Document Service MUSS anhand der übergebenen DocumentUniqueIDs die Gesamtgröße ermitteln und bei Überschreitung von 250 MByte die Verarbeitung ablehnen und die Nachricht mit einem `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. [`<=`]

3.12.1.4.3.53.13.1.4.3.5 Restricted Update Document Set [ITI-92]**A_15061-07 - XDS Document Service – Ablauflogik für Restricted Update Document Set**

Der XDS Document Service MUSS die Umsetzung der Operation `RestrictedUpdateDocumentSet` gemäß der definierten Ablauflogik in [IHE-ITI-RMU#3.92.4.1.2 und 3.92.4.1.3] implementieren und sicherstellen, dass (nur) die folgenden Metadatenobjekte gesendet werden:

- ein neues `SubmissionSet`,
- einen `DocumentEntry` inklusive der `entryUUID` des zu ändernden `DocumentEntry`-Objekts. Das übermittelte `DocumentEntry`-Objekt kann sowohl alle vollständigen Metadatenattribute als auch nur zu ändernde Metadatenattribute enthalten. In jedem Fall dürfen Änderungen ausschließlich gemäß A_15083-* angenommen und durchgeführt werden.
- für das Hinzufügen, Ändern oder Löschen eines einzelnen oder mehrerer Werte in `DocumentEntry.author`, `DocumentEntry.confidentialityCode` und `DocumentEntry.eventCodeList` gilt darüber hinaus:
 - es MÜSSEN alle und nicht nur die zu ändernden Werte (z. B. Autoren) über ihre jeweiligen `<classification classificationScheme="urn:uuid:...>-XML`-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. [`<=`]

A_15083-09A_15083-08 - 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`
- `DocumentEntry.serviceStopTime`
- `DocumentEntry.title`
- `DocumentEntry.typeCode`
- `DocumentEntry.URI`

Wenn das Metadatum `DocumentEntry.referenceIdList` ohne `rootDocumentUniqueId` gesendet wird, MUSS der XDS Document Service den Wert automatisch setzen (identisch zu `rootDocumentId` in `DocumentEntry.referenceIdList` des ersetzten Dokuments). Wenn die `rootDocumentUniqueId` gesendet wird, MUSS der XDS Document Service sicherstellen, dass der Wert dem ansonsten automatisch gesetzten Wert entspricht.

Werden unerlaubte Metadatenänderungen geschickt, muss die Operation mit einem `LocalPolicyRestrictionError`-Fehlercode abgebrochen werden. Werden Metadatenattribute mit leeren Werten übermittelt, signalisiert dies ein Löschen des Metadatums (z.B. `DocumentEntry.comments`). Es müssen die Kardinalitäten in A_14760-* berücksichtigt bzw. ~~dürfen nicht verletzt werden~~. dürfen nicht verletzt werden (Ausnahme für Altdaten: `eventCodeList` darf mehr als einen DMP- oder KDL-Code in der `eventCodeList` enthalten, wenn der alte Metadatensatz bereits dieselben DMP- und KDL-Codes führt). Das Metadatum `DocumentEntry.referenceIdList` MUSS dabei mindestens die `rootDocumentUniqueId` enthalten.

Wenn in der Eingangsnachricht keine Aktualisierung für die erlaubten Metadaten enthalten ist, ist die Weiterverarbeitung abzubrechen und die Nachricht mit einem `LocalPolicyRestrictionError`-Fehlercode zu quittieren. [`<=`]

A_27657 - XDS Document Service – Anhänge hinzufügen oder entfernen mit Restricted Update Document Set

Der XDS Document Service MUSS beim Aktualisieren eines DocumentEntries die folgenden Regeln durchsetzen (der Text bezieht sich auf das Einfügen oder Entfernen eines parentDocument; die analoge Handlungsanweisung für childDocument ist jeweils in Klammern angegeben):

- Wenn dem Feld DocumentEntry.referenceIdList ein Wert mit der Auszeichnung urn:gematik:iti:xds:2025:parentDocument (urn:gematik:iti:xds:2025:childDocument) hinzugefügt wird, MUSS der XDS Document Service prüfen,
 - ob das dort referenzierte Dokument nicht existent oder für das anfragende System nicht sichtbar ist und in diesem Fall die Operation mit dem Fehler XDSNoSuchParent(XDSNoSuchChild) abbrechen.
 - ob die Kennzeichnung des Dokuments als Anhang einen Verweiszirkel verursachen würde und ggf. die Operation mit dem Fehler XDSAttachmentCycle abbrechen;
 - ob durch das Markieren des Dokuments der zusätzliche Verweis nicht auf ein Elterndokument (Kinddokument) gemacht wird, das bereits Teil der Elternketten (Kindkette) ist und ansonsten die Verarbeitung mit dem Fehler XDSInvalidAttachmentHierarchy abbrechen.
- Wenn keiner der genannten Fehlerfälle vorliegt, MUSS der XDS Document Service im referenzierten DocumentEntry den passenden urn:gematik:iti:xds:2025:childDocument (urn:gematik:iti:xds:2025:parentDocument)- Eintrag auf das ursprünglich aktualisierte Dokument in die referenceIdList einfügen.
- Wenn aus dem Feld DocumentEntry.referenceIdList ein Wert mit der Auszeichnung urn:gematik:iti:xds:2025:parentDocument (urn:gematik:iti:xds:2025:childDocument) entfernt wird, MUSS der XDS Document Service im dort referenzierten Dokument den passenden urn:gematik:iti:xds:2025:childDocument (urn:gematik:iti:xds:2025:parentDocument)-Eintrag aus der referenceIdList entfernen.

[<=]

Das Hinzufügen oder Entfernen von bestehenden Anhängen wird also immer entweder über Eltern- oder Kinddokument vorgenommen; das zweite Dokument wird immer automatisch angepasst. Wird über RMU die referenceIdList so gesetzt, dass die Eltern- und Kinddokumentauszeichnungen unverändert bleiben, ist A_27657* nicht relevant.

A_21533 - XDS Document Service – Kein Anlegen von Versionen für Restricted Update Document Set

Der XDS Document Service DARF eine echte Versionierung NICHT umsetzen, d. h. er DARF den alten DocumentEntry NICHT speichern. Insbesondere DARF der XDS Document Service DocumentEntry.version NICHT anlegen und verwalten. [<=]

A_21783-03 - XDS Document Service - Vererbung der geänderten Metadaten für Restricted Update Document Set

Der XDS Document Service MUSS die neu gesetzten Metadaten ebenfalls auf alle mit dem geänderten Dokument assoziierten Dokumente setzen. Als assoziierte Dokumente sind im Sinne dieser Anforderung Dokumente einer RPLC-Kette zu betrachten. [<=]

4876 Metadaten von Dokumenten einer mixed- oder uniform-Sammlung dürfen nicht geändert
4877 werden.

4878 **A_25173 - XDS Document Service - Restricted Update Document Set nicht für**
4879 **MIOs**

4880 Falls die Operation `RestrictedUpdateDocumentSet` für Dokumente einer mixed- oder
4881 uniform-Sammlung aufgerufen wird MUSS der XDS Document Service das Aktualisieren
4882 der Metadatenattribute ablehnen, mit einem `XDSRepositoryMetadataError` quittieren
4883 und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements den
4884 Text "Metadata Update for MIOs not allowed" angeben.
4885 [`<=`]

4886 3.12.1.4.43.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen

4887 **A_24508-01 - XDS Document Service – Prüfung der Policies bei Suchanfrage**

4888 Der XDS Document Service MUSS bei einer Suchanfrage für einen angemeldeten Nutzer
4889 die Suchergebnismenge entsprechend der Legal Policy und der General Deny Policy
4890 filtern, d. h. die Suchergebnismenge enthält ausschließlich XDS-Metadaten, die für einen
4891 angemeldeten Nutzer nicht diesen Policies widersprechen. [`<=`]

4892 **A_26222 - XDS Document Service (EU) – Prüfung Zugriffscode bei Suchanfrage**
4893 **EU-Zugriff**

4894 Der XDS Document Service MUSS für einen angemeldeten Nutzer mit der Rolle
4895 `oid_nceph` bei jeder Suchanfrage und jeder Retrieve-Operation prüfen, dass der im
4896 SOAP-Header der Operation übergebene Zugriffscode identisch ist mit dem im
4897 Entitlement Management für diesen Nutzer hinterlegten Zugriffscode und andernfalls die
4898 Operation mit dem Fehlercode `AccessCodeViolation` beenden. [`<=`]

4899 **A_24509 - XDS Document Service - Prüfung der Legal Policy außer**
4900 **Suchanfragen**

4901 Der XDS Document Service MUSS die Ausführung einer Operation mit dem Fehlercode
4902 `LegalPolicyViolation` beenden, wenn für den angemeldeten Nutzer die Regeln der Legal
4903 Policy nicht erfüllt sind und es sich nicht um eine Suchanfrage handelt.
4904 Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die
4905 Liste der UUIDs (`DocumentEntry.entryUUID`) der identifizierten Dokumente angegeben
4906 werden. [`<=`]

4907 **A_24510-02 - XDS Document Service – Prüfung Herunterladen eines**
4908 **verborgenen oder nicht vorhandenen Dokuments**

4909 Der XDS Document Service MUSS die Ausführung der Retrieve-Operation mit dem
4910 Fehlercode `XDSDocumentUniqueIdError` beenden, wenn das assoziierte Dokument nicht
4911 vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny Policy
4912 nicht erfüllt sind. [`<=`]

4913

4914 **A_24511-01 - XDS Document Service – Prüfung Löschen eines verborgenen**
4915 **Dokuments oder dynamischen Ordners**

4916 Der XDS Document Service MUSS die Ausführung der Remove-Operation mit dem
4917 Fehlercode `XDSDocumentUniqueIdError` beenden, wenn für den angemeldeten Nutzer die
4918 Regeln der General Deny Policy nicht erfüllt sind.
4919 [`<=`]

4920 **A_24512-02 - XDS Document Service – Prüfung Schreiben eines Dokuments in**
4921 **einen nicht vorhandenen oder verborgenen dynamischen Ordner**

4922 Der XDS Document Service MUSS die Ausführung der Provide-Operation mit dem
4923 Fehlercode `UnresolvedReferenceException` beenden, wenn der Ordner nicht existiert oder

4924 für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind.
4925 [`<=`]

4926 **A_24513-02 - XDS Document Service – Prüfung Aktualisierung Metadaten eines**
4927 **verborgenen oder nicht vorhandenen Dokuments**

4928 Der XDS Document Service MUSS die Ausführung der Update-Operation mit dem
4929 Fehlercode `UnresolvedReferenceException` beenden, wenn das assoziierte Dokument
4930 nicht vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny
4931 Policy nicht erfüllt sind. [`<=`]

4932 **3.12.1.53.13.1.5 Fehlerbehandlung in Schnittstellenoperationen**

4933 **A_22516-02 - XDS Document Service - Alternative Verwendung von**
4934 **XDSRegistryMetadataError anstelle von XDSRepositoryMetadataError**

4935 Der XDS Document Service KANN alternativ zum Fehler "XDSRepositoryMetadataError"
4936 den Fehler "XDSRegistryMetadataError" verwenden. [`<=`]

4937 **A_23148-01 - XDS Document Service – Festlegung zu http-Statuscode bei IHE-**
4938 **Responses**

4939 Der XDS Document Service MUSS für den Fall, dass eine IHE-Response in der HTTP-
4940 Response enthalten ist, den http-Statuscode 200 zurückgeben. Das gilt auch, wenn die
4941 IHE-Response einen IHE-Fehler überträgt. [`<=`]

4942 **A_26324-01 - XDS Document Service - Aktenkonto im Umzug**

4943 Falls sich ein Aktenkonto im Zustand `SUSPENDED` befindet MUSS der XDS Document
4944 Service die Verarbeitung ablehnen und mit einem `StatusMismatch`-Fehlercode gemäß
4945 [IHE-ITI-TF3#4.2.4] quittieren. [`<=`]

4946 **A_26325-01 - XDS Document Service - Aktenkonto unbekannt oder im Zustand**
4947 **INITIALIZED**

4948 Falls sich ein Aktenkonto im Zustand `UNKNOWN` oder `INITIALIZED` befindet MUSS der
4949 XDS Document Service die Verarbeitung ablehnen und mit einem `NoHealthRecord`-
4950 Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. [`<=`]

4951 **A_25683-01 - XDS Document Service - Prüfung auf Befugnis**

4952 Falls keine gültige Befugnis für den aufrufenden Nutzer vorliegt MUSS der XDS Document
4953 Service die Verarbeitung ablehnen und mit einem `NotEntitled`-Fehlercode gemäß [IHE-
4954 ITI-TF3#4.2.4] quittieren. [`<=`]

4955 **A_26459 - XDS Document Service - keine Authentisierung des Nutzers**

4956 Falls keine erfolgreiche Authentifizierung des Nutzers vorliegt MUSS der XDS Document
4957 Service die Verarbeitung ablehnen und mit einem `InvalidAuth`-Fehlercode gemäß [IHE-
4958 ITI-TF3#4.2.4] quittieren. [`<=`]

4959 **A_27541 - XDS Document Service - keine Geräteregistrierung des Nutzers**

4960 Falls der Nutzer der Versicherte oder ein Vertreter ist (`oid_versicherter`) und keine
4961 Geräteregistrierung des Nutzers vorliegt, MUSS der XDS Document Service die
4962 Verarbeitung ablehnen und mit einem `UnregisteredDevice`-Fehlercode gemäß [IHE-ITI-
4963 TF3#4.2.4] quittieren. [`<=`]

4964

4965 **3.12.1.63.13.1.6 Schnittstellen im XDS Document Service**

4966 In diesem Abschnitt wird die Außenschnittstelle des XDS Document Service festgelegt.
4967 Einzelne Umsetzungsanforderungen suggerieren eine vermischte Verarbeitung von
4968 Funktionalitäten, welche bei IHE ITI originär getrennt von einer Document Registry und
4969 einem Document Repository (bzw. den Responding Gateways) durchgeführt werden. Da

4970 die Außenschnittstelle des XDS Document Service nicht zwischen Document Registry und
 4971 Document Repository unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit
 4972 differenzierten Pfaden, siehe A_26814-*, werden sonst bei IHE ITI explizite Operationen
 4973 zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne Umsetzung
 4974 angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-Nachricht
 4975 kann an IHE ITI-konforme Akteure ausgerichtet werden.

4976 3.12.1.6.13.13.1.6.1 Schnittstelle I_Document_Management

4977 Weitere Vorgaben zu den Operationen befinden sich in 3.12.1.4.3- Vorgaben zu IHE ITI-
 4978 Transaktionen bei mehreren Schnittstellen 3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen
 4979 bei mehreren Schnittstellen .

4980 **A_14152-02 - XDS Document Service – Implementierung der Schnittstelle** 4981 **I_Document_Management**

4982 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-
 4983 Service-Schnittstelle für den Zugriff von ePA-Clients, die über das zentrale Netz zugreifen
 4984 implementieren.

4985 **Tabelle 25: Schnittstelle I_Document_Management**

Schnittstelle	I_Document_Management	
Version	2.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	ProvideAndRegisterDocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Metadata	Löschen von Dokumenten oder Ordnern
	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
WSDL	[XSDSDocumentService]	

Schnittstelle	I_Document_Management
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd

4986 **[<=]**

4987 Durch die Legal Policy ist geregelt, welche Clients (professionOID) letztendlich zugreifen
4988 dürfen.

4989 3.12.1.6.1-13.13.1.6.1.1 Operation

4990 I_Document_Management::ProvideAndRegisterDocumentSet-b

4991 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
4992 Transaktion "ProvideAndRegisterDocumentSet-b" [ITI-41] sind [IHE-ITI-TF2x] sowie
4993 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

4994 Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner
4995 gesammelt. Das Anlegen eines DiGA-Ordners erfolgt durch den XDS Document Service
4996 unter der Voraussetzung, dass es eine gültige Befugnis für die DiGA gibt. Der DiGA-
4997 Ordner wird vom XDS Document Service mit der Telematik-ID der DiGA verknüpft.
4998 Die Zuordnung von DiGA-Dokumenten beim Schreiben erfolgt implizit über die
4999 TelematikID aus dem IDToken des Nutzers. Da ein DiGA-Ordner im Titel immer den
5000 Namen der DiGA enthält kann ein Client (z.B. LEI) darüber die relvante DiGA auswählen
5001 und auf die Dokumente der DiGA, sofern eine Befugnis für den Nutzer vorliegt, lesend
5002 zugreifen.

5003 Ein Update eines bestehenden Dokuments mit der bekannten DocumentEntry.entryUUID
5004 kann durch einen DiGA-Client erfolgen. Hierzu ist es erforderlich, dass ein DiGA-Client
5005 die DocumentEntry.entryUUID persistiert und keine symbolischen IDs gemäß [IHE-ITI-
5006 TF2b#3.42.4.1.3.7] verwendet.

5007 **A_21512-04 - XDS Document Service – dynamisches Anlegen von DiGA-Ordern**

5008 Falls eine gültige Befugnis für eine konkrete DiGA vorliegt, MUSS der XDS Document
5009 Service beim erstmaligen Einstellen eines Dokumentes für diese DiGA in die Akte des
5010 Versicherten (Operation I_Document_Management::ProvideAndRegisterDocumentSet-
5011 b()) sicherstellen, dass genau ein Ordner für den Versicherten mit den folgenden
5012 Eigenschaften angelegt ist:

- 5013 • DiGA-Ordner der Kategorie diga gemäß A_19388 (Belegung Folder.codeList) unter
5014 Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A_14760
5015 (Belegung der restlichen Metadatenfelder).
- 5016 • Folder.title wird entsprechend des Attributs "organizationName" aus dem IDToken
5017 der zugreifenden DiGA belegt.
- 5018 • Folder.comment wird belegt mit "urn:gematik:diga:<Telematik-ID>", wobei die
5019 Telematik-ID dem Attribut "idNummer" des ID-Token entspricht.

- 5020 • Folder.EntryUUID wird mit einer aus der TelematikID abgeleiteten UUID belegt.
- 5021 Die folder.EntryUUID MUSS wie folgend dargestellt aus der TelematikID der DiGA erzeugt
- 5022 werden:
- 5023 • Algorithmus: Name-Based UUID gemäß [RFC4122#4.3], Version 3 (MD5)
- 5024 • Namensraum-UUID: "e2310a38-0b62-415e-8b44-994dc8312965"
- 5025 • Name: "<TelematikId>"
- 5026 Eine konkrete DiGA wird identifiziert durch die TelematikID und ist als DiGA durch die
- 5027 professionOID gekennzeichnet.
- 5028 [`<=`]
- 5029 **A_22994-01 - XDS Document Service - automatische Folder-Zuordnung für DiGA**
- 5030 Der XDS Document Service MUSS beim Einstellen eines DiGA-Dokumentes in die Akte
- 5031 des Versicherten (Operation
- 5032 `I_Document_Management::ProvideAndRegisterDocumentSet-b()`) sicherstellen, dass das
- 5033 DiGA-Dokument in den durch die TelematikID referenzierten DiGA-Ordner abgelegt wird.
- 5034 Die TelematikID des zu adressierenden Ordners entspricht dem Attribut "idNummer" des
- 5035 ID-Token . [`<=`]
- 5036 **A_21713-03 - XDS Document Service – Kein Einstellen von Ordnern**
- 5037 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und
- 5038 Dokument(en) über die
- 5039 Schnittstelle `I_Document_Management::ProvideAndRegisterDocumentSet-b` ablehnen
- 5040 und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der
- 5041 Eingangsnachricht ein oder mehrere neu anzulegende Folder enthalten sind. Ausnahme:
- 5042 Folder der Kategorie `pregnancy_childbirth` in `Folder.codeList`. [`<=`]
- 5043
- 5044 **A_24497 - XDS Document Service - Verwendung der korrekten Telematik-ID**
- 5045 **beim Einstellen**
- 5046 Der XDS Document Service MUSS die Telematik-ID aus dem ID-Token der aktuellen User
- 5047 Session abgleichen mit der Telematik-ID aus `SubmissionSet.authorInstitution` und
- 5048 das Abweichen der Telematik-Ids mit einem `XDSRepositoryMetadataError`-Fehlercode
- 5049 quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError-`
- 5050 Elements den Text "Telematik-ID does not match" angeben. [`<=`]
- 5051 **A_24456 - XDS Document Service - Durchsetzung von Uniqueness beim**
- 5052 **Einstellen von Notfalldaten**
- 5053 Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien
- 5054 "emergency" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein
- 5055 einzelnes NFD- und ein einzelnes DPE-Dokument im Status "approved" gibt. Der Versuch,
- 5056 innerhalb dieses Ordners ein zweites NFD- oder DPE-Dokument einzustellen, MUSS mit
- 5057 dem IHE-Error `InvalidDocumentContent` abgebrochen werden. Es MUSS im
- 5058 `codeContext`-Attribut des zurückgegebenen `InvalidDocumentContent`-Elements der Text
- 5059 "Medical information object has to be unique" zurückgegeben werden. [`<=`]
- 5060 **A_25137 - XDS Document Service - Durchsetzung von Uniqueness beim**
- 5061 **Einstellen vom Medikationsplan**
- 5062 Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien
- 5063 "emp" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein einzelnes
- 5064 eMP-Dokument im Status "approved" gibt. Der Versuch, innerhalb dieses Ordners ein
- 5065 zweites eMP-Dokument einzustellen, MUSS mit dem IHE-
- 5066 Error `InvalidDocumentContent` abgebrochen werden. Es MUSS im `codeContext`-Attribut

des zurückgegebenen `InvalidDocumentContent`-Elements der Text "Medical information object has to be unique" zurückgegeben werden. [`<=`]

[3.12.1.6.1.23.13.1.6.1.2](#) Operation `I_Document_Management::RegistryStoredQuery`
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

[3.12.1.6.1.33.13.1.6.1.3](#) Operation `I_Document_Management::RemoveMetadata`
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

[3.12.1.6.1.43.13.1.6.1.4](#) Operation `I_Document_Management::RetrieveDocumentSet`
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

[3.12.1.6.1.53.13.1.6.1.5](#) Operation
`I_Document_Management::RestrictedUpdateDocumentSet`
Weitere Details zur Ausgestaltung dieser Operation finden sich bezüglich der dazugehörigen IHE ITI-Transaktion "RestrictedUpdateDocumentSet" [ITI-92] in [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x].

Weitere Anforderungen zur Umsetzung der Operation `RestrictedUpdateDocumentSet` befinden sich in Kapitel [3.12.1.4.3.5- Restricted Update Document Set \[ITI-92\]](#) [3.13.1.4.3.5- Restricted Update Document Set \[ITI-92\]](#) .

[3.12.1.6.23.13.1.6.2](#) Schnittstelle `I_Document_Management_Insurant`

Weitere Vorgaben zu den Operationen befinden sich in [3.12.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen](#) [3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen](#) .

A_14478-01 - XDS Document Service – Implementierung der Schnittstelle `I_Document_Management_Insurant`

Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle für den Zugriff des ePA-FdV implementieren .

Tabelle 26: Schnittstelle `I_Document_Management_Insurant`

Schnittstelle	<code>I_Document_Management_Insurant</code>	
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

Schnittstelle	I_Document_Management_Insurant	
	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	[XSDDocumentService]	
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd 	

5098

5099 [\leq]5100 **A_26460 - XDS Document Service - Zugriff über**5101 **I_Document_Management_Insurant mit nicht registriertem Gerät**

5102 Falls Operationen von I_Document_Management_Insurant ohne registriertes Gerät
 5103 aufgerufen werden MUSS der XDS Document Service die Verarbeitung ablehnen und mit
 5104 einem UnregisteredDevice-Fehlercode quittieren.[\leq]

5105 3.12.1.6.2.13.13.1.6.2.1 Operation

5106 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b

5107 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 5108 Transaktion "Provide And Register Document Set-b" [ITI-41] sind [IHE-ITI-TF2x] sowie
 5109 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5110 **~~A_21481-05A_21481-04~~ - XDS Document Service – Kein Einstellen von Ordnern**
 5111 **und Associations**

5112 Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und
 5113 Dokument(en) über die Schnittstelle

5114 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b() ablehnen und
 5115 mit einem XDSRegistryMetadataError-Fehlercode quittieren, wenn in der
 5116 Eingangsnachricht ein oder mehrere neu anzulegende Folder oder andere als die
 5117 folgenden Assoziationen

5118

- SS-DE

5119 • SS-HM

5120 • FD-DE

5121 • RPLC

5122 • ~~APND~~

5123 enthalten sind. [\leq]

5124 Das Referenzieren bestehender Ordner ist davon nicht berührt, wie dies z. B. beim
5125 Einstellen von Dokumenten in Sammlungen der Fall ist (z. B. Einstellen eines Dokuments
5126 in einen Mutterpass).

5127 **A_23144 - XDS Document Service - Automatische Ablage von Dokumenten im** 5128 **Ordner "technical"**

5129 Der XDS Document Service MUSS sicherstellen, dass Dokumente mit einem formatCode
5130 mit der codeSystem OID "2.25.154081344090540725127779452347992051720",
5131 unabhängig von weiteren Metadaten, im statischen Ordner "technical" abgelegt
5132 werden. [\leq]

5133 3.12.1.6.2.23.13.1.6.2.2 Operation

5134 I_Document_Management_Insurant::RegistryStoredQuery

5135 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
5136 Transaktion "Registry Stored Query" [ITI-18] sind [IHE-ITI-TF2a], [IHE-ITI-TF2x] sowie
5137 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5138 3.12.1.6.2.33.13.1.6.2.3 Operation

5139 I_Document_Management_Insurant::RemoveMetadata

5140 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
5141 Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-
5142 ITI-TF2x] zu entnehmen.

5143 3.12.1.6.2.43.13.1.6.2.4 Operation

5144 I_Document_Management_Insurant::RetrieveDocumentSet

5145 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
5146 Transaktion "RetrieveDocumentSet" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
5147 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5148 3.12.1.6.2.53.13.1.6.2.5 Operation

5149 I_Document_Management_Insurant::RestrictedUpdateDocumentSet

5150 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
5151 Transaktion "RestrictedUpdateDocumentSet" [ITI-92] sind [IHE-ITI-RMU], [IHE-ITI-
5152 TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5153 Weitere Anforderungen zur Umsetzung der Operation RestrictedUpdateDocumentSet

5154 befinden sich in Kapitel ~~3.12.1.4.3.5- Restricted Update Document Set [ITI-~~

5155 ~~92]-3.13.1.4.3.5- Restricted Update Document Set [ITI-92].~~

5156 3.12.1.6.33.13.1.6.3 Schnittstelle I_Document_Management_Ncpeh

5157 Weitere Vorgaben zu den Operationen befinden sich in ~~3.12.1.4.3- Vorgaben zu IHE ITI-~~
5158 ~~Transaktionen bei mehreren Schnittstellen~~ 3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen
5159 bei mehreren Schnittstellen .

5160 **A_27300-01A-27300 - XDS Document Service (EU) – Implementierung der** 5161 **Schnittstelle I_Document_Management_Ncpeh**

5162 Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-
5163 Service-Schnittstelle für den Zugriff ~~des ePA-FdV~~ durch den NCPeH-FD implementieren.

5164 **Tabelle 27: Schnittstelle I_Document_Management_Ncpeh**

Schnittstelle	I_Document_Management_Ncpeh	
Version	2.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
WSDL	[XDSDocumentService]	
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd 	

5165

5166 **[<=]**5167 **3.12.1.6.3.13.13.1.6.3.1 Operation**

5168 I_Document_Management_Ncpeh::RegistryStoredQuery

5169 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 5170 Transaktion "Registry Stored Query " [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
 5171 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5172 **3.12.1.6.3.23.13.1.6.3.2 Operation**

5173 I_Document_Management_Ncpeh::RetrieveDocumentSet

5174 Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-
 5175 Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie
 5176 Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5177 **3.12.1.73.13.1.7 Statische Metadaten**

5178 Statische Inhalte werden vor der ersten Nutzung des XDS Document Service angelegt, d.
 5179 h. bevor auf XDS Metadaten zugegriffen wird. Sie sind unveränderlich.

A_24491-02 - XDS Document Service – Anlegen von statischen Ordnern

Der XDS Document Service MUSS nach der erfolgreichen Anlage der Akte des Versicherten die Kategorienordner unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A_14760* (Belegung der restlichen Metadatenfelder) für den Versicherten gemäß der folgenden Tabelle anlegen. Alle statischen Kategorienordner werden mit jeweils einem Ordner pro Kategorie angelegt. Alle statischen Ordner sind nach dem Anlegen initial leer.

Das Anlegen von Submission Sets und zugehöriger Associations zu den statischen Ordnern ist nicht vorgegeben. Das XDS-Informationsmodell MUSS allerdings hinsichtlich der Folder-DocumentEntry- sowie SubmissionSet-HasMember-Associations bei einer Verarbeitung durch die Document Consumer (z. B. Querying) erfüllt werden.

Tabelle 28: Festlegung Folder.entryUUID zu statischen Ordnern

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
reports	b878db05-49e4-4f74-a329-b3bcdd8082c4
emp	7c1054ea-a4df-4a1b-8e10-209f6d8812ee
emergency	a7bb6be7-d756-46dd-90d4-4020ed55b777
eab	2ed345b1-35a3-49e1-a4af-d71ca4f23e57
dental	af547321-b8e8-4e1d-b9af-51bb4a990bda
child	2c898452-4667-40e3-9d3e-c09d7385b527
vaccination	9c3edaf3-a978-46fe-8e6e-021ff4aca60b
patient	d236c9a2-ab01-4902-a00a-1e1dff439fe7
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d
health_risk_analysis	840a59c7-61d4-4caa-80a7-1857af2f166f
care	2d62bf9e-062a-4aa7-9951-9f33bbc665b5
eau	aa7d10d6-204a-47aa-be73-44bdcb77512f

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
other	605a9f3c-bfe8-4830-a3e3-25a4ec6612cb
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31
rehab	173f4204-fb93-4a1a-a1f6-316703b79539
transcripts	6A8E383D-8705-4B0E-A140-39A5F144501D

[<=]

Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner vom Typ "pregnancy_childbirth", mit dem und verwenden als Folder.title für den Namen des Kindes bzw. ein Kennzeichen der Schwangerschaft (A_22515-).*

A_20216-04A_20216-03 - XDS Document Service – Unveränderlichkeit von statischen Akteninhalten

Der XDS Document Service DARF die Metadaten eines statischen Aktenobjekts gemäß A_24491 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen. Dabei gelten folgende Ausnahmen:

- Folder.lastUpdateTime - Folder.lastUpdateTime wird automatisch vom XDS Document Service aktualisiert, sobald Dokumente in den Ordner eingestellt ~~oder daraus gelöscht werden,~~ (siehe auch [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6]), daraus gelöscht oder darin aktualisiert werden.

[<=]

3.12.1.8.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten

Für den XDS Document Service werden Vorgaben bezüglich zu verwendender IHE XDS-Metadatenattribute auf Ebene von Submission Set, Document Entry sowie Folder vorgenommen. Diese Nutzungsvorgaben referenzieren größtenteils Value Sets der IHE Deutschland Arbeitsgruppe "XDS Value Sets" [IHE-ITI-VS] und sind für die ePA-Fachanwendung verbindlich. Diese XDS-Value Sets sind teilweise von IHE-Deutschland als "offen" gekennzeichnet, um Erweiterungen flexibel einbringen zu können. Für die ePA-Fachanwendung gelten jedoch definierte Vorgaben, wie neue Codes und Value Sets sicher über eine Konfigurationsschnittstelle eingebracht werden können. Daher sind die in dieser Spezifikation beschriebenen Nutzungsvorgaben für Value Sets als fest anzusehen bzw. die Offenheit der XDS Value Sets wird nicht unterstützt.

3.12.1.8.13.1.8.1 Allgemeine Metadatenvorgaben

Die Spalten der unten dargestellten, tabellarischen Übersichten für die Metadaten von Dokumenten (IHE XDS.b Document Entry) und Übertragungspaketen (IHE XDS.b Submission Set) haben die folgenden Bedeutungen:

- Die Spalte "Metadatenattribut XDS.b" listet alle aus dem IHE ITI TF vorgesehenen Metadaten für Document Entry- und Submission Set-Elemente auf.

5224 • Die Spalten "Mult. PS" (Multiplizität Primärsystem; alle Primärsysteme außer PS-
5225 KTR), "Mult. KTR" (Multiplizität "PS-KTR"), "Mult. DS" (Multiplizität "Document
5226 Service"), "Mult. FV" (Multiplizität "ePA-Frontend des Versicherten") kennzeichnen
5227 die Multiplizität des Metadatenattributs beim Erzeugen oder Verarbeiten durch das
5228 jeweilige System.
5229 Die Angabe der jeweiligen Spalte entspricht einem Wertebereich. Die Zeichen [...]
5230 für Wertebereich wurden zum Zwecke der besseren Darstellbarkeit weggelassen.

5231 • Die Spalte "Kurzbeschreibung" beschreibt kurz die Bedeutung des
5232 Metadatenattributs.

5233 • Die Spalte "Nutzungsvorgabe" macht Bedingungen für die Verwendung eines
5234 Metadatenattributs (z. B. erlaubte Wertebereiche und Formatangaben), welche
5235 über die im IHE ITI TF definierten Vorgaben hinausgehen.

5236 • Die Spalte "FV Edit" beschreibt, ob ein bestimmtes Metadatenattribut beim
5237 Einstellen eines Dokuments über das ePA-FdV durch den Versicherten veränderbar
5238 gestaltet werden muss. Es sollten dabei immer nur die für den aktuellen Workflow
5239 relevanten Metadatenattribute angezeigt werden, um die Komplexität für den
5240 Versicherten gering zu halten. Veränderbar gestaltete Metadatenattribute müssen
5241 mit sinnvollen Default-Werten vorbelegt werden.

5242 **A 14760-27A_14760-25 - Nutzungsvorgaben für die Verwendung von XDS-** 5243 **Metadaten**

5244 Der XDS Document Service MUSS sicherstellen, dass Primärsysteme und das ePA-
5245 Frontend des Versicherten zur Registrierung von Dokumenten die nachstehenden
5246 Nutzungsvorgaben für Metadaten berücksichtigen. Der XDS Document Service MUSS
5247 diese Metadaten verarbeiten können und diese Metadaten ggf. während des
5248 Registriervorgangs ergänzen. Metadaten können über die Operationen

5249 • I_Document_Management::ProvideAndRegisterDocumentSet-b sowie

5250 • I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b

5251 registriert oder über die Operationen

5252 • I_Document_Management::RestrictedUpdateDocumentSet

5253 • I_Document_Management_Insurant::RestrictedUpdateDocumentSet

5254 geändert werden.

5255 Für den Produkttyp DiGA gelten die gleichen Vorgaben wie für die Primärsysteme sofern
5256 unter Nutzungsvorgaben keine abweichenden Bedingungen definiert werden.

5257 **Tabelle 29: Nutzungsvorgaben für Metadatenattribute XDS**

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
Metadaten für DocumentEntry							

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
author	1. .n	1. .1	0. .0	0. .n	Person oder System, welche(s) das Dokument erstellt hat	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.1] genügen. Das Primärsystem MUSS mindestens das Subattribut authorPerson oder authorInstitution inhaltlich belegen.	
authorPerson	0. .1	0. .1	0. .0	0. .1	Name des Autors	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 3.12.1.8.2-Metadaten der Dokumente und SubmissionSets3.13.1.8.2-Metadaten der Dokumente und SubmissionSets genügen.	X
authorInstitution	0. .n	0. .n	0. .0	0. .n	Institution, die dem Autor zugeordnet ist	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 3.12.1.8.2-Metadaten der Dokumente und SubmissionSets3.13.1.8.2-Metadaten der Dokumente und SubmissionSets (A_21209) genügen.	X
authorRole	0. .n	0. .n	0. .0	0. .n	Rolle des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS aus [gemTerminologyIG TI Terminology] entsprechen.	X
authorSpecialty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorSpecialtyVS aus [gemTerminologyIG TI Terminology] entsprechen.	X
authorTelecommunication	0. .n	0. .0	0. .0	0. .n	Telekommunikationsdaten des Autors	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
availabilityStatus	0. .0	0. .0	1. .1	0. .0	Status des Dokuments ("Approved" oder "Deprecated")	Der Wert MUSS initial "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
classCode	1. .1	1. .1	0. .0	1. .1	Grobe Klassifizierung des Dokuments	<p>Der Wert MUSS einem Code des Value Sets EPAXDSCClassCodeVS aus [gemTerminologyIG TI Terminology] entsprechen.</p> <p>Sofern das Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.12.1.9- Strukturierte Dokumente3.13.1.9- Strukturierte Dokumente genügen.</p> <p>PS-KTR MUSS für Dokumente</p> <ul style="list-style-type: none"> • der Kategorie receipt ausschließlich den Code "ADM" (Administratives Dokument) verwenden • und für solche der Kategorie health_risk_analysis den Code "ASM" (Assessment) verwenden. 	X
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.4] genügen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
confidentialityCode	0. .n	0. .n	0. .1	0. .n	Vertraulichkeitskennzeichnung des Dokuments	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3# 4.2.3.2.5] genügen und einem Code des Value Sets EPAXDSConfidentialityCodeVS aus [gemTerminologyIG_TI_Terminology] entsprechen.</p> <p>Für ProvideAndRegisterDocuments et-b MUSS für das Verbergen des Dokumentes der Code</p> <ul style="list-style-type: none"> Code = "CON", Display Name = "constraint" <p>aus dem Code System 1.2.276.0.76.5.491 (siehe auch Value Set EPAXDSConfidentialityCodeVS aus [gemTerminologyIG_TI_Terminology]) gesetzt werden.</p>	X
creationTime	1. .1	1. .1	0. .0	1. .1	Erstellungszeitpunkt des Dokuments	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.6] genügen und DARF NICHT in der Zukunft liegen. Bei der Prüfung ist eine Toleranz von 5 Minuten zulässig.</p>	X
entryUUID	1. .1	1. .1	0. .1	1. .1	Intern verwendete, aktenweit eindeutige Kennung des Dokuments	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.7] genügen.</p> <p>Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.</p>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
eventCodeList	0. .n	0. .0	0. .0	0. .n	Ereignisse, die zur Erstellung des Dokuments geführt haben.	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.8] genügen und einem Code<u>Codes</u> des Value Sets<u>Set</u> EPAXDSEventCodeVS aus <u>[gemTerminologyIG TI Terminology]</u> entsprechen.</p> <p><u>Der Wert darf höchstens einen KDL-Code ("Klinische Dokumentenklassen-Liste") und höchstens einen DMP-Code ("Disease Management Programm") enthalten.</u></p> <p><u>Hinweis: Frühere Versionen der ePA für alle haben das Einstellen von mehreren KDL- bzw. DMP-Codes in die eventCodeList nicht unterbunden. Deshalb kann es Altdaten geben, die noch mehr als einen Code der entsprechenden Code-Systeme in der eventCodeList enthalten.</u></p>	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
formatCode	1. .1	1. .1	0. .0	1. .1	<p>Global eindeutiger Code für das Dokumentenformat.</p> <p>Zusammen mit dem DocumentEntry.typeCode eines Dokuments soll es einem potentiellen zugreifenden System erlauben, im Vorfeld festzustellen, ob das Dokument verarbeitet werden kann.</p>	<p>Der Wert MUSS einem Code des Value Sets EPAXDSFormatCode aus [gemTerminologyIG TI Terminology] entsprechen. Der Wert KANN "urn:ihe:iti:xds:2017:mimeTypeSufficient" (siehe [IHE-ITI-TF-3#4.2.3.2.9]) entsprechen, um anzuzeigen, dass über den MIME-Type hinaus keine genaueren Angaben zum Dokumentenformat gemacht werden können oder der MIME-Type ausreichend ist.</p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.12.1.9- Strukturierte Dokumente genügen, 3.13.1.9-Strukturierte Dokumente genügen.</p>	
hash	0. .0	0. .0	1. .1	0. .0	Kryptographische Prüfsumme des Dokuments	Der Wert wird vom XDS Document Service beim Einstellen des Dokuments in die Akte berechnet.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
healthcareFacilityTypeCode	1. .1	1. .1	0. .0	1. .1	Art der Einrichtung, in der das dokumentierte Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSHealthcareFacilityTypeCodeVS aus [gemTerminologyIG TI Terminology] entsprechen. Das PS-KTR MUSS healthcareFacilityTypeCode ausschließlich mit dem Wert "VER" (Versicherungsträger) belegen. Die DiGA MUSS healthcareFacilityTypeCode mit dem Wert "PAT" belegen.	X
homeCommunityId	0. .1	0. .1	0. .0	0. .1		n/a Eine optional übertragene homeCommunityId wird nicht gespeichert.	
languageCode	1. .1	1. .1	0. .0	1. .1	Sprache, in der das Dokument abgefasst ist.	Der Wert MUSS einem Code des Value Sets EPAXDSLLanguageCodeVS aus [gemTerminologyIG TI Terminology] entsprechen. Es MÜSSEN mindestens die in der Tabelle Tab_LanguageCodes angegebenen Codes unterstützt werden, alle weiteren Codes KÖNNEN unterstützt werden.	X
legalAuthenticator	0. .1	0. .0	0. .0	0. .1	Rechtlich Verantwortlicher für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.14] genügen. Das Attribut DARF NICHT gesetzt werden, falls es sich um ein automatisch erstelltes und nicht durch eine natürliche Person freigegebenes Dokument handelt.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierungsattri- but, dass das Metadateneleme- nt DocumentEntry nicht den vollständigen Satz an Metadaten enthält.		
contentType	1. .1	1. .1	0. .0	1. .1	MIME-Type des Dokuments	<p>Ein Wert aus der folgenden Liste gemäß A_24864* und A_25009* MUSS als MIME-Type verwendet werden.</p> <p>PS-KTR MUSS für Dokumente der Kategorie health_risk_analysis ausschließlich den Wert "application/pdf" gemäß A_25009-* verwenden. Als formatCode ist dann entsprechend "urn:ihe:iti:xds:2 017:mimeTypeSufficient" zu verwenden</p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.12.1.9- Strukturierte Dokumente genügen. 3.13.1.9- Strukturierte Dokumente genügen. Anmerkung: In Klammern sind die Extensions angegeben, die beim entsprechenden MIME-Type in DocumentEntry.URI für das URI-scheme "file," zu verwenden sind.</p>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
objectType	1. .1	1. .1	0. .0	1. .1	Typ des Dokuments	Der Wert MUSS immer "urn:uuid:7edca82f-054d- 47f2-a032-9b2a5b5186c1" betragen. Dieser Wert steht für stabile Dokumente im IHE ITI XDS.b-Profil [IHE-ITI- TF3#4.2.5.2].	
patientId	1. .1	1. .1	0. .0	1. .1	Systemweit eindeutige Kennung des Patienten	Der Wert MUSS den Inhalts- und Formatvorgaben aus A_14974* genügen. Außerdem MUSS der Wert der Identität des Akteninhabers entsprechen und MUSS vom XDS Document Service dahingehend bei Registrierung der Metadaten geprüft werden.	
practiceSettingC ode	1. .1	0. .0	0. .0	1. .1	Art der Fachrichtung der erstellenden Einrichtung, in der das dokumentiere Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSPracticeSettingCodeVS aus [gemTerminologyIG TI Termin ology] entsprechen. Die DiGA MUSS practiceSettingCode mit dem Wert "PAT" belegen.	X
referenceIdList	0. .n	0. .1	1. .1	0. .n	Liste von IDs, mit denen das Dokument assoziiert wird.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.28] genügen. Wenn KTR-Clients einen Wert übertragen, muss es sich um die rootDocumentId im Rahmen einer RMU-Operation (Aktualisierung) oder dem Ersetzen (RPLC) eines Dokuments handeln.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
repositoryUniqu eId	0. .1	0. .1	1. .1	0. .1	Kennung des Document Repository, in welches das Dokument eingestellt wird/wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.18] genügen.	
serviceStartTim e	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
serviceStopTim e	0. .1	0. .1	0. .0	0. .1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis beendet wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.20] genügen.	X
size	0. .0	0. .0	1. .1	0. .0	Größe des Dokuments in Bytes	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.21] genügen. Der XDS Document Service MUSS die Größe des Dokuments berechnen und in den Metadaten während des Registriervorgangs setzen (vgl. [IHE-ITI-TF2b#3.41.4.1.3]).	
sourcePatientId	0. .1	0. .0	0. .0	0. .0	Kennung des Patienten im Quellsystem	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.22] genügen.	
sourcePatientInf o	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.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
title	1. .1	1. .1	1. .1	1. .1	Titel des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.24] genügen. Ein leeres Feld <code>DocumentEntry.title=""</code> bzw. ausschließlich mit nicht druckbaren Zeichen befüllt ist nicht erlaubt.	X
typeCode	1. .1	1. .1	0. .0	1. .1	Art des Dokuments	<p>Der Wert MUSS einem Code des Value Sets EPAXDSTypeCodeVS aus [gemTerminologyIG_TI_Terminology] entsprechen.</p> <p>PS-KTR MUSS für Dokumente der Kategorie <code>health_risk_analysis</code> ausschließlich den Code "GRIS" verwenden</p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Inhalts- und Formatvorgaben aus Abschnitt 3.12.1.9- Strukturierte Dokumente genügen. 3.13.1.9- Strukturierte Dokumente genügen.</p>	X
uniqueId	1. .1	1. .1	0. .0	1. .1	Eindeutige, aktenweite Kennung des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.26] genügen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
URI	1. .1	1. .1	0. .0	1. .1	URI für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.27] genügen und mittels A_24524-* normalisiert werden. Die extension der DocumentEntry.URI MUSS wird dem mimetype gemäß A_23447-* angepasst, falls erforderlich.	
Metadaten für SubmissionSet							
author	1. .n	1. .1	0. .0	1. .1	Person oder System, welche(s) das Submission Set erstellt hat.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.3.1] genügen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorPerson	0. .1	0. .1	0. .0	0. .1	Name der einstellenden Per son oder des einstellenden Systems	<p>Der Wert MUSS den Formatvorgaben aus Abschnitt 3.12.1.8.2 <u>Metadaten der Dokumente und SubmissionSets</u> 3.13.1.8.2 <u>Metadaten der Dokumente und SubmissionSets</u> genügen.</p> <p>ePA-FdV: Das ePA-Aktensystem MUSS die KVNR mit den Inhalten der User Session auf Übereinstimmung prüfen. Eine Gleichheit liegt vor, wenn die KVNR aus der XCN-Struktur des Autors nach den Vorgaben von A_14762-* mit dem entsprechenden Wert aus der User Session übereinstimmt. Ist authorPerson nicht gesetzt, MUSS das ePA Aktensystem das Metadatenattribut authorPerson für Versicherte entsprechend der Vorgaben aus A_14762-* unter Verwendung der entsprechenden Informationen aus der User Session (KVNR, family_name und given_name) setzen.</p> <p>Das ePA Aktensystem KANN in einer übergebenen authorPerson den Nachnamen und Vornamen mit Informationen aus der User Session überschreiben. PS/DiGAs können hier im Bedarfsfall Einträge für Software-Komponente bzw. Gerät als Autor entsprechend A_14762-* vornehmen.</p>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorInstitution	0. .1	0. .1	0. .0	0. .0	Institution, welcher die einstellende Pers on oder das einstellende System zugeordnet ist.	<p>Der Wert MUSS den Formatvorgaben aus Abschnitt 3.12.1.8.2-Metadaten der Dokumente und SubmissionSets<u>3.13.1.8.2- Metadaten der Dokumente und SubmissionSets</u> (A_21209*) genügen.</p> <p>Das ePA-Aktensystem MUSS die Identität von TelematikID- basierten Identitäten mit den Inhalten aus authorInstitution prüfen.</p> <p>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.</p> <p>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.</p>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorRole	1. .n	1. .n	0. .0	1. .1	Rolle der einstellenden Per son oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS aus [gemTerminologyIG TI Terminology] entsprechen. Das PS-KTR MUSS den Code "105" (Kostenträgervertreter) verwenden. Das ePA-Frontend des Versicherten MUSS den Code "102" (der Patient selbst) verwenden. Die DiGA MUSS authorRole mit dem Code "12" (dokumentierendes Gerät) verwenden.	
authorSpecial ty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung der einstellenden Per son oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorSpecialtyVS aus [gemTerminologyIG TI Terminology] entsprechen.	
authorTeleco mmunication	0. .n	0. .0	0. .0	0. .n	Telekommunikati onsdaten der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.1.4.5] genügen.	
availabilityStatu s	0. .0	0. .0	1. .1	0. .0	Status des Submission Sets ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approved" entsprechen.	
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise zum Submission Set in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.3.3] genügen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
contentTypeCode	0. .1	0. .1	0. .0	0. .1	Klinische Aktivität, die zum Einstellen des Submission Set geführt hat.	Der Wert MUSS einem Code des Value Sets EPAXDSContentTypeCodeVS aus [gemTerminologyIG_TI_Terminology] entsprechen.	
entryUUID	1. .1	1. .1	0. .1	1. .1	Intern verwendete, aktenweit eindeutige Kennung des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.5] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
intendedRecipient	0. .n	0. .0	0. .0	0. .n	Vorgesehener Adressat des Submission Set	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.7] genügen.	
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierung, welche anzeigt, dass das Submission Set nicht den durch das IHE ITI TF vorgegebenen Satz an Metadaten enthält.		
patientId	1. .1	1. .1	0. .0	1. .1	Patienten-ID, zu der das Submission Set gehört	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
sourceId	0. .0	0. .0	0. .0	0. .0	Weltweit eindeutige, unveränderliche Kennung des einstellenden Systems		

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
submissionTime	1. .1	1. .1	0. .0	1. .1	Zeit, zu der das Submission Set zusammengestellt wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.10] genügen. Der XDS Document Service MUSS prüfen, ob der Wert der aktuellen Systemzeit entspricht. Sollte diese von der lokalen Zeit über mehr als eine Minute abweichen, MUSS der Wert mit der aktuellen Systemzeit ersetzt werden. Diese Systemzeit MUSS dabei synchron zur Systemzeit des Produkttyps Zeitdienst gemäß A_24673 sein.	
title	0. .1	0. .1	0. .0	0. .1	Titel des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.11] genügen.	X
uniqueId	1. .1	1. .1	0. .0	1. .1	Eindeutige Kennung des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.12] genügen.	
Metadaten für dynamische Folder							
availabilityStatus	1. .1	n/ a	0. .0	n/ a	Status des Ordners ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
codeList	1. .1	n/ a	0. .0	n/ a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] und einem Code des Value Sets EPADataCategoryOtherVS aus [gemTerminologyIG TI Terminology] entsprechen. Bei Folder.codeList=pregnancy_childbirth MUSS das Primärsystem diese Codes angeben.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
comments	0. .1	n/ a	0. .0	n/ a	Freitextkommentar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen.	
entryUUID	1. .1	n/ a	1. .1	n/ a	Intern verwendete, aktenweit eindeutige Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
lastUpdateTime	0. .0	n/ a	1. .1	n/ a	Zeitstempel, an dem der Ordner das letzte mal geändert wurde	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.6] genügen. Der XDS Document Service MUSS den Wert automatisch gemäß [IHE-ITI-TF2b#3.42.4.1.3.6] aktuell halten. <u>Zudem MUSS der XDS Document Service den Wert aktualisieren, wenn ein Dokument aus dem Ordner gelöscht oder dessen Metadaten aktualisiert wurden.</u>	
limitedMetadata	Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden.						
patientId	1. .1	n/ a	0. .0	n/ a	Patienten ID, zu der der Ordner gehört.	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
title	1. .1	n/ a	0. .0	n/ a	Titel des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.8] genügen.	
uniqueId	1. .1	n/ a	0. .0	n/ a	Eindeutige, aktenweite Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.9] genügen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
Metadaten für statische Folder							
availabilityStatus	n/a	n/a	1. .1	n/a	Status des Ordners ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
codeList	n/a	n/a	1. .1	n/a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] und einem Code des Value Sets EPADDataCategoryOtherVS und EPADDataCategoryMedicalVS aus [gemTerminologyIG TI Terminology] entsprechen. Der XDS Document Service MUSS codeList gemäß A_19388* setzen.	
comments	n/a	n/a	0. .1	n/a	Freitextkommentar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen.	
entryUUID	n/a	n/a	1. .1	n/a	Intern verwendete, aktenweit eindeutige Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
lastUpdateTime	n/ a	n/ a	1. .1	n/ a	Zeitstempel, an dem der Ordner das letzte mal geändert wurde	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.6] genügen. Der XDS Document Service MUSS den Wert automatisch gemäß [IHE-ITI-TF2b#3.42.4.1.3.6] aktuell halten. <u>Zudem MUSS der XDS Document Service den Wert aktualisieren, wenn ein Dokument aus dem Ordner gelöscht oder dessen Metadaten aktualisiert wurden.</u>	
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.	

5258
5259**Tabelle 30: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language Codes**

Language / Country Code Kombination	Language / Country Code Kombination
bg-BG (bulgarisch, Bulgarien)	it-IT (italienisch, Italien) it-CH (italienisch, Schweiz)
cs-CZ (tschechisch, Tschechien)	lt-LT (litauisch, Litauen)

Language / Country Code Kombination	Language / Country Code Kombination
da-DK (dänisch, Dänemark)	lb-LU (luxemburgisch, Luxemburg)
de-AT (deutsch, Österreich) de-DE (deutsch, Deutschland) de-CH (deutsch, Schweiz) de-LI (deutsch, Liechtenstein) de-LU (deutsch, Luxemburg)	lv-LV (lettisch, Lettland)
el-GR (griechisch, Griechenland)	mt-MT (maltesisch, Malta)
en-GB (englisch, Vereinigtes Königreich)	nl-NL (niederländisch, Niederlande) nl-BE (niederländisch, Belgien)
es-ES (spanisch, Spanien)	no-NO (norwegisch, Norwegen)
et-EE (estnisch, Estland)	pl-PL (polnisch, Polen)
fi-FI (finnisch, Finnland)	pt-PT (portugiesisch, Portugal)
fr-FR (französisch, Frankreich) fr-CH (französisch, Schweiz) fr-LU (französisch, Luxemburg) fr-BE (französisch, Belgien)	rm-CH (rätoromanisch, Schweiz)
ga-IE (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)

5260

5261 **[<=]**5262 3.12.1.8.23.13.1.8.2 Metadaten der Dokumente und SubmissionSets5263 **A_23369-02 - XDS Document Service – Verpflichtender Dokumententitel in**
5264 **DocumentEntry.title**

5265 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
 5266 Dokumenten und dem Ändern von Metadaten an Dokumenten `DocumentEntry.title`
 5267 befüllen. Der Titel des Dokumentes soll eine fachliche Beschreibung des Dokumentes
 5268 enthalten. Bei `DocumentEntry.title` MÜSSEN führende und endende Leerzeichen
 5269 entfernt werden. In `DocumentEntry.title` DARF NICHT leer sein (!= "") (insbesondere
 5270 auch nicht nach etwaigen Entfernen von Leerzeichen vorne und hinten). In
 5271 `Document.title` DÜRFEN keine nicht-druckbaren Zeichen enthalten sein. **[<=]**

A_25188 - XDS Document Service - Input Sanitization

Der XDS Document Service MUSS sicherstellen, dass bei Anlage und Aktualisierung (Ändern) von Metadaten:

1. führende (leading) und endende (trailing) Whitespace von den Attributen automatisch entfernt werden.
2. die notwendigen Attribute nichtleer sind (insbesondere auch noch Whitespace-Entfernung aus 1.). und
3. Die Attribute nur druckbare Zeichen enthalten.

[<=]

A_14762-05 - XDS Document Service – Nutzungsvorgabe für authorPerson als Teil von DocumentEntry.author und SubmissionSet.author

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an `authorPerson` unterhalb von `DocumentEntry.author` und `SubmissionSet.author` neben [IHE-ITI-TF3#4.2.3.1.4.2] auch die folgenden Vorgaben beachten.

Bei Leistungserbringer als Autor:

1. Lebenslange Identifikationsnummer eines Arztes (Lebenslange Arztnummer - LANR 9 Stellen) oder im Falle eines Zahnarztes die Zentrale Zahnarzt Nummer (ZANR)- sofern die ZANR bekannt ist
2. "^"
3. Nachname
4. "^"
5. Vorname
6. "^"
7. Weiterer Vorname
8. "^"
9. Namenszusatz
10. "^"
11. Titel
12. "^^^&" - sofern LANR oder ZANR angegeben, ansonsten "^^^"
13. "1.2.276.0.76.4.16" - sofern LANR angegeben oder "1.2.276.0.76.4.296", falls ZANR angegeben
14. "&ISO" - sofern LANR oder ZANR angegeben

Beispiele:

165746304^Weber^Thilo^^^Dr.^^^&1.2.276.0.76.4.16&ISO
^Zahnschmerz^Eberhard^^^Dr.^^^

Bei Versichertem als Autor:

1. Der unveränderbare Teil der KVNR (10 Stellen)
2. "^"
3. Nachname

- 5314 4. "^"
- 5315 5. Vorname
- 5316 6. "^"
- 5317 7. Weiterer Vorname
- 5318 8. "^"
- 5319 9. Namenszusatz
- 5320 10. "^"
- 5321 11. Titel
- 5322 12. "^^^&"
- 5323 13. "1.2.276.0.76.4.8"
- 5324 14. "&ISO"

5325 Beispiel: G995030566^Gundlach^Monika^^^^^&1.2.276.0.76.4.8&ISO
 5326 Sowohl beim LE als auch beim Versicherten müssen Vorname und Nachname belegt
 5327 werden.

5328
 5329 **Software-Komponente bzw. Gerät als Autor**
 5330 Beim (automatisierten) Einstellen von Dokumenten MUSS der max. 256-Zeichen lange
 5331 Name der Software-Komponente bzw. des Geräts als Nachname und ggf. als Vorname(n)
 5332 eingetragen werden.

5333 Beispiel: ^PHR-Gerät-XY^PHR-Software-XY
 5334 Im Falle einer DiGA MUSS das Feld Autor folgendermaßen aufgebaut sein:

- 5335 1. Telematik-ID der DiGA
- 5336 2. "A"
- 5337 3. Name der DiGA (Name der Verordnungseinheit)
- 5338 4. "A"
- 5339 5. Name des DiGA-Herstellers
- 5340 6. "A"
- 5341 7. optionale Ergänzung der Bezeichnung der SW
- 5342 8. "A"
- 5343 9. optionale Ergänzung der Bezeichnung der SW
- 5344 10. "A"
- 5345 11. optionale Ergänzung der Bezeichnung der SW
- 5346 12. "^^^&"
- 5347 13. <OID für DiGAs, wie in professionOID>
- 5348 14. "&ISO"

5349
 5350 Für alle drei Arten von Autoren (Versicherter, LE, Gerät) MUSS jeweils Vorname und
 5351 Nachname angegeben sein. [<=]

A_14763-03 - XDS Document Service - Nutzungsvorgabe für SubmissionSet.authorInstitution

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an SubmissionSet.authorInstitution neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

Beispiele:

- Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-e518
- gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^8-34923902a

[<=]

A_21511-01 - Nutzungsvorgabe SubmissionSet.authorInstitution für DIGAs

Der XDS Document Service MUSS sicherstellen, dass DiGAs beim Upload von Dokumenten, die folgenden Nutzungsvorgaben für das Metadatenattribut DocumentEntry.authorInstitution sowie SubmissionSet.authorInstitution berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.1.4.1] genügen und ist inhaltlich nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen.

1. Name des Anbieters der DiGA
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der DiGA

[<=]

A_21209-02 - XDS Document Service - Nutzungsvorgabe für DocumentEntry.authorInstitution

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an DocumentEntry.authorInstitution neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"

5395 5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

5396 Die Komponenten 2.-5. sind nur anzugeben, wenn die Telematik ID (5.) der
 5397 Autoreninstitution bekannt ist oder ad-hoc ermittelt werden kann, bspw. über den
 5398 Verzeichnisdienst der TI-Plattform (VZD). Ansonsten wird ausschließlich der Name
 5399 gesetzt.

5400 Beispiele:

5401 • Arztpraxis Dr. Thilo Weber^^^^^1.2.276.0.76.4.188&ISO^^^^1-2c47sd-
 5402 e518

5403 • gematik Betriebskrankenkasse^^^^^1.2.276.0.76.4.188&ISO^^^^8-
 5404 34923902a

5405 • Arztpraxis Dr. Wiebke Werner

5406 [`<=`]

5407 **A_22408-02 - XDS Document Service - DocumentEntry.authorInstitution ohne** 5408 **Telematik-ID**

5409 Der XDS Document Service MUSS Nachrichten zum Registrieren von Dokumenten bei
 5410 fehlender Telematik-ID in `DocumentEntry.authorInstitution` akzeptieren und
 5411 daraufhin alle Zeichen hinter dem Namen der `authorInstitution` abschneiden und
 5412 verwerfen.[`<=`]

5413 **A_14974-02 - XDS Document Service - Nutzungsvorgabe für** 5414 **DocumentEntry.patientId und SubmissionSet.patientId**

5415 Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von
 5416 Dokumenten und dem Ändern von Dokumenten-Metadaten die folgenden
 5417 Nutzungsvorgaben für `DocumentEntry.patientId` und `SubmissionSet.patientId`
 5418 berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.2.16] bzw. [IHE-
 5419 ITI-TF3#4.2.3.3.8] genügen und ist inhaltlich nach der folgenden Vorschrift
 5420 zusammenzufügen bzw. zu belegen:

- 5421 1. Der unveränderbare Teil der KVNR des Akteninhabers (10 Stellen)
- 5422 2. "^^^^&"
- 5423 3. "1.2.276.0.76.4.8" (OID zur Kennzeichnung einer unveränderbaren KVNR)
- 5424 4. "&ISO"

5425 Beispiel: G995030566^^^&1.2.276.0.76.4.8&ISO[`<=`]

5426 3.12.1.8.33.13.1.8.3 Metadaten für Datenkategorien

5427 **A_19388-21 - Nutzungsvorgaben für die Verwendung von Datenkategorien**

5428 Der XDS Document Service MUSS beim Einstellen eines Dokuments und beim Ändern von
 5429 Metadaten die folgende Zuordnung zu einer Datenkategorie (d. h. Assoziierung mit einem
 5430 bestimmten Folder) vornehmen. Dabei haben Auswertungs- und Zuordnungsregeln, die
 5431 sich aus A_14761-* und damit verbunden aus [gemSpec_IG_ePA] ableiten, immer den
 5432 Vorrang gegenüber anderen Auswertungsregeln. Ferner MUSS der XDS Document
 5433 Service sicherstellen, dass bei einer Aktualisierung eines Dokuments derselbe Ordner des
 5434 zu ersetzenden Dokuments zugeordnet wird.

5435

5436 Für eine eindeutige Zuordnung zu einer Datenkategorie MUSS die Auswertung der
 5437 Metadatenvorgaben in der Reihenfolge der folgend dargestellten Einsortierungskriterien
 5438 erfolgen:

5439 **Tabelle 31: Einsortierung_Datenkategorien**

Datenkategorie/Technischer Identifier/Foldercode	Einsortierkriterium (anzuwenden auf DocumentEntry, wenn nicht anders angegeben. Oder-Verknüpfungen, wenn nicht "und" angegeben)
receipt	healthcareFacilityTypeCode = VER und typeCode = ABRE und DocumentEntry.authorRole=105 und Submissionset.authorRole = 105
health_risk_analysis	healthcareFacilityTypeCode = VER und typeCode = GRIS und DocumentEntry.authorRole=105 und Submissionset.authorRole = 105
patient	Dokumente bei denen der Einsteller der Versicherte oder sein Vertreter ist: Submissionset.authorRole = 102 Dokumente bei denen der Einsteller der Kostenträger ist: Submissionset.authorRole = 105
pregnancy_childbirth	healthcareFacilityTypeCode = HEB eventCodeList=SD070104 (KDL-Code Neugeborenenenscreening)
eab	classCode = BRI
care	PracticeSettingCode = PFL*
rehab	practiceSettingCode = REHA
dental	practiceSettingCode = MZKH*
emergency	eventCodeList = <ul style="list-style-type: none"> • ED110102 (KDL-Code Notfalldatenmanagement (NFD)) • AU190104 (KDL-Code Notfalldatensatz) • AD020105 (KDL-Code Notfall-/Vertretungsschein)
transcripts	eventCodeList = <ul style="list-style-type: none"> • UB999997 (KDL-Code Gesamtdokumentation stationäre Versorgung) oder • UB999998 (KDL-Code Gesamtdokumentation ambulante Versorgung)

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

*Falls Basiskonzepte angegeben werden, dann gelten automatisch alle Subkonzepte, z.B. gilt für die Kategorie "care" die Einsortierregel bei PracticeSettingCode = PFL wie auch für die Sub-Konzepte ALT (Altenpflege) und KIN (Kinderpflege). [**<=**]

3.13.1.8.4 Datenmigration

Dieser Abschnitt enthält Vorgaben für Datenanpassungen, die für bestehende Daten im XDS Document Service vorgenommen werden müssen (z. B. wenn sie durch Änderungen im Rahmen einer neuen Version des XDS Document Service notwendig werden).

A 27482 - 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.
[**<=**]

A 27661 - Migration von APND-Assoziationen

Der XDS Document Service MUSS sobald möglich Associations vom Typ "urn:ihe:iti:2007:AssociationType:APND" wie folgt ersetzen:

1. Der DocumentEntry, auf den Association.sourceObject zeigt (der "Anhang"), MUSS in DocumentEntry.referenceIdList mit dem urn:gematik:iti:xds:2025:parentDocument ausgezeichneten Wert der DocumentEntry.uniqueId desjenigen Dokuments ergänzt werden, auf das Association.targetObject zeigt.
2. Der DocumentEntry, auf den Association.targetObject zeigt (der "Hauptdokument"), MUSS in DocumentEntry.referenceIdList mit dem mittels urn:gematik:iti:xds:2025:childDocument ausgezeichneten Wert der DocumentEntry.uniqueId desjenigen Dokuments ergänzt werden, auf das Association.sourceObject zeigt.
3. Anschließend ist die APND-Association zu löschen

[**<=**]

Bei der Migration on APND-Associations können Anhangsketten entstehen, die länger als insgesamt fünf Dokumente umfassen. Das ist über das Einstellen von Dokumenten über Provide and Register Document Set [ITI-41] oder Restricted Update Document Set [ITI-92] nicht möglich.

3.12.1.9 3.13.1.9 Strukturierte Dokumente

Die elektronische Patientenakte unterstützt unterschiedliche sogenannte "strukturierte Dokumente", deren Aufbau über Implementation Guides genau vorgegeben ist. Der Umfang der unterstützten strukturierten Dokumente wird durch den Umfang der veröffentlichten Implementation Guides festgelegt (~~3.12.1.9.2- Konfigurierbarkeit~~)-(3.13.1.9.2- Konfigurierbarkeit). Für alle strukturierten Dokumente gelten spezifische Metadatenvorgaben, um sie eindeutig zu identifizieren und gezielt verarbeiten zu können.

A_14761-08 - Nutzungsvorgaben für die Verwendung von IHE ITI XDS-Metadaten bei strukturierten Dokumenten

Der XDS Document Service MUSS die Nutzungsvorgaben für strukturierte Dokumente unter [gemSpec_IG_ePA] berücksichtigen. Dabei ist das Format des Dokuments, welches über einen Code des Metadatenattributs `formatCode` ausgedrückt wird, führend. Das bedeutet, bei Registrierung eines strukturierten Dokuments mit einem `formatCode` MÜSSEN die weiteren Metadatenattribute `classCode`, `typeCode`, `mimeType` sowie `eventCodeList` entsprechend belegt werden. Der XDS Document Service MUSS eine solche Registrierung diesbzgl. prüfen und im Fehlerfall analog zu A_14938-* antworten. [`<=`]

3.12.1.9 3.13.1.9.1 Sammlungstypen

Je nach Art ihrer Zusammensetzung und ihrer Handhabung existieren unterschiedliche Typen strukturierter Dokumente, sogenannte medizinische Informationsobjekte. Ein medizinisches Informationsobjekt (MIO) ist eine **Sammlung** von Informationen zu medizinischen, strukturellen oder administrativen Sachverhalten, die in sich geschlossen oder entsprechend verschachtelt vorliegt. Zudem ist ein MIO eine klar definierte Vorgabe, wie diese Informationssammlung in der elektronischen Patientenakte gespeichert wird, damit semantische und syntaktische Interoperabilität gewährleistet werden. Die Festlegung dieser Vorgaben ist gemäß SGB V Aufgabe der KBV. Beispiele für medizinische Informationsobjekte sind der Impfpass, das Kinderuntersuchungsheft, der Mutterpass, das zahnärztliche Bonusheft, oder DiGA. MIOs werden über Sammlungen und Sammlungstypen umgesetzt.

Einige strukturierte Dokumente sind für sich genommen vollständig und schlüssig wie z. B. ein Elektronischer Arztbrief. Sie sind ohne Zuhilfenahme weiterer Dokumente in der ePA für einen Benutzer sinnvoll zu verwenden. Andere Typen strukturierter Dokumente müssen hingegen fast immer in Kombination betrachtet werden, z. B. Impfpassdokumente. Bei letzteren spiegelt jedes Impfpassdokument ein oder mehrere Impfungen wieder. Ein Impfpass, wie er in der analogen Welt geläufig und als logisches Konstrukt sinnvoll ist, besteht immer aus der gemeinsamen Betrachtung aller Impfpassdokumente und somit aller vorhandenen Impfeinträge. Die Kombination ein oder mehrerer strukturierter Dokumente ergeben eine Sammlung.

Eine Sammlungsinstanz (z. B. der Mutterpass der ersten Schwangerschaft der Patientin Martha Mustermann) ist eine konkrete Ausprägung der Information, die zwischen den beteiligten Akteuren ausgetauscht wird. Nicht jede Sammlung besteht zwangsläufig aus Dokumenten desselben Formats: Ein Kinderuntersuchungsheft beispielsweise besteht aus Dokumenten mit drei verschiedenen strukturierten Dokumenttypen. Zentral für alle Sammlungstypen ist immer mindestens ein strukturiertes Dokument mit einem festgelegten Dokumentenformat. Für eine technische Umsetzung sind die Sammlungstypen "mixed" und "uniform" zu unterscheiden, die technisch unterschiedlich umgesetzt werden und zum Teil unterschiedliche Operationen erlauben.

Der Sammlungstyp "mixed" fasst semantisch zusammengehörige, strukturierte Dokumente unterschiedlicher Struktur mittels Ordner zu einer Sammlung zusammen. Der

Sammlungstyp "uniform" wird ebenfalls intern über Ordner abgebildet. Dies stellt sicher, dass zukünftige Versionen dieser strukturierten Dokumente/Pässe oder DiGA verlässlich verarbeitet werden können. Ordner gelten als "statische Ordner", bis auf Sammlungen der Kategorie Mutterpass und DiGA ("dynamische Ordner"). Der dynamische Ordner für einen konkreten Mutterpass wird durch den Client angelegt, weil es aus Gründen, die nur der Client kennt (Anzahl der Schwangerschaften), mehrere Ordner dieses Typs geben kann ("nicht-statische Ordner", vgl. A_21610-*). Die Version der Struktur eines Dokuments ist am Format Code erkennbar.

Passdokumente

A_20577-06 - Definition und Zuweisung von Sammlungstypen

Der XDS Document Service MUSS jeder Sammlung einen von zwei Sammlungstypen zuweisen:

Tabelle 32: TAB_EPA_Sammlungstypen

Sammlungstyp	Definition
mixed	Ordner, die einer Sammlung des Typs "mixed" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) mit einem für die Sammlung festgelegten Code in der Folder.codeList abgelegt werden.
uniform	Ordner, die einer Sammlung des Typs "uniform" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) abgelegt werden.

Es gelten die Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA]. In den unter [gemSpec_IG_ePA] gemachten Vorgaben werden auch Ordner-Kardinalitäten für spezifische Sammlungen festgelegt. Diese Angaben sagen aus, wie viele Instanzen einer Sammlung (d. h. minimal und maximal) registriert werden können. [\leq]

A_20707-04 - XDS Document Service – Keine unpassenden Dokumente in nicht-statische Ordner

Falls das Dokument nicht den Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA] entspricht, MUSS der XDS Document Service das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-Fehlercode `BadFolderAssociation` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die UUID (DocumentEntry.entryUUID) des identifizierten Dokuments angegeben werden. [\leq]

A_20581-06 - XDS Document Service – Löschen von Dokumenten aus Sammlungen der Typen "mixed" und "uniform" durch ein ePA-FdV

Der XDS Document Service MUSS beim Löschen eines Dokuments der Sammlungstypen "mixed" und "uniform" durch das ePA-FdV sicherstellen, dass die Operation mit dem Fehler `ReferencesExistException` abgebrochen wird, wenn die Löschanfrage nicht alle Dokumente der Sammlung enthält. Es besteht folgende Ausnahme: Das Löschen einer Elternnotiz im Kinderuntersuchungsheft ist erlaubt. [\leq]

Nur Leistungserbringern ist es erlaubt, einzelne Dokumente aus Sammlungen der Typen "mixed" und "uniform" zu löschen, um die medizinische Interpretation der gesamten Sammlungsinstanz nicht zu gefährden.

5561 *Hinweis: Die zeitliche Gültigkeit ergibt sich aus den Attributen "validFrom" und (optional)*
5562 *"clientReadOnlyFromDate" der Vorgaben in [gemSpec_IG_ePA].*

5563 3.12.1.9.23.13.1.9.2 Konfigurierbarkeit

5564 **A_17546-02 - Konfigurierbarkeit von strukturierten Dokumenten**

5565 Der XDS Document Service MUSS die Liste strukturierter Dokumente konfigurierbar
5566 machen, indem dieser die Unterstützung strukturierter Dokumente unter Angabe
5567 folgender Eigenschaften ermöglicht:

- 5568 • Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA]
5569 konfigurativ hinzufügen bzw. entfernen,
- 5570 • Sammlungen zu TAB_EPA_Sammlungstypen
5571 gemäß [gemSpec_IG_ePA] konfigurativ hinzufügen bzw. entfernen.

5572 [**<=**]

5573 Das Entfernen der Unterstützung von strukturierten Dokumenten oder
5574 Sammlungen bedeutet, dass diese zu einem früheren Zeitpunkt in das Aktensystem
5575 geschrieben werden konnten, aber durch Erreichen von "clientReadOnlyFromDate" nicht
5576 mehr geschrieben werden dürfen. Das Schreiben umfasst das Aktualisieren oder neu
5577 Anlegen. Das Lesen ist weiterhin erlaubt.

5578 **A_17551-01 - Prüfanforderungen zur Konfigurierbarkeit von Value Sets**

5579 Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die zu konfigurierenden
5580 Value Sets des XDS Document Service gemäß der Anforderung A_17546-* den
5581 folgenden Prüfkriterien unterliegen, bevor bestehende, im XDS Document Service
5582 verarbeitete Value Sets verändert werden:

- 5583 • Es DÜRFEN KEINE Codes der Value Sets gelöscht werden, lediglich das Hinzufügen
5584 von Codes zu existierenden Value Sets ist aus Kompatibilitätsgründen erlaubt.
- 5585 • Neue Codes MÜSSEN den Formatvorgaben gemäß Tabelle 4.2.3.1.7-2 in [IHE-ITI-
5586 TF3#4.2.3.1.7] entsprechen und gegenüber einer internen Referenzliste validiert
5587 werden. Dies schließt auch Prüfungen zur Zeichenkodierung, der Datentypen als
5588 auch zu den Längenbeschränkungen ein.

5589 [**<=**]

5590 **A_21212-01 - Restriktionen zur Konfigurierbarkeit von Metadaten für**
5591 **strukturierte Dokumente und Sammlungen**

5592 Der XDS Document Service MUSS durch technische Maßnahmen sicherstellen, dass
5593 Änderungen an den in den Implementierungsvorgaben in [gemSpec_IG_ePA]
5594 spezifizierten Codes ausgeschlossen sind. [**<=**]

5595 **A_21214-03 - Konfiguration strukturierter Dokumente im Rahmen der**
5596 **Veröffentlichung durch die gematik**

5597 Der Anbieter des ePA-Aktensystems MUSS durch organisatorische Maßnahmen
5598 sicherstellen, dass die Konfiguration im Aktensystem zur Unterstützung strukturierter
5599 Dokumente aus [gemSpec_IG_ePA] ausschließlich im Rahmen der Veröffentlichung der
5600 Implementation Guides durch die gematik erfolgt. [**<=**]

5601 Bei Einführung neuer strukturierter Dokumente werden die beschriebenen
5602 Konfigurationsmöglichkeiten so verwendet, dass eine Erweiterung der Spezifikation und
5603 daraus resultierend eine Änderung des ePA-Aktensystems mit erneuter Zulassung nicht
5604 erforderlich sind.

3.13.1.9.3 Verarbeitungsvorgaben für spezifische Dokumente

A 27686 - Einstellen des eArztbriefs mit Dokumentenanhängen

Der XDS Document Service MUSS beim Einstellen eines eArztbriefs gemäß [gemSpec IG ePA] sicherstellen,

- dass alle zusätzlich in der Anfrage enthaltenen Dokumente mit dem enthaltenen eArztbrief-Dokument über die Kennzeichnung als Anhang verbunden werden (`urn:gematik:iti:xds:2025:childDocument/parentDocument`),
- dass kein Dokument (via `urn:gematik:iti:xds:2025:childDocument/parentDocument`) auf ein Elterndokument referenziert, dass nicht der eArztbrief selbst ist.

und ansonsten die Verarbeitung mit dem Fehler `XDSInvalidAttachmentHierarchy` abbrechen.
[<=]

Unter anderem müssen also die Anhänge immer direkt unter den Arztbrief "gehängt" werden; ein "Anhang am Anhang" ist nicht erlaubt.

~~3-12.1.10~~ 3.13.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode

Der Versicherte oder ein Vertreter kann vorhandene Dokumente des Aktenkontos durch die Verwendung der General Deny Policy des Constraint Managements verbergen oder sichtbar machen.

Der Versicherte oder ein Vertreter kann ein neues Dokument auch direkt beim Einstellen in das Aktenkonto verbergen. Dazu wird durch den XDS Document Service beim Einstellen bzw. Aktualisieren (Replace) eines Dokuments der `DocumentEntry.confidentialityCode` der Dokumentmetadaten ausgewertet. Enthält der `confidentialityCode` beim Einstellen bzw. Aktualisieren den Wert "CON" (constraint), wird durch das Aktensystem ein Eintrag in der General Deny Policy erzeugt und das Dokument verborgen.

Diese zusätzliche Art des direkten Verbergens ist dabei grundsätzlich nur auf Dokumententypen anwendbar, welche durch einen Versicherten oder einen Vertreter über ein ePA-FdV eingestellt werden können (keine MIOs oder strukturierten Dokumente).

Das Metadatum `DocumentEntry.confidentialityCode` = "CON" (`codeSystem` = `urn:oid:1.2.276.0.76.5.491`):

1. Führt beim Einstellen und Replace eines Dokuments zum Verbergen des Dokuments, d.h. das Dokument wird auf die General Deny Policy des Aktenkontos gesetzt.
2. Wird im Aktensystem nicht persistiert sondern über dort intern über eine General Deny Policy umgesetzt.
3. Wird im ePA-FdV nicht zur Anzeige gebracht und kann dort auch nicht geändert werden.
4. Ein PS darf `DocumentEntry.confidentialityCode` = "CON" nicht verwenden.

3.12.1.113.13.1.11 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 33: Auswirkungen bei Widerspruch gegen eine Funktion der ePA

widerspruchsfähige Funktion	Auswirkung bei erteiltem Widerspruch
Teilnahme am digital gestützten Medikationsprozess ("medication")	Das Einstellen, Verändern, Lesen oder Suchen von Dokumenten des Ordners "emp" (elektronischer Medikationsplan) wird durch den XDS Document Service abgelehnt. Ausgenommen hiervon sind der Versicherte und befugte Vertreter.
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst ("erp-submission")	Alle vorhandenen Dokumente des Ordners "emp" (elektronischer Medikationsplan) werden gelöscht.

Hinweis zum Medikationsprozess: Dadurch wird verhindert, dass Leistungserbringer im Versorgungsprozess veraltete oder unvollständige Daten verwenden.

A_23860 - XDS Document Service - Löschen der Dokumente des Medikationsprozesses

Der XDS Document Service des Aktensystems MUSS alle Dokumente aus dem Ordner elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") löschen, wenn der Status der widerspruchsfähigen Funktion "Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst" (Id = "erp-submission") auf "Widerspruch erklärt" ("deny") geändert wird. [**<=**]

A_23895-02 - XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch

Falls ein Widerspruch zur widerspruchsfähigen Funktion "Teilnahme am Medikationsprozess" (Id = "medication" und status = "deny") vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für alle Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid_versicherter), ablehnen und die Operation mit dem Fehlercode ConsentDecisionViolation abrechnen. [**<=**]

A_25151-01 - XDS Document Service – Prüfung der Widersprüche bei Suchanfrage

Der XDS Document Service MUSS bei einer Suchanfrage die Suchergebnismenge für alle Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid_versicherter), filtern und sicherstellen, dass diese keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält, wenn ein Widerspruch gegen die widerspruchsfähige Funktion "Teilnahme am digital gestützten Medikationsprozess" (Id = "medication" und status = "deny") vorliegt. [**<=**]

3.12.1.123.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI auf die Dokumente des Aktenkontos

Wird ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI erklärt, verhindert der XDS Document Service, dass auf die Dokumente der Kategorie "emp" zugegriffen werden kann.

A_26429 - XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für diese LEI, ablehnen und die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.
[<=]

A_26430 - XDS Document Service – Prüfung des Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI bei Suchanfrage

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service bei einer Suchanfrage die Suchergebnismenge für diese LEI filtern und sicherstellen, dass die Suchergebnismenge keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält.
[<=]

3.12.1.133.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service

A_24715-01 - XDS Document Service - Protokolleinträge für Zugriffe auf den XDS Document Service

Der XDS Document Service MUSS für die Operationen

- ProvideAndRegisterDocumentSet-b,
- RetrieveDocumentSet,
- RemoveMetadata,
- RestrictedUpdateDocumentSet,
- RegistryStoredQuery (entfällt, wenn Nutzung durch den Versicherten erfolgt)

Protokolleinträge gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 34: XDS Document Service Protokollierung

Strukturelement	Wert	Erläuterung
AuditEvent.type	"document"	
AuditEvent.action	C	Für ProvideAndRegisterDocumentSet-b ohne Replace Option

Strukturelement	Wert	Erläuterung
	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
AuditEvent.entity.detail	type	value[x]
	"DocumentFormatCode"	<DocumentEntry.formatCode>
	"DocumentUniqueId"	<Document.uniqueId>
		wenn in der entity Struktur ein XDSDocument beschrieben wird. kodiert als Datentyp „Coded String“ gemäß [IHE-ITI- TF3]. Wenn es sich beim Wert von DocumentEntry.formatCode um den Code urn:ihe:iti:xds:2017:mimeTypeSufficient (Code System 1.3.6.1.4.1.19376.1.2.3) handelt, MUSS stattdessen der Wert von DocumentEntry.mimeType hier eingetragen werden.
		wenn in der entity Struktur ein XDSDocument beschrieben wird

Strukturelement	Wert		Erläuterung
	"FolderTitle"	<Folder.title>	wenn in der entity Struktur ein XDSFolder beschrieben wird
	"FolderCodeList"	<Folder.codeList>	wenn in der entity Struktur ein XDSFolder beschrieben wird kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3] z.B. "pregnancy_childbirth^^^&1.2.276.0.76.5.512&ISO"
	"FolderEntryUID"	<Folder.entryUUID>	wenn in der entity Struktur ein XDSFolder beschrieben wird
Parameterwerte für die Operation RegistryStoredQuery der Schnittstellen I_Document_Management und I_Document_Management_Insurant (nur Vertreter)			
AuditEvent.entity.name	"AdhocQuery"		fester Wert
AuditEvent.entity.detail	type	value[x]	
	"QueryId"	<Parameter Query ID>	Der Wert MUSS der Parameter Query ID gemäß [IHE-ITI-TF2] #3.18.4.1.2.4 und für das Aktensystem definierten Anfragetypen entsprechen.
Parameterwerte für die Operation RestrictedUpdateDocumentSet			
<p>Alle Metadaten, die geändert wurden, sind mit altem und neuem Wert mit den Parameternamen AuditEvent.entity.detail.type und .value[x] zu protokollieren. In A_15083* sind die Metadaten genannt, die geändert werden können. Der Parameter type ist ein Kompositum aus Objekt (Document) + Attribut in Groß/Kleinschreibung. Wird das geänderte Metadatum adressiert, wird noch der Präfix "prev" ergänzt. z.B. Metadatum: DocumentEntry.formatCode -> Parameter valuetype: DocumentFormatCode und prevDocumentFormatCode. Attributunterstrukturen werden ebenfalls in gemischter Groß/Kleinschreibung zusammengesetzt (z.B. author.Person -> AuthorPerson).</p>			

5720 [**<=**]

5721 *Hinweis: In der AuditEvent.entity Struktur sind Dokumente und/oder Folder zu*
5722 *berücksichtigen, die in der zu protokollierenden Operation referenziert werden.*

5723 **A_24925 - XDS Document Service - Protokolleinträge für Zugriffe gleicher Art**
5724 Werden mehrere XDS Dokumente bzw Folder in der zu protokollierenden Operation
5725 referenziert und die Zugriffe sind gleicher Art (AuditEvent.action) KANN der XDS
5726 Document Service einen Protokolleintrag erzeugen, der mehreren AuditEvent.entity
5727 Strukturen enthält. [**<=**]

5728 Das bedeutet, wenn in einer ProvideAndRegisterDocumentSet-b Operation zehn
5729 Dokumente eingestellt werden, kann für diesen Zugriff ein AuditEvent mit zehn Entity

5730 Strukturen erzeugt werden. Werden zehn Dokumente eingestellt und das zehnte
5731 Dokument ersetzt ein bereits vorhandenes, kann in einem Protokolleintrag das Einstellen
5732 (Create) mit neun Entity Strukturen dokumentiert und muss in einem weiteren
5733 Protokolleintrag ein Ersetzen (Update) (zehnte Dokument) protokolliert werden.

5734 **A_25007 - XDS Document Service - Nicht zu protokollierende Zugriffe**

5735 Werden mit der Operation RestrictedUpdateDocumentSet keine geänderten Metadaten
5736 eines referenzierten DocumentEntry gesendet, d.h. die gesendeten Metadateninhalte
5737 unterscheiden sich nicht von bereits persistierten Werten, DARF der XDS Document
5738 Service diesen Zugriff NICHT protokollieren. [\leq]

5739 **~~A_27253-01A_27253~~ - XDS Document Service - Nicht zu protokollierende**
5740 **Zugriffe auf Ordner "technical"**

5741 Der XDS Document Service DARF Zugriffe auf den statischen Ordner "technical" oder
5742 dessen Inhalte NICHT protokollieren. [~~\leq Ausgenommen hiervon sind Zugriffe auf~~
5743 ~~Dokumente mit Daten der Protokollierung gemäß A_24866-* (Protokolle aus der~~
5744 ~~Migration eines ePA-2.6 Aktenkontos)~~ [~~\leq~~]

5745 **~~A_27254-01A_27254~~ - XDS Document Service - Protokollierung von**
5746 **Nutzerzugriffen auf den Ordner "technical"**

5747 Der XDS Document Service MUSS Nutzerzugriffe auf den Ordner "technical" dann
5748 protokollieren, wenn durch den Zugriff Dokumente ~~gemäß A_24466-*~~
5749 ~~(Protokolldokumente einer ePA-2.6 Aktenkontomigration)~~ betroffen sind. Diese
5750 Protokollierung MUSS gemäß der Vorgaben in A_24715-* erfolgen. [\leq]

5751 **~~3.12.1.143.13.1.14~~ Unterstützungsleistung für das ePA-FdV**

5752 Der XDS Document Service akzeptiert aus Sicherheitsgründen nur bestimmte
5753 Dokumentenformate. Das schränkt auch das Format PDF auf bestimmte PDF/A-Varianten
5754 ein (siehe auch A_25233*). Daher müssen PDF-Dokumente des Versicherten unter
5755 Umständen vor dem Einstellen in die ePA konvertiert werden.

5756 Um das ePA-FdV dabei zu entlasten und Komplexität aus dem ePA-FdV zu nehmen, wird
5757 eine Funktion angeboten, durch die ein PDF in ein PDF/A konvertiert werden kann. Das
5758 ePA-FdV muss aber berücksichtigen, dass die Konvertierung ggf. technisch nicht
5759 durchgeführt werden kann oder das Ergebnis der Konvertierung durch ein geändertes
5760 Layout ggf. nicht verwendbar ist.

5761 **A_25456 - XDS Document Service - Keine negativen Auswirkungen auf**
5762 **Folgekonvertierungen von PDF zu PDF/A**

5763 Der XDS Document Service MUSS sicherstellen, dass eine Konvertierung eines PDF-
5764 Dokuments sich nicht schädlich auf folgende Konvertierungen auswirken kann. [\leq]

5765 Hinweis zu A_25456*: Die Anforderung soll erreichen, dass ein potentiell über ein PDF-
5766 Dokument eingebrachter Schadcode nach der Konvertierung gelöscht wird, z.B. durch
5767 Zurücksetzen der Sandbox oder der VAU-Instanz

5768 **A_25455 - XDS Document Service - Isolation der Konvertierung von PDF zu**
5769 **PDF/A**

5770 Der XDS Document Service MUSS die Verarbeitung von PDF-Dokumenten, die im
5771 Rahmen der Konvertierung in ein PDF/A durchgeführt wird, in einer separaten VAU-
5772 Instanz durchführen, die ausschließlich eine Verbindung zu einem ePA-FdV besitzen
5773 darf. [\leq]

5774 **A_25454 - XDS Document Service - Realisierung der Schnittstelle**
5775 **I_Tool_Convert_PDF_Insurant**

5776 Der XDS Document Service MUSS die Operationen der Schnittstelle
5777 I_Tool_Convert_PDF_Insurant gemäß [I_Tool_Convert_PDF_Insurant] umsetzen [\leq]

A_26129 - ePA-Aktensystem - Rahmenbedingungen bei Nutzung einer Service-VAU für PDF-Konvertierung

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die vom ePA-FdV übermittelten PDF-Dokumente in der Aktenkontoverwaltungs-VAU ausschließlich weitergeleitet aber ansonsten nicht verarbeitet werden. Gleiches gilt für die von der Service-VAU an das ePA-FdV übermittelten konvertierten PDF/A-Dokumente. [\leq]

A_26130 - ePA-Aktensystem - maximale Lebensdauer einer Service-VAU für PDF-Konvertierung

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die Lebensdauer einer solchen Service-VAU-Instanz maximal 12 Stunden beträgt. [\leq]

A_26131 - ePA-Aktensystem - Keine Speicherung von in der Service-VAU für PDF-Konvertierung verarbeiteten Daten

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass weder die vom ePA-FdV übermittelten und zu konvertierenden PDF-Dokumente noch die daraus konvertierten PDF/A-Dokumente von der "PDF-VAU" im ePA-Aktensystem gespeichert werden. [\leq]

A_26121 - ePA-Aktensystem - Keine Verarbeitung von Geräteinformationen

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass keine Geräteinformationen (Device Management) von Nutzern verarbeitet werden. [\leq]

3.12.23.13.2 FHIR Data Services**3.13.2.1 Patient Service****A_26252-03 - Patient Service - Realisierung der Schnittstelle des FHIR IG ePA Basisfunktionalitäten**

Der Patient Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide ePA Basisfunktionalitäten (Patient Service) gemäß [IG Basic] umsetzen. [\leq]

A_26254 - Patient Service - Protokolleinträge für Zugriffe auf den Patient Service

Der Patient Service MUSS einen Protokolleintrag gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 35: Patient Service Protokollierung

<u>Strukturelement</u>	<u>Wert</u>	<u>Erläuterung</u>
<u>AuditEvent.type</u>	<u>"rest"</u>	

<u>Strukturelement</u>	<u>Wert</u>	<u>Erläuterung</u>
<u>AuditEvent.action</u>	<u>U</u>	<u>Update</u>
<u>AuditEvent.entity.name</u>	<u>Patient</u>	
<u>AuditEvent.entity.description</u>	<u>operation:upsertPatient</u>	

[<=]

3.12.2.13.13.2.2 Medication Service

A_26253-01 - Medication Service - Realisierung der Schnittstellen des FHIR IG Medication Service

Der Medication Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide für den Medication Service [IG_Medication_Service] umsetzen. [<=]

A_26317 - Medication Service - Erzeugung eines xHTML-Exports

Der Medication Service MUSS gemäß den Vorgaben von [IG_Medication_Service] für die Generierung der Medikationsliste im xHTML-Format nach [XHTML] sicherstellen, dass kein ausführbarer Code im Export enthalten ist. [<=]

A_24820 - Medication Service - Ablehnung von Request bei vorliegendem Widerspruch

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID != oid_erp-vau, oid_versicherter mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("medication") die Entscheidung ("deny") gesetzt ist. [<=]

A_25152 - Medication Service - Ablehnung neuer Daten bei vorliegendem Widerspruch

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID == oid_erp-vau mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny") gesetzt ist. [<=]

A_25153 - Medication Service - Löschen der Daten des Medication Service

Der Medication Service MUSS alle vorhandenen fachlichen Daten des Medication Service löschen, wenn im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny") gesetzt wird. [<=]

A_26399 - Medication Service - Ablehnung von Request bei vorliegendem Widerspruch gegen die Nutzung durch eine spezifische LEI

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID gemäß A_26406-* mit dem HTTP Status Code 423 (LOCKED) abbrechen, sofern im Consent Decision Management die LEI der User Session in der User Specific Deny Policy des Medication Service enthalten ist. [<=]

A_24841-03 - Medication Service - Schemavalidierung

Der Medication Service MUSS im Body der HTTP-POST-Operation die übertragenen Parameter auf Schadcode prüfen und fachfremde Daten (d.h. Schemavalidierung) prüfen und im Fehlerfall das Ausführen der Operation mit dem HTTP Status Code 400 abbrechen. [<=]

A_24849-03 - 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 36: 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
	OperationId: provideDispensation_MedicationSvc	"C"	Einstellen einer Medikamentenabgabe
	OperationId: cancelPrescription_MedicationSvc	"U"	Stornieren von Verschreibungsdaten
	OperationId: cancelDispensation_MedicationSvc	"U"	Stornieren einer Medikamentenabgabe
	OperationId: getMedicationList_MedicationSvc	"R"	Abruf der Medikationsliste
	OperationId: renderMedicationListToHTML_MedicationSvc	"R"	Abruf der Medikationsliste im HTML-Format
	OperationId: renderMedicationListToPDF_MedicationSvc	"R"	Abruf der Medikationsliste im PDF-Format
	OperationId: listMedications_MedicationSvc	"R"	Abruf von Medikamenteninformationen
	OperationId: listMedicationDispenses_MedicationSvc	"R"	Abruf von Medikamentenabgabeformen

Struktur element [AuditEv ent.]	Operationen der Schnittstellen I_Medication_Service_F HIR und I_Medication_Service_e ML_Render und FHIR Query API	Wert	Erläuterung
	OperationId: listMedicationRequests_Med icationSvc	"R"	Abruf von Verschreibungsin formationen
	FHIR Query API:	"R"	Suche über die FHIR Query API
entity.name		<ul style="list-style-type: none"> "Medical Service" bei Operationen <FHIR Resource Name> bei FHIR Query API 	
Nur, wenn nicht FHIR Query API:			
entity.description		OperationId der ausgeführten Operation, z. B. "providePrescription_MedicationSvc"	
entity.detail.type		"display-text"	
entity.detail.value[x]		Text der oben für die jeweilige OperationId angegebenen Erklärungsspalte, z. B. "Einstellen eines Medikaments"	
Nur bei FHIR Query API:			
entity.detail.type		"search-parameters"	
entity.detail.value[x]		<ResourceName>?parameter1=<value>¶meter2=<value>& ...mehr	Suchkriterien in URL-Query-Notation

Sofern ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF der Medication Service keinen Protokolleintrag erzeugen.

[<=]

Ereignisse, die gemäß A_26298* zu einer Übertragung neuer oder geänderter Daten an das FDZ führen, erzeugen grundsätzlich einen eigenen Protokolleintrag für den Vorgang gemäß der Vorgaben in A_24849*. Liegt kein Widerspruch des Versicherten gegen die

Übermittlung der Daten an das FDZ vor und ist eine Übertragung der Daten des Ereignisses aufgrund der Pseudonymisierbarkeit dieser Daten möglich, so folgt auf das ursächliche Ereignis automatisch der Export der pseudonymisierten Daten.

Diese Übertragung der Daten muss für einen Versicherten aus der Protokollierung ersichtlich sein. Anstelle eines dedizierten Protokolleintrags für die Datenübertragung wird die Datenübertragung als ergänzendes entity.detail des auslösenden Ereignisses protokolliert. Aus dem Protokolleintrag des Ereignisses ist dann ersichtlich, ob die betroffenen Daten in pseudonymisierter Form auch der sekundären Datennutzung zugeführt wurden.

A 27188 - Medication Service - Protokollierung des Datenexports an das FDZ

Der Medication Service MUSS einen Protokolleintrag gemäß A 24849* um das folgend aufgeführte entity.detail mit dem Wert true ergänzen, wenn aus der Operation eine Übertragung von Daten an das FDZ folgt. Diese Ergänzung MUSS entweder den Wert false haben oder entfallen, wenn aus der Operation keine Übertragung von Daten an das FDZ folgt.

Strukturelement	Wert	Erläuterung
entity.detail.type	"data-submission"	Export an das Forschungsdatenzentrum
entity.detail.value[x]	"true" oder "false"	

[<=]

3.13.2.3 MHD Service

A 27667 - MHD Service - Realisierung der Schnittstellen des FHIR IG

Medication Service

Der MHD Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide für den MHD Service [IG MHD Service] umsetzen.[<=]

A 27668 - MHD Service - Filtern von verborgenen Metadaten und Dokumenten

Der MHD Service MUSS bei einer Suchanfrage bei jedem Dokument einer verborgenen Datenkategorie die Metadaten (bzw. korrespondierende FHIR-Ressource DocumentReference filtern sowie den Dokumentenabruf aus DocumentReferences.content.attachment.url verhindern (HTTP Code 404 not found).[<=]

A 27669 - MHD Service – Protokolleinträge für Zugriffe auf den MHD Service

Der MHD Service MUSS einen Protokolleintrag gemäß A 24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 37: MHD Service Protokollierung

<u>Strukturelement</u> <u>[AuditEvent.1]</u>	<u>Operationen der</u> <u>FHIR Query API</u>	<u>Wert</u>	<u>Erläuterung</u>
<u>type</u>		<u>"rest"</u>	
<u>action</u>	<u>OperationId:</u> <u>findDocumentReferences_MHDSvc</u>	<u>"R"</u>	<u>Suche von Dokumenten</u>
	<u>OperationId:</u> <u>retrieveDocument_MHDSvc</u>	<u>"R"</u>	<u>Abruf eines Dokuments</u>
<u>entity.name</u>		<u>"MHD Service"</u>	
<u>entity.detail.type</u>		<u>"search-parameters"</u>	
<u>entity.detail.value[x]</u>		<u><ResourceName>?parameter1=<value>parameter2=<value>& ...mehr</u>	<u>Suchkriterien in URL-Query-Notation</u>

Sofern ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF der MHD Service keinen Protokolleintrag erzeugen. [<=]

3.13.14 Audit Event Service

Ereignisse und Zugriffe auf die ePA eines Versicherten werden im ePA Aktensystem protokolliert. Die Protokollierung dient der Datenschutzkontrolle für den Versicherten. Der Audit Event Service ist ein FHIR Data Service und ermöglicht dem Versicherten, befugten Vertretern bzw. der Ombudsstelle den Zugriff auf diese Protokollinformationen.

A 24704-02 - Audit Event Service - Realisierung der Schnittstelle des FHIR IG ePA Basisfunktionalitäten

~~A_24704 – Audit Event Service – FHIR-Ressource AuditEvent~~ Der Audit Event Service MUSS die Implementierungsvorgaben des FHIR-Ressource AuditEvent gemäß der FHIR-Profilierung [IG– Implementation Guide ePA Basisfunktionalitäten (Audit –Event –Service) gemäß [IG Basic] umsetzen.] unterstützen. [<=]

5916 In der Struktur eines Protokolleintrages (AuditEvents) sind folgende
 5917 Zugriffsinformationen hinterlegt:

5918 **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

5919

5920 Die spezifische Befüllung eines Audit Events gemäß A_24704* wird durch die jeweiligen
 5921 Services vorgegeben. Allgemeine Elemente sind wie folgt zu befüllen:

5922 **A_25154-02A_25154-03 - ePA-Aktensystem - Befüllung der Elemente recorded,**
 5923 **agent und source eines Audit Events**

5924 Das ePA-Aktensystem MUSS die Audit Event Elemente AuditEvent.recorded,
 5925 AuditEvent.agent und AuditEvent.source wie folgt befüllen.

5926 **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"
<u>purposeOfEvent</u>	<u>Zweck(e) des protokollierten Ereignisses gemäß des zulässigen Value-Sets. Nur zu belegen, wenn explizit bei entsprechender Protokollierungsanforderung gefordert.</u>	
<u>system</u>	<u>Das verwendete Codesystem</u>	<u>" https://gematik.de/fhir/epa/ValueSet/epa-auditevent-purpose-of-event-vs"</u>

Element [AuditEvent.]		Beschreibung	Beispiel
	<u>code</u>	<u>Der verwendete Code aus dem Codesystem</u>	<u>"EXPORTFDZ"</u>
	<u>display</u>	<u>Der Bezeichner zur Anzeige aus dem Codesystem</u>	<u>"Export für das Forschungsdatenzentrum Gesundheit"</u>
agent[client].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem; Fest vorgegebener Wert: "http://dicom.nema.org/resources/ontology/DCM"	"http://dicom.nema.org/resources/ontology/DCM"
	code	Der verwendete Code aus dem Codesystem; Fest vorgegebener Wert: "110150"	"110150"
	display	Der Bezeichner zur Anzeige aus dem Codesystem; Fest vorgegebener Wert: "Application"	"Application"
agent[client].who.identifiziert.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/sid/telematik-id"
	value	<Telematik-Id>	"1-883110000092404"
agent[client].	altId	<value> aus agent.who.identifiziert	"1-883110000092404"

Element [AuditEvent.]		Beschreibung	Beispiel
agent[client].	name	<ul style="list-style-type: none"> <display_name> des auslösenden Akteurs aus dem ID-Token der UserSession "Elektronische Patientenakte Fachdienst" für intern ausgelöste AuditEvents 	1) "E-Rezept-Fachdienst" 2) "Elektronische Patientenakte Fachdienst" 3) "Portugal" (Beispiel EU-Zugriff)
agent[client].	requestor	Fest vorgegebener Wert "false"	"false"
agent[user].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	" http://terminology.hl7.org/CodeSystem/v3-RoleClass "
	code	Der verwendete Code aus dem Codesystem	"PROV"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"healthcare provider"
agent[user].who.identifizier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/sid/telematik-id"
	value	<Telematik-Id> oder <KVN<	1) "2-121212121212121" 2) "Z123456789"
agent[user].	altId	<value> aus agent.who.identifizier	1) "2-121212121212121" 2) "Z123456789"
agent[user].role.coding		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthProfessionalRole.	
	system	Das verwendete Codesystem	"urn:oid:1.3.6.1.4.1.12559.1.10.1.3.2.2.2"

Element [AuditEvent.]		Beschreibung	Beispiel
	code	Der verwendete Code aus dem Codesystem	"Resident Physician"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Resident Physician"
agent[user].extension		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthcareFacilityType; extension mit url="https://gematik.de/fhir/dev-epa/StructureDefinition/epa-healthcare-facility-type-extension">	
	system	Das verwendete Codesystem	"urn:oid:2.16.840.1.113883.2.9.6.2.7"
	code	Der verwendete Code aus dem Codesystem	"221"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Medical Doctors"
agent[user].	name	Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: <leiName> / <healthProfessionalName> Andernfalls: <display_name> des auslösenden Akteurs aus dem ID-Token der UserSession	EU-Zugriff: "Dr. Manuel Dos Santos / Clínica de Dos Santos" Andernfalls: "John Doe"
agent[user].	requestor	Fest vorgegebener Wert "false"	false
agent[internal].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	"http://dicom.nema.org/resources/ontology/DCM"

Element [AuditEvent.]		Beschreibung	Beispiel
	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.	
	system	Das verwendete Codesystem	" https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs "
	code	Der verwendete Code aus dem Codesystem	"CDMGMT"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Consent Decision Management"

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
[<=]

A 27689 - Protokollierung von nicht erfolgreichen Zugriffen

Falls für eine Operation ein Protokolleintrag gefordert ist und mit einem Fehler abgebrochen wird, MUSS der Audit Event Service jeweils einen Protokolleintrag gemäß A 24704* erzeugen. Darüberhinaus und ergänzend zu den Vorgaben aus dem Profil EPAAuditEvent gemäß [IG Basic] sind folgende Werte entsprechend zu belegen:

Tabelle 40. Audit Event Management Protokollierung - Fehler

<u>Strukturelement</u>	<u>Wert</u>	<u>Erläuterung</u>
<u>AuditEvent.action</u>	<u>C, R, U, D</u>	<u>Create Read Update Delete</u>
<u>AuditEvent.entity.name</u> -	<u><service name> bei Operationen</u> <u><FHIR Resource Name> bei FHIR Query API</u>	<u>Service Name bzw. FHIR Resource Name, wie für Protokollierung im Service gefordert</u>
<u>Nur, wenn nicht FHIR Query API:</u>		
<u>AuditEvent.entity.description</u>		<u>OperationId der ausgeführten Operation, z. B. "providePrescription_MedicationSvc"</u>
<u>Nur bei FHIR Query API:</u>		
<u>entity.detail.type</u>	<u>"search-parameters"</u>	
<u>entity.detail.value[x]</u>	<u><ResourceName>?parameter1=<value>parameter2=<value>& ...mehr</u>	<u>Suchkriterien in URL-Query-Notation</u>

Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A_25172* entfällt, wenn ein Protokolleintrag mangels eines befugten Nutzers (kein Bezug des SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann. [≤]

A_24503 - ePA-Aktensystem - Aufbewahrungsdauer der Protokolleinträge

Das ePa-Aktensystem MUSS die zum Zwecke der Datenschutzkontrolle für den

Versicherten erstellten

Protokolleinträge für drei Jahre aufbewahren. Danach sind sie vom Aktensystem

automatisch zu löschen. [≤]

Die Protokolleinträge können durch den Versicherten oder durch einen befugten Vertreter mittels ePA-FdV eingesehen werden. Versicherte ohne ePA-FdV können bei ihrer zuständigen Ombudsstelle beantragen, die Protokolldaten zur Verfügung gestellt zu bekommen.

Für eine Abfrage der Protokolleinträge als strukturierte Einträge nutzen ein ePA-FdV und die Ombudsstelle den Audit Event Service [IG_Audit_Event_ServiceBasic].

A_24714-01 - Audit Event Service - Realisierung der Query API: AuditEvent

Der Audit Event Service MUSS die "Query API: AuditEvent" des FHIR Implementation Guide für den Audit Event Service [IG_Audit_Event_ServiceBasic] umsetzen. [≤]

A_24750-02 - Audit Event Service - Realisierung der Render API: PDF Audit

Der Audit Event Service MUSS die "Render API: PDF Audit" des FHIR Implementation Guide für den Audit Event Service [IG_Audit_Event_ServiceBasic] umsetzen. [≤]

A_25172 - Audit Event Service - Speicherung der Protokolldaten

Der Audit Event Service MUSS die Daten der Protokolleinträge verschlüsselt im SecureDataStorage persistieren. [≤]

5965 Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A_25172* entfällt, wenn ein
 5966 Protokolleintrag mangels eines befugten Nutzers (kein Bezug des
 5967 SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann.

5968 **A_25018 - Audit Event Service - PAdES-Signatur in renderAuditEventsToPDF**

5969 Der Audit Event Service MUSS bei der Operation `renderAuditEventsToPDF` beim
 5970 Signieren eines Protokolls im PDF/A-Format eine PAdES-Signatur gemäß [PAdES-3] und
 5971 [PAdES Baseline Profile] erstellen. Bei der Signaturerstellung ist das Attribut `signing`
 5972 `certificate reference` gemäß den Vorgaben aus [PAdES-3] Kapitel 4.4.3 „Signing
 5973 Certificate Reference Attribute“ anzulegen. [**<=**]

5974 Durch die Baseline-Profilierung [PAdES Baseline Profile] wird festgelegt, wie der
 5975 Signaturzeitpunkt, gemessen als Systemzeit des ePA-Aktensystems, in die Signatur
 5976 eingebracht wird.

5977 **A_24991 - Audit Event Service – Protokollierung von Zugriffen auf die** 5978 **Protokolldaten**

5979 Der Audit Event Service MUSS für die Zugriffe der Ombudsstelle oder eines Vertreters auf
 5980 die protokollierten Daten jeweils einen Protokolleintrag gemäß A_24704* erzeugen.

5981 **Tabelle 41: Audit Event Service Protokollierung**

Strukturelement	Wert		Erläuterung
<code>AuditEvent.type</code>	"rest"		
<code>AuditEvent.action</code>	R		Read
<code>AuditEvent.entity.name</code>	"AuditEvent"		
<code>AuditEvent.entity.description</code>	Passend zur ausgeführten Operation ein Wert aus folgender Liste: <ul style="list-style-type: none"> • <code>listAuditEvents</code> • <code>getAuditEventById</code> • <code>renderAuditEventsToPDF</code> 		
<code>AuditEvent.entity.detail</code>	type	value[x]	
	parameters	parameter1=<value>¶meter2=<value>& ...mehr	Nur bei <code>getAuditEventList</code>
	identifizier	<id> des AuditEvents	Nur bei <code>getAuditEvent</code>

5982 [**<=**]

5983 *Hinweis: Zugriffe des Versicherten auf die Protokolle des Aktenkontos werden nicht*
5984 *protokolliert.*

5985

5986 **3.14.13.15 Information Service**

5987 **3.14.13.15.1 Information Service**

5988 Der Information Service ist ohne die Nutzung eines VAU-Kanals nutzbar. Die über den
5989 Information Service genutzten Daten sind ausschließlich persistierte Daten des
5990 Aktenkontos, die weder mit dem SecureAdminStorageKey noch mit dem
5991 SecureDataStorageKey gesichert sind.

5992 Der Zugang erfolgt durch Nutzung der Schnittstelle `I_Information_Service`.

5993 **A_24344 - Information Service - Realisierung der Schnittstelle**

5994 **`I_Information_Service`**

5995 Der Information Service MUSS die Operationen der Schnittstelle `I_Information_Service`
5996 gemäß `[I_Information_Service]` umsetzen. [`<=`]

5997 **A_24345 - Information Service - Kein Zugriff auf verschlüsselte Daten des** 5998 **Aktenkontos**

5999 Der Information Service DARF NICHT auf Daten zugreifen, die nicht explizit für die
6000 Verwendung durch den Informationsdienst bereitgestellt wurden. Dazu gehören
6001 insbesondere alle Daten des Aktenkontos, die mit den versichertenindividuellen
6002 Schlüsseln zur Daten- oder Befugnispersistierung (`SecureDataStorageKey` oder
6003 `SecureAdminStorageKey`) gesichert sind. [`<=`]

6004 **3.14.1.13.15.1.1 Informationen zu Widersprüchen (Consent Decisions)**

6005 Die Widersprüche eines Versicherten gegen die Nutzung von Funktionen der
6006 elektronischen Patientenakte werden durch das Consent Decision Management gesichert
6007 administriert. Änderungen an den Widersprüchen erfolgen dort.

6008 Der Information Service bietet für die Nutzergruppen der ePA eine einfache
6009 Abfragemöglichkeit der aktuell erteilten oder nicht erteilten Widersprüche auch ohne die
6010 Nutzung des Consent Decision Managements an. Liegt ein Widerspruch gegen die
6011 Nutzung einer Funktion vor, kann auf die Ausführung der zur Nutzung dieser Funktion
6012 notwendigen Aktionen mit der ePA eines Versicherten durch den Client verzichtet
6013 werden.

6014 Für diese vereinfachte Abfragemöglichkeit der aktuellen Widersprüche verwendet der
6015 Information Service den durch das Consent Decision Management persistent
6016 übertragenen Zustand der Widersprüche ("Cache" des Zustands der Widersprüche).
6017 Berücksichtigt wird dabei die Widerspruchsinformation, für die eine vereinfachte Abfrage
6018 vorgesehen ist (Widersprüche der Klasse "Versorgungsprozess").

6019 **3.14.1.23.15.1.2 Informationen zur Anwenderperformance (UX** 6020 **Performance)**

6021 Der Information Service stellt für die Umgebung der Leistungserbringer die Operation zur
6022 Sammlung der Messwerte zu den Anwendungsfällen der Nutzererfahrung zur Verfügung.

6023 Die Weiterverarbeitung der gesammelten Daten ist in 2.98-Performance aus
6024 Anwendersicht definiert und vorgegeben.

6025 **3-14-23.15.2 Information Service - Account**

6026 Die Operationen der Information Service - Account werden für den Umzug eines
6027 existierenden Aktenkontos zu einem neuen Anbieter verwendet. Die Nutzung der
6028 Operationen erfolgt exklusiv durch die Aktensystembetreiber.

6029 Die Verwendung der einzelnen Operationen erfolgt im Verbund mit den Operationen der
6030 Schnittstelle I_Health_Record_Relocation_Service für die Umsetzung der
6031 Anwendungsfälle eines automatischen Aktenkontoumzugs und sind in ~~3-2-Health-Record~~
6032 ~~Relocation-Service~~ 3.2- Health Record Relocation Service erläutert.

6033 **A_24424 - Information Service Account - Realisierung der Schnittstelle** 6034 **I_Information_Service_Accounts**

6035 Der Information Service MUSS die Operationen der Schnittstelle
6036 I_Information_Service_Accounts gemäß [I_Information_Service_Accounts]
6037 umsetzen. [\leq]

6038 **A_24665 - Information Service Account - Nutzung beidseitig authentisiertes TLS**

6039 Der Information Service MUSS sicherstellen, dass die Operationen der Schnittstelle
6040 I_Information_Service_Accounts ausschließlich unter Verwendung einer beidseitig
6041 authentisierten TLS-Verbindung zwischen den beteiligten Aktensystemen genutzt werden
6042 und die Operationen ansonsten abgebrochen und mit einer Fehlermeldung gemäß
6043 Vorgaben in [I_Information_Service_Accounts] beantwortet werden. [\leq]

6044 **A_25054 - Information Service Account - Gegenseitige Authentisierung** 6045 **Aktensysteme**

6046 Die Information Service Account Dienste der Aktensysteme MÜSSEN sich mit der TLS-
6047 Identität mit professionOID oid_epa_mgmt mittels des Zertifikats C.FD-TLS-S gegenseitig
6048 authentisieren.
6049 [\leq]

6050 **A_25053 - Information Service Account - Prüfung der TLS-Zertifikate**

6051 Der Information Service Account MUSS bei der Authentifizierung eines jeweils anderen
6052 Aktensystems die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC_PKI_018
6053 durchführen. Zur Prüfung des TLS-Zertifikats C.FD-TLS-S sind dabei die
6054 Parameter PolicyList=oid_fd_tls_s, IntendedKeyUsage=digitalSignature,
6055 intendedExtendedKeyUsage=id-kp-serverAuth, OCSP-Graceperiod=60 Minuten, Offline-
6056 Modus=nein zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD-TLS-C sind dabei die
6057 Parameter PolicyList=oid_fd_tls_c, IntendedKeyUsage=digitalSignature,
6058 intendedExtendedKeyUsage=id-kp-clientAuth, OCSP-Graceperiod=60 Minuten, Offline-
6059 Modus=nein zu verwenden.
6060 [\leq]

6061 **3-153.16 Email Management**

6062 Das Email Management ermöglicht einem FdV-Nutzer die Verwaltung seiner E-Mail-
6063 Adresse und einem Kostenträger die Verwaltung von E-Mail-Adressen von Versicherten,
6064 die bei diesem Kostenträger versichert sind.

6065 Die Schnittstelle zum Verwalten der E-Mail-Adressen durch den Kostenträger dient dem
6066 ausschließlichen Zweck des Einstellens, Lesens und der Änderung von E-Mail-Adressen
6067 auf Verlangen des Versicherten. Dies ermöglicht dem Kostenträger, seinen Versicherten
6068 die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte auf Berichtigung und
6069 Auskunft bzgl. der im Aktensystem verarbeiteten E-Mail-Adresse zu gewährleisten.

6070 Für einen Versicherten kann nur genau eine E-Mail Adresse hinterlegt werden.

6071 A_25435 - Email Management - Realisierung der Schnittstelle**6072 I_Email_Management**

6073 Das Email Management MUSS die Operationen der Schnittstelle

6074 I_Email_Management gemäß [I_Email_Management] umsetzen. [≤]

6075 A_25438 - Email Management - Beschränkung der Schnittstellenoperationen auf E-Mail-Adressen des FdV-Nutzers

6076 Das Email Management MUSS die Operationen der Schnittstelle

6077 I_Email_Management gemäß [I_Email_Management] auf die E-Mail-Adresse des aufrufenden Nutzers einschränken, sofern der Nutzer ein FdV-Nutzer ist. [≤]

6080 A_26161 - Email Management - Nutzen von Email Management auch bei Widerspruch

6081 Das Email Management MUSS sicherstellen, dass das Email Management auch von Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben. [≤]

6084 A_26162 - Email Management - Versicherte nutzen Email Management ausschließlich im Home-AS

6085 Das Email Management des ePA-Aktensystems MUSS sicherstellen, dass das Email Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-Aktensystem das Home-AS ist. [≤]

6089 Hinweis: Für das Email Management ist auch Anforderung A_26154 umzusetzen.

6090 A_25439 - Email Management - Kostenträger kann ausschließlich E-Mail-Adressen der eigenen Versicherten verwalten

6091 Das Email Management MUSS sicherstellen, dass ein Kostenträger mittels der Operationen der Schnittstelle I_Email_Management gemäß [I_Email_Management] ausschließlich E-Mail-Adressen von Versicherten verwalten kann, die beim Kostenträger versichert sind. [≤]

6096 A_25440-01 - Email Management - Benachrichtigung bei Änderung der E-Mail-Adresse

6097 Falls eine E-Mail-Adresse a) ersetzt oder b) ergänzt wird, MUSS das Device Management bei a) eine E-Mail an die alte und die neue E-Mail-Adresse senden und bei b) eine E-Mail an die neue E-Mail-Adresse senden, in der bei a) über die Ersetzung bzw. bei b) die Ergänzung einer E-Mail-Adresse informiert wird. In der E-Mail MUSS darüber informiert werden, wann und ob der FdV-Nutzer selbst oder der Kostenträger die E-Mail ersetzt bzw. ergänzt hat. [≤]

6104 A_25441 - Email Management - Information bzgl. der Ergänzung bei E-Mail-Adressen

6105 Das Email Management MUSS sicherstellen, dass der FdV-Nutzer für eine im Email Management hinterlegte E-Mail-Adresse erkennen kann, wann und von wem diese E-Mail-Adresse ergänzt wurde. [≤]

6109 A_25968-01 - Email Management - Maximale Anzahl E-Mail-Adressen

6110 Das Email Management MUSS sicherstellen, dass für einen Nutzer maximal eine E-Mail-Adresse hinterlegt werden kann. [≤]

6112 A_26163 - Email Management - Keine Persistierung einer im Rahmen der Vertretereinrichtung übergebenen E-Mail-Adresse

6113 Das Email Management MUSS sicherstellen, dass eine im Rahmen des Anwendungsfalls der Vertretereinrichtung vom Nutzer übermittelte E-Mail-Adresse nicht persistiert und spätestens bei Beendigung der User Session gelöscht wird. [≤]

- 6117 **A_26164 - Email Management - Keine Geräteregistrierung mit der im Rahmen**
6118 **der Vertretereinrichtung übergebenen E-Mail-Adresse**
6119 Das Email Management MUSS sicherstellen, dass keine E-Mail-Adressen zur Übermittlung
6120 eines Geräteregistrierungscodes genutzt werden, die dem ePA-Aktensystem im Rahmen
6121 des Anwendungsfalls der Vertretereinrichtung übermittelt wurden. [\leq]
6122 Hinweis zu A_26163 und A_26164: Die im Rahmen des Anwendungsfalls der
6123 Vertretereinrichtung übermittelte E-Mail-Adresse wird ausschließlich zur Information des
6124 Vertreters über die Einrichtung der Vertretung genutzt (vgl. A_24755-*).

6125 **~~3.16.3.17~~ Zusätzliche Anforderungen an den Authorization Service**

- 6126 Der ePA Authorization Service wird sowohl für die Authentisierung der Versicherten über
6127 das FdV als auch für die Authentisierung von Leistungserbringern und Kostenträgern über
6128 deren Primärsystem benötigt. Ebenso muss die Zugriffsautorisierung für andere
6129 Fachdienste wie z.B. E-Rezept geprüft werden. Die Festlegungen für den Authorization
6130 Server finden sich in [gemSpec_IDP_FD]. Dieser Abschnitt des vorliegenden Dokuments
6131 enthält spezifische Anforderungen, die vom Authorization Service des Aktensystems
6132 zusätzlich umzusetzen sind.

6133 **A_24923 - Authorization Service - I_Authorization_Service**

- 6134 Der Authorization Service MUSS die Operationen der
6135 Schnittstelle `I_Authorization_Service` implementieren gemäß
6136 [I_Authorization_Service]. [\leq]

6137 **A_25283 - Authorization Service - Konvertieren von ID-Token**

- 6138 Der Authorization Service MUSS sicherstellen, dass für ein nach erfolgreicher
6139 Authentifizierung des Nutzers vorliegendes ID-Token mittels Regel `rr0` gemäß
6140 `Tab_AS_Entitlement_Registration_Rules` ein HSM-ID-Token erstellt wird, bevor das ID-
6141 Token zeitlich ungültig ist. [\leq]

6142 **~~3.16.13.17.1~~ Anforderungen an den Authorization Service für die**
6143 **Authentisierung von Versicherten (FdV)**

- 6144 Im Rahmen der Authentisierung des Versicherten erfolgt die Prüfung der
6145 Geräteregistrierung (Verifikation) direkt. Das Gerät muss dafür die Geräteparameter
6146 eines zuvor ausgeführten und bestätigten Registrierungsprozesses verwenden
6147 Bisher nicht registrierte Geräte, bzw. Geräteparameter einer bisher nicht bestätigten
6148 Geräteregistrierung, können unter Verwendung des Device Management registriert, bzw.
6149 bestätigt werden (siehe Kapitel ~~3.11.12~~ Device Management).
6150

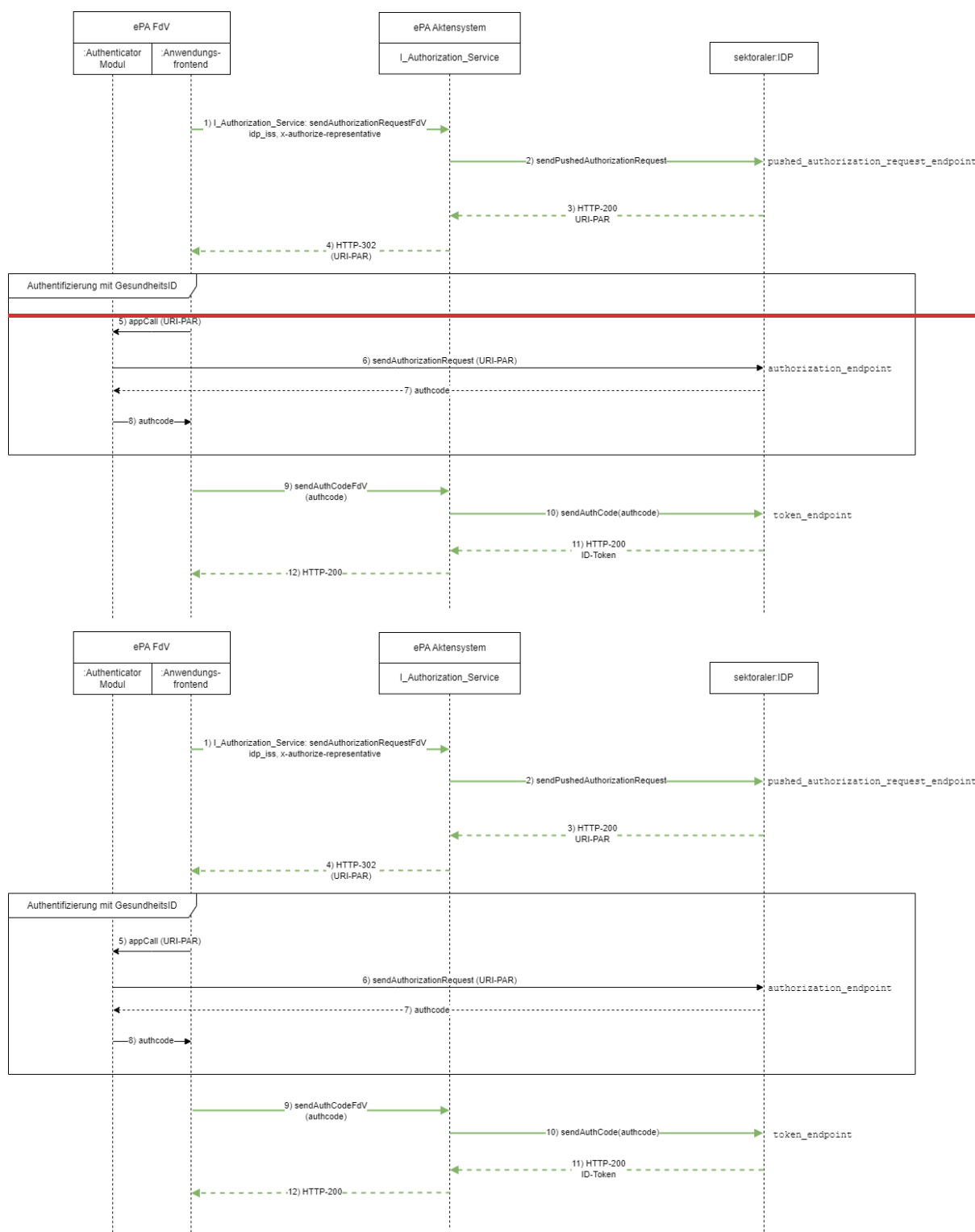


Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP

A_25717-03 - Authorization Service - Pushed Authorization-Request des Authorization Service an sektorale Identity Provider

Der ePA Authorization Service MUSS den Pushed Authorization Request (PAR) 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
<code>scope</code>	"openid urn:telematik:display_name urn:telematik:versicherter urn:telematik:family_name urn:telematik:given_name"	Notwendige Scopes für den Zugriff für die Autorisierung von Nutzern am ePA-Aktensystem
<code>acr_values</code>	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung
<code>redirect_uri</code>	Inhalt des Parameters <code>x-redirecturi</code> [sendAuthorizationRequestFdV in I_Authorization_Service], andernfalls eine herstellerspezifische Standard- <code>redirect_uri</code> .	Diese URI muss unter dem <code>claim redirect_uris</code> im Entity Statement des Authorization Service enthalten sein. Mandanten, welche eine eigene <code>redirect_uri</code> verwenden [sendAuthorizationRequestFdV in I_Authorization_Service], müssen diese im Rahmen des Registrierungsprozesses beim Authorization Service bekannt geben.

[<=]

Hinweis 1: An die `redirect_uri` im Pushed Authorization Request sendet der sektorale IDP den ausgestellten Authorization Code (siehe [gemSpec_IDP_Sek])

Hinweis 2: Der Redirectaufruf, der vom Authenticator Modul an die `redirect_uri` ausgeführt wird, wird vom ePA-FdV über Plattformmechanismen (deeplink/universallink) gefangen und stellt selbst einen POST-Request an den Endpunkt des Authorization Service.

A_26584 - Authorization Service - Liste der `redirect_uris` im Entity Statement

Der Authorization Service MUSS in seinem Entity Statement im `claim redirect_uris` die `redirect_uris` aller Mandanten auflisten, welche bei der Registrierung an einem beliebigen ePA Authorization Service eine eigene `redirect_uri` angegeben haben. Über Änderungen des `claim redirect_uris` MUSS der Anbieter des Federation Master vor produktiver Verwendung informiert werden[<=]

Hinweis: Im Registrierungsprozess eines Mandanten mit eigener `redirect_uri` muss sichergestellt sein,

- dass alle Anbieter von ePA Authorization Servern (ePA Aktensystem Anbieter) entsprechend informiert sind und das Entity Statement anpassen
- dem Hersteller des Federation Master über ein ITSM Change bekannt gemacht wird, dass sich die Entity Statements aller ePA Authorization Server ändern

A_27145 - Synchronisation "redirect_URI" mit Marktteilnehmer - E-Mail-Adresse

Der Anbieter ePA-Aktensystem MUSS der gematik eine E-Mail-Adresse mitteilen, über welche er die eigenverantwortliche Registrierung (von redirect-URIs im Entity-Statement) durchführt und über die der Anbieter bei Änderungen erreichbar ist.

Hinweis: Diese E-Mail-Adressen werden durch das Provider Management der gematik anschließend unter den relevanten Anbietern verteilt bzw. können dort erfragt werden. Die Änderung der E-Mail-Adressen ist ebenfalls zu kommunizieren.

Hintergrund: Für Stellvertretung via ePA-FdV ist eine Synchronisierung der redirect_URIs notwendig. [≤]

A_27186 - Synchronisation "redirect_URI" mit Marktteilnehmer - Information

Der Anbieter ePA-Aktensystem MUSS bei Änderungen der redirect_URIs im eigenen Entity Statement allen anderen Marktteilnehmern des gleichen Fachdiensttyps diese Änderung innerhalb 24 Stunden mitteilen. [≤]

A_27187 - Synchronisation "redirect_URI" mit Marktteilnehmer - Aktualisierung

Der Anbieter ePA-Aktensystem MUSS nach dem Empfang der Mitteilungen über Änderungen der Redirect URIs in einem externen Entity Statement diese Änderung binnen 24 Stunden in den Redirect URIs des eigenen Entity Statement synchronisieren.

Hinweis: Diese Änderung erfordert anschließend keine Information nach A_27186. [≤]

A_24878-01 - Authorization Service - Authentifizierung eines Versicherten am ePA-FdV des Vertreters

Falls der Eingangsparameter `x-authorize-representative=True` der Operation `I_Authorization_Service::sendAuthorizationRequestFdV` gesetzt ist, MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:guest:eGK` belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [≤]

A_26189-01 - Authorization Service - Authentifizierung eines Versicherten im Gastmodus mit eGK und PIN

Falls der Eingangsparameter `x-authorize-egk=True` der Operation `I_Authorization_Service::sendAuthorizationRequestFdV` gesetzt ist, MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:guest:eGK` belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [≤]

A_24937-01 - Authorization Service - Einschränkung bei Authentifizierung eines Versicherten am ePA-FdV des Vertreters

Der Authorization Service MUSS sicherstellen, dass ein mit `x-authorize-representative=True` authentisierter Nutzer ausschließlich Zugriff auf das Entitlement Management erhält. [≤]

A_26159 - Authorization Service - Prüfen der Device Attestation

Der Authorization Service MUSS sicherstellen, dass von einem anderen ePA-Aktensystem signierte Device Attestations ausschließlich akzeptiert werden, wenn

- die Device Attestation gemäß A_25042-* valide von einer Signaturidentität der VAU eines anderen ePA-Aktensystems signiert wurde,
- die KVN-R in der Device Attestation mit der KVN-R im ID-Token des angemeldeten Nutzers übereinstimmt,

- die Device Attestation zeitlich gültig ist.

[<=]

A_26160 - Authorization Service - Keine Persistierung der Device Attestation

Der Authorization Service MUSS sicherstellen, dass die von einem anderen ePA-Aktensystem signierte Device Attestation und deren Inhalte spätestens bei Beendigung der User Session gelöscht und nicht persistiert werden.[<=]

A_25310-01 - Authorization Service - Einschränkung bei Authentifizierung mit einem unregistrierten Gerät

Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wird und der Nutzer nicht mit x-authorize-representative=True authentisiert wurde, MUSS der Authorization Service sicherstellen, dass der Nutzer ausschließlich Zugriff auf das Device Management erhält.[<=]

Hinweis:

Ein vollständiger Zugriff eines authentisierten Nutzers auf alle Dienste des Aktensystems kann nur mit einem Gerät erfolgen, dessen Geräteregistrierung bei der Authentifizierung des Nutzers erfolgreich verifiziert wurde.

Ein Nachweis einer Geräteregistrierung ist entweder DeviceID (deviceIdentifizier und deviceToken), die für den Nutzer im Aktensystem bekannt sind oder die vom Client übergebene Device Attestation (deviceAttestation), die zuvor am Device Management des Home Aktensystems durch den Client abgerufen wurde.

A_24804-01 - Authorization Service - Prüfung auf registriertes Gerät

Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des Vertreters handelt und im Operationsaufruf

I_Authorization_Service::sendAuthCodeFdV eine DeviceID (deviceIdentifizier und deviceToken) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer registriert und bestätigt ist und übereinstimmt.[<=]

A_24914-03 - Authorization Service - Prüfung auf registriertes Gerät - kein registriertes Gerät

Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wurde, MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung abbrechen und die User Session beenden.[<=]

6260

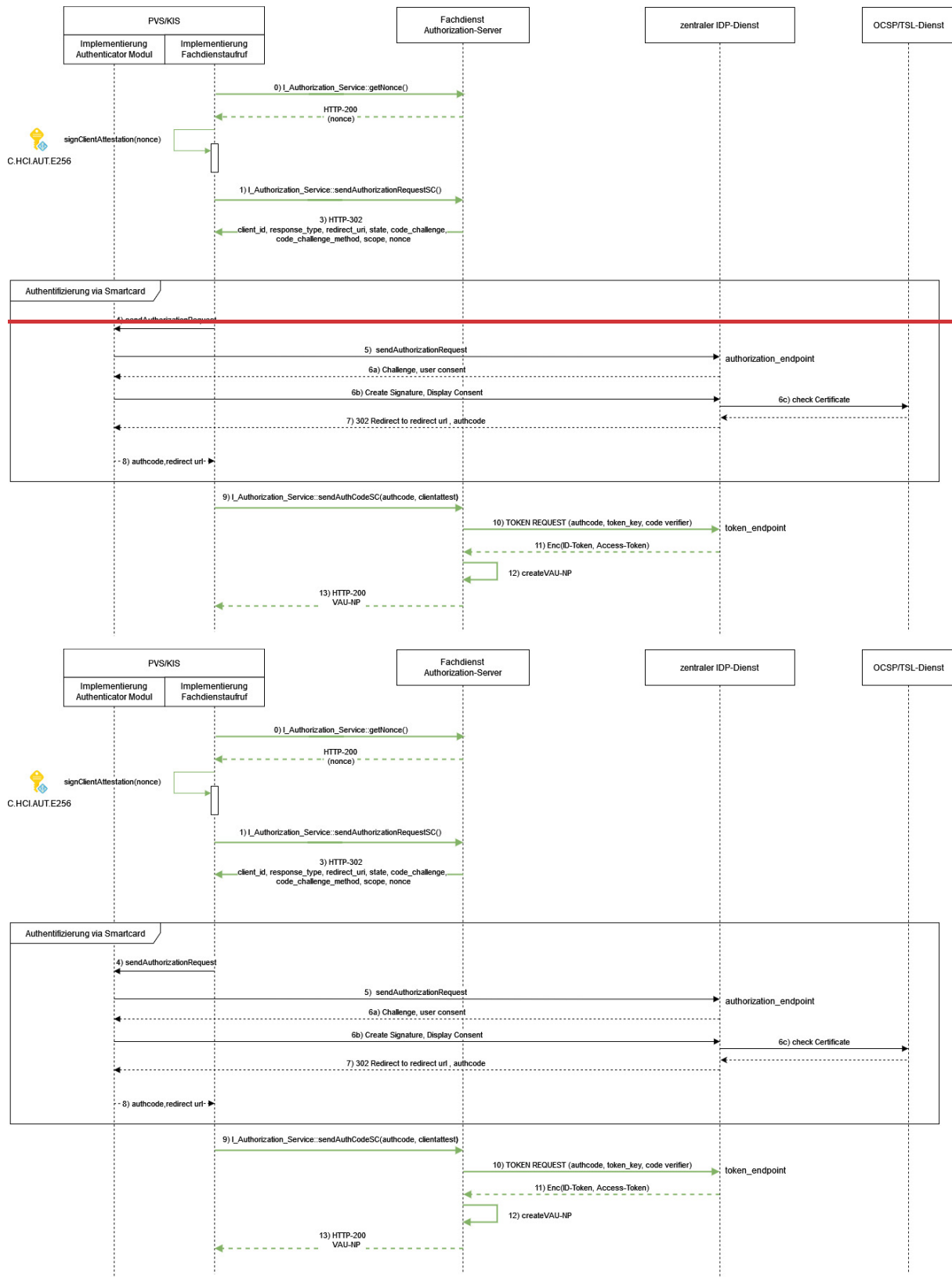
A_24915-01 - Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht bestätigt

Falls als Nachweis einer Geräteregistrierung eine DeviceID (deviceIdentifizier und deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status == 'pending'), MUSS der Authorization Service die Operation sendAuthCodeFdV mit einer Fehlermeldung abbrechen und die User Session beenden.[<=]

6267

6268
6269

3-16-23.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B



6270

6271

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.

3.16.33.17.3 Anforderungen an den Authorization Service für die Authentisierung des E-Rezept-Fachdienstes

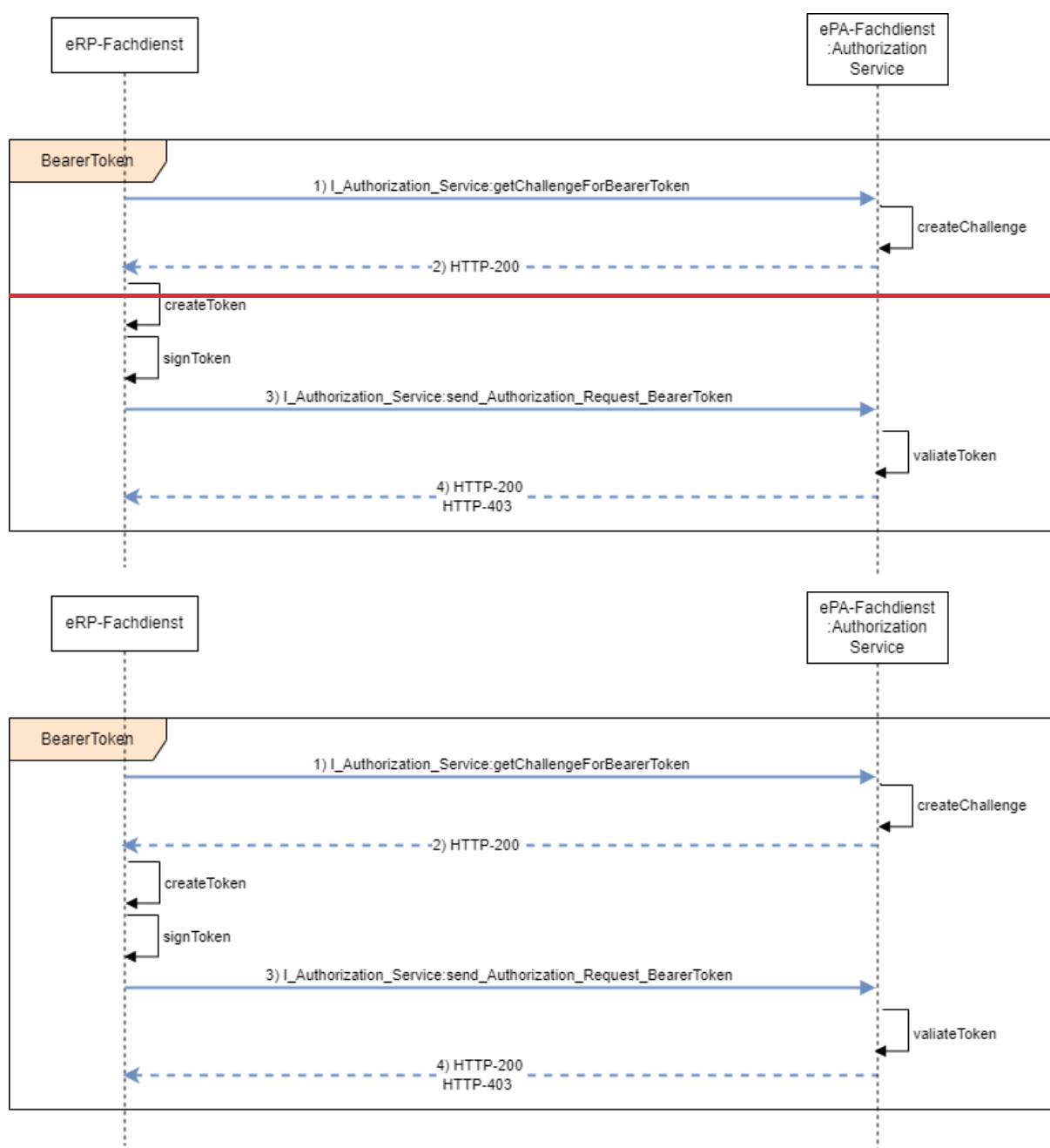


Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes

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.

6309
6310

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Krypt]
	"sub"	Telematik-ID des E-Rezept-Fachdienstes	

6311 [**<=**]

6312 Das Signaturzertifikat zu "x5c" (AUT-Zertifikat der E-Rezept-VAU) kommt aus der
6313 Komponenten-PKI der TI. Basiert der öffentlichen Schlüssel auf der ECC-Kurve
6314 brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve
6315 und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß
6316 [RFC7515] zu erstellen.

6317 ~~3.17~~**3.18** Anbindung Verzeichnisdienst FHIR-Directory

6318 **A_25176 - ePA-Aktensystem - Anbindung Verzeichnisdienst FHIR-Directory**

6319 Das ePA-Aktensystem MUSS bei der Suche des Versicherten nach Einträgen
6320 im Verzeichnisdienst FHIR-Directory und bei der initialen Anlage einer Akte den
6321 Anwendungsfall "AF_10219* - Versicherter sucht Einträge im FHIR-Directory" gemäß
6322 [gemSpec_VZD_FHIR_Directory] als Fachdienst unterstützen und dabei für die Client
6323 Anfrage von search-access_token die Operation getFHIRVZDtoken gemäß
6324 [I_Authorization_Service.yaml] bereitstellen. [**<=**]

6325 ~~3.18~~**3.19** Access Gateway

6326 Das Access Gateway ermöglicht den Versicherten bzw. deren berechtigten Vertretern den
6327 Zugang zum zugehörigen Aktensystem über das Internet. Auf der einen Seite dient es
6328 der Abschottung des ePA-Aktensystems in Richtung Internet, auf der anderen Seite

6329 regelt es den kontrollierten Zugriff der Versicherten auf das Aktensystem mit seinen
6330 funktionalen Komponenten.

6331 **3.18.13.19.1 Paketfilter**

6332 **3.18.1.13.19.1.1 Funktion**

6333 Der Paketfilter stellt die Anbindung des ePA-Aktensystems an das Internet her und
6334 gewährleistet die Abschottung des ePA-Aktensystems in Richtung Internet.

6335 **A_14017 - Access Gateway, Sicherung zum Transportnetz Internet durch** 6336 **Paketfilter**

6337 Das ePA-Aktensystem MUSS zum Transportnetz Internet durch einen Paketfilter (ACL)
6338 gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der
6339 Paketfilter der Komponente Access Gateway MUSS frei konfigurierbar sein auf der
6340 Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse,
6341 IP-Protokoll sowie Quell- und Zielport.[<=]

6342 **A_14018 - Access Gateway, Platzierung des Paketfilters Internet**

6343 Der Paketfilter der Komponente Access Gateway, zum Schutz in Richtung Transportnetz
6344 Internet, DARF NICHT auf den anderen, zum Access Gateway gehörenden, physischen
6345 Komponenten implementiert werden.[<=]

6346 **A_14019-02 - Access Gateway, Richtlinien für den Paketfilter zum Internet**

6347 Der Paketfilter der Komponente Access Gateway MUSS die Weiterleitung von IP-Paketen
6348 an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

- 6349 1. HTTPS, und
6350 2. OCSP-Zugriffe für das OCSP-Stapling (vgl. Hinweis nach A_14019-02), ggf.
6351 notwendige DNS Anfragen (und Antworten).

6352 Ein Verbindungsaufbau aus dem ePA-Aktensystem über das Access Gateway in Richtung
6353 Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 .[<=]

6354 *Hinweis zu A_14019-02: Der Aktensystem-Anbieter muss für seine HTTPS-Schnittstelle*
6355 *ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-*
6356 *Zertifikate also über einen aktuellen Webbrowser prüfbar ist, vgl. A_14776). Für dieses*
6357 *TLS-Zertifikat fragt das Access Gateway (die HTTPS-Schnittstelle ist Teil davon)*
6358 *regelmäßig für das OCSP-Stapling (vgl. [gemSpec_Krypt#A_24913-*) den OCSP-*
6359 *Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält*
6360 *das Access Gateway eine OCSP-Response. Diese wird nach A_19126 geprüft und*
6361 *anschließend von der HTTPS-Schnittstelle verwendet*
6362 *(vgl. <https://tools.ietf.org/html/rfc6066#section-8> und*
6363 *bspw. http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling).*

6364 Um dies zu ermöglichen, muss der Paketfilter entsprechende stateful-Firewall-Regeln
6365 gemäß A_14019-* und A_19126 definieren.

6366 **A_19126-02 - Access Gateway, OCSP-Status für das OCSP-Stapling**

6367 Der Paketfilter der Komponente Access Gateway MUSS bezüglich des OCSP-Stapling
6368 (vgl. A_24913-*) folgende Vorgaben umsetzen:

- 6369 1. Für das vom Aktensystem-Anbieter erworbene TLS-Zertifikat (vgl. Hinweis zu
6370 A_14019-01) MUSS die Komponente initial die IP-Adresse (ggf. die IP-Adressen)
6371 des entsprechenden OCSP-Responser ermitteln.

- 6372 2. Diese IP-Adresse(n) MÜSSEN gemäß A_14019-01 per stateful-Firewalling
6373 Verbindungen von der HTTPS-Schnittstelle an den OCSP-Responder erlaubt
6374 werden.
- 6375 3. Gemäß OCSP-Stapling (<https://tools.ietf.org/html/rfc6066#section-8>) MUSS die
6376 Komponente regelmäßig eine OCSP-Response vom entsprechenden OCSP-
6377 Responder beziehen (Die Regelmäßigkeit wird vom zertifikatsausgebenden TSP
6378 und der Gültigkeitsdauer dessen OCSP-Responses bestimmt).
- 6379 4. Die OCSP-Responses MÜSSEN von der Komponente geprüft werden
6380 (Signaturprüfung, CertID in der OCSP-Response passt zum angefragten
6381 Zertifikat). Falls eine der Prüfung ein nicht-positives Ergebnis liefert, so MUSS die
6382 erhaltene OCSP-Response verworfen werden.
- 6383 5. Sollte die letzte in der Komponente vorhandene OCSP-Response zeitlich nicht
6384 mehr gültig sein (bspw. der OCSP-Responder im Internet war länger nicht
6385 erreichbar), so MUSS diese OCSP-Response verworfen werden und ein von einem
6386 Klienten (ePA FdV) initiiertes TLS-Verbindungsaufbau der HTTPS-Schnittstelle
6387 ohne OCSP-Stapling durchgeführt werden.

6388 [\leq]

6389 **A_14776 - Access Gateway, Richtlinien zum TLS-Verbindungsaufbau**

6390 Die Komponente Access Gateway MUSS sich beim TLS-Verbindungsaufbau gegenüber
6391 dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB
6392 Forum] authentisieren. Das Zertifikat MUSS an die Schnittstelle der Proxy-Komponente
6393 gebunden werden.[\leq]

6394 **~~3.18.1.23.19.1.2~~ Redundanz**

6395 Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf#3.18.1.3]. Die
6396 Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Access
6397 Gateways.

6398 Die Auswahl der Access Gateways wird durch das ePA-Frontend des Versicherten aus
6399 einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des Access
6400 Gateways kann der Anbieter des ePA-Aktensystems durch die Konfiguration und
6401 Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn
6402 jeder Versicherte mit existierendem Konto beim Anbieter des ePA-Aktensystems oder
6403 dessen berechtigter Vertreter die Möglichkeit zum Verbindungsaufbau hat.

6404 Eine hardwaretechnische Hochverfügbarkeit der einzelnen Access Gateways ist über
6405 grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht
6406 dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische
6407 Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern
6408 einzusetzen, so dass jedes einzelne Access Gateway im Ergebnis eine höhere
6409 Verfügbarkeit oder Leistungsfähigkeit besitzt.

6410 **A_14026 - Access Gateway, Redundanz der Paketfilter im Access Gateway**

6411 Die Komponente Access Gateway MUSS sicherstellen, dass bei Ausfall eines von
6412 mehreren Paketfiltern die verbleibenden Paketfilter in dem-selben Standort den
6413 Datenverkehr aller Mandanten des ausgefallenen Paketfilters zusätzlich übernehmen
6414 können.[\leq]

6415 **~~3.18.1.33.19.1.3~~ Konfiguration**

6416 **A_14030 - Access Gateway, Verhalten des Access Gateways bei Volllast**

6417 Die Komponente Access Gateway MUSS den Paketfilter Internet so konfigurieren, dass
6418 bei Volllast der Systemressourcen im ePA-Aktensystem keine weiteren
6419 Verbindungen angenommen werden. [\leq]

6420 Durch die Zurückweisung von Verbindungen wird sichergestellt, dass das ePA-Frontend
6421 des Versicherten einen Verbindungsaufbau mit einem anderen Access Gateway des
6422 jeweiligen ePA-Aktensystems versucht, bei dem die erforderlichen Ressourcen zur
6423 Verfügung stehen.

6424 **~~3.18.1.43.19.1.4~~ Adressierung**

6425 **~~3.18.1.4.13.19.1.4.1~~ Access Gateway zum Transportnetz Internet**

6426 **A_14031 - Access Gateway, IPv4-Adressierung der Internetschnittstellen des**
6427 **Access Gateways**

6428 Der Anbieter des ePA-Aktensystems MUSS jedem Access Gateway genau eine öffentliche
6429 IPv4-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum
6430 Internet konfiguriert werden. Die öffentlichen IP-Adressen des Access Gateways MÜSSEN
6431 vom Anbieter des ePA-Aktensystems zur Verfügung gestellt werden. [\leq]

6432 **A_14032 - Access Gateway, IPv6-Adressierung der Internetschnittstellen des**
6433 **Access Gateways**

6434 Der Anbieter des ePA-Aktensystems SOLL jedem Access Gateway eine IPv6-Adresse
6435 zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert
6436 werden. Die öffentliche IPv6-Adresse MUSS vom Anbieter des Access Gateways zur
6437 Verfügung gestellt werden. [\leq]

6438 **~~3.18.1.4.23.19.1.4.2~~ ePA-Aktensystem zum Zentralen Netz**

6439 Die Adressen des ePA-Aktensystems am Übergang zur TI werden vom Anbieter des
6440 Zentralen Netzes aus dem Adressblock TI_Zentral zugewiesen.

6441 **~~3.18.23.19.2~~ Proxy für das VAU-Protokoll**

6442 Das Access Gateway leitet Anfragen vom ePA-FdV über den VAU-Kanal an die zuständige
6443 VAU-Instanz weiter, damit diese dort in der User Session des Versicherten verarbeitet
6444 werden können.

6445 **A_24331 - Access Gateway - Data Proxy**

6446 Das Access Gateway MUSS die VAU-Protokoll-Kommunikation des ePA-Frontend des
6447 Versicherten an die zuständige VAU-Instanz weiterleiten. [\leq]

6448 **~~3.18.33.19.3~~ Proxy Schlüsselgenerierungsdienst**

6449 Zur Nutzung der in [gemSpec_SGD_ePA] beschriebenen Schlüsselableitungsfunktionalität
6450 für den Schutz von Akten- und Kontextschlüssel einer ePA werden Aufrufe zu den
6451 Schlüsselgenerierungsdiensten SGD 1 und SGD 2 über den "Proxy
6452 Schlüsselgenerierungsdienst" ermöglicht.

6453 Der Proxy SGD stellt sicher, dass ein ePA-FdV Aufrufe an den SGD 1 und SGD 2
6454 durchführen kann.

6455 Die Information, auf welche Anfragen (Pfade) des ePA-FdV der Proxy SGD aktiv wird
 6456 ("/SGD1" für den SGD 1 und "/SGD2" für den SGD 2), sind in [gemSpec_SGD_ePA#2.2
 6457 Tabelle 2] angegeben.

6458 **A_17495 - Access Gateway, Zugriff auf den Schlüsselgenerierungsdienst**
 6459 Der Proxy Schlüsselgenerierungsdienst der Komponente Access Gateway MUSS
 6460 sicherstellen, dass das ePA-FdV auch ohne Authentisierung und Autorisierung Zugriff auf
 6461 den SGD 1 und den SGD 2 erhält.
 6462 [**<=**]

6463 **3.18.43.19.4 Tracing in Nichtproduktivumgebungen**

6464 Für die Fehlersuche - insbesondere bei IOP-Problemen zwischen Produkten verschiedener
 6465 Hersteller in einer fortgeschrittenen Entwicklungsphase - hat es sich als notwendig
 6466 erwiesen, dass ein Fehlersuchender den Klartext der Kommunikation zwischen ePA-Client
 6467 und VAU-Instanz mitlesen kann. (vgl. auch 2.5- Tracing in Nichtproduktivumgebungen)

6468 Das Access Gateway stellt Informationen über die aktuell verfügbaren Sensorpunkte im
 6469 AS bereit. Weiterhin exponiert das Access Gateway die Daten der Sensorpunkte über TCP
 6470 (i. S. v. nicht TLS-gesichert) bspw. über Port 8001,...,8009. Die dort von den
 6471 Sensorpunkten ge-streamten Daten sind nur Testdaten, also keine Echtdaten, d. h. sie
 6472 haben keinen Schutzbedarf bezüglich Vertraulichkeit. Um die exponierten Sensordaten-
 6473 Punkte vor DoS-Angriffen zu schützen, erlaubt das Access Gateway im Fall der Fälle die
 6474 TCP-Ports auf IP-Layer über Firewall-Regeln abzusichern.

6475 **A_21890-01 - Access Gateway, Sensorpunkt für Nichtproduktivumgebungen**
 6476 Die Komponente Access Gateway MUSS genau in Nichtproduktivumgebungen:

- 6477 • die Daten der Sensorpunkte des Aktensystems auf TCP-Ports (bspw. ab Port
 6478 8000) öffentlich (ggf. auch ohne TLS-Sicherung) im Internet zur Verfügung
 6479 stellen, indem die aktuell an den Sensorpunkten auflaufenden Daten auf dem
 6480 TCP-Port am Access Gateway öffentlich gestreamt werden.
- 6481 • die Möglichkeit bieten, den Zugriff auf diese TCP-Ports durch Firewall-
 6482 Einstellungen auf IP-Layer zu beschränken.

6483 Weiterhin MUSS das Access Gateway über die URL /tracingpoints Informationen über die
 6484 aktuell im AS verfügbaren und damit auch im Access Gateway öffentlich exponierten
 6485 Sensorpunkt-Daten als JSON-Array (=> Response-Type 'application/json') der folgenden
 6486 Form bereitstellen:

```
6487 [
6488 {"name" : "zentraler Tigerproxy",
6489  "port" : 8001,
6490  "DoS-protection-type" : „secret_url“
6491  "DoS-protection-port" : „udp/46789“
6492 },
6493 {"name" : "Extra Senor VAU RZ2/B1/R1",
6494  "port" : 8002,
6495  "DoS-protection-type" : „ssh_tunnel“
6496  "DoS-protection-port" : „tcp/46790“
6497 }, ...
6498 ]
```

6499 Sollten keine Sensorpunkte aktuell im AS aktiviert sein (bspw. bei Lasttests) so ist das
 5000 Array leer: [].

5001 Sollte es keinen optionalen DoS-Schutzmechanismus gemäß A_22582-* geben, so fallen
 5002 die DoS-* Attribute in der o. g. Datenstruktur weg (sind nicht existent).

5003 Die einzelnen Felder des Arrays sind associative array (oder auch maps oder dictionaries

6504 genannt). Diese KÖNNEN neben "name" und "port" beliebige vom AS definierbare,
 6505 weitere key-value-Paare enthalten. Der Eintrag "port" gibt an, an welchem öffentlich
 6506 erreichbaren TCP-Port des Access Gateway die Sensordaten des entsprechenden Sensors
 6507 abrufbar sind (gestreamt werden).
 6508 [\leq]

6509 *Hinweis zu A_21890-**: Die semistatische JSON-Datei, welche ein Client unter dem Pfad
 6510 „/tracingpoints“ erhalten kann, ist eine einfache Form von Service-Discovery. Damit kann
 6511 ein Client (Fehlersuchende(r)) erfahren, welche Tracing-Quellen es aktuell im AS gibt i.
 6512 S. v. welche Tracing-Quellen ein Client zur Fehlersuche aktuell verwenden kann.

6513 **A_22582 - Tracing in Nichtproduktivumgebungen, DoS-Schutz**

6514 Die Komponente Access Gateway KANN Sicherheitsmechanismen bereitstellen und
 6515 aktivieren, die es genau in Nichtproduktiv-umgebungen ermöglichen, temporär,
 6516 automatisiert und nur nach erfolgreicher Authentifizierung die TCP-Ports für das
 6517 Streaming der Sensorpunkte für Clients nach A_21890-* freizuschalten. [\leq]

6518 *Hinweis zu A_22582-**: In den Nichtproduktivumgebungen darf es keine Echtdaten
 6519 geben. Es dürfen sich dort nur Daten befinden, deren Schutzbedarf bezüglich
 6520 Vertraulichkeit niedrig ist. Der optionale Schutzmechanismus nach A_22582-* braucht
 6521 nur einen einfachen DoS-Schutz leisten gegen einen Angreifer mit niedrigen
 6522 Angriffspotential. Der Anbieter ist, sofern er einen solchen Mechanismus einsetzen
 6523 möchte, frei, dafür den Mechanismus selbst zu wählen. Er wählt dann bei "DoS-
 6524 protection-type" (vgl. A_21890-*) einen selbstdefinierten (möglichst sprechenden)
 6525 Namen.

6526 Beispiele für Umsetzungsmöglichkeiten:

- 6527 1. Es gibt im Access Gateway eine geheime URL (bspw.
 6528 /tracing/964b059de83d20581f43dd1b867d740c). Ein Client kennt das Geheimnis
 6529 und ruft diese URL auf. Daraufhin wird im Access Gateway für die IP-Adresse des
 6530 Clients die Tracing-Quelle im Access Gateway frei geschaltet (TCP-Port 8000, ...).
- 6531 2. Die gematik stellt eine Beispielimplementierung zur Verfügung. Dort gibt es einen
 6532 UDP-Server (Access Gateway) und einen UDP-Client (Fehlersuchende), die beide
 6533 ein gemeinsames HMAC-Geheimnis teilen. Wenn der Client die aktuelle Zeit und
 6534 dessen IP-Adresse per HMAC authentisiert dem UDP-Server sendet, so schaltet
 6535 der UDP-Server nach erfolgreicher Prüfung des HMACs den entsprechenden TCP-
 6536 Port für die authentifizierte IP-Adresse des Clients frei.
- 6537 3. Auf dem Access Gateway läuft ein SSH-Daemon. Der öffentliche
 6538 Authentisierungsschlüssel eines Clients ist dort als gültiger Nutzer konfiguriert
 6539 (Login-Shell: /bin/false). Die Tracing-Quellen im Access Gateway sind so
 6540 konfiguriert, dass sie nur mittels authentisierten SSH-Port-Forwarding (
 6541 <https://www.ssh.com/academy/ssh/tunneling/example>) erreichbar sind.

6542 **~~3.18.53.19.5~~ Übergreifende Festlegungen**

6543 **A_14249 - Komponente Access Gateway - Separierung der Schnittstellen für** 6544 **verschiedene Umgebungen**

6545 Die Komponente Access Gateway MUSS die Bereitstellung von Schnittstellen für die
 6546 Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen
 6547 Umgebungen der TI (RU/TU, PU) sicherstellen und voneinander separieren. [\leq]

6548 **A_14034 - Access Gateway, Übergang des ePA-Aktensystems zur TI**

6549 Die Komponente Access Gateway MUSS sicherstellen, dass der Zugriff auf Dienste der TI
 6550 ausschließlich über einen Sicheren Zentralen Zugangspunkt (SZZP) erfolgt. [\leq]

A_14036 - Access Gateway, Synchronisierung der Komponenten mit den Stratum-1-NTP-Servern der TI

Die Komponente Access Gateway MUSS alle Komponenten seines Access Gateways mit den Stratum-1-NTP-Servern der TI synchronisieren. [≤]

A_13879 - Access Gateway, Serverseitige Authentisierung

Die Komponente Access Gateway MUSS sich gegenüber dem ePA-Frontend des Versicherten beim Aufbau der TLS-Session durch sein ExtendedValidation-Zertifikat authentisieren. Die Beschaffung des Zertifikats erfolgt durch den Anbieter über eine öffentliche CA. [≤]

A_14033 - Access Gateway, TLS Verschlüsselung

Die Komponente Access Gateway MUSS sicherstellen, dass jede Kommunikation mit dem ePA-Frontend des Versicherten TLS verschlüsselt erfolgt. [≤]

Die Verwendung der SoapAction ermöglicht einer Reverse-Proxy-Komponente innerhalb des Access Gateways, die Nachrichten zu verarbeiten, ohne die http-Payload zu untersuchen.

A_13876 - Access Gateway, Kein direkter Zugriff auf Dienste der zentralen TI-Plattform

Die Komponente Access Gateway MUSS einen direkten Zugriff aus dem Internet auf Dienste der zentralen TI-Plattform verhindern. [≤]

A_14016 - Access Gateway, Schutz vor Angriffen aus dem Internet

Die Komponente Access Gateway MUSS für alle vom Internet erreichbaren Schnittstellen Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS Lösungen verhindert werden. [≤]

A_15196 - Access Gateway, Schutz vor volumetrischen DoS-Angriffen

Die Komponente Access Gateway MUSS bei Beauftragung eines qualifizierten Dienstleisters zum Schutz vor volumetrischen DoS-Angriffen Kriterien des BSI zur Auswahl qualifizierter Dienstleister umsetzen. [≤]

Als Maßnahme gegen volumetrische Denial-of-Service-Angriffe wird die Verwendung von DNS- oder BGP-Routing-Diensten empfohlen. Hinweise des BSI:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos_node.html.

3.20 Data Submission Service

Die Daten der elektronischen Patientenakten sollen nach § 363 Absatz 1 SGB V für die in § 303e Absatz 2 SGB V aufgeführten Sekundärnutzungszwecke zugänglich gemacht und hierfür in pseudonymisierter Form automatisiert von den ePA-Aktensystemen an das Forschungsdatenzentrum Gesundheit (FDZ) nach § 303d SGB V übermittelt werden, sofern Versicherte dem nicht widersprochen haben.

Neben dem FDZ und den ePA-Aktensystemen ist die Vertrauensstelle (VST) nach § 303c SGB V im Prozess involviert. Deren Aufgabe ist es, die von den ePA-Aktensystemen erhaltenen Lieferpseudonyme in periodenübergreifende Pseudonyme umzuwandeln und diese an das FDZ zu übermitteln.

Der Data Submission Service im Aktensystem übernimmt in der Übermittlung der pseudonymisierten medizinischen Daten folgende Aufgaben:

- Erstellung der Lieferpseudonyme (auf Basis der KVNR) und der Arbeitsnummern
- Registrierung der Arbeitsnummer mit dem zugehörigen Lieferpseudonym bei der Vertrauensstellen
- Pseudonymisierung der medizinischen Daten
- Verknüpfung der pseudonymisierten medizinischen Daten mit der Arbeitsnummer
- Übermittlung der pseudonymisierten medizinischen Daten und der zugehörigen Arbeitsnummern an das Forschungsdatenzentrum Gesundheit

Die Übermittlung der Daten erfolgt blockweise. D.h. es wird ein Paket von pseudonymisierten medizinischen Daten mit zugehörigen Arbeitsnummern aus verschiedenen Aktenkonten zusammengestellt (Datenpaket FDZ) und alle für dieses Paket benötigten Arbeitsnummern und Lieferpseudonyme mit einem Mal bei der VST registriert (Datenpaket VST). Die Datenpakete haben eine anbieterübergreifend eindeutige SubmissionID und die SubmissionID zusammengehöriger Datenpakete VST und FDZ ist identisch.

Für die Übermittlung wird zwischen Aktensystem und VST, sowie Aktensystem und FDZ jeweils ein beidseitig authentifierter VAU-Kanal aufgebaut, auf dem sich die Dienste VST und FDZ mit einer Identität ID.FD.AUT mit ihren entsprechenden Rollen authentisieren.

Der Versicherte kann mit Hilfe seines ePA-FdVs oder über die Ombudsstelle des Kostenträgers der Übermittlung seiner pseudonymisierten medizinischen Daten an das FDZ widersprechen oder die möglichen Sekundärnutzungszwecke seiner übermittelten pseudonymisierten medizinischen Daten im FDZ einschränken. Dies erfolgt über das Consent Decision Management im Aktensystem.

3.20.1 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. [<=]

A 26409 - Data Submission Service - keine Erstellung von LP für Validierungsaktenkonten

Der Data Submission Service DARF KEINE Lieferpseudonyme für KVNRn von Validierungsaktenkonten erstellen. [<=]

A 26212 - Data Submission Service - Erstellung der Arbeitsnummer

Der Data Submission Service MUSS für die Arbeitsnummer einen Zufallswert mit einer Mindestentropie von 120 Bit erzeugen und die Kodierung aus [I VST] verwenden. [<=]

A 26410 - Data Submission Service - keine Erstellung von AN für Validierungsaktenkonten

Der Data Submission Service DARF KEINE Arbeitsnummern für Daten aus Validierungsaktenkonten erstellen. [<=]

A 26255 - Data Submission Service - Verwendungsdauer von Lieferpseudonymen und Arbeitsnummern

Der Data Submission Service MUSS für jedes in einem Datenpaket FDZ übermittelte pseudonymisierte medizinische Datum zu einer KVNR eine neue Arbeitsnummer und ein neues Lieferpseudonym generieren. [\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. [\leq]

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. [\leq]

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"). [\leq]

Tabelle 42: Auswahl der zu übertragenden FHIR-Ressourcen

<u>Ressourcentyp / Profil</u>	<u>Filter Expression</u>	<u>Include</u>
<u>MedicationRequest</u> <u>\${epa-medication}/epa-medication-request</u>	<u>status != 'active' and</u> <u>identifier.where(system='https://gematik.de/fhir/epa-medication/sid/rx-</u> <u>prescription-process-</u> <u>identifier').hasValue()</u>	<u>MedicationRequest:me-</u> <u>dication</u>
<u>MedicationDispense</u> <u>\${epa-medication}/epa-medication-response</u>	<u>status != 'in-progress' and</u> <u>extension('https://gematik.de/fhir/epa-</u> <u>medication/StructureDefinition/rx-</u> <u>prescription-process-identifier-</u> <u>extension').hasValue()</u>	<u>MedicationDispense:m-</u> <u>edication</u>

Tabelle 43: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen

<u>Ressourcentyp/Profil</u>	<u>Anmerkung</u>
<u>Medication</u> <u>\${epa-medication}/epa-medication</u>	<u>Referenziert durch MedicationRequest,</u> <u>MedicationDispense</u>

3.20.3 Protokollierung des Datenexports an das FDZ

Ein Datenexport erfolgt immer in Verbindung mit dem Einstellen neuer oder der
Änderung existierender Daten für ein Aktenkonto. Ein Datenexport nach Auswahl der
Daten gemäß A 26298 wird als Bestandteil der Protokollierung des auslösenden
Ereignisses protokolliert (siehe dazu: 3.13.2.2- Medication Service)

3.20.4 Pseudonymisierung von medizinischen Daten

Bevor medizinische Daten an das FDZ übermittelt werden dürfen, müssen diese
pseudonymisiert werden und Daten mit direktem Personenbezug entfernt werden.

A 26300 - Data Submission Service - Pseudonymisierung von medizinischen Daten

Der Data Submission Service MUSS an das FDZ zu übermittelnde medizinische Daten
gemäß der Vorgaben aus [DataPseudonymization] pseudonymisieren. [≤]

A 26408 - Data Submission Service - keine Pseudonymisierung von Daten aus Validierungsaktenkonten

Der Data Submission Service DARF KEINE Daten aus Validierungsaktenkonten (gem. Kapitel 2.4) pseudonymisieren. [\leq]

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. [\leq]

Verständnishinweis:

Die Akten werden regelmäßig nach zu übermittelnden Daten vom ePA-Aktensystem durchsucht. Dabei kann es passiert, dass in einer Akte mehrere Daten zur Übermittlung anfallen, die nach der Pseudonymisierung in einer Reihenfolge in das Datenpaket FDZ gelangen. Deshalb kann die Reihenfolge der Einträge im Datenpaket FDZ statistisch relevante Informationen über den Zusammenhang von Einträgen geben. Durch eine Randomisierung der Reihenfolge der Einträge innerhalb des Datenpakets wird dies verhindert. Die AN werden zufällig erzeugt, eine Sortierung nach AN ist deshalb eine Randomisierung der Reihenfolge.

3.20.5 Übermittlung der pseudonymisierten medizinischen Daten

Die Übermittlung von Datenpaketen an VST und FDZ erfolgt gemäß den Vorgaben des RKI (VST) und BfArM (FDZ) und deren Schnittstellenspezifikationen.

Die Übermittlung der pseudonymisierten Daten eines Aktenkontos für Sekundärnutzungszwecke erfolgt automatisch, sofern kein Widerspruch gegen Sekundärdatennutzung vorliegt. Die Voreinstellung ist dabei "kein Widerspruch erteilt" (siehe: 3.8.1- Widersprüche für Funktionen der ePA). Vor der allerersten Übermittlung solcher Daten wird dem Versicherten daher eine Frist gewährt, gegebenenfalls einen Widerspruch gegen diese Sekundärdatennutzung zu formulieren.

A 26462 - Data Submission Service - Übermittlung Datenpaket nach Ablauf der Widerspruchsfrist

Der Data Submission Service MUSS sicherstellen, dass vor der erstmaligen Übermittlung von Daten eines Aktenkontos die Widerspruchsfrist gemäß den Vorgaben des Kostenträgers abgelaufen ist. [\leq]

Hinweis: Die erste Datenübermittlung ist die erste automatisiert mögliche Übermittlung (nach Aktivierung des Aktenkontos) und nicht die erste Datenübermittlung nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung.

Hinweis: Für eine Übermittlung nach Ablauf dieser Widerspruchsfrist oder nach Rücknahme eines Widerspruchs gegen die Sekundärdatennutzung werden immer nur ab diesem Zeitpunkt neu angefallene Daten berücksichtigt, Es erfolgt keine Übermittlung von vorhandenen Daten des Aktenkontos.

A 26214 - Data Submission Service - Erstellung der SubmissionID

Der Data Submission Service MUSS für zusammengehörige Datenpakete VST und FDZ eine gemeinsame anbieterübergreifend eindeutige SubmissionID erzeugen und diese mit den Datenpaketen übertragen. [\leq]

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. [\leq]

A 26215 - Data Submission Service - Übermittlung Datenpaket VST

Der Data Submission Service MUSS das Datenpaket VST gemäß [I VST] an die Vertrauensstelle übermitteln. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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

[\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

Hinweis zu A 26307: Zum Zeitpunkt des Eingangs des Widerspruchs im Aktensystems bereits in der Übermittlung befindliche Datenpakete sind von der Anforderung ausgeschlossen. Betroffen sind jedoch auch die aktuell in Erstellung befindlichen Datenpakete VST und FDZ, bei denen die Übermittlung an die VST bzw. das FDZ noch nicht begonnen hat.

3.21 Push Notification Management

Nutzer von Anwendungen für Versicherte (ePA-FdV) können mittels Push Notifications direkt über Ereignisse in bestimmten Fachdiensten der TI oder des Kostenträgers auf ihren Endgeräten informiert werden. Diese Notifications erreichen einen Nutzer auch außerhalb aktiver Anmeldungen in diesen Fachdiensten. Die Ereignisse von Interesse zur Benachrichtigung des Nutzers sind dabei individuell abonnierbar.

Der Versand einer Push Notification erfolgt stets durch die einzelnen Fachdienste für Ereignisse ihrer Domäne. Die Übertragung in das Endgerät des Nutzers unter Einbindung der plattformspezifischen, externen Push-Dienste und betreiberspezifischen Push-Gateways wird für alle beteiligten Fachdienste gemeinsam durch ein Push Notification System realisiert. Dieses anwendungsübergreifende System und seine Komponenten für Push Notifications im Gesundheitswesen sind in [gemF PushNotification] und [PushNotificationConcept] detailliert beschrieben.

Dort sind auch die normativen Vorgaben für unterstützende Anwendungen und Fachdienste in Bezug auf Registrierung von Applikationen und Ereignissen für Push Nachrichten, Schnittstellen, sicherheitstechnische Anforderungen und notwendige Artefakte für einen interoperablen Betrieb formuliert.

3.21.1 Push Notification Management des ePA-Aktensystems

Das Push Notification Management des ePA-Aktensystems ist als ein spezifischer Fachdienst in dieses übergreifende System eingebunden und bedient die in [gemF PushNotification] geforderten und in [PushNotificationConcept] beschriebenen Schnittstellen und Verfahren.

Push Notifications der ePA können ausschließlich durch Versicherte für Ereignisse ihres eigenen Aktenkontos genutzt werden. Der Erhalt von Benachrichtigungen aus dem Aktenkonto eines vertretenen Versicherten wird nicht unterstützt.

Der Nutzung des Push Notification Managements der ePA kann nicht widersprochen werden. Dieser Dienst gehört nicht zu den widerspruchsfähigen Funktionen der ePA. Versicherte, die keine Benachrichtigungen der ePA erhalten möchten, können die Benachrichtigungen durch Abwahl der Benachrichtigungskanäle oder auch generell durch den Verzicht des ePA-FdV auf eine Registrierung für Push Notifications unterbinden.

Schnittstellen, die das Push Notification Management der ePA zur Nutzung durch Clients (ePA-FdV) anbietet, sind um ePA-spezifische Verfahren und Anforderungen ergänzt und als OpenApi gemäß [I Push Notification Management] verfügbar.

A 27637 - Push Notification Management - Realisierung der Schnittstelle I Push Notification Management

Das Push Notification Management MUSS die Operationen der Schnittstelle I Push Notification Management gemäß [I Push Notification Management] umsetzen.[<=]

3.21.2 Registrierung eines ePA-FdV als Pusher

(siehe auch: [gemF PushNotification]#Kapitel "Pusher registrieren")

Ein Versicherter kann registrierte Geräte (im Sinne des Device Managements gemäß 3.12- Device Management) zur Nutzung seiner aktivierten elektronischen Patientenakte auch für den Erhalt von Push Nachrichten nutzen, sofern das übergreifende Push Notification System die technologische Infrastruktur für Benachrichtigungen an den Geräte-, bzw. Betriebssystemtyp des Versichertengeräts unterstützt. Dazu kann die ePA-FdV-Anwendung jedes dieser Geräte als ePA-FdV Instanz, bzw. 'Pusher', im eigenen Aktenkonto des Versicherten registriert werden.

Die ePA-FdV Instanz Registrierung eines Gerätes als Pusher erfolgt immer durch und für das auf diesem Gerät installierte ePA-FdV und unter Nutzung der Schnittstelle [I Push Notification Management]. Über diese Schnittstelle werden existierende Registrierungen auch aktualisiert und wieder entfernt.

Die Daten der Registrierungen, inklusive des kryptographischen Materials der Schlüsselableitungen und der Auswahl der Benachrichtigungskanäle, sind Bestandteil des Aktenkontos und werden dort gespeichert. Pro registriertem Gerät kann jeweils nur eine ePA-FdV Instanz im Aktenkonto hinterlegt sein und eine Registrierung gilt immer nur für genau eine bestimmte ePA-FdV Instanz. Eine ePA-FdV Instanz Registrierung ist daher fest an eine Device Registration gebunden.

A 27638 - Push Notification Management- Speicherung der Daten

Das Push Notification Management MUSS alle Daten des Dienstes für einen Versicherten im SecureDataStorage des Aktenkontos des Versicherten speichern. [\leq]

A 27640 - Push Notification Management - automatisches Löschen der Registrierung einer ePA-FdV Instanz

Das Push Notification Management MUSS sicherstellen, dass eine existierende Registrierung einer ePA-FdV Instanz und die dazugehörigen Daten vollständig und automatisch gelöscht werden, wenn die Device Registration des assoziierten Geräts im Device Management des Aktensystems gelöscht wird. [\leq]

A 27639 - Push Notification Management - eindeutiger pushKey

Das Push Notification Management MUSS sicherstellen, dass der `pushKey` einer Registrierung einer ePA-FdV Instanz eindeutig ist und es keine zwei oder mehr Registrierungen mit gleichem `pushKey` gibt. [\leq]

Bei jedem Versand einer Push Nachricht an das Push Gateway kann dieses in den Rückgabewerten der Push Operation einen Eintrag oder eine Liste veralteter, bzw. ungültiger `pushKeys` melden. Eine weitere Nutzung solcher Registrierungen, bzw. `pushKeys`, soll unterbleiben. Die assoziierten Registrierungen von ePA-FdV-Instanzen werden daher aus dem Aktenkonto entfernt.

A 27682 - Push Notification Management - Entfernen ungültiger pushKeys

Das Push Notification Management MUSS Registrierungen von ePA-FdV-Instanzen löschen, wenn `pushKeys` dieser Registrierungen durch das Push Gateway als ungültig gemeldet werden. [\leq]

Hinweis: Es werden nur Registrierungen aus dem versendenden Aktenkonto entfernt. Eventuelle Rückmeldungen des Push Gateways zu `pushKeys`, die nicht oder nicht mehr mit dem versendenden Aktenkonto verbunden sind, werden ignoriert.

3.21.3 Push Notification Channels

(siehe auch: [gemF PushNotification]#Kapitel "Channel/ Trigger Konfiguration")

Das ePA-Aktensystem bietet eine Auswahl an Channels zu Ereignissen, über deren Aktivität ein Versicherter durch Push-Benachrichtigungen informiert werden kann. Der jeweilige Nachrichteninhalte beschreibt dabei in Kurzform das auslösende Ereignis.

Die Grundeinstellung für den Versand von Push-Benachrichtigungen an neu erstellten Registrierungen für ePA-FdV-Instanzen lautet für jeden Channel zunächst deaktiviert ('disabled' - keine Benachrichtigung für diesen Kanal). Ein Versicherter kann diese Grundeinstellung individuell für jede seiner ePA-FdV-Instanzen jederzeit ändern und die Benachrichtigung pro Channel aktivieren ('enabled' - Benachrichtigungen für diesen Kanal), bzw. auch wieder deaktivieren.

Die Verwaltung der individuellen Channelkonfiguration des ePA-Aktenkontos für eine registrierte ePA-FdV-Instanz erfolgt über die Schnittstelle [I Push Notification Management].

A 27641 - Push Notification Management - Push Notification Channels

Das Push Notification Management MUSS ausschließlich für die folgenden Ereignisse Push Nachrichten erstellen können, wenn das Ereignis durch einen Nutzer der definierten

Nutzergruppe ausgelöst wird.

<u>Ereignis</u>	<u>channelId</u>	<u>Beschreibung</u>	<u>Nutzergruppen</u>
<u>Neues Dokument eingestellt</u>	<u>xds.put</u>	<u>Ein Dokument wurde durch einen Nutzer neu eingestellt.</u>	<u>alle, außer Versicherter</u>
<u>Dokument aktualisiert</u>	<u>xds.update</u>	<u>Ein aktualisiertes Dokument wurde durch einen Nutzer eingestellt.</u>	<u>alle, außer Versicherter</u>
<u>Befugnis gelöscht</u>	<u>entitle.del</u>	<u>Eine existierende Befugnis wurde gelöscht.</u>	<u>nur Vertreter</u>
<u>Befugniserstellung im Behandlungskontext</u>	<u>entitle.ps</u>	<u>Eine Befugnis wurde mittels VSDM-Prüfnachweis, bzw. PoPP, erstellt.</u>	<u>alle, außer FdV Nutzer</u>
<u>Verbergen aufgehoben (Dokument)</u>	<u>constraint.del</u>	<u>Ein zuvor verborgenes Dokument ist wieder sichtbar.</u>	<u>nur Vertreter</u>
<u>Verbergen aufgehoben (dynamischer Ordner)</u>		<u>Ein zuvor verborgener dynamischer Ordner ist wieder sichtbar.</u>	<u>nur Vertreter</u>
<u>Verbergen aufgehoben (Kategorie)</u>		<u>Eine zuvor verborgene Kategorie wieder sichtbar.</u>	<u>nur Vertreter</u>

[<=]

3.21.4 Push Notification Nachrichteninhalte

(siehe auch: [gemF PushNotification]#Kapitel "Operation Notify")

Für jedes ausgelöste Ereignis eines Push Channels wird eine Push Notification erstellt. Die Nachrichtendaten für ein Ereignis werden strukturiert gemäß Schema angeordnet und nach den Vorgaben in [gemF PushNotification#A 27610-*] auf konstante Länge aufgefüllt.

A 27645 - Push Notification Management - Push Notification Datenstruktur

Das Push Notification Management MUSS die Nachrichtendaten einer Push Nachricht für den Versand gemäß [Schema PushNotifications] strukturieren.[<=]

Es gibt eine maximal erlaubte Größe für Nachrichteninhalte, die durch das Push Notification System [gemF PushNotification] vorgegeben wird. Es muss sichergestellt werden, dass erzeugte Nachrichteninhalte diese Größe nicht übersteigen.

A 27673 - Push Notification Management - Verkürzung der Nachrichteninhalte

Falls der erzeugte Nachrichtinhalt die maximal erlaubte Größe für Nachrichteninhalte übersteigt MUSS das Push Notification Management die Elemente actor, title, who,

folderTitle so verkürzen, dass die maximal erlaubte Größe für Nachrichteninhalte gerade nicht überschritten wird. [\leq]

Hinweis: Es müssen nicht alle aufgeführten Elemente gleichzeitig verkürzt werden.

A 27674 - Push Notification Management - Art der Verkürzung

Falls Elemente einer Nachricht verkürzt werden, dann sollen diese so verkürzt werden, dass:

- am Ende der Zeichenkette Zeichen entfernt werden
- die Verkürzung mit "..." angezeigt wird.

[\leq]

Hinweis: Es kann sinnvoll sein, nur das längste kürzbare Element zu kürzen. Es wird empfohlen eine Mindestlänge von 50 Bytes nicht zu unterschreiten.

3.21.5 Versenden von Push Nachrichten

(siehe auch: [gemF PushNotification]#Kapitel "Operation Notify" und [PushNotificationConcept]#Concept: "Verschlüsselung des Benachrichtigungsinhalts")

Eine erstellte Push Nachricht wird an jede ePA-FdV-Instanz mit einer Registrierung im Aktenkonto gesendet, wenn für diese der assoziierte Kanal abonniert wurde (Konfiguration channelId == enabled).

Die längenkorrigierte Nachricht wird jeweils mit dem für den aktuellen Monat gültigen SchlüsselAES/CGM-Schlüssel-Jahr-Monat der Registrierung für jede adressierte ePA-FdV-Instanz verschlüsselt. Das Verschlüsselungsergebnis ist der Inhalt von ciphertext der notification für den Versand ([I Push Gateway]).

A 27651 - Push Notification Management - verpflichtende Verschlüsselung der Nachrichteninhalte

Das Push Notification Management MUSS sicherstellen, dass ausschließlich verschlüsselte Nachrichteninhalte als Push Nachricht versendet werden. [\leq]

Jedes einer Push Nachricht zugrundeliegenden Ereignis erzeugt auch einen Protokolleintrag im Audit Event Service. Die Menge der korrespondierenden Protokolleinträge ergibt dadurch im Aktenkonto ein Archiv der Push Ereignisse. Damit Clients ein Push Ereignis zu einem späteren Zeitpunkt, also nachdem die Push Nachricht im Client selbst schon gelöscht ist, restaurieren können, wird jeder Push Nachricht auch der Identifier des Protokolleintrags angehängt.

A 27644 - Push Notification Management - Referenz auf Protokolleintrag

Das Push Notification Management MUSS den eindeutigen Identifier Resource.id des zu einem Push Notification Ereignis gehörenden Protokolleintrags (AuditEvent) des Aktenkontos im Feld notification/identifizier einer Push Notification angeben. [\leq]

3.21.6 Protokollierung

A 27636 - Push Notification Management- Protokollierung der ePA-FdV-Instanz-Registrierung

Das Push Notification Management MUSS für Erstellung und Änderung (CUD) von ePA-FdV-Instanz-Registrierungen jeweils einen Protokolleintrag gemäß A 24704* erzeugen. Dabei ist folgende Wertebegleitung zu berücksichtigen:

Tabelle 44: Constraint Management Protokollierung

<u>Strukturelement</u>	<u>Wert</u>		<u>Erläuterung</u>
<u>AuditEvent.type</u>	<u>"rest"</u>		<u>Bei Änderungen über die API</u>
	<u>"object"</u>		<u>Bei intern ausgelösten Änderungen (internes Löschen einer ePA-FdV-Instanz-Registrierung nach Löschen Device Registration)</u>
<u>AuditEvent.action</u>	<u>C, U, D</u>		
<u>AuditEvent.entity.name</u>	<u>"PushNotificationManagement"</u>		
<u>AuditEvent.entity.detail</u>	<u>type</u>	<u>value[x]</u>	
	<u>"DisplayNamePusher"</u>	<u><device_display_name aus der Pusher Registrierung></u>	
	<u>"DisplayNameDevice"</u>	<u><displayName der Device Registration></u>	

[<=]*Hinweis: DisplayNamePusher und DisplayNameDevice können gleich lauten.***A 27662 - Push Notification Management- Protokollierung von Änderungen der Channel Konfiguration**

Das Push Notification Management MUSS für Änderungen der Channel-Konfiguration jeweils einen Protokolleintrag gemäß A 24704* erzeugen. Dabei ist folgende Wertebegleitung zu berücksichtigen:

Tabelle 45: Constraint Management Protokollierung

<u>Strukturelement</u>	<u>Wert</u>		<u>Erläuterung</u>
<u>AuditEvent.type</u>	<u>"rest"</u>		<u>Bei Änderungen über die API</u>

<u>Strukturelement</u>	<u>Wert</u>		<u>Erläuterung</u>
	<u>"object"</u>		<u>Bei intern ausgelösten Änderungen (internes Löschen einer ePA-FdV-Instanz-Registrierung nach Löschen Device Registration)</u>
<u>AuditEvent.action</u>	<u>U</u>		
<u>AuditEvent.entity.name</u>	<u>"PushNotificationManagement"</u>		
<u>AuditEvent.entity.detail</u>	<u>type</u>	<u>value[x]</u>	
	<u>"channelId"</u>	<u><[enabled, disabled]></u>	<u>value wird auf den neuen Wert gesetzt</u>
	<u>Die Kardinalität der <channelId> <value> Paare ist 1 .. *. Für jeden geänderte Wert eines Channels ist ein Eintrag erforderlich. Erfolgt der Protokolleintrag aufgrund Löschung eines Pushers, so sind die Channels zu erfassen, die vor der Löschung den Wert enabled hatten</u>		
	<u>"DisplayNamePusher"</u>	<u><device display name aus der Pusher Registrierung></u>	
	<u>"DisplayNameDevice"</u>	<u><displayName der Device Registration></u>	

[<=]

Hinweis: Die Speicherung von Protokolleinträgen erfordert einen berechtigten Benutzer, um den Zugriff auf den sicheren Datenspeicher zu gewährleisten. Daher wird die Erstellung von Protokolleinträgen immer übersprungen und es wird kein Protokolleintrag gespeichert, wenn diese Bedingung nicht erfüllt ist.

3-193.22 Schnittstellen (OpenAPI)

Hinweis: Die Vorgaben in den beschreibenden Dateien der REST-Schnittstellen (yaml) sind normativ für den Anbieter der Schnittstellen. Die Anforderungen im vorliegenden Dokument ergänzen diese Vorgaben, insbesondere, wenn diese für sicherheitstechnische Gutachten erforderlich sind.

6999 **~~3.19.1~~3.22.1 Übersicht der Schnittstellen des Aktensystems**

7000 **Tabelle 46: Übersicht der Schnittstellen des Aktensystems**

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)
I_Consent_Decision_Management

Schnittstelle des Consent Decision Managements gemäß
[I_Consent_Decision_Management]

updateConsentDecision	Diese Operation erlaubt dem FdV und der Ombudsstelle die Änderung des Zustand des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA für eine Funktion.
getConsentDecisions	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen aller Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der ePA.
getConsentDecision	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen eines Widerspruchs einer Funktion gegen die Nutzung von widerspruchsfähigen Funktionen.
<u>updateDataUsagePurposes</u>	<u>Diese Operation erlaubt dem FdV und der Ombudsstelle die Änderung der Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden.</u>
<u>getDataUsagePurposes</u>	<u>Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht der aktuellen Entscheidungen zu den Sekundärnutzungszwecken, die an das FDZ übermittelt werden bzw. wurden.</u>
getUserSpecificMedicationDenyList	Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht, welche LEI keinen Zugriff auf den Medication Service haben.
setUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI in die Liste der LEIs aufzunehmen, die keinen Zugriff auf den Medication Service haben.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
getUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine bestimmte LEI aus der Liste der LEIs anzuzeigen, die keinen Zugriff auf den Medication Service haben.
deleteUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI aus der Liste der LEIs zu entfernen, damit diese LEI wieder Zugriff auf den Medication Service haben kann.
I_Constraint_Management_Insurant	
Schnittstelle des Constraint Managements gemäß [I_Constraint_Management_Insurant]	
getDenyPolicyAssignments	Diese Operation gibt eine Liste aller konfigurierten Einträge der General Deny Policy aus.
setPolicyAssignment	Diese Operation fügt der General Deny Policy einen neuen Eintrag hinzu.
deletePolicyAssignment	Diese Operation löscht einen bestimmten Eintrag der General Deny Policy.
I_Entitlement_Management	
Schnittstelle des Entitlement Management gemäß [I_Entitlement_Management] zur Vergabe von Befugnissen und Befugnisausschlüssen	
setEntitlementPs	Diese Operation fügt eine Befugnis für eine Leistungserbringerinstitution in einer Behandlungssituation hinzu- <u>(VSDM Prüfnachweis)</u> .
<u>setEntitlementPsV2</u>	<u>Diese Operation fügt eine Befugnis für eine Leistungserbringerinstitution in einer Behandlungssituation hinzu (PoPP).</u>
getEntitlements	Diese Operation erlaubt dem FdV den Abruf aller aktuellen Befugnisse.
getEntitlement	Diese Operation erlaubt dem FdV den Abruf einer bestimmten Befugnis.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
setEntitlement	Diese Operation erlaubt dem FdV das Setzen einer Befugnis für einen Nutzer.
deleteEntitlement	Diese Operation erlaubt dem FdV den Abruf das Löschen einer existierenden Befugnis.
getBlockedUserPolicyAssignments	Diese Operation erlaubt dem FdV den Abruf der aktuell vorhandenen Befugnisausschlüsse.
setBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Befugnisausschluss für einen Nutzer.
getBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Abruf eines bestimmten Befugnisausschlusses.
deleteBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV die Aufhebung eines Befugnisausschlusses.
I_Entitlement_Management_EU	
Schnittstelle des Entitlement Management EU-Zugriff gemäß [I_Entitlement_Management_EU] zur Verwaltung Befugnis EU-Zugriff	
setEntitlementEu	Diese Operation erlaubt dem FdV das Setzen einer Befugnis EU-Zugriff für einen Versicherten.
getAccessCode	Diese Operation erlaubt dem FdV den Abruf des Zugriffscodes für die Befugnis EU-Zugriff.
Render API: PDF Audit	
Schnittstelle des Audit Event Service gemäß [IG_Audit_Event_ServiceBasic] zum Abruf der Protokolldaten in lesbarer Form	
renderAuditEventsToPDF	Diese Operation erlaubt FdV und Ombudsstelle den Abruf der Protokolldaten als PDF.
Query API: AuditEvent	

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)

Schnittstelle des Audit Event Service gemäß [IG_~~Audit_Event_Service~~Basic] zum Abruf der Protokolldaten im FHIR-Format

listAuditEvents_AuditEventSvc	Diese Operation ermöglicht die Suche nach AuditEvent Instanzen.
-------------------------------	---

getAuditEventById_AuditEventSvc	Diese Operation ermöglicht das Lesen einer AuditEvent Instanz.
---------------------------------	--

I_Health_Record_Relocation_Service

Schnittstelle zur Steuerung des Aktenumzugs aus der Umgebung des Kostenträgers

startPackageCreation	Diese Operation initiiert die Erstellung eines Export Pakets für den Umzug eines Aktenkontos zu einem neuen Anbieter.
----------------------	---

startPackageImport	Diese Operation initiiert den Import eines Export Pakets in ein neu erstelltes Aktenkonto.
--------------------	--

I_Device_Management_Insurant

Schnittstelle zur Geräteverwaltung aus der Umgebung des Versicherten

getDevice	Diese Operation ruft eine bestimmte Geräteregistrierung ab.
-----------	---

getDevices	Diese Operation ruft alle Geräteregistrierungen ab.
------------	---

updateDevice	Diese Operation ändert den Displayname einer Geräteregistrierung.
--------------	---

deleteDevice	Diese Operation löscht eine bestimmte Geräteregistrierung.
--------------	--

registerDevice	Diese Operation erzeugt eine neue Geräteregistrierung und neue Geräteparameter
----------------	--

confirmPendingDevice	Diese Operation bestätigt eine neue Geräteregistrierung mit einem Geräteregistrierungscode
----------------------	--

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
getDeviceAttestation	Diese Operation ruft die Bestätigung einer Geräteregistrierung am Home-AS ab.
I_Authorization_Service	
Schnittstelle der Autorisierung für den Login	
getFHIRVZDtoken	Diese Operation bezieht das search-access-token für den Zugriff auf den FHIR VZD vom Aktensystem
getNonce	Diese Operation bezieht einen eindeutigen einmalig generierten Zufallswert für die Client Attestierung
sendAuthorizationRequestSC	Diese Operation initiiert die Authentifizierung eines Leistungserbringers
sendAuthorizationRequestFdV	Diese Operation initiiert die Authentifizierung eines ePA-FdV
getFreshnessParameter	Diese Operation erzeugt einen Frischeparameter für die Authentisierung mittels Bearer Token
sendAuthorizationRequestBearerToken	Diese Operation initiiert die Authentifizierung über Bearer Token
sendAuthCodeSC	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
sendAuthCodeFdV	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
logoutFdV	Diese Operation beendet aktiv die Sitzung
I_Medication_Service_eML_Render	
renderEMLAsHTML	Diese Operation gibt die Medikationsliste im html-Format zurück.
renderEMLAsPDF	Diese Operation gibt die Medikationsliste im PDF/A-Format zurück.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)
I_Medication_Service_FHIR

REST-Schnittstelle zum Abruf der Medikationsdaten im FHIR-Format

I_Email_Management

getEmailAddress	Diese Operation ruft die hinterlegte E-Mail-Adresse des Versicherten ab.
replaceEmailAddress	Diese Operation setzt oder ändert die E-Mail Adresse für einen Versicherten ab.

I_Tool_Convert_PDF_Insurant

Schnittstelle des XDS Document Managements gemäß [I_Tool_Convert_PDF_Insurant]

convertPDF	Diese Operation konvertiert ein PDF in ein PDF/A Format
------------	---

I Data Submission Service

Schnittstelle des Data Submission Service gemäß [I Data Submission Service]

<u>getSubmissionPackage</u>	<u>Diese Operation stellt dem FDZ ein Datenpaket für eine bestimmte SubmissionID bereit.</u>
-----------------------------	--

I Push Notification Management Insurant

Schnittstelle des Push Notification Managements gemäß [I Push Notification Management]

<u>getPushers</u>	<u>Diese Operation gibt alle Pusher Registrierungen eines Aktenkontos aus</u>
<u>updatePusher</u>	<u>Diese Operation setzt, aktualisiert oder löscht eine Pusher Registrierung</u>
<u>getChannelsOfPusher</u>	<u>Diese Operation gibt die aktuelle Konfiguration der Push Notification Channels für einen Pusher aus</u>
<u>updateChannelsOfPusher</u>	<u>Diese Operation aktualisiert die Auswahl der Push Notification Channels für einen Pusher</u>
<u>getChannels</u>	<u>Diese Operation gibt die möglichen Push Notification Channels der ePA aus</u>

7001

Schnittstellen des Aktensystems (Nutzung ohne VAU-Kanal)	
I_Information_Service	
Schnittstelle des Informationsdienstes gemäß [I_Information_Service]	
getConsentDecisionInformation	Diese Operation liest den aktuellen Zustand der Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der Funktionsklasse "Versorgungsprozess" aus.
setUserExperienceResult	Die Operation dient der Sammlung von Client Performedaten aus der Umgebung der Leistungserbringer.
getRecordStatus	Diese Operation fragt Existenz und Status eines bestimmten Aktenkontos bei einem Betreiber an.
I_Information_Service_Accounts	
Schnittstelle des Information Service gemäß [I_Information_Service_Accounts] für Anbieter Aktensystem im Kontext eines Aktenkontoumzugs	
getGeneralConsentDecision	Diese Operation dient der Abfrage eines Widerspruchs gegen die Nutzung der ePA bei einem anderen Aktensystemanbieter.
startRelocation	Diese Operation initiiert die Erstellung eines Export Pakets für die Relocation.
deleteExportPackage	Diese Operation schließt den Vorgang der Relocation erfolgreich ab.
postExportPackageIncident	Diese Operation erhält Benachrichtigungen zum Relocation-Prozess.
putDownloadUrlForExportPackage	Diese Operation initiiert den Import eines Export Packages.
postPackageDeliveryIncident	Diese Operation erhält Benachrichtigungen zum Relocation-Prozess.
getProviderList	Diese Operation gibt eine Liste von FQDNs der Versicherungen / ePA-Anbieter aus

7002 Die Schnittstellen (REST) und Operationen sind funktional in den Beschreibungen der
 7003 jeweiligen Schnittstelle beschrieben. Darüber hinaus gelten die folgenden übergreifenden
 7004 Anforderungen.

7005 **3.19.23.22.2 Übergreifende Festlegungen zu den Schnittstellen**7006 **A_23918 - Schnittstellen (OpenApi) - Prüfung der Befugnis**

7007 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
7008 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
7009 eine vorhandene und gültige Befugnis (entitlement) für den Nutzer der Operation fordern
7010 und diese nicht vorliegt. [\leq]

7011 *Hinweis: A_23918 deckt auch die Fehlersituationen "kein VAU-Kanal" und "keine User*
7012 *Session" ab, da diese eine Vorbedingung für den Nachweis einer gültigen Befugnis sind.*

7013 **A_24365 - Schnittstellen (OpenApi) - Prüfung des Aktenkontos**

7014 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
7015 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
7016 die Existenz des adressierten Aktenkontos fordern und diese nicht für den
7017 Operationsaufruf verwendet wird. [\leq]

7018 *Hinweis A_24365 deckt auch die Fehlersituation "kein Health Record Context" ab, da*
7019 *dieses nur infolge eines nicht vorhandenen Aktenkontos auftritt.*

7020 **A_24538 - Schnittstellen (OpenApi) - Prüfung des Aktenkontostatus**

7021 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
7022 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
7023 einen vorgegebenen Status des Aktenkontos fordern und dieser nicht vorhanden ist. [\leq]

7024 **A_24366 - Schnittstellen (OpenApi) - Prüfung der Rolle**

7025 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
7026 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
7027 die Zulässigkeit der Operation auf bestimmte Rollen (professionOID) einschränken und
7028 der Nutzer der Operation diese nicht nachweist. [\leq]

7029 **A_24367 - Schnittstellen(OpenApi) - Prüfung des Identifiers**

7030 Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen
7031 ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions)
7032 die Zulässigkeit der Operation auf bestimmte Identifier (KVNR oder Telematik-ID)
7033 einschränken und der Nutzer der Operation diese nicht nachweist. [\leq]

7034 **A_24580 - Schnittstellen (OpenApi) - Protokollierung der Operationen**

7035 Das ePA-Aktensystem MUSS nach der Ausführung der Operationen der REST-
7036 Schnittstellen eine Protokolleintrag erstellen, wenn die Protokollierung in den
7037 Nachbedingungen (Postconditions) der Operationen gefordert ist (log-entry). [\leq]

7038

4 Informationsmodelle

7039

Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten wird nicht benötigt.

7040

7041

5 Anhang A – Verzeichnisse

7042

5.1 Abkürzungen

Kürzel	Erläuterung
AdV	Anwendungen des Versicherten
<u>AN</u>	<u>Arbeitsnummer in der Übermittlung von Daten zur Sekundärnutzung</u>
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
<u>FDZ</u>	<u>Forschungsdatenzentrum Gesundheit</u>
HL7	Health Level Seven
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IHE ITI TF	IHE IT Infrastructure Technical Framework
JWT	JSON-Web-Token
JWS	signiertes JSON-Web-Token

Kürzel	Erläuterung
KTR	Kostenträger
<u>LP</u>	<u>Lieferpseudonym in der Übermittlung von Daten zur Sekundärnutzung</u>
MIO	Medizinisches Informationsobjekt
<u>MHD</u>	<u>Mobile access to Health Documents (FHIR-Service im Aktensystem u.a. für Volltextsuche)</u>
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
<u>VST</u>	<u>Vertrauensstelle Elektronische Patientenakte</u>
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	59
Abbildung 2 – Überblick Service-VAUs	94
Abbildung 3: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP ..	233
Abbildung 4: Ablauf der Authentifizierung einer LEI über den Smartcard IDP	238
Abbildung 5: Ablauf der Authentisierung des E-Rezept-Fachdienstes	239
Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls	59
Abbildung 2 - Überblick Service-VAUs	94
Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung	98
Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer Überschlüsselung	99
Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP ..	233
Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP	238
Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes	239

5.4 Tabellenverzeichnis

Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat	23
Tabelle 2: Protokollierung der Migration der medizinischen Daten	34
Tabelle 3: Protokollierung der Migration der Protokolldaten des Versicherten	35
Tabelle 4: Zustandswechsel im Lebenszyklus eines Aktenkontos	39
Tabelle 5 : Health Record Relocation Service Protokollierung	48
Tabelle 6: Tab_AS_VAU-Token_Modul_Rules-Prüfregeln VAU-Token	60
Tabelle 7: Überblick über die Regeln des Befugnisverifikations-Moduls	66

7069	Tabelle 8: Tab_AS_Entitlement_Registration_Rules—Regeln zur Registrierung von	
7070	Befugnissen.....	68
7071	Tabelle 9: Tab_AS_SDS_Key_Rules—Key Rules—Regeln zur Ableitung der	
7072	versichertenindividuellen Persistierungsschlüssel.....	79
7073	Tabelle 10: Widerspruchsfähige Funktionen der elektronischen Patientenakte	102
7074	Tabelle 11: Consent Decision Management Protokollierung—Widersprüche für Funktionen	
7075	der ePA.....	104
7076	Tabelle 12: Consent Decision Management Protokollierung—User Specific Deny Policy	
7077	Medication.....	109
7078	Tabelle 13: Inhalt einer Befugnis.....	110
7079	Tabelle 14: Befugnisse für berechnigte Nutzergruppen und Nutzer	112
7080	Tabelle 15: Befugnisse EU-Zugriff für berechnigte Nutzergruppen und Nutzer.....	114
7081	Tabelle 16: Entitlement Management Protokollierung	115
7082	Tabelle 17: Inhalt eines Blocked User Policy Eintrags	125
7083	Tabelle 18: Legal Policy	129
7084	Tabelle 19: Legal Policy—EU-Zugriff	132
7085	Tabelle 20: Beschreibung der Kategorien.....	134
7086	Tabelle 21: Constraint Management Protokollierung.....	138
7087	Tabelle 22: Inhalt eines General Deny Policy Eintrags	141
7088	Tabelle 23: Verbergen eines Medical Service	141
7089	Tabelle 24: Kennzeichnung von Optionalitäten	154
7090	Tabelle 25: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den	
7091	Außenschnittstellen des XDS Document Service	155
7092	Tabelle 26: Schnittstelle I_Document_Management	171
7093	Tabelle 27: Schnittstelle I_Document_Management_Insurant	174
7094	Tabelle 28: Schnittstelle I_Document_Management_Ncpeh.....	177
7095	Tabelle 29: Festlegung Folder.entryUUID zu statischen Ordnern	178
7096	Tabelle 30: Nutzungsvorgaben für Metadatenattribute XDS	180
7097	Tabelle 31: Tab_LanguageCodes—Mindestanforderung an zu unterstützende Language	
7098	Codes	199
7099	Tabelle 32: Einsortierung_Datenkategorien.....	205
7100	Tabelle 33: TAB_EPA_Sammlungstypen	208
7101	Tabelle 34: Auswirkungen bei Widerspruch gegen eine Funktion der ePA	211
7102	Tabelle 35: XDS Document Service Protokollierung.....	212
7103	Tabelle 36: Medication Service Protokollierung	218
7104	Tabelle 37 : Inhaltliche Definitionen eines AuditEvent	222
7105	Tabelle 38 Befüllung AuditEvent	222
7106	Tabelle 39: Audit Event Service Protokollierung.....	228

7107	<u>Tabelle 40: Übersicht der Schnittstellen des Aktensystems</u>	259
7108	<u>Tabelle 1: Tab Prüfung Signaturzertifikate Parameter Prüfung Signaturzertifikat</u>	23
7109	<u>Tabelle 2: Zustandswechsel im Lebenszyklus eines Aktenkontos</u>	39
7110	<u>Tabelle 3 : Health Record Relocation Service Protokollierung</u>	48
7111	<u>Tabelle 4: Tab AS VAU Token Modul Rules -Prüfregeln VAU Token</u>	60
7112	<u>Tabelle 5: Überblick über die Regeln des Befugnisverifikations-Moduls</u>	66
7113	<u>Tabelle 6: Tab AS Entitlement Registration Rules - Regeln zur Registrierung von</u>	
7114	<u>Befugnissen</u>	68
7115	<u>Tabelle 7: Tab AS SDS-Key Rules Key Rules - Regeln zur Ableitung der</u>	
7116	<u>versichertenindividuellen Persistierungsschlüssel</u>	79
7117	<u>Tabelle 8: Widerspruchsfähige Funktionen der elektronischen Patientenakte</u>	102
7118	<u>Tabelle 9: Consent Decision Management Protokollierung - Widersprüche für Funktionen</u>	
7119	<u>der ePA</u>	104
7120	<u>Tabelle 10: Consent Decision Management Protokollierung - Widersprüche zu</u>	
7121	<u>Sekundärnutzungszwecken</u>	107
7122	<u>Tabelle 11: Consent Decision Management Protokollierung - User Specific Deny Policy</u>	
7123	<u>Medication</u>	109
7124	<u>Tabelle 12: Inhalt einer Befugnis</u>	110
7125	<u>Tabelle 13: Befugnisse für berechtigte Nutzergruppen und Nutzer</u>	112
7126	<u>Tabelle 14: Befugnisse EU-Zugriff für berechtigte Nutzergruppen und Nutzer</u>	114
7127	<u>Tabelle 15: Entitlement Management Protokollierung</u>	115
7128	<u>Tabelle 16: Inhalt eines Blocked User Policy Eintrags</u>	125
7129	<u>Tabelle 17: Legal Policy</u>	129
7130	<u>Tabelle 18: Legal Policy - EU-Zugriff</u>	132
7131	<u>Tabelle 19: Beschreibung der Kategorien</u>	134
7132	<u>Tabelle 20: Constraint Management Protokollierung</u>	138
7133	<u>Tabelle 21: Inhalt eines General Deny Policy Eintrags</u>	141
7134	<u>Tabelle 22: Verbergen eines Medical Service</u>	141
7135	<u>Tabelle 23: Kennzeichnung von Optionalitäten</u>	154
7136	<u>Tabelle 24: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den</u>	
7137	<u>Außenschnittstellen des XDS Document Service</u>	155
7138	<u>Tabelle 25: Schnittstelle I Document Management</u>	171
7139	<u>Tabelle 26: Schnittstelle I Document Management Insurant</u>	174
7140	<u>Tabelle 27: Schnittstelle I Document Management Ncpeh</u>	177
7141	<u>Tabelle 28: Festlegung Folder.entryUUID zu statischen Ordnern</u>	178
7142	<u>Tabelle 29: Nutzungsvorgaben für Metadatenattribute XDS</u>	180
7143	<u>Tabelle 30: Tab LanguageCodes - Mindestanforderung an zu unterstützende Language</u>	
7144	<u>Codes</u>	199
7145	<u>Tabelle 31: Einsortierung Datenkategorien</u>	205

7146	<u>Tabelle 32: TAB EPA Sammlungstypen</u>	208
7147	<u>Tabelle 33: Auswirkungen bei Widerspruch gegen eine Funktion der ePA</u>	211
7148	<u>Tabelle 34: XDS Document Service Protokollierung</u>	212
7149	<u>Tabelle 35: Patient Service Protokollierung</u>	216
7150	<u>Tabelle 36: Medication Service Protokollierung</u>	218
7151	<u>Tabelle 37: MHD Service Protokollierung</u>	221
7152	<u>Tabelle 38 : Inhaltliche Definitionen eines AuditEvent</u>	222
7153	<u>Tabelle 39 Befüllung AuditEvent</u>	222
7154	<u>Tabelle 40 Audit Event Management Protokollierung - Fehler</u>	227
7155	<u>Tabelle 41: Audit Event Service Protokollierung</u>	228
7156	<u>Tabelle 42: Auswahl der zu übertragenden FHIR-Ressourcen</u>	249
7157	<u>Tabelle 43: Zusätzliche FHIR-Ressourcen, ermittelt über Referenzen</u>	249
7158	<u>Tabelle 44: Constraint Management Protokollierung</u>	257
7159	<u>Tabelle 45: Constraint Management Protokollierung</u>	257
7160	<u>Tabelle 46: Übersicht der Schnittstellen des Aktensystems</u>	259
7161		

7162 5.5 Referenzierte Dokumente

7163 5.5.1 Dokumente der gematik

7164 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
7165 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

[Quelle]	Herausgeber: Titel
[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: https://github.com/gematik/ePA-XDS-Document Path: src/implementation_guides
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory
[gemTerminology]	gematik: Implementation Guide gematik Terminology https://gemspec.gematik.de/fhir/ig/terminology/1.0.5/index.html
[I_Consent_Decision_Management]	gematik: I_Consent_Decision_Management REST-Schnittstelle zum Management der Widersprüche zu Versorgungsprozessen GitHub: https://github.com/gematik/ePA-Basic 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: https://github.com/gematik/ePA-Basic https://github.com/gematik/ePA-XDS-Document Path: src/openapi/I_Constraint_Management_Insurant.yaml
[I_Entitlement_Management]	gematik: I_Entitlement_Management REST-Schnittstelle zur Verwaltung von Befugnissen und Befugnisausschlüssen GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Entitlement_Management.yaml

[I_Entitlement_Management_EU]	gematik: I_Entitlement_Management_EU REST-Schnittstelle zur Verwaltung von Befugnissen EU-Zugriff GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Entitlement_Management_EU.yaml
[I_Device_Management_Insurant]	gematik: I_Device_Management_Insurant.yaml REST-Schnittstelle zur Geräteverwaltung GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Device_Management_Insurant.yaml
[I_Health_Record_Relocation_Service]	gematik: I_Health_Record_Relocation_Service REST-Schnittstelle zum Aktenumzug GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Health_Record_Relocation_Service. yaml
[I_Information_Service_Accounts]	Schnittstellenspezifikation Information Service für Betreiber GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Information_Service_Accounts.yaml
[I_Information_Service]	Schnittstellenspezifikation Information Service GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Information_Service.yaml
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung und impliziten Geräteregistrierung GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Authorization_Service.yaml
[IG_Audit_Event_Service]	gematik: Implementation Guide ePA Audit Event Service https://gemspec.gematik.de/fhir/ig/epa-audit/1.0.5/index.html
[I_Email_Management]	gematik: I_Email_Management REST-Schnittstelle zum Management von E-Mail-Adressen eines Versicherten GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Email_Management.yaml

[I_Tool_Convert_PDF_Insurant]	gematik: I_Tool_Convert_PDF_Insurant Schnittstelle für die PDF Formatkonvertierung GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/openapi/ I_Tool_Convert_PDF_Insurant.yaml
[XDSDocumentService]	gematik: XDSDocumentService.wsdl IHE-Schnittstelle des XDSDocumentService GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/schema
[HealthRecordMigration]	gematik: ref-ePA-HealthRecordMigration Referenzimplementierung und Vorgaben für das Exportpaket bei einem Anbieterwechsel GitHub: https://github.com/gematik/ref-ePA-HealthRecordMigration Branch: ePA-3.1
<u>[IG_Basic]</u>	<u>gematik: FHIR Implementation Guide "ePA Basisfunktionalitäten"</u> <u>gemSpecPages: https://gemspec.gematik.de/fhir/ig/epa/1.1.5/index.html</u>
[IG_Medication_Service]	gematik: <u>FHIR Implementation Guide "ePA Medication Service"</u> <u>https://gemspec.gematik.de/fhir/ig/epa-medication/1.0.5/index.html</u> <u>gemSpecPages: https://gemspec.gematik.de/fhir/ig/epa-medication/1.1.5/index.html</u>
<u>[IG_MHD_Service]</u>	<u>gematik: FHIR Implementation Guide "ePA MHD Service"</u> <u>gemSpecPages: https://gemspec.gematik.de/fhir/ig/epa-mhd/1.0.0/index.html</u>
<u>[IG_TI_Terminology]</u>	<u>gematik: Implementation Guide "TI Terminology"</u> <u>gemSpecPages: https://simplifier.net/packages/de.gematik.terminology/1.0.6</u>
<u>[DataPseudonymization]</u>	<u>gematik: epa-research</u> <u>Vorgaben zur Pseudonymisierung von Daten zur Sekundärnutzung</u> <u>GitHub: https://github.com/gematik/epa-research</u> <u>Path: docs/leitfaden_pseudonymisierung.md</u> <u>Branch: ePA-3.1</u>
<u>[I_Data_Submission_Service]</u>	<u>gematik: I Data Submission Service</u> <u>Schnittstelle für den Abruf eines Datenpaketes FDZ</u> <u>GitHub: https://github.com/gematik/ePA-Basic</u> <u>Path: src/openapi/ I_Data_Submission_Service.yaml</u>

<u>[I Push Notification Management]</u>	<u>gematik: I Push Notification Management Insurant REST-Schnittstelle zum Management des Benachrichtigungsdienstes der ePA</u> <u>GitHub: https://github.com/gematik/ePA-Basic</u> <u>Path: src/openapi/I Push Notification Management Insurant.yaml</u>
<u>[gemF PushNotification]</u>	<u>gematik: Anwendungsübergreifende Push Notification</u>
<u>[PushNotificationConcept]</u>	<u>gematik: Push Notification Concept Repository mit Artefakten und Vorgaben für anwendungsübergreifende Push Notification</u> <u>GitHub: https://github.com/gematik/gem-push-notifications-concept und https://gematik.github.io/gem-push-notifications-concept/</u>
<u>[I Push Gateway]</u>	<u>gematik: Push Gateway API REST-Schnittstelle des Push Gateways zum Versand von Push Nachrichten</u> <u>GitHub: https://github.com/gematik/gem-push-notifications-concept</u> <u>Path: docs/sources/push_gateway_openapi.yaml</u>
<u>[Schema PushNotifications]</u>	<u>gematik: PushNotificationSchema Strukturvorgaben für Nachrichteninhalte des Push Notification Managements</u> <u>GitHub: https://github.com/gematik/ePA-Basic</u> <u>Path: src/schema/PushNotificationSchema.yaml</u>

5.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-RMD]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.6 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-RMU]	IHE International (2021): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.3 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-TF1]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Profile definition, use-case analysis, actor definition, and use of transactions and content, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume1/
[IHE-ITI-TF2]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume2/
[IHE-ITI-TF3]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Document Sharing Metadata and Content Profiles, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume3/
[I_VST]	Vertrauensstelle ePA – Pseudonymisierungskonzept Datenausleitung ePA zu Forschungszwecken Version 2.0 (12.07.2024), Herausgeber: Robert Koch-Institut, Nordufer 20,13353 Berlin
[MIO-UH]	Kassenärztliche Bundesvereinigung (2022): Kinderuntersuchungsheft, https://mio.kbv.de/display/UH1X0X1
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://datatracker.ietf.org/doc/html/rfc2119
[RFC3339]	IETF (2002): Date and Time on the Internet: Timestamps, RFC 3339, https://datatracker.ietf.org/doc/html/rfc3339
[RFC4122]	IETF (2005) A Universally Unique IDentifier (UUID) URN Namespace, RFC 4122 https://datatracker.ietf.org/doc/html/rfc4122
[RFC5246]	IETF (2008): The Transport Layer Security (TLS) Protocol Version 1.2 https://datatracker.ietf.org/doc/html/rfc5246
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231, https://datatracker.ietf.org/doc/html/rfc7231

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC7515]	IETF (2015): JSON Web Signature (JWS), RFC-7515 https://datatracker.ietf.org/doc/html/rfc7515
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), https://www.w3.org/TR/soap12-part1/
[WSA]	OASIS (2004): Web Services Addressing (WS-Addressing), https://www.w3.org/Submission/ws-addressing/
[WSIAP]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[WSIBSP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html
[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/
[XHTML]	W3C (2010): XHTML 1.1 - Module-based XHTML - Second Edition, https://www.w3.org/TR/xhtml1/

6 Anhang B – Erläuternde Informationen

Dieser Anhang enthält nicht normative Informationen, die dazu dienen, das Verständnis der Spezifikation zu vereinfachen.

6.1 Dokumentenanhänge

Der vorliegende Abschnitt enthält einige Abbildungen, die das Konzept der Dokumentenanhänge in der ePA für alle visuell erläutern und damit leichter verständlich machen sollen.

6.2 Überblick

Die folgende Abbildung zeigt fünf Dokumente (bzw. DocumentEntries), die teilweise über Anhangsbeziehungen miteinander verbunden sind:



zu einige Hinweise:

- Dokument #1
 - besitzt zwei Anhänge (Dokumente #2 und #4)
 - ist selbst an kein Dokument angehängt.
- Dokument #2
 - besitzt einen Anhang (Dokument #3).
- Dokument #3
 - besitzt keine Anhänge.
 - ist selbst an Dokument #2 angehängt.
- Dokument #4
 - besitzt keine Anhänge.
 - ist selbst an zwei Dokumente angehängt (Dokumente #1 und #5)
- Dokument #5
 - besitzt einen Anhang (Dokument #4).

Notation

Jedes Dokument verweist auf Dokumentenanhänge über einen Eintrag in seiner `referenceIdList` (`<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2025:childDocument`), wobei `DocumentEntry.uniqueId` sich auf die eindeutige Kennung des Anhangsdokuments bezieht. In der Spezifikation wird der Anhang manchmal als Kinddokument bezeichnet, und das Dokument, an dem es hängt als Elterndokument. In diesem Sinne ist Dokument #3 bspw. das Kinddokument von Dokument #2.

Anzahl Anhänge

Wie aus der Abbildung hervorgeht, kann ein Dokument mehrere Anhänge besitzen; im Beispiel verfügt Dokument über zwei Anhänge. Umgekehrt kann auch jeder Anhang an mehr als einem Dokument hängen (im Beispiel ist Dokument #4 Anhang sowohl für Dokument #1 also auch Dokument #5).

Die Beziehung zwischen Eltern- und Kinddokumenten ist also m:n: Ein Dokument kann beliebig viele Anhänge besitzen und ein Anhang kann an beliebig vielen Dokumenten anhängen.

6.3 Löschen und Verbergen in Anhangsketten

Der Abschnitt illustriert Szenarien, bei denen ein Dokument in der Anhangskette gelöscht wird. Der Fall des Verbergens von Dokumenten (z. B. als Ergebnis des Verbergens einer Kategorie) verläuft analog.

Szenario vor dem Bearbeiten der Löschanfragen von Dokument #2 im Aktenkonto:

I am sorry... This image is not accessible.
Attach a PNG with the same name to the
document so it is visible in exported files.



- Das Aktenkonto befindet sich vor der Löschanfrage in einem konsistenten Zustand (6 Dokumente, untereinander über Anhangbeziehungen verbunden).
- Die Löschanfrage beabsichtigt nun, ein einzelnes Dokument (#2) aus der Mitte einer Anhangskette zu löschen

Szenario nach dem Bearbeiten der Löschanfragen von Dokument #2 im Aktenkonto:



- Beim Löschen arbeitet sich das Aktensystem von Dokument #2 aus die Eltern- und Kindkette entlang.
- Es wird jedes Elterndokument (analog: Kinddokument) gelöscht, das nicht noch andere Kinddokumente (analog: Elterndokument) außerhalb der Kette zu Dokument #2 besitzt.
- Dokument #3 (Kinddokument) besitzt kein weiteres Elterndokument, wird also gelöscht.
- Dokument #4 (Kinddokument) besitzt noch ein weiteres Elterndokument, wird also nicht gelöscht.
- Dokument #1 (Elterndokument) besitzt kein weiteres Kinddokument, wird also gelöscht.
- Dokument #5 (Elterndokument) besitzt kein weiteres Kinddokument, wird also gelöscht.
- Dokument #4 bleibt, das zwar als Kind mit Dokument #2 verbunden war, jedoch mit Dokument #6 noch ein weiteres Elterndokument besitzt, das nicht Teil der Kette zu Dokument #2 ist. Die Referenz von Dokument #4 auf Dokument #2 wurde ebenfalls aus der referenceIdList gelöscht.
- Dokument #6 ist nicht Teil der Eltern- und Kindkette von Dokument #2, verbleibt also im Aktenkonto.

6.4 Ungültige Anhänge

Dieser Abschnitt illustriert einige nicht erlaubte Anhangsszenarien.

6.4.1 Verweiszirkel und doppelte Eltern

Die folgende Abbildung demonstriert Anhänge, wie sie nicht in den XDS Document Service eingebracht werden können:



- Ausgangssituation (unproblematisch):
 - Dokument #3 ist Anhang zu Dokument #2.
 - Dokument #2 ist Anhang zu Dokument #1.
- Falls nun anschließend versucht wird, Dokument #3 als Kind von Dokument #1 einzutragen (roter Pfeil auf der linken Seite), ist dies nicht erlaubt, da ein Dokument nicht Anhang zu zweien seiner "Vorfahren" in der Anhangskette sein darf (denn Dokument #3 ist bereits Anhang von Dokument #2, das wiederum an Dokument #1 hängt).
- Auch der Versuch, Dokument #1 als Anhang zu Dokument #3 zu markieren schlägt fehl, denn es würde ein Verweiszirkel entstehen, in dem ein Kinddokument gleichzeitig Elterndokument für eines seiner Vorfahren ist.

6.4.2 Anhangskette zu lang

Die maximale Länge der Anhangsketten ist auf fünf beschränkt. Die folgende Abbildung zeigt, in welchem Fall das Hinzufügen eines weiteren Anhangs zu Problemen führt (und wann nicht):



- Ausgangssituation (Dokumente #1-#5) unproblematisch. Länge der Anhangskette ist fünf.
- Wenn versucht wird, Dokument #6 einzufügen, ist die Anhangskette zu lang.
 - Das würde auch gelten, wenn der Einstellende bspw. Dokumente #1 und #2 gar nicht sehen könnte (Legal Policy, Verbergen)
 - Es würde ein Fehler zurückgegeben.
- Das Einstellen von Dokument #7 wäre unproblematisch.

7285
7286
7287
7288
7289

- Die Anhangskette von Dokument #7 hätte fünf Dokumente, Dokument #6 gehört also nicht mit dazu.
- Das Dokument könnte auf diese Weise als Anhang an Dokument #4 eingestellt werden.