

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: [1.56.0 CC2](#)
Revision: [241917271091](#)
Stand: [30.0625.08.2020](#)
Status: [zur Abstimmung](#) freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_Dokumentenverwaltung

26

Dokumentinformationen

Änderungen zur Vorversion

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

30

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 4.22A 20191.3.7 -> 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	2226.06.20		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 CC CC2	17.08.20 25.08.20		Einarbeitung der Scope-Themen Anpassungen bzgl. PDSG zur Abstimmung freigegeben	gematik

ENTWURF

Inhaltsverzeichnis

1 Einführung	12
1.1 Zielsetzung	12
1.2 Zielgruppe	12
1.3 Geltungsbereich	12
1.4 Abgrenzungen	12
1.5 Methodik	13
2 Systemkontext	14
3 Zerlegung der Komponente	15
4 Übergreifende Festlegungen	16
4.1 Namensräume	16
4.2 Nutzung von IHE IT Infrastructure Profilen für Speicherung und Abruf von Dokumenten	17
4.2.1 Anforderungen an IHE ITI Akteure	17
4.2.1.1 APPC Content Consumer	19
4.2.1.1.1 Gruppierungen mit anderen IHE ITI Akteuren	19
4.2.1.1.2 Optionen des IHE ITI Akteurs	19
4.2.1.2 RMU Update Responder	20
4.2.1.2.1 Gruppierungen mit anderen IHE ITI Akteuren	20
4.2.1.2.2 Optionen des IHE ITI Akteurs	20
4.2.1.3 XCA Responding Gateway	21
4.2.1.3.1 Gruppierungen mit anderen IHE ITI Akteuren	21
4.2.1.3.2 Optionen des IHE ITI Akteurs	21
4.2.1.4 XCDR Responding Gateway	21
4.2.1.4.1 Gruppierungen mit anderen IHE ITI Akteuren	21
4.2.1.4.2 Optionen des IHE ITI Akteurs	22
4.2.1.5 XDS Document Registry	22
4.2.1.5.1 Gruppierungen mit anderen IHE ITI Akteuren	22
4.2.1.5.2 Optionen des IHE ITI Akteurs	22
4.2.1.6 XDS Document Repository	23
4.2.1.6.1 Gruppierungen mit anderen IHE ITI Akteuren	23
4.2.1.6.2 Optionen des IHE ITI Akteurs	23
4.2.1.7 XUA X-Service Provider	23
4.2.1.7.1 Gruppierungen mit anderen IHE ITI Akteuren	23
4.2.1.7.2 Optionen des IHE ITI Akteurs	23
4.2.2 Überblick über gruppierte IHE ITI Akteure und Optionen	24
4.2.3 Einschränkungen auf IHE ITI Transaktionen bei mehreren Schnittstellen	28

69	4.2.3.1 Provide X-User Assertion [ITI-40].....	28
70	4.2.3.2 Provide and Register Document Set-b [ITI-41].....	29
71	4.2.3.3 Remove Documents [ITI-86].....	30
72	4.3 Fehlerbehandlung in Schnittstellenoperationen	30
73	4.4 Vertrauenswürdige Ausführungsumgebung	31
74	4.4.1 Verarbeitungskontext	32
75	4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	33
76	4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes	34
77	4.4.4 Parallele Zugriffe.....	35
78	4.4.5 Konsistenz der Akte, Logging und Monitoring.....	35
79	4.4.6 Client Verbindungen zum Verarbeitungskontext.....	36
80	4.5 Anforderungen zur sicherheitstechnischen Validierung.....	37
81	4.6 Protokollierung.....	40
82	5 Funktionsmerkmale	49
83	5.1 Dokumentenverwaltung	49
84	5.1.1 Schnittstelle I_Document_Management	49
85	5.1.1.1 Operation I_Document_Management::CrossGatewayDocumentProvide ...	50
86	5.1.1.1.1 Umsetzung	51
87	5.1.1.2 Operation I_Document_Management::CrossGatewayQuery	53
88	5.1.1.2.1 Umsetzung	54
89	5.1.1.3 Operation I_Document_Management::RemoveDocuments	55
90	5.1.1.3.1 Umsetzung	57
91	5.1.1.4 Operation I_Document_Management::CrossGatewayRetrieve	57
92	5.1.1.4.1 Umsetzung	58
93	5.1.2 Schnittstelle I_Document_Management_Insurant.....	59
94	5.1.2.1 Operation	
95	I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b.....	60
96	5.1.2.1.1 Umsetzung	62
97	5.1.2.2 Operation I_Document_Management_Insurant::RegistryStoredQuery.....	62
98	5.1.2.2.1 Umsetzung	63
99	5.1.2.3 Operation I_Document_Management_Insurant::RemoveDocuments.....	66
100	5.1.2.3.1 Umsetzung	68
101	5.1.2.4 Operation I_Document_Management_Insurant::RetrieveDocumentSet ...	68
102	5.1.2.4.1 Umsetzung	69
103	5.1.2.5 Operation	
104	I_Document_Management_Insurant::RestrictedUpdateDocumentSet.....	70
105	5.1.2.5.1 Umsetzung	71
106	5.1.3 Schnittstelle I_Document_Management_Insurance.....	73
107	5.1.3.1 Operation	
108	I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b	73
109	5.1.3.1.1 Umsetzung	75
110	5.2 Aktenkontoverwaltung	76
111	5.2.1 Schnittstelle I_Account_Management_Insurant.....	76
112	5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount.....	77
113	5.2.1.1.1 Umsetzung	79

114	5.2.1.2 Operation I_Account_Management_Insurant::ResumeAccount.....	80
115	5.2.1.2.1 Umsetzung.....	82
116	5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents.....	84
117	5.2.1.3.1 Umsetzung.....	85
118	5.3 Zugriffskontrolle.....	100
119	5.3.1 Grob-, mittel- und feingranulare Berechtigungen.....	100
120	5.3.2 Berufsgruppenspezifische Einschränkungen.....	101
121	5.3.3 Grundsätzliche Umsetzung der Berechtigungsregeln.....	101
122	5.3.4 Vergabe von Zugriffsregeln.....	102
123	5.3.5 Funktionsprinzip Policy Administration.....	102
124	5.3.6 Anforderungen an die Zugriffskontrollprüfung.....	105
125	5.3.6.1 Erstmaliges Öffnen eines Verarbeitungskontextes.....	111
126	5.3.6.2 Berechtigung für einen Versicherten.....	112
127	5.3.6.3 Berechtigung für einen Vertreter.....	113
128	5.3.6.4 Berechtigung für eine Leistungserbringerinstitution.....	113
129	5.3.6.5 Berechtigung für einen Kostenträger.....	113
130	5.3.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4.....	113
131	5.4 Vertrauenswürdige Ausführung.....	115
132	5.4.1 Schnittstelle I_Document_Management_Connect.....	115
133	5.4.1.1 Operation I_Document_Management_Connect::OpenContext.....	120
134	5.4.1.1.1 Umsetzung.....	121
135	5.4.1.2 Operation I_Document_Management_Connect::CloseContext.....	122
136	5.4.1.2.1 Umsetzung.....	123
137	5.4.2 Hardware-Merkmale.....	124
138	5.5 Statische Akteninhalte.....	124
139	6 Informationsmodelle.....	126
140	7 Anhang A – Verzeichnisse.....	127
141	7.1 Abkürzungen.....	127
142	7.2 Glossar.....	129
143	7.3 Abbildungsverzeichnis.....	129
144	7.4 Tabellenverzeichnis.....	129
145	7.5 Referenzierte Dokumente.....	132
146	7.5.1 Dokumente der gematik.....	132
147	7.5.2 Weitere Dokumente.....	133
148	8 Anhang B – XACML 2.0 Profile für Policy Documents (für	
149	Upgrade von ePA 3.1.3).....	137
150	8.1 Policy Document für einen Versicherten.....	137
151	8.1.1 Base Policy.....	137
152	8.1.2 Permission Policy.....	140
153	8.2 Policy Document für einen Vertreter.....	171
154	8.2.1 Base Policy.....	171
155	8.2.2 Permission Policy.....	175
156	8.3 Policy Document für eine Leistungserbringerinstitution.....	203
157	8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente.....	203

158	8.3.2 Permission Policy zum Zugriff auf Leistungserbringer Dokumente	208
159	8.3.3 Permission Policy zum Zugriff auf Versicherten- und Kostenträger Dokumente	234
160	234
161	8.4 Policy Document für einen Kostenträger	258
162	8.4.1 Base Policy	258
163	8.4.2 Permission Policy	261
164	9 Anhang C XACML 2.0 Profile für Policy Documents	265
165	9.1 Policy Document für einen Versicherten	265
166	9.2 Policy Document für einen Vertreter	268
167	9.3 Policy Document für eine Leistungserbringerinstitution	271
168	9.4 Policy Document für einen Kostenträger	300
169	9.5 Statische Permission Policies	306
170	9.5.1 Grobgranulare Berechtigung: Stufe Normal	306
171	9.5.2 Grobgranulare Berechtigung: Stufe Erweitert	307
172	9.5.3 Mittelgranulare Berechtigung: Kategorie "care"	308
173	9.5.4 Mittelgranulare Berechtigung: Kategorie "childsrecord"	308
174	9.5.5 Mittelgranulare Berechtigung: Kategorie "dentalrecord"	309
175	9.5.6 Mittelgranulare Berechtigung: Kategorie "eau"	309
176	9.5.7 Mittelgranulare Berechtigung: Kategorie "ega"	311
177	9.5.8 Mittelgranulare Berechtigung: Kategorie "emp"	311
178	9.5.9 Mittelgranulare Berechtigung: Kategorie "mothersrecord"	312
179	9.5.10 Mittelgranulare Berechtigung: Kategorie "nfd"	312
180	9.5.11 Mittelgranulare Berechtigung: Kategorie "other"	313
181	9.5.12 Mittelgranulare Berechtigung: Kategorie "patientdoc"	315
182	9.5.13 Mittelgranulare Berechtigung: Kategorie "prescription"	315
183	9.5.14 Mittelgranulare Berechtigung: Kategorie "receipt"	316
184	9.5.15 Mittelgranulare Berechtigung: Kategorie "vaccination"	317
185	9.5.16 Mittelgranulare Berechtigung: Kategorie "category_1a1"	317
186	9.5.17 Mittelgranulare Berechtigung: Kategorie "category_1a2"	318
187	9.5.18 Mittelgranulare Berechtigung: Kategorie "category_1a3"	318
188	9.5.19 Mittelgranulare Berechtigung: Kategorie "category_1a4"	319
189	9.5.20 Mittelgranulare Berechtigung: Kategorie "category_1a5"	320
190	9.5.21 Mittelgranulare Berechtigung: Kategorie "category_1a6"	320
191	9.5.22 Mittelgranulare Berechtigung: Kategorie "category_1a7"	321
192	9.5.23 Mittelgranulare Berechtigung: Kategorie "category_1a8"	322
193	9.5.24 Mittelgranulare Berechtigung: Kategorie "category_1a9"	322
194	9.5.25 Mittelgranulare Berechtigung: Kategorie "category_1a10"	323
195	1 Einführung	12
196	1.1 Zielsetzung	12
197	1.2 Zielgruppe	12
198	1.3 Geltungsbereich	12
199	1.4 Abgrenzungen	12
200	1.5 Methodik	13
201	2 Systemkontext	14

3 Zerlegung der Komponente.....	15
4 Übergreifende Festlegungen	16
4.1 Namensräume	16
4.2 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von Dokumenten.....	17
4.2.1 Anforderungen an IHE ITI-Akteure	17
4.2.1.1 APPC Content Consumer	19
4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren	19
4.2.1.1.2 Optionen des IHE ITI-Akteurs	19
4.2.1.2 RMU Update Responder.....	20
4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren	20
4.2.1.2.2 Optionen des IHE ITI-Akteurs	20
4.2.1.3 XCA Responding Gateway.....	21
4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren	21
4.2.1.3.2 Optionen des IHE ITI-Akteurs	21
4.2.1.4 XCDR Responding Gateway	21
4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren	21
4.2.1.4.2 Optionen des IHE ITI-Akteurs	22
4.2.1.5 XDS Document Registry	22
4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren	22
4.2.1.5.2 Optionen des IHE ITI-Akteurs	22
4.2.1.6 XDS Document Repository.....	23
4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
4.2.1.6.2 Optionen des IHE ITI-Akteurs	23
4.2.1.7 XUA X-Service Provider.....	23
4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
4.2.1.7.2 Optionen des IHE ITI-Akteurs	23
4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen.....	24
4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen	28
4.2.3.1 Provide X-User Assertion [ITI-40].....	28
4.2.3.2 Provide and Register Document Set-b [ITI-41].....	29
4.2.3.3 Remove Metadata [ITI-62].....	30
4.3 Fehlerbehandlung in Schnittstellenoperationen	30
4.4 Vertrauenswürdige Ausführungsumgebung	31
4.4.1 Verarbeitungskontext	32
4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	33
4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes	34
4.4.4 Parallele Zugriffe.....	35
4.4.5 Konsistenz der Akte, Logging und Monitoring.....	35
4.4.6 Client-Verbindungen zum Verarbeitungskontext.....	36
4.5 Anforderungen zur sicherheitstechnischen Validierung.....	37
4.6 Protokollierung.....	40
4.6.1 Protokollierung von Berechtigungen	44

5 Funktionsmerkmale	49
5.1 Dokumentenverwaltung	49
5.1.1 Schnittstelle I Document Management	49
5.1.1.1 Operation I Document Management::CrossGatewayDocumentProvide ...	50
5.1.1.1.1 Umsetzung	51
5.1.1.2 Operation I Document Management::CrossGatewayQuery	53
5.1.1.2.1 Umsetzung	54
5.1.1.3 Operation I Document Management::RemoveMetadata	55
5.1.1.3.1 Umsetzung	57
5.1.1.4 Operation I Document Management::CrossGatewayRetrieve	57
5.1.1.4.1 Umsetzung	58
5.1.2 Schnittstelle I Document Management Insurant.....	59
5.1.2.1 Operation	
I Document Management Insurant::ProvideAndRegisterDocumentSet-b.....	60
5.1.2.1.1 Umsetzung	62
5.1.2.2 Operation I Document Management Insurant::RegistryStoredQuery	62
5.1.2.2.1 Umsetzung	63
5.1.2.3 Operation I Document Management Insurant::RemoveMetadata.....	66
5.1.2.3.1 Umsetzung	68
5.1.2.4 Operation I Document Management Insurant::RetrieveDocumentSet ...	68
5.1.2.4.1 Umsetzung	69
5.1.2.5 Operation	
I Document Management Insurant::RestrictedUpdateDocumentSet.....	70
5.1.2.5.1 Umsetzung	71
5.1.3 Schnittstelle I Document Management Insurance.....	73
5.1.3.1 Operation	
I Document Management Insurance::ProvideAndRegisterDocumentSet-b	73
5.1.3.1.1 Umsetzung	75
5.1.4 Anforderungen an Sammlungstypen	75
5.2 Aktenkontoverwaltung	76
5.2.1 Schnittstelle I Account Management Insurant.....	76
5.2.1.1 Operation I Account Management Insurant::SuspendAccount.....	77
5.2.1.1.1 Umsetzung	79
5.2.1.2 Operation I Account Management Insurant::ResumeAccount.....	80
5.2.1.2.1 Umsetzung	82
5.2.1.3 Operation I Account Management Insurant::GetAuditEvents	84
5.2.1.3.1 Umsetzung	85
5.3 Umschlüsselung	85
5.3.1 Übergreifende Anforderungen	86
5.3.2 Schnittstelle I Key Management Insurant.....	90
5.3.2.1 I Key Management Insurant::StartKeyChange()	90
5.3.2.1.1 Umsetzung	92
5.3.2.2 I Key Management Insurant::GetAllDocumentKeys().....	93
5.3.2.2.1 Umsetzung	95
5.3.2.3 Operation I Key Management Insurant::PutAllDocumentKeys()	95
5.3.2.3.1 Umsetzung	97

291	5.3.2.4 Operation I Key Management Insurant::FinishKeyChange()	97
292	5.3.2.4.1 Umsetzung	99
293	5.3.2.5 Protokollierung	99
294	5.4 Zugriffskontrolle	100
295	5.4.1 Grob-, mittel- und feingranulare Berechtigungen	100
296	5.4.2 Berufsgruppenspezifische Einschränkungen	101
297	5.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln	101
298	5.4.4 Vergabe von Zugriffsregeln	102
299	5.4.5 Funktionsprinzip Policy Administration	102
300	5.4.6 Anforderungen an die Zugriffskontrollprüfung	105
301	5.4.6.1 Erstmaliges Öffnen eines Verarbeitungskontextes	111
302	5.4.6.2 Berechtigung für einen Versicherten	112
303	5.4.6.3 Berechtigung für einen Vertreter	113
304	5.4.6.4 Berechtigung für eine Leistungserbringerinstitution	113
305	5.4.6.5 Berechtigung für einen Kostenträger	113
306	5.4.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4	113
307	5.5 Vertrauenswürdige Ausführung	115
308	5.5.1 Schnittstelle I Document Management Connect	115
309	5.5.1.1 Operation I Document Management Connect::OpenContext	120
310	5.5.1.1.1 Umsetzung	121
311	5.5.1.2 Operation I Document Management Connect::CloseContext	122
312	5.5.1.2.1 Umsetzung	123
313	5.5.2 Hardware-Merkmale	124
314	5.6 Statische Akteninhalte	124
315	6 Informationsmodelle	126
316	7 Anhang A – Verzeichnisse	127
317	7.1 Abkürzungen	127
318	7.2 Glossar	129
319	7.3 Abbildungsverzeichnis	129
320	7.4 Tabellenverzeichnis	129
321	7.5 Referenzierte Dokumente	132
322	7.5.1 Dokumente der gematik	132
323	7.5.2 Weitere Dokumente	133
324	8 Anhang B – XACML 2.0-Profile für Policy Documents (für	
325	Upgrade von ePA 3.1.3)	137
326	8.1 Policy Document für einen Versicherten	137
327	8.1.1 Base Policy	137
328	8.1.2 Permission Policy	140
329	8.2 Policy Document für einen Vertreter	171
330	8.2.1 Base Policy	171
331	8.2.2 Permission Policy	175
332	8.3 Policy Document für eine Leistungserbringerinstitution	203
333	8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente	203
334	8.3.2 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente	208

8.3.3	Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente	234
8.4	Policy Document für einen Kostenträger	258
8.4.1	Base Policy	258
8.4.2	Permission Policy	261
9	Anhang C– XACML 2.0-Profile für Policy Documents	265
9.1	Policy Document für einen Versicherten	265
9.2	Policy Document für einen Vertreter	268
9.3	Policy Document für eine Leistungserbringerinstitution	271
9.4	Policy Document für einen Kostenträger	300
9.5	Statische Permission Policies	306
9.5.1	Grobgranulare Berechtigung: Stufe Normal	306
9.5.2	Grobgranulare Berechtigung: Stufe Erweitert	307
9.5.3	Mittelgranulare Berechtigung: Kategorie "care"	308
9.5.4	Mittelgranulare Berechtigung: Kategorie "childsrecord"	308
9.5.5	Mittelgranulare Berechtigung: Kategorie "dentalrecord"	309
9.5.6	Mittelgranulare Berechtigung: Kategorie "eab"	309
9.5.7	Mittelgranulare Berechtigung: Kategorie "eau"	310
9.5.8	Mittelgranulare Berechtigung: Kategorie "ega"	311
9.5.9	Mittelgranulare Berechtigung: Kategorie "emp"	311
9.5.10	Mittelgranulare Berechtigung: Kategorie "mothersrecord"	312
9.5.11	Mittelgranulare Berechtigung: Kategorie "nfd"	312
9.5.12	Mittelgranulare Berechtigung: Kategorie "other"	313
9.5.13	Mittelgranulare Berechtigung: Kategorie "patientdoc"	315
9.5.14	Mittelgranulare Berechtigung: Kategorie "prescription"	315
9.5.15	Mittelgranulare Berechtigung: Kategorie "receipt"	316
9.5.16	Mittelgranulare Berechtigung: Kategorie "vaccination"	317
9.5.17	Mittelgranulare Berechtigung: Kategorie "practitioner"	317
9.5.18	Mittelgranulare Berechtigung: Kategorie "hospital"	318
9.5.19	Mittelgranulare Berechtigung: Kategorie "laboratory"	319
9.5.20	Mittelgranulare Berechtigung: Kategorie "physiotherapy"	320
9.5.21	Mittelgranulare Berechtigung: Kategorie "psychotherapy"	320
9.5.22	Mittelgranulare Berechtigung: Kategorie "dermatology"	321
9.5.23	Mittelgranulare Berechtigung: Kategorie "gynaecology urology"	322
9.5.24	Mittelgranulare Berechtigung: Kategorie "dentistry oms"	322
9.5.25	Mittelgranulare Berechtigung: Kategorie "other medical"	323
9.5.26	Mittelgranulare Berechtigung: Kategorie "other non medical"	324

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.

407 **1.5 Methodik**

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

412
413 **<AFO-ID> - <Titel der Afo>**
414 Text / Beschreibung
415 [\leq]

416 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [\leq]
417 angeführten Inhalte.

418

419

2 Systemkontext

420 Die Komponente ePA-Dokumentenverwaltung des Produkttyps ePA-Aktensystem
421 [gemSpec_Aktensystem] dient dem sicheren Speichern und Auffinden von Dokumenten
422 des Versicherten aus seiner persönlichen Akte durch berechnigte Nutzer. Diese sind der
423 Versicherte selbst oder von ihm benannte Vertreter
424 sowie Leistungserbringerinstitutionen.

425 Zur Umsetzung der ePA-Dokumentenverwaltung wird auf das Repository Registry-
426 Designmuster zurück gegriffen. Eine Document Registry verwaltet Metadaten, welche für
427 die Suche und Navigation von Dokumenten notwendig sind. Die Dokumente werden
428 verschlüsselt in einem Document Repository gespeichert. Die Schnittstellen der
429 Komponente ePA-Dokumentenverwaltung basieren auf den Spezifikationen von
430 Integrating the Healthcare Enterprise (IHE), insbesondere dem Konzept Cross-Enterprise
431 Document Sharing (XDS) zum Speichern und Abrufen von (medizinischen) Dokumenten,
432 welches Teil des IHE ITI Technical Frameworks (IHE ITI TF) ist. IHE ist eine
433 internationale Organisation, welche bestehende Industriestandards für die Umsetzung
434 spezifischer Anwendungsszenarien im digitalisierten Gesundheitswesen profiliert.

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

3 Zerlegung der Komponente

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

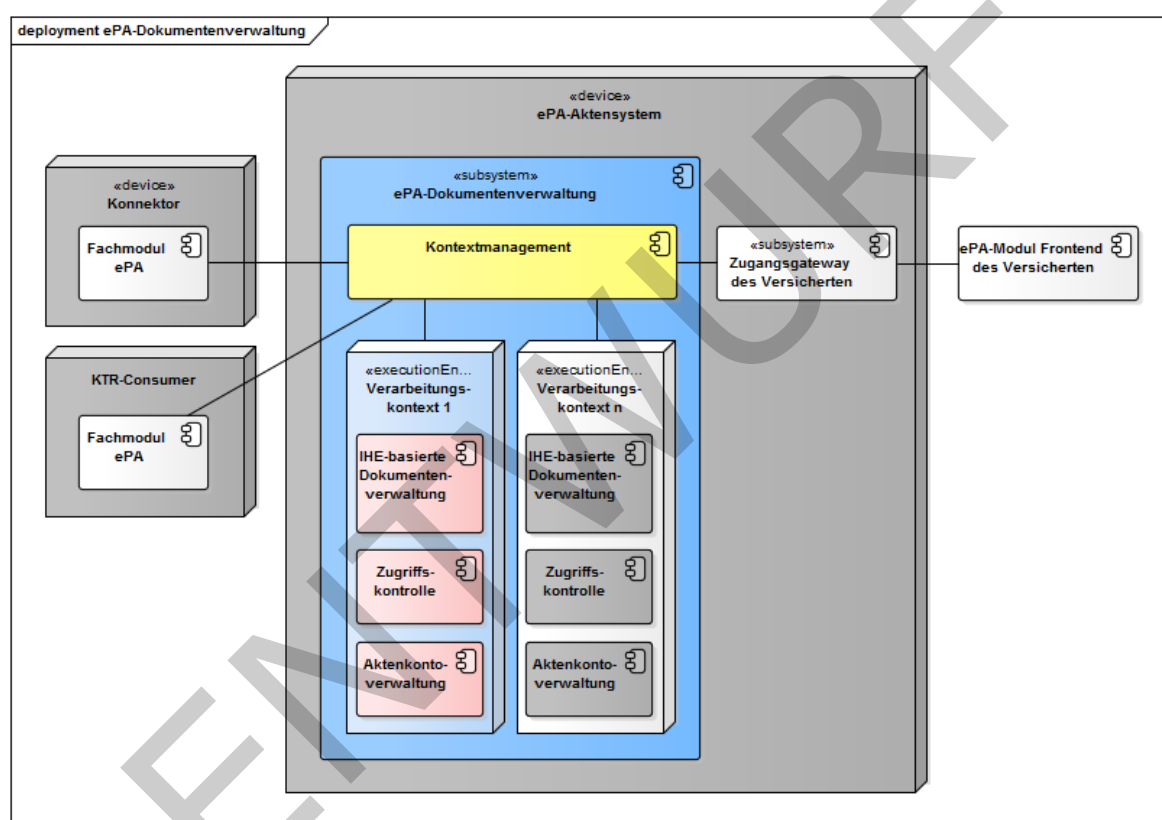


Abbildung 1: Komponentenzersetzung ePA-Dokumentenverwaltung

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 - 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#5.2] 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.[<=]

A_14788 - Komponente ePA-Dokumentenverwaltung – APPC Content Consumer mit "Structured Policy Processing Option"-Option

Die Komponente ePA-Dokumentenverwaltung als APPC-Akteur "Content Consumer" MUSS die Option "Structured Policy Processing Option" unterstützen. [\leq]

4.2.1.2 RMU Update Responder

4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_15093 - Komponente ePA-Dokumentenverwaltung – Gruppierung RMU Update Responder mit XCA Responding Gateway und X-Service Provider

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

A_17571 - Komponente ePA-Dokumentenverwaltung – Gruppierung RMU Update Responder mit APPC Content Consumer

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

4.2.1.2.2 Optionen des IHE ITI-Akteurs

A_15094 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "Forward Update"-Option

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF NICHT die Option "Forward Update" unterstützen.
[\leq]

A_15095 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder mit "XCA Persistence"-Option

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS die Option "XCA Persistence" unterstützen.
[\leq]

A_15096 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "XDS Persistence"-Option

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF NICHT die Option "XDS Persistence" unterstützen.
[\leq]

A_15097 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "XDS Version Persistence"-Option

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF NICHT die Option "XDS Version Persistence" unterstützen.
[\leq]

[Durch Verwendung der XCA Persistence Option und der Gruppierung des XCA Responding Gateways mit der XDS Registry wird von der XDS Registry erwartet, die aktualisierten 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]

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

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

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

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

4.2.1.4.2 Optionen des IHE ITI-Akteurs

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

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

4.2.1.5 XDS Document Registry

4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren

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

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

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

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

4.2.1.5.2 Optionen des IHE ITI-Akteurs

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

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

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

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

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

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

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_14915-02A~~~~14915-01~~ - 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~~~~RemoveMetadata~~
- I_Document_Management::CrossGatewayRetrieve
- 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::~~RemoveDocuments~~~~RemoveMetadata~~
- I_Document_Management_Insurant::RetrieveDocumentSet

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

A_14594 - Komponente ePA-Dokumentenverwaltung – Validierung der Authentication Assertion

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

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

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

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 Registry-Datenobjekt registriert und ein Dokument gespeichert wird.

[\leq]

A_15162-02A_15162-01 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung bei Angabe von Document Entry Relationships in Metadaten

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 die Metadaten die folgenden Association Types nach [IHE-ITI-TF3#4.2.2] enthalten:

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

[\leq]

A_14937 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße prüfen

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

[\leq]

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~~Metadata [ITI-8662]

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

~~A_14926 – Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen der Metadaten bei Löschung von Dokumenten~~Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document RepositoryRegistry" MUSS ~~die mit den~~bei zu löschenden ~~Dokumenten~~ DocumentEntry-Einträgen im selben Zuge auch die assoziierten ~~Metadaten in der Dokumente im~~ "Document RegistryRepository" 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, bevor die Dokumente gelöscht werden können. [`<=`und das assoziierte Submission Set löschen, sofern kein weiteres Dokument mit diesem Submission Set assoziiert ist. [`<=`]

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

~~A_14670-01 – 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 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 `XSDSDocumentUniqueIdError`-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 `XSDSDocumentUniqueIdError` zurückgegeben werden. [`<=`]

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] dos 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.[<=]

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.[<=]

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

[<=]

4.4 Vertrauenswürdige Ausführungsumgebung

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

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

Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der Operationen der Schnittstellen `I_Document_Management_Connect`, `I_Document_Management`, `I_Document_Management_Insurance` sowie `I_Document_Management_Insurant` im Verarbeitungskontext einer Vertrauenswürdigen Ausführungsumgebung (VAU) umsetzen.[<=]

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

Das Kontextmanagement MUSS mit ~~einer VAU-Server-Error-Nachricht~~ und einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") antworten, wenn für eine Web-Service-Operation der Schnittstellen `I_Document_Management`, `I_Document_Management_Insurant`, `I_Document_Management_Insurance` sowie `I_Account_Management_Insurant` für den angemeldeten Nutzer kein Verarbeitungskontext geöffnet wurde.
[<=]

4.4.1 Verarbeitungskontext

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

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

Der Verarbeitungskontext grenzt sich von allen weiteren, im betrieblichen Kontext bei einem Anbieter ePA-Aktensystem vorhandenen Systemen und Prozessen dadurch ab, dass die sensiblen Klartextdaten von Komponenten innerhalb des Verarbeitungskontextes aus erreichbar sind oder sein können, während sie dies von außerhalb des Verarbeitungskontextes nicht sind. Sensible Daten verlassen den Verarbeitungskontext ausschließlich gemäß wohldefinierten (Zugriffs-)Regeln und in verschlüsselter Form.

A_14557 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext der VAU

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

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

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

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

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

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

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

Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS für die Verschlüsselung aller Dokumentmetadaten, Policy Documents und des § 291a-Protokolls

976 des Versicherten sowie eigener technischer Daten den Kontextschlüssel des Aktenkontos
977 verwenden.[<=]

978 **A_14566 - Komponente ePA-Dokumentenverwaltung – Isolation zwischen**
979 **Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU**

980 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die in ihr ablaufenden
981 Verarbeitungen für die Daten eines Verarbeitungskontextes von den Verarbeitungen für
982 die Daten anderer Verarbeitungskontexte in solcher Weise trennen, dass mit technischen
983 Mitteln ausgeschlossen wird, dass die Verarbeitungen eines Verarbeitungskontextes
984 schadhaft auf die Verarbeitungen eines anderen Verarbeitungskontextes einwirken
985 können.[<=]

986 **4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem**
987 **Betriebsumfeld**

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

991 **A_14558 - Komponente ePA-Dokumentenverwaltung – Isolation der VAU von**
992 **Datenverarbeitungsprozessen des Anbieters**

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

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

1000 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS eine Manipulation der
1001 eingesetzten Software erkennen und eine Ausführung der manipulierten Software
1002 verhindern.[<=]

1003 **A_14560 - Komponente ePA-Dokumentenverwaltung – Ausschluss von**
1004 **Manipulationen an der Hardware der VAU**

1005 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die Integrität der
1006 eingesetzten Hardware schützen und damit insbesondere Manipulationen an der
1007 Hardware durch den Anbieter ePA-Aktensystem ausschließen.[<=]

1008 **A_14561 - Komponente ePA-Dokumentenverwaltung – Kontinuierliche**
1009 **Wirksamkeit des Manipulationsschutzes der VAU**

1010 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS den Ausschluss von
1011 Manipulationen an der Hardware und der Software durch den Anbieter ePA-Aktensystem
1012 mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet
1013 werden kann.[<=]

1014 **A_14562 - Komponente ePA-Dokumentenverwaltung – Kein physischer Zugang**
1015 **des Anbieters zu Systemen der VAU**

1016 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln
1017 sicherstellen, dass niemand, auch nicht der Anbieter ePA-Aktensystem, während der
1018 Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische
1019 Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.[<=]

1020 **A_14563 - Komponente ePA-Dokumentenverwaltung – Nutzdatenbereinigung**
1021 **vor physischem Zugang zu Systemen der VAU**

1022 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln
1023 sicherstellen, dass physischer Zugang zu Hardware-Komponenten der

1024 Verarbeitungskontexte nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen
1025 keine Nutzdaten extrahiert werden können.[<=]

1026 **A_14564 - Komponente ePA-Dokumentenverwaltung – Private Schlüssel von**
1027 **Dienstzertifikaten im HSM**

1028 Die Komponente ePA-Dokumentenverwaltung MUSS die folgenden privaten Schlüssel in
1029 einem Hardware Security Module (HSM) erzeugen und anwenden:

- 1030 • TI-Fachdienst-Identität zur Authentisierung des Kontextmanagements gegenüber
1031 dem Fachmodul ePA (TLS)
- 1032 • TI-Fachdienst-Identität zur Authentisierung des Verarbeitungskontextes
1033 gegenüber dem Fachmodul ePA (sicherer Kanal auf Anwendungsebene),
- 1034 • Privater Schlüssel des Schlüsselpaars zur Authentisierung des
1035 Verarbeitungskontextes gegenüber dem ePA-Frontend des Versicherten (sicherer
1036 Kanal auf Anwendungsebene).

1037 Die Prüftiefe des HSM MUSS dabei den in [gemSpec_Aktensystem#A_15156]
1038 angegebenen Standards entsprechen.
1039 [<=]

1040 **A_14565 - Komponente ePA-Dokumentenverwaltung – HSM-**
1041 **Kryptographieschnittstelle verfügbar nur für Instanzen der VAU**

1042 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln, die
1043 auch Manipulationen durch den Anbieter ePA-Aktensystem ausschließen, gewährleisten,
1044 dass nur Instanzen der VAU Zugriff auf die Kryptographieschnittstelle des HSM zur
1045 Nutzung des privaten Schlüsselmaterials für ihre Dienstzertifikate erhalten können.[<=]

1046 **A_14567 - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal vom**
1047 **Client zum Verarbeitungskontext der VAU**

1048 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS den Aufbau eines
1049 vertraulichen und integritätsgeschützten Kommunikationskanals gemäß
1050 [gemSpec_Krypt#3.15] zwischen einem Client und einem Verarbeitungskontext
1051 erzwingen, bevor der Verarbeitungskontext durch Übergabe des Kontextschlüssels durch
1052 den Client aktiviert werden kann.[<=]

1053 **4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes**

1054 Die Vertrauenswürdige Ausführungsumgebung realisiert ein zweistufiges Verfahren zum
1055 Schutz vor unberechtigten Zugriffen auf die verarbeiteten schützenswerten
1056 Klartextdaten. Neben den Verfahren zur Authentisierung und Autorisierung der Nutzer
1057 durch Dienste des Anbieters auf der Basis ihrer Nutzeridentitäten, muss der Nutzer über
1058 einen aktenspezifischen kryptographischen Kontextschlüssel verfügen. Erst nachdem der
1059 Nutzer den Kontextschlüssel sicher an den Verarbeitungskontext übermittelt hat, ist der
1060 Verarbeitungskontext in der Lage, die schützenswerten Daten zu entschlüsseln und zu
1061 verarbeiten.

1062 **A_14568 - Komponente ePA-Dokumentenverwaltung – Aktivierung des**
1063 **Verarbeitungskontextes der VAU**

1064 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln
1065 gewährleisten, dass schützenswerte Nutzdaten im Verarbeitungskontext erst nach
1066 Aktivierung – mittels Übergabe des korrekten *Kontextschlüssels* an den
1067 Verarbeitungskontext durch den Client eines berechtigten Nutzers – entschlüsselt und
1068 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.[<=]

4.4.4 Parallele Zugriffe

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

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

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS parallele Zugriffe auf einen Verarbeitungskontext ermöglichen und dabei die transaktionale Integrität der gespeicherten Daten gewährleisten.[<=]

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

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass parallele Zugriffe auf ein Aktenkonto immer in derselben Instanz der VAU verarbeitet werden. [<=]

4.4.5 Konsistenz der Akte, Logging und Monitoring**A_14573 - Komponente ePA-Dokumentenverwaltung – Konsistenter Systemzustand des Verarbeitungskontextes der VAU**

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

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

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

4.4.6 Client-Verbindungen zum Verarbeitungskontext

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

A_14616 - Komponente ePA-Dokumentenverwaltung – Kontextmanagement der Vertrauenswürdigen Ausführungsumgebung

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS ein Kontextmanagement bereitstellen, das Verarbeitungskontexte bedarfsgesteuert initialisiert und terminiert, über initialisierte Verarbeitungskontexte auf der Basis ihrer RecordIdentifier Buch führt und Verbindung zwischen Clients und den jeweils benötigten 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 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom ePA-Modul Frontend des Versicherten zum Verarbeitungskontextes der VAU über das Zugangsgateway

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS Verbindungen vom ePA-Modul 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.

[<=]

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

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS dem ePA-Modul 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. [<=]

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. [<=]

A_15646 - 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-Modul Frontend des Versicherten mittels der Fachdienstidentität `oid_epa_vau` mit Zertifikatsprofil `C.FD.AUT` ausweisen.

[<=]

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

4.5 Anforderungen zur sicherheitstechnischen Validierung

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

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

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

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

A_14465-01A ~~A_14465~~ - Komponente ePA-Dokumentenverwaltung – XML Schema-Validierung für SOAP-Eingangsnachrichten

Die Komponente ePA-Dokumentenverwaltung MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-Eingangsnachrichten einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen und gemäß

[SOAP] verarbeiten. Sind Nachrichten nicht wohlgeformt oder ~~gültig~~^{ungültig}, MUSS die Komponente ePA-Dokumentenverwaltung die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren. [\leq]

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

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

~~A_13690-02A_13690-01~~ - Komponente ePA-Dokumentenverwaltung – SAML 2.0 Assertion-Validierung

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

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

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

Die Telematik-ID im Signaturzertifikat muss identisch mit der Telematik-ID in der Identitätsbestätigung sein. [\leq]

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

A_18990 - ePA-Dokumentenverwaltung – Beschränkung gültiger Identitätsbestätigungen

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

A_17386-01 - Komponente ePA-Dokumentenverwaltung – Authentication Assertion-Validierung

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

A_17387 - Komponente ePA-Dokumentenverwaltung – Authorization Assertion-Validierung

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

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

Weitere Hinweise zur Validierung von SAML 2.0 Assertions können [OWASP-SAML] 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 - Komponente ePA-Dokumentenverwaltung – Ablehnung von SOAP 1.2-Nachrichten ohne UTF-8 Kodierung

Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Nachrichten mit einem HTTP-Statuscode 406 gemäß [RFC7231] quittieren, sofern die Zeichenkodierung im HTTP Header nicht UTF-8 benennt (`Content-Type: charset=utf-8`).[<=]

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 14813-02A_14813-01 - 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::RemoveDocumentsRemoveMetadata`
- `I_Document_Management::CrossGatewayRetrieve`
- `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::RemoveDocumentsRemoveMetadata`
- `I_Document_Management_Insurant::RetrieveDocumentSet`
- `I_Account_Management_Insurant::GetAuditEvents`
- `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. [\leq]




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.](#) [\leq]

A 20538A_14816-05 - Komponente ePA-Dokumentenverwaltung – Parameter des § 291a-Protokolls

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

1323 Tabelle 5: Tab_Dokv_13 - Parameter des § 291a-Protokolls

Protokoll - parameter	Parameterwerte gemäß aufgerufener Operation
User-ID	<p>Bei Aufrufen einer Operation der Schnittstellen</p> <ul style="list-style-type: none"> <i>I_Document_Management</i>  <i>I_Document_Management_Insurance</i>  <i>I_Account_Management_Insurant</i> sowie <i>I_Document_Management_Insurant</i>: <p>XPath-Ausdruck zur " Subject ID" der im Operationsaufruf übergebenen Authentication Assertion:</p> <pre>//*[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>
User Name	<p>Bei Aufrufen einer Operation der Schnittstellen</p> <ul style="list-style-type: none"> <i>I_Account_Management_Insurant</i> <i>I_Document_Management</i>: <p>XPath-Ausdruck zur "XSPA Organization" der im Operationsaufruf übergebenen Authentication Assertion:</p> <pre>//*[local-name()='Attribute' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion'][@Name='urn:oasis:names:tc:xacml:1.0:subject:organization']/*[local-name()='AttributeValue']/text() [normalize-space()]</pre> <p><u>Bei Aufrufen einer Operation der Schnittstellen:</u></p> <ul style="list-style-type: none">  <i>I_Document_Management_Insurance</i> und <u>sowie</u> <i>I_Document_Management_Insurant</i>: <p>XPath-Ausdruck zum SAML Subject der im Operationsaufruf übergebenen Authentication Assertion:</p> <pre>//*[local-name()='Assertion' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion']/*[local-name()='Subject']/*[local-name()='NameID']/text() [normalize-space()]</pre>

Object-ID	<p>Der unveränderbare Anteil der KVN der <code>extension</code>-Attributs aus dem <code>InsurantId</code>-Element des <code>RecordIdentifier</code>-Elements oder die <code>DocumentEntry.patientId</code> des entsprechenden Operationsaufrufs</p> <p><i>Hinweis: Bei Aufruf von Operationen ohne diesen Parameter wird der Wert im Protokolleintrag nicht belegt.</i></p> <p>Bei Zugriffen auf Dokumente über die Transaktionen <code>CrossGatewayDocumentProvide</code>, <code>ProvideAndRegisterDocumentSet-b</code>, <code>CrossGatewayRetrieve</code>, <code>RetrieveDocumentSet</code>, <code>RemoveDocuments</code>, <code>RestrictedUpdateDocumentSet</code> MUSS die <code>Document Unique ID</code> im Element <code>ParticipantObjectDetail</code> hinterlegt werden. Als Attribut <code>type</code> MUSS der Wert <code>DocumentUniqueId</code> und als Attribut <code>value</code> der Wert der <code>Document Unique ID</code> verwendet werden.</p>								
Object NameDetail	<p>Bei Zugriffen auf Dokumente Zugriff über die Transaktionen:</p> <ul style="list-style-type: none"> • <code>CrossGatewayDocumentProvide</code> • <code>ProvideAndRegisterDocumentSet-b</code> • <code>CrossGatewayRetrieve</code> • <code>RetrieveDocumentSet</code>, <code>RemoveDocuments</code>, • <code>RemoveMetadata</code> • <code>RestrictedUpdateDocumentSet</code> <p>MUSS der <code>Document Title</code> im Element <code>ParticipantObjectDetail</code> hinterlegt werden. Als Attribut beim Zugriff auf Dokumente mit folgenden Wertepaaren (type MUSS der Wert <code>DocumentTitle</code> und als Attribut <code>value</code> der Wert der <code>Document Title</code> verwendet) belegt werden:</p> <table border="1"> <thead> <tr> <th><u>type</u></th><th><u>value</u></th></tr> </thead> <tbody> <tr> <td><u>DocumentUniqueId</u></td><td>Wert von <code>DocumentEntry.uniqueId</code></td></tr> <tr> <td><u>DocumentTitle</u></td><td>Wert von <code>DocumentEntry.title</code></td></tr> <tr> <td><u>DocumentPracticeSetting</u></td><td>Wert von <code>DocumentEntry.practiceSettingCode</code>, 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.</td></tr> </tbody> </table>	<u>type</u>	<u>value</u>	<u>DocumentUniqueId</u>	Wert von <code>DocumentEntry.uniqueId</code>	<u>DocumentTitle</u>	Wert von <code>DocumentEntry.title</code>	<u>DocumentPracticeSetting</u>	Wert von <code>DocumentEntry.practiceSettingCode</code> , 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.
<u>type</u>	<u>value</u>								
<u>DocumentUniqueId</u>	Wert von <code>DocumentEntry.uniqueId</code>								
<u>DocumentTitle</u>	Wert von <code>DocumentEntry.title</code>								
<u>DocumentPracticeSetting</u>	Wert von <code>DocumentEntry.practiceSettingCode</code> , 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.								

DocumentFormat	<p>Der Parameter DeviceID wird im Protokolleintrag nicht belegt. Wert von <code>DocumentEntry.formatCode</code>, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3].., siehe oben.</p> <p>Wenn es sich beim Wert von <code>DocumentEntry.formatCode</code> um den Code <code>urn:ihe:iti:xds:2017:mimeTypeSufficient</code> (Code System 1.3.6.1.4.1.19376.1.2.3) handelt, MUSS stattdessen der Wert von <code>DocumentEntry.mimeType</code> 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 <code>DocumentEntry.mimeType</code> interpretieren.</p>
DocumentConfidentialityCode	<p>Wert von <code>DocumentEntry.confidentialityCode</code>, 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>
<u>FolderCodeList</u>	Wert von <code>Folder.codeList</code> , kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3].., siehe oben. Wird mehr als ein Code dokumentiert, MUSS als Trennzeichen das Tildezeichen („~“) verwendet werden.
<u>FolderUniqueId</u>	Wert von <code>Folder.uniqueId</code>
<u>FolderTitle</u>	Wert von <code>Folder.title</code>
<u>FolderLastUpdateTime</u>	Wert von <code>Folder.lastUpdateTime</code>

[<=]

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"

~~A 14814 – Komponente ePA-Dokumentenverwaltung – Schutz vor Manipulation der Protokolldaten~~ Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die § 291a-Protokolldaten gegen Veränderung und unberechtigtes 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 Protokollierung der Operation verwendet wurden, welche die Löschung des Ordners ausgelöst haben. [\leq]

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

4.6.1 Protokollierung von Berechtigungen

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

A 20564 - Komponente ePA-Dokumentenverwaltung – Protokollierung neuer Berechtigungen

Die Komponente ePA-Dokumentenverwaltung MUSS für bei Zugriffen auf APPC-Policy-Dokumente (gemäß emSpec DM ePA#A 14961) über die Transaktionen

- CrossGatewayDocumentProvide
- ProvideAndRegisterDocumentSet-b

das Protokoll gemäß A 20538 um die folgenden Details ergänzen, sofern noch keine Berechtigung für den von der Policy betroffenen Berechtigten existiert:

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

PermAuthorize dName	Wert des Attributs /PolicySet/PolicySet[1]/Target/Subjects/Subject[2] /SubjectMatch/AttributeValue[@text] aus der eingestellten Policy (bei LEI und Kostenträgern der Organisationsname, bei Vertretern der X.509 Subject Name der eGK).
PermAccessLevel	Gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.
PermCategories	Gewährte mittelgranulare Rechte: kommasseparierte Liste von Kategorien (Technischer Identifier gemäß A 19303-01)
PermWhitelist	Explizit freigegebene Dokumente (feingranulare Berechtigung): kommasseparierte Liste der uniqueIDs der freigegebenen Dokumente
PermBlacklist	Explizit gesperrte Dokumente (feingranulare Berechtigung): kommasseparierte Liste der uniqueIDs der gesperrten Dokumente.

[<=]

A 20565 - Komponente ePA-Dokumentenverwaltung – Protokollierung aktualisierter Berechtigungen

Die Komponente ePA-Dokumentenverwaltung MUSS beim Einstellen von APPC-Policy-Dokumenten (gemäß emSpec DM ePA#A 14961) über die Transaktionen

- [CrossGatewayDocumentProvide](#)
- [ProvideAndRegisterDocumentSet](#)

das Protokoll gemäß A 20538 um die folgenden Details ergänzen, sofern bereits eine Berechtigung für den betroffenen Berechtigten existiert, die durch die neue Berechtigung aktualisiert wird:

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

		<u>Kostenträgern die Betriebsnummer, bei Vertretern die KVNR).</u>
	<u>PermAuthorizedName</u>	<u>Wert des Attributs</u> <u>/PolicySet/PolicySet[1]/Target/Subjects/Subject[2]</u> <u>/SubjectMatch/AttributeValue[@text]</u> <u>aus der eingestellten Policy (bei LEI und Kostenträgern der Organisationsname, bei Vertretern der X.509 Subject Name der eGK).</u>
	<u>PermAccessLevelNew</u>	<u>Neu gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.</u>
	<u>PermAccessLevelOld</u>	<u>Ursprünglich gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.</u>
	<u>PermCategoriesNew</u>	<u>Neu (zusätzlich) gewährte mittelgranulare Rechte: kommasseparierte Liste von Kategorien (Technischer Identifier) gemäß A 19388.</u>
	<u>PermCategoriesRemoved</u>	<u>Ursprünglich gewährte mittelgranulare Rechte, die durch die neue Policy nicht mehr gewährt werden: kommasseparierte Liste von Kategorien (Technischer Identifier) gemäß A 19388.</u>
	<u>PermCategories</u>	<u>Gewährte mittelgranulare Rechte gemäß aktualisierter Policy: kommasseparierte Liste von Kategorien (Technischer Identifier) gemäß A 19388.</u>
	<u>PermWhiteListNew</u>	<u>Neue (zusätzlich) explizit freigegebene Dokumente (feingranulare Berechtigung): kommasseparierte Liste der uniqueIDs der freigegebenen Dokumente.</u>
	<u>PermWhiteListRemoved</u>	<u>Ursprünglich explizit freigegebene Dokumente (feingranulare Berechtigung), die durch die neue Policy nicht mehr explizit freigegeben sind: kommasseparierte Liste der uniqueIDs der freigegebenen Dokumente.</u>
	<u>PermWhitelist</u>	<u>Explizit freigegebene Dokumente (feingranulare Berechtigung) gemäß aktualisierter Berechtigung: kommasseparierte Liste der uniqueIDs der freigegebenen Dokumente.</u>
	<u>PermBlacklistNew</u>	<u>Neue (zusätzlich) explizit gesperrte Dokumente (feingranulare Berechtigung): kommasseparierte Liste der uniqueIDs der gesperrten Dokumente.</u>

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.

[<=]

A 20566 - Komponente ePA-Dokumentenverwaltung – Protokollierung gelöschter Berechtigungen

Die Komponente ePA-Dokumentenverwaltung MUSS beim Löschen von APPC-Policy-Dokumenten (gemäß emSpec DM ePA#A 14961) über die Transaktionen

- [I Document Management Insurant::RemoveMetadata](#)

das Protokoll gemäß A 20538 um die folgenden Details ergänzen:

<u>Protokollparameter</u>	<u>Parameterwerte beim Löschen von Policy-Dokumenten</u>	
Object Detail	<u>type</u>	<u>value</u>
	PermAuthorizedID	Wert des Attributs /PolicySet/PolicySet[1]/Target/Subjects/Subject[1] /SubjectMatch/AttributeValue/InstanceIdentifier[@extension] aus der eingestellten Policy (bei LEI die Telematik ID, bei Kostenträgern die Betriebsnummer, bei Vertretern die KVN).
	PermAuthorizedName	Wert des Attributs /PolicySet/PolicySet[1]/Target/Subjects/Subject[2] /SubjectMatch/AttributeValue[@text] aus der eingestellten Policy (bei LEI und Kostenträgern der Organisationsname, bei Vertretern der X.509 Subject Name der eGK).
	PermAccessLevelOld	Ursprünglich gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.

	PermCategoriesRemoved	Ursprünglich gewährte mittelgranulare Rechte: kommasseparierte Liste von Kategorien (Technischer Identifier gemäß A 19303-01)
	PermWhiteListRemoved	Ursprünglich explizit freigegebene Dokumente (feingranulare Berechtigung): kommasseparierte Liste der uniqueIDs der freigegebenen Dokumente
	PermBlackListRemoved	Ursprünglich explizit gesperrte Dokumente (feingranulare Berechtigung): kommasseparierte Liste der uniqueIDs der gesperrten Dokumente.

geschützt sind: [<=]

1387

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 - 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

	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 	

1406 [\leq]1407 **5.1.1.1 Operation**1408 **I_Document_Management::CrossGatewayDocumentProvide**1409 **A_14153 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-Gateway Document Provide**

1411 Die Komponente ePA-Dokumentenverwaltung MUSS

1412 die Operation I_Document_Management::CrossGatewayDocumentProvide gemäß der
1413 folgenden Signatur implementieren:1414 **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 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 der übermittelten Dokumente übersteigt 25 MByte.	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

1415 [\leq]

1416 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1417 Transaktionen "Cross-Gateway Document Provide" [ITI-80] und "Provide X-User
1418 Assertion" [ITI-40] sind [IHE-ITI-XCDR], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-
1419 TF2x] zu entnehmen.

1420 **5.1.1.1.1 Umsetzung**
1421 **A_15055 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung von**
1422 **gemischten Dokumentenpaketen mit Policy Documents**

1423 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1424 MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und
1425 mit einem XDSRepositoryMetadataError-Fehlercode quittieren, sofern in der
1426 Eingangsnachricht mehr als ein Dokument und Dokumenten-Metadaten gemäß der

1427 Anforderung [gemSpec_DM_ePA#A_14961] für Policy Documents (Advanced Patient
1428 Privacy Consents) enthalten sind.

1429 [\leq]

1430 **A_14941-03A_14941-02 - Komponente ePA-Dokumentenverwaltung – Keine**
1431 **Registrierung bei Angabe von Document Entry Relationships in Metadaten**

1432 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1433 MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und
1434 mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern die Metadaten die
1435 folgenden Association Types nach [IHE-ITI-TF3#4.2.2] enthalten:

- 1436 • `urn:ihe:iti:2007:AssociationType:XFRM` (Transform)
- 1437 • `urn:ihe:iti:2007:AssociationType:XFRM_RPLC` (Replace with Transformation)
- 1438 • `urn:ihe:iti:2007:AssociationType:signs` (Digital Signature)
- 1439 • `urn:ihe:iti:2010:AssociationType:IsSnapshotOf` (Snapshot of On-Demand
1440 document entry)
- 1441 • [`urn:ihe:iti:2010:AssociationType:APND` \(Addendum\)](#)

1442 [\leq]

1443 **A_13838 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße**
1444 **prüfen**

1445 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1446 MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das SubmissionSet
1447 verarbeitet wird. Die Verarbeitung MUSS abgelehnt werden und mit einem mit
1448 einem `MaxDocSizeExceeded`-bzw. `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-
1449 TF3#4.2.4] quittieren, wenn die Gesamtgröße aller übermittelten Dokumente 250 MByte
1450 übersteigt oder die Größe mindestens eines einzelnen übermittelten Dokuments 25
1451 MByte übersteigt.

1452 [\leq]

1453 Das bedeutet, dass Dokumente bis zu einer Größe von 25 MB = $25 * (1024)^2$ Byte in
1454 die ePA hochgeladen werden. Grundlage für die Berechnung der Dokumentengröße ist
1455 das Dokument ohne Verschlüsselung durch den Dokumentenschlüssel und ohne
1456 Transportcodierung. Größere Dokumente können nicht hochgeladen werden.

1457 **A_13798 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung**
1458 **der Metadaten aus ITI Document Sharing-Profilen durch XCDR-Akteur**
1459 **"Responding Gateway"**

1460 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1461 MUSS die SubmissionSet- sowie die DocumentEntry-Metadaten der eingehenden
1462 Nachricht vor einer Zugriffskontrolle gemäß der Konformität zu den Nutzungsvorgaben in
1463 [gemSpec_DM_ePA#A_14760] prüfen. Die Komponente ePA-Dokumentenverwaltung
1464 als XCDR-Akteur "Responding Gateway" MUSS das Registrieren und Speichern von
1465 Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`-
1466 Fehlercode quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben
1467 sind. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-
1468 Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben
1469 entspricht. [\leq]

1470 **A_13715 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-**
1471 **Gateway Document Provide**

1472 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1473 MUSS die Umsetzung der
1474 Operation `I_Document_Management::CrossGatewayDocumentProvide` bzw. die

1475 Verarbeitung des übermittelten Submission Sets gemäß den definierten Ablauflogiken
 1476 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
 1477 3.80.4.2.3] implementieren.[<=]

1478 **A_13657 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
 1479 **Cross-Gateway Document Provide**

1480 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
 1481 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
 1482 Policy Documents (Advanced Patient Privacy Consents) entsprechend der
 1483 Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt registriert und ein
 1484 Dokument gespeichert wird.[<=]

1485 **5.1.1.2 Operation I_Document_Management::CrossGatewayQuery**

1486 **A_14450 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-**
 1487 **Gateway Query**

1488 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 1489 I_Document_Management::CrossGatewayQuery gemäß der folgenden Signatur
 1490 implementieren:

1491 **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 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	

1492
1493

[<=]

1494 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1495 Transaktionen "Cross-Gateway Document Query" [ITI-38] und "Provide X-User Assertion"
1496 [ITI-40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1497 entnehmen.

1498 5.1.1.2.1 Umsetzung

1499 **A_14924 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe von** 1500 **Metadaten zu Policy Documents (Advanced Patient Privacy Consents)**

1501 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
1502 DARF Metadaten zu Policy Documents (Advanced Patient Privacy Consents) gemäß der
1503 Anforderung [gemSpec_DM_ePA#A_14961] NICHT zurückgeben bzw. MUSS diese aus
1504 der Antwortnachricht entfernen, falls diese den Anfragekriterien entsprechen.
1505

[<=]

1506 Die folgende XACML 2.0 Policy repräsentiert die o.g. Anforderung technisch:

```

1507 <?xml version="1.0" encoding="UTF-8"?>
1508 <Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
1509   PolicyId="urn:uuid:6e84f679-5f36-4861-bfb5-607aef021fff"
1510   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
1511 algorithm:deny-overrides">
1512   <Target>
1513     <Resources>
1514       <Resource>
1515         <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
1516           <AttributeValue DataType="urn:hl7-org:v3#CV">
1517             <CodedValue xmlns="urn:hl7-org:v3" code="57016-8"
1518               codeSystem="1.2.276.0.76.11.32"/>
1519           </AttributeValue>
1520           <ResourceAttributeDesignator
1521             AttributeId="urn:ihe:iti:appc:2016:document-entry:class-code"
1522             DataType="urn:hl7-org:v3#CV" MustBePresent="true"/>
1523           </ResourceMatch>
1524         </Resource>
1525       </Resources>
1526     </Target>
1527     <Rule RuleId="urn:uuid:bb42d632-c70c-447d-94aa-011f2c9561f4"
1528       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`. [`<=`]

5.1.1.3 Operation

I_Document_Management::~~RemoveDocuments~~RemoveMetadata

~~A_14489-01 - Komponente ePA-Dokumentenverwaltung – Signatur für RemoveMetadata~~

~~A_14489 – Komponente ePA-Dokumentenverwaltung – Signatur für Remove Documents~~

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

Tabelle 8: Tab_Dokv_17 - Operation [Remove Documents](#)[RemoveMetadata](#)

Operation	I_Document_Management::RemoveDocumentsRemoveMetadata		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management::deleteDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove DocumentsMetadata" [ITI-8662] 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:2017:RemoveDocuments2010:DeleteDocumentSet		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Remove Documents Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocumentsxds>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	opt.
Remove Documents Response Message	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocumentsResponsexds>DeleteDocumentSetResponse Message	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	

[<=]

Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-Transaktionen "~~RemoveDocuments~~~~RemoveMetadata~~" [ITI-~~8662~~] 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 14908-01 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Metadata

~~A 14908 – Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Documents~~ Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository Registry" MUSS die Umsetzung der Operation `I_Document_Management::RemoveDocumentsRemoveMetadata` gemäß der definierten Ablauflogik in [IHE-ITI-RMD#3.86.4.1.2 und 3.86.4.1.3] implementieren. [<=]

A 20713 - Komponente ePA-Dokumentenverwaltung – Remove Metadata mit uniqueIds (Übergangsphase)

Falls in der Anfragenachricht zu `I_Document_Management::RemoveMetadata` im Feld `/RemoveObjectsRequest/ObjectRefList/ObjectRef[@id]` anstelle einer `entryUUID` eine `uniqueId` gesendet wird, MUSS die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" die Operation gemäß A 14908-01 durchführen, als wenn stattdessen dort die `DocumentEntry.entryUUID` des Dokuments hinterlegt wäre, dessen `DocumentEntry.uniqueId` der gesendeten `uniqueId` entspricht. [<=]

A 20633 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Remove Metadata

Die Komponente ePA-Dokumentenverwaltung als RMD-Akteur "Document Registry" 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 (und ein ggf. dazugehöriges Dokument) gelöscht wird. [<=][<=]

5.1.1.4 Operation `I_Document_Management::CrossGatewayRetrieve`

A_14464 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-Gateway Retrieve

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

Tabelle 9: Tab_Dokv_18 - Operation Cross-Gateway Retrieve

Operation	<code>I_Document_Management::CrossGatewayRetrieve</code>
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management::getDocuments</code> 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	optional
Cross-Gateway Retrieve Message	Eingangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetRequest	no
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	no
Ausgangsparameter			
Name	Beschreibung	Typ	optional
Cross-Gateway Retrieve Response Message	Ausgangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetResponse	no
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.	

1614 [**<=**]

1615 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1616 Transaktionen "Cross-Gateway Document Retrieve" [ITI-39] und "Provide X-User
1617 Assertion" [ITI-40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-
1618 TF2x] zu entnehmen.

1619 **5.1.1.4.1 Umsetzung**

1620 **A_14911 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-
1621 Gateway Retrieve**

1622 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
1623 MUSS die Umsetzung der Operation `I_Document_Management::CrossGatewayRetrieve`
1624 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.39.4.1.2 und 3.39.4.1.3] und
1625 [IHE-ITI-TF2b#3.39.4.2.2 und 3.39.4.2.3] implementieren.**[<=]**

A_16201 - Komponente ePA-Dokumentenverwaltung – Prüfung der zurückgegebenen Paketgröße

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

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

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 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 XDSDocumentUniqueIdError-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 XDSDocumentUniqueIdError zurückgegeben werden.[<=]

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 10: 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 	

1658

1659 [\leq]1660 **5.1.2.1 Operation**1661 **I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b**1662 **A_14479 - Komponente ePA-Dokumentenverwaltung – Signatur für Provide And**1663 **Register Document Set-b**

1664 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

1665 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b gemäß der
1666 folgenden Signatur implementieren:1667 **Tabelle 11: 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	opt
Provide And Register Document Set-b Message	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	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
Provide And Register Document Set-b 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 einzelnen übermittelten Dokuments übersteigt 25 MByte.	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

1668
1669
1670

[<=]

1671 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
 1672 Transaktionen "Provide And Register Document Set-b" [ITI-41] und "Provide X-User
 1673 Assertion" [ITI-40] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
 1674 entnehmen.

1675 5.1.2.1.1 Umsetzung

1676 **A_15056 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung von** 1677 **gemischten Dokumentenpaketen mit Policy Documents**

1678 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
 1679 MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und
 1680 mit einem XDSRepositoryMetadataError-Fehlercode quittieren, sofern in der
 1681 Eingangsnachricht mehr als ein Dokument und Dokumenten-Metadaten gemäß der
 1682 Anforderung [gemSpec_DM_ePA#A_14961] für Policy Documents (Advanced Patient
 1683 Privacy Consents) enthalten sind.[<=]

1684 **A_14912 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide** 1685 **And Register Document Set-b**

1686 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
 1687 MUSS die Umsetzung der
 1688 Operation `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b`
 1689 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3] und
 1690 [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3] implementieren.[<=]

1691 **A_16442 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender** 1692 **X-User Assertion**

1693 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
 1694 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12]
 1695 quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
 1696 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
 1697 [<=]

1698 5.1.2.2 Operation

1699 **I_Document_Management_Insurant::RegistryStoredQuery**

1700 **A_14480 - Komponente ePA-Dokumentenverwaltung – Signatur für Registry** 1701 **Stored Query**

1702 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 1703 `I_Document_Management_Insurant::RegistryStoredQuery` gemäß der folgenden
 1704 Signatur implementieren:

1705 **Tabelle 12: Tab_Dokv_22 - Operation Registry Stored Query**

Operation	I_Document_Management_Insurant::RegistryStoredQuery
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management_Insurant::find</code> 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	

1706

1707 [**<=**]

1708 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
 1709 Transaktionen "Registry Stored Query" [ITI-18] und "Provide X-User Assertion" [ITI-
 1710 40] sind [IHE-ITI-TF2a], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
 1711 entnehmen.

1712 5.1.2.2.1 Umsetzung

1713 **A_14913 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Registry** 1714 **Stored Query**

1715 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
 1716 die Umsetzung der

1717 Operation `I_Document_Management_Insurant::RegistryStoredQuery` gemäß der

1718 definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3]
1719 implementieren.[<=]

1720 **A_16436 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender**
1721 **X-User Assertion**

1722 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1723 die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren, falls
1724 die X-User Assertion nicht dem SAML 2.0 Assertion Profil
1725 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
1726 [<=]

1727 **A_17185 - Komponente ePA-Dokumentenverwaltung – Suchanfragen über das**
1728 **Metadatenattribut DocumentEntry.title**

1729 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1730 einen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID
1731 "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben
1732 Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-
1733 ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter
1734 \$XDSDocumentEntryTitle unterstützen, sodass eine Suchergebnismenge über das
1735 Attribut XDSDocumentEntry.title eingeschränkt werden kann. Weiterhin MUSS dieselbe
1736 Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den
1737 Parameter \$XDSDocumentEntryAuthorPerson. Daswsa:Action-Element MUSS den Wert
1738 "urn:ihe:iti:2007:RegistryStoredQuery" besitzen.
1739 [<=]

1740 **A_14588 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
1741 **Registry Stored Query**

1742 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1743 die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy
1744 Documents (Advanced Patient Privacy Consents) entsprechend der
1745 Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt zum ePA-Frontend
1746 des Versicherten (XDS-Akteur "Document Consumer") zurückgegeben wird.
1747

1748 [<=]

1749 **A_20532 - Komponente ePA-Dokumentenverwaltung – Zugriff auf**
1750 **SubmissionSets bei der Suche**

1751 Die Komponente ePA-Dokumentenverwaltung MUSS einen Zugriff auf ein SubmissionSet
1752 im Rahmen der Operationen I Document Management::CrossGatewayQuery sowie
1753 I Document Management Insurant::RegistryStoredQuery unterbinden, wenn der
1754 Zugreifende nicht mindestens für ein Dokument darin berechtigt ist.
1755 [<=]

1756 **A_20533 - Komponente ePA-Dokumentenverwaltung – Zugriff auf Folder bei der**
1757 **Suche**

1758 Die Komponente ePA-Dokumentenverwaltung MUSS einen Zugriff auf einen Folder im
1759 Rahmen der Operationen I Document Management::CrossGatewayQuery sowie
1760 I Document Management Insurant::RegistryStoredQuery unterbinden, wenn der
1761 Zugreifende nicht für mindestens ein Dokument darin berechtigt ist.[<=]

1762 **A_20534 - Komponente ePA-Dokumentenverwaltung – Zugriff auf Associations**
1763 **bei der Suche**

1764 Die Komponente ePA-Dokumentenverwaltung MUSS einen Zugriff auf Associations im
1765 Rahmen der Operationen I Document Management::CrossGatewayQuery sowie
1766 I Document Management Insurant::RegistryStoredQuery unterbinden, wenn der
1767 Zugreifende nicht für beide Endpunkte der Association (DocumentEntries,
1768 SubmissionSets, Folder) berechtigt ist.[<=]

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

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

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

[<=]

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

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

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

Die folgende Anforderung ermöglicht es Clients, eine Suche im "Namen" einer LEI oder eines KTR durchzuführen. Dies ist nützlich, um etwaige Berechtigungsvergaben zu prüfen. Die Anfrage eignet sich also auch, um im Vorfeld eine potentielle Berechtigungsvergabe "durchzuspielen".

5.1.2.2.1.1 Suche mit simulierter Berechtigung

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

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

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

[<=]

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

Die in A_20224 definierte Suche MUSS wie folgt umgesetzt werden:

- Wenn die in A_20224 genannten Bestimmungen nicht erfüllt sind, MUSS die Komponente ePA-Dokumentenverwaltung einen Fehler zurückgeben (ResponseStatusType:Failure).
- Ansonsten gelten folgende Bestimmungen:
 - Die Komponente ePA-Dokumentenverwaltung MUSS die im Base64-Format enthaltene Policy dekodieren.
 - Die Komponente ePA-Dokumentenverwaltung DARF das Policy-Dokument NICHT in der Dokumentenverwaltung hinterlegen. Sie wird also für andere Anfragen an die Schnittstellen der Dokumentenverwaltung nicht beachtet.
 - Die Komponente ePA-Dokumentenverwaltung DARF NICHT ein anderes (etwaig hinterlegtes) Base Policy Dokument für dieselbe LEI oder KTR im Rahmen dieser Suche beachten.
 - Die Komponente ePA-Dokumentenverwaltung MUSS die Klartextpolicy gemäß 5.34.6 behandeln und bei erfolgreicher Zugriffskontrollprüfung ("Permit") die Suche wie in 5.1.2.2 beschrieben unter Beachtung der Policy umsetzen.

[<=]

5.1.2.3 Operation

I_Document_Management_Insurant::RemoveDocumentsRemoveMetadata

A_14488-01 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove Metadata

A_14488 – Komponente ePA-Dokumentenverwaltung – Signatur für Remove Documents Die Komponente ePA-Dokumentenverwaltung MUSS die Operation I_Document_Management_Insurant::RemoveDocumentsRemoveMetadata gemäß der folgenden Signatur implementieren:

Tabelle 13: Tab_Dokv_23 - Operation RemoveDocumentsRemoveMetadata

Operation	I_Document_Management_Insurant::RemoveDocumentsRemoveMetadata
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 DocumentsMetadata" [ITI-8662] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente im ePA-Aktensystem zu löschen.
Formatvorgaben	SOAP Action: urn:ihe:iti:2017:RemoveDocuments2010:DeleteDocumentSet
Eingangsparameter	

Name	Beschreibung	Typ	opt.
Remove Documents-Metadatatadata Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocuments 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 DocumentsMessage Response Message	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocumentsResponse xds:DeleteDocumentSetResponse Message	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	

[<=]

Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-Transaktionen "[RemoveDocumentsRemoveMetadata](#)" [ITI-~~8662~~8662] und Provide X-User Assertion [ITI-40] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5.1.2.3.1 Umsetzung

A_14909-01 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Metadata

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

A_16437-01A_16437 - 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. [\leq]

5.1.2.4 Operation

I_Document_Management_Insurant::RetrieveDocumentSet
A_14481 - Komponente ePA-Dokumentenverwaltung – Signatur für Retrieve Document Set

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

Tabelle 14: 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.	

1876
1877

[<=]

1878 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1879 Transaktionen "RetrieveDocumentSet" [ITI-43] und "Provide X-User Assertion" [ITI-
1880 40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1881 entnehmen.

1882 5.1.2.4.1 Umsetzung

1883 **A_14914 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Retrieve** 1884 **Document Set**

1885 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1886 MUSS die Umsetzung der
1887 Operation `I_Document_Management_Insurant::RetrieveDocumentSet` gemäß den
1888 definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3] und [IHE-ITI-
1889 TF2b#3.43.4.2.2 und 3.43.4.2.3] implementieren.[<=]

1890 **A_16443 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender** 1891 **X-User Assertion**

1892 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1893 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren,
1894 falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
1895 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.

1896 [<=]

A_16200 - Komponente ePA-Dokumentenverwaltung – Prüfung der zurückgegebenen Paketgröße

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

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

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 Repository-Datenobjekt zum ePA-Frontend des Versicherten als XDS-Akteur "Document Consumer" zurückgegeben wird. Ist ein abzurufendes Dokument nicht mehr verfügbar, MUSS gemäß IHE TF ITI der Fehlercode `XDSDocumentUniqueIdError` zurückgegeben werden.

[<=]

5.1.2.5 Operation

I_Document_Management_Insurant::RestrictedUpdateDocumentSet

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

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

Tabelle 15: Tab_Dokv_19 - Operation RestrictedUpdateDocumentSet

Operation	I_Document_Management_Insurant::RestrictedUpdateDocumentSet
Beschreibung	<p>Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management_Insurant::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>Für Änderungen an der Vertraulichkeitsstufe von Dokumenten werden im <code>documentEntry.confidentialityCode</code> die Werte "normal", "restricted" oder "very restricted" mit der <code>updateMetadata</code> 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.			

1923
1924

[<=]

1925 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1926 Transaktionen "RestrictedUpdateDocumentSet" [ITI-92] und "Provide X-User Assertion"
1927 [ITI-40] sind [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1928 entnehmen.

1929 5.1.2.5.1 Umsetzung

1930 **A_15082 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung** 1931 **der Metadaten aus ITI Document Sharing-Profilen durch RMU-Akteur "Update** 1932 **Responder"**

1933 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
1934 die übermittelten DocumentEntry-Metadaten der eingehenden Nachricht dahingehend
1935 prüfen, dass gegenüber den Bestandsdaten das
1936 Metadatenattribut `documentEntry.confidentialityCode` konform zu den
1937 Nutzungsvorgaben in [gemSpec_DM_ePA#A_14760] geändert ist. Die Komponente ePA-
1938 Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS das Aktualisieren
1939 dieses Metadatenattributs ablehnen und mit einem `XDSRepositoryMetadataError`
1940 quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. [<=]

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

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

[<=]

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

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

Operation `I_Document_Management_Insurant::RestrictedUpdateDocumentSet` gemäß der definierten Ablauflogik in [IHE-ITI-RMU#3.92.4.1.2 und 3.92.4.1.3] implementieren und sicherstellen, dass (nur) die folgenden Metadatenobjekte gesendet werden:

- Ein neues `SubmissionSet`
- Einen `DocumentEntry`, der identisch mit dem zu aktualisierenden `DocumentEntry` identisch ist (inklusive `entryUUID`) und sich nur im `confidentialityCode` unterscheidet
- Eine SS-DE HasMember-Association, die das `SubmissionSet` mit dem geschickten `DocumentEntry` verbindet
- Die „lid“ (logicalID) DARF NICHT gesendet werden.
- Der Slot „associationPropagation“ MUSS auf „no“ gesetzt werden.

Die Komponente ePA-Dokumentenverwaltung DARF die gesendete `Association` und das neue `SubmissionSet` NICHT dauerhaft speichern.[<=]

A_15080-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Restricted Update Document Set

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor Metadaten einer oder mehrerer Dokumente aktualisiert werden. Beim Aktualisieren der Metadaten durch das ePA-Frontend des Versicherten können einzelne Dokumente bzw. Metadaten durch den zwischenzeitlichen Entzug einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für die Aktualisierung berechtigt sein. Widerspricht ein Dokument bzw. die damit assoziierten Metadaten einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum betreffenden Dokument einen `XSDSDocumentUniqueIdError`-Fehlercode enthalten und der Wert 4 des `EventOutcomeIndicators` im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein zu aktualisierendes Dokument bzw. Metadaten nicht mehr verfügbar, MUSS gemäß IHE TF ITI der Fehlercode `XSDSDocumentUniqueIdError` zurückgegeben werden.

[<=]

1992 5.1.3 Schnittstelle I_Document_Management_Insurance

1993 A_17438 - Komponente ePA-Dokumentenverwaltung – Implementierung der 1994 Schnittstelle I_Document_Management_Insurance

1995 Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle
1996 definierte Web-Service-Schnittstelle implementieren.

1997 **Tabelle 16: 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 	

1998
1999 [\leq]

2000 5.1.3.1 Operation

2001 I_Document_Management_Insurance::ProvideAndRegisterDocumentSet 2002 -b

2003 A_17439 - Komponente ePA-Dokumentenverwaltung – Signatur für Provide And 2004 Register Document Set-b

2005 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

2006 I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b gemäß der
2007 folgenden Signatur implementieren:

2008

Tabelle 17: 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 ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	n
X-User Assertion	Authentication Assertion des authentifizierten 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.

2009
2010

[<=]

2011 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
2012 Transaktionen "Provide And Register Document Set-b" [ITI-41] und "Provide X-User
2013 Assertion" [ITI-40] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
2014 entnehmen.

2015 **5.1.3.1.1 Umsetzung**

2016 **A_17443 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide**
2017 **And Register Document Set-b**

2018 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2019 MUSS die Umsetzung der
2020 Operation `I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b`
2021 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3] und
2022 [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3] implementieren.

2023 [<=]

2024 **A_17444 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender**
2025 **X-User Assertion**

2026 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
2027 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren,
2028 falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
2029 gemäß [gemSpec_FM_ePA_KTR_Consumer#A_17253, A_17254] entspricht. [<=]

2030 **5.1.4 Anforderungen an Sammlungstypen**

2031 **A_20578 - Komponente ePA-Dokumentenverwaltung – Einstellen von**
2032 **Dokumenten in Sammlungen des Typs "mixed"**

2033 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
2034 beim Einstellen eines Dokuments des Sammlungstyps "mixed" sicherstellen, dass das
2035 Dokument in derselben Operation einem entsprechenden Sammlungstypordner
2036 zugewiesen wird und die Operation ansonsten mit dem
2037 FehlerXDSRegistryMetadataError abbrachen. Die ePA-Dokumentenverwaltung MUSS
2038 sicherstellen, dass der Ordner in derselben Operation angelegt wird, sofern ein nicht
2039 schon bestehender Ordner verwendet wird. [<=]

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

Die Komponente ePA-Dokumentenverwaltung MUSS das Anlegen eines Folders für den Verwaltungstyp "mixed" mit dem Fehler `XDSRegistryMetadataError` unterbinden, wenn nicht in derselben Operation auch mindestens ein entsprechendes Sammlungstyp-spezifisches strukturiertes Dokument (gemäß gemSpec DM ePA#A 20577) eingestellt wird und die Operation mit dem Fehler `ACCESS_DENIED` abbrechen, wenn der Zugreifende nicht die Berechtigung besitzt, den Ordner und alle für den vorgesehenen Ordner mitgesendeten Dokumente anzulegen.

[<=]

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

Die Komponente ePA-Dokumentenverwaltung MUSS das Einstellen von Dokumenten in einen Ordner für Sammlungstyp "mixed" mit dem Fehler `ACCESS_DENIED` abbrechen, wenn das Dokument nicht einem dem Sammlungstyp zugeordneten strukturierten Dokumententyp (gemäß gemSpec DM ePA#A 20577) entspricht.

[<=]

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

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

A_20581 - Komponente ePA-Dokumentenverwaltung – Löschen von Dokumenten des Sammlungstypen "mixed"

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS beim Löschen eines Dokuments der Sammlungstypen "mixed" 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 "mixed" 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-Modul Frontend des Versicherten bereitgestellt.

A_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.

2084 **Tabelle 18: 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
WSDL	AccountManagementService.wsdl	
XML Schema	AccountManagementService.xsd	

2085 [**<=**]2086 **5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount**2087 **A_14805 - Komponente ePA-Dokumentenverwaltung – Signatur für**2088 **I_Account_Management_Insurant::SuspendAccount**

2089 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

2090 I_Account_Management_Insurant::SuspendAccount gemäß der folgenden Signatur

2091 implementieren:

2092 **Tabelle 19: Tab_Dokv_26 - Operation Suspend Account**

Operation	I_Account_Management_Insurant::SuspendAccount
Beschreibung	<p>Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Account_Management_Insurant::SuspendAccount technisch um.</p> <p>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.</p>

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-Aktensystem geladen werden kann	URL mit Prozentkodierung	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.	
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.
----------------------	--	--

2093 [**<=**]

2094 *5.2.1.1.1 Umsetzung*

2095 **A_15530 - Komponente ePA-Dokumentenverwaltung –**

2096 **I_Account_Management_Insurant über sicheren Kanal**

2097 Die Komponente ePA-Dokumentenverwaltung MUSS die von ihr angebotenen
2098 Operationen der Schnittstelle `I_Account_Management_Insurant` ausschließlich über den
2099 sicheren Kanal zum ePA-Modul Frontend des Versicherten verfügbar machen. [**<=**]

2100 Die folgende Anforderung bewirkt, dass nur der Versicherte als Inhaber einer Akte im
2101 Zustand "DISMISSED" die

2102 Operation `I_Account_Management_Insurant::SuspendAccount` ausführen kann.

2103 **A_15062 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
2104 **Suspend Account**

2105 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
2106 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
2107 Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor die
2108 Operation `I_Account_Management_Insurant::SuspendAccount` ausgeführt wird. Bei
2109 einer negativen Autorisierungsentscheidung MUSS die Nachricht mit dem
2110 `ACCESS_DENIED`-Fehlercode quittiert werden. [**<=**]

2111 **A_14885 - Komponente ePA-Dokumentenverwaltung – Exportpaket des**
2112 **Aktenkontos erstellen**

2113 Die Komponente ePA-Dokumentenverwaltung MUSS bei der Ausführung der Operation
2114 `I_Account_Management_Insurant::SuspendAccount` für das Aktenkonto

- 2115 • sämtliche Dokumente einschließlich Policy Documents (Advanced Patient Privacy
- 2116 Consents) des XCDR Responding Gateway bzw. XDS Document Repository,
- 2117 • sämtliche Metadaten der XCA Responding Gateway bzw. XDS Document Registry,
- 2118 • sämtliche § 291a-Protokolldaten,

2119 gemäß den strukturellen Vorgaben in [IHE-ITI-TF2b] zur Transaktion *IHE ITI Cross-*
2120 *Enterprise Document Media Interchange (XDM) - Distribute Document Set on Media [ITI-*
2121 *32]*, in eine ZIP-Datei exportieren.

2122 Die Komponente ePA-Dokumentenverwaltung MUSS dabei abweichend von den Vorgaben
2123 aus [ITI-32],

- 2125 • die ZIP-Datei außerhalb des Verarbeitungskontextes persistieren,
- 2126 • die ZIP-Datei im Zuge des Exports mit dem `ContextKey` gemäß
- 2127 [`gemSpec_Krypt#GS-A_5016`] verschlüsseln, so dass sichergestellt ist, dass nur
- 2128 entsprechend verschlüsselte Daten außerhalb des Verarbeitungskontextes
- 2129 auftreten können sowie
- 2130 • die ZIP-Datei zum Abruf für berechtigte andere Anbieter ePA-Aktensystem
- 2131 verfügbar machen.

2132 Der Verarbeitungskontext MUSS solange geöffnet bleiben, bis die ZIP-Datei erstellt
2133 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-Modul 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-Moduls 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 Export. Die Anforderung A_15623 im nächsten Abschnitt regelt die asynchrone Verarbeitung des Imports.

A_15622 - Komponente ePA-Dokumentenverwaltung – Asynchroner Export

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

A_16076 - Komponente ePA-Dokumentenverwaltung – Frist für Bereitstellung des Exportpakets

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

5.2.1.2 Operation `I_Account_Management_Insurant::ResumeAccount`**A_14807 - Komponente ePA-Dokumentenverwaltung – Signatur für `I_Account_Management_Insurant::ResumeAccount`**

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

2178 Tabelle 20: 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.	
----------------------	--	--

2179 [**<=**]

2180 5.2.1.2.1 Umsetzung

2181 Die Ausführung der Operation `I_Account_Management_Insurant::ResumeAccount` setzt
 2182 voraus, dass der Versicherte mittels seines ePA-Moduls Frontend des Versicherten einen
 2183 sicheren Kanal zum Verarbeitungskontext aufgebaut hat und diesen mittels der Operation
 2184 `I_Document_Management_Connect::OpenContext` kryptographisch aktiviert hat. Darüber
 2185 hinaus muss die Operation `I_Account_Management_Insurant::ResumeAccount`
 2186 aufgerufen werden, bevor weitere Operationen am Verarbeitungskontext ausgeführt
 2187 werden können. Sie muss mit Fehler terminieren, wenn sie für ein Aktenkonto bereits
 2188 vorher erfolgreich ausgeführt wurde.

2189 **A_15526 - Komponente ePA-Dokumentenverwaltung – Voraussetzungen für die** 2190 **Ausführung von Resume Account**

2191 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Operation
 2192 `I_Account_Management_Insurant::ResumeAccount` nur ausgeführt wird, wenn der
 2193 Verarbeitungskontext eines für einen Anbieterwechsel mit Übernahme der Aktendaten
 2194 registriertes Aktenkonto erstmalig durch den Versicherten geöffnet wurde. [**<=**]

2195 **A_15568 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für** 2196 **Resume Account**

2197 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
 2198 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
 2199 Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor die
 2200 Operation `I_Account_Management_Insurant::ResumeAccount` ausgeführt wird. Bei einer
 2201 negativen Autorisierungsentscheidung MUSS die Nachricht mit dem `ACCESS_DENIED`-
 2202 Fehlercode quittiert werden. [**<=**]

2203 **A_15013 - ePA-Aktensystem – Download des Exportpakets**

2204 Das ePA-Aktensystem MUSS nach Eingang des Requests
 2205 `I_Account_Management_Insurant::ResumeAccount` das mittels des Aufrufparameters
 2206 `PackageURL` referenzierte Exportpaket beim vorhergehenden Anbieter ePA-Aktensystem
 2207 des Versicherten abrufen und für den Import durch den Verarbeitungskontext der ePA-
 2208 Dokumentenverwaltung verfügbar machen. [**<=**]

2209 **A_14905 - Komponente ePA-Dokumentenverwaltung – Import des Exportpakets** 2210 **des vorhergehenden Aktenkontos**

2211 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS das vom
 2212 vorhergehenden Anbieter ePA-Aktensystem des Versicherten bezogene Exportpaket, vom
 2213 vorhergehenden Anbieter herunterladen sobald es dort verfügbar ist und in das neue
 2214 Aktenkonto importieren und dazu:

- 2215 • das Exportpaket mittels des `ContextKey` entschlüsseln und
- 2216 • die Struktur des Exportpakets auf Übereinstimmung mit den Festlegungen aus
- 2217 Anforderung A_14885 prüfen.

2218 [**<=**]

2219 **A_15596 - Komponente ePA-Dokumentenverwaltung – Ersetzen der Home**
2220 **Community ID**

2221 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS beim
2222 Import eines Exportpakets in sämtlichen Metadatensätzen den anbieterspezifischen Wert
2223 in den Feldern DocumentEntry.homeCommunityId und SubmissionSet.homeCommunityId
2224 sowie DocumentEntry.repositoryUniqueId mit der neuen Home Community ID
2225 aktualisieren. [≤]

2226 **A_15623 - Komponente ePA-Dokumentenverwaltung – Asynchroner Import**

2227 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die
2228 Antwort auf den Aufruf der Operation

2229 `I_Account_Management_Insurant::ResumeAccount` unmittelbar nach dem Aufruf an den
2230 Client zurückgeben, unabhängig davon, wie lange der Erhalt und Import des
2231 Exportpakets dauert. [≤]

2232 Die folgende Anforderung stellt sicher, dass der neue Anbieter des Aktenkontos
2233 ausreichend lange auf die Bereitstellung des Exportpakets durch den alten Anbieter
2234 wartet, da die Bereitstellung je nach Größe des Exportpakets eine gewisse Zeit in
2235 Anspruch nehmen kann. Der Versicherte kann mit dem neuen Aktenkonto nicht
2236 interagieren, bis der Import abgeschlossen ist. Das ePA-Modul Frontend des Versicherten
2237 muss jedoch nicht auf den Abschluss warten, weil der Vorgang auf Ebene der Dienste
2238 asynchron abgeschlossen ist, nachdem der Versicherte ihn mittels des Aufrufs der
2239 Operation `I_Account_Management_Insurant::SuspendAccount` beim alten Anbieter und
2240 dem direkt anschließenden Aufruf der Operation
2241 `I_Account_Management_Insurant::ResumeAccount` beim neuen Anbieter ausgelöst hat.

2242 **A_15624 - Komponente ePA-Dokumentenverwaltung – Abfrage auf**
2243 **Verfügbarkeit des Exportpakets**

2244 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS nach dem
2245 Aufruf der Operation `I_Account_Management_Insurant::ResumeAccount` bei unmittelbar
2246 vorgesehenem Abruf des Exportpakets bis zum Erfolgsfall periodisch prüfen,
2247 jedoch maximal für einen Zeitraum von drei Werktagen, ob ein Exportpaket unter der
2248 vom Client übergebenen URL bereitsteht. [≤]

2249 **A_15625 - Komponente ePA-Dokumentenverwaltung – Kein Aktenzugriff**
2250 **während des Imports der Daten**

2251 Die Komponente ePA-Dokumentenverwaltung MUSS während der Ausführung der
2252 Operation `I_Account_Management_Insurant::ResumeAccount` für ein Aktenkonto alle
2253 Operationen mit Fehlermeldung "Aktenkonto aufgrund einer andauernden
2254 Datenmigration vorübergehend nicht erreichbar" ablehnen. [≤]

2255 **A_16077 - Komponente ePA-Dokumentenverwaltung – Frist für den Import des**
2256 **Exportpakets**

2257 Die Komponente ePA-Dokumentenverwaltung MUSS den Import eines Exportpakets
2258 innerhalb von drei Werktagen nach Beginn des Downloads vom vorherigen Anbieter
2259 abschließen.
2260 [≤]

2261 **A_17845 - Komponente ePA-Dokumentenverwaltung – Offener**
2262 **Verarbeitungskontext während der Verarbeitung des Exportpakets**

2263 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS den für die
2264 Operation `I_Account_Management_Insurant::ResumeAccount` geöffneten
2265 Verarbeitungskontext so lange geöffnet lassen, bis der Abruf des Exportpakets beim alten
2266 Anbieter erfolgt ist und die Verarbeitung der Daten des Exportpakets durch diesen
2267 Verarbeitungskontext abgeschlossen ist, jedoch maximal drei Tage, falls kein
2268 Exportpaket abgerufen werden kann.
2269 [≤]

5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents

A_14490-01 - 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 21: 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_INV ALID	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.	

2277 [\leq]

2278

2279 5.2.1.3.1 Umsetzung

2280 **A_15229 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
2281 **Get Audit Events**

2282 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
2283 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
2284 Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor eine Audit
2285 Event List zum ePA-Modul Frontend des Versicherten zurückgegeben wird.

2286 [\leq]

2288 **A_15583 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Get Audit**
2289 **Events**

2290 Die Komponente ePA-Dokumentenverwaltung MUSS die Liste der § 291a-
2291 Protokolleinträge als Liste `phr:AuditMessage` zurückgeben. [\leq]

2292 5.3 Umschlüsselung

2293 Die ePA-Dokumentenverwaltung verwaltet verschlüsselte Dokumente: Die Dokumente
2294 selbst sind mit einem dokumentenspezifischen Dokumentenschlüssel verschlüsselt, der
2295 wiederum mit dem Aktenschlüssel verschlüsselt wird und so verpackt dem Dokument
2296 beigelegt wird. Die Dokumentenmetadaten, das Protokoll des Versicherten sowie die
2297 Policy-Dokumente werden zudem über einen Kontextschlüssel gesichert. Akten- und
2298 Kontextschlüssel sind für die gesamte Akte des Versicherten gültig.

2299 Auf eigenen Wunsch kann der Versicherte eine Umschlüsselung seiner Akte anstoßen.
2300 Dabei werden Akten- und Kontextschlüssel ausgetauscht. Die Dokumentenschlüssel
2301 werden *nicht* gewechselt. Die Aufgabe besteht also darin, die verschlüsselten
2302 Dokumentenschlüssel mit dem alten Aktenschlüssel zu entschlüsseln, mit dem neuen
2303 Aktenschlüssel wieder zu verschlüsseln und das entstandene neue Paket wieder dem
2304 entsprechenden Dokument in der Dokumentenverwaltung zuzuordnen. Da die
2305 Dokumentenverwaltung niemals Zugriff auf den Aktenschlüssel im Klartext bekommt,
2306 muss die Ent- und Verschlüsselung im Client stattfinden.

2307 Der Vorgang der Umschlüsselung wird über die folgenden Operationen gesteuert:

- 2308 • I Key Management Insurant::StartKeyChange()

- [I Key Management Insurant::GetAllDocumentKeys\(\)](#)
- [I Key Management Insurant::PutAllDocumentKeys\(\)](#)
- [I Key Management Insurant::FinishKeyChange\(\)](#)

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

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

5.3.1 Übergreifende Anforderungen

A 20466 - Komponente ePA-Dokumentenverwaltung – Erlaubte Zustandsübergänge für Zustand KEY_CHANGE_DOKV

[Die Komponente ePA-Dokumentenverwaltung MUSS zur Umschlüsselung die Zustandsübergänge aus der Abbildung "Zustandsübergänge Schlüsselwechsel" nur die angegebenen Operationen in der angegebenen Reihenfolge erlauben und andere](#)

2330

Zustandsübergänge (Operationsaufrufe) mit einem Fehler ablehnen.

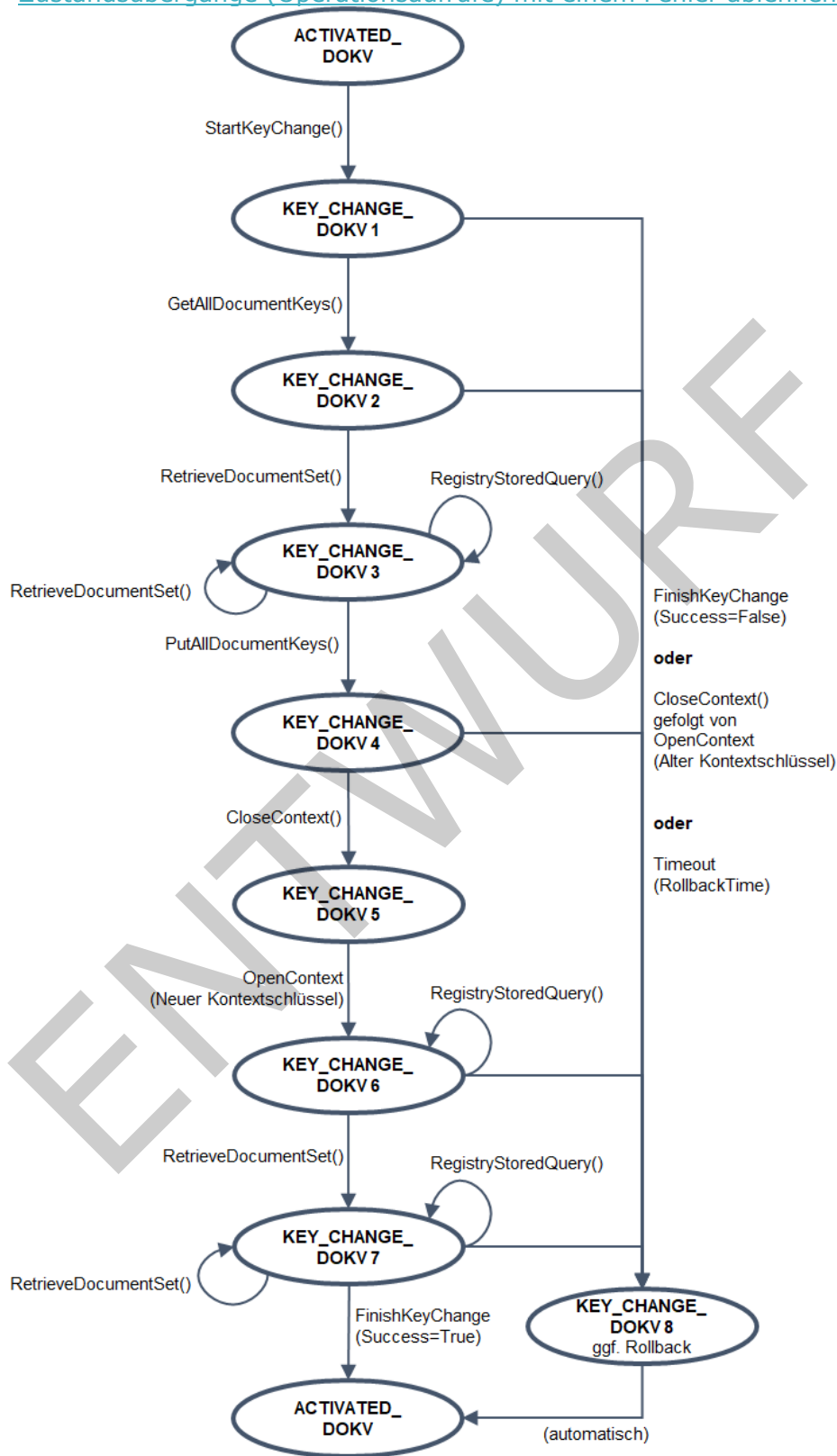


Abbildung 2 Zustandsübergänge Schlüsselwechsel

2331

2332

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()
 - PutAllDocumentKeys():
I Key Management Insurant::PutAllDocumentKeys()
 - FinishKeyChange(): I Key Management Insurant::FinishKeyChange()
 - OpenContext(): I Document Management Connect::OpenContext()
 - CloseContext(): I Document Management Connect::CloseContext()
 - RetrieveDocumentSet():
I Document Management Insurant::RetrieveDocumentSet()
- CloseContext() (gefolgt von OpenContext()) DARF zusätzlich auch in Kombination in den Zuständen Normalbetrieb sowie KEY_CHANGE DOKV 1, 2, 5 und 6 ausgeführt werden. In dem Fall ist der Zustand nach OpenContext() identisch mit dem vor CloseContext(), d.h. sie verändern den internen Zustand der Dokumentenverwaltung nicht. Die entsprechenden Zustandsübergänge sind nur aus Gründen der Übersichtlichkeit nicht im Diagramm enthalten.
- Der Zustände "KEY_CHANGE_DOKV" (mit und ohne angehängte Ziffer) und "ACTIVATED_DOKV" entsprechen nicht direkt den Zuständen "Key_Change" bzw. "Activated" des Aktensystems.
- Der Zustand "ACTIVATED_DOKV" beschreibt den normalen Betriebszustand der Akte, in dem Versicherte bzw. berechnigte weitere Parteien (LEI, KTR) über die jeweilige Schnittstelle auf Dokumente zugreifen können.

[<=]

Nach dem Hinterlegen der neu verschlüsselten Dokumentenschlüssel (Zustand KEY_CHANGE_DOKV4) müssen gemäß Zustandsdiagramm CloseContext() und OpenContext() mindestens einmal ausgeführt werden, um die neuen Kontext- und Aktenschlüssel über die Client-Schnittstelle zu testen.

Die Nummerierung der Zustände dient nur beschreibenden Zwecken, im Folgenden werden die Zustände allgemein häufig als als Zustand "KEY_CHANGE_DOKV" zusammengefasst.

A 20729 - Komponente ePA-Dokumentenverwaltung – Start der Umschlüsselung nur in Zustand Activated

Die Komponente ePA-Dokumentenverwaltung MUSS den Start der Umschlüsselung über die Operation StartKeyChange() ablehnen, wenn sie sich nicht im Zustand "ACTIVATED_DOKV" befindet.[<=]

A 20726 - Komponente ePA-Dokumentenverwaltung – Verbotene Operationen außerhalb Status KEY_CHANGE_DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS die Umschlüsselungsoperationen GetAllDocumentKeys(), PutAllDocumentKeys() sowie FinishKeyChange() mit einem Fehler ablehnen, wenn die Dokumentenverwaltung nicht im Status KEY_CHANGE_DOKV ist. [<=]

A 20727 - Komponente ePA-Dokumentenverwaltung – Validierung der Authentication Assertion

Die Komponente ePA-Dokumentenverwaltung MUSS in allen Eingangsnachrichten der Schnittstelle `I_Key_Management_Insurant` analog eines XUA-Akteur "X-Service Provider" die mitgelieferte X-User Assertion (Authentication Assertion) gemäß der Anforderung A 13690 prüfen und die eingehende Nachricht mit Fehlercodes nach [WSS#12] quittieren, falls diese X-User Assertion nicht gültig ist. [\leq]

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:

```
<?xmlversion="1.0" encoding="UTF-8"?>
<phr:KeyListxmlns: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:EncryptedDataxmlns: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. [\leq]

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. [\leq]

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. [\leq]

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

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

A 20447 - Komponente ePA-Dokumentenverwaltung – Rollback für Zustand KEY_CHANGE_DOKV

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

- Löschen des neuen Kontextschlüssels
- Wiederherstellen bzw. Reaktivierung aller mit dem alten Aktenschlüssel verschlüsselten Dokumentenschlüssel
- Löschen von allen mit dem neuen Aktenschlüssel verschlüsselten Dokumentenschlüssel
- Löschen des neuen Aktenschlüssels
- Verlassen des Status `KEY_CHANGE_DOKV` in den Zustand `ACTIVATED_DOKV`

[<=]

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

5.3.2 Schnittstelle I Key Management Insurant

5.3.2.1 I Key Management Insurant::StartKeyChange()

A 20467 - Komponente ePA-Dokumentenverwaltung – Signatur für I Key Management Insurant::StartKeyChange()

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

Tabelle 22: Tab Dokv XX - Operation I Key Management Insurant::StartKeyChange()

<u>Operation</u>	<u>I Key Management Insurant::StartKeyChange</u>
<u>Beschreibung</u>	<u>Diese Operation setzt die Operation</u> <u>I_Account_Management_Insurant::StartKeyChange</u> <u>technisch</u> <u>um.</u> <u>Mit dieser Operation kann der Versicherte den Prozess der</u>

	Umschlüsselung initiieren.		
<u>Formatvorgaben</u>	SOAP Action: http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/StartKeyChange		
<u>Eingangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt.</u>
<u>X-User Assertion</u>	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhabers)	SAML 2.0 Assertion gemäß [gemSpec Authentisierung Vers# A 14109, A 15631]	n
<u>ContextKey</u>	Neuer Kontextschlüssel	ContextKey	n
<u>RollbackTime</u>	Zeitpunkt (UTC-Zeit), an dem ein Rollback durchgeführt werden muss, sofern bis dahin nicht explizit finishKeyChange() aufgerufen wurde.	Signierte xsd:dateTime, base64-kodiert	n
<u>Ausgangsparameter</u>			
<u>AuthorizedIDList</u>	Liste mit IDs aller zurzeit berechtigten Akteure	phr:AuthorizedIDList	n
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt.</u>
<u>Technische Fehlermeldungen</u>			
<u>Name</u>	<u>Fehlertext</u>	<u>Details</u>	
<u>INTERNAL ERROR</u>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	

<u>ASSERTION INV ALID</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>Fehlerhafte 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>	

[<=]

5.3.2.1.1 Umsetzung

A 20495 - Komponente ePA-Dokumentenverwaltung – Format von phr:AuthorizedIDList

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

```
<?xmlversion="1.0" encoding="UTF-8"?>
<phr:AuthorizedIDList xmlns:phr="http://ws.gematik.de/fa/phrext/v1.0">
  <!--ID des Berechtigten, jeweils eines für jeden Berechtigten-->
  <phr:AuthorizedID>
    <!-- KVNR (bei Versicherten) oder Telematik ID (bei Leistungserbringern und
    Kostenträgern) des Berechtigten -->
    <ID> ... </ID>
    <!-- Typ: "KVNR" oder "TelematikID"-->
    <Type> ... </Type>
  </phr:AuthorizedID>
</phr:AuthorizedIDList>[<=]
```

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

A 20738 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für StartKeyChange()

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 `StartKeyChange()`.

[<=]

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 20530 - Komponente ePA-Dokumentenverwaltung – Prüfung des RollbackTime-Parameters

Die Komponente ePA-Dokumentenverwaltung MUSS die Signatur des Eingangsparameters "RollbackTime" prüfen. Dazu 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 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 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 23: Tab_Dokv_XX -

Operation I Key Management Insurant::GetAllDocumentKeys()

<u>Operation</u>	<u>I Key Management Insurant::GetAllDocumentKeys</u>		
<u>Beschreibung</u>	<u>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.</u>		
<u>Formatvorgabe</u> <u>n</u>	<u>SOAP Action:</u> <u>http://ws.gematik.de/fd/phr/I Account Management Insurant/v1.0/GetAllDocumentKeys</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 (Aktenkonteninhabers)</u>	<u>SAML 2.0 Assertion gemäß [gemSpec Authentisierung Vers#A 14109, A 15631]</u>	<u>n</u>
<u>OkDate</u>	<u>Zeitpunkt, an dem die Komponente Autorisierung PutForReplacement() erfolgreich ausgeführt hat.</u>	<u>Signierte xsd:dateTime, base64-kodiert</u>	<u>n</u>
<u>Ausgangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt</u> :
<u>DocumentKeyList</u>	<u>Liste aller Document Keys, jeweils verschlüsselt mit altem Aktenschlüssel</u>	<u>phr:KeyList</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 IN VALID</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>Fehlerhafte 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>		

[<=]

5.3.2.2.1 Umsetzung

A 20452 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für GetAllDocumentKeys()

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 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 die Signatur des Eingangsparameters "OkDate" prüfen und sicherstellen, dass OkDate einen Zeitpunkt in der Vergangenheit bezeichnet, der nicht mehr als 24 Stunden zurückliegt. Dazu 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 24: Tab Dokv XX -

Operation I Key Management Insurant::PutAllDocumentKeys()

<u>Operation</u>	<u>I Account Management Insurant::PutForReplacement</u>
<u>Beschreibung</u>	<p>Diese Operation setzt die Operation <u>I Key Management Insurant::PutAllDocumentKeys</u> technisch um.</p> <p>Mit dieser Operation kann der Versicherte den Prozess des Schlüsselwechsels einleiten.</p>

<u>Formatvorgaben</u>	SOAP Action: http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/PutAllDocumentKeys		
<u>Eingangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>optional</u> :
<u>X-User Assertion</u>	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhaber)	SAML 2.0 Assertion gemäß [gemSpec Authentisierung Vers #A 14109, A 15631]	n
<u>DocumentKeyList</u>	Liste aller Document Keys, jeweils verschlüsselt mit neuem Aktenschlüssel	phr:KeyList	n
<u>Ausgangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>optional</u> :
<u>Technische Fehlermeldungen</u>			
<u>Name</u>	<u>Fehlertext</u>	<u>Details</u>	
<u>INTERNAL_ERROR</u>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
<u>ASSERTION_INVALID</u>	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
<u>SYNTAX_ERROR</u>	Fehlerhafte Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
<u>ACCESS_DENIED</u>	Der Zugriff für diese Operation konnte nicht gewährt werden.		

[<=]

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 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 25: Tab Dokv XX -

Operation I Account Management Insurant::FinishKeyChange()

<u>Operation</u>	<u>I Key Management Insurant::FinishKeyChange</u>
<u>Beschreibung</u>	Diese Operation setzt die Operation <code>I Key Management Insurant::FinishKeyChange</code> technisch um. Mit dieser Operation kann der Versicherte den Prozess des Schlüsselwechsels beenden und gleichzeitig die Dokumentenverwaltung über Erfolg oder Misserfolg desselben informieren.
<u>Formatvorgaben</u>	SOAP Action: http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/FinishKeyChange
<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 (Aktenkonteninhabers)</u>	<u>SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109, A_15631]</u>	<u>n</u>
<u>Success</u>	<u>Beschreibt, ob die Umschlüsselung aus Sicht des Clients erfolgreich (true) oder nicht erfolgreich (false) beendet werden soll.</u>	<u>xs:boolean</u>	<u>n</u>
<u>Ausgangsparameter</u>			
<u>Name</u>	<u>Beschreibung</u>	<u>Typ</u>	<u>opt.</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>Fehlerhafte 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>		

2605 [<=]

5.3.2.4.1 Umsetzung

A 20454 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für FinishKeyChange()

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 `FinishKeyChange()`.

[<=]

A 20450 - Komponente ePA-Dokumentenverwaltung – Erfolgreicher Abschluss des Schlüsselwechsels

Die Komponente ePA-Dokumentenverwaltung MUSS bei Aufruf von `I Key Management Insurant::FinishKeyChange` mit `Success=True` alle mit dem alten Aktenschlüssel verschlüsselten Dokumentenschlüssel sowie den alten Kontextschlüssel löschen und den Zustand `KEY_CHANGE_DOKV` anschließend verlassen und in den Zustand `ACTIVATED_DOKV` übergehen. [<=]

A 20451 - Komponente ePA-Dokumentenverwaltung – Erfolgreicher Abschluss des Schlüsselwechsels

Die Komponente ePA-Dokumentenverwaltung MUSS bei Aufruf von `I Key Management Insurant::FinishKeyChange` mit `Success=False` ein Rollback gemäß A 20447 durchführen. [<=]

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

5.3.2.5 Protokollierung

A 20470 - Protokollierungszusatz für Status KEY_CHANGE_DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS für alle Operationen, bei der sich die Komponente im Status `KEY_CHANGE_DOKV` befindet, diesen Zustand auslösen oder beenden, der Protokollierung gemäß A 20538 den folgenden Parameter hinzufügen:

Tabelle 26: Tab Dokv XX - Zusätzliche Parameter des § 291a-Protokolls für die Umschlüsselung

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

[<=]

A 20473 - Protokollierungszusatz für Status Rollback im Status KEY CHANGE DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS im Falle eines Rollbacks gemäß A 20447 der Protokollierung gemäß A 20538 einen Protokolleintrag (Event.code=PHR-850) hinzufügen und dabei den folgenden Parameter hinzufügen:

Tabelle 27: Tab Dokv XX - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung

<u>Protokollparameter</u>	<u>Parameterwerte gemäß aufgerufener Operation</u>	
<u>Object-ID</u>	Das Element <code>ParticipantObjectDetail</code> muss zusätzlich mit folgenden Wertepaar (type/value) belegt werden:	
	<u>type</u>	<u>value</u>
	<u>State</u>	<u>KEY CHANGE DOKV</u>

[<=]

5.35.4 Zugriffskontrolle

5.3.15.4.1 Grob-, mittel- und feingranulare Berechtigungen

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

1. Grobgranulare Berechtigung (Vertraulichkeitsstufen)
Allen Dokumenten wird in der Akte eine von drei Vertraulichkeitsstufen zugeordnet ("Streng vertraulich", "Vertraulich" oder "Normal") und jedem Berechtigten eine von zwei Zugriffsrechten ("Normal" oder "Erweitert"). LEI mit Zugriffsrecht "Normal" dürfen auf die Dokumente in Vertraulichkeitsstufe "Normal" zugreifen, jene mit Zugriffsrecht "Erweitert" zusätzlich auf die mit "Vertraulich" gekennzeichneten Dokumente. Dokumente in der Stufe "Streng vertraulich" sind nur für den Versicherten sichtbar (Ausnahme: "Whitelisting", siehe unten).
2. Mittelgranulare Berechtigung (Kategorien)
Ein Versicherter kann Dokumente aus einen oder mehreren vorgegebenen Dokumentenkategorien (z. B. Arztbriefe) freigeben. Die dadurch getätigte Dokumentenauswahl wird mit dem grobgranularen Zugriffsrecht (siehe 1.) des Berechtigten kombiniert. Das heißt, dass eine auf Arztbriefe berechtigte LEI je nach Zugriffsrecht entweder nur die als "Normal" eingestufteten Arztbriefe sehen kann oder auch die als "Vertraulich" gekennzeichneten. Mittelgranulare Berechtigungen schränken die grobgranular vergebene Berechtigungen ggf. ein, erweitern sie aber niemals. Ausschließlich die Metadaten eines Dokuments entscheiden darüber, welchen Kategorien (mindestens einer, potentiell mehreren) ein Dokument zugeordnet ist (siehe auch [A 19388](#) in gemSpec_DM_ePA).
3. Feingranulare Berechtigung (White- und Blacklist)
Der Versicherte kann einer LEI den Zugriff auf einzelne Dokumente gewähren ("Whitelisting") oder entziehen ("Blacklisting"). Die Vergabe von feingranularen

2678 Berechtigungen ist immer unabhängig von den vergebenen mittel- und
 2679 grobgranularen Berechtigungen. Steht also ein Dokument auf White- oder
 2680 Blacklist, spielen etwaige entgegenstehende grob- und feingranulare
 2681 Berechtigungen bei der Zugriffsentscheidung auf dieses Dokument keine Rolle.

2682 **5.3.25.4.2 Berufsgruppenspezifische Einschränkungen**

2683 Darüberhinaus gibt es einige berufsgruppenspezifische Vorgaben, welche die nach obigen
 2684 Methoden vergebenen Berechtigungen insoweit einschränken, dass bestimmten
 2685 Berufsgruppen der Zugriff auf festgelegte Dokumentenkategorien ausnahmslos verboten
 2686 ist oder ausgewählte Operationen auf den dazugehörigen Dokumenten untersagt werden.

2687 Beispielsweise haben Apotheker grundsätzlich keinen Zugriff auf das Zahnbonusheft
 2688 (Kategorie "~~category~~_dentalrecord") des Versicherten (siehe Tab_Dokv_030 -
 2689 Zugriffsunterbindungsregeln).

2690 . Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen,
 2691 ändern oder löschen.

2692 Weder der Versicherte, noch ein anderer Akteur kann die berufsgruppenspezifischen
 2693 Zugriffsbeschränkungen umgehen.

2694 Eine Übersicht über die unterschiedenen Berufsgruppen und die ihnen möglichen
 2695 Berechtigungen finden sich in [Tab_Dokv_030 - Zugriffsunterbindungsregeln].

2696 **5.3.35.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln**

2697 Die Dokumentenverwaltung setzt die oben beschriebenen Berechtigungsvorgaben über
 2698 zwei Mechanismen durch:

- 2699 1. Dynamische Berechtigungs freigaben (wie z. B. die Entscheidung, welche LEI
 2700 überhaupt vom Versicherten berechtigt werden, in welcher Stufe, welchen
 2701 Kategorien und mit welchen Ausnahmen) werden vom über "Policies" in die
 2702 Dokumentenverwaltung eingestellt oder auch gelöscht.
- 2703 2. Unabänderliche Regeln (wie die gesetzlich motivierten Vorgaben für
 2704 Berufsgruppen) werden über entsprechende AFOs realisiert, insbesondere
 2705 A_19303. Es ist natürlich umsetzender Software möglich, auch diese Regeln über
 2706 interne Policies durchzusetzen.

2707 Beide Mechanismen setzen bei der Durchsetzung an den XDS-Metadaten an, mit denen
 2708 alle Dokumente grundsätzlich gekennzeichnet werden.

2709 Die grobgranulare Dokumentenfreigabe wird über über das XDS-Metadatum
 2710 DocumentEntry.confidentialityCode umgesetzt, das die Vertraulichkeitsstufe des
 2711 Dokuments festlegt. Dazu stehen folgende Codes (unter dem Code System Name
 2712 "Confidentiality") zur Verfügung :

- 2713 • Code = "N", Display Name = "normal"
- 2714 • Code = "R", Display Name = "vertraulich"
- 2715 • Code = "V", Display Name = "streng vertraulich"

2716 Mittelgranulare Berechtigungen (kategoriebasiert) werden über verschiedene
 2717 Metadaten(kombinationen) umgesetzt. Die Details sind A_19388 (gemSpec_DM_ePA)
 2718 oder auch direkt den Policies in Anhang C zu entnehmen.

2719 Feingranulare Berechtigungen, d.h. Freigabe oder Sperren einzelner Dokumente, erfolgt
2720 über die Auflistung von DocumentEntry.uniqueId-Kennzeichnern in einer White- bzw.
2721 Blacklist.

2722 **5.3.45.4.4 Vergabe von Zugriffsregeln**

2723 Der Versicherte und sein Vertreter können Berechtigungen aller Art (d.h. grob-, mittel-
2724 und feingranular für alle Zugriffsgruppen) entweder über das ePA-Frontend des
2725 Versicherten oder am KTR-AdV-Terminal in der Kostenträgerumgebung mittels dort zur
2726 Verfügung stehender ePA-FdV AdV vergeben.

2727 Darüberhinaus können LEI über eine Adhoc-Berechtigung beim LEI vor Ort grob- und
2728 mittelgranular berechtigt werden.

2729 Alle erteilten Zugriffsrechte werden zeitlich begrenzt vergeben. Die Dauer wird für jede
2730 einzelne Rechtevergabe vom Versicherten festgelegt und beträgt maximal 540 Tagekann
2731 zeitlich befristet oder unbefristet vergeben werden.

2732

2733

2734

2735 **5.3.55.4.5 Funktionsprinzip Policy Administration**

2736 Die Berechtigungsvergabe an Leistungserbringerinstitutionen und Vertreter des
2737 Versicherten erfolgt durch das Einstellen von Policy Documents (siehe nachstehende
2738 Abbildung). Diese Dokumente werden in den Abschnitten 5.34.6.2 bis 5.34.6.5 für die
2739 ePA-Fachanwendung definiert und setzen ferner das Zugriffskontrollmodell Attribute-
2740 based Access Control (ABAC) um.

2741 Die Registrierung dieser sogenannten Advanced Patient Privacy Consents erfolgt als
2742 unverschlüsselte Dokumente (jedoch über die sichere Verbindung zwischen dem
2743 Fachmodul ePA bzw. dem ePA-Modul Frontend des Versicherten und dem
2744 Verarbeitungskontext) durch Nutzung der IHE ITI-Transaktionen "Cross-Gateway
2745 Document Provide" [ITI-80] sowie "Provide And Register Document Set-b" [ITI-41]. Die
2746 interne Datenhaltung bzgl. der Policy Documents (Advanced Patient Privacy Consents) ist
2747 nicht vorgegeben, allerdings müssen diese Policy Documents über die Standard-
2748 Abfrageschnittstelle über
2749 die Operation `I_Document_Management_Insurant::RegistryStoredQuery` dem ePA-
2750 Modul Frontend des Versicherten zugänglich gemacht werden. Dazu werden die
2751 DocumentEntry-Metadaten gemäß der Anforderung [gemSpec_DM_ePA#A_14961]
2752 vorgegeben.

2753

2754 Die grundlegende Zugriffsstrategie ist "opting-in", sodass ein gewährendes Zugriffsrecht
2755 nur durch Registrierung eines neuen Policy Documents vergeben werden kann. Eine
2756 inhaltliche Änderung eines Policy Documents ist nicht vorgesehen. Stattdessen soll durch
2757 den Client ein zu einem Berechtigten vorhandenes Policy Document gelöscht und ein
2758 neues registriert werden. Wurde ein vorhandenes Policy Document, das demselben
2759 Berechtigten zuzuordnen ist (d.h. `xacml:SubjectMatch`, `xacml:ResourceMatch` sind
2760 identisch), durch den Client nicht gelöscht, wird dieses von der ePA-
2761 Dokumentenverwaltung automatisch gelöscht, während das neue Policy Document
2762 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-Metadaten löschen, bevor ein neues Policy Document gespeichert wird. [\leq]

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

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

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

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

Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Policy Documents (Advanced Patient Privacy Consents) gegen Veränderung und unberechtigtes Löschen geschützt sind. [\leq]

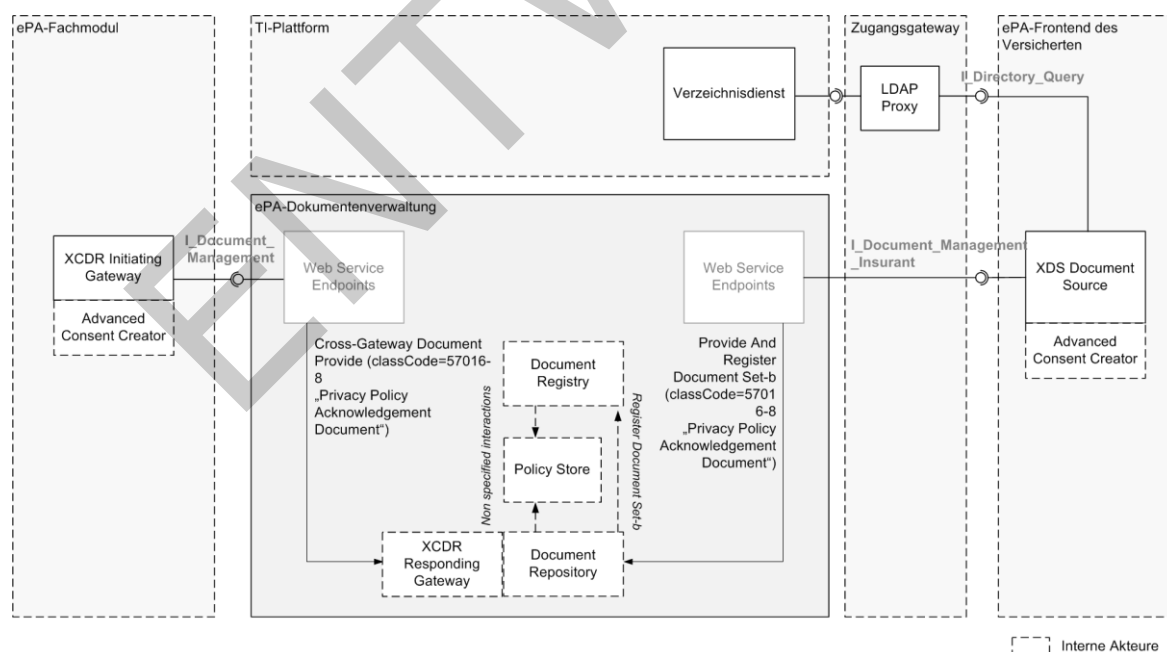


Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen

2793 *Hinweis: Die vorstehende Abbildung verdeutlicht, wie Berechtigungen über die*
2794 *entsprechenden IHE ITI-Transaktionen vergeben werden. Der Transaktion "Cross-*
2795 *Gateway Document Provide" liegt genaugenommen keine IHE ITI-konforme Nachricht*
2796 *des Primärsystems zum Einstellen des Policy Documents durch den Versicherten*
2797 *zugrunde. Stattdessen wird diese Transaktion durch die Web-Service-Operation*
2798 *"RequestFacilityAuthorization" gemäß [\[gemSpec FM ePA#7.2.1.2\]](#) ausgelöst, sodass*
2799 *sich die Verwendung der Transaktion "Cross-Gateway Document Provide"*
2800 *eigentlich verbietet. Aus Praktikabilitätsgründen ist jedoch keine separate Schnittstelle*
2801 *mit der Transaktion "Provide And Register Document Set-b" für die*
2802 *Schnittstelle `I_Document_Management` zum Einstellen eines Policy Documents gegenüber*
2803 *der ePA-Dokumentenverwaltung definiert.*

2804 Der Entzug von Berechtigungen erfolgt über das Löschen von ausgewählten Policy
2805 Documents durch Ausführung der
2806 Operation `I_Document_Management_Insurant::RemoveDocumentsRemoveMetadata`, wie
2807 die folgende Abbildung verdeutlicht.

2808

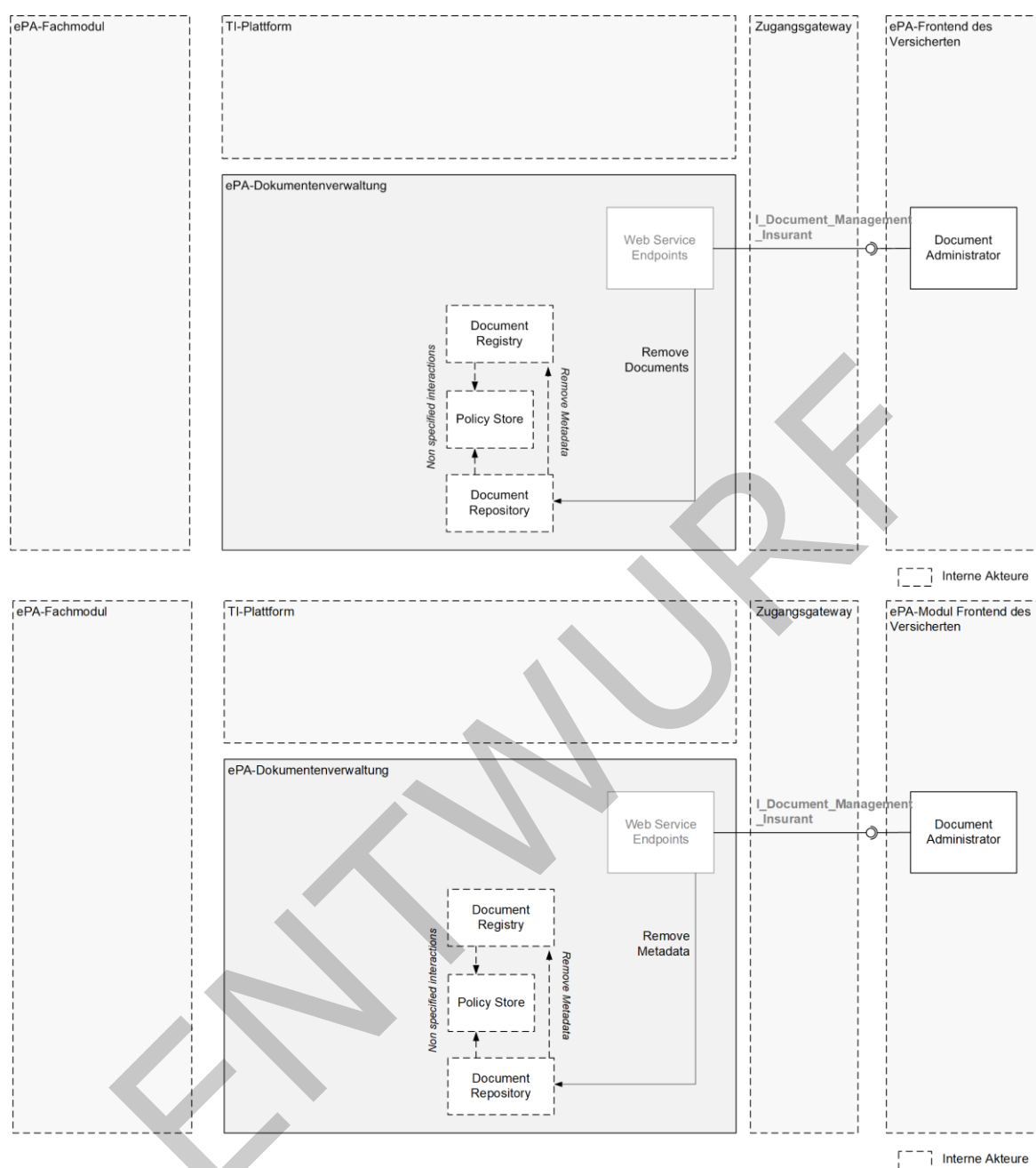


Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen

5.3-65.4.6 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 19303-02A-19303 - Komponente ePA-Dokumentenverwaltung – Berufgruppenspezifische Zugriffsunterbindungsregeln

Die Komponente ePA-Dokumentenverwaltung MUSS alle in der Tabelle Tab_Dokv_030 - Zugriffsunterbindungsregeln aufgeführten berufsgruppenspezifischen

2821 Zugriffsunterbindungsregeln durchsetzen. Die Komponente ePA-Dokumentenverwaltung
 2822 MUSS dazu beim Aufruf einer der Operationen der Schnittstelle
 2823 I_Document_Management die übergebene AuthenticationAssertion dahingehend
 2824 prüfen, ob die ProfessionOID der ZertifikatsExtension Admission gemäß
 2825 [gemSpec_PKI#Anhang A] im Signaturzertifikat C.HCI.OSIG
 2826 (/saml2:Assertion/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate) für
 2827 die Operation, ausgeführt auf eine bestimmte Dokumentenkategorie, zugriffsberechtigt
 2828 ist. Das Ausführen von Operationen auf Dokumentenkategorien, die nicht explizit erlaubt
 2829 sind, muss verhindert werden ("Access Deny").
 2830

2831 **Tabelle 28: Tab_Dokv_030 - Zugriffsunterbindungsregeln**

Dokumentenkategorie ge mäß § 341 PDSG Absatz 2		Zugriffsrecht										
Nr.	Technischer Identifier aus [gemSpec_DM# Tab_DM_Dokumente nkategorie]	Arzt	ZArzt	Ap o	Psy ch	Pfle ge	He ba	Phys	GD	AM	KT R	Ver
1a 1	category_1a1practitioner	CR UD	CR UD	R	CR UD	R	R	R UD	CRU D-	-R	-	RD
1a 2	category_1a2hospital	CR UD	CR UD	R	CR UD	R	R	R UD	CRU D-	-R	-	RD
1a 3	category_1a3laboratory	CR UD	CR UD	R	CR UD	R	R	R UD	CRU D-	-R	-	RD
1a 4	category_1a4physiotherapy	CR UD	CR UD	R	CR UD	R	R	CRU D	CRU D-	-R	-	RD
1a 5	category_1a5psychotherapy	CR UD	CR UD	R	CR UD	R	R	R UD	CRU D-	-R	-	RD
1a 6	category_1a6dermatology	CR UD	CR UD	R	CR UD	R	R	R UD	CRU D-	-R	-	RD
1a 7	category_1a7gynaecology urology	CR UD	CR UD	R	CR UD	R	R	R UD	CRU D-	-R	-	RD
1a 8	category_1a8dentistry oms	CR UD	CR UD	R	CR UD	R	R	R UD	CRU D-	-R	-	RD
1a 9	category_1a9other medical	CR UD	CR UD	R	CR UD	R	R	R UD	CRU D-	-R	-	RD
1a 10	category_1a10other non medical	CR UD	CR UD	R	CR UD	R	R	R UD	- CRU D	-R	-	RD

1b	category__emp	CR UD	CR UD	CR UD	CR UD	R	R	R	- <u>CRU</u> <u>D</u>	-R	-	RD
1c	category__nfd	CR UD	CR UD	R	CR UD	R	R	R	- <u>CRU</u> <u>D</u>	-R	-	RD
1d	category__eab	CR UD	CR UD	R	CR UD	R	R	R	- <u>CRU</u> <u>D</u>	-R	-	RD
2	category__dentalrecor d	CR UD	CR UD	-	CR UD	-R	-	-	- <u>CRU</u> <u>D</u>	-R	-	RD
3	category__childsrecor d	CR UD	CR UD	R	CR UD	R	CR UD	R	R CR UD	-R	-	RD
4	category__mothersrec ord	CR UD	CR UD	R	CR UD	R	CR UD	R	- <u>CRU</u> <u>D</u>	-R	-	RD
5	category__vaccination	CR UD	CR UD	CR UD	CR UD	R	R	-	CRU D	CR UD	-	RD
6	category__patientdoc	RD	RD	R	RD	R	R	R	-RD	-R	-	CR UD
7	category__ega	RD	RD	R	RD	R	R	R	-RD	-R	€ U	CR UD
8	category__receipt	RD	RD	RD	RD	R	R	R	-RD	-R	C U	RD
10	category__care	CR UD	CR UD	R	CR UD	CR UD	R	R	- <u>CRU</u> <u>D</u>	-R	-	RD
11	category__prescription	CR UD	CR UD	CR UD	CR UD	R	R	R	- <u>CRU</u> <u>D</u>	-R	-	RD
12	category__eau	CR UD	CR UD	-	CR UD	-	-	-	- <u>CRU</u> <u>D</u>	-R	-	RD
13	category__other	CR UD	CR UD	-	CR UD	-	-	-	- <u>CRU</u> <u>D</u>	-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::RemoveDocumentsRemoveMetadata, I_Document_Management_Insurant::RemoveDocumentsRemoveMetadata;
- -=keine Zugriffsrechte;

Legende der Institutionen, Zuordnung zur ProfessionOID:

- Arzt=oid_praxis_arzt, oid_krankenhaus, oid_vorsorge_reha, oid_sanitaetsdienst_bundeswehr;
- ZArzt=oid_zahnarztpraxis;
- Apo=oid_öffentliche_apotheke;
- Psych=oid_praxis_psychotherapeut;
- Pflege=oid_institution_pflege;
- Heba=oid_geburtshilfe;
- Phys=oid_praxis_physiotherapeut;
- GD=oid_gesundheitsdienst;
- AM=oid_arbeitsmedizin;
- KTR=oid_kostentraeger_eпа ktr;

Legende Zugriffsberechtigte, Zuordnung über KVNR:

- Ver=Versicherter/Vertreter;

[<=]

A 15173-03A-15173-02 - 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 ~~und~~, A_19998 oder A_20736 explizit erlaubt ist. [<=]

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.

[<=]

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 berechnigte 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 7 und 8 zugreifen, und zwar nach Tabelle ausschließlich mittels C-Operation (create), 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::RemoveDocumentsRemoveMetadata) durch Tab_Dokv_030.

Beispiel 2: Ein Leistungserbringer ist nur auf ein einziges Dokument berechnigt (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 Berechnigung "C" oder "U" besitzt. Letzteres Recht ist ihm auch nicht zu entziehen (außer über den kompletten Entzug der Berechnigung über Löschen der Policy).

Policy Documents, welche die Berechnigung 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
A_19997 - Zugriff durch Versicherten auf Schnittstelle I_Account_Management_Insurant
 Die Komponente ePA-Dokumentenverwaltung MUSS dem Versicherten über A_15173-02 hinaus den Zugriff auf die Operationen der Schnittstelle-Schnittstellen I_DocumentAccount_Management_Insurant und I_Key_Management_Insurant erlauben. [\leq]

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() erlauben. [\leq]

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 400 gemäß [RFC7231] quittieren.[<=]

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 400 gemäß [RFC7231] quittieren:

- *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 5.34.6.2 bis 5.34.6.5 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 KVNR kennzeichnen).
- *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.

[<=]

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>

[<=]

A_16195 - Komponente ePA-Dokumentenverwaltung – UTF-8-Kodierung eines Policy Documents

Die Komponente ePA-Dokumentenverwaltung MUSS ausschließlich UTF-8-kodierte Policy Documents verarbeiten. [<=]

5.3.6.15.4.6.1 Erstmaliges Öffnen eines Verarbeitungskontextes

Beim erstmaligen Öffnen des Verarbeitungskontextes eines neu registrierten Aktenkontos durch den Versicherten muss dieser erkennen, dass er erstmalig geöffnet wird und die Aktenzustände "Registered" und "Registered for Migration"

2991 gemäß [\[gemSpec_AktenSystem#6.1.1\]](#) unterscheiden. Darüber hinaus ist der
2992 Verarbeitungskontext für den Versicherten gemäß der Anforderung A_15250 zu
2993 personalisieren. Die für die Personalisierung und die Unterscheidung der Aktenzustände
2994 erforderliche Konfiguration des Verarbeitungskontextes für das Aktenkonto erfolgt über
2995 die Authorization Assertion.

2996 **A_15603 - Komponente ePA-Dokumentenverwaltung – Nur Resume Account**
2997 **bei erforderlicher Datenübernahme möglich**

2998 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass ausschließlich die
2999 Operation `I_Account_Management_Insurant::ResumeAccount` ausgeführt werden kann,
3000 wenn der Verarbeitungskontext erstmalig vom Versicherten geöffnet wurde und eine
3001 Übernahme von Daten aus dem Aktenkonto des Versicherten bei einem vorherigen
3002 Anbieter erforderlich ist, d.h. das Aktenkonto mit der Option "Registered for Migration"
3003 registriert wurde. [`<=`]

3004 **[5.3.6-25.4.6.2](#) Berechtigung für einen Versicherten**

3005 **A_15437-01 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben**
3006 **zum Inhalt eines Policy Documents zur Berechtigung eines Versicherten**

3007 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS eine
3008 XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-
3009 ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_500 in
3010 Anhang C durchsetzen. [`<=`]

3011 Um dem Versicherten Zugriff auf seine Akte zu gewähren, wird die Akte im Zuge ihrer
3012 Erstbenutzung durch den Versicherten personalisiert und ein Versicherten-Policy-
3013 Document erstellt bzw. aktiviert.

3014 **A_15250 - Komponente ePA-Dokumentenverwaltung – Aktivierung des Policy**
3015 **Documents "urn:gematik:policy-set-id:insurant"**

3016 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS eine
3017 Personalisierung durchführen. Dazu MUSS die Komponente ePA-Dokumentenverwaltung
3018 das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set
3019 ID "urn:gematik:policy-set-id:insurant" aktivieren und anschließend die darin
3020 festgelegten Regeln bei Zugriffsanfragen durchsetzen. Der Verarbeitungskontext der
3021 Komponente ePA-Dokumentenverwaltung MUSS die Personalisierung im Zuge des ersten
3022 Aufrufs einer fachlichen Operation durchführen und das Policy Document unmittelbar auf
3023 die fachliche Operation anwenden, die die Personalisierung ausgelöst hat. Der Aufruf
3024 der Operation `I_Document_Management_Connect::OpenContext` zur kryptographischen
3025 Aktivierung gilt in diesem Zusammenhang nicht als fachliche Operation. [`<=`]

3026 Die Festlegung des Zeitpunkts der Personalisierung in der vorstehenden Anforderung
3027 verhindert die Personalisierung eines Verarbeitungskontexts für den Fall, dass für ein mit
3028 der Option "Registered for Migration" registriertes Aktenkonto der Verarbeitungskontext
3029 geöffnet wird, ohne dass unmittelbar anschließend die

3030 ~~Operation~~ [Operation I_Account_Management_Insurant::ResumeAccount](#) aufgerufen
3031 wird. Der Verarbeitungskontext verbleibt damit in seinem initialen (d.h. ungenutzten)
3032 Zustand, so dass der Vorgang konsistent neu gestartet werden kann.

3033 **A_15178 - Komponente ePA-Dokumentenverwaltung – Unveränderliches Policy**
3034 **Document "urn:gematik:policy-set-id:insurant"**

3035 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass das Policy
3036 Document (Advanced Patient Privacy Consent) mit der Policy Set
3037 ID "urn:gematik:policy-set-id:insurant" nach ihrer Aktivierung kontinuierlich und
3038 dauerhaft unverändert für die Zugriffskontrollprüfung wirksam ist. [`<=`]

5-3-6-35.4.6.3 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]

5-3-6-45.4.6.4 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. [\leq]

5-3-6-55.4.6.5 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. [\leq]

5-3-75.4.7 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.

[<=]

A_20049-01A_20049 - 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:

- Das Ablaufdatum MUSS übernommen werden.
- Bei der Ersetzung der XACML 2.0 Policies ohne Versionsangabe (alt) durch XACML 2.0 Policies mit Versionsangabe (neu) MÜSSEN folgende Zugriffsregeln umgesetzt werden (Zugriffsrecht alt wird zu Zugriffsrecht neu):
 - alt: LEI, neu: category_treatment*, category_practitioner, hospital, laboratory, physiotherapy, psychotherapy, dermatology, gynaecology urology, dentistry oms, other medical, other non medical, emp, category_nfd, category_eab;
 - alt: PAT, neu: category_patientdoc;
 - alt: KTR, neu: category_receipt;
 - neu: Die Vertrauensstufe "normal" (grobgranulare Berechtigung) wird vergeben

[<=]

A_20046 - Komponente ePA-Dokumentenverwaltung – Transformation des confidentialityCodes bei eingestellten Dokumenten

Die Komponente ePA-Dokumentenverwaltung MUSS bei allen Dokumenten eines Versicherten, bei denen der confidentialityCode "PAT", "LEI", "LEÄ" oder "KTR" gesetzt ist, diesen Eintrag löschen und stattdessen den confidentialityCode "normal" setzen. Diese Transformation MUSS durch die Komponente ePA-Dokumentenverwaltung nach dem ersten erfolgreichen Öffnen der Akte des Versicherten (Operation I_Document_Managemet_Connect::OpenContext()) und nachfolgend beim Einstellen jedes DocumentEntry, der noch alte confidentialityCodes enthält, durchgeführt werden.

[<=]

Damit soll die Transformation zum frühestmöglichen Zeitpunkt durch die ePA_Dokumentenverwaltung durchgeführt werden.

A_20050-01A_20050 - Komponente ePA-Dokumentenverwaltung – Abbildung von Suchanfragen nach confidentialityCodes und deren Ergebnisse

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS bei Aufruf der Operation `I_Document_Management::CrossGatewayQuery` mit Suchparametern zum `confidentialityCode` "LEI", "PAT" oder "KTR" die Suche stattdessen auf die folgenden Kategorien abbilden (alt: eingehende Suchanfrage, neu: durchsuchte Kategorien) und entsprechende Ergebnisse zurückliefern:

- alt: LEI, neu: `category_la*`, `category_practitioner`, `hospital`, `laboratory`, `physiotherapy`, `psychotherapy`, `dermatology`, `gynaecology`, `urology`, `dentistry`, `oms`, `other medical`, `other non medical`, `emp`, `category_nfd`, `category_eab`;
- alt: PAT, neu: `category_patientdoc`;
- alt: KTR, neu: `category_receipt`;

[<=]

Etwaige Berechtigungsregeln, die der Herausgabe einzelner Dokumente an den Client entgegenstehen (z. B. Blacklisting einzelner Dokumente oder nichterteilte Zugriffsberechtigung auf `category_emp`) müssen dabei weiterhin berücksichtigt werden.

5.45.5 Vertrauenswürdige Ausführung

5.4.15.5.1 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-Modul 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-Moduls Frontend 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_15592-01 - Komponente ePA-Dokumentenverwaltung – Erweiterung des sicheren Verbindungsprotokolls

Ein Client (d.h. ePA-Fachmodul, ePA-Modul 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 - 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-Moduls Frontends 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 ePA sowie des Fachmoduls ePA KTR-Consumer verfügbar machen.

[<=]

A_15588 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext bei Bedarf verfügbar machen

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS Verarbeitungskontexte bedarfsgesteuert für autorisierte Nutzer verfügbar machen. [<=]

[A_14633-02A_14633](#) - Komponente ePA-Dokumentenverwaltung – Vermittlung der Verbindung zwischen Client und Verarbeitungskontext

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die Verbindung zwischen Client, d.h. dem ePA-Modul Frontend des Versicherten bzw. dem Fachmodul ePA oder Fachmodul ePA KTR-Consumer, und Verarbeitungskontext vermitteln und dabei

- die Base64-dekodierte Authorization Assertion der `VAUClientHello`-Nachricht auf Gültigkeit gemäß Anforderung [A_13690](#) sowie auf den gültigen Berechtigungstyp (`AuthorizationType = "DOCUMENT_AUTHORIZATION"`) prüfen und bei ungültiger Authorization Assertion den Verbindungsaufbau abbrechen und mit dem HTTP-Fehler 403 antworten,
- den Record Identifier des Verarbeitungskontextes über den Wert des Attributs `Resource ID` aus der Authorization Assertion der `VAUClientHello`-Nachricht ermitteln,
- für Clients vom Typ ePA-Modul Frontend des Versicherten die Verbindung auf der Grundlage des vom Zugangsgateway gesetzten HTTP Header-Feldes `Session` registrieren,
- für Clients vom Typ Fachmodul ePA die Verbindung auf Grundlage der TLS-Sitzung ([Session-ID](#)) oder auf Grundlage der [KeyID des VAU-Kanals \[gemSpec Krypt\]](#) (mit der Ausnahme, dass im Rahmen des Handshakes `VAUClientHelloDataHash` zur Zuordnung des Verarbeitungskontext verwendet wird), registrieren,
- während der Dauer der Sitzung alle eingehenden Requests auf der Grundlage der registrierten Verbindung an den Zielverarbeitungskontext weiterleiten sowie

- nach dem Ende der Sitzung, aufgrund eines Timeouts bzw. aufgrund einer Beendigung durch den Nutzer, die Registrierung der Verbindung löschen.

[<=]

A_20580 - Komponente ePA-Dokumentenverwaltung – TLS Session Resumption mittels Session-ID nutzen

Falls die Komponente ePA-Dokumentenverwaltung im Kontextmanagement die Vermittlung der Verbindung zwischen Client und Verarbeitungskontext für Clients vom Typ Fachmodul ePA die Verbindung auf Grundlage der TLS-Sitzung verwendet, MUSS die Komponente ePA-Dokumentenverwaltung TLS Session Resumption mittels Session-ID gemäß RFC 5246 nutzen. Dadurch wird sichergestellt dass, für den wiederholten Aufbau von TLS-Verbindungen die bereits ausgehandelten Session-Parameter genutzt werden.

[<=]

A_14617-01 - Komponente ePA-Dokumentenverwaltung – Ablauf des Verbindungsaufbaus

Die Komponente ePA-Dokumentenverwaltung MUSS den Verbindungsaufbau von Clients, d.h. von einem ePA-Modul Frontend des Versicherten oder einem Fachmodul so umsetzen, dass der folgende Ablauf in angegebener Reihenfolge ausgeführt wird, nachdem ein HTTP Request mit einer VAUClientHello-Nachricht von einem Client empfangen wurde:

Tabelle 29: 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

		VAU_ServerHello-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
7	Verarbeitungskontext	Senden der VAU_ServerHello-Nachricht
8	Kontextmanagement	Weiterleiten der VAU_ServerHello-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 VAU_ClientSigFin-Nachricht)
10	Kontextmanagement	Weiterleiten der VAU_ClientSigFin-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 VAU_ServerError-Nachricht beantwortet werden.
12	Verarbeitungskontext	Erzeugen der VAU_ServerFin-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
13	Kontextmanagement	Weiterleiten der VAU_ServerFin-Nachricht an den Client

3241 [**<=**]

3242 Der abgeleitete Sitzungsschlüssel wird anschließend vom Client und vom
3243 Verarbeitungskontext gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6] genutzt,
3244 um alle fachlichen Eingangs- und Ausgangsnachrichten zu ver- und entschlüsseln.

3245 [A_14545-02 - Komponente ePA-Dokumentenverwaltung – Operationen des](#)
3246 [Dokumenten-, Konto- und Schlüsselmanagements nur über sicheren Kanal](#)

3247 ~~[A_14545-01 – Komponente ePA-Dokumentenverwaltung – Operationen des](#)~~
3248 ~~[Dokumentenmanagements nur über sicheren Kanal nutzbar](#)~~Der

3249 Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die folgenden
3250 Operationen ausschließlich über den sicheren Kanal zwischen dem ePA-Modul Frontend
3251 des Versicherten bzw. dem Fachmodul ePA und dem Verarbeitungskontext verfügbar
3252 machen:

- 3253
- I_Document_Management::CrossGatewayDocumentProvide
- 3254
- I_Document_Management::CrossGatewayQuery
- 3255
- I_Document_Management::~~RemoveDocuments~~[RemoveMetadata](#)

- 3256 • I_Document_Management::CrossGatewayRetrieve
- 3257 • I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- 3258 • I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- 3259 • I_Document_Management_Insurant::RestrictedUpdateDocumentSet
- 3260 • I_Document_Management_Insurant::RegistryStoredQuery
- 3261 • I_Document_Management_Insurant::~~RemoveDocuments~~RemoveMetadata
- 3262 • I_Document_Management_Insurant::RetrieveDocumentSet
- 3263 • I_Account_Management_Insurant::GetAuditEvents
- 3264 • I_Account_Management_Insurant::SuspendAccount
- 3265 • I_Account_Management_Insurant::ResumeAccount
- 3266 • I_Key_Management_Insurant::StartKeyChange
- 3267 • I_Key_Management_Insurant::GetAllDocumentKeys
- 3268 • I_Key_Management_Insurant::PutAllDocumentKeys
- 3269 • I_Key_Management_Insurant::FinishKeyChange
- 3270 • I_Document_Management_Connect::OpenContext
- 3271 • I_Document_Management_Connect::CloseContext

Weiterhin MUSS der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung bei sämtlichen genannten Operationen (bis auf Open Context und Close Context) prüfen, ob das Subjekt der übergebenen Authentication Assertion mit dem der registrierten Authorization Assertion übereinstimmt und im Fehlerfall eine `VAUServerError`-Nachricht mit HTTP-Fehler 403 (Fehlermeldung "Access Denied") gemäß [gemSpec_Krypt#6.9] returnieren. [≤]

A_14645 - Komponente ePA-Dokumentenverwaltung – Nutzung des sicheren Kanals zwischen ePA-Modul Frontend des Versicherten bzw. Fachmodul ePA, Fachmodul ePA KTR-Consumer und Verarbeitungskontext

Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS den mit dem ePA-Modul Frontend des Versicherten bzw. mit dem Fachmodul ePA sowie dem Fachmodul ePA KTR-Consumer gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6] ausgehandelten Sitzungsschlüssel verwenden, um alle Eingangsnachrichten zu entschlüsseln und alle Ausgangsnachrichten zu verschlüsseln. [≤]

A_14457 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management_Connect

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

3293 **Tabelle 30: 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	

3294 [**<=**]3295 **5.4.1.15.5.1.1 Operation**3296 **I_Document_Management_Connect::OpenContext**3297 **A_14426 - Komponente ePA-Dokumentenverwaltung – Signatur für**3298 **I_Document_Management_Connect::OpenContext**

3299 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

3300 I_Document_Management_Connect::OpenContext gemäß der folgenden Signatur

3301 implementieren:

3302 **Tabelle 31: 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_AUT_KEY	Der Kontextschlüssel ist ungültig.	Wenn der Vergleich mit einem bereits im Verarbeitungskontext vorhandenen Kontextschlüssel keine Übereinstimmung ergibt, oder das Entschlüsseln von Kontextdaten fehlschlägt	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	

3303 [\leq]3304 [5.4.1.1.15.5.1.1.1](#) Umsetzung

3305 **A_14687 - Komponente ePA-Dokumentenverwaltung – Ablauf der Operation**

3306 **Open Context**

3307 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

3308 `I_Document_Management_Connect::OpenContext` so umsetzen, dass nach einem Aufruf

3309 der Operation durch einen Client, d.h. durch ein ePA-Modul Frontend des Versicherten,

3310 ein Fachmodul ePA oder ein Fachmodul ePA KTR-Consumer, der folgende Ablauf in

3311 angegebener Reihenfolge (1 - 6) ausgeführt wird:

3312 **Tabelle 32: 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	<p>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.</p> <p>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 <code>INVALID_AUT_KEY</code> abgebrochen.</p>
5	Verarbeitungskontext	Senden der <code>OpenContextResponse</code> -Nachricht
6	Kontextmanagement	Weiterleiten der <code>OpenContextResponse</code> -Nachricht an den Client

3313 [`<=`]

3314 Der Verarbeitungskontext ist anschließend für die Verarbeitung von fachlichen
 3315 Operationen bereit.

3316 **5.4.1-25.5.1.2 Operation**3317 **I_Document_Management_Connect::CloseContext**3318 **A_14462 - Komponente ePA-Dokumentenverwaltung – Signatur für**3319 **I_Document_Management_Connect::CloseContext**

3320 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

3321 `I_Document_Management_Connect::CloseContext` gemäß der folgenden Signatur
 3322 implementieren:

3323 **Tabelle 33: 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	

3324 [**<=**]3325 [5.4.1.2-15.5.1.2.1](#) Umsetzung3326 **A_14707-01 - Komponente ePA-Dokumentenverwaltung – Ablauf der Operation**
3327 **Close Context**

3328 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

3329 I_Document_Management_Connect::CloseContext so umsetzen, dass nach einem Aufruf

3330 der Operation durch einen Client, d. h. durch ein ePA-Modul Frontend des Versicherten,

3331 ein Fachmodul ePA oder ein Fachmodul ePA KTR-Consumer, der folgende Ablauf in

3332 angegebener Reihenfolge (1 - 6) ausgeführt wird:

3333 **Tabelle 34: 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

3334 [`<=`]3335 **5.4.25.5.2 Hardware-Merkmale**

3336 Die Vertrauenswürdige Ausführungsumgebung setzt die Nutzung eines HSM zur
 3337 Speicherung und Anwendung der privaten Schlüssel von Dienstzertifikaten und
 3338 Schlüsselpaaren gemäß Anforderung A_14564 voraus.

3339 **5.55.6 Statische Akteninhalte**

3340 Statische Inhalte werden vor der ersten echten Nutzung der Akte angelegt, d.h. bevor
 3341 auf Akteninhalte zugegriffen wird. Sie sind (mit wenigen Ausnahmen) unveränderlich.

3342 **A_20191 - Komponente ePA-Dokumentenverwaltung – Anlegen von statischen**
 3343 **Ordern**

3344 Die Komponente ePA-Dokumentenverwaltung MUSS nach dem ersten erfolgreichen
 3345 Öffnen der Akte des Versicherten (`Operation`
 3346 `I_Document_Managemet_Connect::OpenContext()`) die folgenden Ordner für den
 3347 Versicherten anlegen:
 3348

- 3349 • ~~Kategorie 1a-Ordner~~Kategorienordner, jeweils einen pro Kategorie 1a*
 3350 gemäß gemSpec_DM_ePA#A_20190-
 3351 01_gemSpec_DM_ePA#A_20190 (Belegung `Folder.codeList`) unter Berücksichtigung
 3352 allgemeiner Vorgaben für Folder-Metadaten in gemSpec_DM_ePA#A_14760-01 (Belegung
 3353 der restlichen Metadatenfelder).

- 3354 • ~~Kategorie "eGA"-Ordner~~gemSpec_DM_ePA#A_20190 (Belegung `Folder.codeList`)

Alle statischen Ordner sind nach dem Anlegen initial leer. [≤]

A_20214 - Komponente ePA-Dokumentenverwaltung – Anlegen von Permission Policies

Die Komponente ePA-Dokumentenverwaltung MUSS nach dem ersten erfolgreichen Öffnen der Akte des Versicherten (`Operation`

`I_Document_Managemet_Connect::OpenContext()`) alle in Abschnitt 9.5 aufgeführten

Permission Policies für den Versicherten anlegen. [≤]

A_20215 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe von Permission Policies

Die Komponente ePA-Dokumentenverwaltung DARF statische Policy-Dokumente (Advanced Patient Privacy Consent) gemäß Abschnitt 9.5 NICHT über Suchoperationen dem ePA-Frontend des Versicherten zur Verfügung stellen. Ferner MUSS die Komponente ePA-Dokumentenverwaltung ein Herunterladen verhindern. [≤]

A_20216 - Komponente ePA-Dokumentenverwaltung – Unveränderlichkeit von statischen Akteninhalten

Die Komponente ePA-Dokumentenverwaltung DARF die Metadaten eines statischen Aktenobjekts nach Abschnitt 5.56 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen. Dabei gelten folgende Ausnahmen:

- `Folder.lastUpdateTime`

[≤]

`Folder.lastUpdateTime` wird automatisch von der Dokumentenverwaltung aktualisiert, sobald Dokumente in den Ordner eingestellt oder daraus gelöscht werden, siehe auch [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6].

3379

6 Informationsmodelle

3380 Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten
3381 wird nicht benötigt.

ENTWURF

3382

7 Anhang A – Verzeichnisse

3383

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 ProfileProfileGetAllDocumentKeys
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	15
Abbildung 2: Schematische Darstellung zur Vergabe von Berechtigungen	103
Abbildung 3: Schematische Darstellung zum Entzug von Berechtigungen	105
Abbildung 1: Komponentenzerlegung ePA-Dokumentenverwaltung	15
Abbildung 2 Zustandsübergänge Schlüsselwechsel	87
Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen	103
Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen	105

7.4 Tabellenverzeichnis

Tabelle 1: Tab_Dokv_10 – Kennzeichnung von Optionalitäten	24
Tabelle 2: Tab_Dokv_11 – Übersicht über gruppierte IHE ITI Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung	24
Tabelle 3: Tab_Dokv_12 – Fehlercodes zu Fehlern gemäß Operationsdefinition	31
Tabelle 4: Tab_Dokv_35 – Eingangsparameter für TUC_PKI_018	38
Tabelle 5: Tab_Dokv_13 – Parameter des § 291a-Protokolls	41
Tabelle 6: Tab_Dokv_14 – Schnittstelle I_Document_Management	49
Tabelle 7: Tab_Dokv_16 – Operation Cross-Gateway Query	53
Tabelle 8: Tab_Dokv_17 – Operation Remove Documents	56
Tabelle 9: Tab_Dokv_18 – Operation Cross-Gateway Retrieve	57
Tabelle 10: Tab_Dokv_20 – Schnittstelle I_Document_Management_Insurant	59
Tabelle 11: Tab_Dokv_21 – Operation Provide And Register Document Set b	60
Tabelle 12: Tab_Dokv_22 – Operation Registry Stored Query	62
Tabelle 13: Tab_Dokv_23 – Operation Remove Documents	66
Tabelle 14: Tab_Dokv_24 – Operation Retrieve Document Set	68

3412	Tabelle 15: Tab_Dokv_19—Operation RestrictedUpdateDocumentSet	70
3413	Tabelle 16: Tab_Dokv_36—Schnittstelle I_Document_Management_Insurance	73
3414	Tabelle 17: Tab_Dokv_37—Operation Provide And Register Document Set b	74
3415	Tabelle 18: Tab_Dokv_25—Schnittstelle I_Account_Management_Insurant	77
3416	Tabelle 19: Tab_Dokv_26—Operation Suspend Account	77
3417	Tabelle 20: Tab_Dokv_27—Operation Resume Account	81
3418	Tabelle 21: Tab_Dokv_28—Operation Get Audit Events	84
3419	Tabelle 22 : Tab_Dokv_030—Zugriffsunterbindungsregeln	106
3420	Tabelle 23: Tab_Dokv_29—Ablauf Operation Hello	117
3421	Tabelle 24: Tab_Dokv_30—Schnittstelle I_Document_Management_Connect	120
3422	Tabelle 25: Tab_Dokv_31—Operation OpenContext	120
3423	Tabelle 26: Tab_Dokv_32—Ablauf der Operation Open Context	121
3424	Tabelle 27: Tab_Dokv_33—Operation Close Context	123
3425	Tabelle 28: Tab_Dokv_34—Ablauf Operation CloseContext	123
3426	Tabelle 29: Tab_Dokv_99—Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	137
3427	Tabelle 30: Tab_Dokv_100—XACML 2.0 Policy für einen Versicherten (Base Policy)....	137
3428	Tabelle 31: Tab_Dokv_101—XACML 2.0 Policy mit erlaubten Operationen für einen	
3429	Versicherten (Permission Policy)	140
3430	Tabelle 32: Tab_Dokv_200—XACML 2.0 Policy für einen Vertreter (Base Policy)	171
3431	Tabelle 33: Tab_Dokv_201—XACML 2.0 Policy mit erlaubten Operationen für einen	
3432	Vertreter (Permission Policy)	175
3433	Tabelle 34 Tabelle : Tab_Dokv_300_01—XACML 2.0 Policy für eine	
3434	Leistungserbringerinstitution (Base Policy)	203
3435	Tabelle 35: Tab_Dokv_301—XACML 2.0 Policy mit erlaubten Operationen für eine	
3436	Leistungserbringerinstitution zum Zugriff auf Leistungserbringer Dokumente	
3437	(Permission Policy)	208
3438	Tabelle 36: Tab_Dokv_302—XACML 2.0 Policy mit erlaubten Operationen für eine	
3439	Leistungserbringerinstitution zum Zugriff auf Versicherten und Kostenträger-	
3440	Dokumente (Permission Policy)	234
3441	Tabelle 37: Tab_Dokv_400—XACML 2.0 Policy für einen Kostenträger (Base Policy) ...	258
3442	Tabelle 38: Tab_Dokv_401—XACML 2.0 Policy mit erlaubten Operationen für einen	
3443	Kostenträger (Permission Policy)	261
3444	Tabelle 39: Tab_Dokv_99—Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	265
3445	Tabelle 40: Tab_Dokv_500—XACML 2.0 Policy für einen Versicherten	265
3446	Tabelle 41: Tab_Dokv_501—XACML 2.0 Policy für einen Vertreter	268
3447	Tabelle 42: Tab_Dokv_502—XACML 2.0 Policy für eine Leistungserbringerinstitution ..	271
3448	Tabelle 43: Tab_Dokv_503—XACML 2.0 Policy für einen Kostenträger	300
3449	Tabelle 1: Tab Dokv 10 - Kennzeichnung von Optionalitäten	24

3450	Tabelle 2: Tab Dokv 11 - Übersicht über gruppierte IHE ITI-Akteure und Optionen an	
3451	den Außenschnittstellen der ePA-Dokumentenverwaltung	24
3452	Tabelle 3: Tab Dokv 12 - Fehlercodes zu Fehlern gemäß Operationsdefinition	31
3453	Tabelle 4: Tab Dokv 35 - Eingangsparameter für TUC PKI 018	38
3454	Tabelle 5: Tab Dokv 13 - Parameter des § 291a-Protokolls	41
3455	Tabelle 6: Tab Dokv 14 - Schnittstelle I Document Management	49
3456	Tabelle 7: Tab Dokv 16 - Operation Cross-Gateway Query	53
3457	Tabelle 8: Tab Dokv 17 - Operation RemoveMetadata	56
3458	Tabelle 9: Tab Dokv 18 - Operation Cross-Gateway Retrieve	57
3459	Tabelle 10: Tab Dokv 20 - Schnittstelle I Document Management Insurant	59
3460	Tabelle 11: Tab Dokv 21 - Operation Provide And Register Document Set-b	60
3461	Tabelle 12: Tab Dokv 22 - Operation Registry Stored Query	62
3462	Tabelle 13: Tab Dokv 23 - Operation RemoveMetadata	66
3463	Tabelle 14: Tab Dokv 24 - Operation Retrieve Document Set	68
3464	Tabelle 15: Tab Dokv 19 - Operation RestrictedUpdateDocumentSet	70
3465	Tabelle 16: Tab Dokv 36 - Schnittstelle I Document Management Insurance	73
3466	Tabelle 17: Tab Dokv 37 - Operation Provide And Register Document Set-b	74
3467	Tabelle 18: Tab Dokv 25 - Schnittstelle I Account Management Insurant	77
3468	Tabelle 19: Tab Dokv 26 - Operation Suspend Account	77
3469	Tabelle 20: Tab Dokv 27 - Operation Resume Account	81
3470	Tabelle 21: Tab Dokv 28 - Operation Get Audit Events	84
3471	Tabelle 22: Tab Dokv XX - Operation I Key Management Insurant::StartKeyChange()	
3472	90
3473	Tabelle 23: Tab Dokv XX -	
3474	Operation I Key Management Insurant::GetAllDocumentKeys()	93
3475	Tabelle 24: Tab Dokv XX -	
3476	Operation I Key Management Insurant::PutAllDocumentKeys()	95
3477	Tabelle 25: Tab Dokv XX -	
3478	Operation I Account Management Insurant::FinishKeyChange()	97
3479	Tabelle 26: Tab Dokv XX - Zusätzliche Parameter des § 291a-Protokolls für die	
3480	Umschlüsselung	99
3481	Tabelle 27: Tab Dokv XX - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback	
3482	im Rahmen der Umschlüsselung	100
3483	Tabelle 28 : Tab Dokv 030 - Zugriffsunterbindungsregeln	106
3484	Tabelle 29: Tab Dokv 29 - Ablauf Operation Hello	117
3485	Tabelle 30: Tab Dokv 30 - Schnittstelle I Document Management Connect	120
3486	Tabelle 31: Tab Dokv 31 - Operation OpenContext	120
3487	Tabelle 32: Tab Dokv 32 - Ablauf der Operation Open Context	121
3488	Tabelle 33: Tab Dokv 33 - Operation Close Context	123

Tabelle 34: Tab Dokv 34 - Ablauf Operation CloseContext.....	123
Tabelle 35: Tab Dokv 99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	137
Tabelle 36: Tab Dokv 100 - XACML 2.0 Policy für einen Versicherten (Base Policy)....	137
Tabelle 37: Tab Dokv 101 - XACML 2.0 Policy mit erlaubten Operationen für einen Versicherten (Permission Policy).....	140
Tabelle 38: Tab Dokv 200 - XACML 2.0 Policy für einen Vertreter (Base Policy).....	171
Tabelle 39: Tab Dokv 201 - XACML 2.0 Policy mit erlaubten Operationen für einen Vertreter (Permission Policy).....	175
Tabelle 40 Tabelle : Tab Dokv 300-01 - XACML 2.0 Policy für eine Leistungserbringerinstitution (Base Policy).....	203
Tabelle 41: Tab Dokv 301 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente (Permission Policy)	208
Tabelle 42: Tab Dokv 302 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-Dokumente (Permission Policy)	234
Tabelle 43: Tab Dokv 400 - XACML 2.0 Policy für einen Kostenträger (Base Policy) ...	258
Tabelle 44: Tab Dokv 401 - XACML 2.0 Policy mit erlaubten Operationen für einen Kostenträger (Permission Policy)	261
Tabelle 45: Tab Dokv 99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	265
Tabelle 46: Tab Dokv 500 - XACML 2.0 Policy für einen Versicherten	265
Tabelle 47: Tab Dokv 501 - XACML 2.0 Policy für einen Vertreter	268
Tabelle 48: Tab Dokv 502 - XACML 2.0 Policy für eine Leistungserbringerinstitution ..	271
Tabelle 49: Tab Dokv 503 - XACML 2.0 Policy für einen Kostenträger	300

7.5 Referenzierte Dokumente

7.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer ist in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die 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

3524 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-Profiles 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 35: 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 36: 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 KVN R) -->					
	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 R (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.

3536 **8.1.2 Permission Policy**

3537 **Tabelle 37: Tab_Dokv_101 - XACML 2.0 Policy mit erlaubten Operationen für einen**
 3538 **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.	
				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:Regis tryStoredQuery" MUSS gesetzt werden.	
				ActionAttribut eDesignator		R		
					@Attri buteId	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.

3539 8.2 Policy Document für einen Vertreter

3540 8.2.1 Base Policy

3541 Tabelle 38: 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 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.
				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-Modul 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.

3542 8.2.2 Permission Policy

3543 **Tabelle 39: Tab_Dokv_201 - XACML 2.0 Policy mit erlaubten Operationen für einen**
 3544 **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: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.
<!-- '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: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: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: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: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: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: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.

3545 8.3 Policy Document für eine Leistungserbringerinstitution

3546 8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente

3547

3548 **Tabelle 40 Tabelle : Tab_Dokv_300-01 - XACML 2.0 Policy für eine**
 3549 **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 41: 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 42: 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]	Opt.	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 (@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 (@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: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: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: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/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

[illegible]

					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.

3560 8.4 Policy Document für einen Kostenträger

3561

3562 8.4.1 Base Policy

3563 **Tabelle 43: 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.

3564 8.4.2 Permission Policy

3565 **Tabelle 44: Tab_Dokv_401 - XACML 2.0 Policy mit erlaubten Operationen für einen**
 3566 **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:hl7-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:hl7-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.

3567

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 45: 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 46: 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 R) -->					
	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 R (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.
<!-- KVNDR 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 KVNDR (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.

3577

3578

3579 **9.2 Policy Document für einen Vertreter**3580 **Tabelle 47: 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 KVRN (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-Modul 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.

3581

3582

3583 9.3 Policy Document für eine Leistungserbringerinstitution

3584 Tabelle 48: Tab_Dokv_502 - XACML 2.0 Policy für eine Leistungserbringerinstitution

Element-, Attribut- oder Textknoten gemäß [XACML]	O	Nutzungsvorgabe
---	---	-----------------

										t	
P	o	l	i	c	y	S	e	t		R	
										R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:base" MUSS gesetzt werden.
@P	o	l	i	c	y	S	e	t		R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
@P	o	l	i	c	y	C	o	m	b	R	Der Wert "4.0" MUSS gesetzt werden.
@V	e	r	s	i	o	n				R	Das Element MUSS leer bleiben.
T	a	r	g	e	t					R	
P	o	l	i	c	y	S	e	t		R	
		@P	o	l	i	c	y	S	e	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:containe

									r" 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
		<!-- 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.
							Instance Identifier	R	
							@xml:ns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
							@r:ot	R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
							@extension	R	Als Wert MUSS die Telematik-ID der zu berechtigenden LEI 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.
		<!-- 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.
		Instance Identifier						R	
		@xml:s						R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
		@root						R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
		@exte						R	Als Wert MUSS der unveränderbare Teil der

								n s i o n	KVNR (10 Stellen) gesetzt werden.
						ResourceAttributeDe signator		R	
						@Attribu teId		R	Der Wert "urn:ihe:iti: ser:2016:pat ient-id" MUSS gesetzt werden.
						@DataT ype		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:na mes:tc:xacml :1.0: function:dat e-less-than- or-equal" MUSS gesetzt werden.
						AttributeValue		R	
						@DataT ype		R	Der Wert "http://www.w 3.org/2001/X MLSchema#dat e" 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.
						@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	

							@DataT ype	R	Der Wert "http://www.w 3.org/2001/X MLSchema#dat e" 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 eintrag barewä hlbare Anzahl Tage in der Spanne von 1 bis 540 oder • "heute " + 100 Jahre
						EnvironmentAttribut eDesignator		R	
						@Attribu teId		R	Der Wert "urn:oasis:na mes:tc:xacml :1.0: environment: current-date" MUSS gesetzt werden.

							@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
<-- Entweder (Vertrauensstufe AND Kategorie erlaubt AND notBlacklisted) ODER Whitelist. Wenn JA, dann Permit, ansonsten Deny -->									
	PolicySet							R	
	@PolicySetId							R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:all-permissions" MUSS gesetzt werden.
	@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	Der Wert MUSS leer bleiben.
<-- Feingranulare Berechtigung: Whitelist -->									

		PolicyId Referenc e							R Der Wert "urn:gematik: policy- id:permissio ns-access- group- hcp:whitelis t" MUSS gesetzt werden.
		<-- Vertrauensstufe AND Kategorie erlaubt AND not Blacklisted -->							
		PolicySe t							R
			@Policy SetId						R Der Wert "urn:gem atik:policy- set- id:permissio ns-access- group- hcp:base:che ck-wo- whitelist" MUSS gesetzt werden.
			@Policy Combini ngAlgId						R Der Wert "urn:oasis:na mes:tc:xacml :1.0: policy- combining- algorithm:de ny-overrides" MUSS gesetzt werden.
			@Versio n						R Der Wert "4.0" MUSS gesetzt werden.
			Target						R Der Wert MUSS leer bleiben.

			PolicyId Referenc e						R Der Wert "urn:gematik: policy-set- id:permissio ns-access- group- hcp:levels" MUSS gesetzt werden.
			PolicyId Referenc e						R Der Wert "urn:gematik: policy-set- id:permissio ns-access- group- hcp:category es" MUSS gesetzt werden.
			PolicyId Referenc e						R Der Wert "urn:gematik: policy-set- id:permissio ns-access- group- hcp:blacklis t" MUSS gesetzt werden.
<--Default Policy, die immer Deny zurückgibt -->									
		Policy							R
			@PolicyI d						R Der Wert "urn:ge matik:policy - id:permissio ns-access- group- hcp:base:def ault-deny" MUSS gesetzt werden.

			@RuleCombiningAlgId						R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
			Target						R	Der Wert MUSS leer bleiben.
			Rule						R	
				@RuleId					R	Der Wert "urn:gematik:rule-id:permissions-access-group-hcp:base:default-deny" MUSS gesetzt werden.
				@Effect					R	Der Wert "Deny" MUSS gesetzt werden.
<-- Setzen der grobgranularen Berechtigung -->										
PolicySet									R	
		@PolicySetId							R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:levels" MUSS gesetzt werden.

		@Policy Combini ngAlgId							R Der Wert "urn:oasis:na mes:tc:xacml :1.0: policy- combining- algorithm:pe rmit- overrides" MUSS gesetzt werden.
		@Versio n							R Der Wert "4.0" MUSS gesetzt werden.
		Target							R Der Wert MUSS leer bleiben.
		<-- Grobgranulare Berechtigung "normal" (immer vorhanden) -->							
		PolicyId Referenc e							R Der Wert "urn:gematik: policy- id:permissio ns-access- group- hcp:levels:n ormal" MUSS gesetzt werden.
		<-- Grobgranulare Berechtigung "erweitert" (nur bei Bedarf vorhanden) -->							
		PolicyId Referenc e							O Das Element MUSS genau dann vorhanden sein, wenn "erweiterte Berechtigung" erteilt werden soll, und dann den Wert "urn:gematik: policy- id:permissio ns-access- group-

									hcp:levels:extended" besitzen.
		<-- Default Policy, die immer Deny zurückgibt -->							
		PolicyId Referenc e							R Der Wert "urn:gematik: policy- id:permissio ns-access- group- hcp:base:def ault-deny" MUSS gesetzt sein.
		<-- Setzen der mittelgranularen Berechtigung -->							
		Poli cyS et							R
		@Policy SetId							R Der Wert "urn:gematik :policy-set- id:permissio ns-access- group- hcp:category es" MUSS gesetzt werden.
		@Policy Combini ngAlgId							R Der Wert "urn:oasis:na mes:tc:xacml :1.0: policy- combining- algorithm:pe rmit- overrides" MUSS gesetzt werden.
		@Versio n							R Der Wert "4.0" MUSS gesetzt werden.

		Target							R	Der Wert MUSS leer bleiben.
		<--Setzen der Berechtigung auf Kategorie " <u>category_emp</u> " -->								
		PolicyId Referenc e							O	Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie " <u>category_emp</u> " erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:emp" besitzen.
		<--Setzen der Berechtigung auf Kategorie " <u>category_nfd</u> " -->								
		PolicyId Referenc e							O	Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie " <u>category_nfd</u> " erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:nfd" besitzen.

		<--Setzen der Berechtigung auf Kategorie "category_eab" -->							
		PolicyId Referenc e							<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "category_eab" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:eab" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "category_dentalrecord" -->							
		PolicyId Referenc e							<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "category_dentalrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:dentalrecord" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "category_childsrecord" -->							

		PolicyId Referenc e								<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "<u>category_chi</u>ldsrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:childsrecord" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "<u>category_mothersrecord</u>" -->								
		PolicyId Referenc e								<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "<u>category_mot</u>hersrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:mothersrecord" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "<u>category_vaccination</u>" -->								
		PolicyId Referenc e								<p>O Das Element MUSS genau dann vorhanden</p>

									sein, wenn die Berechtigung auf Kategorie " <u>category_vac</u> cination" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:vaccination" besitzen.
		<-- Setzen der Berechtigung auf Kategorie " <u>category_patientdoc</u> " -->							
		PolicyId Referenc e							O Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie " <u>category_pat</u> ientdoc" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:patientdoc" besitzen.
		<-- Setzen der Berechtigung auf Kategorie " <u>category_ega</u> " -->							
		PolicyId Referenc e							O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie " <u>category_ega</u> " erteilt

									werden soll, und dann den Wert "urn:gematik: policy- id:permissio ns-access- group- hcp:category es:ega" besitzen.
		<-- Setzen der Berechtigung auf Kategorie "category_receipt" -->							
		PolicyId Referenc e							<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "category_receipt" erteilt werden soll, und dann den Wert "urn:gematik: policy- id:permissio ns-access- group- hcp:category es:receipt" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "category_care" -->							
		PolicyId Referenc e							<p>O Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "category_care" erteilt werden soll, und dann den Wert "urn:gematik: policy-</p>

									id:permissions-access-group-hcp:categories:care" besitzen.
		<-- Setzen der Berechtigung auf Kategorie "category_prescription" -->							
		PolicyId Referenc e							<p>O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "category_prescription" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:prescription" besitzen.</p>
		<-- Setzen der Berechtigung auf Kategorie "category_eau" -->							
		PolicyId Referenc e							<p>O Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "category_eau" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:"</p>

									es: eau" besitzen.
		<-- Setzen der Berechtigung auf Kategorie "category_other" -->							
		PolicyId Referenc e							O Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "category_oth er" erteilt werden soll, und dann den Wert "urn:gematik: policy- id:permissio ns-access- group- hcp:category es:other" besitzen.
		<-- Setzen der Berechtigung für Kategorien category_1a1, category_1a2, category_1a3, categ ory_1a4, category_1a5, category_1a6, category_ 1a7, category_1a8, category_1a9practitioner, hos pital, laboratory, physiotherapy, psychotherapy, d ermatology, gynaecology urology, dentistry oms, other_medical und category_1a10other_non_medical -->							
		PolicyId Referenc e							O Das Element MUSS genau dann vorhanden sein, wenn auf eine der Kategorien "category_1a <n>" = {practitione r/hospital/l aboratory/ph ysiotherapy psychotherap y/dermatolog y/ gynaecology_

										<p> 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_1a<n>" besitzen, wobei <n> jeweils der Kategorienummer (1-10) der zu berechtigende n-Kategorie entspricht. </p> <p> Beispiel: Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:category_1a9other medical" berechtigt auf die Kategorie "category_1a9other medical". </p> <p> Das Element wird für jede zu berechtigende Kategorie (mit jeweils der Kategorie entsprechende n Wert) </p>
--	--	--	--	--	--	--	--	--	--	--

									wiederholt.
		<-- Default Policy, die immer Deny zurückgibt							
		PolicyId Referenc e							R Der Wert "urn:gematik: policy- id:permissio ns-access- group- hcp:base:def ault-deny" MUSS gesetzt sein.
		<-- Setzen der feingranularen Berechtigung: Blacklist - ->							
	Poli cy								R
		@PolicyId							R Der Wert "urn:ge matik:policy - id:permissio ns-access- group- hcp:blacklis t" MUSS gesetzt werden.
		@RuleC omibinin gAlgId							R Der Wert "urn:oasis:na mes:tc:xacml :1.0: rule- combining- algorithm:de ny-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	
					Resource Match			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 DocumentEntry.uniqueId des Dokuments entsprechen, das auf die Blacklist gesetzt werden soll.
						@DataType		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.
						@DataType		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

									<p>Wert der DocumentEntry.uniqueId des Dokuments entsprechen, das auf die Whitelist gesetzt werden soll.</p> <p>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).</p>
							@DataType	R	<p>Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.</p>
						ResourceAttributeDesignator		R	
							@AttributeId	R	<p>Der Wert "urn:oasis:names:tc:xacml:1.0:resource:resource-id" MUSS</p>

									gesetzt werden.
							@DataT ype	R	Der Wert "http://www.w3 .org/2001/XM LSchema#stri ng" MUSS gesetzt werden.
		<-- Default Rule, das immer Deny zurückgibt -->							
		Rule						R	
			@RuleId					R	Der Wert "urn:gematik: rule- id:permissio ns-access- group- hcp:whitelis t:default- deny" MUSS gesetzt werden.
			@Effect					R	Der Wert "Deny" MUSS gesetzt werden.

3585

3586 9.4 Policy Document für einen Kostenträger

3587 **Tabelle 49: Tab_Dokv_503 - XACML 2.0 Policy für einen Kostenträger**

Element-, Attribut- oder Textknoten gemäß [XACML]		Opt.	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: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 "1.2.276.0.76.4.188" 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:h17-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 Leistungserbringereinstitution 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 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	
				@DataTyp e		R	Der Wert "urn:h17- org:v3#II" MUSS gesetzt werden.
				InstanceI dentifizier		R	
				@xml ns		R	Der Wert "urn:h17- org:v3" MUSS gesetzt werden.
				@root		R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@exte nsion		R	Als Wert MUSS der 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:h17-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. <u>in UTC</u>
			EnvironmentAttributeDesignator		R	

				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.
				@DataTyper		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:environment:current-date" MUSS gesetzt werden.
				AttributeValue		R	
				@DataTyper		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 <u>in UTC</u>) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen: <ul style="list-style-type: none"> • <u>"heute" + freie eintragbarewählbare Anzahl Tage in der Spanne von 1 bis 540 oder</u> • <u>"heute " + 100 Jahre</u>
				EnvironmentAttributeDesignator		R	

					@Attribut eId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: environment:current- date" MUSS gesetzt werden.
					@DataTyp e		R	Der Wert "http://www.w3.org/2001 /XMLSchema#date" MUSS gesetzt werden.
<!-- Prüfung der Berechtigungskategorien -->								
<-- Setzen der Berechtigung auf Kategorie "category_receipt" -->								
					PolicyIdReference		R	Der Wert "urn:gematik:poli- cy-id:permissions- access-group- hcp:categories:receipt" MUSS gesetzt werden.
<-- Setzen der Berechtigung auf Kategorie "category_ega" -->								
					PolicyIdReference		R	Der Wert "urn:gematik:poli- cy-id:permissions- access-group- hcp:categories:ega" MUSS gesetzt werden.

3588

3589 9.5 Statische Permission Policies

3590 Dieses Kapitel listet alle Permission Policies. Sie werden statisch in der
3591 Dokumentenverwaltung hinterlegt.

3592 9.5.1 Grobgranulare Berechtigung: Stufe Normal

```

3593 <?xml version="1.0" encoding="UTF-8"?>
3594 <Policy
3595 xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" RuleCombiningAlgId="urn:oa
3596 sis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3597 overrides" PolicyId="urn:gematik:policy-id:permissions-access-group-
3598 hcp:levels:normal" Version="4.0">

```

```

3599     <Target/>
3600     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:levels:normal"
3601     Effect="Permit">
3602         <Target>
3603             <Resources>
3604                 <Resource>
3605                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3606                         <AttributeValue DataType="urn:hl7-org:v3#CV">
3607                             <CodedValue xmlns="urn:hl7-org:v3" code="N"
3608 codeSystem="2.16.840.1.113883.5.25" displayName="normal"/>
3609                         </AttributeValue>
3610                         <ResourceAttributeDesignator
3611 AttributeId="urn:ihe:iti:apcc:2016:confidentiality-code" DataType="urn:hl7-
3612 org:v3#CV"/>
3613                     </ResourceMatch>
3614                 </Resource>
3615             </Resources>
3616         </Target>
3617     </Rule>
3618     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3619     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3620 hcp:levels:normal:default-deny" Effect="Deny"/>
3621 </Policy>

```

3622 9.5.2 Grobgranulare Berechtigung: Stufe Erweitert

```

3623 <?xml version="1.0" encoding="UTF-8"?>
3624 <Policy
3625     xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
3626     RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3627 overrides"
3628     PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:levels:extended"
3629     Version="4.0">
3630     <Target/>
3631     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:levels:extended"
3632     Effect="Permit">
3633         <Target>
3634             <Resources>
3635                 <Resource>
3636                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3637                         <AttributeValue DataType="urn:hl7-org:v3#CV">
3638                             <CodedValue xmlns="urn:hl7-org:v3" code="R"
3639 codeSystem="2.16.840.1.113883.5.25" displayName="restricted"/>
3640                         </AttributeValue>
3641                         <ResourceAttributeDesignator
3642 AttributeId="urn:ihe:iti:apcc:2016:confidentiality-code" DataType="urn:hl7-
3643 org:v3#CV"/>
3644                     </ResourceMatch>
3645                 </Resource>
3646             </Resources>
3647         </Target>
3648     </Rule>
3649     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3650     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-

```

```

3651 hcp:levels:extended:default-deny" Effect="Deny"/>
3652 </Policy>

```

3653 9.5.3 Mittelgranulare Berechtigung: Kategorie "care"

```

3654 <?xml version="1.0" encoding="UTF-8"?>
3655 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:care"
3656 xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" RuleCombiningAlgId="urn:oasi
3657 s:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" Version="4.0">
3658   <Target/>
3659   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:care"
3660 Effect="Permit">
3661     <Target>
3662       <Resources>
3663         <Resource>
3664           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3665             <AttributeValue DataType="urn:hl7-org:v3#CV">
3666               <CodedValue xmlns="urn:hl7-org:v3" code="PFL"
3667 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.5"/>
3668             </AttributeValue>
3669             <ResourceAttributeDesignator
3670 AttributeId="urn:ihe:iti:appc:2016:document-entry:practice-setting-code"
3671 DataType="urn:hl7-org:v3#CV"/>
3672             </ResourceMatch>
3673           </Resource>
3674         </Resources>
3675       </Target>
3676     </Rule>
3677     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3678     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3679 hcp:categories:care:default-deny" Effect="Deny"/>
3680 </Policy>

```

3681 9.5.4 Mittelgranulare Berechtigung: Kategorie "childsrecord"

```

3682 <?xml version="1.0" encoding="UTF-8"?>
3683 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
3684 hcp:categories:childsrecord" xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
3685 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3686 overrides" Version="4.0">
3687   <Target/>
3688   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3689 hcp:categories:childsrecord" Effect="Permit">
3690     <Target>
3691       <Resources>
3692         <Resource>
3693           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3694             <AttributeValue DataType="urn:hl7-org:v3#CV">
3695               <CodedValue xmlns="urn:hl7-org:v3"
3696 code="urn:gematik:ig:Kinderuntersuchungsheft:r4.0"
3697 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
3698             </AttributeValue>
3699             <ResourceAttributeDesignator

```

```

3700 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-related-folder:code"
3701 DataType="urn:hl7-org:v3#CV"/>
3702     </ResourceMatch>
3703     </Resource>
3704 </Resources>
3705 </Target>
3706 </Rule>
3707 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3708 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3709 hcp:categories:childsrecord:default-deny" Effect="Deny"/>
3710 </Policy>

```

3711 9.5.5 Mittelgranulare Berechtigung: Kategorie "dentalrecord"

```

3712 <?xml version="1.0" encoding="UTF-8"?>
3713 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
3714 hcp:categories:dentalrecord" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
3715 combining-algorithm:deny-overrides" Version="4.0">
3716     <Target/>
3717     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3718 hcp:categories:dentalrecord" Effect="Permit">
3719         <Target>
3720             <Resources>
3721                 <Resource>
3722                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3723                         <AttributeValue DataType="urn:hl7-org:v3#CV">
3724                             <CodedValue xmlns="urn:hl7-org:v3"
3725 code="urn:gematik:ig:Zahnbonusheft:r4.0"
3726 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
3727                             </AttributeValue>
3728                             <ResourceAttributeDesignator
3729 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
3730 org:v3#CV"/>
3731                             </ResourceMatch>
3732                         </Resource>
3733                     </Resources>
3734                 </Target>
3735             </Rule>
3736 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3737 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3738 hcp:categories:dentalrecord:default-deny" Effect="Deny"/>
3739 </Policy>

```

3740 9.5.6 Mittelgranulare Berechtigung: Kategorie "eab"

```

3741 <?xml version="1.0" encoding="UTF-8"?>
3742 <!-- Mittelgranular: Kategorie "eArztbrief" -->
3743 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:eab"
3744 xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
3745 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3746 overrides" Version="4.0">
3747     <Target/>
3748     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:eab"

```



```

3749 Effect="Permit">
3750   <Target>
3751     <Resources>
3752       <Resource>
3753         <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3754           <AttributeValue DataType="urn:hl7-org:v3#CV">
3755             <CodedValue xmlns="urn:hl7-org:v3"
3756 code="urn:gematik:ig:Arztbrief:r3.1"
3757 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
3758           </AttributeValue>
3759           <ResourceAttributeDesignator
3760 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-
3761 code"
3762 urn:hl7-org:v3#CV"/>
3763         </ResourceMatch>
3764       </Resource>
3765     </Resources>
3766   </Target>
3767 </Rule>
3768 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3769 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3770 hcp:categories:eab:default-deny" Effect="Deny"/>
3771 </Policy>
3772

```

9.5.69.5.7 Mittelgranulare Berechtigung: Kategorie "eau"

```

3774 <?xml version="1.0" encoding="UTF-8"?>
3775 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:eau"
3776 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3777 overrides" Version="4.0">
3778   <Target/>
3779   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:eau"
3780 Effect="Permit">
3781     <Target>
3782       <Resources>
3783         <Resource>
3784           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3785             <AttributeValue DataType="urn:hl7-org:v3#CV">
3786               <CodedValue xmlns="urn:hl7-org:v3"
3787 code="urn:gematik:ig:Arbeitsunfähigkeitsbescheinigung:r4.0"
3788 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
3789             </AttributeValue>
3790             <ResourceAttributeDesignator
3791 AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
3792 org:v3#CV"/>
3793           </ResourceMatch>
3794         </Resource>
3795       </Resources>
3796     </Target>
3797   </Rule>
3798   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3799   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3800 hcp:categories:eau:default-deny" Effect="Deny"/>

```

3801 </Policy>
3802

3803 9.5.79.5.8 Mittelgranulare Berechtigung: Kategorie "ega"

```
3804 <?xml version="1.0" encoding="UTF-8"?>
3805 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
3806 hcp:categories:category_ega" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
3807 combining-algorithm:deny-overrides" Version="4.0">
3808   <Target/>
3809   <!--Prüfung, ob folder.codeList den Code "category_1a1practitioner" enthält (TODO:
3810 Code System hier und unten ergänzen) -->
3811   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3812 hcp:categories:category_ega" Effect="Permit">
3813     <Target>
3814       <Resources>
3815         <Resource>
3816           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3817             <AttributeValue DataType="urn:hl7-org:v3#CV">
3818               <CodedValue xmlns="urn:hl7-org:v3" code="category_ega"
3819 codeSystem="TODO"/>
3820             </AttributeValue>
3821             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
3822 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
3823           </ResourceMatch>
3824         </Resource>
3825       </Resources>
3826     </Target>
3827   </Rule>
3828   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3829   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3830 hcp:categories:category_ega:default_deny" Effect="Deny"/>
3831 </Policy>
```

3832 9.5.89.5.9 Mittelgranulare Berechtigung: Kategorie "emp"

```
3833 <?xml version="1.0" encoding="UTF-8"?>
3834 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:emp"
3835 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3836 overrides" Version="4.0">
3837   <Target/>
3838   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:emp"
3839 Effect="Permit">
3840     <Target>
3841       <Resources>
3842         <Resource>
3843           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3844             <AttributeValue DataType="urn:hl7-org:v3#CV">
3845               <CodedValue xmlns="urn:hl7-org:v3"
3846 code="urn:gematik:ig:Medikationsplan:r3.1"
3847 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
3848             </AttributeValue>
3849             <ResourceAttributeDesignator AttributeId="urn:ihe:iti:apcc:2016:docum
```

```

3850 ent-entry:format-code" DataType="urn:hl7-org:v3#CV"/>
3851     </ResourceMatch>
3852     </Resource>
3853   </Resources>
3854 </Target>
3855 </Rule>
3856 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3857 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3858 hcp:categories:emp:default-deny" Effect="Deny"/>
3859 </Policy>

```

3860 **9.5.99.5.10 Mittelgranulare Berechtigung: Kategorie** 3861 **"mothersrecord"**

```

3862 <?xml version="1.0" encoding="UTF-8"?>
3863 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
3864 hcp:categories:mothersrecord"
3865 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3866 overrides" Version="4.0">
3867   <Target/>
3868   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3869 hcp:categories:mothersrecord" Effect="Permit">
3870     <Target>
3871       <Resources>
3872         <Resource>
3873           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3874             <AttributeValue DataType="urn:hl7-org:v3#CV">
3875               <CodedValue xmlns="urn:hl7-org:v3"
3876 code="urn:gematik:ig:Mutterpass:r4.0" codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
3877             </AttributeValue>
3878             <ResourceAttributeDesignator
3879 AttributeId="urn:ihe:iti:appc:2016:document-entry:format-related-folder:code"
3880 DataType="urn:hl7-org:v3#CV"/>
3881           </ResourceMatch>
3882         </Resource>
3883       </Resources>
3884     </Target>
3885   </Rule>
3886   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3887   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3888 hcp:categories:mothersrecord:default-deny" Effect="Deny"/>
3889 </Policy>

```

3890 **9.5.109.5.11 Mittelgranulare Berechtigung: Kategorie "nfd"**

```

3891 <?xml version="1.0" encoding="UTF-8"?>
3892 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:nfd"
3893 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
3894 overrides" Version="4.0">
3895   <Target/>
3896   <!--Notfalldatensatz -->
3897   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3898 hcp:categories:nfd:nfd" Effect="Permit">

```

```

3899     <Target>
3900       <Resources>
3901         <Resource>
3902           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3903             <AttributeValue DataType="urn:hl7-org:v3#CV">
3904               <CodedValue xmlns="urn:hl7-org:v3"
3905 code="urn:gematik:ig:Notfalldatensatz:r3.1"
3906 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
3907             </AttributeValue>
3908             <ResourceAttributeDesignator
3909 AttributeId="urn:ihe:iti:appc:2016:document-entry:format-code" DataType="urn:hl7-
3910 org:v3#CV"/>
3911           </ResourceMatch>
3912         </Resource>
3913       </Resources>
3914     </Target>
3915   </Rule>
3916   <!-- Persönliche Erklärung -->
3917   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:nfd:pe"
3918 Effect="Permit">
3919     <Target>
3920       <Resources>
3921         <Resource>
3922           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3923             <AttributeValue DataType="urn:hl7-org:v3#CV">
3924               <CodedValue xmlns="urn:hl7-org:v3"
3925 code="urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1"
3926 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
3927             </AttributeValue>
3928             <ResourceAttributeDesignator
3929 AttributeId="urn:ihe:iti:appc:2016:document-entry:format-code" DataType="urn:hl7-
3930 org:v3#CV"/>
3931           </ResourceMatch>
3932         </Resource>
3933       </Resources>
3934     </Target>
3935   </Rule>
3936   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
3937   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3938 hcp:categories:nfd:default-deny" Effect="Deny"/>
3939 </Policy>

```

9.5.11 9.5.12 Mittelgranulare Berechtigung: Kategorie "other"

```

3941 <?xml version="1.0" encoding="UTF-8"?>
3942 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
3943 hcp:categories:category_other"
3944 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
3945 overrides" Version="4.0">
3946   <!-- practiceSettingCode = 1.3.6.1.4.1.19376.3.276.1.5.4 (ärztlich) -->
3947   <Target>
3948     <Resources>
3949       <Resource>
3950         <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-

```

```

3951 equal">
3952     <AttributeValue
3953     DataType="http://www.w3.org/2001/XMLSchema#string">
3954         <CodedValue codeSystem="1.3.6.1.4.1.19376.3.276.1.5.4"/>
3955     </AttributeValue>
3956     <ResourceAttributeDesignator
3957     AttributeId="urn:ihe:iti:apcc:2016:document-entry:practice-setting-code"
3958     DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
3959     </ResourceMatch>
3960 </Resource>
3961 </Resources>
3962 </Target>
3963 <!-- typeCode = ABRE, PATI oder SCHR -->
3964 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
3965 hcp:categories:category_other:type-code" Effect="Permit">
3966     <Target>
3967         <Resources>
3968             <Resource>
3969                 <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3970                     <AttributeValue DataType="urn:hl7-org:v3#CV">
3971                         <CodedValue xmlns="urn:hl7-org:v3" code="ABRE"
3972 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
3973                     </AttributeValue>
3974                     <ResourceAttributeDesignator
3975     AttributeId="urn:ihe:iti:apcc:2016:document-entry:type-code" DataType="urn:hl7-
3976     org:v3#CV" MustBePresent="true"/>
3977                     </ResourceMatch>
3978                 </Resource>
3979                 <Resource>
3980                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3981                         <AttributeValue DataType="urn:hl7-org:v3#CV">
3982                             <CodedValue xmlns="urn:hl7-org:v3" code="PATI"
3983 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
3984                         </AttributeValue>
3985                         <ResourceAttributeDesignator
3986     AttributeId="urn:ihe:iti:apcc:2016:document-entry:type-code" DataType="urn:hl7-
3987     org:v3#CV" MustBePresent="true"/>
3988                         </ResourceMatch>
3989                     </Resource>
3990                     <Resource>
3991                         <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
3992                             <AttributeValue DataType="urn:hl7-org:v3#CV">
3993                                 <CodedValue xmlns="urn:hl7-org:v3" code="SCHR"
3994 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
3995                             </AttributeValue>
3996                             <ResourceAttributeDesignator
3997     AttributeId="urn:ihe:iti:apcc:2016:document-entry:type-code" DataType="urn:hl7-
3998     org:v3#CV" MustBePresent="true"/>
3999                             </ResourceMatch>
4000                         </Resource>
4001                     </Resources>
4002                 </Target>
4003             </Rule>
4004             <Rule RuleId="urn:gematik:rule-id:permissions-access-group-

```

```

4005 hcp:categories:category_other:default-deny" Effect="Deny"/>
4006 </Policy>

```

4007 ~~9.5.12~~9.5.13 Mittelgranulare Berechtigung: Kategorie "patientdoc"

```

4008 <?xml version="1.0" encoding="UTF-8"?>
4009 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4010 hcp:categories:patientdoc" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4011 combining-algorithm:deny-overrides" Version="4.0">
4012   <Target/>
4013   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4014 hcp:categories:patientdoc" Effect="Permit">
4015     <Target>
4016       <Resources>
4017         <Resource>
4018           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4019             <AttributeValue DataType="urn:hl7-org:v3#CV">
4020               <CodedValue code="102"
4021 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.13"/>
4022             </AttributeValue>
4023             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4024 entry:related-submission-set:author-role" DataType="urn:hl7-org:v3#CV"/>
4025           </ResourceMatch>
4026         </Resource>
4027       </Resources>
4028     </Target>
4029   </Rule>
4030   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4031   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4032 hcp:categories:patientdoc:default-deny" Effect="Deny"/>
4033 </Policy>

```

4034 ~~9.5.13~~9.5.14 Mittelgranulare Berechtigung: Kategorie 4035 "prescription"

```

4036 <?xml version="1.0" encoding="UTF-8"?>
4037 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4038 hcp:categories:prescription" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4039 combining-algorithm:deny-overrides" Version="4.0">
4040   <Target/>
4041   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4042 hcp:categories:prescription" Effect="Permit">
4043     <Target>
4044       <Resources>
4045         <Resource>
4046           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4047             <AttributeValue DataType="urn:hl7-org:v3#CV">
4048               <CodedValue xmlns="urn:hl7-org:v3"
4049 code="urn:gematik:ig:VerordnungsdatensatzMedikation:r4.0"
4050 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
4051             </AttributeValue>
4052             <ResourceAttributeDesignator
4053 AttributeId="urn:ihe:iti:apbc:2016:document-entry:format-code" DataType="urn:hl7-

```



```

4054 org:v3#CV"/>
4055     </ResourceMatch>
4056   </Resource>
4057 </Resources>
4058 </Target>
4059 </Rule>
4060 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4061 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4062 hcp:categories:prescription:default-deny" Effect="Deny"/>
4063 </Policy>

```

4064 ~~9.5.14~~9.5.15 Mittelgranulare Berechtigung: Kategorie "receipt"

```

4065 <?xml version="1.0" encoding="UTF-8"?>
4066 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4067 hcp:categories:receipt" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
4068 combining-algorithm:deny-overrides" Version="4.0">
4069   <Target/>
4070   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:receipt"
4071 Effect="Permit">
4072     <Target>
4073       <Resources>
4074         <Resource>
4075           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4076             <AttributeValue DataType="urn:hl7-org:v3#CV">
4077               <CodedValue xmlns="urn:hl7-org:v3" code="VER"
4078 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.3"/>
4079             </AttributeValue>
4080             <ResourceAttributeDesignator
4081 AttributeId="urn:ihe:iti:appc:2016:document-entry:healthcare-facility-type-code"
4082 DataType="urn:hl7-org:v3#CV"/>
4083           </ResourceMatch>
4084         </Resource>
4085         <Resource>
4086           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4087             <AttributeValue DataType="urn:hl7-org:v3#CV">
4088               <CodedValue xmlns="urn:hl7-org:v3" code="ABRE"
4089 codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
4090             </AttributeValue>
4091             <ResourceAttributeDesignator
4092 AttributeId="urn:ihe:iti:appc:2016:document-entry:type-code" DataType="urn:hl7-
4093 org:v3#CV"/>
4094           </ResourceMatch>
4095         </Resource>
4096       </Resources>
4097     </Target>
4098   </Rule>
4099   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4100   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4101 hcp:categories:receipt:default-deny" Effect="Deny"/>
4102 </Policy>

```

9.5.159.5.16 Mittelgranulare Berechtigung: Kategorie "vaccination"

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:vaccination" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:deny-overrides" Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:vaccination" 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="urn:gematik:ig:Impfausweis:r4.0"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" 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:vaccination:default-deny" Effect="Deny"/>
</Policy>
```

9.5.169.5.17 Mittelgranulare Berechtigung: Kategorie "category_1a1practitioner"

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:category_1a1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:permit-overrides" Version="4.0">
  <Target/>
  <!-- Prüfung, ob folder.codeList den Code "category_1a1" enthält (TODO: Code
System hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:category_1a1" 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="category_1a1"
codeSystem="TODO"/>
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
```



```

4153 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4154 </ResourceMatch>
4155 </Resource>
4156 </Resources>
4157 </Target>
4158 </Rule>
4159 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4160 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4161 hcp:categories:category_1a1:default-deny" Effect="Deny">
4162 <Target/>
4163 </Rule>
4164 </Policy>

```

9.5.17 Mittelgranulare Berechtigung: Kategorie "category_1a2"

```

4166 <?xml version="1.0" encoding="UTF-8"?><?xml version="1.0" encoding="UTF-8"?>
4167 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4168 hcp:categories:category_1a2practitioner"
4169 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4170 overrides" Version="4.0">
4171 <Target/>
4172 <!--Prüfung, ob folder.codeList den Code "category_1a1practitioner" enthält (TODO:
4173 Code System hier und unten ergänzen) -->
4174 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4175 hcp:categories:category_1a2practitioner" Effect="Permit">
4176 <Target>
4177 <Resources> codelist
4178 <Resource>
4179 <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4180 <AttributeValue DataType="urn:hl7-org:v3#CV">
4181 <CodedValue xmlns="urn:hl7-org:v3"
4182 code="category_1a2practitioner" codeSystem="TODO"/>
4183 </AttributeValue>
4184 <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4185 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4186 </ResourceMatch>
4187 </Resource>
4188 </Resources>
4189 </Target>
4190 </Rule>
4191 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4192 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4193 hcp:categories:category_1a2practitioner:default-deny" Effect="Deny">
4194 <Target/>
4195 </Rule>
4196 </Policy>

```

9.5.18 Mittelgranulare Berechtigung: Kategorie "category_1a3hospital"

```

4199 <?xml version="1.0" encoding="UTF-8"?><?xml version="1.0" encoding="UTF-8"?>
4200 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4201 hcp:categories:category_1a3hospital"

```

```

4202 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4203 overrides" Version="4.0">
4204   <Target/>
4205   <!--Prüfung, ob folder.codeList den Code "category_1a3practitioner" enthält (TODO:
4206   Code System hier und unten ergänzen) -->
4207   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4208   hcp:categories:category_1a3hospital" Effect="Permit">
4209     <Target>
4210       <Resources>
4211         <Resource>
4212           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4213             <AttributeValue DataType="urn:hl7-org:v3#CV">
4214               <CodedValue xmlns="urn:hl7-org:v3" code="category_1a3hospital"
4215               codeSystem="TODO"/>
4216             </AttributeValue>
4217             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4218             entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4219           </ResourceMatch>
4220         </Resource>
4221       </Resources>
4222     </Target>
4223   </Rule>
4224   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4225   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4226   hcp:categories:category_1a3hospital:default-deny" Effect="Deny">
4227     <Target/>
4228   </Rule>
4229 </Policy>

```

9.5.19 Mittelgranulare Berechtigung: Kategorie "category_1a4laboratory"

```

4230
4231
4232 <?xml version="1.0" encoding="UTF-8"?><?xml version="1.0" encoding="UTF-8"?>
4233 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4234 hcp:categories:category_1a4laboratory"
4235 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4236 overrides" Version="4.0">
4237   <Target/>
4238   <!--Prüfung, ob folder.codeList den Code "category_1a4laboratory" enthält (TODO:
4239   Code System hier und unten ergänzen) -->
4240   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4241   hcp:categories:category_1a4laboratory" Effect="Permit">
4242     <Target>
4243       <Resources>
4244         <Resource>
4245           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4246             <AttributeValue DataType="urn:hl7-org:v3#CV">
4247               <CodedValue xmlns="urn:hl7-org:v3"
4248               code="category_1a4laboratory" codeSystem="TODO"/>
4249             </AttributeValue>
4250             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4251             entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4252           </ResourceMatch>

```

```

4253         </Resource>
4254     </Resources>
4255 </Target>
4256 </Rule>
4257 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4258 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4259 hcp:categories:category_1a4laboratory:default-deny" Effect="Deny">
4260     <Target/>
4261 </Rule>
4262 </Policy>

```

9.5.20 Mittelgranulare Berechtigung: Kategorie "category_1a5physiotherapy"

```

4263 <?xml version="1.0" encoding="UTF-8"?><?xml version="1.0" encoding="UTF-8"?>
4264 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4265 hcp:categories:category_1a5physiotherapy"
4266 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4267 overrides" Version="4.0">
4268     <Target/>
4269     <!--Prüfung, ob folder.codeList den Code "category_1a1practitioner" enthält (TODO:
4270 Code System hier und unten ergänzen) -->
4271     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4272 hcp:categories:category_1a5physiotherapy" Effect="Permit">
4273         <Target>
4274             <Resources>
4275                 <Resource>
4276                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4277                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4278                             <CodedValue xmlns="urn:hl7-org:v3"
4279 code="category_1a5physiotherapy" codeSystem="TODO"/>
4280                         </AttributeValue>
4281                         <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4282 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4283                     </ResourceMatch>
4284                 </Resource>
4285             </Resources>
4286         </Target>
4287     </Rule>
4288     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4289     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4290 hcp:categories:category_1a5physiotherapy:default-deny" Effect="Deny">
4291         <Target/>
4292     </Rule>
4293 </Policy>

```

9.5.21 Mittelgranulare Berechtigung: Kategorie "category_1a6psychotherapy"

```

4296 <?xml version="1.0" encoding="UTF-8"?><?xml version="1.0" encoding="UTF-8"?>
4297 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4298 hcp:categories:category_1a6psychotherapy"
4299 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-

```

```

4302 overrides" Version="4.0">
4303   <Target/>
4304   <!--Prüfung, ob folder.codeList den Code "category_1a1practitioner" enthält (TODO:
4305   Code System hier und unten ergänzen) -->
4306   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4307   hcp:categories:category_1a6psychotherapy" Effect="Permit">
4308     <Target>
4309       <Resources>
4310         <Resource>
4311           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4312             <AttributeValue DataType="urn:hl7-org:v3#CV">
4313               <CodedValue xmlns="urn:hl7-org:v3"
4314               code="category_1a6psychotherapy" codeSystem="TODO"/>
4315             </AttributeValue>
4316             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4317             entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4318           </ResourceMatch>
4319         </Resource>
4320       </Resources>
4321     </Target>
4322   </Rule>
4323   <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4324   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4325   hcp:categories:category_1a6psychotherapy:default-deny" Effect="Deny">
4326     <Target/>
4327   </Rule>
4328 </Policy>

```

9.5.22 Mittelgranulare Berechtigung: Kategorie

"category_1a7dermatology"

```

4329 <?xml version="1.0" encoding="UTF-8"?><?xml version="1.0" encoding="UTF-8"?>
4330 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4331 hcp:categories:category_1a7dermatology"
4332 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4333 overrides" Version="4.0">
4334   <Target/>
4335   <!--Prüfung, ob folder.codeList den Code "category_1a1practitioner" enthält (TODO:
4336   Code System hier und unten ergänzen) -->
4337   <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4338   hcp:categories:category_1a7dermatology" Effect="Permit">
4339     <Target>
4340       <Resources>
4341         <Resource>
4342           <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4343             <AttributeValue DataType="urn:hl7-org:v3#CV">
4344               <CodedValue xmlns="urn:hl7-org:v3"
4345               code="category_1a7dermatology" codeSystem="TODO"/>
4346             </AttributeValue>
4347             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4348             entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4349           </ResourceMatch>
4350         </Resource>
4351       </Resources>
4352     </Target>

```

```

4353         </Resources>
4354     </Target>
4355 </Rule>
4356 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4357 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4358 hcp:categories:category_1a7dermatology:default-deny" Effect="Deny">
4359     <Target/>
4360 </Rule>
4361 </Policy>

```

9.5.23 Mittelgranulare Berechtigung: Kategorie

"category_1a8gynaecology urology"

```

4362 <?xml version="1.0" encoding="UTF-8"?><?xml version="1.0" encoding="UTF-8"?>
4363
4364 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4365 hcp:categories:category_1a8gynaecology urology"
4366 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4367 overrides" Version="4.0">
4368     <Target/>
4369     <!--Prüfung, ob folder.codeList den Code "category_1a1practitioner" enthält (TODO:
4370 Code System hier und unten ergänzen) -->
4371 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4372 hcp:categories:category_1a8gynaecology urology" Effect="Permit">
4373     <Target>
4374         <Resources>
4375             <Resource>
4376                 <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4377                     <AttributeValue DataType="urn:hl7-org:v3#CV">
4378                         <CodedValue xmlns="urn:hl7-org:v3"
4379 code="category_1a8gynaecology urology" codeSystem="TODO"/>
4380                     </AttributeValue>
4381                     <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4382 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4383                 </ResourceMatch>
4384             </Resource>
4385         </Resources>
4386     </Target>
4387 </Rule>
4388 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4389 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4390 hcp:categories:category_1a8gynaecology urology:default-deny" Effect="Deny">
4391     <Target/>
4392 </Rule>
4393 </Policy>

```

9.5.24 Mittelgranulare Berechtigung: Kategorie

"category_1a9dentistry oms"

```

4395 <?xml version="1.0" encoding="UTF-8"?><?xml version="1.0" encoding="UTF-8"?>
4396
4397 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4398 hcp:categories:category_1a9dentistry oms"
4399 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4400 overrides" Version="4.0">
4401

```

```

4402     <Target/>
4403     <!--Prüfung, ob folder.codeList den Code "category_1a1practitioner" enthält (TODO:
4404 Code System hier und unten ergänzen) -->
4405     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4406 hcp:categories:category_1a9dentistry oms" Effect="Permit">
4407         <Target>
4408             <Resources>
4409                 <Resource>
4410                     <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4411                         <AttributeValue DataType="urn:hl7-org:v3#CV">
4412                             <CodedValue xmlns="urn:hl7-org:v3"
4413 code="category_1a9dentistry oms" codeSystem="TODO"/>
4414                         </AttributeValue>
4415                         <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4416 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4417                     </ResourceMatch>
4418                 </Resource>
4419             </Resources>
4420         </Target>
4421     </Rule>
4422     <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4423     <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4424 hcp:categories:category_1a9dentistry oms:default-deny" Effect="Deny">
4425         <Target/>
4426     </Rule>
4427 </Policy>

```

9.5.25 Mittelgranulare Berechtigung: Kategorie

"category_1a10other_medical"

```

4430 <?xml version="1.0" encoding="UTF-8"?><?xml version="1.0" encoding="UTF-8"?>
4431 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4432 hcp:categories:category_1a10"
4433 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4434 overrides" Version="4.0">
4435     <Target/>
4436     <!--Prüfung, ob folder.codeList den Code "category_1a10other_medical"
4437 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4438 overrides" Version="4.0">
4439         <Target/>
4440         <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
4441 hier und unten ergänzen) -->
4442         <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4443 hcp:categories:other_medical" Effect="Permit">
4444             <Target>
4445                 <Resources>
4446                     <Resource>
4447                         <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4448                             <AttributeValue DataType="urn:hl7-org:v3#CV">
4449                                 <CodedValue xmlns="urn:hl7-org:v3" code="other_medical"
4450 codeSystem="TODO"/>
4451                             </AttributeValue>
4452                             <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-

```



```

4453 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4454 </ResourceMatch>
4455 </Resource>
4456 </Resources>
4457 </Target>
4458 </Rule>
4459 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4460 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4461 hcp:categories:other_medical:default-deny" Effect="Deny">
4462 <Target/>
4463 </Rule>
4464 </Policy>

```

9.5.26 Mittelgranulare Berechtigung: Kategorie "other non medical"

```

4467 <?xml version="1.0" encoding="UTF-8"?>
4468 <Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
4469 hcp:categories:other_non_medical"
4470 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
4471 overrides" Version="4.0">
4472 <Target/>
4473 <!--Prüfung, ob folder.codeList den Code "other_non_medical" enthält (TODO: Code
4474 System hier und unten ergänzen) -->
4475 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4476 hcp:categories:category_1a10other_non_medical" Effect="Permit">
4477 <Target>
4478 <Resources>
4479 <Resource>
4480 <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
4481 <AttributeValue DataType="urn:hl7-org:v3#CV">
4482 <CodedValue xmlns="urn:hl7-org:v3"
4483 code="category_1a10other_non_medical" codeSystem="TODO"/>
4484 </AttributeValue>
4485 <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
4486 entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
4487 </ResourceMatch>
4488 </Resource>
4489 </Resources>
4490 </Target>
4491 </Rule>
4492 <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
4493 <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
4494 hcp:categories:category_1a10other_non_medical:default-deny" Effect="Deny">
4495 <Target/>
4496 </Rule>
4497 </Policy>

```