

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation ePA- Dokumentenverwaltung

Version: 1.67.0 CC
Revision: 294776304772
Stand: 09.12.11.2020
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich Entwurf
Referenzierung: gemSpec_Dokumentenverwaltung

Dokumentinformationen

Änderungen zur Vorversion

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

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	18.12.18		freigegeben	gematik
1.1.0	15.05.19		<p>Einarbeitung Änderungsliste P18.1, Afos aus Kapitel 4 wurden in die zugehörigen Umsetzungsabschnitte in 5.1 verschoben, da sie keinen übergreifenden Charakter haben. Dazu zählen:</p> <p>A_14588 von ehemals 4.2.3.1 -> 5.1.2.2.1 A_13585 von ehemals 4.2.3.3 -> 5.1.1.2.1 A_14585 von ehemals 4.2.3.4 -> 5.1.1.4.1 A_14589 von ehemals 4.2.3.7 -> 5.1.2.4.1 A_13657 von ehemals 4.2.3.7 -> 5.1.1.1.1 A_14052 von ehemals 4.2.3.7 -> 5.1.1.1.1 A_13656 von ehemals 4.2.3.7 -> 5.1.1.1.1 A_15080 von ehemals 4.2.3.10 -> 5.1.1.5.1</p> <p>Umgekehrt wurden übergreifende Afos nach Kapitel 4 verschoben und Afo-Duplikate storniert</p> <p>A_14926 von 5.1.2.3.1 -> 4.2.3.4 A_15162 von 5.1.2.1.1 -> 4.2.3.3 A_14937 von 5.1.2.1.1 -> 4.2.3.3 A_14938 von 5.1.2.1.1 -> 4.2.3.3</p>	gematik
1.2.0	28.06.19		Einarbeitung Änderungsliste P19.1	gematik
1.3.0	02.10.19		Einarbeitung Änderungsliste P20.1/2	gematik
1.4.0	02.03.20		Einarbeitung Änderungsliste P21.1	gematik

1.4.1	26.06.20		Einarbeitung Änderungsliste P21.3	gematik
1.5.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
1.6.0	12. 11 <u>10</u> .20		Einarbeitung der Scope-Themen aus R4.0.1, PDSG-Änderungen	gematik
<u>1.7.0</u> <u>CC</u>	<u>09.12.20</u>		<u>Einarbeitung Änderungsliste P22.5</u>	<u>gematik</u>

31

Inhaltsverzeichnis

32	1 Einführung	13
33	1.1 Zielsetzung	13
34	1.2 Zielgruppe	13
35	1.3 Geltungsbereich	13
36	1.4 Abgrenzungen	13
37	1.5 Methodik	14
38	2 Systemkontext	15
39	3 Zerlegung der Komponente	16
40	4 Übergreifende Festlegungen	18
41	4.1 Namensräume	18
42	4.2 Nutzung von IHE IT Infrastructure Profilen für Speicherung und Abruf von	
43	Dokumenten	19
44	4.2.1 Anforderungen an IHE ITI-Akteure	19
45	4.2.1.1 APPC Content Consumer	21
46	4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren	21
47	4.2.1.1.2 Optionen des IHE ITI-Akteurs	21
48	4.2.1.2 RMU Update Responder	22
49	4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren	22
50	4.2.1.2.2 Optionen des IHE ITI-Akteurs	22
51	4.2.1.3 XCA Responding Gateway	23
52	4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
53	4.2.1.3.2 Optionen des IHE ITI-Akteurs	23
54	4.2.1.4 XCDR Responding Gateway	23
55	4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
56	4.2.1.4.2 Optionen des IHE ITI-Akteurs	24
57	4.2.1.5 XDS Document Registry	24
58	4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren	24
59	4.2.1.5.2 Optionen des IHE ITI-Akteurs	24
60	4.2.1.6 XDS Document Repository	25
61	4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren	25
62	4.2.1.6.2 Optionen des IHE ITI-Akteurs	25
63	4.2.1.7 XUA X-Service Provider	25
64	4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren	25
65	4.2.1.7.2 Optionen des IHE ITI-Akteurs	25
66	4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen	26
67	4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen	30

68	4.2.3.1 Provide X-User Assertion [ITI-40].....	30
69	4.2.3.2 Provide and Register Document Set-b [ITI-41].....	31
70	4.2.3.3 Remove Metadata [ITI-62].....	32
71	4.3 Fehlerbehandlung in Schnittstellenoperationen	33
72	4.4 Vertrauenswürdige Ausführungsumgebung	34
73	4.4.1 Verarbeitungskontext	34
74	4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	35
75	4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes	37
76	4.4.4 Parallele Zugriffe.....	38
77	4.4.5 Konsistenz der Akte, Logging und Monitoring.....	38
78	4.4.6 Client-Verbindungen zum Verarbeitungskontext.....	38
79	4.5 Anforderungen zur sicherheitstechnischen Validierung	40
80	4.6 Protokollierung.....	42
81	4.6.1 Protokollierung von Berechtigungen	49
82	5 Funktionsmerkmale	54
83	5.1 Dokumentenverwaltung	54
84	5.1.1 Schnittstelle I_Document_Management	54
85	5.1.1.1 Operation I_Document_Management::CrossGatewayDocumentProvide ...	55
86	5.1.1.1.1 Umsetzung	56
87	5.1.1.2 Operation I_Document_Management::CrossGatewayQuery	58
88	5.1.1.2.1 Umsetzung	59
89	5.1.1.3 Operation I_Document_Management::RemoveMetadata	62
90	5.1.1.3.1 Umsetzung	63
91	5.1.1.4 Operation I_Document_Management::CrossGatewayRetrieve	64
92	5.1.1.4.1 Umsetzung	65
93	5.1.2 Schnittstelle I_Document_Management_Insurant.....	68
94	5.1.2.1 Operation	
95	I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b.....	69
96	5.1.2.1.1 Umsetzung	71
97	5.1.2.2 Operation I_Document_Management_Insurant::RegistryStoredQuery.....	71
98	5.1.2.2.1 Umsetzung	73
99	5.1.2.3 Operation I_Document_Management_Insurant::RemoveMetadata.....	76
100	5.1.2.3.1 Umsetzung	77
101	5.1.2.4 Operation I_Document_Management_Insurant::RetrieveDocumentSet ...	77
102	5.1.2.4.1 Umsetzung	79
103	5.1.2.5 Operation	
104	I_Document_Management_Insurant::RestrictedUpdateDocumentSet.....	79
105	5.1.2.5.1 Umsetzung	81
106	5.1.3 Schnittstelle I_Document_Management_Insurance.....	82
107	5.1.3.1 Operation	
108	I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b	83
109	5.1.3.1.1 Umsetzung	85
110	5.1.4 Anforderungen an Sammlungstypen	85
111	5.2 Aktenkontoverwaltung	86
112	5.2.1 Schnittstelle I_Account_Management_Insurant.....	86

113	5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount.....	87
114	5.2.1.1.1 Umsetzung.....	88
115	5.2.1.2 Operation I_Account_Management_Insurant::ResumeAccount.....	90
116	5.2.1.2.1 Umsetzung.....	91
117	5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents.....	93
118	5.2.1.3.1 Umsetzung.....	94
119	5.3 Umschlüsselung.....	96
120	5.3.1 Übergreifende Anforderungen.....	97
121	5.3.2 Schnittstelle I_Key_Management_Insurant.....	102
122	5.3.2.1 I_Key_Management_Insurant::StartKeyChange().....	102
123	5.3.2.1.1 Umsetzung.....	104
124	5.3.2.2 I_Key_Management_Insurant::GetAllDocumentKeys().....	105
125	5.3.2.2.1 Umsetzung.....	106
126	5.3.2.3 Operation I_Key_Management_Insurant::PutAllDocumentKeys().....	107
127	5.3.2.3.1 Umsetzung.....	109
128	5.3.2.4 Operation I_Key_Management_Insurant::FinishKeyChange().....	109
129	5.3.2.4.1 Umsetzung.....	111
130	5.3.2.5 Protokollierung.....	111
131	5.4 Zugriffskontrolle.....	113
132	5.4.1 Grob-, mittel- und feingranulare Berechtigungen.....	113
133	5.4.2 Berufsgruppenspezifische Einschränkungen.....	114
134	5.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln.....	114
135	5.4.4 Vergabe von Zugriffsregeln.....	115
136	5.4.5 Funktionsprinzip Policy Administration.....	115
137	5.4.6 Anforderungen an die Zugriffskontrollprüfung.....	119
138	5.4.6.1 Erstmaliges Öffnen eines Verarbeitungskontextes.....	125
139	5.4.6.2 Berechtigung für einen Versicherten.....	125
140	5.4.6.3 Berechtigung für einen Vertreter.....	126
141	5.4.6.4 Berechtigung für eine Leistungserbringerinstitution.....	127
142	5.4.6.5 Berechtigung für einen Kostenträger.....	127
143	5.4.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4.....	127
144	5.5 Vertrauenswürdige Ausführung.....	129
145	5.5.1 Schnittstelle I_Document_Management_Connect.....	129
146	5.5.1.1 Operation I_Document_Management_Connect::OpenContext.....	134
147	5.5.1.1.1 Umsetzung.....	135
148	5.5.1.2 Operation I_Document_Management_Connect::CloseContext.....	136
149	5.5.1.2.1 Umsetzung.....	137
150	5.5.2 Hardware-Merkmale.....	138
151	5.6 Statische Akteninhalte.....	138
152	6 Informationsmodelle.....	139
153	7 Anhang A Verzeichnisse.....	140
154	7.1 Abkürzungen.....	140
155	7.2 Glossar.....	142
156	7.3 Abbildungsverzeichnis.....	142

157	7.4 Tabellenverzeichnis	142
158	7.5 Referenzierte Dokumente	146
159	7.5.1 Dokumente der gematik	146
160	7.5.2 Weitere Dokumente	147
161	8 Anhang B XACML 2.0 Profile für Policy Documents (für	
162	Upgrade von ePA 3.1.3)	150
163	8.1 Policy Document für einen Versicherten	150
164	8.1.1 Base Policy	150
165	8.1.2 Permission Policy	153
166	8.2 Policy Document für einen Vertreter	184
167	8.2.1 Base Policy	184
168	8.2.2 Permission Policy	188
169	8.3 Policy Document für eine Leistungserbringereinstitution	216
170	8.3.1 Base Policy zum Zugriff auf Leistungserbringer Dokumente	216
171	8.3.2 Permission Policy zum Zugriff auf Leistungserbringer Dokumente	221
172	8.3.3 Permission Policy zum Zugriff auf Versicherten und Kostenträger Dokumente	
173		247
174	8.4 Policy Document für einen Kostenträger	271
175	8.4.1 Base Policy	271
176	8.4.2 Permission Policy	274
177	9 Anhang C XACML 2.0 Profile für Policy Documents	278
178	9.1 Policy Document für einen Versicherten	278
179	9.2 Policy Document für einen Vertreter	281
180	9.3 Policy Document für eine Leistungserbringereinstitution	284
181	9.4 Policy Document für einen Kostenträger	306
182	9.5 Statische Permission Policies	311
183	9.5.1 Grobgranulare Berechtigung: Stufe Normal	311
184	9.5.2 Grobgranulare Berechtigung: Stufe Erweitert	312
185	9.5.3 Mittelgranulare Berechtigung: Kategorie "care"	312
186	9.5.4 Mittelgranulare Berechtigung: Kategorie "childsrecord"	313
187	9.5.5 Mittelgranulare Berechtigung: Kategorie "dentalrecord"	313
188	9.5.6 Mittelgranulare Berechtigung: Kategorie "eab"	314
189	9.5.7 Mittelgranulare Berechtigung: Kategorie "eau"	315
190	9.5.8 Mittelgranulare Berechtigung: Kategorie "ega"	315
191	9.5.9 Mittelgranulare Berechtigung: Kategorie "emp"	316
192	9.5.10 Mittelgranulare Berechtigung: Kategorie "mothersrecord"	316
193	9.5.11 Mittelgranulare Berechtigung: Kategorie "nfd"	317
194	9.5.12 Mittelgranulare Berechtigung: Kategorie "other"	318
195	9.5.13 Mittelgranulare Berechtigung: Kategorie "patientdoc"	319
196	9.5.14 Mittelgranulare Berechtigung: Kategorie "prescription"	320
197	9.5.15 Mittelgranulare Berechtigung: Kategorie "receipt"	320
198	9.5.16 Mittelgranulare Berechtigung: Kategorie "vaccination"	321
199	9.5.17 Mittelgranulare Berechtigung: Kategorie "practitioner"	322
200	9.5.18 Mittelgranulare Berechtigung: Kategorie "hospital"	322
201	9.5.19 Mittelgranulare Berechtigung: Kategorie "laboratory"	323
202	9.5.20 Mittelgranulare Berechtigung: Kategorie "physiotherapy"	324
203	9.5.21 Mittelgranulare Berechtigung: Kategorie "psychotherapy"	324

204	9.5.22 Mittelgranulare Berechtigung: Kategorie "dermatology"	325
205	9.5.23 Mittelgranulare Berechtigung: Kategorie "gynaecology_urology"	325
206	9.5.24 Mittelgranulare Berechtigung: Kategorie "dentistry_oms"	326
207	9.5.25 Mittelgranulare Berechtigung: Kategorie "other_medical"	327
208	9.5.26 Mittelgranulare Berechtigung: Kategorie "other_non_medical"	327
209	1 Einführung	13
210	1.1 Zielsetzung	13
211	1.2 Zielgruppe	13
212	1.3 Geltungsbereich	13
213	1.4 Abgrenzungen	13
214	1.5 Methodik	14
215	2 Systemkontext.....	15
216	3 Zerlegung der Komponente.....	16
217	4 Übergreifende Festlegungen	18
218	4.1 Namensräume	18
219	4.2 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von	
220	Dokumenten.....	19
221	4.2.1 Anforderungen an IHE ITI-Akteure	19
222	4.2.1.1 APPC Content Consumer	21
223	4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren	21
224	4.2.1.1.2 Optionen des IHE ITI-Akteurs	21
225	4.2.1.2 RMU Update Responder.....	22
226	4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren	22
227	4.2.1.2.2 Optionen des IHE ITI-Akteurs	22
228	4.2.1.3 XCA Responding Gateway.....	23
229	4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
230	4.2.1.3.2 Optionen des IHE ITI-Akteurs	23
231	4.2.1.4 XCDR Responding Gateway	23
232	4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
233	4.2.1.4.2 Optionen des IHE ITI-Akteurs	24
234	4.2.1.5 XDS Document Registry	24
235	4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren	24
236	4.2.1.5.2 Optionen des IHE ITI-Akteurs	24
237	4.2.1.6 XDS Document Repository.....	25
238	4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren	25
239	4.2.1.6.2 Optionen des IHE ITI-Akteurs	25
240	4.2.1.7 XUA X-Service Provider	25
241	4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren	25
242	4.2.1.7.2 Optionen des IHE ITI-Akteurs	25

243	4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen.....	26
244	4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen	30
245	4.2.3.1 Provide X-User Assertion [ITI-40].....	30
246	4.2.3.2 Provide and Register Document Set-b [ITI-41].....	31
247	4.2.3.3 Remove Documents [ITI-86]	32
248	4.2.3.4 Remove Metadata [ITI-62]	32
249	4.3 Fehlerbehandlung in Schnittstellenoperationen	33
250	4.4 Vertrauenswürdige Ausführungsumgebung	34
251	4.4.1 Verarbeitungskontext	34
252	4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	35
253	4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes	37
254	4.4.4 Parallele Zugriffe.....	38
255	4.4.5 Konsistenz der Akte, Logging und Monitoring.....	38
256	4.4.6 Client-Verbindungen zum Verarbeitungskontext.....	38
257	4.5 Anforderungen zur sicherheitstechnischen Validierung.....	40
258	4.6 Protokollierung.....	42
259	4.6.1 Protokollierung von Berechtigungen	49
260	5 Funktionsmerkmale	54
261	5.1 Dokumentenverwaltung	54
262	5.1.1 Schnittstelle I Document Management	54
263	5.1.1.1 Operation I Document Management::CrossGatewayDocumentProvide ...	55
264	5.1.1.1.1 Umsetzung	56
265	5.1.1.2 Operation I Document Management::CrossGatewayQuery	58
266	5.1.1.2.1 Umsetzung	59
267	5.1.1.3 Operation I Document Management::RemoveDocuments (abgekündigt) ..	61
268	5.1.1.3.1 Umsetzung	62
269	5.1.1.4 Operation I Document Management::RemoveMetadata	62
270	5.1.1.4.1 Umsetzung	63
271	5.1.1.5 Operation I Document Management::CrossGatewayRetrieve	64
272	5.1.1.5.1 Umsetzung	65
273	5.1.1.6 Operation I Document Management::RestrictedUpdateDocumentSet.....	66
274	5.1.1.6.1 Umsetzung	68
275	5.1.2 Schnittstelle I Document Management Insurant.....	68
276	5.1.2.1 Operation	
277	I Document Management Insurant::ProvideAndRegisterDocumentSet-b.....	69
278	5.1.2.1.1 Umsetzung	71
279	5.1.2.2 Operation I Document Management Insurant::RegistryStoredQuery.....	71
280	5.1.2.2.1 Umsetzung	73
281	5.1.2.3 Operation I Document Management Insurant::RemoveMetadata.....	76
282	5.1.2.3.1 Umsetzung	77
283	5.1.2.4 Operation I Document Management Insurant::RetrieveDocumentSet ...	77
284	5.1.2.4.1 Umsetzung	79
285	5.1.2.5 Operation	
286	I Document Management Insurant::RestrictedUpdateDocumentSet.....	79
287	5.1.2.5.1 Umsetzung	81

288	5.1.3 Schnittstelle I Document Management Insurance.....	82
289	5.1.3.1 Operation	
290	I Document Management Insurance::ProvideAndRegisterDocumentSet-b	83
291	5.1.3.1.1 Umsetzung	85
292	5.1.4 Anforderungen an Sammlungstypen	85
293	5.2 Aktenkontoverwaltung	86
294	5.2.1 Schnittstelle I Account Management Insurant.....	86
295	5.2.1.1 Operation I Account Management Insurant::SuspendAccount.....	87
296	5.2.1.1.1 Umsetzung	88
297	5.2.1.2 Operation I Account Management Insurant::ResumeAccount.....	90
298	5.2.1.2.1 Umsetzung	91
299	5.2.1.3 Operation I Account Management Insurant::GetAuditEvents	93
300	5.2.1.3.1 Umsetzung	94
301	5.2.1.4 Operation I Account Management Insurant::GetSignedAuditEvents	95
302	5.2.1.4.1 Umsetzung	96
303	5.3 Umschlüsselung	96
304	5.3.1 Übergreifende Anforderungen	97
305	5.3.2 Schnittstelle I Key Management Insurant.....	102
306	5.3.2.1 I Key Management Insurant::StartKeyChange()	102
307	5.3.2.1.1 Umsetzung	104
308	5.3.2.2 I Key Management Insurant::GetAllDocumentKeys().....	105
309	5.3.2.2.1 Umsetzung	106
310	5.3.2.3 Operation I Key Management Insurant::PutAllDocumentKeys()	107
311	5.3.2.3.1 Umsetzung	109
312	5.3.2.4 Operation I Key Management Insurant::FinishKeyChange()	109
313	5.3.2.4.1 Umsetzung	111
314	5.3.2.5 Protokollierung.....	111
315	5.4 Zugriffskontrolle.....	113
316	5.4.1 Grob-, mittel- und feingranulare Berechtigungen	113
317	5.4.2 Berufsgruppenspezifische Einschränkungen	114
318	5.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln	114
319	5.4.4 Vergabe von Zugriffsregeln	115
320	5.4.5 Funktionsprinzip Policy Administration	115
321	5.4.6 Anforderungen an die Zugriffskontrollprüfung	119
322	5.4.6.1 Erstmaliges Öffnen eines Verarbeitungskontextes.....	125
323	5.4.6.2 Berechtigung für einen Versicherten	125
324	5.4.6.3 Berechtigung für einen Vertreter	126
325	5.4.6.4 Berechtigung für eine Leistungserbringerinstitution	127
326	5.4.6.5 Berechtigung für einen Kostenträger.....	127
327	5.4.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4	127
328	5.5 Vertrauenswürdige Ausführung.....	129
329	5.5.1 Schnittstelle I Document Management Connect.....	129
330	5.5.1.1 Operation I Document Management Connect::OpenContext.....	134
331	5.5.1.1.1 Umsetzung	135
332	5.5.1.2 Operation I Document Management Connect::CloseContext.....	136
333	5.5.1.2.1 Umsetzung	137
334	5.5.2 Hardware-Merkmale	138

5.6 Statische Akteninhalte	138
6 Informationsmodelle	139
7 Anhang A – Verzeichnisse	140
7.1 Abkürzungen	140
7.2 Glossar	142
7.3 Abbildungsverzeichnis	142
7.4 Tabellenverzeichnis	142
7.5 Referenzierte Dokumente	146
7.5.1 Dokumente der gematik	146
7.5.2 Weitere Dokumente	147
8 Anhang B – XACML 2.0-Profile für Policy Documents (für Upgrade von ePA 3.1.3)	150
8.1 Policy Document für einen Versicherten	150
8.1.1 Base Policy	150
8.1.2 Permission Policy	153
8.2 Policy Document für einen Vertreter	184
8.2.1 Base Policy	184
8.2.2 Permission Policy	188
8.3 Policy Document für eine Leistungserbringerinstitution	216
8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente	216
8.3.2 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente	221
8.3.3 Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente	247
8.4 Policy Document für einen Kostenträger	271
8.4.1 Base Policy	271
8.4.2 Permission Policy	274
9 Anhang C– XACML 2.0-Profile für Policy Documents	278
9.1 Policy Document für einen Versicherten	278
9.2 Policy Document für einen Vertreter	281
9.3 Policy Document für eine Leistungserbringerinstitution	284
9.4 Policy Document für einen Kostenträger	306
9.5 Statische Permission Policies	311
9.5.1 Grobgranulare Berechtigung: Stufe Normal	311
9.5.2 Grobgranulare Berechtigung: Stufe Erweitert	312
9.5.3 Mittelgranulare Berechtigung: Kategorie "care"	312
9.5.4 Mittelgranulare Berechtigung: Kategorie "childsrecord"	313
9.5.5 Mittelgranulare Berechtigung: Kategorie "dentalrecord"	313
9.5.6 Mittelgranulare Berechtigung: Kategorie "eab"	314
9.5.7 Mittelgranulare Berechtigung: Kategorie "eau"	315
9.5.8 Mittelgranulare Berechtigung: Kategorie "ega"	315
9.5.9 Mittelgranulare Berechtigung: Kategorie "emp"	316
9.5.10 Mittelgranulare Berechtigung: Kategorie "mothersrecord"	316

377	9.5.11 Mittelgranulare Berechtigung: Kategorie "nfd"	317
378	9.5.12 Mittelgranulare Berechtigung: Kategorie "other"	318
379	9.5.13 Mittelgranulare Berechtigung: Kategorie "patientdoc"	319
380	9.5.14 Mittelgranulare Berechtigung: Kategorie "prescription"	320
381	9.5.15 Mittelgranulare Berechtigung: Kategorie "receipt"	320
382	9.5.16 Mittelgranulare Berechtigung: Kategorie "vaccination"	321
383	9.5.17 Mittelgranulare Berechtigung: Kategorie "practitioner"	322
384	9.5.18 Mittelgranulare Berechtigung: Kategorie "hospital"	322
385	9.5.19 Mittelgranulare Berechtigung: Kategorie "laboratory"	323
386	9.5.20 Mittelgranulare Berechtigung: Kategorie "physiotherapy"	324
387	9.5.21 Mittelgranulare Berechtigung: Kategorie "psychotherapy"	324
388	9.5.22 Mittelgranulare Berechtigung: Kategorie "dermatology"	325
389	9.5.23 Mittelgranulare Berechtigung: Kategorie "gynaecology urology"	325
390	9.5.24 Mittelgranulare Berechtigung: Kategorie "dentistry oms"	326
391	9.5.25 Mittelgranulare Berechtigung: Kategorie "other medical"	327
392	9.5.26 Mittelgranulare Berechtigung: Kategorie "other non medical"	327
393		

1 Einführung

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zur Herstellung, Test und Betrieb der Teilkomponente ePA-Dokumentenverwaltung des Produkttyps ePA-Aktensystem [gemSpec_Aktensystem]. Diese Teilkomponente ermöglicht das Speichern und Abrufen von (medizinischen) Dokumenten aus der persönlichen Akte eines Versicherten.

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 der Dokumentenverwaltung des Produkttyps ePA-Aktensystem nutzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, 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.

428 **1.5 Methodik**

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

433
434 **<AFO-ID> - <Titel der Afo>**
435 Text / Beschreibung
436 [**<=>**]

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

439

ENTWURF

440

2 Systemkontext

441 Die Komponente ePA-Dokumentenverwaltung des Produkttyps ePA-Aktensystem
442 [gemSpec_Aktensystem] dient dem sicheren Speichern und Auffinden von Dokumenten
443 des Versicherten aus seiner persönlichen Akte durch berechnigte Nutzer. Diese sind der
444 Versicherte selbst oder von ihm benannte Vertreter, Leistungserbringerinstitutionen und
445 Kostenträger.

446 Zur Umsetzung der ePA-Dokumentenverwaltung wird auf das Repository Registry-
447 Designmuster zurück gegriffen. Eine Document Registry verwaltet Metadaten, welche für
448 die Suche und Navigation von Dokumenten notwendig sind. Die Dokumente werden
449 verschlüsselt in einem Document Repository gespeichert. Die Schnittstellen der
450 Komponente ePA-Dokumentenverwaltung basieren auf den Spezifikationen von
451 Integrating the Healthcare Enterprise (IHE), insbesondere dem Konzept Cross-Enterprise
452 Document Sharing (XDS) zum Speichern und Abrufen von (medizinischen) Dokumenten,
453 welches Teil des IHE ITI Technical Frameworks (IHE ITI TF) ist. IHE ist eine
454 internationale Organisation, welche bestehende Industriestandards für die Umsetzung
455 spezifischer Anwendungsszenarien im digitalisierten Gesundheitswesen profiliert.

456 Neben der verschlüsselten Datenhaltung für Dokumente sieht die Komponente ePA-
457 Dokumentenverwaltung eine Vertrauenswürdige Ausführungsumgebung (VAU) vor,
458 welche es erlaubt, Metadaten im Klartext zu verarbeiten und somit Suchanfragen auf
459 Dokumente bedienen zu können. Mit der Abschottung dieser VAU auch gegenüber dem
460 Anbieter ePA-Aktensystem und seinen Mitarbeitern wird sichergestellt, dass ein Anbieter
461 ePA-Aktensystem auch in seinem betrieblichen Kontext vom Zugriff auf die verarbeiteten
462 Daten des Versicherten sicher ausgeschlossen ist. Eine VAU stellt die sichere
463 Laufzeitumgebung für das IHE ITI-basierte Dokumentenmanagement bereit.

464

3 Zerlegung der Komponente

465 Die Komponente ePA-Dokumentenverwaltung untergliedert sich in das
466 Kontextmanagement und die aktenindividuellen Verarbeitungskontexte. Diese Kontexte
467 stellen die Funktionsmerkmale "IHE-basierte Dokumentenverwaltung", "Zugriffskontrolle"
468 sowie "Aktenkontoverwaltung" für die Clients bereit. Das Kontextmanagement wird vom
469 Client Fachmodul ePA mittels TLS-Kanal über die TI erreicht. Anfragen vom Client ePA-
470 Frontend des Versicherten werden durch das Zugangsgateway TI an das
471 Kontextmanagement weitergeleitet. Das Kontextmanagement steuert die Instanziierung
472 der Verarbeitungskontexte und leitet Anfragen der Clients an diese weiter.

473

ENTWURF

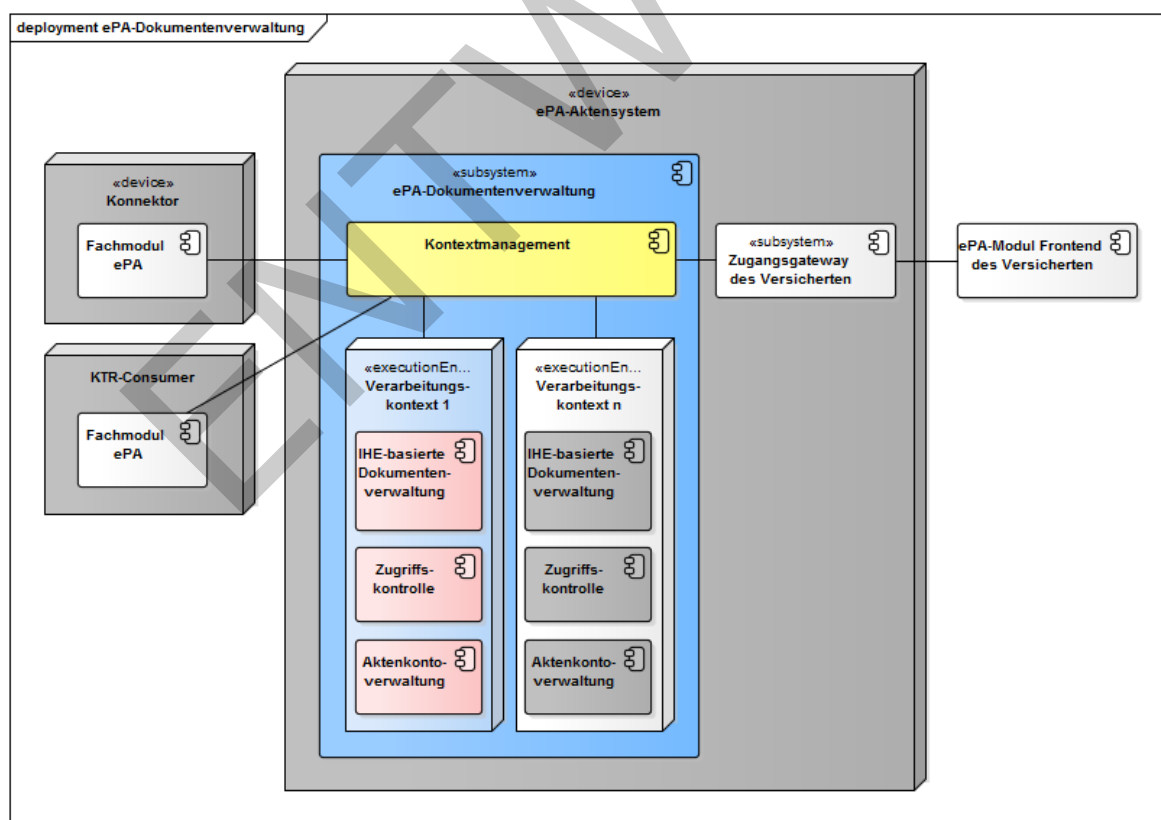
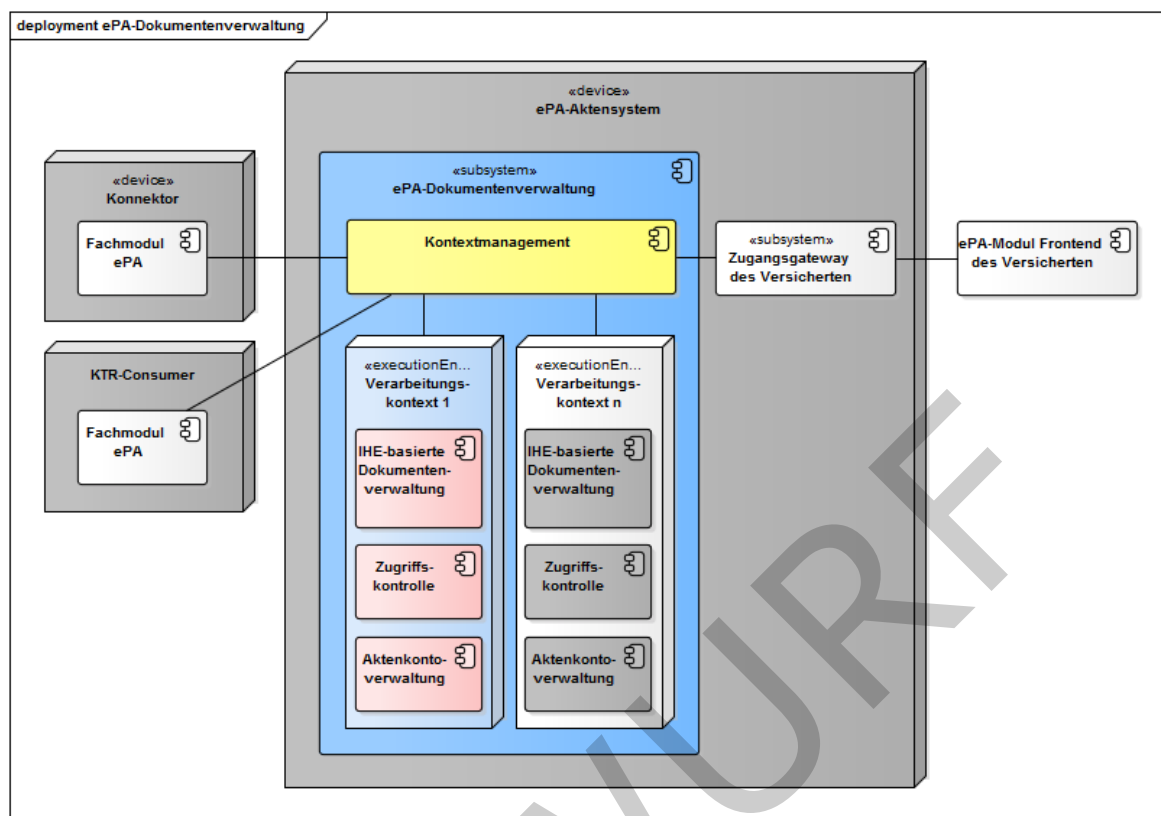


Abbildung 1: Komponentenzерlegung ePA-Dokumentenverwaltung

4 Übergreifende Festlegungen

A_15033 - Komponente ePA-Dokumentenverwaltung – Verwendung des SAML Token Profile 1.1 für Web Services Security bei SAML 2.0 Assertions

Die Komponente ePA-Dokumentenverwaltung MUSS die Anforderungen aus [WSS-SAML] umsetzen, wenn eine SAML 2.0 Assertion Teil einer SOAP 1.2-Eingangsnachricht ist. [≤]

A_15035 - Komponente ePA-Dokumentenverwaltung – Verwendung von SOAP Message Security 1.1

Die Komponente ePA-Dokumentenverwaltung MUSS die Sicherheitsanforderungen aus SOAP Message Security 1.1 [WSS] für die Verarbeitung von SOAP 1.2-Nachrichten umsetzen. [≤]

A_15034 - Komponente ePA-Dokumentenverwaltung – Unterstützung von Profilen der Web Services Interoperability Organization (WS-I)

Die Komponente ePA-Dokumentenverwaltung 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. [≤]

4.1 Namensräume

Für die Spezifikation der Schnittstellen der Komponente ePA-Dokumentenverwaltung werden die folgenden XML-Präfixe verwendet, um den Namensraum bzw. das Vokabular des XML-Dokuments zu kennzeichnen.

Präfix	Namensraum
lcm	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0
rmd	urn:ihe:iti:rmd:2017
rs	urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0
saml	urn:oasis:names:tc:SAML:2.0:assertion
wsa	http://schemas.xmlsoap.org/ws/2004/08/addressing
wss	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
xacml	urn:oasis:names:tc:xacml:2.0:policy:schema:os

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

4.2 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von Dokumenten

In diesem Abschnitt werden Anforderungen und Einschränkungen an relevante IHE ITI-Akteure und -Transaktionen der Komponente ePA-Dokumentenverwaltung gestellt, um die geforderte IHE ITI-Semantik zum ePA-Aktensystem zu bewahren. Werden IHE ITI-Akteure mit weiteren Sub-Akteuren gruppiert, so werden die Anforderungen der Sub-Akteure zum gruppierten Akteur übernommen. Eine Übersicht und Herleitung der IHE ITI-Akteure ist [\[gemSpec_DM_ePA#2.1.3\]](#) zu entnehmen. In Abschnitt 4.2.2 wird ein zusammenfassender Überblick über die Akteurgruppierungen und Optionen aus Abschnitt 4.2.1 gegeben.

Hinweis: Alle spezifizierten Anforderungen der IHE ITI-Akteure in Abschnitt 4.2.1 definieren das zu implementierende Verhalten an den Außenschnittstellen I_Document_Management, I_Document_Management_Insurance sowie I_Document_Management_Insurant. Dies schließt keine zusätzlich implementierten IHE-Funktionalitäten innerhalb der ePA-Dokumentenverwaltung aus.

A_17826 - Komponente ePA-Dokumentenverwaltung – Außenverhalten der IHE ITI-Implementierung

Die Komponente ePA-Dokumentenverwaltung DARF NICHT vom Verhalten der definierten Außenschnittstellen

I_Document_Management, I_Document_Management_Insurance sowie I_Document_Management_Insurant aus Abschnitt 5.1 abweichen. Dies schließt von Abschnitt 4.2.1 hinausgehende Implementierungen von IHE ITI-Akteuren und Optionen innerhalb der Komponente ePA-Dokumentenverwaltung mit ein, sodass zusätzlich implementierte IHE-Funktionalitäten keine Auswirkungen an den definierten Außenschnittstellen aufweisen dürfen. Ferner DARF zusätzliche IHE-Funktionalität Nachrichten an Komponenten außerhalb der ePA-Dokumentenverwaltung NICHT kommunizieren.[<=]

4.2.1 Anforderungen an IHE ITI-Akteure

A_13805 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XCDR Responding Gateway

Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XCDR Responding Gateway" gemäß [IHE-ITI-XCDR] implementieren.[<=]

A_13806 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XDS Document Registry

Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XDS Document Registry" gemäß [IHE-ITI-TF1] implementieren.[<=]

A_14727 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XDS Document Repository

Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XDS Document Repository" gemäß [IHE-ITI-TF1] implementieren. [<=]

A_13807 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XCA Responding Gateway

Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XCA Responding Gateway" 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 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs ATNA Audit Record Repository

Die Komponente ePA-Dokumentenverwaltung 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" (vgl. Abschnitt 4.4) umgesetzt, sodass die Nutzung des Integrationsprofils ATNA diesbzgl. eingeschränkt wird.

A_17166 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung der IHE ITI-Akteure ATNA Secure Node sowie ATNA Secure Application für Node Authentication

Die Komponente ePA-Dokumentenverwaltung 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 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs CT Time Client

Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "CT Time Client" gemäß [IHE-ITI-TF1] implementieren. [<=]

~~A_14655-01A_14655~~ - Komponente ePA-Dokumentenverwaltung – Zeitsynchronisation über Zeitdienst in der TI

Die Komponente ePA-Dokumentenverwaltung MUSS die Systemzeit über den Zeitdienst in der TI gemäß [gemSpec_Net#56.2] synchronisieren. [<=]

A_14597 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XUA X-Service Provider

Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XUA X-Service Provider" gemäß [IHE-ITI-TF1] implementieren. [<=]

A_14665 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Document Source

Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS Document Source" gemäß [IHE-ITI-TF1] implementieren. [<=]

A_14667 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Integrated Document Source/Repository

Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS Integrated Document Source/Repository" gemäß [IHE-ITI-TF1] implementieren.
[<=]

A_14668 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Document Consumer

Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS Document Consumer" gemäß [IHE-ITI-TF1] implementieren.[<=]

A_14666 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Patient Identity Source

Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS Patient Identity Source" gemäß [IHE-ITI-TF1] implementieren.
[<=]

A_14669 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS On-Demand Document Source

Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS On-Demand Document Source" gemäß [IHE-ITI-TF1] implementieren.
[<=]

A_14782 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs APPC Content Consumer

Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "APPC Content Consumer" gemäß [IHE-ITI-APPC] implementieren.[<=]

A_14950 - Komponente ePA-Dokumentenverwaltung – Keine Angabe einer Fehlerlokalisierung im RegistryError-Element

Die Komponente ePA-Dokumentenverwaltung DARF NICHT das `location`-Attribut im `rs:RegistryError`-Element in der IHE ITI-Ausgangsnachricht verwenden, sofern ein Fehler bei der Verarbeitung einer IHE ITI-Eingangsnachricht auftritt. Diese Einschränkung gilt nur für Error Stack Traces bzw. der Offenbarung von Programmierdetails.
[<=]

A_15081 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs RMU Update Responder

Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "RMU Update Responder" gemäß [IHE-ITI-RMU] implementieren.[<=]

4.2.1.1 APPC Content Consumer

4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren

Gruppierungen mit diesem IHE ITI-Akteur sind weiter unten definiert.

4.2.1.1.2 Optionen des IHE ITI-Akteurs

A_14787 - Komponente ePA-Dokumentenverwaltung – APPC Content Consumer ohne "View Option"-Option

Die Komponente ePA-Dokumentenverwaltung als APPC-Akteur "Content Consumer" DARF NICHT die Option "View Option" unterstützen.[<=]

620 **A_14788 - Komponente ePA-Dokumentenverwaltung – APPC Content Consumer**
 621 **mit "Structured Policy Processing Option"-Option**
 622 Die Komponente ePA-Dokumentenverwaltung als APPC-Akteur "Content Consumer"
 623 MUSS die Option "Structured Policy Processing Option" unterstützen. [\leq]

624 **4.2.1.2 RMU Update Responder**

625 *4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren*

626 **A_15093 - Komponente ePA-Dokumentenverwaltung – Gruppierung RMU**
 627 **Update Responder mit XCA Responding Gateway und X-Service Provider**
 628 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
 629 mit dem XCA-Akteur "Responding Gateway" gemäß [IHE-ITI-RMU] sowie mit dem XUA-
 630 Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions
 631 verarbeiten.
 632 [\leq]

633 **A_17571 - Komponente ePA-Dokumentenverwaltung – Gruppierung RMU**
 634 **Update Responder mit APPC Content Consumer**
 635 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
 636 mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert sein. [\leq]

637 *4.2.1.2.2 Optionen des IHE ITI-Akteurs*

638 **A_15094 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder**
 639 **ohne "Forward Update"-Option**
 640 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF
 641 NICHT die Option "Forward Update" unterstützen.
 642 [\leq]

643 **A_15095 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder**
 644 **mit "XCA Persistence"-Option**
 645 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
 646 die Option "XCA Persistence" unterstützen.
 647 [\leq]

648 **A_15096 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder**
 649 **ohne "XDS Persistence"-Option**
 650 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF
 651 NICHT die Option "XDS Persistence" unterstützen.
 652 [\leq]

653 **A_15097 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder**
 654 **ohne "XDS Version Persistence"-Option**
 655 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF
 656 NICHT die Option "XDS Version Persistence" unterstützen.
 657 [\leq]

658 Durch Verwendung der XCA Persistence Option und der Gruppierung des XCA Responding
 659 Gateways mit der XDS Registry wird von der XDS Registry erwartet, die aktualisierten
 660 Metadaten zu persistieren.

4.2.1.3 XCA Responding Gateway

4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_14598 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit X-Service Provider

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS mit dem XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions verarbeiten. [\leq]

A_14725 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit XDS Document Registry

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS mit dem XDS-Akteur "Document Registry" gemäß [IHE-ITI-TF1] gruppiert sein. [\leq]

A_14726 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit XDS Document Repository

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS mit dem XDS-Akteur "Document Repository" gemäß [IHE-ITI-TF1] gruppiert sein. [\leq]

A_14784 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit APPC Content Consumer

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert sein. [\leq]

4.2.1.3.2 Optionen des IHE ITI-Akteurs

A_13819 - Komponente ePA-Dokumentenverwaltung – XCA Responding Gateway ohne "On-Demand Documents"-Option

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" DARF NICHT die Option "On-Demand Documents" unterstützen. [\leq]

A_13820 - Komponente ePA-Dokumentenverwaltung – XCA Responding Gateway ohne "Persistence of Retrieved Documents"-Option

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" DARF NICHT die Option "Persistence of Retrieved Documents" unterstützen. [\leq]

4.2.1.4 XCDR Responding Gateway

4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_13648 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit X-Service Provider

Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS mit dem XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions verarbeiten. [\leq]

A_14723 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit XDS Document Registry

Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS mit dem XDS-Akteur "Document Registry" gemäß [IHE-ITI-XCDR] gruppiert sein. [\leq]

704 **A_14724 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR**
705 **Responding Gateway mit XDS Document Repository**

706 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
707 MUSS mit dem XDS-Akteur "Document Repository" gemäß [IHE-ITI-XCDR] gruppiert
708 sein. [≤]

709 **A_14783 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR**
710 **Responding Gateway mit APPC Content Consumer**

711 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
712 MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert
713 sein. [≤]

714 *4.2.1.4.2 Optionen des IHE ITI-Akteurs*

715 **A_13650 - Komponente ePA-Dokumentenverwaltung – XCDR Responding**
716 **Gateway ohne "Basic Patient Privacy Enforcement"-Option**

717 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
718 DARF NICHT die Option "Basic Patient Privacy Enforcement" unterstützen. [≤]

719

720 **4.2.1.5 XDS Document Registry**

721 *4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren*

722 **A_14599 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS**
723 **Document Registry mit X-Service Provider**

724 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS mit dem
725 XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions
726 verarbeiten. [≤]

727 **A_14785 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS**
728 **Document Registry mit APPC Content Consumer**

729 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS mit dem
730 APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert sein. [≤]

731 *4.2.1.5.2 Optionen des IHE ITI-Akteurs*

732 **A_14637 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry**
733 **ohne "Asynchronous Web Services Exchange"-Option**

734 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF NICHT die
735 Option "Asynchronous Web Services Exchange" unterstützen. [≤]

736 **A_14638 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry**
737 **mit "Reference ID"-Option**

738 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
739 die Option "Reference ID" unterstützen. [≤]

740 **A_14639 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry**
741 **ohne "Patient Identity Feed"-Option**

742 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF
743 NICHT die Option "Patient Identity Feed" unterstützen.
744 [≤]

A_14640 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "Patient Identity Feed HL7v3"-Option

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF NICHT die Option "Patient Identity Feed HL7v3" unterstützen.

[<=]

A_14641 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "On-Demand Documents"-Option

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF NICHT die Option "On-Demand Documents" unterstützen.

[<=]

A_14642 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "Document Metadata Update"-Option

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF NICHT die Option "Document Metadata Update" unterstützen.[<=]

4.2.1.6 XDS Document Repository

4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_14600 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS Document Repository mit X-Service Provider

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS mit dem XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions verarbeiten.[<=]

A_14786 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS Document Repository mit APPC Content Consumer

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert sein.[<=]

4.2.1.6.2 Optionen des IHE ITI-Akteurs

A_14636 - Komponente ePA-Dokumentenverwaltung – XDS Document Repository ohne "Asynchronous Web Services Exchange"-Option

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" DARF NICHT die Option "Asynchronous Web Services Exchange" unterstützen.[<=]

4.2.1.7 XUA X-Service Provider

4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren

Gruppierungen mit diesem IHE ITI-Akteur sind bereits weiter oben definiert.

4.2.1.7.2 Optionen des IHE ITI-Akteurs

A_14612 - Komponente ePA-Dokumentenverwaltung – XUA X-Service Provider ohne "Subject-Role"-Option

Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" DARF NICHT die Option "Subject-Role" unterstützen.[<=]

A_14613 - Komponente ePA-Dokumentenverwaltung – XUA X-Service Provider ohne "Authz-Consent"-Option

Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" DARF NICHT die Option "Authz-Consent" unterstützen.[<=]

A_14614 - Komponente ePA-Dokumentenverwaltung – XUA X-Service Provider ohne "PurposeOfUse"-Option

Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" DARF NICHT die Option "PurposeOfUse" unterstützen.[<=]

4.2.2 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 1: Tab_Dokv_10 - 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.

Tabelle 2: Tab_Dokv_11 - Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung

IHE ITI-Akteur	Opt.			Umzusetzende Option des IHE ITI-Akteurs	Opt.
		Gruppierung mit anderem IHE ITI-Akteur	Opt.		
APPC Content Consumer	R			View Option	X
				Structured Policy Processing Option	R
		RMU Update Responder	R		
		XCA Responding Gateway	R		
		XCDR Responding Gateway	R		

		XDS Document Registry	R	
		XDS Document Repository	R	
ATNA Audit Record Repository	X			
CT Time Client	X			
RMU Update Responder	R		Forward Update	X
			XCA Persistence	R
			XDS Persistence	X
			XDS Version Persistence	X
		APPC Content Consumer	R	
		XCA Responding Gateway	R	
		X-Service Provider	R	
XCDR Responding Gateway	R		Basic Patient Privacy Enforcement	X
		APPC Content Consumer	R	
		ATNA Secure Node oder Secure Application für Node	X	

		Authentication		
		XDS Document Registry	R	
		XDS Document Repository	R	
		XUA X-Service Provider	R	
XCA Responding Gateway	R		On-Demand Documents	X
			Persistence of Retrieved Documents	X
		APPC Content Consumer	R	
		ATNA Secure Node oder Secure Application für Node Authentication	X	
		RMU Update Responder	R	
		XDS Document Registry	R	
		XDS Document Repository	R	
		XUA X-Service Provider	R	
XDS Document Consumer	X			
XDS Document Registry	R		Asynchronous Web Services Exchange	X
			Document Metadata Update	X
			On-Demand Documents	X
			Patient Identity Feed	X

				Patient Identity Feed HL7v3	X
				Reference ID	R
		APPC Content Consumer	R		
		ATNA Secure Node oder Secure Application für Node Authentication	X		
		X-Service Provider	R		
XDS Document Repository	R			Asynchronous Web Services Exchange	X
		APPC Content Consumer	R		
		ATNA Secure Node oder Secure Application für Node Authentication	X		
		X-Service Provider	R		
XDS Document Source	X				
XDS Integrated Document Source / Repository	X				
XDS On- Demand Document Source	X				
XDS Patient Identity Source	X				
XUA X- Service Provider	R			Subject-Role	X
				Authz-Consent	X

				PurposeOfUse	X
		XCDR Responding Gateway	R		
		RMU Update Responder	R		
		XCA Responding Gateway	R		
		XDS Document Registry	R		
		XDS Document Repository	R		

4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen

A_17832 - Komponente ePA-Dokumentenverwaltung – Unterstützung MTOM/XOP

Die Komponente ePA-Dokumentenverwaltung MUSS gemäß den Anforderungen von [IHE-ITI-TF2x#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] verwenden. [≤]

4.2.3.1 Provide X-User Assertion [ITI-40]

~~A_14915-03A~~ ~~14915-02~~ - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide X-User Assertion

Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" DARF NICHT die Umsetzung der Operationen

- I_Document_Management::CrossGatewayDocumentProvide
- I_Document_Management::CrossGatewayQuery
- ~~I_Document_Management::RemoveDocuments~~
- ~~I_Document_Management::RemoveMetadata~~
- I_Document_Management::CrossGatewayRetrieve
- ~~I_Document_Management::RestrictedUpdateDocumentSet~~
- I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::RestrictedUpdateDocumentSet
- I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::RegistryStoredQuery
- I_Document_Management_Insurant::RemoveMetadata
- I_Document_Management_Insurant::RetrieveDocumentSet

825 hinsichtlich der Validierung der X-User Assertion (Authentication Assertion) gemäß der
826 definierten Ablauflogik in [IHE-ITI-TF2b#3.40.4.1.2 und 3.40.4.1.3]
827 implementieren.[<=]

828

829 **A_14594 - Komponente ePA-Dokumentenverwaltung – Validierung der**
830 **Authentication Assertion**

831 Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" MUSS
832 die X-User Assertion (Authentication Assertion) gemäß der Anforderung A_13690 prüfen
833 und die eingehende Nachricht mit Fehlercodes nach [WSS#12] quittieren, falls diese X-
834 User Assertion nicht gültig ist.[<=]

835 **4.2.3.2 Provide and Register Document Set-b [ITI-41]**

836 **A_14549 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
837 **Provide and Register Document Set-b**

838 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
839 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
840 Policy Documents (Advanced Patient Privacy Consents) entsprechend der
841 Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt registriert und ein
842 Dokument gespeichert wird.

843

844 [<=]

845 **A_15162-02 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung**
846 **bei Angabe von Document Entry Relationships in Metadaten**

847 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
848 MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und
849 mit einem XDSRepositoryMetadataError-Fehlercode quittieren, sofern die Metadaten die
850 folgenden Association Types nach [IHE-ITI-TF3#4.2.2] enthalten:

- 851 • urn:ihe:iti:2007:AssociationType:XFRM (Transform)
- 852 • urn:ihe:iti:2007:AssociationType:XFRM_RPLC (Replace with Transformation)
- 853 • urn:ihe:iti:2007:AssociationType:signs (Digital Signature)
- 854 • urn:ihe:iti:2010:AssociationType:IsSnapshotOf (Snapshot of On-Demand
855 document entry)
- 856 • urn:ihe:iti:2007:AssociationType:APND (Addendum)

857 [<=]

858 **A_14937 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße**
859 **prüfen**

860 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
861 MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das SubmissionSet
862 verarbeitet wird. Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur
863 "Document Repository" MUSS die Verarbeitung ablehnen und mit
864 einem MaxDocSizeExceeded- bzw. MaxPkgSizeExceeded-Fehlercode gemäß [IHE-ITI-
865 TF3#4.2.4] quittieren, wenn die Gesamtgröße aller übermittelten Dokumente 250 MByte
866 übersteigt oder die Größe mindestens eines einzelnen Dokuments 25 MByte übersteigt.

867 [<=]

A_14938 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung der Metadaten aus ITI Document Sharing-Profilen durch XDS-Akteur "Document Repository"

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die SubmissionSet- sowie die DocumentEntry-Metadaten der eingehenden Nachricht vor einer Zugriffskontrolle gemäß Konformität zu den Nutzungsvorgaben in [gemSpec_DM_ePA#A_14760] prüfen. Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" 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. [`<=`]

4.2.3.3 Remove Documents [ITI-86]

A_21186 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen der Metadaten bei Löschung von Dokumenten

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die mit den zu löschenden Dokumenten assoziierten Metadaten in der Document Registry löschen, bevor die Dokumente gelöscht werden und das assoziierte Submission Set löschen, sofern keine weiteren Dokumente oder Ordner mit diesem Submission Set assoziiert sind. [`<=`]

A_21187 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Remove Documents

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor ein Dokument oder mehrere Dokumente gelöscht werden. Bei einem Löschen von mehreren Dokumenten durch das ePA-Fachmodul können einzelne Dokumente durch den zwischenzeitlichen Entzug einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für das Löschen berechtigt sein. Widerspricht ein zu löschendes Dokument einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum betreffenden Dokument einen `XDSDocumentUniqueIdError`-Fehlercode enthalten und der Wert 4 des `EventOutcomeIndicators` im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein zu löschendes Dokument nicht mehr verfügbar, MUSS gemäß IHE TF ITI der Fehlercode `XDSDocumentUniqueIdError` zurückgegeben werden. [`<=`]

4.2.3.4 Remove Metadata [ITI-62]

A_14926-01 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen der Dokumente bei Remove Metadata

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS bei zu löschenden DocumentEntry-Einträgen im selben Zuge auch die assoziierten Dokumente im "Document Repository" löschen. [`<=`]

A_20701 - Komponente ePA-Dokumentenverwaltung – Unwiderrufliches Löschen bei Remove Metadata

Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass einmal gelöschte Dokumente und Metadatenobjekte nicht wiederhergestellt werden können. [`<=`]

A_14670-02 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Remove Metadata

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor ein oder mehrere Dokumente oder Metadatenobjekte gelöscht werden. Bei einem Löschen von mehreren Dokumenten oder Metadatenobjekten durch das ePA-Fachmodul können einzelne Dokumente durch den zwischenzeitlichen Entzug einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für das Löschen berechtigt sein. Widerspricht ein zu löschendes Dokument einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum betreffenden Dokument einen `XDSDocumentUniqueIdError`-Fehlercode enthalten und der Wert 4 des `EventOutcomeIndicators` im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein zu löschendes Dokument nicht mehr verfügbar, MUSS gemäß IHE TF ITI der Fehlercode `XDSDocumentUniqueIdError` zurückgegeben werden. [\leq]

4.3 Fehlerbehandlung in Schnittstellenoperationen

Bei Fehlern in der internen Verarbeitung oder fachlichen Fehlern in der Nutzung der von der Komponente ePA-Dokumentenverwaltung bereitgestellten Schnittstellen werden Operationsaufrufe von Nicht-IHE-Operationen mit gematik-Fehlermeldungen gemäß der Definition in [gemSpec_OM] beantwortet. Die Fehlermeldungen werden als SOAP-Fault gemäß [TelematikError.xsd] strukturiert. Abweichend von den Festlegungen in [gemSpec_OM] ~~des~~ sind zu meldende Fehler wie folgt mit Informationen zu füllen.

A_15664 - Komponente ePA-Dokumentenverwaltung – Fehlername

Die Komponente ePA-Dokumentenverwaltung MUSS in einer GERROR-Fehlermeldung gemäß [TelematikError.xsd] den in der Operationsdefinition festgelegten Fehlernamen Name im Feld `tel:Error/tel:Trace/tel:EventID` verwenden. [\leq]

A_15665 - Komponente ePA-Dokumentenverwaltung – Fehlertext

Die Komponente ePA-Dokumentenverwaltung MUSS in einer GERROR-Fehlermeldung gemäß [TelematikError.xsd] den in der Operationsdefinition festgelegten Fehlerdetailtext `Fehlertext` im Feld `tel:Error/tel:Trace/tel:ErrorText` verwenden. [\leq]

A_15666 - Komponente ePA-Dokumentenverwaltung – Fehlernummer

Die Komponente ePA-Dokumentenverwaltung MUSS in einer GERROR-Fehlermeldung gemäß [TelematikError.xsd] die folgenden Fehlercodes im Feld `tel:Error/tel:Trace/tel:Code` verwenden:

Tabelle 3: Tab_Dokv_12 - Fehlercodes zu Fehlern gemäß Operationsdefinition

Name	Fehlercode
INTERNAL_ERROR	7500
SYNTAX_ERROR	7510
ASSERTION_INVALID	7520

ACCESS_DENIED	7530
TEMP_UNAVAILABLE	7550
INVALID_AUT_KEY	7560

953 [\leq]

954 4.4 Vertrauenswürdige Ausführungsumgebung

955 In diesem Abschnitt werden die Anforderungen an die ePA-Dokumentenverwaltung zur
 956 Umsetzung einer Vertrauenswürdigen Ausführungsumgebung (VAU) gestellt. Die VAU
 957 dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von
 958 schützenswerten Klartextdaten innerhalb des ePA-Aktensystem. Die VAU stellt dazu
 959 aktenindividuelle Verarbeitungskontexte (d.h. Instanzen der VAU) bereit, in denen die
 960 Verarbeitung sensibler Daten im Klartext erfolgen kann. Diese Verarbeitungskontexte
 961 sind entsprechend zu schützen.

962 **A_14472-01 - Komponente ePA-Dokumentenverwaltung – Umsetzung des** 963 **Dokumentenmanagements in einer Vertrauenswürdigen Ausführungsumgebung** 964 **(VAU)**

965 Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der Operationen
 966 der Schnittstellen `I_Document_Management_Connect`,
 967 `I_Document_Management`, `I_Document_Management_Insurance` sowie
 968 `I_Document_Management_Insurant` im Verarbeitungskontext einer Vertrauenswürdigen
 969 Ausführungsumgebung (VAU) umsetzen. [\leq]

970 **A_18714-01 - Komponente ePA-Dokumentenverwaltung – Verhalten des** 971 **Kontextmanagements bei ungeöffnetem Verarbeitungskontext**

972 Das Kontextmanagement MUSS mit einem HTTP-Fehler 403 (Fehlermeldung "Access
 973 Denied") antworten, wenn für eine Web-Service-Operation der
 974 Schnittstellen `I_Document_Management`, `I_Document_Management_Insurant`,
 975 `I_Document_Management_Insurance` sowie `I_Account_Management_Insurant` für den
 976 angemeldeten Nutzer kein Verarbeitungskontext geöffnet wurde.
 977 [\leq]

978 4.4.1 Verarbeitungskontext

979 Die Gesamtheit aus der für eine Klartextverarbeitung erforderlichen Software, dem für
 980 eine Klartextverarbeitung genutzten physikalischen System sowie den für die Integrität
 981 einer Klartextverarbeitung erforderlichen organisatorischen und physischen
 982 Rahmenbedingungen bildet den Verarbeitungskontext der Vertrauenswürdigen
 983 Ausführungsumgebung.

984 Zur Vertrauenswürdigen Ausführungsumgebung gehören neben den
 985 Verarbeitungskontexten alle für ihre Erreichbarkeit und betriebliche Steuerung
 986 erforderlichen Komponenten.

987 Der Verarbeitungskontext grenzt sich von allen weiteren, im betrieblichen Kontext bei
 988 einem Anbieter ePA-Aktensystem vorhandenen Systemen und Prozessen dadurch ab,
 989 dass die sensiblen Klartextdaten von Komponenten innerhalb des Verarbeitungskontextes
 990 aus erreichbar sind oder sein können, während sie dies von außerhalb des

991 Verarbeitungskontextes nicht sind. Sensible Daten verlassen den Verarbeitungskontext
992 ausschließlich gemäß wohldefinierten (Zugriffs-)Regeln und in verschlüsselter Form.

993 **A_14557 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext**
994 **der VAU**

995 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS sämtliche
996 physikalischen Systemkomponenten sowie sämtliche Softwarekomponenten umfassen,
997 deren Sicherheitseigenschaften sich auf den Schutz der personenbezogenen
998 medizinischen Daten vor Zugriff durch Unbefugte bei ihrer Verarbeitung im Klartext
999 auswirken können. [<=]

1000 *Hinweis: Sofern zusätzliche Funktionalität in der ePA-Dokumentenverwaltung*
1001 *implementiert ist, welche innerhalb der VAU ausgeführt wird, muss diese durch ein*
1002 *Produktgutachten geprüft werden.*

1003 **A_14581 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung von**
1004 **außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten**

1005 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS
1006 sicherstellen, dass sämtliche schützenswerten Daten vor einer Speicherung außerhalb der
1007 VAU verschlüsselt werden. [<=]

1008 **A_14582 - Komponente ePA-Dokumentenverwaltung – Geschützte Weitergabe**
1009 **von Daten an autorisierte Nutzer durch die VAU**

1010 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS
1011 sicherstellen, dass sämtliche schützenswerten Daten ausschließlich über sichere
1012 Verbindungen an autorisierte Nutzer weitergegeben werden. [<=]

1013 **A_14583 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung der**
1014 **Dokumentmetadaten und technischen Daten der VAU**

1015 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS für die
1016 Verschlüsselung aller Dokumentmetadaten, Policy Documents und des § 291a-Protokolls
1017 des Versicherten sowie eigener technischer Daten den Kontextschlüssel des Aktenkontos
1018 verwenden. [<=]

1019 **A_14566 - Komponente ePA-Dokumentenverwaltung – Isolation zwischen**
1020 **Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU**

1021 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die in ihr ablaufenden
1022 Verarbeitungen für die Daten eines Verarbeitungskontextes von den Verarbeitungen für
1023 die Daten anderer Verarbeitungskontexte in solcher Weise trennen, dass mit technischen
1024 Mitteln ausgeschlossen wird, dass die Verarbeitungen eines Verarbeitungskontextes
1025 schadhaft auf die Verarbeitungen eines anderen Verarbeitungskontextes einwirken
1026 können. [<=]

1027 **4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem**
1028 **Betriebsumfeld**

1029 Der Schutzbedarf der in der VAU verarbeiteten Klartextdaten erfordert den technischen
1030 Ausschluss von Zugriffen des Anbieters. Dies umfasst insbesondere Zugriffe durch
1031 Personen aus dem betrieblichen Umfeld des Anbieters.

1032 **A_14558 - Komponente ePA-Dokumentenverwaltung – Isolation der VAU von**
1033 **Datenverarbeitungsprozessen des Anbieters**

1034 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die in ihren
1035 Verarbeitungskontexten ablaufenden Datenverarbeitungsprozesse von allen sonstigen
1036 Datenverarbeitungsprozessen des Anbieters trennen und damit gewährleisten, dass der
1037 Anbieter ePA-Aktensystem vom Zugriff auf die in der VAU verarbeiteten schützenswerten
1038 Daten ausgeschlossen ist. [<=]

A_14559 - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Software der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS eine Manipulation der eingesetzten Software erkennen und eine Ausführung der manipulierten Software verhindern. [≤]

A_14560 - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Hardware der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter ePA-Aktensystem ausschließen. [≤]

A_14561 - Komponente ePA-Dokumentenverwaltung – Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter ePA-Aktensystem mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann. [≤]

A_14562 - Komponente ePA-Dokumentenverwaltung – Kein physischer Zugang des Anbieters zu Systemen der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter ePA-Aktensystem, während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird. [≤]

A_14563 - Komponente ePA-Dokumentenverwaltung – Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln sicherstellen, dass physischer Zugang zu Hardware-Komponenten der Verarbeitungskontexte nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten extrahiert werden können. [≤]

A_14564 - Komponente ePA-Dokumentenverwaltung – Private Schlüssel von Dienstzertifikaten im HSM

Die Komponente ePA-Dokumentenverwaltung MUSS die folgenden privaten Schlüssel in einem Hardware Security Module (HSM) erzeugen und anwenden:

- TI-Fachdienst-Identität zur Authentisierung des Kontextmanagements gegenüber dem Fachmodul ePA (TLS)
- TI-Fachdienst-Identität zur Authentisierung des Verarbeitungskontextes gegenüber dem Fachmodul ePA (sicherer Kanal auf Anwendungsebene),
- Privater Schlüssel des Schlüsselpaars zur Authentisierung des Verarbeitungskontextes gegenüber dem ePA-Frontend des Versicherten (sicherer Kanal auf Anwendungsebene).

Die Prüftiefe des HSM MUSS dabei den in [gemSpec_Aktensystem#A_15156] angegebenen Standards entsprechen. [≤]

A_14565 - Komponente ePA-Dokumentenverwaltung – HSM-Kryptographieschnittstelle verfügbar nur für Instanzen der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln, die auch Manipulationen durch den Anbieter ePA-Aktensystem ausschließen, gewährleisten, dass nur Instanzen der VAU Zugriff auf die Kryptographieschnittstelle des HSM zur Nutzung des privaten Schlüsselmaterials für ihre Dienstzertifikate erhalten können. [≤]

A_14567 - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal vom Client zum Verarbeitungskontext der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS den Aufbau eines vertraulichen und integritätsgeschützten Kommunikationskanals gemäß [gemSpec_Krypt#3.15] zwischen einem Client und einem Verarbeitungskontext erzwingen, bevor der Verarbeitungskontext durch Übergabe des Kontextschlüssels durch den Client aktiviert werden kann.[<=]

4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes

Die Vertrauenswürdige Ausführungsumgebung realisiert ein zweistufiges Verfahren zum Schutz vor unberechtigten Zugriffen auf die verarbeiteten schützenswerten Klartextdaten. Neben den Verfahren zur Authentisierung und Autorisierung der Nutzer durch Dienste des Anbieters auf der Basis ihrer Nutzeridentitäten, muss der Nutzer über einen aktenspezifischen kryptographischen Kontextschlüssel verfügen. Erst nachdem der Nutzer den Kontextschlüssel sicher an den Verarbeitungskontext übermittelt hat, ist der Verarbeitungskontext in der Lage, die schützenswerten Daten zu entschlüsseln und zu verarbeiten.

A_14568 - Komponente ePA-Dokumentenverwaltung – Aktivierung des Verarbeitungskontextes der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln gewährleisten, dass schützenswerte Nutzdaten im Verarbeitungskontext erst nach Aktivierung – mittels Übergabe des korrekten *Kontextschlüssels* an den Verarbeitungskontext durch den Client eines berechtigten Nutzers – entschlüsselt und verarbeitet werden können.[<=]

A_15085 - Komponente ePA-Dokumentenverwaltung – Prüfung des Kontextschlüssels durch die VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die Korrektheit des übergebenen Kontextschlüssels prüfen und dabei die folgenden zwei Fälle unterscheiden:

- Eine durch den sich verbindenden Nutzer initialisierte VAU MUSS den Kontextschlüssel durch Anwendung auf Daten des Verarbeitungskontextes mittels AES-GCM prüfen.
- Eine bereits initialisierte VAU MUSS den Kontextschlüssel eines sich zusätzlich verbindenden Nutzers durch Prüfung der Übereinstimmung mit dem bereits genutzten Kontextschlüssel prüfen.

Im Falle einer fehlgeschlagenen Prüfung des Kontextschlüssels MUSS die VAU die Verbindung zum Nutzer mit einer Fehlermeldung sofort beenden. Im Sonderfall eines erstmaligen Verbindungsaufbaus mit einem Verarbeitungskontext DARF die VAU die Verbindung NICHT abbrechen und MUSS die Daten des Verarbeitungskontextes mit Hilfe des Kontextschlüssels verschlüsseln.[<=]

A_14570 - Komponente ePA-Dokumentenverwaltung – Keine Speicherung des Kontextschlüssels in der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung DARF den Kontextschlüssel NICHT über das Ende der Sitzung des letzten verbundenen Nutzers hinaus speichern oder verwenden.[<=]

A_15841 - Komponente ePA-Dokumentenverwaltung – Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS sämtliche aktenbezogenen Daten (Nutzdaten, Konfigurationsdaten und Schlüsselmaterial) sicher löschen, wenn die Sitzung des letzten verbundenen Nutzers beendet wird.[<=]

1135 4.4.4 Parallele Zugriffe

1136 Die folgenden Anforderungen tragen dem Umstand Rechnung, dass sich mehr als ein
1137 Nutzer gleichzeitig mit dem Aktenkonto eines Versicherten verbinden kann.

1138 **A_14571 - Komponente ePA-Dokumentenverwaltung – Parallele Zugriffe auf** 1139 **den Verarbeitungskontext der VAU**

1140 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS parallele Zugriffe auf einen
1141 Verarbeitungskontext ermöglichen und dabei die transaktionale Integrität der
1142 gespeicherten Daten gewährleisten. [\leq]

1143 **A_14572 - Komponente ePA-Dokumentenverwaltung – Eindeutige VAU-Instanz** 1144 **für einen Verarbeitungskontext der VAU**

1145 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass parallele
1146 Zugriffe auf ein Aktenkonto immer in derselben Instanz der VAU verarbeitet
1147 werden. [\leq]

1148 4.4.5 Konsistenz der Akte, Logging und Monitoring

1149 **A_14573 - Komponente ePA-Dokumentenverwaltung – Konsistenter** 1150 **Systemzustand des Verarbeitungskontextes der VAU**

1151 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass ein
1152 konsistenter Zustand des Verarbeitungskontextes auch bei Bedienfehlern oder
1153 technischen Problemen immer erhalten bleibt bzw. wiederhergestellt werden kann. [\leq]

1154 **A_14574 - Komponente ePA-Dokumentenverwaltung – Datenschutzkonformes** 1155 **Logging und Monitoring des Verarbeitungskontextes der VAU**

1156 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die für den Betrieb eines
1157 Fachdienstes erforderlichen Logging- und Monitoring-Informationen in solcher Art und
1158 Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass
1159 dem Anbieter ePA-Aktensystem vertrauliche oder zur Profilbildung geeignete Daten zur
1160 Kenntnis gelangen. [\leq]

1161 4.4.6 Client-Verbindungen zum Verarbeitungskontext

1162 Um Verbindungen vom Fachmodul ePA nach [gemSpec_FM_ePA,
1163 gemSpec_FM_ePA_KTR_Consumer] und ePA-Frontend des Versicherten nach
1164 [gemSpec_FdV_ePA] zum Verarbeitungskontext des Aktenkontos zu ermöglichen, ist ein
1165 Kontextmanagement erforderlich. Das Kontextmanagement ist im Netzwerk der TI für
1166 das Fachmodul ePA und für das ePA-Frontend des Versicherten unter mindestens einer
1167 IP-Adresse/Port-Kombination erreichbar, die im Namensdienst der TI registriert sein
1168 muss. Das Kontextmanagement initialisiert und terminiert Verarbeitungskontexte
1169 bedarfsgesteuert und vermittelt die Verbindungen zwischen dem Client und dem jeweils
1170 benötigten Verarbeitungskontext.

1171 **A_14616 - Komponente ePA-Dokumentenverwaltung – Kontextmanagement der** 1172 **Vertrauenswürdigen Ausführungsumgebung**

1173 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS ein Kontextmanagement
1174 bereitstellen, das Verarbeitungskontexte bedarfsgesteuert initialisiert und terminiert,
1175 über initialisierte Verarbeitungskontexte auf der Basis ihrer RecordIdentifier Buch
1176 führt und Verbindung zwischen Clients und den jeweils benötigten
1177 Verarbeitungskontexten vermittelt. [\leq]

A_14575 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontexte der VAU über gemeinsame Host-Adresse erreichbar

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS ihre Verarbeitungskontexte über gemeinsame IP-Adressen und Ports des Kontextmanagements der ePA-Dokumentenverwaltung erreichbar machen. [\leq]

A_14576-01 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom ePA-Frontend des Versicherten zum Verarbeitungskontextes der VAU über das Zugangsgateway

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS Verbindungen vom ePA-Frontend des Versicherten ausschließlich über das Zugangsgateway des Versicherten akzeptieren. [\leq]

A_15528 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom Fachmodul ePA zum Verarbeitungskontextes der VAU über das Kontextmanagement

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS Verbindungen vom Fachmodul ePA ausschließlich über TLS akzeptieren. Es MUSS die TLS-Verbindung terminieren und HTTP Requests und Responses zwischen dem Fachmodul ePA und dem für die jeweilige Sitzung zugeordneten Verarbeitungskontext der VAU vermitteln. [\leq]

A_17834 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom Fachmodul ePA KTR-Consumer zum Verarbeitungskontextes der VAU über das Kontextmanagement

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS Verbindungen vom Fachmodul ePA KTR-Consumer ausschließlich über TLS akzeptieren. Es MUSS die TLS-Verbindung terminieren und HTTP Requests und Responses zwischen dem Fachmodul ePA KTR-Consumer und dem für die jeweilige Sitzung zugeordneten Verarbeitungskontext der VAU vermitteln. [\leq]

A_14577-01 - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal zum Verarbeitungskontext der VAU auf Inhaltsebene

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS dem ePA-Frontend des Versicherten, dem Fachmodul ePA sowie dem Fachmodul ePA KTR-Consumer den Aufbau eines sicheren Kanals, d.h. einen Verbindungsaufbau gemäß [gemSpec_Krypt#3.15], zum Verarbeitungskontext auf Inhaltsebene ermöglichen. [\leq]

A_14580 - Komponente ePA-Dokumentenverwaltung – Identität der Dokumentenverwaltung für das Fachmodul ePA und Fachmodul ePA KTR-Consumer

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS sich innerhalb der TI mittels der Fachdienstidentität `oid_epa_dvw` mit Zertifikatsprofil `C.FD.TLS-S` ausweisen. [\leq]

A_15646-01 - Komponente ePA-Dokumentenverwaltung – Identität des Verarbeitungskontextes für Clients

Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS sich gegenüber dem Fachmodul ePA, dem Fachmodul ePA KTR-Consumer sowie dem ePA-Frontend des Versicherten mittels der Fachdienstidentität `oid_epa_vau` mit Zertifikatsprofil `C.FD.AUT` ausweisen. [\leq]

A_15183 - Komponente ePA-Dokumentenverwaltung – Automatisierter Abbau des sicheren Kanals bei Inaktivität

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS den sicheren Kanal zu einem Client nach 20 Minuten Inaktivität abbauen, sodass

1229 anschließend keine Zugriffe dieses Clients auf den Verarbeitungskontext mehr möglich
1230 sind, ohne dass eine neue Verbindung aufgebaut wird. [≤]

1231 4.5 Anforderungen zur sicherheitstechnischen Validierung

1232 **A_15186 - Komponente ePA-Dokumentenverwaltung – Prüfung der** 1233 **Kombination von WS-Addressing Action und SOAP Body**

1234 Die Komponente ePA-Dokumentenverwaltung MUSS vor einer Weiterverarbeitung
1235 sämtliche SOAP 1.2-Eingangsnachrichten dahingehend prüfen, ob die angegebene WS-
1236 Addressing Action zum SOAP Body passt. Ist diese Kombination nicht passend, MUSS die
1237 Komponente ePA-Dokumentenverwaltung die Nachricht mit einem HTTP-Statuscode 400
1238 gemäß [RFC7231] quittieren und die Verarbeitung der Nachricht abbrechen. [≤]

1239 **A_15585 - Komponente ePA-Dokumentenverwaltung – Gleichheit von SOAP** 1240 **Action und WS-Addressing Action**

1241 Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Eingangsnachrichten mit
1242 einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und die Verarbeitung der
1243 Nachricht abbrechen, falls die Werte aus SOAP Action (HTTP Header) und des Action-
1244 Elements [WSA] des SOAP Headers nicht übereinstimmen. [≤]

1245 **A_14465-01 - Komponente ePA-Dokumentenverwaltung – XML Schema-** 1246 **Validierung für SOAP-Eingangsnachrichten**

1247 Die Komponente ePA-Dokumentenverwaltung MUSS vor einer Weiterverarbeitung
1248 sämtliche SOAP 1.2-Eingangsnachrichten einer XML Schema-Validierung auf Basis
1249 ausschließlich intern vorliegender XML Schema-Definitionen unterziehen und gemäß
1250 [SOAP] verarbeiten. Sind Nachrichten nicht wohlgeformt oder ungültig, MUSS die
1251 Komponente ePA-Dokumentenverwaltung die Nachricht mit einem HTTP-Statuscode 400
1252 gemäß [RFC7231] quittieren. [≤]

1253 **A_14809 - Komponente ePA-Dokumentenverwaltung – Keine Verwendung des** 1254 **"xsi:schemaLocation"-Attributs**

1255 Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Eingangsnachrichten mit
1256 einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren, falls ein xsi:schemaLocation-
1257 Attribut gemäß [XMLSchema#2.6.3] enthalten ist. [≤]

1258 **A_13690-02 - Komponente ePA-Dokumentenverwaltung – SAML 2.0 Assertion-** 1259 **Validierung**

1260 Die Komponente ePA-Dokumentenverwaltung MUSS die vorliegende Assertion einer
1261 grundsätzlichen XML Schema-Prüfung, einer Prüfung gemäß den Prüfvorschriften aus
1262 [gemSpec_TBAuth#3.2] sowie einer Prüfung auf Übereinstimmung mit dem
1263 erforderlichen SAML 2.0 Assertion-Profil aus [gemSpec_FM_ePA#A_14927,
1264 A_15638], [gemSpec_Authentisierung_Vers#A_14109, A_15631],
1265 [gemSpec_Autorisierung#A_14491] oder [gemSpec_FM_ePA_KTR_Consumer#A_17253,
1266 A_17254] unterziehen und die Verarbeitung der begleitenden Nachricht abbrechen und
1267 gemäß [WSS#12] bzw. im Sonderfall der Authorization Assertion mit einem HTTP-Fehler
1268 403 (Fehlermeldung "Access Denied") quittieren, falls eine Übereinstimmung nicht
1269 festgestellt werden kann.

1270
1271 Insbesondere MUSS das in der SAML 2.0 Assertion enthaltende Signaturzertifikat mittels
1272 [gemSpec_PKI_018#TUC_PKI_018] mit den folgenden Parametern geprüft werden:

1273 **Tabelle 4: Tab_Dokv_35 - Eingangsparameter für TUC_PKI_018**

Parameter	Belegung
-----------	----------

	SAML 2.0 Assertion des Fachmodul ePA
Zertifikat	Signaturzertifikat
PolicyList	oid_smc_b_osig
intendedKeyUsage	nonRepudiation
intendedExtendedKeyUsage	(leer)
OCSP-Graceperiod	60 Minuten
Offline-Modus	nein
Prüfmodus	OCSP

1274
1275 Die Telematik-ID im Signaturzertifikat muss identisch mit der Telematik-ID in der
1276 Identitätsbestätigung sein.[<=]

1277 Der Hinweis unter [gemSpec_Autorisierung]#A_17655 gilt auch im vorliegenden
1278 Prüfkontext, d.h. die dort beschriebene vereinfachte Prüfung kann für selbst ausgestellte
1279 Identitätsbestätigungen dementsprechend auch im Kontext der hier thematisierten
1280 Prüfung umgesetzt werden.

1281 **A_18990 - ePA-Dokumentenverwaltung – Beschränkung gültiger** 1282 **Identitätsbestätigungen**

1283 Die Komponente ePA-Dokumentenverwaltung DARF in Aufrufen aus Richtung der
1284 Komponente Zugangsgateway KEINE Identitätsbestätigung akzeptieren, die nicht durch
1285 die Komponente Authentisierung (Versicherter) erstellt wurde[<=]

1286 **A_17386-01 - Komponente ePA-Dokumentenverwaltung – Authentication** 1287 **Assertion-Validierung**

1288 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass Authentication
1289 Assertions nur akzeptiert werden, wenn das zugehörige Signaturzertifikat zeitlich gültig
1290 ist, nicht gesperrt wurde und entweder nach dem Zertifikatsprofil C.FD.SIG auf die
1291 Identität der Komponente Authentisierung Versicherter oder aber nach dem
1292 Zertifikatsprofil C.HCI.OSIG auf die Identität einer SM-B ausgestellt wurde.[<=]

1293 **A_17387 - Komponente ePA-Dokumentenverwaltung – Authorization Assertion-** 1294 **Validierung**

1295 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass Authorization
1296 Assertions nur akzeptiert werden, wenn das zugehörige Signaturzertifikat zeitlich gültig
1297 ist, nicht gesperrt wurde und nach dem Zertifikatsprofil C.FD.SIG auf die Identität der
1298 Komponente Autorisierung ausgestellt wurde.
1299 [<=]

1300 Dies kann durch eine aktuell gehaltene Konfiguration vertrauenswürdiger Zertifikate
1301 umgesetzt werden und ersetzt eine detaillierte Prüfung der Signaturzertifikate gem.
1302 [gemSpec_TBAuth#A_15557].

1303 Weitere Hinweise zur Validierung von SAML 2.0 Assertions können [OWASP-SAML]
1304 entnommen werden.

A_14735 - Komponente ePA-Dokumentenverwaltung – Verpflichtende Nutzung des "mustUnderstand"-Attributs im SOAP Security Header

Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Nachrichten mit SAML 2.0 Assertions im SOAP Security Header mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren, sofern das SOAP 1.2 `mustUnderstand`-Attribut im SOAP Security Header nicht angegeben ist oder den Wert `false` bzw. 0 hat ([SOAP12#5.2.3] [WSS#5]).[<=]

A_14810 - Komponente ePA-Dokumentenverwaltung – Erkennung von Denial-of-Service-Angriffen hinsichtlich dem Parsen von SOAP 1.2-Nachrichten

Die Komponente ePA-Dokumentenverwaltung MUSS die folgenden Angriffstypen in eingehenden SOAP 1.2-Nachrichten erkennen und mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren:

- XML Injection
- XPath Query Tampering
- XML External Entity Injection

[<=]

Weitere Hinweise zur Erkennung von Denial-of-Service-Angriffen können [OWASP-WSS] und [OWASP-IP] entnommen werden.

~~A_14811-01A_14811~~ - Komponente ePA-Dokumentenverwaltung – Ablehnung von SOAP 1.2-Nachrichten ohne UTF-8 Kodierung

Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Nachrichten mitdahingehend prüfen, dass diese der Zeichenkodierung UTF-8 entsprechen, andernfalls die Operation einem geeigneten HTTP-Statuscode 406 gemäß [RFC7231] ablehnen.[<=quittieren, sofern die Zeichenkodierung im HTTP Header nicht UTF-8 benennt (Content-Type: charset=utf-8).[<=]

~~A_21200~~ - Komponente ePA-Dokumentenverwaltung und Clients – UTF-8 Kodierung von SOAP 1.2-Nachrichten

Die Komponente ePA-Dokumentenverwaltung und deren Clients 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.

4.6 Protokollierung

Die Anforderungen an die Protokollierung für die Komponente ePA-Dokumentenverwaltung leiten sich aus dem Konzept der Protokollierung aus [\[gemSysL_ePA#2.5.5\]](#) ab.

~~A_14813-03A_14813-02~~ - Komponente ePA-Dokumentenverwaltung – Protokollierung in der Komponente ePA-Dokumentenverwaltung

Die Komponente ePA-Dokumentenverwaltung MUSS beim Aufruf einer der folgenden Operationen

- `I_Document_Management::CrossGatewayDocumentProvide`
- `I_Document_Management::CrossGatewayQuery`
- `I_Document_Management::RemoveMetadata`
- `I_Document_Management::RemoveDocuments`

- I_Document_Management::CrossGatewayRetrieve
- I_Document_Management::RestrictedUpdateDocumentSet
- I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::RestrictedUpdateDocumentSet
- I_Document_Management_Insurant::RegistryStoredQuery
- I_Document_Management_Insurant::RemoveMetadata
- I_Document_Management_Insurant::RetrieveDocumentSet
- I_Account_Management_Insurant::GetAuditEvents
- I_Account_Management_Insurant::GetSignedAuditEvents
- I_Account_Management_Insurant::SuspendAccount
- I_Account_Management_Insurant::ResumeAccount
- I_Key_Management_Insurant::StartKeyChange
- ~~I_Key_Management_Insurant::GetAllDocumentKeys~~
- ~~I_Key_Management_Insurant::PutAllDocumentKeys~~
- ~~I_Key_Management_Insurant::FinishKeyChange~~

je einen Eintrag im § 291a-Protokoll für den Versicherten gemäß [gemSpec_DM_ePA#A_14471] mit folgenden vom Operationsaufruf abhängigen Parametern vornehmen: UserID, UserName, ObjectID, ~~und~~ ObjectName ~~und ObjectDetail.~~ -[<=]

A_14814 - Komponente ePA-Dokumentenverwaltung – Schutz vor Manipulation der Protokolldaten

Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die § 291a-Protokolldaten gegen Veränderung und unberechtigtes Löschen geschützt sind. [≤]

A_20538-01A_20538 - Komponente ePA-Dokumentenverwaltung – Parameter des § 291a-Protokolls

Die Komponente ePA-Dokumentenverwaltung MUSS einen Protokolleintrag gemäß der Festlegung in [gemSpec_DM_ePA#A_14471] mit folgenden Ergänzungen erzeugen:

Tabelle 5: Tab_Dokv_13 - Parameter des § 291a-Protokolls

Protoko ll- parame ter	Parameterwerte gemäß aufgerufener Operation
---------------------------------	---

<p><u>User-ID</u> <u>UserID</u> <u>D</u></p>	<p>Bei Aufrufen einer Operation <u>Wert des AttributeStatements</u> der <u>Schnittstellen</u></p> <ul style="list-style-type: none"> • I_Document_Management • I_Document_Management_Insurance • I_Account_Management_Insurant sowie • I_Document_Management_Insurant <p><u>übergebenen übergebenen AuthenticationAssertion in</u> <u>SAML:Assertion/SAML:AttributeStatement</u></p> <p><u>Variante a: Akteur des Aufrufs ist Versicherter bzw. Vertreter</u> <u>(unveränderbare Anteil der KVNR des aufrufenden Versicherten bzw. Vertreters)</u> XPath-Ausdruck zur "Subject ID" der im Operationsaufruf übergebenen Authentication Assertion:</p> <pre>//*[local-name()='Assertion' and namespace-uri()='urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri()='urn:oasis:names:tc:SAML:2.0:assertion'][@Name='urn:gematik:subject:subject-id']/*[local-name()='AttributeValue']/*[local-name()='InstanceIdentifier']/data(@extension)</pre> <p><u>Variante b: Akteur des Aufrufs ist LEI oder Kostenträger</u> <u>(Telematik-ID der aufrufenden LEI oder Kostenträgers)</u> XPath-Ausdruck zur "Organization ID" der im Operationsaufruf übergebenen Authentication Assertion:</p> <pre>//*[local-name()='Assertion' and namespace-uri()='urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri()='urn:oasis:names:tc:SAML:2.0:assertion'][@Name='urn:gematik:subject:organization-id']/*[local-name()='AttributeValue']/*[local-name()='InstanceIdentifier']/data(@extension)</pre>
<p><u>User Name</u> <u>NameUs</u> <u>erName</u></p>	<p>Bei Aufrufen einer Operation der Schnittstellen</p> <ul style="list-style-type: none"> • I_Account_Management_Insurant • I_Document_Management <p>XPath-Ausdruck zur "<u>XSPA Organization</u>" <u>Behauptung "name" (beinhaltet commonName aus dem X.509-Zertifikat)</u>, der im Operationsaufruf übergebenen Authentication Assertion:</p> <pre>//*[local-name()='Assertion' and namespace-uri()='urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri()='urn:oasis:names:tc:SAML:2.0:assertion'][@Name='urn:oasis:names:tc:xaaml:1.0:subject:organization' and namespace-uri()='http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name']/*[local-name()='AttributeValue']/text()[normalize-space()='']</pre> <p>Bei Aufrufen einer Operation der Schnittstellen:</p> <ul style="list-style-type: none"> • I_Document_Management_Insurance sowie

	<p>• <u>I_Document_Management_Insurant:</u></p> <p>XPath-Ausdruck zum SAML-Subject der im Operationsaufruf übergebenen Authentication Assertion:</p> <p><code>//*[local-name()='Assertion' and namespace-uri()='urn:oasis:names:tc:SAML:2.0:assertion']/*[local-name()='Subject']/*[local-name()='NameID']/text()[normalize-space()='']</code></p>				
Object- ID <u>Object ID</u>	<p>Der unveränderbare Anteil der KVNR des extension-Attributs aus dem InsurantId-Element des RecordIdentifier-Elements oder die DocumentEntry.patientId des entsprechenden Operationsaufrufs</p> <p><i>Hinweis: Bei Aufruf von Operationen ohne diesen Parameter wird der Wert im Protokolleintrag nicht belegt.</i></p>				
Object Detail ObjectD etail <u>Object Detail ObjectD etail</u>	<p>Bei Zugriff über Für alle Operationen gilt: Falls die Transaktionen:Operation mit einem Fehler ASSERTION INVALID aufgrund einer ungültigen übergebenen Authentication Assertion abbricht.</p> <p>• <u>CrossGatewayDocumentProvide</u></p> <p>• <u>ProvideAndRegisterDocumentSet-b</u></p> <p>• <u>CrossGatewayRetrieve</u></p> <p>• <u>RetrieveDocumentSet</u></p> <p>• <u>RemoveMetadata</u></p> <p>• <u>RestrictedUpdateDocumentSet</u></p> <p>MUSS ParticipantObjectDetail beim Zugriff auf Dokumente mit folgenden Wertepaaren (type/value) belegt werden:</p> <table> <tr> <th>type</th><th>value</th></tr> <tr> <td><u>ErrorInformation</u></td><td><u>"fehlgeschlagene Authentifizierung des Zugreifenden"</u></td></tr> </table> <p><u>Bei Zugriff über die Operationen:</u></p> <p>• <u>CrossGatewayDocumentProvide</u></p> <p>• <u>ProvideAndRegisterDocumentSet-b</u></p> <p>• <u>CrossGatewayRetrieve</u></p> <p>• <u>RetrieveDocumentSet</u></p> <p>• <u>RemoveMetadata</u></p> <p>• <u>RemoveDocuments</u></p> <p>• <u>RestrictedUpdateDocumentSet</u></p>	type	value	<u>ErrorInformation</u>	<u>"fehlgeschlagene Authentifizierung des Zugreifenden"</u>
type	value				
<u>ErrorInformation</u>	<u>"fehlgeschlagene Authentifizierung des Zugreifenden"</u>				

<u>MUSS ParticipantObjectDetail beim Zugriff auf Dokumente mit folgenden Wertepaaren (type/value) belegt werden:</u>	
<u>type</u>	<u>value</u>
DocumentUniqueId	Wert von DocumentEntry.uniqueId
DocumentTitle	Wert von DocumentEntry.title
DocumentPracticeSetting	<p>Wert von DocumentEntry.practiceSettingCode, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3]. (Beispiel: „ALLG^^^&1.3.6.1.4.1.19376.3.276.1.5.4&ISO“, wobei ALLG für den Code und 1.3.6.1.4.1.19376.3.276.1.5.4 für das Code System steht.</p>
DocumentFormat	<p>Wert von DocumentEntry.formatCode, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3]., siehe oben. 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.</p> <p>Hinweis: Ein verarbeitendes System muss also, falls der hinterlegte Wert nicht dem Coded String-Format entspricht, den Wert als mimeType gemäß DocumentEntry.mimeType interpretieren.</p>
DocumentConfidentialityCode	<p>Wert von DocumentEntry.confidentialityCode, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3]., siehe oben.</p>
und beim Zugriff auf Ordner mit den folgenden Wertepaaren (type/value) belegt werden:	
<u>type</u>	<u>value</u>
FolderCodeList	<p>Wert von Folder.codeList, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3], siehe oben. Wird mehr als ein Code dokumentiert, MUSS als Trennzeichen das Tildezeichen ('~') verwendet werden.</p>

FolderUniqueId	Wert von Folder.uniqueId
FolderTitle	Wert von Folder.title
FolderLastUpdateTime	Wert von Folder.lastUpdateTime

1377 [**<=**]

1378 **A 21213 - Komponente ePA-Dokumentenverwaltung - Protokollierung von**
 1379 **Suchparametern**

1380 Die Komponente ePA-Dokumentenverwaltung MUSS beim Zugriff auf die Operationen
 1381 I Document Management Insurant::RegistryStoredQuery sowie
 1382 I Document Management::CrossGatewayQuery einen Protokolleintrag gemäß A 20538-
 1383 * vornehmen und darüberhinaus ParticipantObjectDetail um folgende Wertepaaren
 1384 (type/value) ergänzen:

Protokoll- parameter	Parameterwerte gemäß aufgerufener Operation	
<u>Object- Detail</u>	<u>type</u>	<u>value</u>
	<u>ParameterQueryId</u>	<u>Der Wert MUSS der Parameter Query ID gemäß [IHE-ITI-TF3]#3.18.4.1.2.4 entsprechen.</u>
<p><u>Darüberhinaus MUSS jeder gesendete Suchparameter mit Parametername (type) und -wert (value) protokolliert werden. Dabei gelten folgenden Regeln für Werte, die per UND/ODER verknüpft sind (entsprechend [IHE-ITI-TF2a]#3.18.4.1.2.3.5):</u></p> <ul style="list-style-type: none"> <u>Falls innerhalb desselben <Slot> verschiedene <Value>-Elemente innerhalb der <ValueList> gesendet werden (ODER-Verknüpfung), MÜSSEN die Werte protokolliert werden, als wenn sie kommasepariert innerhalb eines einzelnen <Value>-Elements gesendet worden wären. Längenbeschränkungen des Query Schemas auf dem <Value>-Element sind dabei für die entsprechende Transformation außer Kraft gesetzt.</u> <u>Falls derselbe Parametername in mehreren Slots angefragt wird (UND-Verknüpfung), MUSS der Parametername mehrmals (jeweils einmal pro Slot) mit dem jeweils dazugehörigen Wert protokolliert werden.</u> 		
<u>Object- Detail</u>	<u>type</u>	<u>value</u>
	<u>Query Parameter Name (UUID-Format: "urn:uuid:...")</u>	<u>Parameterwert</u>

1385 [**<=**]

1386 Die folgende Tabelle zeigt Beispiele für Parameternamen und -werte, wie sie als Teil des
 1387 Protollierungseintrags für eine FindDocuments-Query
 1388

("ParameterQueryId"="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d")
 protokolliert werden würden. Etwaige weitere Parameter
 wie \$XDSDocumentEntryPatientId werden nicht gezeigt:

type	value
<u>Queryparameter auf einzelnen Wert (Code):</u>	
"\$XDSDocumentEntryFormatCode"	"('urn:gematik:ig:Arztbrief:r3.1^1.3.6.1.4.1.19376.3.276.1.5.6')"
<u>Query auf zwei ODER-verknüpfte Werte:</u>	
Ein Eintrag mit mehreren Werten für den entsprechenden Parameter:	-
"\$XDSDocumentEntryConfidentialityCode"	"('N^2.16.840.1.113883.5.25'), ('R^2.16.840.1.113883.5.25')"
<u>Query auf zwei UND-verknüpfte Werte</u>	
Zwei Einträge für denselben Parameter:	1. " ('H3^1.3.6.1.4.1.19376.3.276.1.5.15')
1. "\$XDSDocumentEntryEventCodeList"	2. " ('E100^1.3.6.1.4.1.19376.3.276.1.5.16')"
2. "\$XDSDocumentEntryEventCodeList"	

Die UND/ODER-Verknüpfung kann entsprechend kombiniert werden (d.h. mehrere Einträge für denselben Parameter und potentiell mehrere Werte pro Eintrag).

A_20144 - Komponente ePA-Dokumentenverwaltung - Aufteilen von Protokolleinträgen für mehrere Dokumente

Bei Operationen, welche die Protokollierung von Details mehrerer Dokumente erfordern, MUSS die Komponente ePA-Dokumentenverwaltung genau einen Protokolleintrag für jedes von der Operation betroffene Dokument anlegen.[<=]

Statt eines einzelnen Protokolleintrags mit Einträgen für bspw. zehn Dokumente werden zehn Protokolleinträge für jeweils ein einzelnes Dokument erzeugt, so als wären alle zehn Dokumente einzeln eingestellt worden. Dies ermöglicht die eindeutige Zuordnung der anzugebenden Dokumentendetails (wie Titel und uniqueId in "Object-ID" und "Object Name") zum jeweiligen Dokument, was in einem "Sammelprotokolleintrag" nicht möglich wäre.

A_20708 - Komponente ePA-Dokumentenverwaltung – Protokollierung gelöschter Ordner für Dokumente des Sammlungstyp "mixed"

Die Komponente ePA-Dokumentenverwaltung MUSS beim Löschen eines Ordners gemäß A_20579 einen Protokolleintrag gemäß A_20538-* vornehmen und dabei für die Parameter "User ID", "User Name" und "Object-ID" die Werte wählen, die für die

1411 Protokollierung der Operation verwendet wurden, welche die Löschung des Ordners
1412 ausgelöst haben. [<=]

1413 Da Ordner des Sammlungstyps "mixed" automatisch vom Aktensystem gelöscht werden
1414 und für den Versicherten die Information relevant ist, dass das letzte zum Ordner
1415 dazugehörige Dokument aus dem Ordner entfernt und damit der Ordner (z. B. der
1416 Mutterpass) selbst gelöscht wurden, wird eine separate Protokollierung hierfür verlangt.
1417 Auslöser der Ordnerlöschvorgangs ist im Protokoll damit derjenige, der das letzte
1418 Dokument aus dem Ordner entfernt hat.

1419 **A_21210 - Komponente ePA-Dokumentenverwaltung – Protokollierung von** 1420 **Metadaten ohne Inhalt**

1421 Die Komponente ePA-Dokumentenverwaltung MUSS bei der Protokollierung von
1422 Metadaten für den Fall, dass die Metadaten keinen Inhalt besitzen bzw. im Request nicht
1423 gesendet wurden, den Inhalt des Metadatums als "" protokollieren. [<=]

1424 Wird beispielsweise das optionale Metadatum DocumentEntry.title im Request vom Client
1425 nicht oder mit leerem Wert ("") gesendet, so wird in beiden Fällen folgendes key-value-
1426 Paar bei der Protokollierung erwartet:
1427 DocumentTitle = ""

1428

1429 **4.6.1 Protokollierung von Berechtigungen**

1430 Falls Berechtigungen angepasst werden, muss die Dokumentenverwaltung noch weitere
1431 Details protokollieren, die es dem Versicherten ermöglichen, den Verlauf der
1432 Berechtigungsvergabe für einzelne Berechtigte nachzuvollziehen. Dabei wird zwischen
1433 dem Einstellen, Aktualisieren und vollständigen Löschen von Berechtigungen
1434 unterschieden.

1435 **A_20564 - Komponente ePA-Dokumentenverwaltung – Protokollierung neuer** 1436 **Berechtigungen**

1437 Die Komponente ePA-Dokumentenverwaltung MUSS bei Zugriffen auf APPC-Policy-
1438 Dokumente (gemäß emSpec_DM_ePA#A_14961) über die Transaktionen

- 1439 • CrossGatewayDocumentProvide
- 1440 • ProvideAndRegisterDocumentSet-b

1441 das Protokoll gemäß A_20538-* um die folgenden Details ergänzen, sofern noch keine
1442 Berechtigung für den von der Policy betroffenen Berechtigten existiert:

Protokollparameter	Parameterwerte beim Einstellen von Policy-Dokumenten	
Object Detail	type	value
	PermAuthorizedID	<p>Wert des Attributs</p> <p>/PolicySet/PolicySet[1]/Target/Subjects/Subject[1] /SubjectMatch/AttributeValue/InstanceIdentifier[@extension]</p> <p>aus der eingestellten Policy (bei LEI die Telematik ID, bei</p>

		Kostenträgern die Betriebsnummer, bei Vertretern die KVNR).
	PermAuthorizedName	<p>Wert des Attributs</p> <p>/PolicySet/PolicySet[1]/Target/Subjects/Subject[2] /SubjectMatch/AttributeValue[@text]</p> <p>aus der eingestellten Policy (bei LEI und Kostenträgern der Organisationsname, bei Vertretern der X.509 Subject Name der eGK).</p>
	PermAccessLevel	Gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.
	PermCategories	Gewährte mittelgranulare Rechte: kommaseparierte Liste von Kategorien (Technischer Identifier gemäß A_19303- 01 -*)
	PermWhitelist	Explizit freigegebene Dokumente (feingranulare Berechtigung): kommaseparierte Liste der uniqueIDs der freigegebenen Dokumente
	PermBlacklist	Explizit gesperrte Dokumente (feingranulare Berechtigung): kommaseparierte Liste der uniqueIDs der gesperrten Dokumente.

1443 [**<=**]

1444 **A_20565 - Komponente ePA-Dokumentenverwaltung – Protokollierung**

1445 **aktualisierter Berechtigungen**

1446 Die Komponente ePA-Dokumentenverwaltung MUSS beim Einstellen von APPC-Policy-

1447 Dokumenten (gemäß emSpec_DM_ePA#A_14961) über die Transaktionen

1448

1449

- CrossGatewayDocumentProvide

1450

- ProvideAndRegisterDocumentSet

1451 das Protokoll gemäß A_20538-~~*~~ um die folgenden Details ergänzen, sofern bereits eine

1452 Berechtigung für den betroffenen Berechtigten existiert, die durch die neue Berechtigung

1453 aktualisiert wird:

Protokollparameter	Parameterwerte beim Aktualisieren von Policy-Dokumenten	
	type	value

Object Detail	PermAuthorizedID	<p>Wert des Attributs</p> <p>/PolicySet/PolicySet[1]/Target/Subjects/Subject[1] /SubjectMatch/AttributeValue/InstanceIdentifier[@extension]</p> <p>aus der eingestellten Policy (bei LEI die Telematik ID, bei Kostenträgern die Betriebsnummer, bei Vertretern die KVNR).</p>
	PermAuthorizedName	<p>Wert des Attributs</p> <p>/PolicySet/PolicySet[1]/Target/Subjects/Subject[2] /SubjectMatch/AttributeValue[@text]</p> <p>aus der eingestellten Policy (bei LEI und Kostenträgern der Organisationsname, bei Vertretern der X.509 Subject Name der eGK).</p>
	PermAccessLevelNew	Neu gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.
	PermAccessLevelOld	Ursprünglich gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.
	PermCategoriesNew	Neu (zusätzlich) gewährte mittelgranulare Rechte: kommaseparierte Liste von Kategorien (Technischer Identifier) gemäß A_19388.
	PermCategoriesRemoved	Ursprünglich gewährte mittelgranulare Rechte, die durch die neue Policy nicht mehr gewährt werden: kommaseparierte Liste von Kategorien (Technischer Identifier) gemäß A_19388.
	PermCategories	Gewährte mittelgranulare Rechte gemäß aktualisierter Policy: kommaseparierte Liste von Kategorien (Technischer Identifier) gemäß A_19388.
	PermWhiteListNew	Neue (zusätzlich) explizit freigegebene Dokumente (feingranulare Berechtigung): kommaseparierte Liste der uniqueIDs der freigegebenen Dokumente.
	PermWhiteListRemoved	Ursprünglich explizit freigegebene Dokumente (feingranulare Berechtigung), die durch die neue Policy nicht mehr explizit freigegeben sind: kommaseparierte Liste der uniqueIDs der freigegebenen Dokumente.

	PermWhitelist	Explizit freigegebene Dokumente (feingranulare Berechtigung) gemäß aktualisierter Berechtigung: kommasseparierte Liste der uniqueIDs der freigegebenen Dokumente.
	PermBlacklistNew	Neue (zusätzlich) explizit gesperrte Dokumente (feingranulare Berechtigung): kommasseparierte Liste der uniqueIDs der gesperrten Dokumente.
	PermBlacklistRemoved	Ursprünglich explizit gesperrte Dokumente (feingranulare Berechtigung), die in der neuen Policy nicht mehr explizit gesperrt sind: kommasseparierte Liste der uniqueIDs der gesperrten Dokumente.
	PermBlackList	Explizit gesperrte Dokumente (feingranulare Berechtigung) gemäß aktualisierter Berechtigung: kommasseparierte Liste der uniqueIDs der gesperrten Dokumente.

1454 [\leq]

1455 **A_20566 - Komponente ePA-Dokumentenverwaltung – Protokollierung**

1456 **gelöschter Berechtigungen**

1457 Die Komponente ePA-Dokumentenverwaltung MUSS beim Löschen von APPC-Policy-

1458 Dokumenten (gemäß emSpec_DM_ePA#A_14961) über die Transaktionen

1459

- 1460 • I_Document_Management_Insurant::RemoveMetadata

1461 das Protokoll gemäß A_20538-~~*~~ um die folgenden Details ergänzen:

1462

Protokollparameter	Parameterwerte beim Löschen von Policy-Dokumenten	
Object Detail	type	value
	PermAuthorizedID	<p>Wert des Attributs</p> <p>/PolicySet/PolicySet[1]/Target/Subjects/Subject[1] /SubjectMatch/AttributeValue/InstanceIdentifier[@extension]</p> <p>aus der eingestellten Policy (bei LEI die Telematik ID, bei Kostenträgern die Betriebsnummer, bei Vertretern die KVNR).</p>
	PermAuthorizedName	<p>Wert des Attributs</p> <p>/PolicySet/PolicySet[1]/Target/Subjects/Subject[2] /SubjectMatch/AttributeValue[@text]</p>

		aus der eingestellten Policy (bei LEI und Kostenträgern der Organisationsname, bei Vertretern der X.509 Subject Name der eGK).
	PermAccessLevel Old	Ursprünglich gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.
	PermCategoriesR emoved	Ursprünglich gewährte mittelgranulare Rechte: kommasseparierte Liste von Kategorien (Technischer Identifier gemäß -A_19303- 01 -*)
	PermWhiteListRe moved	Ursprünglich explizit freigegebene Dokumente (feingranulare Berechtigung): kommasseparierte Liste der uniqueIDs der freigegebenen Dokumente
	PermBlackListRe moved	Ursprünglich explizit gesperrte Dokumente (feingranulare Berechtigung): kommasseparierte Liste der uniqueIDs der gesperrten Dokumente.

[<=]

1465

5 Funktionsmerkmale

5.1 Dokumentenverwaltung

In diesem Abschnitt wird die Außenschnittstelle der IHE ITI-basierten Dokumentenverwaltung festgelegt. Einzelne Umsetzungsanforderungen suggerieren eine vermischte Verarbeitung von Funktionalitäten, welche bei IHE ITI originär getrennt von einer Document Registry und einem Document Repository (bzw. den Responding Gateways) durchgeführt werden. Da die Außenschnittstelle der ePA-Dokumentenverwaltung nicht zwischen Document Registry und Document Repository unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit differenzierten Pfaden siehe [gemSpec_Aktensystem#A_17969]), werden sonst bei IHE ITI explizite Operationen zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne Umsetzung angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-Nachricht kann an IHE ITI-konforme Akteure ausgerichtet werden.

5.1.1 Schnittstelle I_Document_Management

A 14152-01A-14152 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management

Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle implementieren.

Tabelle 6: Tab_Dokv_14 - Schnittstelle I_Document_Management

Schnittstelle	I_Document_Management	
Version	1.0.1	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Cross-Gateway Document Provide	Speichern und Registrieren ein oder mehrerer Dokumente
	Cross-Gateway Query	Abfrage von Metadaten zu registrierten Dokumenten
	Cross-Gateway Retrieve	Anfrage von registrierten Dokumenten
	Remove Documents	Löschen ein oder mehrerer Dokumente

	Remove Metadata	Löschen von Dokumenten oder Ordnern
	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
WSDL	DocumentManagementService.wsdl	
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 	

1484 [\leq]**5.1.1.1 Operation****I_Document_Management::CrossGatewayDocumentProvide****A_14153 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-Gateway Document Provide**

Die Komponente ePA-Dokumentenverwaltung MUSS

die Operation `I_Document_Management::CrossGatewayDocumentProvide` gemäß der folgenden Signatur implementieren:**Tabelle 7: Tab_Dokv_15 - Operation Cross-Gateway Document Provide**

Operation	I_Document_Management::CrossGatewayDocumentProvide		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management::putDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Cross-Gateway Document Provide" [ITI-80] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente mitsamt Metadaten im ePA-Aktensystem dauerhaft zu speichern.		
Formatvorgabe n	SOAP Action: urn:ihe:iti:2015:CrossGatewayDocumentProvide		
Eingangsparameter			
Name	Beschreibung	Typ	opt.

Cross-Gateway Document Provide Message	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution, des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638] oder [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Cross-Gateway Document Provide Response Message	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	rs:RegistryResponse	n
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	
MaxDocSizeExceeded	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines der übermittelten Dokumente übersteigt 25 MByte.	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

1493 [**<=**]

1494 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
 1495 Transaktionen "Cross-Gateway Document Provide" [ITI-80] und "Provide X-User
 1496 Assertion" [ITI-40] sind [IHE-ITI-XCDR], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-
 1497 TF2x] zu entnehmen.

1498 **5.1.1.1.1 Umsetzung**

1499 **A_15055 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung von**
 1500 **gemischten Dokumentenpaketen mit Policy Documents**

1501 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
 1502 MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und
 1503 mit einem XDSRepositoryMetadataError-Fehlercode quittieren, sofern in der
 1504 Eingangsnachricht mehr als ein Dokument und Dokumenten-Metadaten gemäß der

1505 Anforderung [gemSpec_DM_ePA#A_14961] für Policy Documents (Advanced Patient
1506 Privacy Consents) enthalten sind.

1507 [\leq]

1508 **A_14941-03 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung**
1509 **bei Angabe von Document Entry Relationships in Metadaten**

1510 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1511 MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und
1512 mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern die Metadaten die
1513 folgenden Association Types nach [IHE-ITI-TF3#4.2.2] enthalten:

- 1514 • `urn:ihe:iti:2007:AssociationType:XFRM` (Transform)
- 1515 • `urn:ihe:iti:2007:AssociationType:XFRM_RPLC` (Replace with Transformation)
- 1516 • `urn:ihe:iti:2007:AssociationType:signs` (Digital Signature)
- 1517 • `urn:ihe:iti:2010:AssociationType:IsSnapshotOf` (Snapshot of On-Demand
1518 document entry)
- 1519 • `urn:ihe:iti:2010:AssociationType:APND` (Addendum)

1520 [\leq]

1521 **A_13838 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße**
1522 **prüfen**

1523 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1524 MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das SubmissionSet
1525 verarbeitet wird. Die Verarbeitung MUSS abgelehnt werden und mit einem mit
1526 einem `MaxDocSizeExceeded`-bzw. `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-
1527 TF3#4.2.4] quittieren, wenn die Gesamtgröße aller übermittelten Dokumente 250 MByte
1528 übersteigt oder die Größe mindestens eines einzelnen übermittelten Dokuments 25
1529 MByte übersteigt.

1530 [\leq]

1531 Das bedeutet, dass Dokumente bis zu einer Größe von 25 MB = $25 * (1024)^2$ Byte in
1532 die ePA hochgeladen werden. Grundlage für die Berechnung der Dokumentengröße ist
1533 das Dokument ohne Verschlüsselung durch den Dokumentenschlüssel und ohne
1534 Transportcodierung. Größere Dokumente können nicht hochgeladen werden.

1535 **A_13798 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung**
1536 **der Metadaten aus ITI Document Sharing-Profilen durch XCDR-Akteur**
1537 **"Responding Gateway"**

1538 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1539 MUSS die SubmissionSet- sowie die DocumentEntry-Metadaten der eingehenden
1540 Nachricht vor einer Zugriffskontrolle gemäß der Konformität zu den Nutzungsvorgaben in
1541 [gemSpec_DM_ePA#A_14760] prüfen. Die Komponente ePA-Dokumentenverwaltung
1542 als XCDR-Akteur "Responding Gateway" MUSS das Registrieren und Speichern von
1543 Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`-
1544 Fehlercode quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben
1545 sind. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-
1546 Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben
1547 entspricht. [\leq]

1548 **A_13715 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-**
1549 **Gateway Document Provide**

1550 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1551 MUSS die Umsetzung der
1552 Operation `I_Document_Management::CrossGatewayDocumentProvide` bzw. die

1553 Verarbeitung des übermittelten Submission Sets gemäß den definierten Ablauflogiken
 1554 in [IHE-ITI-XCDR#3.80.4.1.2 und 3.80.4.1.3] und [IHE-ITI-XCDR#3.80.4.2.2 und
 1555 3.80.4.2.3] implementieren.[<=]

1556 **A_13657 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für** 1557 **Cross-Gateway Document Provide**

1558 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
 1559 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
 1560 Policy Documents (Advanced Patient Privacy Consents) entsprechend der
 1561 Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt registriert und ein
 1562 Dokument gespeichert wird.[<=]

1563 **5.1.1.2 Operation I_Document_Management::CrossGatewayQuery**

1564 **A_14450 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-** 1565 **Gateway Query**

1566 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 1567 `I_Document_Management::CrossGatewayQuery` gemäß der folgenden Signatur
 1568 implementieren:

1569 **Tabelle 7: Tab_Dokv_16 - Operation Cross-Gateway Query**

Operation	I_Document_Management::CrossGatewayQuery		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management::find technisch um. Sie basiert auf den IHE ITI-Transaktionen "Cross-Gateway Query" [ITI-38] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, Metadaten zu XDS.b-Objekten im ePA-Aktensystem abzufragen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:CrossGatewayQuery		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Cross-Gateway Query Message	Eingangsnachricht zur Suche nach Metadaten zu XDS.b-Objekten	query:AdhocQueryRequest	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.

Cross-Gateway Query Response Message	Ausgangsnachricht zur Suche nach Metadaten zu XDS.b-Objekten	query:AdhocQueryResponse	n
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	

1570

1571 [**<=**]

1572 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
 1573 Transaktionen "Cross-Gateway Document Query" [ITI-38] und "Provide X-User Assertion"
 1574 [ITI-40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
 1575 entnehmen.

1576 5.1.1.2.1 Umsetzung

1577 **A_14924 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe von**
 1578 **Metadaten zu Policy Documents (Advanced Patient Privacy Consents)**

1579 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
 1580 DARF Metadaten zu Policy Documents (Advanced Patient Privacy Consents) gemäß der
 1581 Anforderung [gemSpec_DM_ePA#A_14961] NICHT zurückgeben bzw. MUSS diese aus
 1582 der Antwortnachricht entfernen, falls diese den Anfragekriterien entsprechen.

1583 [**<=**]

1584 Die folgende XACML 2.0 Policy repräsentiert die o.g. Anforderung technisch:

```

1585 <?xml version="1.0" encoding="UTF-8"?>
1586 <Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
1587   PolicyId="urn:uuid:6e84f679-5f36-4861-bfb5-607aef021fff"
1588   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
1589 algorithm:deny-overrides">
1590   <Target>
1591     <Resources>
1592       <Resource>
1593         <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
1594           <AttributeValue DataType="urn:hl7-org:v3#CV">
1595             <CodedValue xmlns="urn:hl7-org:v3" code="57016-8"
1596               codeSystem="1.2.276.0.76.11.32"/>
1597           </AttributeValue>
1598           <ResourceAttributeDesignator
1599             AttributeId="urn:ihe:iti:appc:2016:document-entry:class-code"
1600             DataType="urn:hl7-org:v3#CV" MustBePresent="true"/>
1601           </ResourceMatch>
1602         </Resource>
1603       </Resources>
1604     </Target>
1605     <Rule RuleId="urn:uuid:bb42d632-c70c-447d-94aa-011f2c9561f4"
1606       Effect="Deny"/>

```


</Policy>

A_14910 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-Gateway Query

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS die Umsetzung der Operation `I_Document_Management::CrossGatewayQuery` gemäß der definierten Ablauflogik in [IHE-ITI-TF2b#3.38.4.1.2 und 3.38.4.1.3] implementieren. [<=]

A_17184 - Komponente ePA-Dokumentenverwaltung – Suchanfragen über das Metadatenattribut DocumentEntry.title

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" 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-ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter `$XDSDocumentEntryTitle` unterstützen, sodass eine Suchergebnismenge über das Attribut `XDSDocumentEntry.title` eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter `$XDSDocumentEntryAuthorPerson`. Das `wsa:Action`-Element MUSS den Wert "urn:ihe:iti:2007:CrossGatewayQuery" besitzen. [<=]

A_13585 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Cross-Gateway Query

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt zum Fachmodul ePA als XCA-Akteur "Initiating Gateway" zurückgegeben wird. Widerspricht die Suchergebnismenge ganz oder teilweise einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Suchergebnismenge dahingehend gefiltert werden, dass nur berechtigte Metadaten (d.h. Document Entries sowie Submission Sets) an den Document Consumer zurückgegeben werden. [<=]

A_18069 - Komponente ePA-Dokumentenverwaltung – Suche über Author Institution bei Cross-Gateway Query

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS für den Anfragetyp "FindDocumentsByTitle" den weiteren optionalen Parameter `$XDSDocumentEntryAuthorInstitution` verarbeiten können, sodass eine Suchergebnismenge über den `authorInstitution`-Slot der `XDSDocumentEntry.authorClassification` (Wertemenge des `authorInstitution`-Sub-Attributs) eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter `$XDSDocumentEntryAuthorPerson`. [<=]

A_21131 - Komponente ePA-Dokumentenverwaltung – Rückgabe unscharfer Suchergebnisse für Cross-Gateway-Query

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" SOLL bei der Ermittlung der Ergebnisse einer Cross-Gateway Query bei Verwendung der folgenden Suchparameter in der Query-Anfragenachricht beim Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d.h. bezogen auf das jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht abweichende Ergebnisse zurückliefern:

- `$XDSDocumentEntryTitle`
- `$XDSDocumentEntryAuthorInstitution`

- [\\$XDSDocumentEntryAuthorPerson](#)

- [\\$XDSSubmissionSetAuthorPerson](#)

[<=]

Das zur Ermittlung unscharfer Ergebnisse von der Dokumentenverwaltung 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") oder Nichtbeachtung von Groß-/Kleinschreibung vorenthalten worden wäre.

5.1.1.3 Operation I Document Management::RemoveDocuments (abgekündigt)

Die Operation removeDocuments wird aus Kompatibilitätsgründen weiterhin angeboten. Ziel ist es diese Operation in späteren Releases nicht mehr zu unterstützen. Die Operation removeMetadata löst die Operation removeDocuments ab.

A 21183 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove Documents

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I Document Management::RemoveDocuments` gemäß der folgenden Signatur implementieren:

Tabelle 8: Tab Dokv 17 - Operation Remove Documents

<u>Operation</u>	<u>I Document Management::RemoveDocuments</u>		
<u>Beschreibung</u>	<u>Diese Operation setzt die in [gemSysL ePA] definierte Operation I Document Management::deleteDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove Documents" [ITI-86] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente eines Aktenkontos im ePA-Aktensystem zu löschen.</u>		
<u>Formatvorgaben</u>	<u>SOAP Action: urn:ihe:iti:2017:RemoveDocuments</u>		
<u>Eingangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt</u>
<u>Remove Documents Message</u>	<u>Eingangsnachricht zum Löschen ein oder mehrerer Dokumente</u>	<u>rmd:RemoveDocuments Message</u>	<u>n</u>
<u>X-User Assertion</u>	<u>Authentication Assertion der authentifizierten Leistungserbringereinstitution</u>	<u>SAML 2.0 Assertion gemäß [gemSpec FM ePA#A 14927, A 15638]</u>	<u>n</u>

<u>Ausgangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt</u>
<u>Remove Documents Response Message</u>	<u>Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente</u>	<u>rmd:RemoveDocumentsResponse Message</u>	<u>n</u>
<u>Technische Fehlermeldungen</u>			
<u>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</u>			
<u>Name</u>	<u>Fehlertext</u>	<u>Details</u>	

[<=]

Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-Transaktionen "RemoveDocuments" [ITI-86] und "Provide X-User Assertion" [ITI-40] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5.1.1.3.1 Umsetzung**A_21184 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Documents**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Umsetzung der Operation `I_Document_Management::RemoveDocuments` gemäß der definierten Ablauflogik in [IHE-ITI-RMD#3.86.4.1.2 und 3.86.4.1.3] implementieren.

[<=]**5.1.1.3.5.1.1.4 Operation `I_Document_Management::RemoveMetadata`****A_14489-01 - Komponente ePA-Dokumentenverwaltung – Signatur für RemoveMetadata**

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I_Document_Management::RemoveMetadata` gemäß der folgenden Signatur implementieren:

Tabelle 9: Tab_Dokv_17 - Operation RemoveMetadata

Operation	<code>I_Document_Management::RemoveMetadata</code>
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management::deleteDocuments</code> technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove Metadata" [ITI-62] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl.

	umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente eines Aktenkontos im ePA-Aktensystem zu löschen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2010:DeleteDocumentSet		
Eingangsparameter			
Name	Beschreibung	Typ	optional
Remove Documents Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	xds:DeleteDocumentSet_Message	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
Ausgangsparameter			
Name	Beschreibung	Typ	optional
Remove Documents Response Message	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	xds:DeleteDocumentSetResponse_Message	n
Technische Fehlermeldungen			
<i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	

1697 [**<=**]

1698 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1699 Transaktionen "RemoveMetadata" [ITI-62] und "Provide X-User Assertion" [ITI-
1700 40] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

1701 [5.1.1.3.15.1.1.4.1](#) Umsetzung

1702 **A_14908-01 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für**
1703 **Remove Metadata**

1704 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1705 die Umsetzung der Operation `I_Document_Management::RemoveMetadata` gemäß der

1706 definierten Ablauflogik in [IHE-ITI-RMD#3.86.4.1.2 und 3.86.4.1.3]
 1707 implementieren. [<=]

1708
 1709 ~~**A_20713 – Komponente ePA-Dokumentenverwaltung – Remove Metadata mit**~~
 1710 ~~**uniqueIds (Übergangsphase)**~~
 1711 ~~Falls in der Anfragenachricht zu `I_Document_Management::RemoveMetadata` im Feld~~
 1712 ~~`/RemoveObjectsRequest/ObjectRefList/ObjectRef[@id]` anstelle einer `entryUUID` eine~~
 1713 ~~`uniqueId` gesendet wird, MUSS die Komponente ePA-Dokumentenverwaltung als XDS-~~
 1714 ~~Akteur "Document Registry" die Operation gemäß A_14908-01 durchführen, als wenn~~
 1715 ~~stattdessen dort die `DocumentEntry.entryUUID` des Dokuments hinterlegt wäre, dessen~~
 1716 ~~`DocumentEntry.uniqueId` der gesendeten `uniqueId` entspricht. [<=]~~

1717 **A_20633 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für** 1718 **Remove Metadata**

1719 Die Komponente ePA-Dokumentenverwaltung als RMD-Akteur "Document Registry"
 1720 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
 1721 Policy Documents (Advanced Patient Privacy Consents) entsprechend der
 1722 Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt (und ein ggf.
 1723 dazugehöriges Dokument) gelöscht wird. [<=]

1724 **5.1.1.45.1.1.5 Operation**

1725 **I_Document_Management::CrossGatewayRetrieve**

1726 **A_14464 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-** 1727 **Gateway Retrieve**

1728 Die Komponente ePA-Dokumentenverwaltung MUSS
 1729 die Operation `I_Document_Management::CrossGatewayRetrieve` gemäß der folgenden
 1730 Signatur implementieren:

1731 **Tabelle 10: Tab_Dokv_18 - Operation Cross-Gateway Retrieve**

Operation	I_Document_Management::CrossGatewayRetrieve		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management::getDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Cross-Gateway Retrieve" [ITI-39] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente aus dem ePA-Aktensystem abzufragen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:CrossGatewayRetrieve		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Cross-Gateway Retrieve Message	Eingangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetRequest	n

X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringereinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt
Cross-Gateway Retrieve Response Message	Ausgangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetResponse	n
Technische Fehlermeldungen Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.			
Name	Fehlertext	Details	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße der angefragten Dokumente übersteigt 250 MByte.	

1732 [\leq]

1733 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1734 Transaktionen "Cross-Gateway Document Retrieve" [ITI-39] und "Provide X-User
1735 Assertion" [ITI-40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-
1736 TF2x] zu entnehmen.

1737 5.1.1.4-15.1.1.5.1 Umsetzung

1738 **A_14911 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-**
1739 **Gateway Retrieve**

1740 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
1741 MUSS die Umsetzung der Operation `I_Document_Management::CrossGatewayRetrieve`
1742 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.39.4.1.2 und 3.39.4.1.3] und
1743 [IHE-ITI-TF2b#3.39.4.2.2 und 3.39.4.2.3] implementieren. [\leq]

1744 **A_16201 - Komponente ePA-Dokumentenverwaltung – Prüfung der**
1745 **zurückgegebenen Paketgröße**

1746 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
1747 MUSS anhand der übergebenen DocumentUniqueIDs die Gesamtgröße ermitteln und bei
1748 Überschreitung von 250 MByte die Verarbeitung ablehnen und die Nachricht mit
1749 einem `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.
1750 [\leq]

1751 **A_14548-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement**
1752 **für Cross-Gateway Retrieve**

1753 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
1754 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
1755 Policy Documents (Advanced Patient Privacy Consents) entsprechend der

Anforderung A_14822 durchsetzen, bevor ein Repository-Datenobjekt zum Fachmodul ePA als XCA-Akteur "Initiating Gateway" zurückgegeben wird. Bei einem Abruf von mehreren Dokumenten können einzelne Dokumente durch den zwischenzeitlichen Entzug einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für den Abruf berechtigt sein. Widerspricht ein abzurufendes Dokument einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum betreffenden Dokument einen `XSDocumentUniqueIdError`-Fehlercode enthalten (das Dokument wird nicht herausgegeben) und der Wert 4 des `EventOutcomeIndicators` im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein angefordertes Dokument nicht mehr verfügbar (d.h. es wurde gelöscht), MUSS gemäß IHE ITI der Fehlercode `XSDocumentUniqueIdError` zurückgegeben werden. [\leq]

5.1.1.6 Operation

I Document Management::RestrictedUpdateDocumentSet

Die Operation `I Document Management::RestrictedUpdateDocumentSet` wird aus Kompatibilitätsgründen weiterhin angeboten. Ziel ist es, diese Operation in späteren Releases nicht mehr zu unterstützen. Die Operation liefert bei jedem Aufruf einen wohldefinierten Fehler zurück, da die früher (ePA bis Release 3.1.3) ausgelöste Funktionalität nicht mehr durch ePA ab Release 4 unterstützt wird.

A 21190 - Komponente ePA-Dokumentenverwaltung – Signatur für Restricted Update Document Set

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I Document Management::RestrictedUpdateDocumentSet` gemäß der folgenden Signatur implementieren:

Tabelle 11: Tab Dokv_45 - Operation Restricted Update Document Set

Operation	<u>I Document Management::RestrictedUpdateDocumentSet</u>
Beschreibung	<p>Diese Operation setzt die in [gemSysL ePA] definierte Operation <code>I_PHR_Management::updateMetadata</code> technisch um. Sie basiert auf den IHE ITI-Transaktionen "Restricted Update Document Set" [ITI-92] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, Metadaten zu Dokumenten zu ändern.</p> <p>Die Operation wurde in früheren ePA-Releases dazu genutzt, Dokumente von Versicherten oder Kostenträger als "leistungserbringeräquivalent" zu kennzeichnen oder eine entsprechende Kennzeichnung zu entfernen. Da eine entsprechende Kennzeichnung nicht mehr möglich ist, liefert der Aufruf der Operation nun in jedem Fall einen Fehler zurück.</p>
Formatvorgabe	SOAP Action: <code>urn:ihe:iti:2018:RestrictedUpdateDocumentSet</code>

<u>Eingangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt</u> :
<u>Update Responder Restricted Update Document Set</u>	<u>Eingangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten</u>	<u>lcm:SubmitObjectsRequest</u>	<u>n</u>
<u>X-User Assertion</u>	<u>Authentication Assertion der authentifizierten Leistungserbringerinstitution</u>	<u>SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_149_27, A_15638]</u>	<u>n</u>
<u>Ausgangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt</u> :
<u>Update Responder Restricted Update Document Set Response</u>	<u>Ausgangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten</u>	<u>rs:RegistryResponse</u>	<u>n</u>
<u>Technische Fehlermeldungen</u>			
<u>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</u>			
<u>Name</u>	<u>Fehlertext</u>	<u>Details</u>	

Weitere Details zur Ausgestaltung dieser Operation finden sich in ePA Release 3.1.3 und bezüglich der dazugehörigen IHE ITI-Transaktionen "RestrictedUpdateDocumentSet" [ITI-92] und "Provide X-User Assertion" [ITI-40] in [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x].[<=]

5.1.1.6.1 Umsetzung

A 21191 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Restricted Update Document Set

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF NICHT die Umsetzung der

Operation I Document Management::RestrictedUpdateDocumentSet gemäß der definierten Ablauflogik in [IHE-ITI-RMU#3.92.4.1.2 und 3.92.4.1.3] implementieren. [≤]

D.h. insbesondere, dass die Komponente ePA-Dokumentenverwaltung keinerlei Metadaten aktualisieren darf.

A 21192 - Komponente ePA-Dokumentenverwaltung – Fehler für Restricted Update Document Set

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS beim Aufruf der

Operation I Document Management::RestrictedUpdateDocumentSet immer den folgenden Fehler zurückliefern:

- Der übergeordnete rs:RegistryResponse/@status MUSS den Wert rn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure besitzen.
- Für jedes darin ggf. enthaltene rs:RegistryResponse/rs:RegistryErrorList/rs:RegistryError Element MUSS die folgende Belegung gewählt werden:
 - @severity=urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Error gemäß [IHE-ITI-RMU#3.92.4.2.2]
 - @errorCode=UnmodifiableMetadataError gemäß [IHE-ITI-RMU#4.2.4.1]
 - @codeContext MUSS mit dem Wert "Fehler für Dokument mit Kennung \$entryUUID: Ein Metadatenupdate ist in dieser ePA-Version nicht möglich." belegt werden, wobei \$entryUUID der DocumentEntry.entryUUID des jeweiligen Dokuments entspricht, für das die Metadatenaktualisierung angefragt wurde.

[≤]

5.1.2 Schnittstelle I_Document_Management_Insurant

A_14478 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management_Insurant

Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle implementieren.

Tabelle 12: Tab_Dokv_20 - Schnittstelle I_Document_Management_Insurant

Schnittstelle	I_Document_Management_Insurant	
Version	1.0.1	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung

	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente in der Dokumentenverwaltung
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Documents	Löschen ein oder mehrerer Dokumente
WSDL	DocumentManagementService.wsdl	
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 	

1824
1825 [\leq]

1826 5.1.2.1 Operation

1827 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b

1828 A_14479 - Komponente ePA-Dokumentenverwaltung – Signatur für Provide And

1829 Register Document Set-b

1830 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

1831 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b gemäß der

1832 folgenden Signatur implementieren:

1833 **Tabelle 13: Tab_Dokv_21 - Operation Provide And Register Document Set-b**

Operation	I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::putDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Provide And Register Document Set-b" [ITI-41] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation

	erlaubt es, ein oder mehrere Dokumente mitsamt Metadaten im ePA-Aktensystem dauerhaft zu speichern.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b		
Eingangsparameter			
Name	Beschreibung	Typ	optional
Provide And Register Document Set-b Message	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	no
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers# A_14109, A_15631]	no
Ausgangsparameter			
Name	Beschreibung	Typ	optional
Provide And Register Document Set-b Response Message	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	rs:RegistryResponse	no
Technische Fehlermeldungen			
<i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	
MaxDocSizeExceeded	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines einzelnen übermittelten Dokuments übersteigt 25 MByte.	

MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.
---------------------------	--	---

[<=]

Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-Transaktionen "Provide And Register Document Set-b" [ITI-41] und "Provide X-User Assertion" [ITI-40] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5.1.2.1.1 Umsetzung

A_15056 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung von gemischten Dokumentenpaketen mit Policy Documents

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern in der Eingangsnachricht mehr als ein Dokument und Dokumenten-Metadaten gemäß der Anforderung [gemSpec_DM_ePA#A_14961] für Policy Documents (Advanced Patient Privacy Consents) enthalten sind.[<=]

A_14912 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide And Register Document Set-b

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Umsetzung der Operation `I_Document_Management_Insurant::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_16442 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht. [<=]

5.1.2.2 Operation

I_Document_Management_Insurant::RegistryStoredQuery

A_14480 - Komponente ePA-Dokumentenverwaltung – Signatur für Registry Stored Query

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I_Document_Management_Insurant::RegistryStoredQuery` gemäß der folgenden Signatur implementieren:

Tabelle 14: Tab_Dokv_22 - Operation Registry Stored Query

Operation	<code>I_Document_Management_Insurant::RegistryStoredQuery</code>
-----------	--

Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::find technisch um. Sie basiert auf den IHE ITI-Transaktionen "Registry Stored Query" [ITI-18] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, Metadaten zu XDS.b-Objekten im ePA-Aktensystem abzufragen.		
Formatvorgabe n	SOAP Action: urn:ihe:iti:2007:RegistryStoredQuery		
Eingangsparameter			
Name	Beschreibung	Typ	opt .
Registry Stored Query Message	Eingangsnachricht zur Suche nach Metadaten zu XDS.b-Objekten	query:AdhocQueryRequest	n
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt .
Registry Stored Query Response Message	Ausgangsnachricht zur Suche nach Metadaten zu XDS.b-Objekten	query:AdhocQueryResponse	n
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	

1872

1873 [**<=**]

1874 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
 1875 Transaktionen "Registry Stored Query" [ITI-18] und "Provide X-User Assertion" [ITI-

1876 40] sind [IHE-ITI-TF2a], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1877 entnehmen.

1878 5.1.2.2.1 Umsetzung

1879 **A_14913 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Registry** 1880 **Stored Query**

1881 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1882 die Umsetzung der

1883 Operation `I_Document_Management_Insurant::RegistryStoredQuery` gemäß der
1884 definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3]
1885 implementieren. [`<=`]

1886 **A_16436 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender** 1887 **X-User Assertion**

1888 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1889 die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren, falls
1890 die X-User Assertion nicht dem SAML 2.0 Assertion Profil
1891 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
1892 [`<=`]

1893 **A_17185 - Komponente ePA-Dokumentenverwaltung – Suchanfragen über das** 1894 **Metadatenattribut DocumentEntry.title**

1895 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1896 einen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID
1897 "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben
1898 Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-
1899 ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter
1900 `$XSDDocumentEntryTitle` unterstützen, sodass eine Suchergebnismenge über das
1901 Attribut `XSDDocumentEntry.title` eingeschränkt werden kann. Weiterhin MUSS dieselbe
1902 Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den
1903 Parameter `$XSDDocumentEntryAuthorPerson`. Das `wsa:Action-Element` MUSS den Wert
1904 "urn:ihe:iti:2007:RegistryStoredQuery" besitzen.
1905 [`<=`]

1906 **A_14588 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für** 1907 **Registry Stored Query**

1908 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1909 die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy
1910 Documents (Advanced Patient Privacy Consents) entsprechend der
1911 Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt zum ePA-Frontend
1912 des Versicherten (XDS-Akteur "Document Consumer") zurückgegeben wird.

1913
1914 [`<=`]

1915 **A_20532 - Komponente ePA-Dokumentenverwaltung – Zugriff auf** 1916 **SubmissionSets bei der Suche**

1917 Die Komponente ePA-Dokumentenverwaltung MUSS einen Zugriff auf ein `SubmissionSet`
1918 im Rahmen der Operationen `I_Document_Management::CrossGatewayQuery` sowie
1919 `I_Document_Management_Insurant::RegistryStoredQuery` unterbinden, wenn der
1920 Zugreifende nicht mindestens für ein Dokument darin berechtigt ist.
1921 [`<=`]

1922 **A_20533 - Komponente ePA-Dokumentenverwaltung – Zugriff auf Folder bei der** 1923 **Suche**

1924 Die Komponente ePA-Dokumentenverwaltung MUSS einen Zugriff auf einen Folder im
1925 Rahmen der Operationen `I_Document_Management::CrossGatewayQuery` sowie

1926 I_Document_Management_Insurant::RegistryStoredQuery unterbinden, wenn der
1927 Zugreifende nicht für mindestens ein Dokument darin berechtigt ist.[<=]

1928 **A_20534 - Komponente ePA-Dokumentenverwaltung – Zugriff auf Associations** 1929 **bei der Suche**

1930 Die Komponente ePA-Dokumentenverwaltung MUSS einen Zugriff auf Associations im
1931 Rahmen der Operationen I_Document_Management::CrossGatewayQuery sowie
1932 I_Document_Management_Insurant::RegistryStoredQuery unterbinden, wenn der
1933 Zugreifende nicht für beide Endpunkte der Association (DocumentEntries,
1934 SubmissionSets, Folder) berechtigt ist.[<=]

1935 **A_20535 - Komponente ePA-Dokumentenverwaltung – Fehlerbehandlung bei** 1936 **fehlender Berechtigung auf SubmissionSets, Folders und Associations bei der** 1937 **Suche**

1938 Die Komponente ePA-Dokumentenverwaltung MUSS bei einem Zugriff auf
1939 SubmissionSets, Folders und Associations (kurz allgemein: Objekt), für die keine
1940 Zugriffsberechtigung besteht, wie folgt reagieren:

- 1941 • Wird das Objekt über seine eindeutige Kennung (uniqueId, entryUUID)
1942 angefordert, MUSS die Dokumentenverwaltung denselben Fehler zurückgeben,
1943 den sie zurückgeben würde, wäre das Objekt tatsächlich nicht vorhanden.
- 1944 • Ist das Objekt anderweitig Teil der (vorläufigen) Ergebnismenge, MUSS die
1945 Dokumentenverwaltung das Objekt vor Rückgabe aus der endgültigen
1946 Ergebnismenge entfernen und DARF NICHT für dieses Objekt einen expliziten
1947 Fehler senden.

1948 [<=]

1949 Damit soll analog zum nichtberechtigten Zugriffsversuch auf Dokumente erreicht werden,
1950 dass ein Angreifer keine Information über die Existenz oder die Natur eines Objekts
1951 erhält, für das er keine Zugriffsberechtigung besitzt.

1952 **A_18070 - Komponente ePA-Dokumentenverwaltung – Suche über Author** 1953 **Institution bei Registry Stored Query**

1954 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1955 für den Anfragetyp "FindDocumentsByTitle" den weiteren optionalen Parameter
1956 \$XDSDocumentEntryAuthorInstitution verarbeiten können, sodass eine
1957 Suchergebnismenge über den authorInstitution-Slot der XDSDocumentEntry.author-
1958 Classification (Wertemenge des authorInstitution-Sub-Attributs) eingeschränkt werden
1959 kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein,
1960 wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson.[<=]

1961 Die folgende Anforderung ermöglicht

1962 **A_21132 - Komponente ePA-Dokumentenverwaltung – Rückgabe unscharfer** 1963 **Suchergebnisse bei Registry Stored Query**

1964 Die Komponente ePA-Dokumentenverwaltung als als XDS-Akteur "Document Registry"
1965 SOLL bei der Ermittlung der Ergebnisse einer Registry Stored Query bei Verwendung der
1966 folgenden Suchparameter in der Query-Anfragenachricht beim Durchsuchen des
1967 dazugehörigen Suchfelds auch unscharfe, d.h. bezogen auf das jeweilige Suchfeld nicht
1968 nur exakt auf die Metadaten passende, sondern auch leicht abweichende Ergebnisse
1969 zurückliefern:

- 1970 • \$XDSDocumentEntryTitle
- 1971 • \$XDSDocumentEntryAuthorInstitution
- 1972 • \$XDSDocumentEntryAuthorPerson
- 1973 • \$XDSSubmissionSetAuthorPerson

1974 [**<=**]

1975 Das zur Ermittlung unscharfer Ergebnisse von der Dokumentenverwaltung einzusetzende
1976 Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu liefern, die ihm
1977 möglicherweise sonst wegen beispielsweise falscher Schreibweise eines Namens (z. B.
1978 "Meyer" vs. "Maier") oder Nichtbeachtung von Groß-/Kleinschreibung vorenthalten
1979 worden wäre.

1981 5.1.2.2.1.1 Suche mit simulierter Berechtigung

1982 Die folgenden Anforderungen ermöglichen es Clients, eine Suche im "Namen" einer LEI
1983 oder eines KTR durchzuführen. Dies ist nützlich, um etwaige Berechtigungsvergaben zu
1984 prüfen. Die Anfrage eignet sich also auch, um im Vorfeld eine potentielle
1985 Berechtigungsvergabe "durchzuspielen".

1986 ~~5.1.2.2.1.11.1.1.1.1.1.1 Suche mit simulierter Berechtigung~~

1988 **A_20224 - Komponente ePA-Dokumentenverwaltung – Suche mit simulierter** 1989 **Berechtigung: Anfrageformat**

1990 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1991 für alle Anfragen ("Stored Queries") den optionalen Parameter \$impersonatePolicy
1992 verarbeiten können. Die Komponente ePA-Dokumentenverwaltung prüft dazu die
1993 folgenden Bestimmungen:

- 1994 • Der Parameter wird als Slot mit dem Namen `impersonatePolicy` kodiert.
- 1995 • Der Parameter MUSS eine vollständige Base Policy für eine LEI (gemäß [9.3](#)) oder
1996 eines Kostenträgers (gemäß [9.4](#)) enthalten.
- 1997 • Der Wert (die XML-Policy) MUSS Base64-kodiert im Datentyp `String` gemäß [IHE-
1998 ITI-TF3] abgelegt werden
- 1999 • Der Parameter (sofern gesendet) MUSS immer die Multiplizität 1 besitzen.
- 2000 • Wenn der Parameter nicht genutzt wird, dann DARF der entsprechende Slot nicht
2001 gesendet werden (d. h. es darf nicht stattdessen ein leerer Wert gesendet
2002 werden).

2003 [**<=**]

2004 **A_20227 - Komponente ePA-Dokumentenverwaltung – Suche mit simulierter** 2005 **Berechtigung: Umsetzung**

2006 Die in A_20224 definierte Suche MUSS wie folgt umgesetzt werden:

- 2007 • Wenn die in A_20224 genannten Bestimmungen nicht erfüllt sind, MUSS die
2008 Komponente ePA-Dokumentenverwaltung einen Fehler zurückgeben
2009 (`ResponseStatusType:Failure`).
- 2010 • Ansonsten gelten folgende Bestimmungen:
 - 2011 • Die Komponente ePA-Dokumentenverwaltung MUSS die im Base64-Format
2012 enthaltene Policy dekodieren.
 - 2013 • Die Komponente ePA-Dokumentenverwaltung DARF das Policy-Dokument
2014 NICHT in der Dokumentenverwaltung hinterlegen. Sie wird also für andere
2015 Anfragen an die Schnittstellen der Dokumentenverwaltung nicht beachtet.
 - 2016 • Die Komponente ePA-Dokumentenverwaltung DARF NICHT ein anderes
2017 (etwaig hinterlegtes) Base Policy Dokument für dieselbe LEI oder KTR im
2018 Rahmen dieser Suche beachten.

- 2019 • Die Komponente ePA-Dokumentenverwaltung MUSS die Klartextpolicy gemäß
 2020 5.4.6 behandeln und bei erfolgreicher Zugriffskontrollprüfung ("Permit") die
 2021 Suche wie in 5.1.2.2 beschrieben unter Beachtung der Policy umsetzen.

2022 [\leq]

2023 5.1.2.3 Operation **I_Document_Management_Insurant::RemoveMetadata** 2024 **A_14488-01 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove** 2025 **Metadata**

2026 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 2027 **I_Document_Management_Insurant::RemoveMetadata** gemäß der folgenden Signatur
 2028 implementieren:

2029 **Tabelle 15: Tab_Dokv_23 - Operation RemoveMetadata**

Operation	I_Document_Management_Insurant::RemoveMetadata		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::deleteDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove Metadata" [ITI-62] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente im ePA-Aktensystem zu löschen.		
Formatvorgabe n	SOAP Action: urn:ihe:iti:2010:DeleteDocumentSet		
Eingangsparameter			
Name	Beschreibung	Typ	opt .
Remove Metadata Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	xds:DeleteDocumentSet_Message	n
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt .
Remove Metadata	Ausgangsnachricht zum Löschen ein	xds:DeleteDocumentSetResponse_Messag e	n

Response Message	oder mehrerer Dokumente		
Technische Fehlermeldungen Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.			
Name	Fehlertext	Details	

2030
2031

[<=]

2032 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
2033 Transaktionen "RemoveMetadata" [ITI-62] und Provide X-User Assertion [ITI-
2034 40] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

2035 5.1.2.3.1 Umsetzung

2036 **A_14909-01 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für** 2037 **Remove Metadata**

2038 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2039 MUSS die Umsetzung der
2040 Operation `I_Document_Management_Insurant::RemoveMetadata` gemäß der definierten
2041 Ablauflogik in [IHE-ITI-RMD#3.86.4.1.2 und 3.86.4.1.3] implementieren.[<=]

2042 **A_16437-01 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht** 2043 **passender X-User Assertion**

2044 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2045 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren,
2046 falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
2047 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
2048 [<=]

2049 **5.1.2.4 Operation** 2050 **I_Document_Management_Insurant::RetrieveDocumentSet**

2051 **A_14481 - Komponente ePA-Dokumentenverwaltung – Signatur für Retrieve** 2052 **Document Set**

2053 Die Komponente ePA-Dokumentenverwaltung MUSS
2054 die Operation `I_Document_Management_Insurant::RetrieveDocumentSet` gemäß der
2055 folgenden Signatur implementieren:

2056 **Tabelle 16: Tab_Dokv_24 - Operation Retrieve Document Set**

Operation	I_Document_Management_Insurant::RetrieveDocumentSet
------------------	--

Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::getDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Retrieve Document Set" [ITI-43] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente aus dem ePA-Aktensystem abzufragen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:RetrieveDocumentSet		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Retrieve Document Set Message	Eingangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetRequest	n
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Retrieve Document Set Response Message	Ausgangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetResponse	n
Technische Fehlermeldungen			
<i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße der angefragten Dokumente übersteigt 250 MByte.	

2057
2058

[<=]

2059 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
2060 Transaktionen "RetrieveDocumentSet" [ITI-43] und "Provide X-User Assertion" [ITI-
2061 40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
2062 entnehmen.

2063 5.1.2.4.1 Umsetzung

2064 **A_14914 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Retrieve** 2065 **Document Set**

2066 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2067 MUSS die Umsetzung der
2068 Operation `I_Document_Management_Insurant::RetrieveDocumentSet` gemäß den
2069 definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3] und [IHE-ITI-
2070 TF2b#3.43.4.2.2 und 3.43.4.2.3] implementieren.[<=]

2071 **A_16443 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender** 2072 **X-User Assertion**

2073 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2074 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren,
2075 falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
2076 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
2077 [<=]

2078 **A_16200 - Komponente ePA-Dokumentenverwaltung – Prüfung der** 2079 **zurückgegebenen Paketgröße**

2080 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2081 MUSS anhand der übergebenen `DocumentUniqueIDs` die Gesamtgröße ermitteln und bei
2082 Überschreitung von 250 MByte die Verarbeitung ablehnen und die Nachricht mit
2083 einem `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.
2084 [<=]

2085 **A_14589 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für** 2086 **Retrieve Document Set**

2087 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2088 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
2089 Policy Documents (Advanced Patient Privacy Consents) entsprechend der
2090 Anforderung A_14822 durchsetzen, bevor ein Repository-Datenobjekt zum ePA-Frontend
2091 des Versicherten als XDS-Akteur "Document Consumer" zurückgegeben wird. Ist ein
2092 abzurufendes Dokument nicht mehr verfügbar, MUSS gemäß IHE TF ITI der
2093 Fehlercode `XDSDocumentUniqueIdError` zurückgegeben werden.

2094
2095 [<=]

2096 5.1.2.5 Operation

2097 **I_Document_Management_Insurant::RestrictedUpdateDocumentSet**

2098 **A_15057-01 - Komponente ePA-Dokumentenverwaltung – Signatur für** 2099 **Restricted Update Document Set**

2100 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
2101 `I_Document_Management_Insurant::RestrictedUpdateDocumentSet` gemäß der
2102 folgenden Signatur implementieren:

2103

Tabelle 17: Tab_Dokv_19 - Operation RestrictedUpdateDocumentSet

Operation	I_Document_Management_Insurant::RestrictedUpdateDocumentSet		
Beschreibung	<p>Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::updateMetadata technisch um. Sie basiert auf den IHE ITI-Transaktionen "Restricted Update Document Set" [ITI-92] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, Metadaten zu Dokumenten zu ändern.</p> <p>Für Änderungen an der Vertraulichkeitsstufe von Dokumenten werden im documentEntry.confidentialityCode die Werte "normal", "restricted" oder "very restricted" mit derupdateMetadata Operation umgesetzt. Andere Änderungen sind mit dieser Operation nicht möglich.</p>		
Formatvorgabe n	SOAP Action: urn:ihe:iti:2018:RestrictedUpdateDocumentSet		
Eingangsparameter			
Name	Beschreibung	Typ	opt .
Update Responder Restricted Update Document Set	Eingangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	lcm:SubmitObjectsRequest	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_149 27, A_15638]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt .
Update Responder Restricted Update Document Set Response	Ausgangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	rs:RegistryResponse	n
Technische Fehlermeldungen			
Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert,			

welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.

2104
2105

[<=]

2106 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
2107 Transaktionen "RestrictedUpdateDocumentSet" [ITI-92] und "Provide X-User Assertion"
2108 [ITI-40] sind [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
2109 entnehmen.

2110 5.1.2.5.1 Umsetzung

2111 **A_15082 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung** 2112 **der Metadaten aus ITI Document Sharing-Profilen durch RMU-Akteur "Update** 2113 **Responder"**

2114 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
2115 die übermittelten DocumentEntry-Metadaten der eingehenden Nachricht dahingehend
2116 prüfen, dass gegenüber den Bestandsdaten das
2117 Metadatenattribut `documentEntry.confidentialityCode` konform zu den
2118 Nutzungsvorgaben in [gemSpec_DM_ePA#A_14760] geändert ist. Die Komponente ePA-
2119 Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS das Aktualisieren
2120 dieses Metadatenattributs ablehnen und mit einem `XDSRepositoryMetadataError`
2121 quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind.[<=]

2122 **A_15083-01 - Komponente ePA-Dokumentenverwaltung – Prüfung auf** 2123 **ausschließliche Aktualisierung des Metadatenattributs** 2124 **`documentEntry.confidentialityCode`**

2125 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
2126 die übermittelten DocumentEntry-Metadaten der eingehenden Nachricht dahingehend
2127 prüfen, dass gegenüber den Bestandsdaten ausschließlich das
2128 Metadatenattribut `documentEntry.confidentialityCode` geändert werden soll . Es ist
2129 nur das Ändern von Confidentiality Codes "normal", "restricted" und "very
2130 restricted" in einen anderen dieser Werte erlaubt. Wenn andere Aktualisierungen für
2131 die übermittelten Metadatenattribute in der Eingangsnachricht enthalten sind, MUSS die
2132 Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" die
2133 Weiterverarbeitung abbrechen und die Nachricht mit
2134 einem `LocalPolicyRestrictionError`-Fehlercode quittieren.

2135 [<=]

2136

2137

2138 **A_15061-01 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für** 2139 **Restricted Update Document Set**

2140 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
2141 die Umsetzung der
2142 Operation `I_Document_Management_Insurant::RestrictedUpdateDocumentSet` gemäß
2143 der definierten Ablauflogik in [IHE-ITI-RMU#3.92.4.1.2 und 3.92.4.1.3]
2144 implementieren und sicherstellen, dass (nur) die folgenden Metadatenobjekte gesendet
2145 werden:

- 2146 • Ein neues `SubmissionSet`
- 2147 • Einen `DocumentEntry`, der identisch mit dem zu aktualisierenden `DocumentEntry`
2148 identisch ist (inklusive `entryUUID`) und sich nur im `confidentialityCode` unterscheidet
- 2149 • Eine SS-DE HasMember-Association, die das `SubmissionSet` mit dem geschickten

2150 DocumentEntry verbindet

2151 • Die „lid“ (logicalID) DARF NICHT gesendet werden.

2152 • Der Slot „associationPropagation“ MUSS auf „no“ gesetzt werden.

2153 Die Komponente ePA-Dokumentenverwaltung DARF die gesendete Association und das

2154 neue SubmissionSet NICHT dauerhaft speichern. [≤]

2155 **A_15080-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement**

2156 **für Restricted Update Document Set**

2157 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS

2158 die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy

2159 Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822

2160 durchsetzen, bevor Metadaten einer oder mehrerer Dokumente aktualisiert werden. Beim

2161 Aktualisieren der Metadaten durch das ePA-Frontend des Versicherten können einzelne

2162 Dokumente bzw. Metadaten durch den zwischenzeitlichen Entzug einer Berechtigung

2163 durch den Versicherten oder Ablauf nicht mehr für die Aktualisierung berechtigt sein.

2164 Widerspricht ein Dokument bzw. die damit assoziierten Metadaten einer anwendbaren

2165 Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die

2166 Antwortnachricht zum betreffenden Dokument einen XSDDocumentUniqueIdError-

2167 Fehlercode enthalten und der Wert 4 des EventOutcomeIndicators im

2168 Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein zu aktualisierendes

2169 Dokument bzw. Metadaten nicht mehr verfügbar, MUSS gemäß IHE TF ITI der Fehlercode

2170 XSDDocumentUniqueIdError zurückgegeben werden.

2171 [≤]

2172

2173 **5.1.3 Schnittstelle I_Document_Management_Insurance**

2174 **A_17438 - Komponente ePA-Dokumentenverwaltung – Implementierung der**

2175 **Schnittstelle I_Document_Management_Insurance**

2176 Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle

2177 definierte Web-Service-Schnittstelle implementieren.

2178 **Tabelle 18: Tab_Dokv_36 - Schnittstelle I_Document_Management_Insurance**

Schnittstelle	I_Document_Management_Insurance	
Version	1.0.1	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente in der Dokumentenverwaltung
WSDL	DocumentManagementService.wsdl	

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
-------------------	---

2179

2180 [\leq]2181 **5.1.3.1 Operation**2182 **I_Document_Management_Insurance::ProvideAndRegisterDocumentSet**
2183 **-b**2184 **A_17439 - Komponente ePA-Dokumentenverwaltung – Signatur für Provide And**
2185 **Register Document Set-b**

2186 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

2187 I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b gemäß der
2188 folgenden Signatur implementieren:2189 **Tabelle 19: Tab_Dokv_37 - Operation Provide And Register Document Set-b**

Operation	I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurance::putDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Provide And Register Document Set-b" [ITI-41] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente mitsamt Metadaten im ePA-Aktensystem dauerhaft zu speichern.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b		
Eingangsparameter			
Name	Beschreibung	Typ	opt
Provide And Register Document Set-b Message	Eingangsnachricht zum Registrieren und Speichern	xdsb:ProvideAndRegisterDocumentSetRequest	n

	ein oder mehrerer Dokumente		
X-User Assertion	Authentication Assertion des authentifizierte n Kostenträgers	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA_KTR_Consumer #A_17253, A_17254]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Provide And Register Document Set-b Response Message	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	rs:RegistryResponse	n
Technische Fehlermeldungen Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.			
Name	Fehlertext	Details	
MaxDocSizeExceeded	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines einzelnen übermittelten Dokuments übersteigt 25 MByte.	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

2190

2191 [**<=**]

2192 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
2193 Transaktionen "Provide And Register Document Set-b" [ITI-41] und "Provide X-User
2194 Assertion" [ITI-40] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
2195 entnehmen.

2196 5.1.3.1.1 Umsetzung

2197 **A_17443 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide** 2198 **And Register Document Set-b**

2199 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2200 MUSS die Umsetzung der
2201 Operation `I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b`
2202 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3] und
2203 [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3] implementieren.
2204 [`<=`]

2205 **A_17444 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender** 2206 **X-User Assertion**

2207 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2208 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren,
2209 falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
2210 gemäß [gemSpec_FM_ePA_KTR_Consumer#A_17253, A_17254] entspricht.[`<=`]

2211 5.1.4 Anforderungen an Sammlungstypen

2212 **A_20578 - Komponente ePA-Dokumentenverwaltung – Einstellen von** 2213 **Dokumenten in Sammlungen des Typs "mixed"**

2214 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry"
2215 MUSS beim Einstellen eines Dokuments des Sammlungstyps "mixed" sicherstellen, dass
2216 das Dokument in derselben Operation einem entsprechenden Sammlungstypordner
2217 zugewiesen wird und die Operation ansonsten mit dem
2218 Fehler `XDSRegistryMetadataError` abbrechen. Die ePA-Dokumentenverwaltung MUSS
2219 sicherstellen, dass der Ordner in derselben Operation angelegt wird, sofern ein nicht
2220 schon bestehender Ordner verwendet wird.[`<=`]

2221 **A_20627 - Komponente ePA-Dokumentenverwaltung – Kein Ordner für** 2222 **Sammlungstyp "mixed" ohne entsprechendes strukturiertes Dokument**

2223 Die Komponente ePA-Dokumentenverwaltung MUSS das Anlegen eines Folders für den
2224 Verwaltungstyp "mixed" mit dem Fehler `XDSRegistryMetadataError` unterbinden, wenn
2225 nicht in derselben Operation auch mindestens ein entsprechendes Sammlungstyp-
2226 spezifisches strukturiertes Dokument (gemäß [gemSpec_DM_ePA#A_20577](#)) eingestellt
2227 wird und die Operation mit dem Fehler `ACCESS_DENIED` abbrechen, wenn der
2228 Zugreifende nicht die Berechtigung besitzt, den Ordner und alle für den vorgesehenen
2229 Ordner mitgesendeten Dokumente anzulegen.
2230 [`<=`]

2231 **A_20707 - Komponente ePA-Dokumentenverwaltung– Keine unpassenden** 2232 **Dokumente in Ordner für Sammlungstyp "mixed"**

2233 Die Komponente ePA-Dokumentenverwaltung MUSS das Einstellen von Dokumenten in
2234 einen Ordner für Sammlungstyp "mixed" mit dem Fehler `ACCESS_DENIED` abbrechen,
2235 wenn das Dokument nicht einem dem Sammlungstyp zugeordneten strukturierten
2236 Dokumententyp (gemäß [gemSpec_DM_ePA#A_20577](#)) entspricht.
2237 [`<=`]

2238 **A_20579 - Komponente ePA-Dokumentenverwaltung – Löschen von Ordnern** 2239 **des Sammlungstyp "mixed"**

2240 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry"
2241 MUSS beim Löschen des letzten Dokuments aus einem Ordner für Sammlungstyp
2242 "mixed" sicherstellen, dass der Ordner automatisch durch die "Document Registry"
2243 mitgelöscht wird.[`<=`]

A_20581 - Komponente ePA-Dokumentenverwaltung – Löschen von Dokumenten aus Sammlungen der Typen "mixed" und "uniform"

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS beim Löschen eines Dokuments der Sammlungstypen "mixed" und "uniform" über die Operation `I_Document_Management_Insurant::RemoveMetadata` sicherstellen, dass alle Dokumente desselben Passes in derselben Operation mitgelöscht werden und die Operation ansonsten mit dem Fehler `ReferencesExistsException` abbrechen.

[<=]

Nur Leistungserbringern ist es erlaubt, einzelne Dokumente aus Sammlungen ~~des Typs~~ der Typen "mixed" und "uniform" zu löschen, um die medizinische Interpretation der gesamten Sammlungsinstanz nicht zu gefährden.

5.2 Aktenkontoverwaltung

5.2.1 Schnittstelle I_Account_Management_Insurant

Diese Schnittstelle setzt einen Teil der in [gemSysL_ePA] definierten Schnittstelle `I_Account_Management_Insurant` technisch um. Die Operationen der Schnittstelle werden vom Verarbeitungskontext über den sicheren Kanal zum ePA-Frontend des Versicherten bereitgestellt.

~~A_14804-01A_14804~~ - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Account_Management_Insurant

Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle implementieren.

Tabelle 20: Tab_Dokv_25 - Schnittstelle I_Account_Management_Insurant

Schnittstelle	I_Account_Management_Insurant	
Version	1.0.1	
Namensraum	http://ws.gematik.de/fd/phr/I_Account_Management/v1.0	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Suspend Account	Die Akten Daten werden in ein Exportpaket exportiert und das Aktenkonto geht in den Zustand "Bereit für Anbieterwechsel" über.
	Resume Account	Das neue Aktenkonto (bei einem anderen Anbieter) wird mit den Daten aus einem Exportpaket befüllt.
	Get Audit Events	Abfrage von Protokollen

	Get Signed Audit Events	Abfrage einer signierten Liste von Protokolleneinträgen
WSDL	AccountManagementService.wsdl	
XML Schema	AccountManagementService.xsd	

2266 [\leq]2267 **5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount**2268 **A_14805 - Komponente ePA-Dokumentenverwaltung – Signatur für**2269 **I_Account_Management_Insurant::SuspendAccount**

2270 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

2271 I_Account_Management_Insurant::SuspendAccount gemäß der folgenden Signatur
2272 implementieren:2273 **Tabelle 21: Tab_Dokv_26 - Operation Suspend Account**

Operation	I_Account_Management_Insurant::SuspendAccount		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Account_Management_Insurant::SuspendAccount technisch um. Mit dieser Operation werden die Daten aus der Akte eines Versicherten bei einem Anbieter ePA-Aktensystem in ein für andere Anbieter ePA-Aktensystem verarbeitbares Paket konsolidiert.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/SuspendAccount		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
X-User Assertion	Authentication Assertion des authentifizierten Versicherten als Inhaber der Akte	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109, A_15631]	n
Ausgangsparameter			
Package URL	URL, über die das erzeugte Exportpaket vom neuen Anbieter ePA-	URL mit Prozentkodierung	n

	Aktensystem geladen werden kann		
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig.	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
TEMP_UNAVAILABLE	Aktenkonto aufgrund einer andauernden Datenmigration vorübergehend nicht erreichbar	Dies sollte nur auftreten, wenn ein Anbieterwechsel angestoßen, aber noch nicht abgeschlossen wurde.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.	Der Nutzer hat nicht die erforderliche Berechtigung.	

2274 [`<=`]

2275 5.2.1.1.1 Umsetzung

2276 **A_15530-02 - Komponente ePA-Dokumentenverwaltung –**2277 **I_Account_Management_Insurant über sicheren Kanal**

2278 Die Komponente ePA-Dokumentenverwaltung MUSS die von ihr angebotenen
 2279 Operationen der Schnittstelle `I_Account_Management_Insurant` ausschließlich über den
 2280 sicheren Kanal zum ePA-Frontend des Versicherten verfügbar machen. [`<=`]

2281 Die folgende Anforderung bewirkt, dass nur der Versicherte als Inhaber einer Akte im
 2282 Zustand "DISMISSED" die

2283 Operation `I_Account_Management_Insurant::SuspendAccount` ausführen kann.

2284 **A_15062 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
 2285 **Suspend Account**

2286 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
 2287 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
 2288 Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor die
 2289 Operation `I_Account_Management_Insurant::SuspendAccount` ausgeführt wird. Bei
 2290 einer negativen Autorisierungsentscheidung MUSS die Nachricht mit dem
 2291 `ACCESS_DENIED`-Fehlercode quittiert werden. [`<=`]

A_14885 - Komponente ePA-Dokumentenverwaltung – Exportpaket des Aktenkontos erstellen

Die Komponente ePA-Dokumentenverwaltung MUSS bei der Ausführung der Operation `I_Account_Management_Insurant::SuspendAccount` für das Aktenkonto

- sämtliche Dokumente einschließlich Policy Documents (Advanced Patient Privacy Consents) des XCDR Responding Gateway bzw. XDS Document Repository,
- sämtliche Metadaten der XCA Responding Gateway bzw. XDS Document Registry,
- sämtliche § 291a-Protokolldaten,

gemäß den strukturellen Vorgaben in [IHE-ITI-TF2b] zur Transaktion *IHE ITI Cross-Enterprise Document Media Interchange (XDM) - Distribute Document Set on Media [ITI-32]*, in eine ZIP-Datei exportieren.

Die Komponente ePA-Dokumentenverwaltung MUSS dabei abweichend von den Vorgaben aus [ITI-32],

- die ZIP-Datei außerhalb des Verarbeitungskontextes persistieren,
- die ZIP-Datei im Zuge des Exports mit dem `ContextKey` gemäß [gemSpec_Krypt#GS-A_5016] verschlüsseln, so dass sichergestellt ist, dass nur entsprechend verschlüsselte Daten außerhalb des Verarbeitungskontextes auftreten können sowie
- die ZIP-Datei zum Abruf für berechtigte andere Anbieter ePA-Aktensystem verfügbar machen.

Der Verarbeitungskontext MUSS solange geöffnet bleiben, bis die ZIP-Datei erstellt worden ist. [`<=`]

A_15012 - Komponente ePA-Dokumentenverwaltung – Korrektheit des Exportpakets sicherstellen

Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln die Integrität der Daten und Datenstrukturen des Exportpakets während der Erstellung, Bereitstellung und Übermittlung an einen neuen Anbieter ePA-Aktensystem schützen, um damit ein Scheitern des Imports bei einem neuen Anbieter ePA-Aktensystem aufgrund eines fehlerhaften oder beschädigten Exportpakets auszuschließen. [`<=`]

Die Herausgabe des Exportpakets an den neuen Anbieter des Versicherten ist über Anforderungen in [gemSpec_Aktensystem#6.1.4] geregelt.

A_15005 - Komponente ePA-Dokumentenverwaltung – Kein Aktenzugriff während des Exports der Daten

Die Komponente ePA-Dokumentenverwaltung MUSS während der Ausführung der Operation `I_Account_Management_Insurant::SuspendAccount` für ein Aktenkonto alle Operationen mit der Fehlermeldung "Aktenkonto vorübergehend nicht erreichbar" ablehnen. [`<=`]

Für das ePA-Frontend des Versicherten endet die Operation

`I_Account_Management_Insurant::SuspendAccount` mit dem Erhalt der Download-URL für das Exportpaket. Bis zur vollständigen Übertragung des Exportpakets an den neuen Anbieter bleibt der vorherige Anbieter jedoch für die Daten des Versicherten verantwortlich.

Da der Anbieterwechsel als ein zusammenhängender Vorgang aus Sicht des ePA-Frontend des Versicherten ablaufen soll, der Export und anschließende Import je nach Größe des Exportpakets jedoch einige Zeit in Anspruch nehmen können, soll der Vorgang im Backend asynchron ablaufen können. Die folgende Anforderung regelt dies für den

2340 Export. Die Anforderung A_15623 im nächsten Abschnitt regelt die asynchrone
2341 Verarbeitung des Imports.

2342 **A_15622 - Komponente ePA-Dokumentenverwaltung – Asynchroner Export**

2343 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die URL
2344 des Exportpakets bestimmen und unmittelbar danach die Antwort auf den Aufruf der
2345 Operation `I_Account_Management_Insurant::SuspendAccount` an den Client
2346 zurückgeben, unabhängig davon, wie lange die Erstellung und Bereitstellung des
2347 Exportpakets dauert. [\leq]

2348 **A_16076 - Komponente ePA-Dokumentenverwaltung – Frist für Bereitstellung
2349 des Exportpakets**

2350 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS das
2351 Exportpaket innerhalb von drei Werktagen für den Download durch den neuen Anbieter
2352 bereitstellen. [\leq]

2353 **5.2.1.2 Operation `I_Account_Management_Insurant::ResumeAccount`**

2354 **A_14807 - Komponente ePA-Dokumentenverwaltung – Signatur für**

2355 **`I_Account_Management_Insurant::ResumeAccount`**

2356 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
2357 `I_Account_Management_Insurant::ResumeAccount` gemäß der folgenden Signatur
2358 implementieren:

2359 **Tabelle 22: Tab_Dokv_27 - Operation Resume Account**

Operation	I_Account_Management_Insurant::ResumeAccount		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Account_Management_Insurant::ResumeAccount technisch um. Mit dieser Operation wird das Paket mit den Daten aus der Akte eines Versicherten beim vorhergehenden Anbieter ePA-Aktensystem bezogen und importiert.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/ResumeAccount		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Package URL	URL, über die das vom vorhergehenden Anbieter ePA-Aktensystem erzeugte Exportpaket geladen werden kann	URL mit Prozentkodierung	n

X-User Assertion	Authentication Assertion des authentifizierten des Versicherten als Inhaber der Akte	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers# A_14109, A_15631]	n
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig.	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.		

2360 [<=]

2361 5.2.1.2.1 Umsetzung

2362 Die Ausführung der Operation `I_Account_Management_Insurant::ResumeAccount` setzt
 2363 voraus, dass der Versicherte mittels seines ePA-Frontend des Versicherten einen
 2364 sicheren Kanal zum Verarbeitungskontext aufgebaut hat und diesen mittels der Operation
 2365 `I_Document_Management_Connect::OpenContext` kryptographisch aktiviert hat. Darüber
 2366 hinaus muss die Operation `I_Account_Management_Insurant::ResumeAccount`
 2367 aufgerufen werden, bevor weitere Operationen am Verarbeitungskontext ausgeführt
 2368 werden können. Sie muss mit Fehler terminieren, wenn sie für ein Aktenkonto bereits
 2369 vorher erfolgreich ausgeführt wurde.

2370 **A_15526 - Komponente ePA-Dokumentenverwaltung – Voraussetzungen für die**
 2371 **Ausführung von Resume Account**

2372 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Operation
 2373 `I_Account_Management_Insurant::ResumeAccount` nur ausgeführt wird, wenn der
 2374 Verarbeitungskontext eines für einen Anbieterwechsel mit Übernahme der Akten Daten
 2375 registriertes Aktenkonto erstmalig durch den Versicherten geöffnet wurde. [<=]

2376 **A_15568 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
 2377 **Resume Account**

2378 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
 2379 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
 2380 Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor die
 2381 Operation `I_Account_Management_Insurant::ResumeAccount` ausgeführt wird. Bei einer

2382 negativen Autorisierungsentscheidung MUSS die Nachricht mit dem `ACCESS_DENIED-`
2383 Fehlercode quittiert werden.[<=]

2384 **A_15013 - ePA-Aktensystem – Download des Exportpakets**

2385 Das ePA-Aktensystem MUSS nach Eingang des Requests

2386 `I_Account_Management_Insurant::ResumeAccount` das mittels des Aufrufparameters
2387 `PackageURL` referenzierte Exportpaket beim vorhergehenden Anbieter ePA-Aktensystem
2388 des Versicherten abrufen und für den Import durch den Verarbeitungskontext der ePA-
2389 Dokumentenverwaltung verfügbar machen.[<=]

2390 **A_14905 - Komponente ePA-Dokumentenverwaltung – Import des Exportpakets 2391 des vorhergehenden Aktenkontos**

2392 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS das vom
2393 vorhergehenden Anbieter ePA-Aktensystem des Versicherten bezogene Exportpaket, vom
2394 vorhergehenden Anbieter herunterladen sobald es dort verfügbar ist und in das neue
2395 Aktenkonto importieren und dazu:

- 2396 • das Exportpaket mittels des `ContextKey` entschlüsseln und
- 2397 • die Struktur des Exportpakets auf Übereinstimmung mit den Festlegungen aus
2398 Anforderung A_14885 prüfen.

2399 [<=]

2400 **A_15596 - Komponente ePA-Dokumentenverwaltung – Ersetzen der Home 2401 Community ID**

2402 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS beim
2403 Import eines Exportpakets in sämtlichen Metadatensätzen den anbieterspezifischen Wert
2404 in den Feldern `DocumentEntry.homeCommunityId` und `SubmissionSet.homeCommunityId`
2405 sowie `DocumentEntry.repositoryUniqueId` mit der neuen Home Community ID
2406 aktualisieren.[<=]

2407 **A_15623 - Komponente ePA-Dokumentenverwaltung – Asynchroner Import**

2408 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die
2409 Antwort auf den Aufruf der Operation

2410 `I_Account_Management_Insurant::ResumeAccount` unmittelbar nach dem Aufruf an den
2411 Client zurückgeben, unabhängig davon, wie lange der Erhalt und Import des
2412 Exportpakets dauert.[<=]

2413 Die folgende Anforderung stellt sicher, dass der neue Anbieter des Aktenkontos
2414 ausreichend lange auf die Bereitstellung des Exportpakets durch den alten Anbieter
2415 wartet, da die Bereitstellung je nach Größe des Exportpakets eine gewisse Zeit in
2416 Anspruch nehmen kann. Der Versicherte kann mit dem neuen Aktenkonto nicht
2417 interagieren, bis der Import abgeschlossen ist. Das ePA-Frontend des Versicherten muss
2418 jedoch nicht auf den Abschluss warten, weil der Vorgang auf Ebene der Dienste
2419 asynchron abgeschlossen ist, nachdem der Versicherte ihn mittels des Aufrufs der
2420 Operation `I_Account_Management_Insurant::SuspendAccount` beim alten Anbieter und
2421 dem direkt anschließenden Aufruf der Operation

2422 `I_Account_Management_Insurant::ResumeAccount` beim neuen Anbieter ausgelöst hat.

2423 **A_15624 - Komponente ePA-Dokumentenverwaltung – Abfrage auf 2424 Verfügbarkeit des Exportpakets**

2425 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS nach dem
2426 Aufruf der Operation `I_Account_Management_Insurant::ResumeAccount` bei unmittelbar
2427 vorgesehenem Abruf des Exportpakets bis zum Erfolgsfall periodisch prüfen,
2428 jedoch maximal für einen Zeitraum von drei Werktagen, ob ein Exportpaket unter der
2429 vom Client übergebenen URL bereitsteht.[<=]

A_15625 - Komponente ePA-Dokumentenverwaltung – Kein Aktenzugriff während des Imports der Daten

Die Komponente ePA-Dokumentenverwaltung MUSS während der Ausführung der Operation `I_Account_Management_Insurant::ResumeAccount` für ein Aktenkonto alle Operationen mit Fehlermeldung "Aktenkonto aufgrund einer andauernden Datenmigration vorübergehend nicht erreichbar" ablehnen. [\leq]

A_16077 - Komponente ePA-Dokumentenverwaltung – Frist für den Import des Exportpakets

Die Komponente ePA-Dokumentenverwaltung MUSS den Import eines Exportpakets innerhalb von drei Werktagen nach Beginn des Downloads vom vorherigen Anbieter abschließen.

[\leq]

A_17845 - Komponente ePA-Dokumentenverwaltung – Offener Verarbeitungskontext während der Verarbeitung des Exportpakets

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS den für die Operation `I_Account_Management_Insurant::ResumeAccount` geöffneten Verarbeitungskontext so lange geöffnet lassen, bis der Abruf des Exportpakets beim alten Anbieter erfolgt ist und die Verarbeitung der Daten des Exportpakets durch diesen Verarbeitungskontext abgeschlossen ist, jedoch maximal drei Tage, falls kein Exportpaket abgerufen werden kann.

[\leq]

5.2.1.3 Operation `I_Account_Management_Insurant::GetAuditEvents`

A_14490-03 - Komponente ePA-Dokumentenverwaltung – Signatur für Get Audit Events

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I_Account_Management_Insurant::GetAuditEvents` gemäß der folgenden Signatur implementieren:

Tabelle 23: Tab_Dokv_28 - Operation Get Audit Events

Operation	I_Account_Management_Insurant::GetAuditEvents		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Account_Management_Insurant::GetAuditEvents technisch um. Mit dieser Operation kann der Versicherte bzw. sein berechtigter Vertreter das § 291a-Zugriffsprotokoll eines Aktenkontos herunterladen.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/GetAuditEvents		
Eingangsparameter			
Name	Beschreibung	Typ	opt.

X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Audit Event List	Liste der Zugriffsprotokolleinträge	phr:AuditMessage	n
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.		

2458 [**<=**]

2459 5.2.1.3.1 Umsetzung

2460 **A_15229-02 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement**

2461 **für Get Audit Events**

2462 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
 2463 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
 2464 Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor eine Audit
 2465 Event List zum ePA-Frontend des Versicherten zurückgegeben wird.

2466 [**<=**]

2467

A_15583 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Get Audit Events

Die Komponente ePA-Dokumentenverwaltung MUSS die Liste der § 291a-Protokolleinträge als Liste `phr:AuditMessage` zurückgeben. [`<=`]

5.2.1.4 Operation

I Account Management Insurant::GetSignedAuditEvents

A_21110 - Komponente ePA-Dokumentenverwaltung – Signatur für Get Signed Audit Events

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation I Account Management Insurant::GetSignedAuditEvents gemäß der folgenden Signatur implementieren:

Tabelle 24: Tab Dokv 44 - Operation Get Signed Audit Events

<u>Operation</u>	<u>I Account Management Insurant::GetSignedAuditEvents</u>		
<u>Beschreibung</u>	<u>Mit dieser Operation erhält der Versicherte bzw. sein berechtigter Vertreter eine signierte Liste aller in der Dokumentenverwaltung vorliegenden Protokolleinträge des Versicherten.</u>		
<u>Formatvorgabe n</u>	<u>SOAP Action:</u> <u>http://ws.gematik.de/fd/phr/I Account Management Insurant/v1.0/GetSignedAuditEvents</u>		
<u>Eingangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt.</u>
<u>X-User Assertion</u>	<u>Authentication Assertion des authentifizierten Versicherten oder des Vertreters</u>	<u>SAML 2.0 Assertion gemäß [gemSpec Authentisierung V ers#A 14109, A 15631]</u>	<u>n</u>
<u>Ausgangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt.</u>
<u>Signed Audit Event List</u>	<u>Signierte Liste der Zugriffsprotokolleinträge</u>	<u>Signiertes PDF/A-Dokument</u>	<u>n</u>
<u>Technische Fehlermeldungen</u>			
<u>Name</u>	<u>Fehlertext</u>	<u>Details</u>	

<u>INTERNAL ERROR</u>	<u>Es ist ein interner Fehler aufgetreten.</u>	<u>Interner Fehler in der Verarbeitungslogik</u>
<u>ASSERTION INVALID</u>	<u>Die übergebene Authentication Assertion ist ungültig</u>	<u>Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig</u>
<u>SYNTAX ERROR</u>	<u>Fehlerhafter Aufrufparameter</u>	<u>Es wurde ein fehlerhafter Aufrufparameter übergeben.</u>
<u>ACCESS DENIED</u>	<u>Der Zugriff für diese Operation konnte nicht gewährt werden.</u>	

[<=]

5.2.1.4.1 Umsetzung

A 21111 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Get Signed Audit Events

Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A 14822 durchsetzen, bevor eine Signed Audit Event List zum ePA-Frontend des Versicherten zurückgegeben wird.[<=]

A 21112 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Get Signed Audit Events

Die Komponente ePA-Dokumentenverwaltung MUSS die Liste der § 291a-Protokolleinträge als signiertes PDF/A-Dokument zurückgeben, wobei für die Signatur der Liste der private Schlüssel der Ausstelleridentität ID.FD.SIG genutzt wird, dessen zugehöriges Zertifikat C.FD.SIG die Rolle "oid_eпа_logging" enthält.[<=]

Es wird das gesamte PDF-Dokument signiert. Beim Anlegen des PDF-Dokuments muss Platz für die Signatur vorgesehen werden.

5.3 Umschlüsselung

Die ePA-Dokumentenverwaltung verwaltet verschlüsselte Dokumente: Die Dokumente selbst sind mit einem dokumentenspezifischen Dokumentenschlüssel verschlüsselt, der wiederum mit dem Aktenschlüssel verschlüsselt wird und so verpackt dem Dokument beigelegt wird. Die Dokumentenmetadaten, das Protokoll des Versicherten sowie die Policy-Dokumente werden zudem über einen Kontextschlüssel gesichert. Akten- und Kontextschlüssel sind für die gesamte Akte des Versicherten gültig.

Auf eigenen Wunsch kann der Versicherte eine Umschlüsselung seiner Akte anstoßen. Dabei werden Akten- und Kontextschlüssel ausgetauscht. Die Dokumentenschlüssel werden *nicht* gewechselt. Die Aufgabe besteht also darin, die verschlüsselten Dokumentenschlüssel mit dem alten Aktenschlüssel zu entschlüsseln, mit dem neuen Aktenschlüssel wieder zu verschlüsseln und das entstandene neue Paket wieder dem

2510 entsprechenden Dokument in der Dokumentenverwaltung zuzuordnen. Da die
2511 Dokumentenverwaltung niemals Zugriff auf den Aktenschlüssel im Klartext bekommt,
2512 muss die Ent- und Verschlüsselung im Client stattfinden.

2513 Der Vorgang der Umschlüsselung wird über die folgenden Operationen gesteuert:

- 2514 • I_Key_Management_Insurant::StartKeyChange()
- 2515 • I_Key_Management_Insurant::GetAllDocumentKeys()
- 2516 • I_Key_Management_Insurant::PutAllDocumentKeys()
- 2517 • I_Key_Management_Insurant::FinishKeyChange()

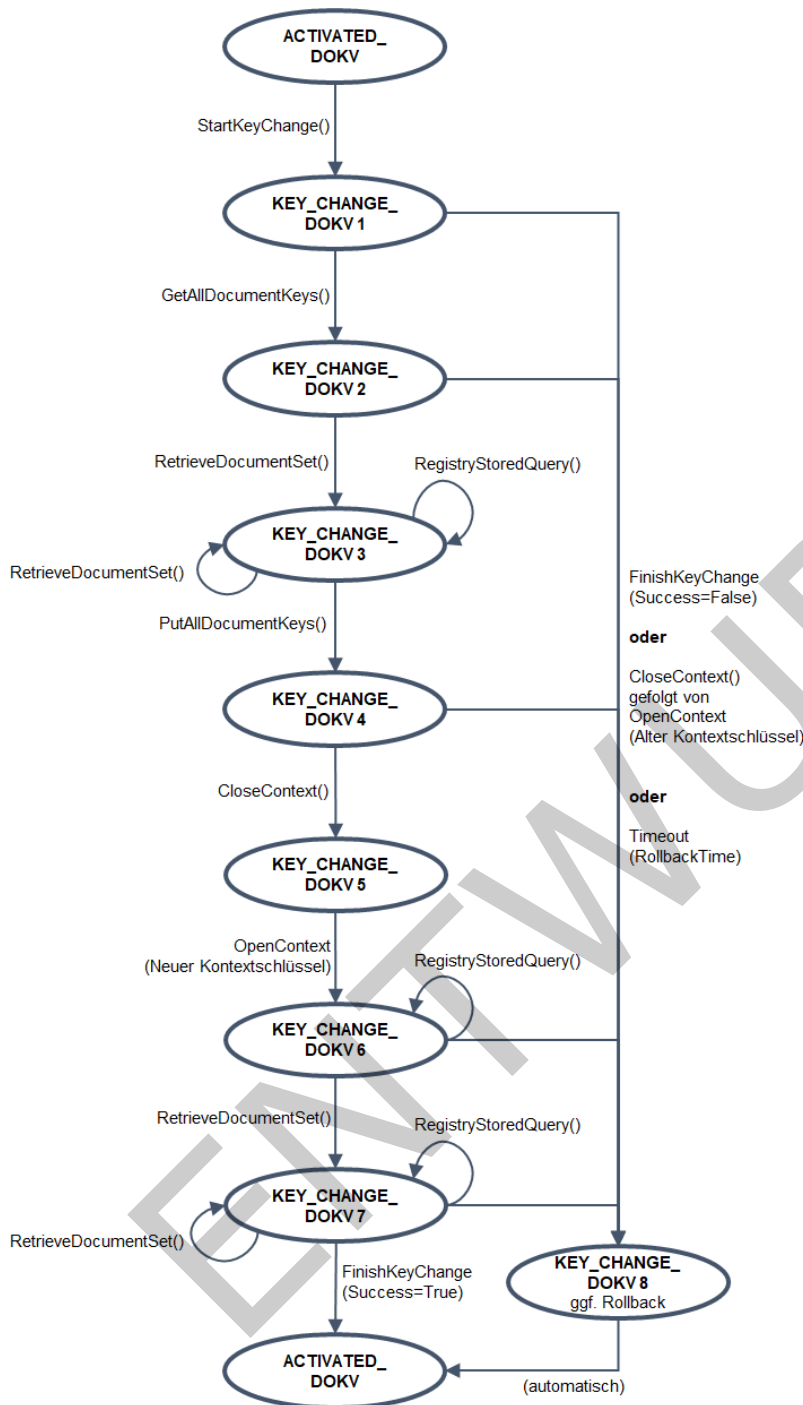
2518 Die Dokumentenverwaltung befindet sich nach erfolgreicher Einleitung der
2519 Umschlüsselung (StartKeyChange()) im logischen Zustand "KEY_CHANGE_DOKV". Sie ist
2520 dabei für alle Teilnehmer außer den Versicherten sowie für alle Operationen, die nicht die
2521 Umschlüsselung betreffen, gesperrt.

2522 Die Umschlüsselung wird vom Client mittels FinishKeyChange() abgeschlossen und die
2523 Dokumentenverwaltung über diesen Aufruf über Erfolg oder Misserfolg aus Sicht des
2524 Clients informiert. Im Falle eines Misserfolgs startet die Dokumentenverwaltung ein
2525 Rollback, in dem alle umgeschlüsselten Dokumentenschlüssel wieder durch die alten
2526 Fassung (verschlüsselt mit altem Aktenschlüssel) ersetzt werden und auch der neue
2527 Kontextschlüssel wieder durch den alten ersetzt wird. Im Erfolgsfall werden alle alten
2528 Schlüssel und entsprechenden Chiffre gelöscht. Ein Zugriff ist dann nur noch über die
2529 neuen Akten- und Kontextschlüssel möglich.

2530 5.3.1 Übergreifende Anforderungen

2531 **A_20466 - Komponente ePA-Dokumentenverwaltung – Erlaubte** 2532 **Zustandsübergänge für Zustand KEY_CHANGE_DOKV**

2533 Die Komponente ePA-Dokumentenverwaltung MUSS zur Umschlüsselung die
2534 Zustandsübergänge aus der Abbildung "Zustandsübergänge Schlüsselwechsel" nur die
2535 angegebenen Operationen in der angegebenen Reihenfolge erlauben und andere
2536 Zustandsübergänge (Operationsaufrufe) mit einem Fehler ablehnen.
2537



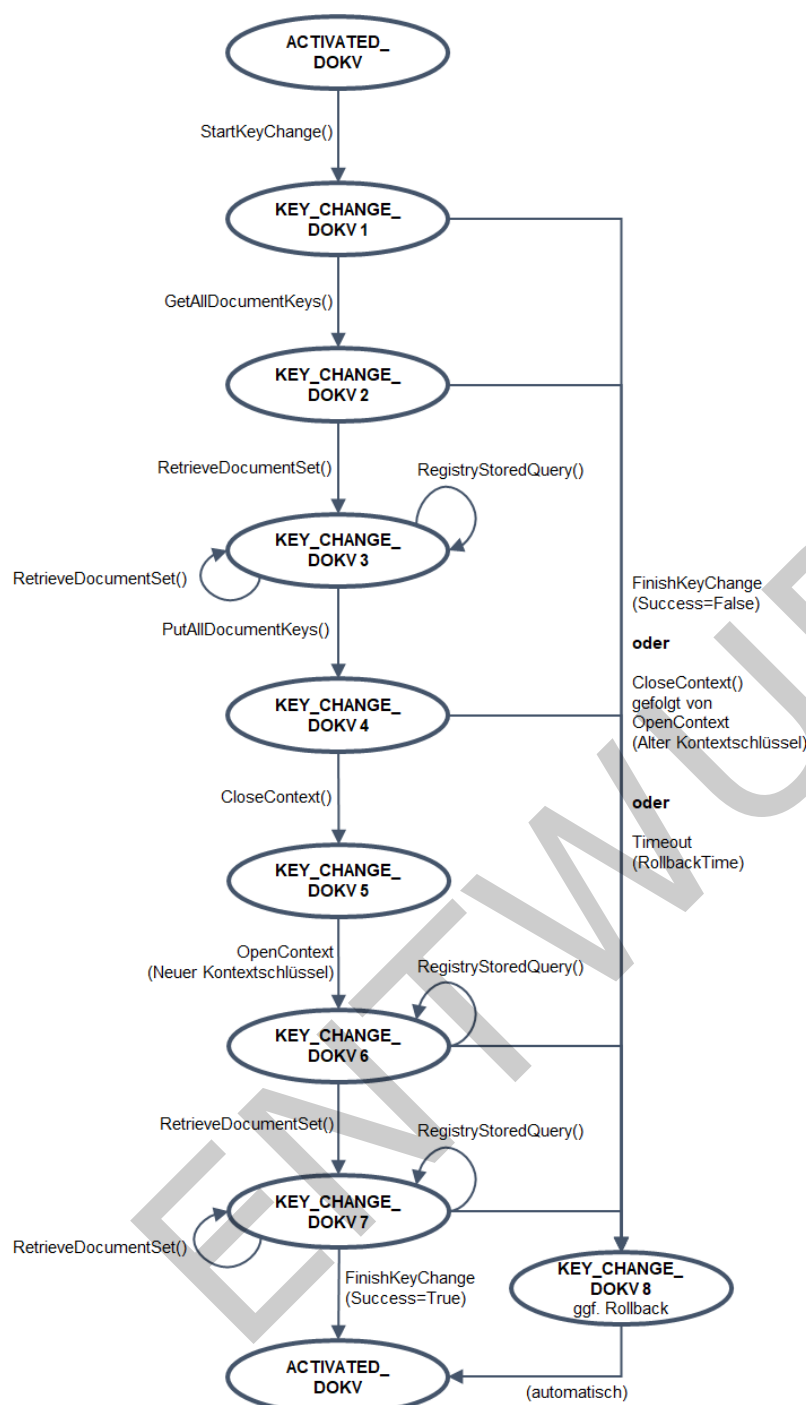


Abbildung 2: Zustandsübergänge Schlüsselwechsel

Erläuterungen:

- Die abgebildeten Operationen stehen als Kurzform für die folgenden Operationen der Dokumentenverwaltung:
- `StartKeyChange() : I_Key_Management_Insurant::StartKeyChange()`
- `GetAllDocumentKeys() : I_Key_Management_Insurant::GetAllDocumentKeys()`

- 2548 • `PutAllDocumentKeys()`:
- 2549 `I_Key_Management_Insurant::PutAllDocumentKeys()`
- 2550 • `FinishKeyChange()`: `I_Key_Management_Insurant::FinishKeyChange()`
- 2551 • `OpenContext()`: `I_Document_Management_Connect::OpenContext()`
- 2552 • `CloseContext()`: `I_Document_Management_Connect::CloseContext()`
- 2553 • `RetrieveDocumentSet()`:
- 2554 `I_Document_Management_Insurant::RetrieveDocumentSet()`
- 2555 • `CloseContext()` (gefolgt von `OpenContext()`) DARF zusätzlich auch in
- 2556 Kombination in den Zuständen Normalbetrieb sowie `KEY_CHANGE_DOKV 1, 2, 5`
- 2557 und `6` ausgeführt werden. In dem Fall ist der Zustand nach `OpenContext()`
- 2558 identisch mit dem vor `CloseContext()`, d.h. sie verändern den internen Zustand
- 2559 der Dokumentenverwaltung nicht. Die entsprechenden Zustandsübergänge sind
- 2560 nur aus Gründen der Übersichtlichkeit nicht im Diagramm enthalten.
- 2561 • Der Zustände "`KEY_CHANGE_DOKV`" (mit und ohne angehängte Ziffer) und
- 2562 "`ACTIVATED_DOKV`" entsprechen nicht direkt den Zuständen "`Key_Change`" bzw.
- 2563 "`Activated`" des Aktensystems.
- 2564 • Der Zustand "`ACTIVATED_DOKV`" beschreibt den normalen Betriebszustand der
- 2565 Akte, in dem Versicherte bzw. berechnigte weitere Parteien (LEI, KTR) über die
- 2566 jeweilige Schnittstelle auf Dokumente zugreifen können.

2567 [`<=`]

2568 Nach dem Hinterlegen der neu verschlüsselten Dokumentenschlüssel (Zustand

2569 `KEY_CHANGE_DOKV4`) müssen gemäß Zustandsdiagramm `CloseContext()` und

2570 `OpenContext()` mindestens einmal ausgeführt werden, um die neuen Kontext- und

2571 Aktenschlüssel über die Client-Schnittstelle zu testen.

2572 Die Nummerierung der Zustände dient nur beschreibenden Zwecken, im Folgenden

2573 werden die Zustände allgemein häufig als als Zustand "`KEY_CHANGE_DOKV`"

2574 zusammengefasst.

2575 **A_20729 - Komponente ePA-Dokumentenverwaltung – Start der**

2576 **Umschlüsselung nur in Zustand Activated**

2577 Die Komponente ePA-Dokumentenverwaltung MUSS den Start der Umschlüsselung über

2578 die Operation `StartKeyChange()` ablehnen, wenn sie sich nicht im Zustand

2579 "`ACTIVATED_DOKV`" befindet. [`<=`]

2580 **A_20726 - Komponente ePA-Dokumentenverwaltung – Verbotene Operationen**

2581 **außerhalb Status KEY_CHANGE_DOKV**

2582 Die Komponente ePA-Dokumentenverwaltung MUSS die Umschlüsselungsoperationen

2583 `GetAllDocumentKeys()`, `PutAllDocumentKeys()` sowie `FinishKeyChange()` mit einem

2584 Fehler ablehnen, wenn die Dokumentenverwaltung nicht im Status `KEY_CHANGE_DOKV` ist.

2585 [`<=`]

2586 **A_20727 - Komponente ePA-Dokumentenverwaltung – Validierung der**

2587 **Authentication Assertion**

2588 Die Komponente ePA-Dokumentenverwaltung MUSS in allen Eingangsnachrichten der

2589 Schnittstelle `I_Key_Management_Insurant` analog eines XUA-Akteur "X-Service

2590 Provider" die mitgelieferte X-User Assertion (Authentication Assertion) gemäß der

2591 Anforderung A_13690 prüfen und die eingehende Nachricht mit Fehlercodes nach

2592 [WSS#12] quittieren, falls diese X-User Assertion nicht gültig ist. [`<=`]

2593 Die Authentication Assertion wird als Teil des SOAP Headers mitgeschickt.

A_20444 - Komponente ePA-Dokumentenverwaltung – Format phr:KeyList für Zustand KEY_CHANGE_DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS zur Übertragung einer Liste von mit Aktenschlüssel verschlüsselten Dokumentenschlüssel im Zustand KEY_CHANGE_DOKV das folgende Format verwenden:

```
<?xml version="1.0" encoding="UTF-8"?>
<phr:KeyList xmlns:phr="http://ws.gematik.de/fa/phrext/v1.0">
  <!-- Schlüsseleinträge, eines pro verschlüsseltem Dokumentenschlüssel -->
  <phr:Key>
    <!-- DocumentEntry.uniqueId des Dokuments -->
    <DocumentUniqueId> ... </DocumentUniqueId>
    <!-- <xenc:EncryptedData>-Elemente gemäß gemSpec_DM_ePA#A_14977 -->
    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc"
      Type="http://www.w3.org/2001/04/xmlenc#Content"> ...
    </xenc::EncryptedData>
  </phr:Key>
  <!-- ... weitere Dokumentenschlüssel ... -->
</phr:KeyList>
```

Dabei gelten folgende Anforderungen:

- Das Element <xenc:EncryptedData> MUSS wie in [gemSpec_DM_ePA#14977](#) angegeben gefüllt sein
- Abweichend davon MÜSSEN das Element <xenc:CipherData> und das Element <ds:KeyInfo> mit leerem Elementwert gesendet werden.

Einzelne Operationen schränken das angegebene Format ggf. noch weiter ein. [≤]

A_20446 - Komponente ePA-Dokumentenverwaltung – Gültigkeit des Kontextschlüssels für Zustand KEY_CHANGE_DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS im Zustand KEY_CHANGE_DOKV sowohl den alten als auch den neuen Kontextschlüssel beim Aufruf von `I_Document_Management_Connect::OpenContext()` akzeptieren.

[≤]

A_20468 - Komponente ePA-Dokumentenverwaltung – Login mit altem Kontextschlüssel im Zustand KEY_CHANGE_DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS bei einem Login des Versicherten mithilfe des alten Kontextschlüssels, falls sie sich im Zustand KEY_CHANGE_DOKV befindet, ein Rollback gemäß A_20447 durchführen und den Zustand KEY_CHANGE_DOKV nach ACTIVATED_DOKV verlassen. [≤]

A_20735 - Komponente ePA-Dokumentenverwaltung – Exklusiver Versichertenzugriff im Zustand KEY_CHANGE_DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS im Zustand KEY_CHANGE_DOKV alle Login-Versuche (`I_Document_Management_Connect::OpenContext()`) ablehnen. Ausnahme ist ein Login-Versuch des Versicherten (Aktenkontoinhaber), der nur dann nicht grundsätzlich abgelehnt wird, wenn die Sitzung, über die `StartKeyChange()` aufgerufen wurde, nicht mehr aktiv ist. [≤]

A_20442 - Komponente ePA-Dokumentenverwaltung – Timeout für Zustand KEY_CHANGE_DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS im Status KEY_CHANGE_DOKV nach Erreichen des Zeitpunkts in `RollbackTime` (Parameter `StartKeyChange()`) zum frühestmöglichen Zeitpunkt ein Rollback gemäß A_20447 durchführen. Wenn der Versicherte bei

2644 Erreichen von `RollbackTime` noch eingeloggt ist, MUSS die Komponente ePA-
2645 Dokumentenverwaltung die Sitzung des Versicherten beenden und eine etwaig
2646 ausstehende Operation mit einem Fehler abbrechen. [`<=`]

2647 Da der Kontext in dem Moment, in dem die `RollbackTime` erreicht wird, unter
2648 Umständen noch geschlossen ist, kann die Dokumentenverwaltung den Rollback in
2649 diesem Fall erst bei einem erneuten Login des Versicherten durchführen.

2650 **A_20447 - Komponente ePA-Dokumentenverwaltung – Rollback für Zustand** 2651 **KEY_CHANGE_DOKV**

2652 Die Komponente ePA-Dokumentenverwaltung MUSS bei einem Rollback die folgenden
2653 Aktionen durchführen:

- 2654 • Löschen des neuen Kontextschlüssels
- 2655 • Wiederherstellen bzw. Reaktivierung aller mit dem alten Aktenschlüssel
2656 verschlüsselten Dokumentenschlüssel
- 2657 • Löschen von allen mit dem neuen Aktenschlüssel verschlüsselten
2658 Dokumentenschlüssel
- 2659 • Löschen des neuen Aktenschlüssels
- 2660 • Verlassen des Status `KEY_CHANGE_DOKV` in den Zustand `ACTIVATED_DOKV`

2661 [`<=`]

2662 Das Ziel des Rollback ist es, die Dokumentenverwaltung in den Zustand vor dem Aufruf
2663 von `I_Account_Management_Insurant::StartKeyChange()` zurückzusetzen.

2664 **5.3.2 Schnittstelle I_Key_Management_Insurant**

2665 **5.3.2.1 I_Key_Management_Insurant::StartKeyChange()**

2666 **A_20467 - Komponente ePA-Dokumentenverwaltung – Signatur für** 2667 **I_Key_Management_Insurant::StartKeyChange()**

2668 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
2669 `I_Account_Management_Insurant::StartKeyChange` gemäß der folgenden Signatur
2670 implementieren:
2671

2672 **Tabelle 25: Tab_Dokv_38 - Operation I_Key_Management_Insurant::StartKeyChange()**

Operation	I_Key_Management_Insurant::StartKeyChange
Beschreibung	Diese Operation setzt die Operation <code>I_Account_Management_Insurant::StartKeyChange</code> technisch um. Mit dieser Operation kann der Versicherte den Prozess der Umschlüsselung initiieren.
Formatvorgaben	SOAP Action: <code>http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/StartKeyChange</code>
Eingangsparameter	

Name	Beschreibung	Typ	opt.
X-User Assertion	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhabers)	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers# A_14109, A_15631]	n
ContextKey	Neuer Kontextschlüssel	ContextKey	n
RollbackTime	Zeitpunkt (UTC-Zeit), an dem ein Rollback durchgeführt werden muss, sofern bis dahin nicht explizit finishKeyChange() aufgerufen wurde.	Signierte xsd:dateTime, base64-kodiert	n
Ausgangsparameter			
AuthorizedIDList	Liste mit IDs aller zurzeit berechtigten Akteure	phr:AuthorizedIDList	n
Name	Beschreibung	Typ	opt.
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafte Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	

ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.	
----------------------	--	--

2673
2674 [**<=**]

2675 5.3.2.1.1 Umsetzung

2676 **A_20495 - Komponente ePA-Dokumentenverwaltung – Format von** 2677 **phr:AuthorizedIDList**

2678 Die Komponente ePA-Dokumentenverwaltung MUSS bei Aufruf von `StartKeyChange()` für
2679 den Parameter `AuthorizedKeyList` die folgende XML-Struktur (`phr:AuthorizedIDList`)
2680 zurückgeben:

```
2681
2682 <?xml version="1.0" encoding="UTF-8"?>
2683 <phr:AuthorizedIDList xmlns:phr="http://ws.gematik.de/fa/phrext/v1.0">
2684   <!--ID des Berechtigten, jeweils eines für jeden Berechtigten-->
2685   <phr:AuthorizedID>
2686     <!-- KVN (bei Versicherten) oder Telematik ID (bei Leistungserbringern und
2687     Kostenträgern) des Berechtigten -->
2688     <ID> ... </ID>
2689     <!-- Typ: "KVN" oder "TelematikID"-->
2690     <Type> ... </Type>
2691   </phr:AuthorizedID>
2692 </phr:AuthorizedIDList> [<=]
```

2693 Die Liste der Berechtigten so wie die zu übertragenden Details lassen sich aus den aktuell
2694 hinterlegten Policies ableiten. Es sind nur aktive, d.h. zeitlich noch gültige Policies, zu
2695 berücksichtigen.

2696 **A_20738 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für** 2697 **StartKeyChange()**

2698 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
2699 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
2700 Privacy Consents) entsprechend der Anforderung A_14822-01 durchsetzen vor Ausführen
2701 der Operation `StartKeyChange()`.

2702 [**<=**]

2703 **A_20757 - Komponente ePA-Dokumentenverwaltung – Prüfung des ContextKey-** 2704 **Parameters**

2705 Die Komponente ePA-Dokumentenverwaltung MUSS prüfen, ob der im
2706 Parameter `"ContextKey"` mitgelieferten neue Kontextschlüssel den Strukturvorgaben
2707 gemäß gemSpec Krypt#A 18004 entspricht und ansonsten den Fehler `"ACCESS_DENIED"`
2708 zurückgeben.

2709 [**<=**]

2710 **A_20530 - Komponente ePA-Dokumentenverwaltung – Prüfung des** 2711 **RollbackTime-Parameters**

2712 Die Komponente ePA-Dokumentenverwaltung MUSS die `RollbackTime` Base64-
2713 dekodieren, das Format gemäß `xsd:dateTime` sowie die Signatur des Eingangsparameters
2714 `"RollbackTime"` prüfen. Für die Signaturprüfung MUSS die Komponente ePA-
2715 Dokumentenverwaltung auch prüfen, ob das zugehörige Signaturzertifikat zeitlich gültig
2716 ist, nicht gesperrt wurde und nach dem Zertifikatsprofil C.FD.SIG auf die Identität der
2717 Komponente Autorisierung in seiner fachlichen Rolle `oid_epa_authz` gemäß

[gemSpec_OID] ausgestellt wurde. Falls Signatur oder Zertifikat fehlerhaft sind oder die RollbackTime mehr als 24 Stunden in der Zukunft liegt, MUSS die Komponente ePA-Dokumentenverwaltung den Fehler "ACCESS_DENIED" zurückgeben.

[<=]

Dies kann durch eine aktuell gehaltene Konfiguration vertrauenswürdiger Zertifikate umgesetzt werden und ersetzt eine detaillierte Prüfung der Signaturzertifikate.

~~A_20728 – Komponente ePA-Dokumentenverwaltung – Verwendung des Parameters ContextKey~~

~~Die Komponente ePA-Dokumentenverwaltung MUSS den im Parameter "ContextKey" mitgelieferten neuen Kontextschlüssel in der Dokumentenverwaltung hinterlegen und zusammen mit dem bereits bestehenden, alten Kontextschlüssel speichern. Im StatusKEY_CHANGE_DOKV kann der Kontext dann anschließend über OpenContext() über wahlweise einen beider Schlüssel geöffnet werden.~~

~~[<=]~~

A_20422 - Komponente ePA-Dokumentenverwaltung – Beenden bestehender Sitzungen bei StartKeyChange()

Die Komponente ePA-Dokumentenverwaltung MUSS bei Aufruf von StartKeyChange() anderweitig bestehende Sitzungen (d.h. alle außer derjenigen, über die StartKeyChange() aufgerufen wurde) nach Ausführung dort bereits laufender Operationen, spätestens aber eine Minute nach Aufruf von StartKeyChange() beenden. Nach fehlerfreier Ausführung befindet sich die Dokumentenverwaltung im logischen Zustand KEY_CHANGE_DOKV. [<=]

5.3.2.2 I_Key_Management_Insurant::GetAllDocumentKeys()

A_20443 - Komponente ePA-Dokumentenverwaltung – Signatur für

I_Key_Management_Insurant::GetAllDocumentKeys()

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation I_Key_Management_Insurant::GetAllDocumentKeys gemäß der folgenden Signatur implementieren:

Tabelle 26: Tab_Dokv_39 -

Operation I_Key_Management_Insurant::GetAllDocumentKeys()

Operation	I_Key_Management_Insurant::GetAllDocumentKeys		
Beschreibung	Diese Operation setzt die Operation I_Key_Management_Insurant::GetAllDocumentKeys technisch um. Mit dieser Operation kann der Versicherte alle mit dem Aktenschlüssel verschlüsselte Dokumentenschlüssel abrufen.		
Formatvorgabe n	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/ /GetAllDocumentKeys		
Eingangsparameter			
Name	Beschreibung	Typ	opt.

X-User Assertion	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhabers)	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
OkDate	Zeitpunkt, an dem die Komponente Autorisierung <code>PutForReplacement()</code> erfolgreich ausgeführt hat.	Signierte <code>xsd:dateTime</code> , base64-kodiert	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
DocumentKeyList	Liste aller Document Keys, jeweils verschlüsselt mit altem Aktenschlüssel	<code>phr:KeyList</code>	n
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafte Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.		

2749
2750 [**<=**]

2751 5.3.2.2.1 Umsetzung

2752 **A_20452 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für GetAllDocumentKeys()**

2753 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
2754 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
2755

Privacy Consents) entsprechend der Anforderung A_14822-01 durchsetzen vor Ausführen der Operation GetAllDocumentKeys().

[<=]

A_20425 - Komponente ePA-Dokumentenverwaltung – Rückgabe aller verschlüsselter Dokumentenschlüssel

Die Komponente ePA-Dokumentenverwaltung MUSS als Rückgabewert von GetAllDocumentKeys() alle jeweils mit dem Aktenschlüssel verschlüsselten Dokumentenschlüssel über eine XML-Struktur (phr:KeyList) gemäß A_20444 zurückgeben. Die Komponente ePA-Dokumentenverwaltung MUSS dabei die alten verschlüsselten Dokumentenschlüssel für den Fall eines späteren Rollbacks und zum Abgleich für die Operation PutAllDocumentKeys() sichern.

[<=]

A_20528 - Komponente ePA-Dokumentenverwaltung – Prüfung des OkDate-Parameters

Die Komponente ePA-Dokumentenverwaltung MUSS den Eingangsparameter "OkDate" Base64-dekodieren, das Format gemäß xsd:dateTime sowie die Signatur prüfen und sicherstellen, dass OkDate einen Zeitpunkt in der Vergangenheit bezeichnet, der nicht mehr als 24 Stunden zurückliegt. Zur Signaturprüfung MUSS die Komponente ePA-Dokumentenverwaltung auch prüfen, ob das zugehörige Signaturzertifikat zeitlich gültig ist, nicht gesperrt wurde und nach dem Zertifikatsprofil C.FD.SIG auf die Identität der Komponente Autorisierung in seiner fachlichen Rolle oid_epa_authz gemäß [gemSpec_OID] ausgestellt wurde. Falls Signatur oder Zertifikat fehlerhaft sind, MUSS die Komponente ePA-Dokumentenverwaltung den Fehler "ACCESS_DENIED" zurückgeben und ein Rollback gemäß A_20447 durchführen.

[<=]

Dies kann durch eine aktuell gehaltene Konfiguration vertrauenswürdiger Zertifikate umgesetzt werden und ersetzt eine detaillierte Prüfung der Signaturzertifikate.

5.3.2.3 Operation I_Key_Management_Insurant::PutAllDocumentKeys()

A_20436 - Komponente ePA-Dokumentenverwaltung – Signatur für I_Key_Management_Insurant::PutAllDocumentKeys()

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation I_Key_Management_Insurant::PutAllDocumentKeys gemäß der folgenden Signatur implementieren:

Tabelle 27: Tab_Dokv_40 -

Operation I_Key_Management_Insurant::PutAllDocumentKeys()

Operation	I_Account_Management_Insurant::PutForReplacement
Beschreibung	Diese Operation setzt die Operation I_Key_Management_Insurant::PutAllDocumentKeys technisch um. Mit dieser Operation kann der Versicherte den Prozess des Schlüsselwechsels einleiten.
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/PutAllDocumentKeys

Eingangsparameter			
Name	Beschreibung	Typ	opt .
X-User Assertion	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhaber)	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109, A_15631]	n
DocumentKeyList	Liste aller Document Keys, jeweils verschlüsselt mit neuem Aktenschlüssel	phr:KeyList	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt .
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafte Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.		

2791 [**<=**]

5.3.2.3.1 Umsetzung

A_20453 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für PutAllDocumentKeys()

Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822-01 durchsetzen vor Ausführen der Operation PutAllDocumentKeys().

[<=]

A_20448 - Komponente ePA-Dokumentenverwaltung – Hochladen aller verschlüsselter Dokumentenschlüssel

Die Komponente ePA-Dokumentenverwaltung MUSS als Eingabeparameter von PutAllDocumentKeys() alle mit dem neuen Aktenschlüssel verschlüsselten Dokumentenschlüssel über eine XML-Struktur (phr:KeyList) gemäß A_20444 einstellen. Die Komponente ePA-Dokumentenverwaltung MUSS dabei sicherstellen, dass Schlüssel für dieselben Dokumente hochgeladen werden, wie sie beim vorhergehenden Aufruf von GetAllDocumentKeys() von der Dokumentenverwaltung übertragen wurde.

[<=]

A_20758 - Komponente ePA-Dokumentenverwaltung – Prüfung des DocumentKeyList-Parameters

Die Komponente ePA-Dokumentenverwaltung MUSS prüfen, ob die im Parameter "DocumentKeyList" gesendeten Daten den Strukturvorgaben gemäß A_20495 entspricht und ansonsten den Fehler "ACCESS_DENIED" zurückgeben.

[<=]

A_20730 - Komponente ePA-Dokumentenverwaltung – Rollback bei fehlgeschlagenem PutAllDocumentKeys()

Die Komponente ePA-Dokumentenverwaltung MUSS, falls die Operation PutAllDocumentKeys() fehlschlägt, einen Fehler zurückgeben und ein Rollback gemäß A_20447 durchführen.

[<=]

5.3.2.4 Operation I_Key_Management_Insurant::FinishKeyChange()

A_20449 - Komponente ePA-Dokumentenverwaltung – Signatur für I_Key_Management_Insurant::FinishKeyChange()

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation I_Key_Management_Insurant::FinishKeyChange gemäß der folgenden Signatur implementieren:

Tabelle 28: Tab_Dokv_41 -

Operation I_Account_Management_Insurant::FinishKeyChange()

Operation	I_Key_Management_Insurant::FinishKeyChange
Beschreibung	Diese Operation setzt die Operation I_Key_Management_Insurant::FinishKeyChange technisch um. Mit dieser Operation kann der Versicherte den Prozess des Schlüsselwechsels beenden und gleichzeitig die Dokumentenverwaltung über Erfolg oder Misserfolg desselben informieren.

Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/FinishKeyChange		
Eingangsparameter			
Name	Beschreibung	Typ	optional
X-User Assertion	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhabers)	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109, A_15631]	nein
Success	Beschreibt, ob die Umschlüsselung aus Sicht des Clients erfolgreich (<code>true</code>) oder nicht erfolgreich (<code>false</code>) beendet werden soll.	xs:boolean	nein
Ausgangsparameter			
Name	Beschreibung	Typ	optional
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafte Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.		

2829 [`<=`]

2830 5.3.2.4.1 Umsetzung

2831 **A_20454 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für** 2832 **FinishKeyChange()**

2833 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
2834 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
2835 Privacy Consents) entsprechend der Anforderung A_14822-01 durchsetzen vor Ausführen
2836 der Operation `FinishKeyChange()`.

2837 [`<=`]

2838 **A_20450 - Komponente ePA-Dokumentenverwaltung – Erfolgreicher Abschluss** 2839 **des Schlüsselwechsels**

2840 Die Komponente ePA-Dokumentenverwaltung MUSS bei Aufruf
2841 von `I_Key_Management_Insurant::FinishKeyChange` mit `Success=True` alle mit dem alten
2842 Aktenschlüssel verschlüsselten Dokumentenschlüssel sowie den alten Kontextschlüssel löschen und
2843 den Zustand `KEY_CHANGE_DOKV` anschließend verlassen und in den Zustand `ACTIVATED_DOKV`
2844 übergehen. [`<=`]

2845 **A_21141 - Komponente ePA-Dokumentenverwaltung – Protokollierung** 2846 **erfolgreicher Abschluss des Schlüsselwechsels**

2847 Die Komponente ePA-Dokumentenverwaltung MUSS nach Abschluss des Aufrufs
2848 `I_Key_Management_Insurant::FinishKeyChange` mit `Success=True`, d.h. nach
2849 vollständiger, erfolgreicher Durchführung des Schlüsselwechsels und Betreten des
2850 Zustands `ACTIVATED_DOKV`, einen Eintrag im § 291a-Protokoll für den Versicherten
2851 gemäß [gemSpec_DM_ePA#A_14471] mit `EventID.code_PHR-870` protokollieren.

2852 [`<=`]

2853 **A_20451 - Komponente ePA-Dokumentenverwaltung – Erfolgloser Abschluss** 2854 **des Schlüsselwechsels**

2855 Die Komponente ePA-Dokumentenverwaltung MUSS bei Aufruf
2856 von `I_Key_Management_Insurant::FinishKeyChange` mit `Success=False` ein Rollback
2857 gemäß A_20447 durchführen. [`<=`]

2858

2859 ~~Der Anbieter der Komponente ePA-Dokumentenverwaltung muss dafür Sorge tragen,~~
2860 ~~dass im Falle einer erfolgreichen Umschlüsselung vorhandenes veraltetes~~
2861 ~~Schlüsselmateriale im Zwischenspeicher konform zum Backupkonzept des Anbieters~~
2862 ~~aufbewahrt, bzw. gelöscht wird. Das veraltete Schlüsselmateriale sollte so lange~~
2863 ~~aufbewahrt werden, wie es zur Entschlüsselung von Backups gegebenenfalls erforderlich~~
2864 ~~ist, aber nicht darüber hinaus.~~

2865 5.3.2.5 Protokollierung

2866 **A_20470-01 - Komponente ePA-Dokumentenverwaltung -** 2867 **Protokollierungszusatz für Status `KEY_CHANGE_DOKV`**

2868 **A_20470 – Protokollierungszusatz für Status `KEY_CHANGE_DOKV`** Die Komponente
2869 ePA-Dokumentenverwaltung MUSS für alle Operationen, bei der sich die Komponente im
2870 Status `KEY_CHANGE_DOKV` befindet, diesen Zustand auslösen oder beenden, der
2871 Protokollierung gemäß A_20538-* den folgenden Parameter hinzufügen:

Tabelle 29: Tab_Dokv_42 - Zusätzliche Parameter des § 291a-Protokolls für die Umschlüsselung

<u>Protokollparameter</u>	<u>Parameterwerte gemäß aufgerufener Operation</u>
<u>ObjectDetail</u>	<u>Das Element ParticipantObjectDetail muss zusätzlich mit folgenden Wertepaar (type/value) belegt werden:</u>
<u>type</u>	<u>value</u>
<u>State</u>	<u>KEY_CHANGE_DOKV</u>

[<=]

A 20473-02 - Komponente ePA-Dokumentenverwaltung - Protokollierungszusatz für Status Rollback im Status KEY_CHANGE_DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS im Falle eines Rollbacks gemäß A 20447 der Protokollierung gemäß gemSpec DM ePA#A 14505 einen Protokolleintrag (Event.code=PHR-860) hinzufügen und dabei den folgenden Parameter hinzufügen:

Tabelle 30: Tab_Dokv_43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung

<u>Protokollparameter</u>	<u>Parameterwerte gemäß aufgerufener Operation</u>
<u>Object- IDObjectDetail</u>	<u>Das Element ParticipantObjectDetail muss zusätzlich mit folgenden Wertepaar (type/value) belegt werden:</u>
<u>type</u>	<u>value</u>
<u>State</u>	<u>KEY_CHANGE_DOKV</u>

{<=>}[<=]

A 21157 - Komponente ePA-Dokumentenverwaltung - Protokollierungszusatz für Verwaltungsprotokolleintrag für Aufruf der Operation FinishKeyChange

A 20473-01 - Protokollierungszusatz für Status Rollback im Status KEY_CHANGE_DOKV Die Komponente ePA-Dokumentenverwaltung MUSS im Falle eines Rollbacks gemäß A 20447 der des Aufrufs von FinishKeyChange bei der Protokollierung gemäß A 20538 gemSpec DM ePA#A 14505 einen Protokolleintrag (Event.code=PHR-860840) hinzufügen und dabei den folgenden Parameter hinzufügen:

Tabelle 31: Tab_Dokv_43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung

<u>Protokollparameter</u>	<u>Parameterwerte gemäß aufgerufener Operation</u>
<u>Object- IDObjectDetail</u>	<u>Das Element ParticipantObjectDetail muss zusätzlich mit folgendenfolgendem Wertepaar (type/value) belegt werden:</u>

type	value
<u>StateDetails</u>	<u>KEY_CHANGE_DOKV</u> Der Wert ist abhängig vom Aufrufparameter <u>Success</u> der Operation <u>FinishKeyChange</u> . <u>Success = 1:</u> <u>"Umschlüsselung erfolgreich beenden"</u> <u>Success = 0:</u> <u>"Umschlüsselung abbrechen"</u>

2895 [\leq]2896

5.4 Zugriffskontrolle

2897

5.4.1 Grob-, mittel- und feingranulare Berechtigungen

2898 Die Zugriffskontrolle muss sicherstellen, dass nur solche Zugriffe zugelassen werden, die
 2899 vom Versicherten berechtigt wurden. Zur Berechtigungsvergabe an
 2900 Leistungserbringerinstitutionen (LEI) stehen dem Versicherten dazu grundsätzlich drei
 2901 Ansätze zur Verfügung:

- 2902 1. Grobgranulare Berechtigung (Vertraulichkeitsstufen)
 2903 Allen Dokumenten wird in der Akte eine von drei Vertraulichkeitsstufen
 2904 zugeordnet ("Streng vertraulich", "Vertraulich" oder "Normal") und jedem
 2905 Berechtigten eine von zwei Zugriffsrechten ("Normal" oder "Erweitert"). LEI mit
 2906 Zugriffsrecht "Normal" dürfen auf die Dokumente in Vertraulichkeitsstufe "Normal"
 2907 zugreifen, jene mit Zugriffsrecht "Erweitert" zusätzlich auf die mit "Vertraulich"
 2908 gekennzeichneten Dokumente. Dokumente in der Stufe "Streng vertraulich" sind
 2909 nur für den Versicherten sichtbar (Ausnahme: "Whitelisting", siehe unten).
- 2910 2. Mittelgranulare Berechtigung (Kategorien)
 2911 Ein Versicherter kann Dokumente aus einen oder mehreren vorgegebenen
 2912 Dokumentenkategorien (z. B. Arztbriefe) freigeben. Die dadurch getätigte
 2913 Dokumentenauswahl wird mit dem grobgranularen Zugriffsrecht (siehe 1.) des
 2914 Berechtigten kombiniert. Das heißt, dass eine auf Arztbriefe berechtigte LEI je
 2915 nach Zugriffsrecht entweder nur die als "Normal" eingestuftten Arztbriefe sehen
 2916 kann oder auch die als "Vertraulich" gekennzeichneten. Mittelgranulare
 2917 Berechtigungen schränken die grobgranular vergebene Berechtigungen ggf. ein,
 2918 erweitern sie aber niemals. Die Metadaten eines Dokuments bzw. ihre
 2919 Zugehörigkeit zu einem Ordner entscheiden darüber, welchen Kategorien
 2920 (mindestens einer, potentiell mehreren) ein Dokument zugeordnet ist (siehe
 2921 auch [A_19388](#) in gemSpec_DM_ePA).
- 2922 3. Feingranulare Berechtigung (White- und Blacklist)
 2923 Der Versicherte kann einer LEI den Zugriff auf einzelne Dokumente gewähren
 2924 ("Whitelisting") oder entziehen ("Blacklisting"). Die Vergabe von feingranularen
 2925 Berechtigungen ist immer unabhängig von den vergebenen mittel- und
 2926 grobgranularen Berechtigungen. Steht also ein Dokument auf White- oder
 2927 Blacklist, spielen etwaige entgegenstehende grob- und feingranulare
 2928 Berechtigungen bei der Zugriffsentscheidung auf dieses Dokument keine Rolle.

5.4.2 Berufsgruppenspezifische Einschränkungen

Darüberhinaus gibt es einige berufsgruppenspezifische Vorgaben, welche die nach obigen Methoden vergebenen Berechtigungen insoweit einschränken, dass bestimmten Berufsgruppen der Zugriff auf festgelegte Dokumentenkategorien ausnahmslos verboten ist oder ausgewählte Operationen auf den dazugehörigen Dokumenten untersagt werden.

Beispielsweise haben Apotheker grundsätzlich keinen Zugriff auf das Zahnbonusheft (Kategorie "dentalrecord") des Versicherten (siehe Tab_Dokv_030 - Zugriffsunterbindungsregeln).

Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen, ändern oder löschen.

Weder der Versicherte, noch ein anderer Akteur kann die berufsgruppenspezifischen Zugriffsbeschränkungen umgehen.

Eine Übersicht über die unterschiedenen Berufsgruppen und die ihnen möglichen Berechtigungen finden sich in [Tab_Dokv_030 - Zugriffsunterbindungsregeln].

5.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln

Die Dokumentenverwaltung setzt die oben beschriebenen Berechtigungsvorgaben über zwei Mechanismen durch:

1. Dynamische Berechtigungsfreigaben (wie z. B. die Entscheidung, welche LEI überhaupt vom Versicherten berechtigt werden, in welcher Stufe, welchen Kategorien und mit welchen Ausnahmen) werden über "Policies" in die Dokumentenverwaltung eingestellt oder auch gelöscht.
2. Unabänderliche Regeln (wie die gesetzlich motivierten Vorgaben für Berufsgruppen) werden über entsprechende AFOs realisiert, insbesondere A_19303. Es ist natürlich umsetzender Software möglich, auch diese Regeln über interne Policies durchzusetzen.

Beide Mechanismen setzen bei der Durchsetzung an den XDS-Metadaten an, mit denen alle Dokumente grundsätzlich gekennzeichnet werden.

Die grobgranulare Dokumentenfreigabe wird über das XDS-Metadatum DocumentEntry.confidentialityCode umgesetzt, das die Vertraulichkeitsstufe des Dokuments festlegt. Dazu stehen folgende Codes (unter dem Code System Name "Confidentiality") zur Verfügung :

- Code = "N", Display Name = "normal"
- Code = "R", Display Name = "vertraulich"
- Code = "V", Display Name = "streng vertraulich"

Mittelgranulare Berechtigungen (kategoriebasiert) werden über verschiedene Metadaten(kombinationen) umgesetzt. Die Details sind A_19388 (gemSpec_DM_ePA) oder auch direkt den Policies in Anhang C zu entnehmen.

Feingranulare Berechtigungen, d.h. Freigabe oder Sperren einzelner Dokumente, erfolgt über die Auflistung von DocumentEntry.uniqueId-Kennzeichnern in einer White- bzw. Blacklist.

5.4.4 Vergabe von Zugriffsregeln

Der Versicherte und sein Vertreter können Berechtigungen aller Art (d.h. grob-, mittel- und feingranular für alle Zugriffsgruppen) entweder über das ePA-Frontend des Versicherten oder am KTR-AdV-Terminal in der Kostenträgerumgebung mittels dort zur Verfügung stehender ePA-FdV AdV vergeben.

Darüberhinaus können LEI über eine Adhoc-Berechtigung beim LEI vor Ort grob- und mittelgranular berechtigt werden.

Die zeitliche Gültigkeit der erteilten Zugriffsrechte wird vom Versicherten festgelegt. Sie wird zeitlich befristet oder unbefristet vergeben.

5.4.5 Funktionsprinzip Policy Administration

Die Berechtigungsvergabe an Leistungserbringerinstitutionen und Vertreter des Versicherten erfolgt durch das Einstellen von Policy Documents (siehe nachstehende Abbildung). Diese Dokumente werden in den Abschnitten 5.4.6.2 bis 5.4.6.5 für die ePA-Fachanwendung definiert und setzen ferner das Zugriffskontrollmodell Attribute-based Access Control (ABAC) um.

Die Registrierung dieser sogenannten Advanced Patient Privacy Consents erfolgt als unverschlüsselte Dokumente (jedoch über die sichere Verbindung zwischen dem Fachmodul ePA bzw. dem ePA-Frontend des Versicherten und dem Verarbeitungskontext) durch Nutzung der IHE ITI-Transaktionen "Cross-Gateway Document Provide" [ITI-80] sowie "Provide And Register Document Set-b" [ITI-41]. Die interne Datenhaltung bzgl. der Policy Documents (Advanced Patient Privacy Consents) ist nicht vorgegeben, allerdings müssen diese Policy Documents über die Standard-Abfrageschnittstelle über die Operation `I_Document_Management_Insurant::RegistryStoredQuery` dem ePA-Frontend des Versicherten zugänglich gemacht werden. Dazu werden die `DocumentEntry`-Metadaten gemäß der Anforderung [gemSpec_DM_ePA#A_14961] vorgegeben.

Die grundlegende Zugriffsstrategie ist "opting-in", sodass ein gewährendes Zugriffsrecht nur durch Registrierung eines neuen Policy Documents vergeben werden kann. Eine inhaltliche Änderung eines Policy Documents ist nicht vorgesehen. Stattdessen soll durch den Client ein zu einem Berechtigten vorhandenes Policy Document gelöscht und ein neues registriert werden. Wurde ein vorhandenes Policy Document, das demselben Berechtigten zuzuordnen ist (d.h. `xacml:SubjectMatch`, `xacml:ResourceMatch` sind identisch), durch den Client nicht gelöscht, wird dieses von der ePA-Dokumentenverwaltung automatisch gelöscht, während das neue Policy Document eingestellt wird.

A_14998 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen vom Policy Document bei neuem Policy Document mit demselben Berechtigten

Die Komponente ePA-Dokumentenverwaltung MUSS über die Operationen

`I_Document_Management::CrossGatewayDocumentProvide` sowie

`I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b` eine Prüfung auf ein bereits registriertes Policy Document (Advanced Patient Privacy Consent) mit demselben Berechtigten sowie der Aktenidentität (d.h. `xacml:SubjectMatch` und `xacml:ResourceMatch` sind identisch) durchführen und bei Existenz dieses Policy Documents (Advanced Patient Privacy Consent) dieses samt IHE ITI-XDS-

3015 Metadaten löschen, bevor ein neues Policy Document gespeichert wird.
3016 [\leq]

3017 **A_14892-02 - Komponente ePA-Dokumentenverwaltung – Automatisiertes**
3018 **Löschen ungültiger Policy Documents**

3019 Die Komponente ePA-Dokumentenverwaltung SOLL Policy Documents (Advanced Patient
3020 Privacy Consents) und zugehörige IHE ITI-XDS-Metadaten löschen, wenn diese Policy
3021 Documents ihre zeitliche Gültigkeit verlieren. [\leq]

3022

3023 Der durch die vorstehende Anforderung motivierte Vorgang kann nur ausgeführt werden,
3024 wenn der Verarbeitungskontext für das Aktenkonto durch einen berechtigten Nutzer
3025 aktiviert wurde.

3026 **A_14895 - Komponente ePA-Dokumentenverwaltung – Schutz vor Manipulation**
3027 **der Policy Documents**

3028 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Policy
3029 Documents (Advanced Patient Privacy Consents) gegen Veränderung und unberechtigtes
3030 Löschen geschützt sind.

3031 [\leq]

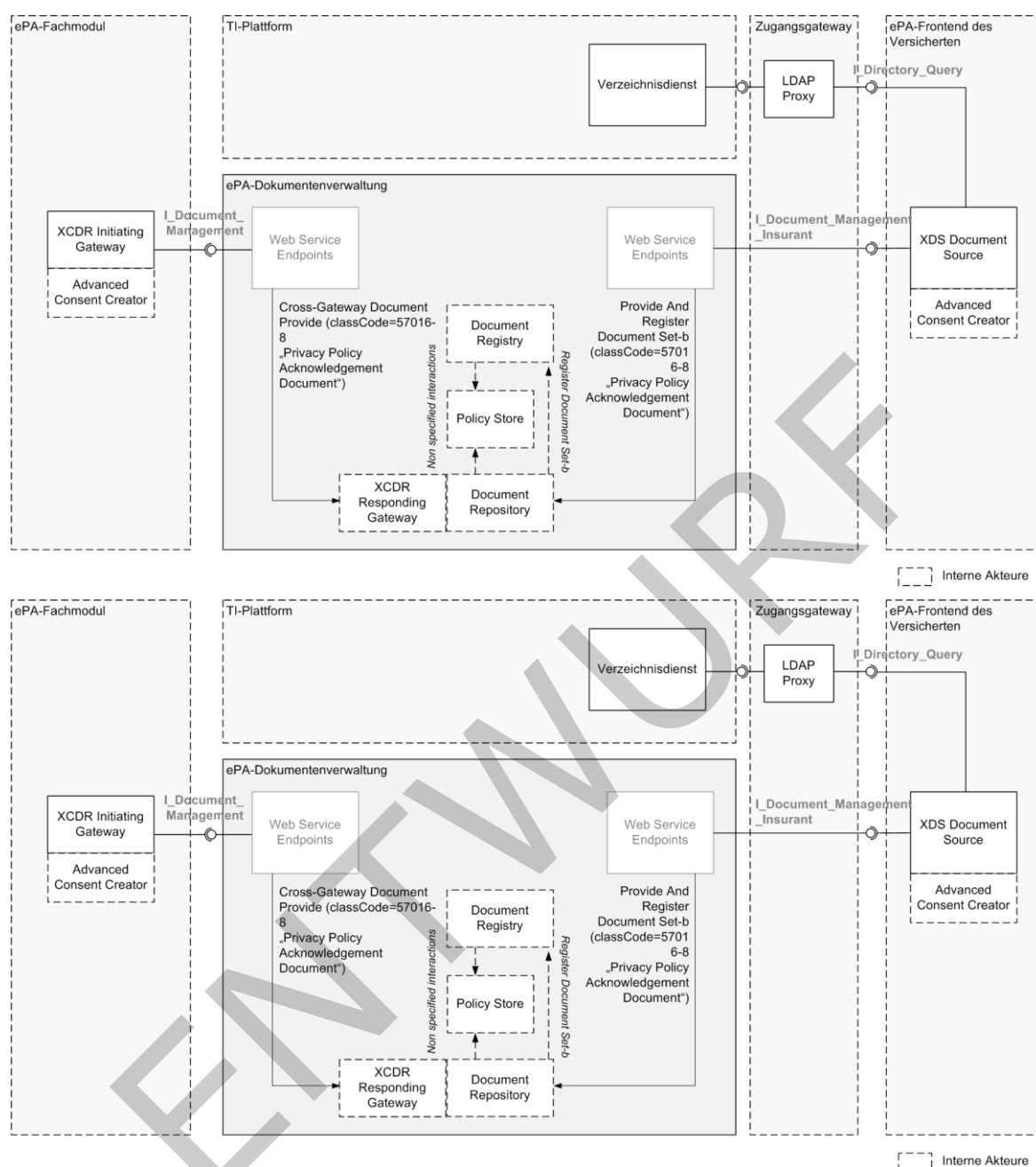


Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen

Hinweis: Die vorstehende Abbildung verdeutlicht, wie Berechtigungen über die entsprechenden IHE ITI-Transaktionen vergeben werden. Der Transaktion "Cross-Gateway Document Provide" liegt genaugenommen keine IHE ITI-konforme Nachricht des Primärsystems zum Einstellen des Policy Documents durch den Versicherten zugrunde. Stattdessen wird diese Transaktion durch die Web-Service-Operation "RequestFacilityAuthorization" gemäß [\[gemSpec FM ePA#7.2.1.2\]](#) ausgelöst, sodass sich die Verwendung der Transaktion "Cross-Gateway Document Provide" eigentlich verbietet. Aus Praktikabilitätsgründen ist jedoch keine separate Schnittstelle mit der Transaktion "Provide And Register Document Set-b" für die

3046 Schnittstelle I_Document_Management zum Einstellen eines Policy Documents gegenüber
3047 der ePA-Dokumentenverwaltung definiert.

3048 Der Entzug von Berechtigungen erfolgt über das Löschen von ausgewählten Policy
3049 Documents durch Ausführung der
3050 Operation `I_Document_Management_Insurant::RemoveMetadata`, wie die folgende
3051 Abbildung verdeutlicht.

3052

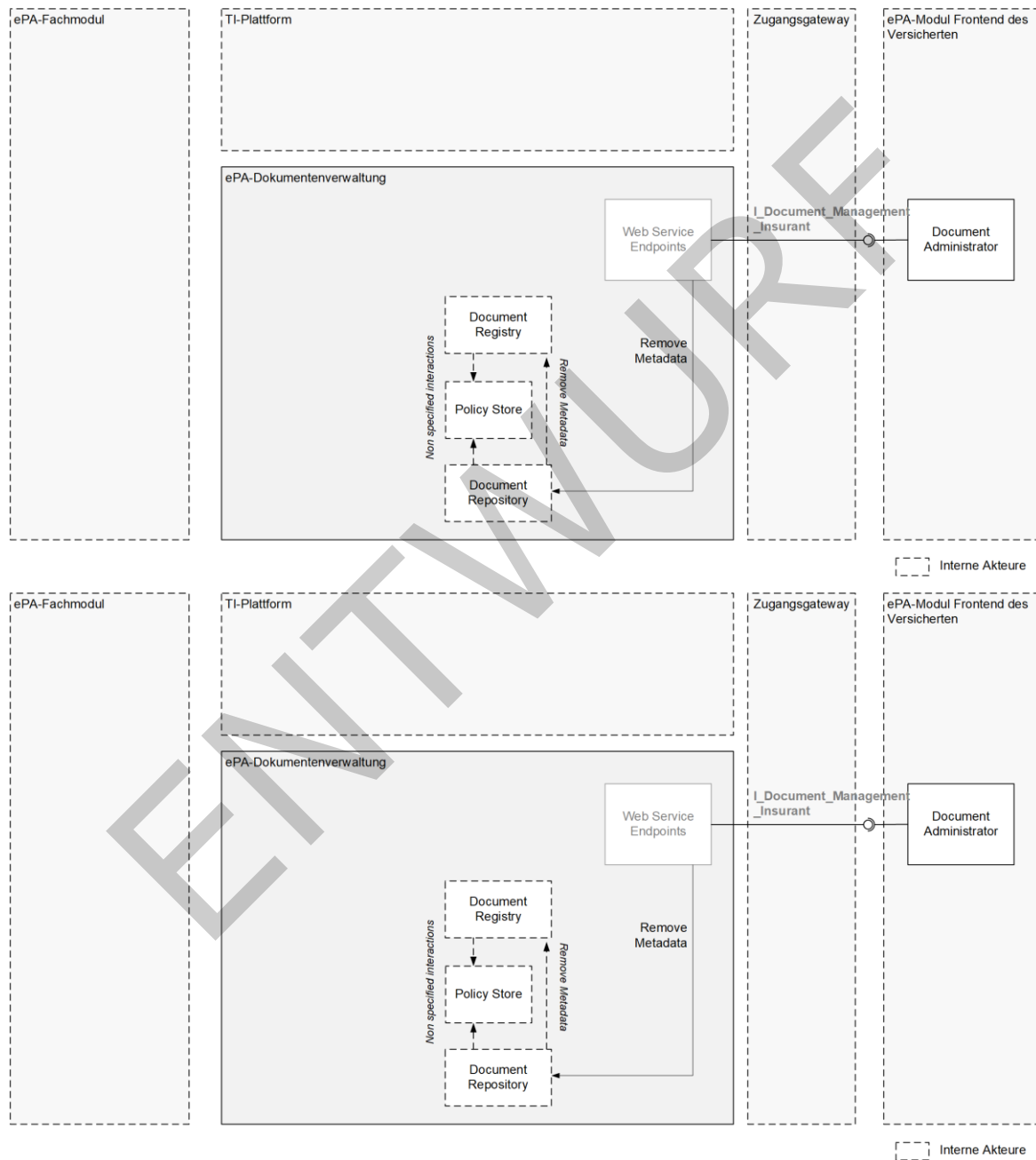


Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen

5.4.6 Anforderungen an die Zugriffskontrollprüfung

Die Zugriffskontrollprüfung innerhalb des Verarbeitungskontextes der Komponente ePA-Dokumentenverwaltung erfolgt aufbauend auf einer Grundeinstellung, die jeden Zugriff verweigert, wenn er nicht explizit erlaubt ist und setzt die Berechtigungsszenarien um.

A_19303-03 - Komponente ePA-Dokumentenverwaltung - Zugriffsunterbindungsregeln

~~A_19303-02 - Komponente ePA-Dokumentenverwaltung - Berufgruppenspezifische Zugriffsunterbindungsregeln~~

Die Komponente ePA-Dokumentenverwaltung MUSS alle in der Tabelle Tab_Dokv_030 - Zugriffsunterbindungsregeln aufgeführten ~~berufgruppenspezifischen~~ Zugriffsunterbindungsregeln durchsetzen. Die Komponente ePA-Dokumentenverwaltung MUSS ~~dazu~~ beim Aufruf einer der Operationen der Schnittstelle I_Document_Management die übergebene AuthenticationAssertion dahingehend prüfen, ob die ProfessionOID der ZertifikatsExtension Admission gemäß [gemSpec_PKI#Anhang A] im Signaturzertifikat C.HCI.OSIG (/saml2:Assertion/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate) für die Operation, ausgeführt auf eine bestimmte Dokumentenkategorie, zugriffsberechtigt ist. Das Ausführen von Operationen auf Dokumentenkategorien, die nicht explizit erlaubt sind, muss verhindert werden ("Access Deny").

Tabelle 32: Tab_Dokv_030 - Zugriffsunterbindungsregeln

Dokumentenkategorie gemäß § 341 PDSG Absatz 2		Zugriffsrecht										
Nr.	Technischer Identifizier	Arzt	ZArzt	Apo	Psych	Pflege	Heb	Phys	GD	AM	KTR	Ver
1a1	practitioner	CRUD	CRUD	R	CRUD	R	R	R	CRUD	R	-	RD
1a2	hospital	CRUD	CRUD	R	CRUD	R	R	R	CRUD	R	-	RD
1a3	laboratory	CRUD	CRUD	R	CRUD	R	R	R	CRUD	R	-	RD
1a4	physiotherapy	CRUD	CRUD	R	CRUD	R	R	CRUD	CRUD	R	-	RD
1a5	psychotherapy	CRUD	CRUD	R	CRUD	R	R	R	CRUD	R	-	RD
1a6	dermatology	CRUD	CRUD	R	CRUD	R	R	R	CRUD	R	-	RD

1a7	gynaecology_u rology	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RD
1a8	dentistry_oms	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RD
1a9	other_medical	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RD
1a10	other_non_me dical	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RD
1b	emp	CRU D	CRU D	CRU D	CRU D	R	R	R	CRU D	R	-	RD
1c	nfd	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RD
1d	eab	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RD
2	dentalrecord	CRU D	CRU D	-	CRU D	R	-	-	CRU D	R	-	RD
3	childsrecord	CRU D	CRU D	R	CRU D	R	CRU D	R	CRU D	R	-	RD
4	mothersrecord	CRU D	CRU D	R	CRU D	R	CRU D	R	CRU D	R	-	RD
5	vaccination	CRU D	CRU D	CRU D	CRU D	R	R	-	CRU D	CRU D	-	RD
6	patientdoc	RD	RD	R	RD	R	R	R	RD	R	-	CRU D
7	ega	RD	RD	R	RD	R	R	R	RD	R	-	CRU D
8	receipt	RD	RD	RD	RD	R	R	R	RD	R	CU	RD
10	care	CRU D	CRU D	R	CRU D	CRU D	R	R	CRU D	R	-	RD
11	prescription	CRU D	CRU D	CRU D	CRU D	R	R	R	CRU D	R	-	RD
12	eau	CRU D	CRU D	-	CRU D	-	-	-	CRU D	R	-	RD

13	other	CRU D	CRU D	-	CRU D	-	-	-	CRU D	R	-	RD
----	-------	----------	----------	---	----------	---	---	---	----------	---	---	----

Legende der Zugriffsrecht CRUD, Zuordnung zur Operation:

- C (create), U (update)=I_Document_Management::CrossGatewayDocumentProvide, I_Document_Management_Insurant::RestrictedUpdateDocumentSet, I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b, I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b;
- R (read)=I_Document_Management::CrossGatewayQuery, I_Document_Management::CrossGatewayRetrieve, I_Document_Management_Insurant::CrossGatewayQuery, I_Document_Management_Insurant::CrossGatewayRetrieve;
- D (delete)=I_Document_Management::RemoveMetadata, I_Document_Management::RemoveDocuments, I_Document_Management Insurant::RemoveMetadata;
- == "-" = keine Zugriffsrechte;

Legende der Institutionen, Zuordnung zur ProfessionOID:

- Arzt=oid_praxis_arzt, oid_krankenhaus, oid_institution-vorsorge-reha, oid_sanitaetsdienst-bundeswehr;
- ZArzt=oid_zahnarztpraxis;
- Apo=oid_öffentliche_apotheke;
- Psych=oid_praxis_psychotherapeut;
- Pflege=oid_institution-pflege;
- Heba=oid_institution-geburtshilfe;
- Phys=oid_praxis-physiotherapeut;
- GD=oid_institution-oegd;
- AM=oid_institution-arbeitsmedizin;
- KTR=oid_epa_ktr;

Legende Zugriffsberechtigte, Zuordnung über KVNR:

- Ver=Versicherter/Vertreter;

[<=]

Ein Document Replacement (urn:ihe:iti:2007:AssociationType:XFRM RPLC) ändert den DocumentEntry.availabilityStatus des ersetzten Dokuments auf "Deprecated" und ist deshalb im Rahmen von A_19303 als Create-Operation ("C") für das neue Dokument und als Update-Operation ("U") für das ersetzte Dokument zu werten.

A_21211 - Komponente ePA-Dokumentenverwaltung - Änderungen von Zugriffsunterbindungsregeln nicht erlauben

Die Komponente ePA-Dokumentenverwaltung MUSS durch technische Maßnahmen sicherstellen, dass Änderungen von Tab Dokv_030 - Zugriffsunterbindungsregeln ausgeschlossen sind.

[<=]

A_15173-03 - Komponente ePA-Dokumentenverwaltung – Zugriffsstrategie "Opting-in" mit "Access Deny" als Standardeinstellung

Die Komponente ePA-Dokumentenverwaltung MUSS jeden Zugriff verweigern, der nicht auf der Grundlage definierter Policy Documents (Advanced Patient Privacy Consents) in Kombination mit der entsprechenden Operation gemäß

A_19303, A_19997, A_19998 oder A_20736 explizit erlaubt ist. [\leq]

A_20736 - Komponente ePA-Dokumentenverwaltung – Generelles schreibendes Zugriffsrecht für LEI

Die Komponente ePA-Dokumentenverwaltung MUSS einen schreibenden Zugriff ("C" und "U" gemäß Tabelle in A_19303) für eine per Policy gemäß 9.3 berechnete LEI zulassen, selbst wenn die Policy diesen nicht ausdrücklich erlaubt. Wenn A_19303 der LEI als Angehöriger einer bestimmten Berufsgruppe allgemein Zugriff auf die gewählte Dokumentenkategorie untersagt (d.h. für die Kategorie generell weder "C" noch "U" erlaubt), MUSS der Zugriff jedoch weiterhin abgelehnt werden.

[\leq]

Policy Documents nach Anhang C steuern den erlaubten Zugriff für Versicherte, deren Vertreter, für Leistungserbringerinstitutionen sowie Kostenträger. Tatsächlich sind die erlaubten Operationen für alle diese Gruppen jedoch statisch: Sobald ein bestimmter Leistungserbringer (oder ein Angehöriger einer anderen Gruppe) grundsätzlich berechtigt ist, stehen die erlaubten Operationen (Dokumente einstellen, suchen, herunterladen, ...) unveränderlich fest.

Aus diesem Grund ist der Bereich "Actions", der die erlaubten Operationen üblicherweise in APPC-Policy-Dokumenten beschreibt dort nicht gesetzt, um die APPC-Dokumente übersichtlich zu halten. Stattdessen werden die gemäß Berufsgruppe zur Verfügung stehenden Operationen in Tab_Dokv_030 (via A_15173-02) festgelegt und geprüft.

Eine Ausnahme ist die generelle Erlaubnis für grundsätzlich berechnete LEI (d.h. solche, für die eine wie auch immer geartete Policy eingestellt wurde), Dokumente in die Akte einzustellen, sofern sie für die gewählte Dokumentenkategorie generell das Zugriffsrecht "C" oder "U" gemäß Tab_Dokv_030 besitzen.

Beispiel: Ein gemäß APPC-Policy-Dokument berechtigter Kostenträger darf nur Dokumente der Kategorie 8 zugreifen, und zwar nach Tabelle ausschließlich mittels CU-Operation (create, update), d.h. I_Document_Management::CrossGatewayDocumentProvide. Ein Zugriff auf andere Dokumentenkategorien würde durch das APPC-Policy-Dokument verhindert, ein Zugriff durch andere Operationen (bspw. ein Löschen via I_Document_Management::RemoveMetadata) durch Tab_Dokv_030.

Beispiel 2: Ein Leistungserbringer ist nur auf ein einziges Dokument berechtigt (ein Whitelist-Eintrag). Es ist also weder ein grobgranulares noch ein mittelgranulares Zugriffsrecht vergeben worden. Der Leistungserbringer darf damit nur auf dieses eine Dokument lesend ("R") und ggf. löschend ("D") zugreifen, darf aber gemäß A_20736 alle Dokumente einstellen, für deren Kategorie er nach Tab_Dokv_030 die Berechtigung "C" oder "U" besitzt. Letzteres Recht ist ihm auch nicht zu entziehen (außer über den kompletten Entzug der Berechtigung über Löschen der Policy).

Policy Documents, welche die Berechtigung für klassifizierte Nutzer steuern (d.h. für den Versicherten, seine Vertreter, für Leistungserbringerinstitutionen sowie Kostenträger), referenzieren jeweils eine oder mehrere statische, akteninterne XACML 2.0 Policy (Permission Policies). Diese statischen Policies müssen für die Zugriffskontrollprüfung innerhalb des Verarbeitungskontextes verfügbar sein und verlassen die ePA-Dokumentenverwaltung nicht. XACML 2.0 Policies, welche interne Permission Policies referenzieren, heißen im Folgenden Base Policies.

A_19997-01 - Zugriff durch Versicherten auf Schnittstelle

I_Account_Management_Insurant und I_Key_Management_Insurant

Die Komponente ePA-Dokumentenverwaltung MUSS dem Versicherten über A_15173-02 hinaus den Zugriff auf die Operationen der Schnittstellen I_Account_Management_Insurant und I_Key_Management_Insurant erlauben. [\leq]

A_19998-01 - Zugriff durch Vertreter auf Operation

I_Account_Management_Insurant::GetAuditEvents und GetSignedAuditEvents

A_19998—Zugriff durch Vertreter auf Operation

~~I_Account_Management_Insurant::GetAuditEvents~~ Die Komponente ePA-Dokumentenverwaltung MUSS einem berechtigten Vertreter des Versicherten über A_15173-02 hinaus den Zugriff auf die Operation

I_Account_Management_Insurant::GetAuditEvents() und

I_Account_Management_Insurant::GetSignedAuditEvents() erlauben.

[\leq]

~~A_14933-01~~A_14933 - Komponente ePA-Dokumentenverwaltung – XML

Schema-Validierung eines Policy Documents

Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Documents (Advanced Patient Privacy Consents) dieses einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen. Ist ein Policy Document nicht wohlgeformt oder gültig, MUSS die Komponente ePA-Dokumentenverwaltung die Nachricht mit einem HTTP-Statuscode 200 oder 400 gemäß [RFC7231] quittieren und einen geeigneten Fehler in der IHE-Antwortnachricht zurückgeben. [\leq]

~~A_15536-02~~A_15536-01 - Komponente ePA-Dokumentenverwaltung – Prüfungen bei Registrierung eines Policy Documents

Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Documents (Advanced Patient Privacy Consents) folgende inhaltlichen Prüfungen durchführen und im Fehlerfall die Nachricht mit einem HTTP-Statuscode 200 oder 400 gemäß [RFC7231] quittieren und einen geeigneten Fehler in der IHE-Antwortnachricht zurückgeben:

- *Prüfung der XACML 2.0 Policy-Konformität*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn das Profil der vorliegenden XACML 2.0 Policy nicht mit den Anforderungen aus den Abschnitten 5.4.6.2 bis 5.4.6.5 übereinstimmt.
- *Prüfung der Aktenidentität*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn das Resource-Element mit der Attribut-ID "urn:ihe:iti:ser:2016:patient-id" nicht mit der Identität der Akte aus dem internen Policy Document mit der Policy Set ID "urn:gematik:policy-set-id:insurant" übereinstimmt.
- *Prüfung des Einstellers*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn die in der Nachricht enthaltene SAML 2.0 Assertion (Authentication Assertion / X-User Assertion) nicht dem Versicherten oder einem seiner Vertreter zugeordnet ist (d.h. das root-Attribut des InstanceIdentifier-Elements innerhalb des SubjectMatch-Elements muss mit der OID "1.2.276.0.76.4.8" eine KVN Kennzeichen).
- *Keine Verwendung des "xsi:schemaLocation"-Attributs*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML

2.0 Policy abbrechen, wenn ein xsi:schemaLocation-Attribut gemäß [XMLSchema#2.6.3] enthalten ist.

- Verstöße gegen Policy-Struktur und -Inhalte
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn sie Verstöße gegen die Vorgaben aus [gemSpec_DM_ePA#A_14961] verstößt.

[<=]

A_14822-01 - Komponente ePA-Dokumentenverwaltung – Attribute für Anfrage einer Autorisierungsentscheidung

Die Komponente ePA-Dokumentenverwaltung MUSS das "Policy Pull"-Muster gemäß [IHE-ITI-ACWP] umsetzen und die folgenden Daten für eine Berechtigungsprüfung extrahieren sowie eine Autorisierungsanfrage gegen die vorhandenen Policy Documents (Advanced Patient Privacy Consents) stellen, um die autorisierte Verarbeitung eines Dokuments sicherzustellen:

- Subject ID oder XSPA Organization ID der Authentication Assertion / X-User Assertion
- unveränderbarer Teil der KVNR aus der Eingangsnachricht oder serverseitig mit Hilfe von Anfrageparametern beschafft (Aktenidentität)
- wsa:Action-Element aus der Eingangsnachricht
- ggf. Metadaten des DocumentEntry (u.a. confidentialityCode), des dazugehörigen SubmissionSets und etwaiger verbundener Ordner

[<=]

A_20217 - Komponente ePA-Dokumentenverwaltung – APPC Erweiterung für SubmissionSet.authorRole

Die Komponente ePA-Dokumentenverwaltung MUSS das XACML-Attribute "urn:gematik:ig:document-entry:related-submission-set:author-role" wie folgt unterstützen:

XACML Target Section	Resource
XACML Attribute ID	urn:gematik:ig:document-entry:related-submission-set:author-role
XACML Data Type	urn:hl7-org:v3#CV
XACML MatchID	urn:hl7-org:v3:function:CV-equal
XACML Attribute Value Content	Use CX.4.2 as codeSystem and CX.1 as extension

XACML Beispiel	<pre> <Resource> <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal"> <AttributeValue DataType="urn:hl7-org:v3#CV"> <CodedValue code="102" codeSystem="1.3.6.1.4.1.19376.3.276.1.5.13"/> </AttributeValue> <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-entry:related-submission- set:author-role" DataType="urn:hl7-org:v3#CV"/> </ResourceMatch> </Resource> </pre>
-------------------	--

3245
3246

[<=]

3247 **A_16195 - Komponente ePA-Dokumentenverwaltung – UTF-8-Kodierung eines**
3248 **Policy Documents**

3249 Die Komponente ePA-Dokumentenverwaltung MUSS ausschließlich UTF-8-kodierte Policy
3250 Documents verarbeiten.[<=]

3251 **5.4.6.1 Erstmaliges Öffnen eines Verarbeitungskontextes**

3252 Beim erstmaligen Öffnen des Verarbeitungskontextes eines neu registrierten Aktenkontos
3253 durch den Versicherten muss dieser erkennen, dass er erstmalig geöffnet wird und die
3254 Aktenzustände "Registered" und "Registered for Migration"
3255 gemäß [gemSpec Aktensystem#6.1.1](#) unterscheiden. Darüber hinaus ist der
3256 Verarbeitungskontext für den Versicherten gemäß der Anforderung A_15250 zu
3257 personalisieren. Die für die Personalisierung und die Unterscheidung der Aktenzustände
3258 erforderliche Konfiguration des Verarbeitungskontextes für das Aktenkonto erfolgt über
3259 die Authorization Assertion.

3260 **A_15603 - Komponente ePA-Dokumentenverwaltung – Nur Resume Account**
3261 **bei erforderlicher Datenübernahme möglich**

3262 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass ausschließlich die
3263 Operation `I_Account_Management_Insurant::ResumeAccount` ausgeführt werden kann,
3264 wenn der Verarbeitungskontext erstmalig vom Versicherten geöffnet wurde und eine
3265 Übernahme von Daten aus dem Aktenkonto des Versicherten bei einem vorherigen
3266 Anbieter erforderlich ist, d.h. das Aktenkonto mit der Option "Registered for Migration"
3267 registriert wurde.[<=]

3268 **5.4.6.2 Berechtigung für einen Versicherten**

3269 **A_15437-01 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben**
3270 **zum Inhalt eines Policy Documents zur Berechtigung eines Versicherten**

3271 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS eine
3272 XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-
3273 ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_500 in
3274 Anhang C durchsetzen.[<=]

3275 Um dem Versicherten Zugriff auf seine Akte zu gewähren, wird die Akte im Zuge ihrer
3276 Erstbenutzung durch den Versicherten personalisiert und ein Versicherten-Policy-
3277 Document erstellt bzw. aktiviert.

A_15250 - Komponente ePA-Dokumentenverwaltung – Aktivierung des Policy Documents "urn:gematik:policy-set-id:insurant"

Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS eine Personalisierung durchführen. Dazu MUSS die Komponente ePA-Dokumentenverwaltung das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-id:insurant" aktivieren und anschließend die darin festgelegten Regeln bei Zugriffsanfragen durchsetzen. Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die Personalisierung im Zuge des ersten Aufrufs einer fachlichen Operation durchführen und das Policy Document unmittelbar auf die fachliche Operation anwenden, die die Personalisierung ausgelöst hat. Der Aufruf der Operation `I_Document_Management_Connect::OpenContext` zur kryptographischen Aktivierung gilt in diesem Zusammenhang nicht als fachliche Operation. [\leq]

Die Festlegung des Zeitpunkts der Personalisierung in der vorstehenden Anforderung verhindert die Personalisierung eines Verarbeitungskontexts für den Fall, dass für ein mit der Option "Registered for Migration" registriertes Aktenkonto der Verarbeitungskontext geöffnet wird, ohne dass unmittelbar anschließend die Operation `I_Account_Management_Insurant::ResumeAccount` aufgerufen wird. Der Verarbeitungskontext verbleibt damit in seinem initialen (d.h. ungenutzten) Zustand, so dass der Vorgang konsistent neu gestartet werden kann.

A_15178 - Komponente ePA-Dokumentenverwaltung – Unveränderliches Policy Document "urn:gematik:policy-set-id:insurant"

Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-id:insurant" nach ihrer Aktivierung kontinuierlich und dauerhaft unverändert für die Zugriffskontrollprüfung wirksam ist. [\leq]

5.4.6.3 Berechtigung für einen Vertreter**A_15440-01 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Vertreters**

Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten übermittelte XACML 2.0 Policy auf Konformität als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in Tab_Dokv_501 in Anhang C prüfen. [\leq]

A_15441-01 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Vertreters mit erlaubten Operationen

Die Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_501 in Anhang C erstellen und durchsetzen. [\leq]

A_15180 - Komponente ePA-Dokumentenverwaltung – Prüfung auf weitere, unerlaubte Vertreterberechtigungen

Die Komponente ePA-Dokumentenverwaltung MUSS ein von einem Vertreter übermitteltes Policy Document (Advanced Patient Privacy Consent) ablehnen, falls das XACML 2.0 Subject nicht das Attribut "urn:gematik:subject:organization-id" enthält. [\leq]

5.4.6.4 Berechtigung für eine Leistungserbringerinstitution

A_15442-02 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung einer Leistungserbringerinstitution

Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten bzw. vom Fachmodul ePA übermittelte XACML 2.0 Policy auf Konformität als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt von Tab_Dokv_502 in Anhang C prüfen.

[<=]

5.4.6.5 Berechtigung für einen Kostenträger

A_17460-01 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Kostenträgers

Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten übermittelte XACML 2.0 Policy auf Konformität als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in Tab_Dokv_503 in Anhang C prüfen.[<=]

5.4.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4

Bei einem Upgrade von ePA Release 3.1.3 auf Release 4 ändert sich das Berechtigungssystem. Deshalb müssen zum einen Dokumentenmetadaten (confidentialityCode) und zum anderen die Berechtigungsregeln selbst (APPC Policy-Dokumente) angepasst werden. Davon sind nicht nur neue Dokumente betroffen, sondern es müssen auch bestehende Metadaten und Policies angepasst werden.

Im Ergebnis akzeptiert die ePA-Dokumentenverwaltung in Release 4 alte Policy-Dokumente und Dokumente mit alten confidentialityCodes (beides gemäß (gemäß ePA Release 3.1.3), liefert nach außen jedoch beides nur nach neuen Vorgaben (Release 4) zurück. Dieses Verhalten soll es auch (insbesondere) Primärsystemen nach alter Spezifikation erlauben, mit einem aktuellen Aktensystem zu kommunizieren.

A_20039 - Komponente ePA-Dokumentenverwaltung – Transformation von Policy-Dokumenten hin zu neuerer Version

Die Komponente ePA-Dokumentenverwaltung MUSS sämtliche XACML 2.0 Policies gemäß Anhang B umwandeln in XACML 2.0 Policies gemäß Anhang C, sobald

- eine XACML 2.0 Policy gemäß Anhang B eingestellt wird,
- ein Zugriffsversuch auf eine XACML 2.0 Policy gemäß Anhang B erfolgt.

[<=]

Während die Transformation der Policy-Dokumente stattfindet, und solange sie nicht abgeschlossen ist, werden weitere Zugriffsversuche mit der Fehlermeldung "Aktenkonto vorübergehend nicht erreichbar" abgelehnt.

A_20049-01 - Komponente ePA-Dokumentenverwaltung – Regeln für die Policy-Transformation

Bei der Transformation der XACML 2.0 Policy ohne die Versionsangabe @Version MUSS die vom Client eingestellten Base- und ggf. vorhandene Permission Policies durch eine entsprechende XACML 2.0 Policy mit Versionsangabe @Version ersetzt werden. Bei der Transformation gelten folgende Vorgaben:

- 3370 • Das Ablaufdatum MUSS übernommen werden.
- 3371 • Bei der Ersetzung der XACML 2.0 Policies ohne Versionsangabe (alt) durch XACML
- 3372 2.0 Policies mit Versionsangabe (neu) MÜSSEN folgende Zugriffsregeln umgesetzt
- 3373 werden (Zugriffsrecht alt wird zu Zugriffsrecht neu):
- 3374 • alt: LEI, neu: practitioner, hospital, laboratory, physiotherapy,
- 3375 psychotherapy, dermatology, gynaecology_urology, dentistry_oms,
- 3376 other_medical, other_non_medical, emp, nfd, eab;
- 3377 • alt: PAT, neu: patientdoc;
- 3378 • alt: KTR, neu: receipt;
- 3379 • neu: Die Vertrauensstufe "normal" (grobgranulare Berechtigung) wird vergeben
- 3380 [\leq]
- 3381 **A_20046 - Komponente ePA-Dokumentenverwaltung – Transformation des**
- 3382 **confidentialityCodes bei eingestellten Dokumenten**
- 3383 Die Komponente ePA-Dokumentenverwaltung MUSS bei allen Dokumenten eines
- 3384 Versicherten, bei denen der confidentialityCode "PAT", "LEI", "LEÄ" oder "KTR"
- 3385 gesetzt ist, diesen Eintrag löschen und stattdessen den confidentialityCode "normal"
- 3386 setzen. Diese Transformation MUSS durch die Komponente ePA-Dokumentenverwaltung
- 3387 nach dem ersten erfolgreichen Öffnen der Akte des Versicherten (Operation
- 3388 I_Document_Managemet_Connect::OpenContext()) und nachfolgend beim Einstellen
- 3389 jedes DocumentEntry, der noch alte confidentialityCodes enthält, durchgeführt werden.
- 3390 [\leq]
- 3391 Damit soll die Transformation zum frühestmöglichen Zeitpunkt durch die
- 3392 ePA_Dokumentenverwaltung durchgeführt werden.
- 3393 **A_20050-01 - Komponente ePA-Dokumentenverwaltung – Abbildung von**
- 3394 **Suchanfragen nach confidentialityCodes und deren Ergebnisse**
- 3395 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
- 3396 MUSS bei Aufruf der Operation I_Document_Management::CrossGatewayQuery mit
- 3397 Suchparametern zum confidentialityCode "LEI", "PAT" oder "KTR" die Suche
- 3398 stattdessen auf die folgenden Kategorien abbilden (alt: eingehende Suchanfrage, neu:
- 3399 durchsuchte Kategorien) und entsprechende Ergebnisse zurückliefern:
- 3400 • alt: LEI, neu: practitioner, hospital, laboratory, physiotherapy,
- 3401 psychotherapy, dermatology, gynaecology_urology, dentistry_oms,
- 3402 other_medical, other_non_medical, emp, nfd, eab;
- 3403 • alt: PAT, neu: patientdoc;
- 3404 • alt: KTR, neu: receipt;
- 3405 [\leq]
- 3406 Etwaige Berechtigungsregeln, die der Herausgabe einzelner Dokumente an den Client
- 3407 entgegenstehen (z. B. Blacklisting einzelner Dokumente oder nichterteilte
- 3408 Zugriffsberechtigung auf emp) müssen dabei weiterhin berücksichtigt werden.

5.5 Vertrauenswürdige Ausführung

5.5.1 Schnittstelle I_Document_Management_Connect

Diese Schnittstelle setzt die in [gemSysL_ePA] definierte Schnittstelle `I_Document_Management_Connect` technisch um. Die logische Operation `I_Document_Management_Connect::ConnectToContext` aus [gemSysL_ePA] wird durch den Verbindungsaufbau der Clients zum Verarbeitungskontext der ePA-Dokumentenverwaltung umgesetzt. Die Client-Verbindungen vom Fachmodul ePA zu der Schnittstelle sowie vom ePA-Frontend des Versicherten zu der Schnittstelle werden über HTTP hergestellt. Die Schnittstelle ermöglicht beiden Clients den Aufbau eines sicheren Kanals auf Inhaltsebene zum Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung (VAU), die Aktivierung des Verarbeitungskontextes mittels Übergabe des Kontextschlüssels sowie die Beendigung ihrer Client-Verbindung. Das Fachmodul ePA baut zum Kontextmanagement je Aktensession eine TLS-Verbindung auf. Die Verbindung des ePA-Frontends des Versicherten zum Kontextmanagement erfolgt mittels Weiterleitung der HTTP Requests und HTTP Responses durch das Zugangsgateway, welches auch einen HTTP Header zur Identifikation der Sitzung setzt.

Das Protokoll für den Verbindungsaufbau zwischen Clients und dem Verarbeitungskontext folgt den Spezifikationen in [gemSpec_Krypt#3.15] und [\[gemSpec_Krypt#6\]](#). Zur Prüfung der Autorisierung des Clients durch das Kontextmanagement wird das dort beschriebene Protokoll um zwei zusätzliche Schlüssel-Wert-Paare ergänzt, die die Authorization Assertion im HTTP Body in der `VAUClientHello`-Nachricht und optional einen Sitzungsbezeichner im HTTP Header übermitteln.

A_15587 - Komponente ePA-Dokumentenverwaltung – Implementierung des sicheren Verbindungsprotokolls

Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS für die Schnittstelle `I_Document_Management_Connect` das Kommunikationsprotokoll gemäß den Vorgaben aus [gemSpec_Krypt#3.15] und [\[gemSpec_Krypt#6\]](#) umsetzen.
[<=]

A_15592-03 - Komponente ePA-Dokumentenverwaltung – Erweiterung des sicheren Verbindungsprotokolls

Ein Client (d.h. ePA-Fachmodul, ePA-Frontend des Versicherten, Fachmodul ePA KTR-Consumer) MUSS bei der Erzeugung der `VAUClientHello`-Nachricht (vgl. [A_16883-01](#)) im Datenfeld `AuthorizationAssertion` die Base64-kodierte Authorization Assertion eintragen.

Weiterhin MUSS der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung ein optionales Schlüssel-Wert-Paar zur Übermittlung eines Sitzungsbezeichners an das Kontextmanagement im HTTP-Request-Header prüfen und akzeptieren. Das Schlüssel-Wert-Paar hat die Form
`Session: ...Sitzungsbezeichner vom Zugangsgateway...` [<=]

A_14631-02 - Komponente ePA-Dokumentenverwaltung – HTTP-Schnittstelle I_Document_Management_Connect

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die Schnittstelle `I_Document_Management_Connect` für über das Zugangsgateway vermittelte HTTP-Verbindungen des ePA-Frontend des Versicherten verfügbar machen. [<=]

A_15540 - Komponente ePA-Dokumentenverwaltung – TLS-Schnittstelle I_Document_Management_Connect

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die Schnittstelle `I_Document_Management_Connect` für TLS-Verbindungen des Fachmoduls

3457 ePA sowie des Fachmoduls ePA KTR-Consumer verfügbar machen.

3458 [`<=`]

3459 **A_15588 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext**
3460 **bei Bedarf verfügbar machen**

3461 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS

3462 Verarbeitungskontexte bedarfsgesteuert für autorisierte Nutzer verfügbar machen. [`<=`]

3463 **A_14633-02 - Komponente ePA-Dokumentenverwaltung – Vermittlung der**
3464 **Verbindung zwischen Client und Verarbeitungskontext**

3465 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die

3466 Verbindung zwischen Client, d.h. dem ePA-Frontend des Versicherten bzw. dem

3467 Fachmodul ePA oder Fachmodul ePA KTR-Consumer, und Verarbeitungskontext

3468 vermitteln und dabei

- 3469 • die Base64-dekodierte Authorization Assertion der `VAUClientHello`-Nachricht auf
3470 Gültigkeit gemäß Anforderung A_13690 sowie auf den gültigen Berechtigungstyp
3471 (`AuthorizationType = "DOCUMENT_AUTHORIZATION"`) prüfen und bei ungültiger
3472 Authorization Assertion den Verbindungsaufbau abbrechen und mit dem HTTP-
3473 Fehler 403 antworten,
- 3474 • den Record Identifier des Verarbeitungskontextes über den Wert des Attributs
3475 `Resource ID` aus der Authorization Assertion der `VAUClientHello`-Nachricht
3476 ermitteln,
- 3477 • für Clients vom Typ ePA-Frontend des Versicherten die Verbindung auf der
3478 Grundlage des vom Zugangsgateway gesetzten HTTP Header-
3479 Feldes `Session` registrieren,
- 3480 • für Clients vom Typ Fachmodul ePA die Verbindung auf Grundlage der TLS-Sitzung
3481 (`Session-ID`) oder auf Grundlage der `KeyID` des VAU-Kanals [`gemSpec_Krypt`]
3482 (mit der Ausnahme, dass im Rahmen des Handshakes `VAUClientHelloDataHash`
3483 zur Zuordnung des Verarbeitungskontext verwendet wird), registrieren,
- 3484 • während der Dauer der Sitzung alle eingehenden Requests auf der Grundlage der
3485 registrierten Verbindung an den Zielverarbeitungskontext weiterleiten sowie
- 3486 • nach dem Ende der Sitzung, aufgrund eines Timeouts bzw. aufgrund einer
3487 Beendigung durch den Nutzer, die Registrierung der Verbindung löschen.

3488 [`<=`]

3489 **A_20580 - Komponente ePA-Dokumentenverwaltung – TLS Session Resumption**
3490 **mittels Session-ID nutzen**

3491 Falls die Komponente ePA-Dokumentenverwaltung im Kontextmanagement die

3492 Vermittlung der Verbindung zwischen Client und Verarbeitungskontext für Clients vom

3493 Typ Fachmodul ePA die Verbindung auf Grundlage der TLS-Sitzung verwendet, MUSS

3494 die Komponente ePA-Dokumentenverwaltung TLS Session Resumption mittels Session-ID

3495 gemäß RFC 5246 nutzen. Dadurch wird sichergestellt dass, für den wiederholten Aufbau

3496 von TLS-Verbindungen die bereits ausgehandelten Session-Parameter genutzt werden.

3497 [`<=`]

3498 **A_14617-02 - Komponente ePA-Dokumentenverwaltung – Ablauf des**
3499 **Verbindungsaufbaus**

3500 Die Komponente ePA-Dokumentenverwaltung MUSS den Verbindungsaufbau von Clients,

3501 d.h. von einem ePA-Frontend des Versicherten oder einem Fachmodul so umsetzen, dass

3502 der folgende Ablauf in angegebener Reihenfolge ausgeführt wird, nachdem ein HTTP

3503 Request mit einer `VAUClientHello`-Nachricht von einem Client empfangen wurde:

3504 **Tabelle 33: Tab_Dokv_29 - Ablauf Operation Hello**

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden des HTTP Request mit VAUClientHello-Nachricht)
1	Kontextmanagement	Prüfen der Authorization Assertion der VAUClientHello-Nachricht auf Gültigkeit gemäß Anforderung A_13690 und Abbruch des Verbindungsaufbaus mit HTTP-Fehler 403 (Fehlermeldung "Access Denied") bei ungültiger Authorization Assertion.
2	Kontextmanagement	Extrahieren des Record Identifiers über den Wert des Attributs XSPA Resource ID aus der Authorization Assertion
3	Kontextmanagement	Prüfen, ob ein Verarbeitungskontext für den Record Identifier bereits initialisiert ist und Starten eines Verarbeitungskontextes, falls dies nicht der Fall ist
4	Kontextmanagement	Registrieren der Verbindung zwischen dem Client und dem Verarbeitungskontext für den Record Identifier für die Vermittlung des folgenden Nachrichtenaustauschs
5	Kontextmanagement	Weiterleiten der VAUClientHello-Nachricht an den Verarbeitungskontext für den Record Identifier
6	Verarbeitungskontext	Registrieren der Authorization Assertion der VAUClientHello-Nachricht und Erzeugen der VAUServerHello-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
7	Verarbeitungskontext	Senden der VAUServerHello-Nachricht
8	Kontextmanagement	Weiterleiten der VAUServerHello-Nachricht an den Client
9	Verarbeitungskontext	Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
	(Client)	(Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6])
	(Client)	(Erzeugen und Senden der VAUClientSigFin-Nachricht)
10	Kontextmanagement	Weiterleiten der VAUClientSigFin-Nachricht an den Verarbeitungskontext für den RecordIdentifier Record Identifier

11	Verarbeitungskontext	Prüfen auf Identität des authentifizierten Nutzers (Subject::Subject-id bzw. Subject::Organization-id der Authorization Assertion entspricht der KVNR bzw. Telematik-ID des übergebenen Zertifikats der Client-Authentisierung gemäß [gemSpec_Krypt#A_17070]) Im Fehlerfall MUSS der Verbindungsaufbau abgebrochen und mit einer VAUServerError-Nachricht beantwortet werden.
12	Verarbeitungskontext	Erzeugen der VAUServerErrorFin-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
13	Kontextmanagement	Weiterleiten der VAUServerErrorFin-Nachricht an den Client

3505 [**<=**]

3506 Der abgeleitete Sitzungsschlüssel wird anschließend vom Client und vom
3507 Verarbeitungskontext gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6] genutzt,
3508 um alle fachlichen Eingangs- und Ausgangsnachrichten zu ver- und entschlüsseln.

3509 **A_14545-03A_14545-02 - Komponente ePA-Dokumentenverwaltung -**
3510 **Operationen des Dokumenten-, Konto- und Schlüsselmanagements nur über**
3511 **sicheren Kanal**

3512 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die
3513 folgenden Operationen ausschließlich über den sicheren Kanal zwischen dem ePA-
3514 Frontend des Versicherten bzw. dem Fachmodul ePA und dem Verarbeitungskontext
3515 verfügbar machen:

- 3516 • I_Document_Management::CrossGatewayDocumentProvide
- 3517 • I_Document_Management::CrossGatewayQuery
- 3518 • I_Document_Management::RemoveMetadata
- 3519 • I_Document_Management::~~CrossGatewayRetrieve~~RemoveDocuments
- 3520 • I_Document_Management::CrossGatewayRetrieve
- 3521 • I_Document_Management::RestrictedUpdateDocumentSet
- 3522 • I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- 3523 • I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- 3524 • I_Document_Management_Insurant::RestrictedUpdateDocumentSet
- 3525 • I_Document_Management_Insurant::RegistryStoredQuery
- 3526 • I_Document_Management_Insurant::RemoveMetadata
- 3527 • I_Document_Management_Insurant::RetrieveDocumentSet
- 3528 • I_Account_Management_Insurant::GetAuditEvents
- 3529 • I_Account_Management_Insurant::GetSignedAuditEvents
- 3530 • I_Account_Management_Insurant::SuspendAccount
- 3531 • I_Account_Management_Insurant::ResumeAccount
- 3532 • I_Key_Management_Insurant::StartKeyChange

- 3533 • I_Key_Management_Insurant::GetAllDocumentKeys
- 3534 • I_Key_Management_Insurant::PutAllDocumentKeys
- 3535 • I_Key_Management_Insurant::FinishKeyChange
- 3536 • I_Document_Management_Connect::OpenContext
- 3537 • I_Document_Management_Connect::CloseContext

3538 Weiterhin MUSS der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung
 3539 bei sämtlichen genannten Operationen (bis auf Open Context und Close Context) prüfen,
 3540 ob das Subjekt der übergebenen Authentication Assertion mit dem der registrierten
 3541 Authorization Assertion übereinstimmt und im Fehlerfall eine `VAUServerError`-Nachricht
 3542 mit HTTP-Fehler 403 (Fehlermeldung "Access Denied") gemäß [gemSpec_Krypt#6.9]
 3543 returnieren. [≤]

3544

3545 **A_14645-01 - Komponente ePA-Dokumentenverwaltung – Nutzung des sicheren**
 3546 **Kanals zwischen ePA-Frontend des Versicherten bzw. Fachmodul ePA,**
 3547 **Fachmodul ePA KTR-Consumer und Verarbeitungskontext**

3548 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS den mit
 3549 dem ePA-Frontend des Versicherten bzw. mit dem Fachmodul ePA sowie dem Fachmodul
 3550 ePA KTR-Consumer gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
 3551 ausgehandelten Sitzungsschlüssel verwenden, um alle Eingangsnachrichten zu
 3552 entschlüsseln und alle Ausgangsnachrichten zu verschlüsseln. [≤]

3553

3554 **A_14457 - Komponente ePA-Dokumentenverwaltung – Implementierung der**
 3555 **Schnittstelle I_Document_Management_Connect**

3556 Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle
 3557 definierte Web-Service-Schnittstelle implementieren.

3558 **Tabelle 34: Tab_Dokv_30 - Schnittstelle I_Document_Management_Connect**

Schnittstelle I_Document_Management_Connect		
Version	1.0.1	
Namensraum	http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Open Context	Übergabe des Kontextschlüssels vom Client an den Verarbeitungskontext der Akte
	Close Context	Beendigung der Client-Verbindung und ggf. Beendigung des Verarbeitungskontextes der Akte
WSDL	DocumentManagementConnectService.wsdl	

XML Schema	DocumentManagementConnectService.xsd
-------------------	--------------------------------------

3559 [\leq]3560 **5.5.1.1 Operation I_Document_Management_Connect::OpenContext**3561 **A_14426 - Komponente ePA-Dokumentenverwaltung – Signatur für**3562 **I_Document_Management_Connect::OpenContext**

3563 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

3564 I_Document_Management_Connect::OpenContext gemäß der folgenden Signatur

3565 implementieren:

3566 **Tabelle 35: Tab_Dokv_31 - Operation OpenContext**

Operation	I_Document_Management_Connect::OpenContext		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Connect::OpenContext technisch um. Mit dieser Operation wird der Kontextschlüssel an den Verarbeitungskontext übergeben.		
Formatvorgabe n	SOAP Action: http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0/OpenContext		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
ContextKey	Der Kontextschlüssel	ContextKey	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
-	-	-	-
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
INVALID_AUTH_KEY	Der Kontextschlüssel ist ungültig.	Wenn der Vergleich mit einem bereits im Verarbeitungskontext	

		vorhandenen Kontextsschlüssel keine Übereinstimmung ergibt, oder das Entschlüsseln von Kontextdaten fehlschlägt
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.

3567 [**<=**]

3568 5.5.1.1.1 Umsetzung

3569 **A_14687-01 - Komponente ePA-Dokumentenverwaltung – Ablauf der Operation**

3570 **Open Context**

3571 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

3572 `I_Document_Management_Connect::OpenContext` so umsetzen, dass nach einem Aufruf

3573 der Operation durch einen Client, d.h. durch ein ePA-Frontend des Versicherten, ein

3574 Fachmodul ePA oder ein Fachmodul ePA KTR-Consumer, der folgende Ablauf in

3575 angegebener Reihenfolge (1 - 6) ausgeführt wird:

3576 **Tabelle 36: Tab_Dokv_32 - Ablauf der Operation Open Context**

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden der <code>OpenContextRequest</code> -Nachricht über den sicheren Kanal zwischen Client und Verarbeitungskontext)
1	Kontextmanagement	Weiterleiten der <code>OpenContextRequest</code> -Nachricht an den Verarbeitungskontext gemäß den vorgehaltenen Zuordnungsdaten (siehe Anforderung A_14633)
2	Verarbeitungskontext	Entnahme des im Eingangsparameter <code>ContextKey</code> enthaltenen Kontextschlüssels
3	Verarbeitungskontext	Falls bereits eine Sitzung mit einem Nutzer besteht, Prüfung des neu erhaltenen Kontextschlüssels auf Übereinstimmung mit dem aus der bestehenden Sitzung bereits registrierten Kontextschlüssel und Abbruch mit Fehlermeldung <code>INVALID_AUT_KEY</code> bei Nichtübereinstimmung
4	Verarbeitungskontext	Falls nicht bereits eine Sitzung mit einem Nutzer besteht, Laden der benötigten Kontextdaten aus dem Speichersystem, Entschlüsseln mit dem erhaltenen Kontextschlüssel und Abbruch mit Fehlermeldung <code>INVALID_AUT_KEY</code> , falls die Entschlüsselung der Kontextdaten fehlschlägt. Sind keine Kontextdaten mit dem Verarbeitungskontext assoziiert (d.h. erstmaliges Öffnen) MUSS der

		Kontextschlüssel in der Sitzung verwendet werden, um die neu erzeugten Kontextdaten zu verschlüsseln. In diesem beschriebenen Fall wird die Verarbeitung nicht mit der Fehlermeldung INVALID_AUT_KEY abgebrochen.
5	Verarbeitungskontext	Senden der OpenContextResponse-Nachricht
6	Kontextmanagement	Weiterleiten der OpenContextResponse-Nachricht an den Client

3577 [\leq]

3578 Der Verarbeitungskontext ist anschließend für die Verarbeitung von fachlichen
3579 Operationen bereit.

3580 **5.5.1.2 Operation I_Document_Management_Connect::CloseContext**3581 **A_14462 - Komponente ePA-Dokumentenverwaltung – Signatur für**3582 **I_Document_Management_Connect::CloseContext**

3583 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

3584 I_Document_Management_Connect::CloseContext gemäß der folgenden Signatur

3585 implementieren:

3586 **Tabelle 37: Tab_Dokv_33 - Operation Close Context**

Operation	I_Document_Management_Connect::CloseContext		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] in definierte Operation I_Document_Management_Connect::CloseContext technisch um. Mit dieser Operation wird die Verbindung zum Verarbeitungskontext beendet. Der Verarbeitungskontext kann geschlossen werden, falls nicht eine andere Verbindung noch besteht.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0/CloseContext		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
-	-	-	-
Ausgangsparameter			
Name	Beschreibung	Typ	opt.

-	-	-	-
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	

3587 [\leq]

3588 5.5.1.2.1 Umsetzung

3589 **A_14707-02 - Komponente ePA-Dokumentenverwaltung – Ablauf der Operation**
 3590 **Close Context**

3591 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 3592 `I_Document_Management_Connect::CloseContext` so umsetzen, dass nach einem Aufruf
 3593 der Operation durch einen Client, d. h. durch ein ePA-Frontend des Versicherten, ein
 3594 Fachmodul ePA oder ein Fachmodul ePA KTR-Consumer, der folgende Ablauf in
 3595 angegebener Reihenfolge (1 - 6) ausgeführt wird:

3596 **Tabelle 38: Tab_Dokv_34 - Ablauf Operation CloseContext**

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden der <code>CloseContextRequest</code> -Nachricht über den sicheren Kanal zwischen Client und Verarbeitungskontext)
1	Kontextmanagement	Weiterleiten der <code>CloseContextRequest</code> -Nachricht an den Verarbeitungskontext gemäß den vorgehaltenen Zuordnungsdaten (siehe Anforderung A_14633)
2	Verarbeitungskontext	Senden der <code>CloseContextResponse</code> -Nachricht
3	Kontextmanagement	Weiterleiten der <code>CloseContextResponse</code> -Nachricht an den Client
4	Verarbeitungskontext	Prüfen, ob mindestens eine weitere Sitzung existiert, ignorieren der <code>CloseContextRequest</code> -Nachricht, falls dies der Fall ist und Abbruch der Operation
5	Verarbeitungskontext	Falls keine weitere Sitzung existiert, persistieren geänderter Kontextdaten und Beenden des Verarbeitungskontextes
6	Kontextmanagement	Löschen der Verbindungszuordnung zwischen Client und Verarbeitungskontext

3597 [\leq]

3598 5.5.2 Hardware-Merkmale

3599 Die Vertrauenswürdige Ausführungsumgebung setzt die Nutzung eines HSM zur
3600 Speicherung und Anwendung der privaten Schlüssel von Dienstzertifikaten und
3601 Schlüsselpaaren gemäß Anforderung A_14564 voraus.

3602 5.6 Statische Akteninhalte

3603 Statische Inhalte werden vor der ersten echten Nutzung der Akte angelegt, d.h. bevor
3604 auf Akteninhalte zugegriffen wird. Sie sind (mit wenigen Ausnahmen) unveränderlich.

3605 **A_20191 - Komponente ePA-Dokumentenverwaltung – Anlegen von statischen Ordnern**

3606 Die Komponente ePA-Dokumentenverwaltung MUSS nach dem ersten erfolgreichen
3607 Öffnen der Akte des Versicherten (`Operation`
3608 `I_Document_Managemet_Connect::OpenContext()`) die folgenden Ordner für den
3609 Versicherten anlegen:
3610
3611

- 3612 • Kategorienordner, jeweils einen pro Kategorie 1a* gemäß [gemSpec_DM_ePA#A_20190-](#)
3613 [01](#) [gemSpec_DM_ePA#A_20190](#) (Belegung `Folder.codeList`) unter Berücksichtigung
3614 allgemeiner Vorgaben für Folder-Metadaten in [gemSpec_DM_ePA#A_14760-01](#) (Belegung
3615 der restlichen Metadatenfelder).

3616 Alle statischen Ordner sind nach dem Anlegen initial leer. [`<=`]

3617 **A_20214 - Komponente ePA-Dokumentenverwaltung – Anlegen von Permission Policies**

3618 Die Komponente ePA-Dokumentenverwaltung MUSS nach dem ersten erfolgreichen
3619 Öffnen der Akte des Versicherten (`Operation`
3620 `I_Document_Managemet_Connect::OpenContext()`) alle in Abschnitt 9.5 aufgeführten
3621 Permission Policies für den Versicherten anlegen. [`<=`]
3622

3623 **A_20215 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe von Permission Policies**

3624 Die Komponente ePA-Dokumentenverwaltung DARF statische Policy-Dokumente
3625 (Advanced Patient Privacy Consent) gemäß Abschnitt 9.5 NICHT über Suchoperationen
3626 dem ePA-Frontend des Versicherten zur Verfügung stellen. Ferner MUSS die Komponente
3627 ePA-Dokumentenverwaltung ein Herunterladen verhindern. [`<=`]
3628

3629 **A_20216 - Komponente ePA-Dokumentenverwaltung – Unveränderlichkeit von statischen Akteninhalten**

3630 Die Komponente ePA-Dokumentenverwaltung DARF die Metadaten eines statischen
3631 Aktenobjekts nach Abschnitt 5.6 nach dem Anlegen NICHT ändern oder das statische
3632 Aktenobjekt selbst löschen. Dabei gelten folgende Ausnahmen:
3633

- 3634 • `Folder.lastUpdateTime`

3635 [`<=`]

3636 `Folder.lastUpdateTime` wird automatisch von der Dokumentenverwaltung aktualisiert,
3637 sobald Dokumente in den Ordner eingestellt oder daraus gelöscht werden, siehe auch
3638 [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6].

3639

6 Informationsmodelle

3640

Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten wird nicht benötigt.

3641

ENTWURF

3642

7 Anhang A – Verzeichnisse

3643

7.1 Abkürzungen

Kürzel	Erläuterung
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BPPC	Basic Patient Privacy Consents
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
MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
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
W3C	World Wide Web Consortium
WS-I	Web-Services Interoperability Consortium
XCA	Cross-Community Access Profile
XDR	Cross-Enterprise Document Reliable Interchange Profile
XDS	Cross-Enterprise Document Sharing ProfileGetAllDocumentKeys
XCDR	Cross-Community Document Reliable Interchange Profile
XACML	eXtensible Access Control Markup Language
XDW	Cross-Enterprise Document Workflow Profile
XOP	XML-binary Optimized Packaging
XSPA	Cross-Enterprise Security and Privacy Authorization Profile
XUA	Cross-Enterprise User Assertion Profile

7.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.

7.3 Abbildungsverzeichnis

Abbildung 1: Komponentenzerlegung ePA-Dokumentenverwaltung	17
Abbildung 2: Zustandsübergänge Schlüsselwechsel	99
Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen	117
Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen	118
Abbildung 1: Komponentenzerlegung ePA-Dokumentenverwaltung	17
Abbildung 2: Zustandsübergänge Schlüsselwechsel	99
Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen	117
Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen	118

7.4 Tabellenverzeichnis

Tabelle 1: Tab_Dokv_10 – Kennzeichnung von Optionalitäten	26
Tabelle 2: Tab_Dokv_11 – Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung	26
Tabelle 3: Tab_Dokv_12 – Fehlercodes zu Fehlern gemäß Operationsdefinition	33
Tabelle 4: Tab_Dokv_35 – Eingangsparameter für TUC_PKI_018	40
Tabelle 5: Tab_Dokv_13 – Parameter des § 291a-Protokolls	43
Tabelle 6: Tab_Dokv_14 – Schnittstelle I_Document_Management	54
Tabelle 7: Tab_Dokv_16 – Operation Cross-Gateway Query	58
Tabelle 8: Tab_Dokv_17 – Operation RemoveMetadata	62
Tabelle 9: Tab_Dokv_18 – Operation Cross-Gateway Retrieve	64
Tabelle 10: Tab_Dokv_20 – Schnittstelle I_Document_Management_Insurant	68
Tabelle 11: Tab_Dokv_21 – Operation Provide And Register Document Set b	69
Tabelle 12: Tab_Dokv_22 – Operation Registry Stored Query	71
Tabelle 13: Tab_Dokv_23 – Operation RemoveMetadata	76

3672	Tabelle 14: Tab_Dokv_24—Operation Retrieve Document Set	77
3673	Tabelle 15: Tab_Dokv_19—Operation RestrictedUpdateDocumentSet	80
3674	Tabelle 16: Tab_Dokv_36—Schnittstelle I_Document_Management_Insurance	82
3675	Tabelle 17: Tab_Dokv_37—Operation Provide And Register Document Set b.....	83
3676	Tabelle 18: Tab_Dokv_25—Schnittstelle I_Account_Management_Insurant	86
3677	Tabelle 19: Tab_Dokv_26—Operation Suspend Account.....	87
3678	Tabelle 20: Tab_Dokv_27—Operation Resume Account.....	90
3679	Tabelle 21: Tab_Dokv_28—Operation Get Audit Events	93
3680	Tabelle 22: Tab_Dokv_38—Operation I_Key_Management_Insurant::StartKeyChange()	
3681	102
3682	Tabelle 23: Tab_Dokv_39—	
3683	Operation I_Key_Management_Insurant::GetAllDocumentKeys()	105
3684	Tabelle 24: Tab_Dokv_40—	
3685	Operation I_Key_Management_Insurant::PutAllDocumentKeys().....	107
3686	Tabelle 25: Tab_Dokv_41—	
3687	Operation I_Account_Management_Insurant::FinishKeyChange().....	109
3688	Tabelle 26: Tab_Dokv_42—Zusätzliche Parameter des § 291a Protokolls für die	
3689	Umschlüsselung	112
3690	Tabelle 27: Tab_Dokv_43—Zusätzliche Parameter des § 291a Protokolls für ein Rollback	
3691	im Rahmen der Umschlüsselung.....	112
3692	Tabelle 28: Tab_Dokv_030—Zugriffsunterbindungsregeln	119
3693	Tabelle 29: Tab_Dokv_29—Ablauf Operation Hello	131
3694	Tabelle 30: Tab_Dokv_30—Schnittstelle I_Document_Management_Connect	133
3695	Tabelle 31: Tab_Dokv_31—Operation OpenContext.....	134
3696	Tabelle 32: Tab_Dokv_32—Ablauf der Operation Open Context	135
3697	Tabelle 33: Tab_Dokv_33—Operation Close Context.....	136
3698	Tabelle 34: Tab_Dokv_34—Ablauf Operation CloseContext.....	137
3699	Tabelle 35: Tab_Dokv_99—Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	150
3700	Tabelle 36: Tab_Dokv_100—XACML 2.0 Policy für einen Versicherten (Base Policy)....	150
3701	Tabelle 37: Tab_Dokv_101—XACML 2.0 Policy mit erlaubten Operationen für einen	
3702	Versicherten (Permission Policy).....	153
3703	Tabelle 38: Tab_Dokv_200—XACML 2.0 Policy für einen Vertreter (Base Policy).....	184
3704	Tabelle 39: Tab_Dokv_201—XACML 2.0 Policy mit erlaubten Operationen für einen	
3705	Vertreter (Permission Policy).....	188
3706	Tabelle 40 Tabelle : Tab_Dokv_300-01—XACML 2.0 Policy für eine	
3707	Leistungserbringerinstitution (Base Policy).....	216
3708	Tabelle 41: Tab_Dokv_301—XACML 2.0 Policy mit erlaubten Operationen für eine	
3709	Leistungserbringerinstitution zum Zugriff auf Leistungserbringer Dokumente	
3710	(Permission Policy)	221

3711	Tabelle 42: Tab_Dokv_302 – XACML 2.0 Policy mit erlaubten Operationen für eine	
3712	Leistungserbringerinstitution zum Zugriff auf Versicherten und Kostenträger-	
3713	Dokumente (Permission Policy)	247
3714	Tabelle 43: Tab_Dokv_400 – XACML 2.0 Policy für einen Kostenträger (Base Policy) ...	271
3715	Tabelle 44: Tab_Dokv_401 – XACML 2.0 Policy mit erlaubten Operationen für einen	
3716	Kostenträger (Permission Policy)	274
3717	Tabelle 45: Tab_Dokv_99 – Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	278
3718	Tabelle 46: Tab_Dokv_500 – XACML 2.0 Policy für einen Versicherten	278
3719	Tabelle 47: Tab_Dokv_501 – XACML 2.0 Policy für einen Vertreter	281
3720	Tabelle 48: Tab_Dokv_502 – XACML 2.0 Policy für eine Leistungserbringerinstitution ..	284
3721	Tabelle 49: Tab_Dokv_503 – XACML 2.0 Policy für einen Kostenträger	306
3722	Tabelle 1: Tab Dokv 10 - Kennzeichnung von Optionalitäten	26
3723	Tabelle 2: Tab Dokv 11 - Übersicht über gruppierte IHE ITI-Akteure und Optionen an	
3724	den Außenschnittstellen der ePA-Dokumentenverwaltung	26
3725	Tabelle 3: Tab Dokv 12 - Fehlercodes zu Fehlern gemäß Operationsdefinition	33
3726	Tabelle 4: Tab Dokv 35 - Eingangsparameter für TUC PKI 018	40
3727	Tabelle 5: Tab Dokv 13 - Parameter des § 291a-Protokolls	43
3728	Tabelle 6: Tab Dokv 14 - Schnittstelle I Document Management	54
3729	Tabelle 7: Tab Dokv 16 - Operation Cross-Gateway Query	58
3730	Tabelle 8: Tab Dokv 17 - Operation Remove Documents	61
3731	Tabelle 9: Tab Dokv 17 - Operation RemoveMetadata	62
3732	Tabelle 10: Tab Dokv 18 - Operation Cross-Gateway Retrieve	64
3733	Tabelle 11: Tab Dokv 45 - Operation Restricted Update Document Set	66
3734	Tabelle 12: Tab Dokv 20 - Schnittstelle I Document Management Insurant	68
3735	Tabelle 13: Tab Dokv 21 - Operation Provide And Register Document Set-b	69
3736	Tabelle 14: Tab Dokv 22 - Operation Registry Stored Query	71
3737	Tabelle 15: Tab Dokv 23 - Operation RemoveMetadata	76
3738	Tabelle 16: Tab Dokv 24 - Operation Retrieve Document Set	77
3739	Tabelle 17: Tab Dokv 19 - Operation RestrictedUpdateDocumentSet	80
3740	Tabelle 18: Tab Dokv 36 - Schnittstelle I Document Management Insurance	82
3741	Tabelle 19: Tab Dokv 37 - Operation Provide And Register Document Set-b	83
3742	Tabelle 20: Tab Dokv 25 - Schnittstelle I Account Management Insurant	86
3743	Tabelle 21: Tab Dokv 26 - Operation Suspend Account	87
3744	Tabelle 22: Tab Dokv 27 - Operation Resume Account	90
3745	Tabelle 23: Tab Dokv 28 - Operation Get Audit Events	93
3746	Tabelle 24: Tab Dokv 44 - Operation Get Signed Audit Events	95
3747	Tabelle 25: Tab Dokv 38 - Operation I Key Management Insurant::StartKeyChange()	
3748	102

3749	<u>Tabelle 26: Tab Dokv 39 -</u>	
3750	<u>Operation I Key Management Insurant::GetAllDocumentKeys()</u>	105
3751	<u>Tabelle 27: Tab Dokv 40 -</u>	
3752	<u>Operation I Key Management Insurant::PutAllDocumentKeys().....</u>	107
3753	<u>Tabelle 28: Tab Dokv 41 -</u>	
3754	<u>Operation I Account Management Insurant::FinishKeyChange().....</u>	109
3755	<u>Tabelle 29: Tab Dokv 42 - Zusätzliche Parameter des § 291a-Protokolls für die</u>	
3756	<u>Umschlüsselung</u>	112
3757	<u>Tabelle 30: Tab Dokv 43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback</u>	
3758	<u>im Rahmen der Umschlüsselung</u>	112
3759	<u>Tabelle 31: Tab Dokv 43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback</u>	
3760	<u>im Rahmen der Umschlüsselung</u>	112
3761	<u>Tabelle 32: Tab Dokv 030 - Zugriffsunterbindungsregeln</u>	119
3762	<u>Tabelle 33: Tab Dokv 29 - Ablauf Operation Hello</u>	131
3763	<u>Tabelle 34: Tab Dokv 30 - Schnittstelle I Document Management Connect</u>	133
3764	<u>Tabelle 35: Tab Dokv 31 - Operation OpenContext.....</u>	134
3765	<u>Tabelle 36: Tab Dokv 32 - Ablauf der Operation Open Context</u>	135
3766	<u>Tabelle 37: Tab Dokv 33 - Operation Close Context.....</u>	136
3767	<u>Tabelle 38: Tab Dokv 34 - Ablauf Operation CloseContext.....</u>	137
3768	<u>Tabelle 39: Tab Dokv 99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..</u>	150
3769	<u>Tabelle 40: Tab Dokv 100 - XACML 2.0 Policy für einen Versicherten (Base Policy)....</u>	150
3770	<u>Tabelle 41: Tab Dokv 101 - XACML 2.0 Policy mit erlaubten Operationen für einen</u>	
3771	<u>Versicherten (Permission Policy).....</u>	153
3772	<u>Tabelle 42: Tab Dokv 200 - XACML 2.0 Policy für einen Vertreter (Base Policy).....</u>	184
3773	<u>Tabelle 43: Tab Dokv 201 - XACML 2.0 Policy mit erlaubten Operationen für einen</u>	
3774	<u>Vertreter (Permission Policy).....</u>	188
3775	<u>Tabelle 44 Tabelle : Tab Dokv 300-01 - XACML 2.0 Policy für eine</u>	
3776	<u>Leistungserbringerinstitution (Base Policy).....</u>	216
3777	<u>Tabelle 45: Tab Dokv 301 - XACML 2.0 Policy mit erlaubten Operationen für eine</u>	
3778	<u>Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente</u>	
3779	<u>(Permission Policy)</u>	221
3780	<u>Tabelle 46: Tab Dokv 302 - XACML 2.0 Policy mit erlaubten Operationen für eine</u>	
3781	<u>Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-</u>	
3782	<u>Dokumente (Permission Policy)</u>	247
3783	<u>Tabelle 47: Tab Dokv 400 - XACML 2.0 Policy für einen Kostenträger (Base Policy) ...</u>	271
3784	<u>Tabelle 48: Tab Dokv 401 - XACML 2.0 Policy mit erlaubten Operationen für einen</u>	
3785	<u>Kostenträger (Permission Policy)</u>	274
3786	<u>Tabelle 49: Tab Dokv 99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..</u>	278
3787	<u>Tabelle 50: Tab Dokv 500 - XACML 2.0 Policy für einen Versicherten</u>	278
3788	<u>Tabelle 51: Tab Dokv 501 - XACML 2.0 Policy für einen Vertreter.....</u>	281
3789	<u>Tabelle 52: Tab Dokv 502 - XACML 2.0 Policy für eine Leistungserbringerinstitution ..</u>	284

3790	Tabelle 53: Tab Dokv 503 - XACML 2.0 Policy für einen Kostenträger	306
3791	Tabelle 54: Tab Dokv 17 - Operation Remove Metadata	328
3792		

3793 7.5 Referenzierte Dokumente

3794 7.5.1 Dokumente der gematik

3795 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 3796 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der
 3797 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
 3798 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und
 3799 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
 3800 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer ist in der
 3801 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die
 3802 vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemSpec_Aktensystem]	gematik: Spezifikation ePA-Aktensystem
[gemSpec_Authentisierung_Vers]	gematik: Spezifikation Authentisierung des Versicherten ePA
[gemSpec_Autorisierung]	gematik: Spezifikation Autorisierung ePA
[gemSpec_DM_ePA]	gematik: Datenmodell ePA
[gemSpec_FdV_ePA]	gematik: Spezifikation ePA-Frontend des Versicherten
[gemSpec_FM_ePA]	gematik: Spezifikation Fachmodul ePA
[gemSpec_FM_ePA_KTR_Consumer]	gematik: Spezifikation Fachmodul ePA im KTR-Consumer
[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_TBAuth]	gematik: Spezifikation Tokenbasierte Authentisierung

[gemSysL_ePA]

gematik: Systemspezifisches Konzept ePA

3803

7.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-ACWP]	IHE International (2009): IHE IT Infrastructure White Paper Access Control, Revision 1.3, http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf
[IHE-ITI-APPC]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Advanced Patient Privacy Consents (APPC), Revision 1.2 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf
[IHE-ITI-RMD]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.2 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-RMU]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.1 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf
[IHE-ITI-TF1]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Integration Profiles, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
[IHE-ITI-TF2a]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2a (ITI TF-2a) – Transactions Part A, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf
[IHE-ITI-TF2b]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf

[IHE-ITI-TF2x]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2x) – Volume 2 Appendices, Revision 15.1, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf
[IHE-ITI-TF3]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Transaction Specifications and Content Specifications, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf
[IHE-ITI-XCDR]	IHE International (2017): IHE IT Infrastructure (ITI) Technical Framework Supplement, Cross-Community Document Reliable Interchange (XCDR), Revision 1.4 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[OWASP-IP]	Open Web Application Security Project (OWASP) (2017): Input Validation Cheat Sheet, https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet
[OWASP-SAML]	Open Web Application Security Project (OWASP) (2017): SAML Security Cheat Sheet, https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet
[OWASP-WSS]	Open Web Application Security Project (OWASP) (2017): Web Service Security Cheat Sheet, https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, http://tools.ietf.org/html/rfc2119
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231, https://tools.ietf.org/html/rfc7231
[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
[WSS-SAML]	OASIS (2006): Web Services Security: SAML Token Profile 1.1, https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTOKENProfile.pdf
[XACML]	OASIS (2005): eXtensible Access Control Markup Language (XACML) Version 2.0, https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/

8 Anhang B – XACML 2.0-Profile für Policy Documents (für Upgrade von ePA 3.1.3)

Die folgende Notation wird zur Kennzeichnung von Optionalitäten (Opt.) in den XACML 2.0 Policies verwendet:

Tabelle 39: Tab_Dokv_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies

Code	Bedeutung
R	Required - Mit "R" gekennzeichnete Element-, Attribut- oder Textknoten MÜSSEN verwendet werden.
O	Optional - Mit "O" gekennzeichnete Element-, Attribut- oder Textknoten KÖNNEN verwendet werden.
X	Mit "X" gekennzeichnete Element-, Attribut- oder Textknoten DÜRFEN NICHT verwendet werden.

Beispiele zu den folgenden XACML 2.0-Profilen der Base Policies können dem beiliegenden Dokumentenpaket entnommen werden.

8.1 Policy Document für einen Versicherten

8.1.1 Base Policy

Tabelle 40: Tab_Dokv_100 - XACML 2.0 Policy für einen Versicherten (Base Policy)

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:insurant" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.

		Target	R	Das Element MUSS leer bleiben.
←! Versicherter (repräsentiert durch seine KVNR) →				
		Subjects	R	
		Subject	R	
		SubjectMatch	R	
		@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
		AttributeValue	R	
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		InstanceIdentifier	R	
		@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
		@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
		@extension	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
		SubjectAttributeDesignator	R	
		@AttributeId	R	Der Wert "urn:gematik:subject:subject-id" MUSS gesetzt werden.

			@DataType	R	Der Wert "urn:h17-org:v3#II" MUSS gesetzt werden.
			@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
<!-- KVN R als Aktenidentifikator -->					
		Resources		R	
		Resource		R	
		ResourceMatch		R	
		@MatchId		R	Der Wert "urn:h17-org:v3:function:II-equal" MUSS gesetzt werden.
		AttributeValue		R	
		@DataType		R	Der Wert "urn:h17-org:v3#II" MUSS gesetzt werden.
		InstanceIdentifier		R	
		@xmlns		R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
		@root		R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
		@extension		R	Als Wert MUSS den unveränderbare Teil der KVN R (10 Stellen) gesetzt werden.
		ResourceAttributeDesignator		R	

		@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		PolicySetIdReference	R	
		text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurant" MUSS gesetzt werden.

3815 8.1.2 Permission Policy

3816 **Tabelle 41: Tab_Dokv_101 - XACML 2.0 Policy mit erlaubten Operationen für einen**
 3817 **Versicherten (Permission Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurant" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
Target	R	Das Element MUSS leer bleiben.

Policy					R	
	@PolicyId				R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@RuleCombiningAlgId				R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target				R	
	Resources				R	
	Resource				R	
	ResourceMatch				R	
		@MatchId			R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
		AttributeValue			R	
			@DataType		R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
			CodedValue		R	

					@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
					@code	R	Der Wert "PAT" MUSS gesetzt werden.
					@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
					@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
					@displayName	O	Der Wert "Dokument eines Versicherten" MUSS gesetzt werden.
				ResourceAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:appc:2016:confidentiality-code" MUSS gesetzt werden.
					@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
					@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Actions		R	

<!-- 'CrossGatewayDocumentProvide' -->									
					Action		R		
					ActionMatch		R		
					@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.	
					AttributeValue		R		
					@DataType		R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.	
					text()		R	Der Wert "urn:ihe:iti:2015: CrossGatewayDocumentPro vide" MUSS gesetzt werden.	
					ActionAttributeDesignator		R		
					@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.	
					@DataType		R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.	
<!-- 'ProvideAndRegisterDocumentSet-b' -->									

				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007: ProvideAndRegisterDocum entSet-b" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				Rule	R	
				@RuleId	R	Es MUSS ein URN- kodierter, global eindeutiger Identifikator

					gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
			@Effect	R	Der Wert "Permit" MUSS gesetzt werden.
			Policy	R	
			@PolicyId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
			@RuleCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
			Target	R	
			Actions	R	
<!-- Registry Stored Query 'FindDocuments' -->					
			Action	R	
			ActionMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.

				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

					text()	R	Der Wert "urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindSubmissionSets' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbc1a9" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis tryStoredQuery:

							queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAll' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocuments' -->							

				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:Regis tryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:

							function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:5c4f972b- d56b-40ac-a5fc- c8ca9b40b9d4" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis- tryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAssociations' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xac- ml:1.0: function:anyURI-equal" MUSS gesetzt werden.

					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

					text()	R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocumentsAndAssociations' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:bab9529a- 4a10-40b3-a01f- f68a615d247a" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis tryStoredQuery:

							queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSets' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:51224314-5390-4169-9b91-b1980040715a" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSetAndContents' -->							

				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:Regis tryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:

							function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:e8e3cb2c- e39c-46b9-99e4- c12f57260b83" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis- tryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetRelatedDocuments' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xac- ml:1.0: function:anyURI-equal" MUSS gesetzt werden.

				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

					text()	R	Der Wert "urn:uuid:d90e5407-b356-4d91-a89f-873917b4b0e6" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByReferenceId' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:12941a89- e02e-4be5-967c- ce4bfc8fe492" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis- tryStoredQuery:"

								queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.	
<!-- Registry Stored Query 'FindDocumentsByTitle' -->								
		Act ion				R		
		Action Match				R		
			@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.	
			AttributeValue			R		
				@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.	
				text()		R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.	
			ActionAttributeDesignator			R		
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:	

								action:action-id" MUSS gesetzt werden.
					@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			Action Match				R	
				@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue				R	
				@Data Type			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()			R	Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
			ActionAttributeDesignator				R	
				@AttributeId			R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.

					@Data Type	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RemoveDocuments -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xac ml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2017:Remov eDocuments" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xac ml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS

						gesetzt werden.
<!-- RetrieveDocumentSet -->						
				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:Retri eveDocumentSet" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
<!-- GetAuditEvents -->						

				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "http://ws.gematik.de/f d/phr/ I_Account_Management_In surant/v1.0/ GetAuditEvents" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action- id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
<!-- ResumeAccount -->						
				Action	R	

					ActionMatch	R	
					@MatchId	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/ResumeAccount" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					Rule	R	
					@RuleId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B]

						vergeben werden.
			@Effect	R		Der Wert "Permit" MUSS gesetzt werden.
<!-- SuspendAccount -->						
			Policy	R		
			@PolicyId	R		Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
			@RuleCombiningAlgId	R		Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
			Target	R		
			Resources	R		
			Resource	R		
			ResourceMatch	R		
			@MatchId	R		Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
			AttributeValue	R		

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
					text()	R	Der Wert "DISMISSED" MUSS gesetzt werden.
				ResourceAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:gematik:fa:phr:1.0:status:status-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
				Actions		R	
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

					text()	R	Der Wert "http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/SuspendAccount" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				Rule		R	
				@RuleId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
				@Effect		R	Der Wert "Permit" MUSS gesetzt werden.

3818 8.2 Policy Document für einen Vertreter

3819 8.2.1 Base Policy

3820 Tabelle 42: Tab_Dokv_200 - XACML 2.0 Policy für einen Vertreter (Base Policy)

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt .	Nutzungsvorgabe
---	-------	-----------------

PolicySet		R	
	@PolicySetId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target	R	Das Element MUSS leer bleiben.
<!-- Vertreter (repräsentiert durch seine KVNR) -->			
	Subjects	R	
	Subject	R	
	SubjectMatch	R	
	@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
	AttributeValue	R	
	@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
	InstanceIdentifier	R	
	@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.

				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS der unveränderbare Teil der KVN (10 Stellen) gesetzt werden.
				SubjectAttributeDesignator	R	
				@AttributeId	R	Der Wert " urn:gematik:subject:subject-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Subject	R	
				SubjectMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:string-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
				text()	R	Der Common Name des X.509 Subject Name der eGK MUSS gesetzt werden, um die Lesbarkeit für den Versicherten im ePA- Frontend des Versicherten zu erhöhen, d.h. wem er ein Zugriffsrecht eingeräumt hat.

				SubjectAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:subject:subject" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVNR als Aktenidentifikator -->						
				Resources	R	
				Resource	R	
				ResourceMatch	R	
				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.

				ResourceAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				PolicySetIdReference	R	
				text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-representative" MUSS gesetzt werden.

3821 8.2.2 Permission Policy

3822 **Tabelle 43: Tab_Dokv_201 - XACML 2.0 Policy mit erlaubten Operationen für einen**
 3823 **Vertreter (Permission Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-representative" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.

				Target	R	Das Element MUSS leer bleiben.
				Policy	R	
				@PolicyId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
				@RuleCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
				Target	R	
				Resources	R	
				Resource	R	
				ResourceMatch	R	
				@MatchId	R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.

						CodedValue	R	
						@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
						@code	R	Der Wert "PAT" MUSS gesetzt werden.
						@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	O	Der Wert "Dokument eines Versicherten" MUSS gesetzt werden.
					ResourceAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
					Actions		R	

<!-- 'CrossGatewayDocumentProvide' -->									
								Action	R
								ActionMatch	R
								@MatchId	R Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
								AttributeValue	R
								@DataType	R Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
								text()	R Der Wert "urn:ihe:iti:2015: CrossGatewayDocumentPr ovide" MUSS gesetzt werden.
								ActionAttributeDesignator	R
								@AttributeId	R Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
								@DataType	R Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- 'ProvideAndRegisterDocumentSet-b' -->									

				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007: ProvideAndRegisterDocumentSet-b" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				Rule	R	
				@RuleId	R	Es MUSS ein URN- kodierter, global eindeutiger Identifikator

						gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
			@Effect		R	Der Wert "Permit" MUSS gesetzt werden.
			Policy		R	
			@PolicyId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
			@RuleCombiningAlgId		R	Der Wert "urn:oasis:names:tc:xa-cml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
			Target		R	
			Actions		R	
<!-- Registry Stored Query 'FindDocuments' -->						
			Action		R	
			ActionMatch		R	
			@MatchId		R	Der Wert "urn:oasis:names:tc:xa-cml:1.0:function:anyURI-equal" MUSS gesetzt werden.

				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

					text()	R	Der Wert "urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindSubmissionSets' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbc1a9" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regi stryStoredQuery:

							queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAll' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.

				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			ActionMatch		R	
			@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue		R	
			@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			text()		R	Der Wert "urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3" MUSS gesetzt werden.
			ActionAttributeDesignator		R	
			@AttributeId		R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
			@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocuments' -->						

				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:Regi stryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0:

							function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:uuid:5c4f972b-d56b-40ac-a5fc-c8ca9b40b9d4" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAssociations' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.

				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

					text()	R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocumentsAndAssociations' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:bab9529a-4a10-40b3-a01f-f68a615d247a" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:"

							queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSets' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xcml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xcml:1.0: action:action-id" MUSS gesetzt werden.

				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			ActionMatch		R	
			@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue		R	
			@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			text()		R	Der Wert "urn:uuid:51224314-5390-4169-9b91-b1980040715a" MUSS gesetzt werden.
			ActionAttributeDesignator		R	
			@AttributeId		R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
			@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSetAndContents' -->						

				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:Regi stryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0:

							function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:uuid:e8e3cb2c-e39c-46b9-99e4-c12f57260b83" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetRelatedDocuments' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.

				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

					text()	R	Der Wert "urn:uuid:d90e5407-b356-4d91-a89f-873917b4b0e6" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByReferenceId' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:12941a89- e02e-4be5-967c- ce4bfc8fe492" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regi stryStoredQuery:

								queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.	
<!-- Registry Stored Query 'FindDocumentsByTitle' -->								
		Act ion				R		
		Action Match				R		
			@MatchId			R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.	
			AttributeValu e			R		
				@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.	
				text()		R	Der Wert "urn:ihe:iti:2007:Regi stryStoredQuery" MUSS gesetzt werden.	
			ActionAttribut eDesignator			R		
				@Attri buteId		R	Der Wert "urn:oasis:names:tc:xa cml:1.0:	

								action:action-id" MUSS gesetzt werden.
					@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			Action Match				R	
				@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue			R	
				@Data Type			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()			R	Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
			ActionAttributeDesignator				R	
				@AttributeId			R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RemoveDocuments -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2017:RemoveDocuments" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI"

						MUSS gesetzt werden.
<!-- RetrieveDocumentSet -->						
			Action		R	
			ActionMatch		R	
			@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue		R	
			@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			text()		R	Der Wert "urn:ihe:iti:2007:RetrieveDocumentSet" MUSS gesetzt werden.
			ActionAttributeDesignator		R	
			@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
			@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- GetAuditEvents -->						

				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "http://ws.gematik.de/ fd/phr/ I_Account_Management_I nsurant/v1.0/ GetAuditEvents" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
				@RuleId	R	Es MUSS ein URN- kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus

				[IHE-ITI-TF2x#Appendix B] vergeben werden.
		@Effect	R	Der Wert "Permit" MUSS gesetzt werden.

3824 8.3 Policy Document für eine Leistungserbringerinstitution

3825 8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente

3826

3827 **Tabelle 44 Tabelle : Tab_Dokv_300-01 - XACML 2.0 Policy für eine**
 3828 **Leistungserbringerinstitution (Base Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt .	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
Target	R	Das Element MUSS leer bleiben.
<!-- Leistungserbringerinstitution (repräsentiert durch ihre Telematik-ID) -->		
Subjects	R	
Subject	R	
SubjectMatch	R	

				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS die Telematik-ID gesetzt werden.
				SubjectAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:gematik:subject:organization-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Subject	R	
				SubjectMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
				AttributeValue	R	

				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
				text()	R	Als Wert MUSS der Name der Leistungserbringerinstitution gesetzt werden.
				SubjectAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xspa:1.0:subject:organization" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVN als Aktenidentifikator -->						
				Resources	R	
				Resource	R	
				ResourceMatch	R	
				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.

					@extension	R	Als Wert MUSS der unveränderbare Teil der KVN (10 Stellen) gesetzt werden.
					ResourceAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
<!-- Gültigkeitszeitraum des Policy Documents -->							
					Environments	R	
					Environment	R	
					EnvironmentMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:date-less-than-or-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
					text()	R	Der Wert muss dem Tag der Ausstellung (Format YYYY-MM-DD nach ISO 8601:2004) des Policy Documents entsprechen.
					EnvironmentAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.

				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				EnvironmentMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:date-greater-than" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				text()	R	Der Wert muss dem Enddatum (Format YYYY-MM-DD nach ISO 8601:2004) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen: "heute" + frei eintragbare Anzahl Tage in der Spanne von 1 bis 540
				EnvironmentAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				PolicySetIdReference	R	

text()	R	<p>Die Policy Set ID Reference steuert, ob Leistungserbringerinstitutionen Zugriff auf durch Leistungserbringer (permissions-access-group-hcp), Versicherte und Vertreter (permissions-access-group-hcp-insurant-documents) sowie Kostenträger (permissions-access-group-hcp-insurance-documents) eingestellte Dokumente erhalten sollen oder nicht. Das Hinzufügen einer betreffenden Policy Set ID Reference gewährt der Leistungserbringerinstitution Zugriffsrechte.</p> <p>Es muss mindestens ein und maximal drei der folgenden Werte gesetzt werden:</p> <ul style="list-style-type: none"> • "urn:gematik:policy-set-id:permissions-access-group-hcp" • "urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents" • "urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents"
--------	---	---

8.3.2 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente

Tabelle 45: Tab_Dokv_301 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente (Permission Policy)

Element-, Attribut- oder Textknoten gemäß [XACML]	Op t.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-

[illegible]

						CodedValue	R	
						@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
						@code	R	Der Wert "LEI" MUSS gesetzt werden.
						@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	O	Der Wert "Dokument einer Leistungserbringerinstitution" MUSS gesetzt werden.
						ResourceAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:ihe:iti:appc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
						Actions	R	
<!-- 'CrossGatewayDocumentProvide' -->								
						Action	R	

					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2015:CrossGatewayDocumentProvide" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					Rule	R	
					@RuleId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
					@Effect	R	Der Wert "Permit" MUSS gesetzt werden.

Policy					R	
	@PolicyId				R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@RuleCombiningAlgId				R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target				R	
	Resources				R	
	Resource				R	
	ResourceMatch				R	
		@MatchId			R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
		AttributeValue			R	
			@DataType		R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
			CodedValue		R	
				@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.

						@code	R	Der Wert "LEI" MUSS gesetzt werden.
						@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	R	Der Wert "Dokument einer Leistungserbringerinstitution" MUSS gesetzt werden.
				ResourceAttributeDesignator			R	
						@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
			Resource				R	
			ResourceMatch				R	
						@MatchId	R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
				AttributeValue			R	

					@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
					CodedValue	R	
					@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
					@code	R	Der Wert "LEÄ" MUSS gesetzt werden.
					@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
					@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
					@displayName	R	Der Wert "Leistungserbringeräquivalentes Dokument eines Versicherten oder Kostenträgers" MUSS gesetzt werden.
				ResourceAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
					@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
					@MustBePresent		Der Wert "true" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocuments' -->							
				Action		R	

					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d" " MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" " MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
<!-- Registry Stored Query 'FindSubmissionSets' -->							
				Action		R	
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" " MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cr

							ossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbcla9" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery: queryId" MUSS gesetzt werden.

				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAll' -->						
			Action		R	
			ActionMatch		R	
			@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue		R	
			@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
			text()		R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
			ActionAttributeDesignator		R	
			@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
			@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
			ActionMatch		R	

				@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:10b545ea- 725c-446d-9b95- 8aeb444eddf3" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocuments' -->						
				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.

				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:5c4f972b-d56b-40ac-a5fc-c8ca9b40b9d4" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAssociations' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" " MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				text()		R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" " MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" " MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocumentsAndAssociations' -->							
				Action		R	
				ActionMatch		R	

				@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2

						001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R Der Wert "urn:uuid:bab9529a-4a10-40b3-a01f-f68a615d247a" MUSS gesetzt werden.
					ActionAttributeDesignator	R
					@AttributeId	R Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R Der Wert "http://www.w3.org/2001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSets' -->						
					Action	R
					ActionMatch	R
					@MatchId	R Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R
					@DataType	R Der Wert "http://www.w3.org/2001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:51224314- 5390-4169-9b91- b1980040715a" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2

						001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSetAndContents' -->						
				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0:action: action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:

						xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:e8e3cb2c- e39c-46b9-99e4- c12f57260b83" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetRelatedDocuments' -->						
				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:d90e5407-b356-4d91-a89f-873917b4b0e6" MUSS gesetzt werden.
				ActionAttributeDesignator		R	

					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByReferenceId' -->							
				Action		R	
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2

								001/XMLSchema#anyURI " MUSS gesetzt werden.
				ActionMatch			R	
					@MatchId		R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue		R	
					@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()		R	Der Wert "urn:uuid:12941a89- e02e-4be5-967c- ce4bfc8fe492" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
					@AttributeId		R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByTitle' -->								
			Acti on				R	
			Action Match				R	

				@MatchId			R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue			R	
					@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()		R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator			R	
					@AttributeId		R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
			Action Match				R	
				@MatchId			R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue			R	
					@DataType		R	Der Wert "http://www.w3.org/2

								001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()		R	Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
				ActionAttribut eDesignator			R	
					@AttributeId		R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RemoveDocuments -->								
				Action			R	
				ActionMatch			R	
					@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue			R	
					@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()		R	Der Wert "urn:ihe:iti:2017:RemoveDocuments" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- CrossGatewayRetrieve -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayRetrieve" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				Rule		R	
				@RuleId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
				@Effect		R	Der Wert "Permit" MUSS gesetzt werden.

8.3.3 Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente

Tabelle 46: Tab_Dokv_302 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-Dokumente (Permission Policy)

Element-, Attribut- oder Textknoten gemäß [XACML]	Optional	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	<p>Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents" MUSS gesetzt werden, sofern dieses Policy Set den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden.</p> <p>Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-</p>

						documents" MUSS gesetzt werden, sofern dieses Policy Set den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden.
				@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
				Target	R	Das Element MUSS leer bleiben.
				Policy	R	
				@PolicyId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
				@RuleCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
				Target	R	
				Resources	R	
				Resource	R	
				ResourceMatch	R	

					@MatchId	R	Der Wert "urn:hl7-org:v3:function:CV-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
					CodedValue	R	
					@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
					@code	R	<p>Der Wert "KTR" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents").</p> <p>Der Wert "PAT" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents").</p>
					@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.

						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	O	<p>Der Wert "Dokument eines Kostenträgers" aus MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden</p> <p>(@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents").</p> <p>Der Wert "Dokument eines Versicherten" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden</p> <p>(@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents").</p>
					ResourceAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.

				Actions		R	
<!-- Registry Stored Query 'FindDocuments' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:x

							acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:14d4debf- 8f97-4251-9a74- a90016b0af0d" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindSubmissionSets' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbcl9" MUSS gesetzt werden.
				ActionAttributeDesignator		R	

					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAll' -->							
				Action		R	
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20

								01/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch		R	
					@MatchId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue		R	
					@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()		R	Der Wert "urn:uuid:10b545ea- 725c-446d-9b95- 8aeb444eddf3" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
					@AttributeId		R	Der Wert "urn:ihe:iti:2016:Reg istryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocuments' -->								
					Action		R	
					ActionMatch		R	

					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:5c4f972b- d56b-40ac-a5fc- c8ca9b40b9d4" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAssociations' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocumentsAndAssociations' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:x

							acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:bab9529a- 4a10-40b3-a01f- f68a615d247a" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Reg istryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSets' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:51224314-5390-4169-9b91-b1980040715a" MUSS gesetzt werden.
				ActionAttributeDesignator		R	

					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSetAndContents' -->							
				Action		R	
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:uuid:e8e3cb2c- e39c-46b9-99e4- c12f57260b83" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:ihe:iti:2016:Reg istryStoredQuery: queryId" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetRelatedDocuments' -->							
				Action		R	
				ActionMatch		R	

					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:d90e5407- b356-4d91-a89f- 873917b4b0e6" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByReferenceId' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:12941a89-e02e-4be5-967c-ce4bfc8fe492" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20

								01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByTitle' -->								
			Ac tio n					R
			Actio nMat ch					R
				@MatchId				R Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeVal ue				R
					@DataType			R Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()			R Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.
				ActionAttrib uteDesignat or				R
					@AttributeI d			R Der Wert "urn:oasis:names:tc:x acml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType			R Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.

				ActionMatch				R	
					@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue				R	
					@DataType			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()			R	Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
				ActionAttributeDesignator				R	
					@AttributeId			R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- CrossGatewayRetrieve -->									
				Action				R	
				ActionMatch				R	
					@MatchId			R	Der Wert "urn:oasis:names:tc:x

							acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:Cro ssGatewayRetrieve" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RemoveDocuments -->							
			Action			R	
			ActionMatch			R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.

					AttributeValue		R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2017:RemoveDocuments" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RestrictedUpdateDocumentSet -->								
				Action			R	
				ActionMatch			R	
					@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue			R	
					@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

						text()	R	Der Wert "urn:ihe:iti:2018:RestrictedUpdateDocumentSet" MUSS gesetzt werden.
						ActionAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					Rule		R	
					@RuleId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
					@Effect		R	Der Wert "Permit" MUSS gesetzt werden.

3839 8.4 Policy Document für einen Kostenträger

3840

3841 8.4.1 Base Policy

3842 **Tabelle 47: Tab_Dokv_400 - XACML 2.0 Policy für einen Kostenträger (Base Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt .	Nutzungsvorgabe
PolicySet	R	

@PolicySetId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
@PolicyCombiningAlgId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
Target		R	Das Element MUSS leer bleiben.
<!-- Kostenträger (repräsentiert durch ihre Betriebsnummer) -->			
Subjects		R	
Subject		R	
SubjectMatch		R	
@MatchId		R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
AttributeValue		R	
@DataType		R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
InstanceIdentifier		R	
@xmlns		R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
@root		R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
@extension		R	Als Wert MUSS die Betriebsnummer gesetzt werden.
SubjectAttributeDesignator		R	

				@AttributeId	R	Der Wert " urn:gematik:subject:organization-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Subject	R	
				SubjectMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:string-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#stri ng" MUSS gesetzt werden.
				text()	R	Als Wert MUSS der Name des Kostenträgers gesetzt werden.
				SubjectAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xspa:1.0: subject:organization" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#stri ng" MUSS gesetzt werden.
<!-- KVNR als Aktenidentifikator -->						
				Resources	R	
				Resource	R	

				ResourceMatch	R	
				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS der unveränderbare Teil der KVRN (10 Stellen) gesetzt werden.
				ResourceAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				PolicySetIdReference	R	
				text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurance" MUSS gesetzt werden.

3843 8.4.2 Permission Policy

3844 **Tabelle 48: Tab_Dokv_401 - XACML 2.0 Policy mit erlaubten Operationen für einen**
 3845 **Kostenträger (Permission Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt .	Nutzungsvorgabe
---	----------	-----------------

PolicySet				R	
	@PolicySetId			R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurance" MUSS gesetzt werden.
	@PolicyCombiningAlgId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target			R	Das Element MUSS leer bleiben.
	Policy			R	
	@PolicyId			R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@RuleCombiningAlgId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target			R	
	Resources			R	
	Resource			R	
	ResourceMatch			R	
		@MatchId		R	Der Wert "urn:hl7-org:v3:function:CV-equal" MUSS gesetzt werden.
		AttributeValue		R	
		@DataType		R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.

			CodedValue	R	
			@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
			@code	R	Der Wert "KTR" MUSS gesetzt werden.
			@codeSystem	R	Der Wert "1.2.276.0.76.5.491 " MUSS gesetzt werden.
			@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
			@displayName	O	Der Wert "Dokument eines Kostenträgers" MUSS gesetzt werden.
			ResourceAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
			@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
			@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
			Actions	R	
<!-- 'ProvideAndRegisterDocumentSet-b' -->					
			Action	R	
			ActionMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					Rule	R	
					@RuleId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
					@Effect	R	Der Wert "Permit" MUSS gesetzt werden.

3846

9 Anhang C– XACML 2.0-Profiles für Policy Documents

Die folgende Notation wird zur Kennzeichnung von Optionalitäten (Opt.) in den XACML 2.0 Policies verwendet:

Tabelle 49: Tab_Dokv_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies

Code	Bedeutung
R	Required - Mit "R" gekennzeichnete Element-, Attribut- oder Textknoten MÜSSEN verwendet werden.
O	Optional - Mit "O" gekennzeichnete Element-, Attribut- oder Textknoten KÖNNEN verwendet werden.
X	Mit "X" gekennzeichnete Element-, Attribut- oder Textknoten DÜRFEN NICHT verwendet werden.

Beispiele zu den folgenden XACML 2.0-Profilen können dem beiliegenden Dokumentenpaket entnommen werden.

9.1 Policy Document für einen Versicherten

Tabelle 50: Tab_Dokv_500 - XACML 2.0 Policy für einen Versicherten

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:insurant" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
@Version	R	Der Wert "4.0" MUSS gesetzt werden

		Target	R	Das Element MUSS leer bleiben.
<!-- Versicherter (repräsentiert durch seine KVN) -->				
		Subjects	R	
		Subject	R	
		SubjectMatch	R	
		@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
		AttributeValue	R	
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		InstanceIdentifier	R	
		@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
		@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
		@extension	R	Als Wert MUSS der unveränderbare Teil der KVN (10 Stellen) gesetzt werden.
		SubjectAttributeDesignator	R	
		@AttributeId	R	Der Wert "urn:gematik:subject:subject-id" MUSS gesetzt werden.

			@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
			@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
<!-- KVN R als Aktenidentifikator -->					
			Resources	R	
			Resource	R	
			ResourceMatch	R	
			@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
			AttributeValue	R	
			@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
			InstanceIdentifier	R	
			@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
			@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
			@extension	R	Als Wert MUSS den unveränderbare Teil der KVN R (10 Stellen) gesetzt werden.
			ResourceAttributeDesignator	R	

				@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurant" MUSS gesetzt sein.

3856

3857

3858 9.2 Policy Document für einen Vertreter

3859 **Tabelle 51: Tab_Dokv_501 - XACML 2.0 Policy für einen Vertreter**

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-representative:base" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
@Version	R	Der Wert "4.0" MUSS gesetzt werden.
Target	R	Das Element MUSS leer bleiben.
<!-- Vertreter (repräsentiert durch seine KVNR) -->		

		Subjects	R	
		Subject	R	
		SubjectMatch	R	
		@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
		AttributeValue	R	
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		InstanceIdentifier	R	
		@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
		@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
		@extension	R	Als Wert MUSS der unveränderbare Teil der KVN (10 Stellen) gesetzt werden.
		SubjectAttributeDesignator	R	
		@AttributeId	R	Der Wert "urn:gematik:subject:subject-id" MUSS gesetzt werden.
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.

			Subject	R	
			SubjectMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
			AttributeValue	R	
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
			text()	R	Der Common Name des X.509 Subject Name der eGK MUSS gesetzt werden, um die Lesbarkeit für den Versicherten im ePA-Frontend des Versicherten zu erhöhen, d.h. wem er ein Zugriffsrecht eingeräumt hat.
			SubjectAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:subject:subject" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVNR als Aktenidentifikator -->					
			Resources	R	
			Resource	R	
			ResourceMatch	R	

				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS der unveränderbare Teil der KVN (10 Stellen) gesetzt werden.
				ResourceAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.

3860

3861

3862 9.3 Policy Document für eine Leistungserbringerinstitution

3863 Tabelle 52: Tab_Dokv_502 - XACML 2.0 Policy für eine Leistungserbringerinstitution

Element-, Attribut- oder Textknoten gemäß [XACML]	O p	Nutzungsvorgabe
---	--------	-----------------

										t	
Po lic y S et										R	
	@Poli cySetI d									R	Der Wert "urn:gematik:policy -set-id:permissions- access-group- hcp:base" MUSS gesetzt werden.
	@Poli cyCo mbini ngAlg Id									R	Der Wert "urn:oasis:names:tc: xacml:1.0: policy-combining- algorithm:deny- overrides" MUSS gesetzt werden.
	@Vers ion									R	Der Wert "4.0" MUSS gesetzt werden.
	Targe t									R	Das Element MUSS leer bleiben.
	Policy Set									R	
		@Poli cySetI d								R	Der Wert "urn:gematik:policy -set-id:permissions- access-group- hcp:container" MUSS gesetzt werden.
		@Poli cyCo mbini ngAlg Id								R	Der Wert "urn:oasis:names:tc: xacml:1.0: policy-combining- algorithm:deny- overrides" MUSS gesetzt werden.
		@Vers ion								R	Der Wert "4.0" MUSS gesetzt werden.

		Targe t							R	
		<!-- Leistungserbringerinstitution (repräsentiert durch ihre Telematik- ID) -->								
			Subjects						R	
				Subject					R	
					SubjectMatch				R	
						@MatchId			R	Der Wert "urn:h17-org:v3:function:II-equal" MUSS gesetzt werden.
						AttributeValue			R	
							@Dat aTyp e		R	Der Wert "urn:h17-org:v3#II" MUSS gesetzt werden.
							Insta nceId entifi er		R	
								@x ml ns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
								@r oo t	R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
								@e xte nsi on	R	Als Wert MUSS die Telematik-ID der zu berechtigenden LEI gesetzt werden.

						SubjectAttribut eDesignator		R	
						@Attr ibuteI d		R	Der Wert " urn:gematik:subject :organization-id" MUSS gesetzt werden.
						@Dat aTyp e		R	Der Wert "urn:h17- org:v3#II" MUSS gesetzt werden.
						@Mus tBePr esent		R	Der Wert "true" MUSS gesetzt werden.
					Subject			R	
					SubjectMatch			R	
					@MatchId			R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:string- equal" MUSS gesetzt werden.
					AttributeValue			R	
					@Dat aTyp e			R	Der Wert "http://www.w3.org/2 001/XMLSchema#string " MUSS gesetzt werden.
					text()			R	Als Wert MUSS der Name der Leistungserbringerinsti tution gesetzt werden.
					SubjectAttribut eDesignator			R	
					@Attr ibuteI d			R	Der Wert "urn:oasis:names:tc: xspa:1.0: subject:organization " MUSS gesetzt werden.

							@Data Type	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVN-R als Aktenidentifikator -->									
							Resources	R	
							Resource	R	
							ResourceMatch	R	
							@MatchId	R	Der Wert "urn:h17-org:v3:function:II-equal" MUSS gesetzt werden.
							AttributeValue	R	
							@Data Type	R	Der Wert "urn:h17-org:v3#II" MUSS gesetzt werden.
							Instance Identifier	R	
							@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
							@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
							@extension	R	Als Wert MUSS der unveränderbare Teil der KVN-R (10 Stellen) gesetzt werden.
							ResourceAttribute Designator	R	

							@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
							@DataTyp	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
<!-- Gültigkeitszeitraum des Policy Documents -->									
			Environments					R	
			Environment					R	
			EnvironmentMatch					R	
							@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:date-less-than-or-equal" MUSS gesetzt werden.
						AttributeValue		R	
							@DataTyp	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
							text()	R	Der Wert muss dem Tag der Ausstellung (Format YYYY-MM-DD nach ISO 8601:2004 in UTC) des Policy Documents entsprechen.
							EnvironmentAttributeDesignator	R	

						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.
						@DataTypeId	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
					EnvironmentMatch		R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:date-greater-than" MUSS gesetzt werden.
						AttributeValue	R	
						@DataTypeId	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
						text()	R	Der Wert muss dem Enddatum (Format YYYY-MM-DD nach ISO 8601:2004 in UTC) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen: <ul style="list-style-type: none"> • "heute" + frei wählbare Anzahl Tage in der Spanne von 1 bis 540 oder • "(maximal heute " + 100 Jahre)
						EnvironmentAttributeDesignator	R	

								@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.
								@DateType		R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
<p><-- EntwederDer folgende Teil setzt folgende Auswertungsmechanik um: Permit, wenn (Vertrauensstufe AND Kategorie erlaubt AND notBlacklisted) ODEROR Whitelist. Wenn JA, dann Permit, Ansonsten Deny --></p>											
	Policy Set									R	
		@PolicySetId								R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:all-permissions" MUSS gesetzt werden.
		@PolicyCombiningAlgorithmId								R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides" MUSS gesetzt werden.
		@Version								R	Der Wert "4.0" MUSS gesetzt werden.
		Target								R	Der Wert MUSS leer bleiben.
	<-- Feingranulare Berechtigung: Whitelist -->										
		PolicyIdReference								R	Der Wert "urn:gematik:policy-id:permissions-access-group-

										hcp:whitelist" MUSS gesetzt werden.
		<-- Vertrauensstufe AND Kategorie erlaubt AND not Blacklisted -->								
		Policy Set							R	
		@PolicySetId							R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:base:check-wo-whitelist" MUSS gesetzt werden.
		@PolicyCombiningAlgorithmId							R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
		@Version							R	Der Wert "4.0" MUSS gesetzt werden.
		Target							R	Der Wert MUSS leer bleiben.
		PolicyIdReference							R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:levels" MUSS gesetzt werden.
		PolicyIdReference							R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:categories" MUSS gesetzt werden.

			Policy IdRef erenc e						R	Der Wert "urn:gematik:policy- set-id:permissions- access-group- hcp:blacklist" MUSS gesetzt werden.
		<--Default Policy, die immer Deny zurückgibt -->								
		Policy							R	
			@Poli cyId						R	Der Wert "urn:gematik:po licy-id:permissions- access-group- hcp:base:default- deny" MUSS gesetzt werden.
			@Rule Comib iningA lgId						R	Der Wert "urn:oasis:names:tc: xacml:1.0: rule-combining- algorithm:deny- overrides" MUSS gesetzt werden.
			Targe t						R	Der Wert MUSS leer bleiben.
			Rule						R	
			@ R ul eI d						R	Der Wert "urn:gematik:rule- id:permissions- access-group- hcp:base:default- deny" MUSS gesetzt werden.
			@ Ef fe ct						R	Der Wert "Deny" MUSS gesetzt werden.

<-- Setzen der grobgranularen Berechtigung -->									
Policy Set								R	
	@PolicySetId							R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:levels" MUSS gesetzt werden.
	@PolicyCombiningAlgorithmId							R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides" MUSS gesetzt werden.
	@Version							R	Der Wert "4.0" MUSS gesetzt werden.
	Target							R	Der Wert MUSS leer bleiben.
<-- Grobgranulare Berechtigung "normal" (immer vorhanden) -->									
	PolicyIdReference							R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:levels:normal" MUSS gesetzt werden.
<-- Grobgranulare Berechtigung "erweitert" (nur bei Bedarf vorhanden) -->									
	PolicyIdReference							O	Das Element MUSS genau dann vorhanden sein, wenn "erweiterte Berechtigung" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-

										access-group-hcp:levels:extended" besitzen.
		<-- Default Policy, die immer Deny zurückgibt -->								
		Policy IdReference							R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:base:default-deny" MUSS gesetzt sein.
		<-- Setzen der mittelgranularen Berechtigung -->								
		Policy Set							R	
		@PolicySetId							R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:categories" MUSS gesetzt werden.
		@PolicyCombiningAlgorithmId							R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides" MUSS gesetzt werden.
		@Version							R	Der Wert "4.0" MUSS gesetzt werden.
		Target							R	Der Wert MUSS leer bleiben.
		<--Setzen der Berechtigung auf Kategorie "emp" -->								
		Policy IdReference							O	Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "emp" erteilt

										werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:emp" besitzen.
		<--Setzen der Berechtigung auf Kategorie "nfd" -->								
		Policy IdReference								O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "nfd" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:nfd" besitzen.
		<--Setzen der Berechtigung auf Kategorie "eab" -->								
		Policy IdReference								O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "eab" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:eab" besitzen.
		<-- Setzen der Berechtigung auf Kategorie "dentalrecord" -->								
		Policy IdReference								O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "dentalrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-

										id:permissions-access-group-hcp:categories:dentalrecord" besitzen.
		<-- Setzen der Berechtigung auf Kategorie "childsrecord" -->								
		Policy IdReference								<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "childsrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:childsrecord" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "mothersrecord" -->								
		Policy IdReference								<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "mothersrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:mothersrecord" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "vaccination" -->								
		Policy IdReference								<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "vaccination" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-</p>

										access-group-hcp:categories:vaccination" besitzen.
		<-- Setzen der Berechtigung auf Kategorie "patientdoc" -->								
		Policy IdReference								<p>O Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "patientdoc" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:patientdoc" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "ega" -->								
		Policy IdReference								<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "ega" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:ega" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "receipt" -->								
		Policy IdReference								<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "receipt" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:receipt" besitzen.</p>

		<-- Setzen der Berechtigung auf Kategorie "care" -->							
		Policy IdRef erenc e							O Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "care" erteilt werden soll, und dann den Wert <code>"urn:gematik:policy-id:permissions-access-group-hcp:categories:care"</code> besitzen.
		<-- Setzen der Berechtigung auf Kategorie "prescription" -->							
		Policy IdRef erenc e							O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "prescription" erteilt werden soll, und dann den Wert <code>"urn:gematik:policy-id:permissions-access-group-hcp:categories:prescription"</code> besitzen.
		<-- Setzen der Berechtigung auf Kategorie "eau" -->							
		Policy IdRef erenc e							O Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "eau" erteilt werden soll, und dann den Wert <code>"urn:gematik:policy-id:permissions-access-group-hcp:categories:eau"</code> besitzen.
		<-- Setzen der Berechtigung auf Kategorie "other" -->							
		Policy IdRef							O Das Element MUSS genau dann vorhanden

		erence								sein, wenn die Berechtigung auf Kategorie "other" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:other" besitzen.
		<-- Setzen der Berechtigung für Kategorien practitioner, hospital, laboratory, physiotherapy, psychotherapy, dermatology, gynaecology_urology, dentistry_oms, other_medical und other_non_medical -->								
		Policy IdReference								<p>O Das Element MUSS genau dann vorhanden sein, wenn auf eine der Kategorien category = {practitioner hospital laboratory physiotherapy psychotherapy dermatology, gynaecology_urology dentistry_oms other_medical other_non_medical} berechtigt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:<category>" besitzen.</p> <p>Beispiel: Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:other_medical" berechtigt auf die Kategorie "other_medical".</p> <p>Das Element wird für jede zu berechtigende Kategorie (mit jeweils der Kategorie entsprechenden Wert)</p>

									wiederholt.
		<-- Default Policy, die immer Deny zurückgibt							
		Policy IdReference						R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:base:default-deny" MUSS gesetzt sein.
		<-- Setzen der feingranularen Berechtigung: Blacklist -->							
	Policy							R	
		@PolicyId						R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:blacklist" MUSS gesetzt werden.
		@RuleCombiningAlgorithmId						R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
		Target						R	
		Rule						R	
			@RuleId					R	Der Wert "urn:gematik:rule-id:permissions-access-group-hcp:blacklist" MUSS gesetzt sein.
			@Effect					R	Der Wert "Deny" MUSS gesetzt werden.

			Target					R	
				Resources				O	Das Element MUSS genau dann vorhanden sein, wenn mindestens ein Dokument auf die Blacklist gesetzt werden soll.
				Resource				R	Das Element MUSS genau ein mal für jedes Dokument vorhanden sein, dass auf die Blacklist gesetzt werden soll.
								R	
				ResourceMatch				R	
					@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
					AttributeValue			R	Der Wert MUSS dem Wert der <code>DocumentEntry.uniqueId</code> des Dokuments entsprechen, das auf die Blacklist gesetzt werden soll.
						@DataTyp		R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
					ResourceAttributeDesignator			R	

							@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:resource:resource-id" MUSS gesetzt werden.
							@DataTyp	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
		<-- Default Rule, das immer Permit zurückgibt -->							
		Rule						R	
			@RuleId					R	Der Wert "urn:gematik:rule-id:permissions-access-group-hcp:blacklist:default-permit" MUSS gesetzt werden.
			@Effect					R	Der Wert "Permit" MUSS gesetzt werden.
		<--Setzen der feingranularen Berechtigung: Whitelist -->							
		Policy						R	
			@PolicyId					R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:whitelist" MUSS gesetzt werden.
			@RuleCombiningAlgorithmId					R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides" MUSS gesetzt werden.

		Target							R	
		Rule							R	
		@RuleId							R	Der Wert "urn:gematik:rule-id:permissions-access-group-hcp:whitelist" MUSS gesetzt sein.
		@Effect							R	Der Wert "Permit" MUSS gesetzt werden.
		Target							R	
					Resources				O	Das Element MUSS genau dann vorhanden sein, wenn mindestens ein Dokument auf die Whitelist gesetzt werden soll.
					Resource				R	Das Element MUSS genau ein mal für jedes Dokument vorhanden sein, dass auf die Whitelist gesetzt werden soll.
					ResourceMatch				R	
					@MatchId				R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
					AttributeValue				R	Der Wert MUSS dem Wert der <code>DocumentEntry.uniqueId</code> des Dokuments entsprechen, das auf die Whitelist gesetzt werden soll.

									Der Wert DARF NICHT gleichzeitig in//Policy/Rule[@PolicyId=-'urn:gematik:policy-id:permissions-access-group-hcp:blacklist']/Target/Resources/Resource/ResourceMatch/AttributeValue enthalten sein (Dokument ist nie gleichzeitig auf Black- und Whitelist gelistet).
						@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
						ResourceAttributeDesignator		R	
						@Attribute Id		R	Der Wert "urn:oasis:names:tc:xacml:1.0:resource:resource-id" MUSS gesetzt werden.
						@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<-- Default Rule, das immer Deny zurückgibt -->									
		Rule						R	
		@Rule Id						R	Der Wert "urn:gematik:rule-id:permissions-access-group-hcp:whitelist:default-deny" MUSS gesetzt werden.
		@Effect						R	Der Wert "Deny" MUSS gesetzt werden.

3864

3865 **9.4 Policy Document für einen Kostenträger**3866 **Tabelle 53: Tab_Dokv_503 - XACML 2.0 Policy für einen Kostenträger**

Element-, Attribut- oder Textknoten gemäß [XACML]				Op t.	Nutzungsvorgabe
PolicySet				R	
@PolicySetId				R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-ktr:base" MUSS gesetzt sein.
@PolicyCombiningAlgId				R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides" MUSS gesetzt werden.
@Version				R	Der Wert "4.0" MUSS gesetzt werden.
Target				R	Das Element MUSS leer bleiben.
<!-- Kostenträger (repräsentiert durch ihre Betriebsnummer) -->					
Subjects				R	
Subject				R	
SubjectMatch				R	
			@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
			AttributeValue	R	

					@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
					InstanceIdentifier	R	
					@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
					@root	R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
					@extension	R	Als Wert MUSS die Betriebsnummer gesetzt werden.
				SubjectAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:gematik:subject:organization-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
					@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Subject		R	
				SubjectMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema" MUSS gesetzt werden.

								Schema#string" MUSS gesetzt werden.
					text()	R		Als Wert MUSS der Name <u>der Leistungserbringerinstitution des Kostenträgers</u> gesetzt werden.
					SubjectAttributeDesignator	R		
					@AttributeId	R		Der Wert "urn:oasis:names:tc:xspa:1.0:subject:organization" MUSS gesetzt werden.
					@DataType	R		Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVN als Aktenidentifikator -->								
					Resources	R		
					Resource	R		
					ResourceMatch	R		
					@MatchId	R		Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
					Attribute Value	R		
					@DataType	R		Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
					InstanceIdentifier	R		
					@xmlns	R		Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.

					@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
					@extension	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
					ResourceAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
←! Gültigkeitszeitraum des Policy Documents →							
					Environments	R	
					Environment	R	
					EnvironmentMatch	R	
					@MatchId	R	Der Wert " urn:oasis:names:tc:xaaml:1.0: function:date-less-than-or-equal " MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert " http://www.w3.org/2001/XMLSchema#date " MUSS gesetzt werden.
					text()	R	Der Wert muss dem Tag der Ausstellung (Format YYYY-MM-DD nach ISO-8601:2004 in UTC)
					EnvironmentAttributeDesignator	R	

				@AttributeId	R	Der Wert "urn:oasis:names:tc:xaeml:1.0:environment:current-date" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
			EnvironmentMatch		R	
			@MatchId		R	Der Wert "urn:oasis:names:tc:xaeml:1.0:function:date-greater-than" MUSS gesetzt werden.
			AttributeValue		R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
			text()		R	Der Wert muss dem Enddatum (Format YYYY-MM-DD nach ISO 8601:2004 in UTC) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen: <ul style="list-style-type: none"> • "heute" + frei wählbare Anzahl Tage in der Spanne von 1 bis 540 oder • "heute" + 100 Jahre
			EnvironmentAttributeDescriptor		R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xaeml:1.0:environment:current-date" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.

<!-- Prüfung der Berechtigungskategorien -->		
<-- Setzen der Berechtigung auf Kategorie "receipt" -->		
PolicyIdReference	R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:receipt" MUSS gesetzt werden.
<-- Setzen der Berechtigung auf Kategorie "ega" -->		
PolicyIdReference	R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:ega" MUSS gesetzt werden.

3867

3868

9.5 Statische Permission Policies

3869 Dieses Kapitel listet alle Permission Policies. Sie werden statisch in der
3870 Dokumentenverwaltung hinterlegt.

3871

9.5.1 Grobgranulare Berechtigung: Stufe Normal

```

3872 <?xmlversion="1.0" encoding="UTF-8"?>
3873 <Policy
3874 xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" RuleCombiningAlgId="urn:oa
3875 sis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3876 overrides" PolicyId="urn:gematik:policy-id:permissions-access-group-
3877 hcp:levels:normal" Version="4.0">
3878   <Target/>
3879   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:levels:normal"
3880 Effect="Permit">
3881     <Target>
3882       <Resources>
3883         <Resource>
3884           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3885             <AttributeValue DataType="urn:hl7-org:v3#CV">
3886               <CodedValue xmlns="urn:hl7-org:v3" code="N"
3887 codeSystem="2.16.840.1.113883.5.25" displayName="normal"/>
3888             </AttributeValue>
3889             <ResourceAttributeDesignator
3890 AttributeId="urn:ihe:iti:appc:2016:confidentiality-code" DataType="urn:hl7-
3891 org:v3#CV"/>
3892           </ResourceMatch>
3893         </Resource>
3894       </Resources>

```

```

3895     </Target>
3896   </Rule>
3897   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3898   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3899 hcp:levels:normal:default-deny" Effect="Deny"/>
3900 </Policy>

```

3901 9.5.2 Grobgranulare Berechtigung: Stufe Erweitert

```

3902 <?xml version="1.0" encoding="UTF-8"?>
3903 <Policy
3904   xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
3905   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3906 overrides"
3907   PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:levels:extended"
3908   Version="4.0">
3909   <Target/>
3910   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:levels:extended"
3911 Effect="Permit">
3912     <Target>
3913       <Resources>
3914         <Resource>
3915           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3916             <AttributeValue DataType="urn:hl7-org:v3#CV">
3917               <CodedValue xmlns="urn:hl7-org:v3" code="R"
3918 codeSystem="2.16.840.1.113883.5.25" displayName="restricted"/>
3919             </AttributeValue>
3920             <ResourceAttributeDesignator
3921 AttributeId="urn:ihe:iti:apcc:2016:confidentiality-code" DataType="urn:hl7-
3922 org:v3#CV"/>
3923           </ResourceMatch>
3924         </Resource>
3925       </Resources>
3926     </Target>
3927   </Rule>
3928   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3929   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3930 hcp:levels:extended:default-deny" Effect="Deny"/>
3931 </Policy>

```

3932 9.5.3 Mittelgranulare Berechtigung: Kategorie "care"

```

3933 <?xml version="1.0" encoding="UTF-8"?>
3934 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:care"
3935 xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" RuleCombiningAlgId="urn:oasi
3936 s:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" Version="4.0">
3937   <Target/>
3938   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:care"
3939 Effect="Permit">
3940     <Target>
3941       <Resources>
3942         <Resource>
3943           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">

```

```

3944         <AttributeValue DataType="urn:hl7-org:v3#CV">
3945             <CodedValue xmlns="urn:hl7-org:v3" code="PFL"
3946 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.5"/>
3947         </AttributeValue>
3948         <ResourceAttributeDesignator
3949 AttributeId="urn:ihe:iti:apcc:2016:document-entry:practice-setting-code"
3950 DataType="urn:hl7-org:v3#CV"/>
3951     </ResourceMatch>
3952 </Resource>
3953 </Resources>
3954 </Target>
3955 </Rule>
3956 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3957 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3958 hcp:categories:care:default-deny" Effect="Deny"/>
3959 </Policy>

```

3960 9.5.4 Mittelgranulare Berechtigung: Kategorie "childsrecord"

```

3961 <?xml version="1.0" encoding="UTF-8"?>
3962 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
3963 hcp:categories:childsrecord" xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
3964 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3965 overrides" Version="4.0">
3966     <Target/>
3967     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3968 hcp:categories:childsrecord" Effect="Permit">
3969         <Target>
3970             <Resources>
3971                 <Resource>
3972                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3973                         <AttributeValue DataType="urn:hl7-org:v3#CV">
3974                             <CodedValue xmlns="urn:hl7-org:v3"
3975 code="urn:gematik:ig:Kinderuntersuchungsheft:r4.0"
3976 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
3977                         </AttributeValue>
3978                         <ResourceAttributeDesignator
3979 AttributeId="urn:ihe:iti:apcc:2016:document-entry:related-folder:code"
3980 DataType="urn:hl7-org:v3#CV"/>
3981                     </ResourceMatch>
3982                 </Resource>
3983             </Resources>
3984         </Target>
3985     </Rule>
3986 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3987 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3988 hcp:categories:childsrecord:default-deny" Effect="Deny"/>
3989 </Policy>

```

3990 9.5.5 Mittelgranulare Berechtigung: Kategorie "dentalrecord"

```

3991 <?xml version="1.0" encoding="UTF-8"?>
3992 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-

```

```

3993 hcp:categories:dentalrecord" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
3994 combining-algorithm:deny-overrides" Version="4.0">
3995   <Target/>
3996   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3997 hcp:categories:dentalrecord" Effect="Permit">
3998     <Target>
3999       <Resources>
4000         <Resource>
4001           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4002             <AttributeValue DataType="urn:hl7-org:v3#CV">
4003               <CodedValue xmlns="urn:hl7-org:v3"
4004 code="urn:gematik:ig:Zahnbonusheft:r4.0"
4005 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4006             </AttributeValue>
4007             <ResourceAttributeDesignator
4008 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
4009 org:v3#CV"/>
4010           </ResourceMatch>
4011         </Resource>
4012       </Resources>
4013     </Target>
4014   </Rule>
4015   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4016   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4017 hcp:categories:dentalrecord:default-deny" Effect="Deny"/>
4018 </Policy>

```

9.5.6 Mittelgranulare Berechtigung: Kategorie "eab"

```

4020 <?xml version="1.0" encoding="UTF-8"?>
4021 <!-- Mittelgranular: Kategorie "eArztbrief" -->
4022 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:eab"
4023 xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
4024 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
4025 overrides" Version="4.0">
4026   <Target/>
4027   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:eab"
4028 Effect="Permit">
4029     <Target>
4030       <Resources>
4031         <Resource>
4032           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4033             <AttributeValue DataType="urn:hl7-org:v3#CV">
4034               <CodedValue xmlns="urn:hl7-org:v3"
4035 code="urn:gematik:ig:Arztbrief:r3.1"
4036 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4037             </AttributeValue>
4038             <ResourceAttributeDesignator
4039 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-
4040 code"
4041 urn:hl7-org:v3#CV"/>
4042           </ResourceMatch>
4043         </Resource>
4044       </Resources>

```

DataType="


```

4045     </Target>
4046 </Rule>
4047 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4048 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4049 hcp:categories:eab:default-deny" Effect="Deny"/>
4050 </Policy>
4051

```

4052 9.5.7 Mittelgranulare Berechtigung: Kategorie "eau"

```

4053 <?xml version="1.0" encoding="UTF-8"?>
4054 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:eau"
4055 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
4056 overrides" Version="4.0">
4057   <Target/>
4058   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:eau"
4059 Effect="Permit">
4060     <Target>
4061       <Resources>
4062         <Resource>
4063           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4064             <AttributeValue DataType="urn:hl7-org:v3#CV">
4065               <CodedValue xmlns="urn:hl7-org:v3"
4066 code="urn:gematik:ig:Arbeitsunfähigkeitsbescheinigung:r4.0"
4067 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4068             </AttributeValue>
4069             <ResourceAttributeDesignator
4070 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
4071 org:v3#CV"/>
4072           </ResourceMatch>
4073         </Resource>
4074       </Resources>
4075     </Target>
4076   </Rule>
4077   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4078   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4079 hcp:categories:eau:default-deny" Effect="Deny"/>
4080 </Policy>
4081

```

4082 9.5.8 Mittelgranulare Berechtigung: Kategorie "ega"

```

4083 <?xml version="1.0" encoding="UTF-8"?>
4084 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:ega"
4085 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
4086 overrides" Version="4.0">
4087   <Target/>
4088   <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
4089 hier und unten ergänzen) -->
4090   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:ega"
4091 Effect="Permit">
4092     <Target>
4093       <Resources>

```

```

4094         <Resource>
4095             <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4096                 <AttributeValue DataType="urn:hl7-org:v3#CV">
4097                     <CodedValue xmlns="urn:hl7-org:v3" code="ega"
4098 codeSystem="TODO"/>
4099                 </AttributeValue>
4100                 <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4101 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4102             </ResourceMatch>
4103         </Resource>
4104     </Resources>
4105 </Target>
4106 </Rule>
4107 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4108 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4109 hcp:categories:ega:default_deny" Effect="Deny"/>
4110 </Policy>

```

9.5.9 Mittelgranulare Berechtigung: Kategorie "emp"

```

4112 <?xml version="1.0" encoding="UTF-8"?>
4113 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:emp"
4114 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
4115 overrides" Version="4.0">
4116     <Target/>
4117     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:emp"
4118 Effect="Permit">
4119         <Target>
4120             <Resources>
4121                 <Resource>
4122                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4123                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4124                             <CodedValue xmlns="urn:hl7-org:v3"
4125 code="urn:gematik:ig:Medikationsplan:r3.1"
4126 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4127                         </AttributeValue>
4128                         <ResourceAttributeDesignator AttributeId="urn:ihe:iti:apcc:2016:docum
4129 ent-entry:format-code" DataType="urn:hl7-org:v3#CV"/>
4130                     </ResourceMatch>
4131                 </Resource>
4132             </Resources>
4133         </Target>
4134     </Rule>
4135 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4136 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4137 hcp:categories:emp:default-deny" Effect="Deny"/>
4138 </Policy>

```

9.5.10 Mittelgranulare Berechtigung: Kategorie "mothersrecord"

```

4140 <?xml version="1.0" encoding="UTF-8"?>
4141 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4142 hcp:categories:mothersrecord"

```

```

4143 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
4144 overrides" Version="4.0">
4145   <Target/>
4146   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4147 hcp:categories:mothersrecord" Effect="Permit">
4148     <Target>
4149       <Resources>
4150         <Resource>
4151           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4152             <AttributeValue DataType="urn:hl7-org:v3#CV">
4153               <CodedValue xmlns="urn:hl7-org:v3"
4154 code="urn:gematik:ig:Mutterpass:r4.0" codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4155             </AttributeValue>
4156             <ResourceAttributeDesignator
4157 AttributeId="urn:ihe:iti:apcc:2016:document-entry:related-folder:code"
4158 DataType="urn:hl7-org:v3#CV"/>
4159           </ResourceMatch>
4160         </Resource>
4161       </Resources>
4162     </Target>
4163   </Rule>
4164   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4165   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4166 hcp:categories:mothersrecord:default-deny" Effect="Deny"/>
4167 </Policy>

```

4168 9.5.11 Mittelgranulare Berechtigung: Kategorie "nfd"

```

4169 <?xml version="1.0" encoding="UTF-8"?>
4170 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:nfd"
4171 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
4172 overrides" Version="4.0">
4173   <Target/>
4174   <!--Notfalldatensatz -->
4175   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4176 hcp:categories:nfd:nfd" Effect="Permit">
4177     <Target>
4178       <Resources>
4179         <Resource>
4180           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4181             <AttributeValue DataType="urn:hl7-org:v3#CV">
4182               <CodedValue xmlns="urn:hl7-org:v3"
4183 code="urn:gematik:ig:Notfalldatensatz:r3.1"
4184 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4185             </AttributeValue>
4186             <ResourceAttributeDesignator
4187 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
4188 org:v3#CV"/>
4189           </ResourceMatch>
4190         </Resource>
4191       </Resources>
4192     </Target>
4193   </Rule>
4194   <!--Persönliche Erklärung -->

```

```

4195     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:nfd:pe"
4196     Effect="Permit">
4197         <Target>
4198             <Resources>
4199                 <Resource>
4200                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4201                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4202                             <CodedValue xmlns="urn:hl7-org:v3"
4203                             code="urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1"
4204                             codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4205                         </AttributeValue>
4206                         <ResourceAttributeDesignator
4207                             AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
4208                             org:v3#CV"/>
4209                     </ResourceMatch>
4210                 </Resource>
4211             </Resources>
4212         </Target>
4213     </Rule>
4214     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4215     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4216     hcp:categories:nfd:default-deny" Effect="Deny"/>
4217 </Policy>

```

9.5.12 Mittelgranulare Berechtigung: Kategorie "other"

```

4219 <?xml version="1.0" encoding="UTF-8"?>
4220 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:other"
4221 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4222 overrides" Version="4.0">
4223     <!-- practiceSettingCode = 1.3.6.1.4.1.19376.3.276.1.5.4 (ärztlich) -->
4224     <Target>
4225         <Resources>
4226             <Resource>
4227                 <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
4228                 equal">
4229                     <AttributeValue
4230                     DataType="http://www.w3.org/2001/XMLSchema#string">
4231                         <CodedValue codeSystem="1.3.6.1.4.1.19376.3.276.1.5.4"/>
4232                     </AttributeValue>
4233                     <ResourceAttributeDesignator
4234                     AttributeId="urn:ihe:iti:apcc:2016:document-entry:practice-setting-code"
4235                     DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
4236                 </ResourceMatch>
4237             </Resource>
4238         </Resources>
4239     </Target>
4240     <!-- typeCode = ABRE, PATI oder SCHR -->
4241     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4242     hcp:categories:other:type-code" Effect="Permit">
4243         <Target>
4244             <Resources>
4245                 <Resource>
4246                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">

```

```

4247         <AttributeValue DataType="urn:hl7-org:v3#CV">
4248             <CodedValue xmlns="urn:hl7-org:v3" code="ABRE"
4249 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
4250         </AttributeValue>
4251         <ResourceAttributeDesignator
4252 AttributeId="urn:ihe:iti:apcc:2016:document-entry:type-code" DataType="urn:hl7-
4253 org:v3#CV" MustBePresent="true"/>
4254     </ResourceMatch>
4255 </Resource>
4256 <Resource>
4257     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4258         <AttributeValue DataType="urn:hl7-org:v3#CV">
4259             <CodedValue xmlns="urn:hl7-org:v3" code="PATI"
4260 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
4261         </AttributeValue>
4262         <ResourceAttributeDesignator
4263 AttributeId="urn:ihe:iti:apcc:2016:document-entry:type-code" DataType="urn:hl7-
4264 org:v3#CV" MustBePresent="true"/>
4265     </ResourceMatch>
4266 </Resource>
4267 <Resource>
4268     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4269         <AttributeValue DataType="urn:hl7-org:v3#CV">
4270             <CodedValue xmlns="urn:hl7-org:v3" code="SCHR"
4271 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
4272         </AttributeValue>
4273         <ResourceAttributeDesignator
4274 AttributeId="urn:ihe:iti:apcc:2016:document-entry:type-code" DataType="urn:hl7-
4275 org:v3#CV" MustBePresent="true"/>
4276     </ResourceMatch>
4277 </Resource>
4278 </Resources>
4279 </Target>
4280 </Rule>
4281 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4282 hcp:categories:other:default-deny" Effect="Deny"/>
4283 </Policy>

```

9.5.13 Mittelgranulare Berechtigung: Kategorie "patientdoc"

```

4284
4285 <?xmlversion="1.0" encoding="UTF-8"?>
4286 <PolicyPolicyId="urn:gematik:policy-id:permissions-access-group-
4287 hcp:categories:patientdoc" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4288 combining-algorithm:deny-overrides" Version="4.0">
4289     <Target/>
4290     <RuleRuleId="urn:gematik:rule-id:permissions-access-group-
4291 hcp:categories:patientdoc" Effect="Permit">
4292         <Target>
4293             <Resources>
4294                 <Resource>
4295                     <ResourceMatchMatchId="urn:hl7-org:v3:function:CV-equal">
4296                         <AttributeValueDataType="urn:hl7-org:v3#CV">
4297                             <CodedValuecode="102"
4298 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.13"/>

```

```

4299         </AttributeValue>
4300         <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4301 entry:related-submission-set:author-role" DataType="urn:hl7-org:v3#CV"/>
4302     </ResourceMatch>
4303 </Resource>
4304 </Resources>
4305 </Target>
4306 </Rule>
4307 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4308 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4309 hcp:categories:patientdoc:default-deny" Effect="Deny"/>
4310 </Policy>

```

4311 9.5.14 Mittelgranulare Berechtigung: Kategorie "prescription"

```

4312 <?xml version="1.0" encoding="UTF-8"?>
4313 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4314 hcp:categories:prescription" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4315 combining-algorithm:deny-overrides" Version="4.0">
4316     <Target/>
4317     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4318 hcp:categories:prescription" Effect="Permit">
4319         <Target>
4320             <Resources>
4321                 <Resource>
4322                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4323                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4324                             <CodedValue xmlns="urn:hl7-org:v3"
4325 code="urn:gematik:ig:VerordnungsdatensatzMedikation:r4.0"
4326 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4327                         </AttributeValue>
4328                         <ResourceAttributeDesignator
4329 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
4330 org:v3#CV"/>
4331                     </ResourceMatch>
4332                 </Resource>
4333             </Resources>
4334         </Target>
4335     </Rule>
4336 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4337 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4338 hcp:categories:prescription:default-deny" Effect="Deny"/>
4339 </Policy>

```

4340 9.5.15 Mittelgranulare Berechtigung: Kategorie "receipt"

```

4341 <?xml version="1.0" encoding="UTF-8"?>
4342 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4343 hcp:categories:receipt" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4344 combining-algorithm:deny-overrides" Version="4.0">
4345     <Target/>
4346     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:receipt"
4347 Effect="Permit">

```



```

4348     <Target>
4349         <Resources>
4350             <Resource>
4351                 <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4352                     <AttributeValue DataType="urn:hl7-org:v3#CV">
4353                         <CodedValue xmlns="urn:hl7-org:v3" code="VER"
4354 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.3"/>
4355                     </AttributeValue>
4356                     <ResourceAttributeDesignator
4357 AttributeId="urn:ihe:iti:apcc:2016:document-entry:healthcare-facility-type-code"
4358 DataType="urn:hl7-org:v3#CV"/>
4359                 </ResourceMatch>
4360             </Resource>
4361             <Resource>
4362                 <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4363                     <AttributeValue DataType="urn:hl7-org:v3#CV">
4364                         <CodedValue xmlns="urn:hl7-org:v3" code="ABRE"
4365 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
4366                     </AttributeValue>
4367                     <ResourceAttributeDesignator
4368 AttributeId="urn:ihe:iti:apcc:2016:document-entry:type-code" DataType="urn:hl7-
4369 org:v3#CV"/>
4370                 </ResourceMatch>
4371             </Resource>
4372         </Resources>
4373     </Target>
4374 </Rule>
4375 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4376 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4377 hcp:categories:receipt:default-deny" Effect="Deny"/>
4378 </Policy>

```

9.5.16 Mittelgranulare Berechtigung: Kategorie "vaccination"

```

4380 <?xml version="1.0" encoding="UTF-8"?>
4381 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4382 hcp:categories:vaccination" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4383 combining-algorithm:deny-overrides" Version="4.0">
4384     <Target/>
4385     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4386 hcp:categories:vaccination" Effect="Permit">
4387         <Target>
4388             <Resources>
4389                 <Resource>
4390                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4391                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4392                             <CodedValue xmlns="urn:hl7-org:v3"
4393 code="urn:gematik:ig:Impfausweis:r4.0"
4394 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4395                         </AttributeValue>
4396                         <ResourceAttributeDesignator
4397 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
4398 org:v3#CV"/>
4399                     </ResourceMatch>

```

```

4400         </Resource>
4401     </Resources>
4402 </Target>
4403 </Rule>
4404 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4405 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4406 hcp:categories:vaccination:default-deny" Effect="Deny"/>
4407 </Policy>

```

4408 9.5.17 Mittelgranulare Berechtigung: Kategorie "practitioner"

```

4409 <?xml version="1.0" encoding="UTF-8"?>
4410 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4411 hcp:categories:practitioner" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4412 combining-algorithm:permit-overrides" Version="4.0">
4413     <Target/>
4414     <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
4415 hier und unten ergänzen) -->
4416     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4417 hcp:categories:practitioner" Effect="Permit">
4418         <Target>
4419             <Resources>codelist
4420                 <Resource>
4421                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4422                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4423                             <CodedValue xmlns="urn:hl7-org:v3" code="practitioner"
4424 codeSystem="TODO"/>
4425                         </AttributeValue>
4426                         <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4427 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4428                     </ResourceMatch>
4429                 </Resource>
4430             </Resources>
4431         </Target>
4432     </Rule>
4433     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4434     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4435 hcp:categories:practitioner:default-deny" Effect="Deny">
4436         <Target/>
4437     </Rule>
4438 </Policy>

```

4439 9.5.18 Mittelgranulare Berechtigung: Kategorie "hospital"

```

4440 <?xml version="1.0" encoding="UTF-8"?>
4441 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4442 hcp:categories:hospital" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4443 combining-algorithm:permit-overrides" Version="4.0">
4444     <Target/>
4445     <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
4446 hier und unten ergänzen) -->
4447     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4448 hcp:categories:hospital" Effect="Permit">

```



```

4449     <Target>
4450       <Resources>
4451         <Resource>
4452           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4453             <AttributeValue DataType="urn:hl7-org:v3#CV">
4454               <CodedValue xmlns="urn:hl7-org:v3" code="hospital"
4455 codeSystem="TODO"/>
4456             </AttributeValue>
4457             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4458 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4459           </ResourceMatch>
4460         </Resource>
4461       </Resources>
4462     </Target>
4463   </Rule>
4464   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4465   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4466 hcp:categories:hospital:default-deny" Effect="Deny">
4467     <Target/>
4468   </Rule>
4469 </Policy>

```

9.5.19 Mittelgranulare Berechtigung: Kategorie "laboratory"

```

4470
4471 <?xml version="1.0" encoding="UTF-8"?>
4472 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4473 hcp:categories:laboratory" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4474 combining-algorithm:permit-overrides" Version="4.0">
4475   <Target/>
4476   <!--Prüfung, ob folder.codeList den Code "laboratory" enthält (TODO: Code System
4477 hier und unten ergänzen) -->
4478   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4479 hcp:categories:laboratory" Effect="Permit">
4480     <Target>
4481       <Resources>
4482         <Resource>
4483           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4484             <AttributeValue DataType="urn:hl7-org:v3#CV">
4485               <CodedValue xmlns="urn:hl7-org:v3" code="laboratory"
4486 codeSystem="TODO"/>
4487             </AttributeValue>
4488             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4489 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4490           </ResourceMatch>
4491         </Resource>
4492       </Resources>
4493     </Target>
4494   </Rule>
4495   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4496   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4497 hcp:categories:laboratory:default-deny" Effect="Deny">
4498     <Target/>
4499   </Rule>
4500 </Policy>

```

9.5.20 Mittelgranulare Berechtigung: Kategorie "physiotherapy"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:physiotherapy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
  <Target/>
  <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:physiotherapy" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="physiotherapy"
codeSystem="TODO"/>
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:physiotherapy:default-deny" Effect="Deny">
    <Target/>
  </Rule>
</Policy>

```

9.5.21 Mittelgranulare Berechtigung: Kategorie "psychotherapy"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:psychotherapy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
  <Target/>
  <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:psychotherapy" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="psychotherapy"
codeSystem="TODO"/>

```

```

4551         </AttributeValue>
4552         <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4553 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4554     </ResourceMatch>
4555 </Resource>
4556 </Resources>
4557 </Target>
4558 </Rule>
4559 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4560 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4561 hcp:categories:psychotherapy:default-deny" Effect="Deny">
4562     <Target/>
4563 </Rule>
4564 </Policy>

```

9.5.22 Mittelgranulare Berechtigung: Kategorie "dermatology"

```

4566 <?xml version="1.0" encoding="UTF-8"?>
4567 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4568 hcp:categories:dermatology" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4569 combining-algorithm:permit-overrides" Version="4.0">
4570     <Target/>
4571     <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
4572 hier und unten ergänzen) -->
4573     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4574 hcp:categories:dermatology" Effect="Permit">
4575         <Target>
4576             <Resources>
4577                 <Resource>
4578                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4579                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4580                             <CodedValue xmlns="urn:hl7-org:v3" code="dermatology"
4581 codeSystem="TODO"/>
4582                         </AttributeValue>
4583                         <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4584 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4585                     </ResourceMatch>
4586                 </Resource>
4587             </Resources>
4588         </Target>
4589     </Rule>
4590     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4591     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4592 hcp:categories:dermatology:default-deny" Effect="Deny">
4593         <Target/>
4594     </Rule>
4595 </Policy>

```

9.5.23 Mittelgranulare Berechtigung: Kategorie "gynaecology_urology"

```

4596 <?xml version="1.0" encoding="UTF-8"?>
4597 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-

```

```

4600 hcp:categories:gynaecology_urology"
4601 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4602 overrides" Version="4.0">
4603   <Target/>
4604   <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
4605 hier und unten ergänzen) -->
4606   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4607 hcp:categories:gynaecology_urology" Effect="Permit">
4608     <Target>
4609       <Resources>
4610         <Resource>
4611           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4612             <AttributeValue DataType="urn:hl7-org:v3#CV">
4613               <CodedValue xmlns="urn:hl7-org:v3" code="gynaecology_urology"
4614 codeSystem="TODO"/>
4615             </AttributeValue>
4616             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4617 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4618           </ResourceMatch>
4619         </Resource>
4620       </Resources>
4621     </Target>
4622   </Rule>
4623   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4624   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4625 hcp:categories:gynaecology_urology:default-deny" Effect="Deny">
4626     <Target/>
4627   </Rule>
4628 </Policy>

```

9.5.24 Mittelgranulare Berechtigung: Kategorie "dentistry_oms"

```

4630 <?xml version="1.0" encoding="UTF-8"?>
4631 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4632 hcp:categories:dentistry_oms"
4633 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4634 overrides" Version="4.0">
4635   <Target/>
4636   <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
4637 hier und unten ergänzen) -->
4638   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4639 hcp:categories:dentistry_oms" Effect="Permit">
4640     <Target>
4641       <Resources>
4642         <Resource>
4643           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4644             <AttributeValue DataType="urn:hl7-org:v3#CV">
4645               <CodedValue xmlns="urn:hl7-org:v3" code="dentistry_oms"
4646 codeSystem="TODO"/>
4647             </AttributeValue>
4648             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4649 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4650           </ResourceMatch>
4651         </Resource>

```

```

4652         </Resources>
4653     </Target>
4654 </Rule>
4655     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4656     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4657 hcp:categories:dentistry_oms:default-deny" Effect="Deny">
4658         <Target/>
4659     </Rule>
4660 </Policy>

```

4661 9.5.25 Mittelgranulare Berechtigung: Kategorie "other_medical"

```

4662 <?xml version="1.0" encoding="UTF-8"?>
4663 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4664 hcp:categories:other_medical"
4665 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4666 overrides" Version="4.0">
4667     <Target/>
4668     <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
4669 hier und unten ergänzen) -->
4670     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4671 hcp:categories:other_medical" Effect="Permit">
4672         <Target>
4673             <Resources>
4674                 <Resource>
4675                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4676                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4677                             <CodedValue xmlns="urn:hl7-org:v3" code="other_medical"
4678 codeSystem="TODO"/>
4679                         </AttributeValue>
4680                         <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4681 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4682                     </ResourceMatch>
4683                 </Resource>
4684             </Resources>
4685         </Target>
4686     </Rule>
4687     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4688     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4689 hcp:categories:other_medical:default-deny" Effect="Deny">
4690         <Target/>
4691     </Rule>
4692 </Policy>

```

4693 9.5.26 Mittelgranulare Berechtigung: Kategorie 4694 "other_non_medical"

```

4695 <?xml version="1.0" encoding="UTF-8"?>
4696 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4697 hcp:categories:other_non_medical"
4698 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4699 overrides" Version="4.0">
4700     <Target/>

```

```


4701     <!--Prüfung, ob folder.codeList den Code "other_non_medical" enthält (TODO: Code
4702     System hier und unten ergänzen) -->
4703     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4704     hcp:categories:other_non_medical" Effect="Permit">
4705         <Target>
4706             <Resources>
4707                 <Resource>
4708                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4709                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4710                             <CodedValue xmlns="urn:hl7-org:v3" code="other_non_medical"
4711                             codeSystem="TODO"/>
4712                         </AttributeValue>
4713                         <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4714                         entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4715                     </ResourceMatch>
4716                 </Resource>
4717             </Resources>
4718         </Target>
4719     </Rule>
4720     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4721     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4722     hcp:categories:other_non_medical:default-deny" Effect="Deny">
4723         <Target/>
4724     </Rule>
4725 </Policy>

```

A 14489 - Komponente ePA-Dokumentenverwaltung – Signatur für RemoveMetadata

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I Document Management::RemoveMetadata` gemäß der folgenden Signatur implementieren:

Tabelle 54: Tab Dokv 17 - Operation Remove Metadata

<u>Operation</u>		<u>I Document Management::RemoveMetadata</u>	
<u>Beschreibung</u>		Diese Operation setzt die in [gemSysL_ePA] definierte Operation <u>I Document Management::deleteDocuments</u> technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove Metadata" [ITI-62] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente, Ordner und/oder Associations eines Aktenkontos im ePA-Aktensystem zu löschen.	
<u>Formatvorgaben</u>		SOAP Action: <u>urn:ihe:iti:2010>DeleteDocumentSet</u>	
<u>Eingangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt</u>
			

<u>Remove Documents Message</u>	<u>Eingangsnachricht zum Löschen ein oder mehrerer Dokumente, Ordner und/oder Associations</u>	<u>xds:DeleteDocumentSet_Message</u>	<u>n</u>
<u>X-User Assertion</u>	<u>Authentication Assertion der authentifizierten Leistungserbringerinstitution</u>	<u>SAML 2.0 Assertion gemäß [gemSpec FM ePA#A 14927, A 15638]</u>	<u>n</u>
<u>Ausgangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt</u> :
<u>Remove Documents Response Message</u>	<u>Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente, Ordner und/oder Associations.</u>	<u>xds:DeleteDocumentSetResponse_Message</u>	<u>n</u>
<u>Technische Fehlermeldungen</u> <u>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</u>			
<u>Name</u>	<u>Fehlertext</u>	<u>Details</u>	

[<=]