

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

7 Elektronische Gesundheitskarte und Telematikinfrastruktur

8 9 10 11 12 13 **Spezifikation** 14 **ePA-** 15 **Dokumentenverwaltung**

16
17
18
19
20
21
22
Version: 1.4.01 CC
Revision: ~~199199238075~~
Stand: ~~02.0320.05.2020~~
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_Dokumentenverwaltung

23
24

25

Dokumentinformationen

Änderungen zur Vorversion

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

29

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 4.2.3.7 -> 5.1.1.1.1 A_13656 von ehemals 4.2.3.7 -> 5.1.1.1.1 A_15080 von ehemals 4.2.3.10 -> 5.1.1.5.1</p> <p>Umgekehrt wurden übergreifende Afos nach Kapitel 4 verschoben und Afo-Duplikate storniert</p> <p>A_14926 von 5.1.2.3.1 -> 4.2.3.4 A_15162 von 5.1.2.1.1 -> 4.2.3.3 A_14937 von 5.1.2.1.1 -> 4.2.3.3 A_14938 von 5.1.2.1.1 -> 4.2.3.3</p>	gematik
1.2.0	28.06.19		Einarbeitung Änderungsliste P19.1	gematik
1.3.0	02.10.19		Einarbeitung Änderungsliste P20.1/2	gematik
1.34.0	02.10.19 03.20		freigegeben Einarbeitung Änderungsliste P21.1	gematik

1.4.01 CC	02.03 20.05.20		freigegebenEinarbeitung Änderungsliste P21.3	gematik
--------------	---------------------------	--	---	---------

ENTWURF

31

Inhaltsverzeichnis

32	1 Einführung	10
33	1.1 Zielsetzung	10
34	1.2 Zielgruppe	10
35	1.3 Geltungsbereich	10
36	1.4 Abgrenzungen	10
37	1.5 Methodik	11
38	2 Systemkontext	12
39	3 Zerlegung der Komponente	13
40	4 Übergreifende Festlegungen	14
41	4.1 Namensräume	14
42	4.2 Nutzung von IHE IT Infrastructure Profilen für Speicherung und Abruf von	
43	Dokumenten	15
44	4.2.1 Anforderungen an IHE ITI Akteure.....	15
45	4.2.1.1 APPC Content Consumer.....	17
46	4.2.1.1.1 Gruppierungen mit anderen IHE ITI Akteuren.....	17
47	4.2.1.1.2 Optionen des IHE ITI Akteurs.....	17
48	4.2.1.2 RMU Update Responder.....	18
49	4.2.1.2.1 Gruppierungen mit anderen IHE ITI Akteuren.....	18
50	4.2.1.2.2 Optionen des IHE ITI Akteurs.....	18
51	4.2.1.3 XCA Responding Gateway.....	19
52	4.2.1.3.1 Gruppierungen mit anderen IHE ITI Akteuren.....	19
53	4.2.1.3.2 Optionen des IHE ITI Akteurs.....	19
54	4.2.1.4 XCDR Responding Gateway.....	19
55	4.2.1.4.1 Gruppierungen mit anderen IHE ITI Akteuren.....	19
56	4.2.1.4.2 Optionen des IHE ITI Akteurs.....	20
57	4.2.1.5 XDS Document Registry.....	20
58	4.2.1.5.1 Gruppierungen mit anderen IHE ITI Akteuren.....	20
59	4.2.1.5.2 Optionen des IHE ITI Akteurs.....	20
60	4.2.1.6 XDS Document Repository.....	21
61	4.2.1.6.1 Gruppierungen mit anderen IHE ITI Akteuren.....	21
62	4.2.1.6.2 Optionen des IHE ITI Akteurs.....	21
63	4.2.1.7 XUA X Service Provider.....	21
64	4.2.1.7.1 Gruppierungen mit anderen IHE ITI Akteuren.....	21
65	4.2.1.7.2 Optionen des IHE ITI Akteurs.....	21
66	4.2.2 Überblick über gruppierte IHE ITI Akteure und Optionen.....	22
67	4.2.3 Einschränkungen auf IHE ITI Transaktionen bei mehreren Schnittstellen.....	26

68	4.2.3.1 Provide X-User Assertion [ITI-40].....	26
69	4.2.3.2 Provide and Register Document Set-b [ITI-41].....	27
70	4.2.3.3 Remove Documents [ITI-86].....	28
71	4.3 Fehlerbehandlung in Schnittstellenoperationen	28
72	4.4 Vertrauenswürdige Ausführungsumgebung	29
73	4.4.1 Verarbeitungskontext	30
74	4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	31
75	4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes	32
76	4.4.4 Parallele Zugriffe.....	33
77	4.4.5 Konsistenz der Akte, Logging und Monitoring	33
78	4.4.6 Client-Verbindungen zum Verarbeitungskontext	33
79	4.5 Anforderungen zur sicherheitstechnischen Validierung.....	35
80	4.6 Protokollierung.....	37
81	5 Funktionsmerkmale	40
82	5.1 Dokumentenverwaltung	40
83	5.1.1 Schnittstelle I_Document_Management.....	40
84	5.1.1.1 Operation I_Document_Management::CrossGatewayDocumentProvide ..	41
85	5.1.1.1.1 Umsetzung	42
86	5.1.1.2 Operation I_Document_Management::CrossGatewayQuery	44
87	5.1.1.2.1 Umsetzung	45
88	5.1.1.3 Operation I_Document_Management::RemoveDocuments	47
89	5.1.1.3.1 Umsetzung	48
90	5.1.1.4 Operation I_Document_Management::CrossGatewayRetrieve	48
91	5.1.1.4.1 Umsetzung	49
92	5.1.1.5 Operation I_Document_Management::RestrictedUpdateDocumentSet....	50
93	5.1.1.5.1 Umsetzung	52
94	5.1.2 Schnittstelle I_Document_Management_Insurant	53
95	5.1.2.1 Operation	
96	I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b.....	54
97	5.1.2.1.1 Umsetzung	56
98	5.1.2.2 Operation I_Document_Management_Insurant::RegistryStoredQuery....	57
99	5.1.2.2.1 Umsetzung	58
100	5.1.2.3 Operation I_Document_Management_Insurant::RemoveDocuments	59
101	5.1.2.3.1 Umsetzung	60
102	5.1.2.4 Operation I_Document_Management_Insurant::RetrieveDocumentSet...	61
103	5.1.2.4.1 Umsetzung	62
104	5.1.3 Schnittstelle I_Document_Management_Insurance	63
105	5.1.3.1 Operation	
106	I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b.....	64
107	5.1.3.1.1 Umsetzung	65
108	5.2 Aktenkontoverwaltung	66
109	5.2.1 Schnittstelle I_Account_Management_Insurant	66
110	5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount.....	66
111	5.2.1.1.1 Umsetzung	68
112	5.2.1.2 Operation I_Account_Management_Insurant::ResumeAccount.....	70

113	5.2.1.2.1 Umsetzung	71
114	5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents	73
115	5.2.1.3.1 Umsetzung	74
116	5.3 Zugriffskontrolle.....	74
117	5.3.1 Funktionsprinzip Policy Administration.....	75
118	5.3.2 Anforderungen an die Zugriffskontrollprüfung.....	78
119	5.3.2.1 Erstmalsiges Öffnen eines Verarbeitungskontextes	80
120	5.3.2.2 Berechtigung für einen Versicherten.....	80
121	5.3.2.3 Berechtigung für einen Vertreter.....	81
122	5.3.2.4 Berechtigung für eine Leistungserbringerinstitution	82
123	5.3.2.5 Berechtigung für einen Kostenträger	87
124	5.4 Vertrauenswürdige Ausführung.....	88
125	5.4.1 Schnittstelle I_Document_Management_Connect.....	88
126	5.4.1.1 Operation I_Document_Management_Connect::OpenContext	93
127	5.4.1.1.1 Umsetzung	94
128	5.4.1.2 Operation I_Document_Management_Connect::CloseContext	95
129	5.4.1.2.1 Umsetzung	96
130	5.4.2 Hardware Merkmale	97
131	6 Informationsmodelle	98
132	7 Anhang A Verzeichnisse.....	99
133	7.1 Abkürzungen	99
134	7.2 Glossar	101
135	7.3 Abbildungsverzeichnis.....	101
136	7.4 Tabellenverzeichnis.....	101
137	7.5 Referenzierte Dokumente.....	104
138	7.5.1 Dokumente der gematik.....	104
139	7.5.2 Weitere Dokumente.....	105
140	8 Anhang B XACML 2.0 Profile für Policy Documents	108
141	8.1 Policy Document für einen Versicherten.....	108
142	8.1.1 Base Policy.....	108
143	8.1.2 Permission Policy	111
144	8.2 Policy Document für einen Vertreter	142
145	8.2.1 Base Policy.....	142
146	8.2.2 Permission Policy	146
147	8.3 Policy Document für eine Leistungserbringerinstitution	174
148	8.3.1 Permission Policy zum Zugriff auf Leistungserbringer Dokumente.....	174
149	8.3.2 Permission Policy zum Zugriff auf Versicherten und Kostenträger Dokumente	200
150	200
151	8.4 Policy Document für einen Kostenträger	224
152	8.4.1 Base Policy.....	224
153	8.4.2 Permission Policy	227
154	1 Einführung	10

155	1.1 Zielsetzung	10
156	1.2 Zielgruppe	10
157	1.3 Geltungsbereich	10
158	1.4 Abgrenzungen	10
159	1.5 Methodik	11
160	2 Systemkontext.....	12
161	3 Zerlegung der Komponente.....	13
162	4 Übergreifende Festlegungen	14
163	4.1 Namensräume	14
164	4.2 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von	
165	Dokumenten.....	15
166	4.2.1 Anforderungen an IHE ITI-Akteure	15
167	4.2.1.1 APPC Content Consumer.....	17
168	4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren.....	17
169	4.2.1.1.2 Optionen des IHE ITI-Akteurs.....	17
170	4.2.1.2 RMU Update Responder.....	18
171	4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren.....	18
172	4.2.1.2.2 Optionen des IHE ITI-Akteurs.....	18
173	4.2.1.3 XCA Responding Gateway.....	19
174	4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren.....	19
175	4.2.1.3.2 Optionen des IHE ITI-Akteurs.....	19
176	4.2.1.4 XCDR Responding Gateway.....	19
177	4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren.....	19
178	4.2.1.4.2 Optionen des IHE ITI-Akteurs.....	20
179	4.2.1.5 XDS Document Registry	20
180	4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren.....	20
181	4.2.1.5.2 Optionen des IHE ITI-Akteurs.....	20
182	4.2.1.6 XDS Document Repository.....	21
183	4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren.....	21
184	4.2.1.6.2 Optionen des IHE ITI-Akteurs.....	21
185	4.2.1.7 XUA X-Service Provider	21
186	4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren.....	21
187	4.2.1.7.2 Optionen des IHE ITI-Akteurs.....	21
188	4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen.....	22
189	4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen.....	26
190	4.2.3.1 Provide X-User Assertion [ITI-40].....	26
191	4.2.3.2 Provide and Register Document Set-b [ITI-41].....	27
192	4.2.3.3 Remove Documents [ITI-86].....	28
193	4.3 Fehlerbehandlung in Schnittstellenoperationen	28
194	4.4 Vertrauenswürdige Ausführungsumgebung	29

195	4.4.1 Verarbeitungskontext	30
196	4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	31
197	4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes	32
198	4.4.4 Parallele Zugriffe.....	33
199	4.4.5 Konsistenz der Akte, Logging und Monitoring	33
200	4.4.6 Client-Verbindungen zum Verarbeitungskontext	33
201	4.5 Anforderungen zur sicherheitstechnischen Validierung	35
202	4.6 Protokollierung.....	37
203	5 Funktionsmerkmale	40
204	5.1 Dokumentenverwaltung	40
205	5.1.1 Schnittstelle I_Document_Management.....	40
206	5.1.1.1 Operation I_Document_Management::CrossGatewayDocumentProvide ..	41
207	5.1.1.1.1 Umsetzung	42
208	5.1.1.2 Operation I_Document_Management::CrossGatewayQuery	44
209	5.1.1.2.1 Umsetzung	45
210	5.1.1.3 Operation I_Document_Management::RemoveDocuments	47
211	5.1.1.3.1 Umsetzung	48
212	5.1.1.4 Operation I_Document_Management::CrossGatewayRetrieve	48
213	5.1.1.4.1 Umsetzung	49
214	5.1.1.5 Operation I_Document_Management::RestrictedUpdateDocumentSet	50
215	5.1.1.5.1 Umsetzung	52
216	5.1.2 Schnittstelle I_Document_Management_Insurant	53
217	5.1.2.1 Operation	
218	I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b.....	54
219	5.1.2.1.1 Umsetzung	56
220	5.1.2.2 Operation I_Document_Management_Insurant::RegistryStoredQuery	57
221	5.1.2.2.1 Umsetzung	58
222	5.1.2.3 Operation I_Document_Management_Insurant::RemoveDocuments	59
223	5.1.2.3.1 Umsetzung	60
224	5.1.2.4 Operation I_Document_Management_Insurant::RetrieveDocumentSet...	61
225	5.1.2.4.1 Umsetzung	62
226	5.1.3 Schnittstelle I_Document_Management_Insurance	63
227	5.1.3.1 Operation	
228	I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b.....	64
229	5.1.3.1.1 Umsetzung	65
230	5.2 Aktenkontoverwaltung	66
231	5.2.1 Schnittstelle I_Account_Management_Insurant	66
232	5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount	66
233	5.2.1.1.1 Umsetzung	68
234	5.2.1.2 Operation I_Account_Management_Insurant::ResumeAccount	70
235	5.2.1.2.1 Umsetzung	71
236	5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents	73
237	5.2.1.3.1 Umsetzung	74
238	5.3 Zugriffskontrolle.....	74
239	5.3.1 Funktionsprinzip Policy Administration.....	75

240	5.3.2 Anforderungen an die Zugriffskontrollprüfung.....	78
241	5.3.2.1 Erstmaliges Öffnen eines Verarbeitungskontextes	80
242	5.3.2.2 Berechtigung für einen Versicherten.....	80
243	5.3.2.3 Berechtigung für einen Vertreter.....	81
244	5.3.2.4 Berechtigung für eine Leistungserbringerinstitution	82
245	5.3.2.5 Berechtigung für einen Kostenträger	87
246	5.4 Vertrauenswürdige Ausführung.....	88
247	5.4.1 Schnittstelle I_Document_Management_Connect.....	88
248	5.4.1.1 Operation I_Document_Management_Connect::OpenContext	93
249	5.4.1.1.1 Umsetzung	94
250	5.4.1.2 Operation I_Document_Management_Connect::CloseContext.....	95
251	5.4.1.2.1 Umsetzung	96
252	5.4.2 Hardware-Merkmale	97
253	6 Informationsmodelle	98
254	7 Anhang A – Verzeichnisse	99
255	7.1 Abkürzungen	99
256	7.2 Glossar	101
257	7.3 Abbildungsverzeichnis.....	101
258	7.4 Tabellenverzeichnis.....	101
259	7.5 Referenzierte Dokumente.....	104
260	7.5.1 Dokumente der gematik.....	104
261	7.5.2 Weitere Dokumente.....	105
262	8 Anhang B – XACML 2.0-Profile für Policy Documents	108
263	8.1 Policy Document für einen Versicherten.....	108
264	8.1.1 Base Policy.....	108
265	8.1.2 Permission Policy	111
266	8.2 Policy Document für einen Vertreter	142
267	8.2.1 Base Policy.....	142
268	8.2.2 Permission Policy	146
269	8.3 Policy Document für eine Leistungserbringerinstitution	174
270	8.3.1 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente.....	174
271	8.3.2 Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente	
272	200
273	8.4 Policy Document für einen Kostenträger	224
274	8.4.1 Base Policy.....	224
275	8.4.2 Permission Policy	227
276		

277

1 Einführung

278 1.1 Zielsetzung

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

284 1.2 Zielgruppe

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

288 1.3 Geltungsbereich

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

294 Schutzrechts-/Patentrechtshinweis

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

303 1.4 Abgrenzungen

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

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

311 **1.5 Methodik**

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

316
317 **<AFO-ID> - <Titel der Afo>**
318 Text / Beschreibung
319 [\leq]

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

322

ENTWURF

323

2 Systemkontext

324 Die Komponente ePA-Dokumentenverwaltung des Produkttyps ePA-Aktensystem
325 [gemSpec_Aktensystem] dient dem sicheren Speichern und Auffinden von Dokumenten
326 des Versicherten aus seiner persönlichen Akte durch berechnigte Nutzer. Diese sind der
327 Versicherte selbst oder von ihm benannte Vertreter
328 sowie Leistungserbringerinstitutionen.

329 Zur Umsetzung der ePA-Dokumentenverwaltung wird auf das Repository Registry-
330 Designmuster zurück gegriffen. Eine Document Registry verwaltet Metadaten, welche für
331 die Suche und Navigation von Dokumenten notwendig sind. Die Dokumente werden
332 verschlüsselt in einem Document Repository gespeichert. Die Schnittstellen der
333 Komponente ePA-Dokumentenverwaltung basieren auf den Spezifikationen von
334 Integrating the Healthcare Enterprise (IHE), insbesondere dem Konzept Cross-Enterprise
335 Document Sharing (XDS) zum Speichern und Abrufen von (medizinischen) Dokumenten,
336 welches Teil des IHE ITI Technical Frameworks (IHE ITI TF) ist. IHE ist eine
337 internationale Organisation, welche bestehende Industriestandards für die Umsetzung
338 spezifischer Anwendungsszenarien im digitalisierten Gesundheitswesen profiliert.

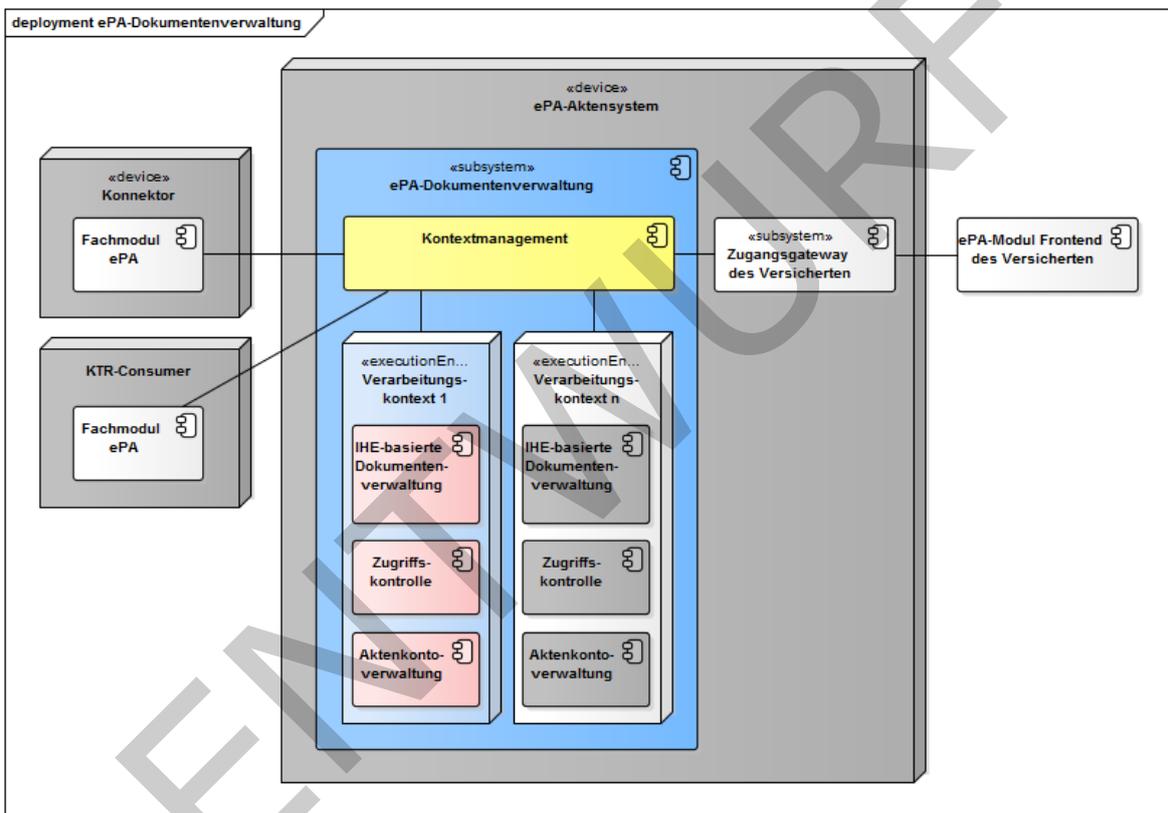
339 Neben der verschlüsselten Datenhaltung für Dokumente sieht die Komponente ePA-
340 Dokumentenverwaltung eine Vertrauenswürdige Ausführungsumgebung (VAU) vor,
341 welche es erlaubt, Metadaten im Klartext zu verarbeiten und somit Suchanfragen auf
342 Dokumente bedienen zu können. Mit der Abschottung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

347

3 Zerlegung der Komponente

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

356



357

358

Abbildung 1: Komponentenzersetzung ePA-Dokumentenverwaltung

359

4 Übergreifende Festlegungen

360 **A_15033 - Komponente ePA-Dokumentenverwaltung – Verwendung des SAML**
 361 **Token Profile 1.1 für Web Services Security bei SAML 2.0 Assertions**
 362 Die Komponente ePA-Dokumentenverwaltung MUSS die Anforderungen aus [WSS-SAML]
 363 umsetzen, wenn eine SAML 2.0 Assertion Teil einer SOAP 1.2-Eingangsnachricht ist. [<=]

364 **A_15035 - Komponente ePA-Dokumentenverwaltung – Verwendung von SOAP**
 365 **Message Security 1.1**
 366 Die Komponente ePA-Dokumentenverwaltung MUSS die Sicherheitsanforderungen aus
 367 SOAP Message Security 1.1 [WSS] für die Verarbeitung von SOAP 1.2-Nachrichten
 368 umsetzen. [<=]

369 **A_15034 - Komponente ePA-Dokumentenverwaltung – Unterstützung von**
 370 **Profilen der Web Services Interoperability Organization (WS-I)**
 371 Die Komponente ePA-Dokumentenverwaltung MUSS das WS-I Basic Profile
 372 V2.0 [WSIBP], das WS-I Basic Security Profile Version V1.1 [WSIBSP] sowie das WS-I
 373 Attachment Profile V1.0 [WSIAP] für die Kommunikation über Web Services
 374 berücksichtigen. [<=]

4.1 Namensräume

376 Für die Spezifikation der Schnittstellen der Komponente ePA-Dokumentenverwaltung
 377 werden die folgenden XML-Präfixe verwendet, um den Namensraum bzw. das Vokabular
 378 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

379 4.2 Nutzung von IHE IT Infrastructure-Profilen für Speicherung 380 und Abruf von Dokumenten

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

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

394 **A_17826 - Komponente ePA-Dokumentenverwaltung – Außenverhalten der IHE** 395 **ITI-Implementierung**

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

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

405 4.2.1 Anforderungen an IHE ITI-Akteure

406 **A_13805 - Komponente ePA-Dokumentenverwaltung – Implementierung des** 407 **IHE ITI-Akteurs XCDR Responding Gateway**

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

410 **A_13806 - Komponente ePA-Dokumentenverwaltung – Implementierung des** 411 **IHE ITI-Akteurs XDS Document Registry**

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

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

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

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

420 Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XCA Responding
421 Gateway" gemäß [IHE-ITI-TF1] implementieren. [<=]

422 Die § 291a-konforme Protokollierung von Zugriffen erfolgt mit Mechanismen außerhalb
423 des IHE ITI-TF. Eine technische Protokollierung via ATNA kann gemäß der Anforderung
424 A_17826 dennoch erfolgen.

425 **A_13809 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung**
426 **des IHE ITI-Akteurs ATNA Audit Record Repository**

427 Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "ATNA
428 Audit Record Repository" gemäß [IHE-ITI-TF1] implementieren. [<=]

429 Die Mechanismen der IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure
430 Application" zur Node Authentication werden über das Konzept "Vertrauenswürdige
431 Ausführungsumgebung" (vgl. Abschnitt 4.4) umgesetzt, sodass die Nutzung des
432 Integrationsprofils ATNA diesbzgl. eingeschränkt wird.

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

436 Die Komponente ePA-Dokumentenverwaltung DARF zur Node Authentication die IHE ITI-
437 Akteure "ATNA Secure Node" sowie "ATNA Secure Application" gemäß [IHE-ITI-TF1]
438 NICHT implementieren.

439 [<=]

440 Der Zeitdienst der Telematikinfrastruktur unterstützt das Network Time Protocol in
441 Version 4. Das IHE ITI-TF verlangt hingegen, das Zeitsynchronisierungsprotokoll in
442 Version 3.

443 **A_14654 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung**
444 **des IHE ITI-Akteurs CT Time Client**

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

447 **A_14655 - Komponente ePA-Dokumentenverwaltung – Zeitsynchronisation über**
448 **Zeitdienst in der TI**

449 Die Komponente ePA-Dokumentenverwaltung MUSS die Systemzeit über den Zeitdienst
450 in der TI gemäß [gemSpec_Net#5.2] synchronisieren.

451 [<=]

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

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

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

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

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

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

464 [\leq]

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

467 Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS
468 Document Consumer" gemäß [IHE-ITI-TF1] implementieren. [\leq]

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

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

473 [\leq]

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

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

478 [\leq]

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

481 Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "APPC Content
482 Consumer" gemäß [IHE-ITI-APPC] implementieren. [\leq]

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

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

489 [\leq]

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

492 Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "RMU Update
493 Responder" gemäß [IHE-ITI-RMU] implementieren. [\leq]

494 **4.2.1.1 APPC Content Consumer**

495 *4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren*

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

497 *4.2.1.1.2 Optionen des IHE ITI-Akteurs*

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

500 Die Komponente ePA-Dokumentenverwaltung als APPC-Akteur "Content Consumer" DARF
501 NICHT die Option "View Option" unterstützen. [\leq]

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

504 Die Komponente ePA-Dokumentenverwaltung als APPC-Akteur "Content Consumer"
505 MUSS die Option "Structured Policy Processing Option" unterstützen.[<=]

506 **4.2.1.2 RMU Update Responder**

507 *4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren*

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

510 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
511 mit dem XCA-Akteur "Responding Gateway" gemäß [IHE-ITI-RMU] sowie mit dem XUA-
512 Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions
513 verarbeiten.
514 [<=]

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

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

519 *4.2.1.2.2 Optionen des IHE ITI-Akteurs*

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

522 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF
523 NICHT die Option "Forward Update" unterstützen.
524 [<=]

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

527 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
528 die Option "XCA Persistence" unterstützen.
529 [<=]

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

532 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF
533 NICHT die Option "XDS Persistence" unterstützen.
534 [<=]

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

537 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF
538 NICHT die Option "XDS Version Persistence" unterstützen.
539 [<=]

540 4.2.1.3 XCA Responding Gateway

541 4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren

542 **A_14598 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA** 543 **Responding Gateway mit X-Service Provider**

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

547 **A_14725 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA** 548 **Responding Gateway mit XDS Document Registry**

549 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
550 MUSS mit dem XDS-Akteur "Document Registry" gemäß [IHE-ITI-TF1] gruppiert
551 sein.[<=]

552 **A_14726 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA** 553 **Responding Gateway mit XDS Document Repository**

554 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
555 MUSS mit dem XDS-Akteur "Document Repository" gemäß [IHE-ITI-TF1] gruppiert
556 sein.[<=]

557 **A_14784 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA** 558 **Responding Gateway mit APPC Content Consumer**

559 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
560 MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert
561 sein.[<=]

562 4.2.1.3.2 Optionen des IHE ITI-Akteurs

563 **A_13819 - Komponente ePA-Dokumentenverwaltung – XCA Responding** 564 **Gateway ohne "On-Demand Documents"-Option**

565 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
566 DARF NICHT die Option "On-Demand Documents" unterstützen.[<=]

567 **A_13820 - Komponente ePA-Dokumentenverwaltung – XCA Responding** 568 **Gateway ohne "Persistence of Retrieved Documents"-Option**

569 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
570 DARF NICHT die Option "Persistence of Retrieved Documents" unterstützen.[<=]

571 4.2.1.4 XCDR Responding Gateway

572 4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren

573 **A_13648 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR** 574 **Responding Gateway mit X-Service Provider**

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

578 **A_14723 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR** 579 **Responding Gateway mit XDS Document Registry**

580 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
581 MUSS mit dem XDS-Akteur "Document Registry" gemäß [IHE-ITI-XCDR] gruppiert
582 sein.[<=]

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

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

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

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

593 *4.2.1.4.2 Optionen des IHE ITI-Akteurs*

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

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

598

599 **4.2.1.5 XDS Document Registry**

600 *4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren*

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

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

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

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

610 *4.2.1.5.2 Optionen des IHE ITI-Akteurs*

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

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

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

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

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

621 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF
622 NICHT die Option "Patient Identity Feed" unterstützen.
623 [<=]

624 **A_14640 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry**
625 **ohne "Patient Identity Feed HL7v3"-Option**
626 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF
627 NICHT die Option "Patient Identity Feed HL7v3" unterstützen.
628 [**<=**]

629 **A_14641 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry**
630 **ohne "On-Demand Documents"-Option**
631 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF
632 NICHT die Option "On-Demand Documents" unterstützen.
633 [**<=**]

634 **A_14642 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry**
635 **ohne "Document Metadata Update"-Option**
636 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF
637 NICHT die Option "Document Metadata Update" unterstützen. [**<=**]

638 **4.2.1.6 XDS Document Repository**

639 *4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren*

640 **A_14600 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS**
641 **Document Repository mit X-Service Provider**
642 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
643 MUSS mit dem XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und
644 X-User Assertions verarbeiten. [**<=**]

645 **A_14786 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS**
646 **Document Repository mit APPC Content Consumer**
647 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
648 MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert
649 sein. [**<=**]

650 *4.2.1.6.2 Optionen des IHE ITI-Akteurs*

651 **A_14636 - Komponente ePA-Dokumentenverwaltung – XDS Document**
652 **Repository ohne "Asynchronous Web Services Exchange"-Option**
653 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
654 DARF NICHT die Option "Asynchronous Web Services Exchange" unterstützen. [**<=**]

655 **4.2.1.7 XUA X-Service Provider**

656 *4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren*

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

658 *4.2.1.7.2 Optionen des IHE ITI-Akteurs*

659 **A_14612 - Komponente ePA-Dokumentenverwaltung – XUA X-Service Provider**
660 **ohne "Subject-Role"-Option**
661 Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" DARF
662 NICHT die Option "Subject-Role" unterstützen. [**<=**]

663 **A_14613 - Komponente ePA-Dokumentenverwaltung – XUA X-Service Provider**
 664 **ohne "Authz-Consent"-Option**
 665 Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" DARF
 666 NICHT die Option "Authz-Consent" unterstützen.[<=]

667 **A_14614 - Komponente ePA-Dokumentenverwaltung – XUA X-Service Provider**
 668 **ohne "PurposeOfUse"-Option**
 669 Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" DARF
 670 NICHT die Option "PurposeOfUse" unterstützen.[<=]

671

672 **4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen**

673 Die folgende Tabelle fasst die oben definierten Anforderungen zu Gruppierungen und
 674 Optionen zusammen. Dabei wird die folgende Notation für Optionalitäten (Opt.)
 675 verwendet:

676 **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.

677

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

IHE ITI-Akteur	Opt.	Gruppierung mit anderem IHE ITI-Akteur		Umzusetzende Option des IHE ITI-Akteurs	Opt.
			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	

680 **4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren**
 681 **Schnittstellen**

682 **A_17832 - Komponente ePA-Dokumentenverwaltung – Unterstützung**
 683 **MTOM/XOP**

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

687 **4.2.3.1 Provide X-User Assertion [ITI-40]**

688 **A_14915 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide**
 689 **X-User Assertion**

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

- 692 • I_Document_Management::CrossGatewayDocumentProvide
- 693 • I_Document_Management::CrossGatewayQuery
- 694 • I_Document_Management::RemoveDocuments
- 695 • I_Document_Management::CrossGatewayRetrieve
- 696 • I_Document_Management::RestrictedUpdateDocumentSet
- 697 • I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- 698 • I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- 699 • I_Document_Management_Insurant::RegistryStoredQuery
- 700 • I_Document_Management_Insurant::RemoveDocuments
- 701 • I_Document_Management_Insurant::RetrieveDocumentSet

702 hinsichtlich der Validierung der X-User Assertion (Authentication Assertion) gemäß der
 703 definierten Ablauflogik in [IHE-ITI-TF2b#3.40.4.1.2 und 3.40.4.1.3] implementieren.
 704 [<=]

705 **A_14594 - Komponente ePA-Dokumentenverwaltung – Validierung der**
706 **Authentication Assertion**

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

711 **4.2.3.2 Provide and Register Document Set-b [ITI-41]**

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

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

719
720 [<=]

721 **A_15162 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung bei**
722 **Angabe von Document Entry Relationships in Metadaten**

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

- 727
- `urn:ihe:iti:2007:AssociationType:RPLC` (Replace)
 - 728 • `urn:ihe:iti:2007:AssociationType:XFRM` (Transform)
 - 729 • `urn:ihe:iti:2007:AssociationType:APND` (Addendum)
 - 730 • `urn:ihe:iti:2007:AssociationType:XFRM_RPLC` (Replace with Transformation)
 - 731 • `urn:ihe:iti:2007:AssociationType:signs` (Digital Signature)
 - 732 • `urn:ihe:iti:2010:AssociationType:IsSnapshotOf` (Snapshot of On-Demand
733 document entry)

734 [<=]

735 **A_14937 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße**
736 **prüfen**

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

744 [<=]

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

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

752 als XDS-Akteur "Document Repository" MUSS das Registrieren und Speichern von
753 Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`
754 quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. Es MUSS
755 im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements angegeben
756 werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht.[<=]

757 **4.2.3.3 Remove Documents [ITI-86]**

758 **A_14926 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen** 759 **der Metadaten bei Löschung von Dokumenten**

760 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
761 MUSS die mit den zu löschenden Dokumenten assoziierten Metadaten in der Document
762 Registry löschen, bevor die Dokumente gelöscht werden und das assoziierte Submission
763 Set löschen, sofern kein weiteres Dokument mit diesem Submission Set assoziiert
764 ist.[<=]

765 **A_14670-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement** 766 **für Remove Documents**

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

780 **4.3 Fehlerbehandlung in Schnittstellenoperationen**

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

787 **A_15664 - Komponente ePA-Dokumentenverwaltung – Fehlername**

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

791 **A_15665 - Komponente ePA-Dokumentenverwaltung – Fehlertext**

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

796 **A_15666 - Komponente ePA-Dokumentenverwaltung – Fehlernummer**
 797 Die Komponente ePA-Dokumentenverwaltung MUSS in einer GERROR-Fehlermeldung
 798 gemäß [TelematikError.xsd] die folgenden Fehlercodes im
 799 Feld `tel:Error/tel:Trace/tel:Code` verwenden:

800
 801 **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

802 [`<=`]

803 4.4 Vertrauenswürdige Ausführungsumgebung

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

§11 **A_14472-01A_14472 - Komponente ePA-Dokumentenverwaltung – Umsetzung 812 des Dokumentenmanagements in einer Vertrauenswürdigen 813 Ausführungsumgebung (VAU)**

814 Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der Operationen
 815 der Schnittstellen `I_Document_Management_Connect`,
 §16 `I_Document_ManagementManagement`, `I_Document_Management_Insurance` sowie
 817 `I_Document_Management_Insurant` im Verarbeitungskontext einer Vertrauenswürdigen
 818 Ausführungsumgebung (VAU) umsetzen. [`<=`]

§19

820 **A_18714 - Komponente ePA-Dokumentenverwaltung – Verhalten des 821 Kontextmanagements bei ungeöffnetem Verarbeitungskontext**

822 Das Kontextmanagement MUSS mit einer `VAUServerError`-Nachricht und HTTP-Fehler
 823 403 (Fehlermeldung "Access Denied") antworten, wenn für eine Web-Service-Operation
 824 der Schnittstellen `I_Document_Management`, `I_Document_Management_Insurant`,
 825 `I_Document_Management_Insurance` sowie `I_Account_Management_Insurant` für den
 826 angemeldeten Nutzer kein Verarbeitungskontext geöffnet wurde.
 827 [`<=`]

828 4.4.1 Verarbeitungskontext

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

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

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

843 **A_14557 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext** 844 **der VAU**

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

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

853 **A_14581 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung von** 854 **außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten**

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

858 **A_14582 - Komponente ePA-Dokumentenverwaltung – Geschützte Weitergabe** 859 **von Daten an autorisierte Nutzer durch die VAU**

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

863 **A_14583 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung der** 864 **Dokumentmetadaten und technischen Daten der VAU**

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

869 **A_14566 - Komponente ePA-Dokumentenverwaltung – Isolation zwischen** 870 **Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU**

871 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die in ihr ablaufenden
872 Verarbeitungen für die Daten eines Verarbeitungskontextes von den Verarbeitungen für
873 die Daten anderer Verarbeitungskontexte in solcher Weise trennen, dass mit technischen
874 Mitteln ausgeschlossen wird, dass die Verarbeitungen eines Verarbeitungskontextes
875 schadhaf auf die Verarbeitungen eines anderen Verarbeitungskontextes einwirken
876 können.[<=]

877 **4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem** 878 **Betriebsumfeld**

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

882 **A_14558 - Komponente ePA-Dokumentenverwaltung – Isolation der VAU von** 883 **Datenverarbeitungsprozessen des Anbieters**

884 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die in ihren
885 Verarbeitungskontexten ablaufenden Datenverarbeitungsprozesse von allen sonstigen
886 Datenverarbeitungsprozessen des Anbieters trennen und damit gewährleisten, dass der
887 Anbieter ePA-Aktensystem vom Zugriff auf die in der VAU verarbeiteten schützenswerten
888 Daten ausgeschlossen ist. [\leq]

889 **A_14559 - Komponente ePA-Dokumentenverwaltung – Ausschluss von** 890 **Manipulationen an der Software der VAU**

891 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS eine Manipulation der
892 eingesetzten Software erkennen und eine Ausführung der manipulierten Software
893 verhindern. [\leq]

894 **A_14560 - Komponente ePA-Dokumentenverwaltung – Ausschluss von** 895 **Manipulationen an der Hardware der VAU**

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

899 **A_14561 - Komponente ePA-Dokumentenverwaltung – Kontinuierliche** 900 **Wirksamkeit des Manipulationsschutzes der VAU**

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

905 **A_14562 - Komponente ePA-Dokumentenverwaltung – Kein physischer Zugang** 906 **des Anbieters zu Systemen der VAU**

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

911 **A_14563 - Komponente ePA-Dokumentenverwaltung – Nutzdatenbereinigung** 912 **vor physischem Zugang zu Systemen der VAU**

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

917 **A_14564 - Komponente ePA-Dokumentenverwaltung – Private Schlüssel von** 918 **Dienstzertifikaten im HSM**

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

- 921 • TI-Fachdienst-Identität zur Authentisierung des Kontextmanagements gegenüber
922 dem Fachmodul ePA (TLS)
- 923 • TI-Fachdienst-Identität zur Authentisierung des Verarbeitungskontextes
924 gegenüber dem Fachmodul ePA (sicherer Kanal auf Anwendungsebene),

- 925 • Privater Schlüssel des Schlüsselpaars zur Authentisierung des
926 Verarbeitungskontextes gegenüber dem ePA-Frontend des Versicherten (sicherer
927 Kanal auf Anwendungsebene).

928 Die Prüftiefe des HSM MUSS dabei den in [gemSpec_Aktensystem#A_15156]
929 angegebenen Standards entsprechen.
930 [<=]

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

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

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

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

944 **4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes**

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

953 **A_14568 - Komponente ePA-Dokumentenverwaltung – Aktivierung des
954 Verarbeitungskontextes der VAU**

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

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

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

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

970 Im Falle einer fehlgeschlagenen Prüfung des Kontextschlüssels MUSS die VAU die
971 Verbindung zum Nutzer mit einer Fehlermeldung sofort beenden. Im Sonderfall eines
972 erstmaligen Verbindungsaufbaus mit einem Verarbeitungskontext DARF die VAU die

973 Verbindung NICHT abbrechen und MUSS die Daten des Verarbeitungskontextes mit Hilfe
974 des Kontextschlüssels verschlüsseln. [<=]

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

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

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

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

985 **4.4.4 Parallele Zugriffe**

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

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

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

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

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

998 **4.4.5 Konsistenz der Akte, Logging und Monitoring**

999 **A_14573 - Komponente ePA-Dokumentenverwaltung – Konsistenter**
1000 **Systemzustand des Verarbeitungskontextes der VAU**

1001 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass ein
1002 konsistenter Zustand des Verarbeitungskontextes auch bei Bedienfehlern oder
1003 technischen Problemen immer erhalten bleibt bzw. wiederhergestellt werden kann. [<=]

1004 **A_14574 - Komponente ePA-Dokumentenverwaltung – Datenschutzkonformes**
1005 **Logging und Monitoring des Verarbeitungskontextes der VAU**

1006 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die für den Betrieb eines
1007 Fachdienstes erforderlichen Logging- und Monitoring-Informationen in solcher Art und
1008 Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass
1009 dem Anbieter ePA-Aktensystem vertrauliche oder zur Profilbildung geeignete Daten zur
1010 Kenntnis gelangen. [<=]

1011 **4.4.6 Client-Verbindungen zum Verarbeitungskontext**

1012 Um Verbindungen vom Fachmodul ePA nach [gemSpec_FM_ePA,
1013 gemSpec_FM_ePA_KTR_Consumer] und ePA-Modul Frontend des Versicherten nach
1014 [gemSpec_FdV_ePA] zum Verarbeitungskontext des Aktenkontos zu ermöglichen, ist ein
1015 Kontextmanagement erforderlich. Das Kontextmanagement ist im Netzwerk der TI für
1016 das Fachmodul ePA und für das ePA-Modul Frontend des Versicherten unter mindestens

1017 einer IP-Adresse/Port-Kombination erreichbar, die im Namensdienst der TI registriert
1018 sein muss. Das Kontextmanagement initialisiert und terminiert Verarbeitungskontexte
1019 bedarfsgesteuert und vermittelt die Verbindungen zwischen dem Client und dem jeweils
1020 benötigten Verarbeitungskontext.

1021 **A_14616 - Komponente ePA-Dokumentenverwaltung – Kontextmanagement der**
1022 **Vertrauenswürdigen Ausführungsumgebung**

1023 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS ein Kontextmanagement
1024 bereitstellen, das Verarbeitungskontexte bedarfsgesteuert initialisiert und terminiert,
1025 über initialisierte Verarbeitungskontexte auf der Basis ihrer RecordIdentifier Buch
1026 führt und Verbindung zwischen Clients und den jeweils benötigten
1027 Verarbeitungskontexten vermittelt. [`<=`]

1028 **A_14575 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontexte**
1029 **der VAU über gemeinsame Host-Adresse erreichbar**

1030 Die VAU der Komponente ePA-Dokumentenverwaltung MUSS ihre Verarbeitungskontexte
1031 über gemeinsame IP-Adressen und Ports des Kontextmanagements der ePA-
1032 Dokumentenverwaltung erreichbar machen. [`<=`]

1033 **A_14576 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom ePA-**
1034 **Modul Frontend des Versicherten zum Verarbeitungskontextes der VAU über das**
1035 **Zugangsgateway**

1036 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS
1037 Verbindungen vom ePA-Modul Frontend des Versicherten ausschließlich über das
1038 Zugangsgateway des Versicherten akzeptieren. [`<=`]

1039 **A_15528 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom**
1040 **Fachmodul ePA zum Verarbeitungskontextes der VAU über das**
1041 **Kontextmanagement**

1042 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS
1043 Verbindungen vom Fachmodul ePA ausschließlich über TLS akzeptieren. Es MUSS die
1044 TLS-Verbindung terminieren und HTTP Requests und Responses zwischen dem
1045 Fachmodul ePA und dem für die jeweilige Sitzung zugeordneten Verarbeitungskontext
1046 der VAU vermitteln. [`<=`]

1047 **A_17834 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom**
1048 **Fachmodul ePA KTR-Consumer zum Verarbeitungskontextes der VAU über das**
1049 **Kontextmanagement**

1050 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS
1051 Verbindungen vom Fachmodul ePA KTR-Consumer ausschließlich über TLS akzeptieren.
1052 Es MUSS die TLS-Verbindung terminieren und HTTP Requests und Responses zwischen
1053 dem Fachmodul ePA KTR-Consumer und dem für die jeweilige Sitzung zugeordneten
1054 Verarbeitungskontext der VAU vermitteln.
1055 [`<=`]

1056 **A_14577 - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal zum**
1057 **Verarbeitungskontext der VAU auf Inhaltsebene**

1058 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS dem ePA-
1059 Modul Frontend des Versicherten, dem Fachmodul ePA sowie dem Fachmodul ePA KTR-
1060 Consumer den Aufbau eines sicheren Kanals, d.h. einen Verbindungsaufbau gemäß
1061 [gemSpec_Krypt#3.15], zum Verarbeitungskontext auf Inhaltsebene ermöglichen. [`<=`]

1062 **A_14580 - Komponente ePA-Dokumentenverwaltung – Identität der**
1063 **Dokumentenverwaltung für das Fachmodul ePA und Fachmodul ePA KTR-**
1064 **Consumer**

1065 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS sich
1066 innerhalb der TI mittels der Fachdienstidentität `oid_epa_dvw` mit Zertifikatsprofil
1067 `C.FD.TLS-S` ausweisen. [`<=`]

1068 **A_15646 - Komponente ePA-Dokumentenverwaltung – Identität des**
1069 **Verarbeitungskontextes für Clients**
1070 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS sich
1071 gegenüber dem Fachmodul ePA, dem Fachmodul ePA KTR-Consumer sowie dem ePA-
1072 Modul Frontend des Versicherten mittels der Fachdienstidentität `oid_epa_vau` mit
1073 Zertifikatsprofil `C.FD.AUT` ausweisen.
1074 [`<=`]

1075 **A_15183 - Komponente ePA-Dokumentenverwaltung – Automatisierter Abbau**
1076 **des sicheren Kanals bei Inaktivität**
1077 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS den
1078 sicheren Kanal zu einem Client nach 20 Minuten Inaktivität abbauen, sodass
1079 anschließend keine Zugriffe dieses Clients auf den Verarbeitungskontext mehr möglich
1080 sind, ohne dass eine neue Verbindung aufgebaut wird. [`<=`]

1081 **4.5 Anforderungen zur sicherheitstechnischen Validierung**

1082 **A_15186 - Komponente ePA-Dokumentenverwaltung – Prüfung der**
1083 **Kombination von WS-Addressing Action und SOAP Body**
1084 Die Komponente ePA-Dokumentenverwaltung MUSS vor einer Weiterverarbeitung
1085 sämtliche SOAP 1.2-Eingangsnachrichten dahingehend prüfen, ob die angegebene WS-
1086 Addressing Action zum SOAP Body passt. Ist diese Kombination nicht passend, MUSS die
1087 Komponente ePA-Dokumentenverwaltung die Nachricht mit einem HTTP-Statuscode 400
1088 gemäß [RFC7231] quittieren und die Verarbeitung der Nachricht abbrechen. [`<=`]

1089 **A_15585 - Komponente ePA-Dokumentenverwaltung – Gleichheit von SOAP**
1090 **Action und WS-Addressing Action**
1091 Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Eingangsnachrichten mit
1092 einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und die Verarbeitung der
1093 Nachricht abbrechen, falls die Werte aus SOAP Action (HTTP Header) und des `Action-`
1094 Elements [WSA] des SOAP Headers nicht übereinstimmen. [`<=`]

1095 **A_14465 - Komponente ePA-Dokumentenverwaltung – XML Schema-Validierung**
1096 **für SOAP-Eingangsnachrichten**
1097 Die Komponente ePA-Dokumentenverwaltung MUSS vor einer Weiterverarbeitung
1098 sämtliche SOAP 1.2-Eingangsnachrichten einer XML Schema-Validierung auf Basis
1099 ausschließlich intern vorliegender XML Schema-Definitionen unterziehen und gemäß
1100 [SOAP] verarbeiten. Sind Nachrichten nicht wohlgeformt oder gültig, MUSS die
1101 Komponente ePA-Dokumentenverwaltung die Nachricht mit einem HTTP-Statuscode 400
1102 gemäß [RFC7231] quittieren. [`<=`]

1103 **A_14809 - Komponente ePA-Dokumentenverwaltung – Keine Verwendung des**
1104 **"xsi:schemaLocation"-Attributs**
1105 Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Eingangsnachrichten mit
1106 einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren, falls ein `xsi:schemaLocation-`
1107 Attribut gemäß [XMLSchema#2.6.3] enthalten ist. [`<=`]

1108 **A_13690-01 - Komponente ePA-Dokumentenverwaltung – SAML 2.0 Assertion-**
1109 **Validierung**
1110 Die Komponente ePA-Dokumentenverwaltung MUSS die vorliegende Assertion einer
1111 grundsätzlichen XML Schema-Prüfung, einer Prüfung gemäß den Prüfvorschriften aus
1112 [gemSpec_TBAuth#3.2] sowie einer Prüfung auf Übereinstimmung mit dem
1113 erforderlichen SAML 2.0 Assertion-Profil aus [gemSpec_FM_ePA#A_14927,
1114 A_15638], [gemSpec_Authentisierung_Vers#A_14109, A_15631],
1115 [gemSpec_Autorisierung#A_14491] oder [gemSpec_FM_ePA_KTR_Consumer#A_17253,

1116 A_17254] unterziehen und die Verarbeitung der begleitenden Nachricht abbrechen und
 1117 gemäß [WSS#12] bzw. im Sonderfall der Authorization Assertion mit einer
 1118 VAUServerError-Nachricht (HTTP-Fehler 403, Fehlermeldung "Access Denied")
 1119 quittieren, falls eine Übereinstimmung nicht festgestellt werden kann.
 1120
 1121 Insbesondere MUSS das in der SAML 2.0 Assertion enthaltende Signaturzertifikat mittels
 1122 [gemSpec_PKI_018#TUC_PKI_018] mit den folgenden Parametern geprüft werden:

1123 **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

1124 Die Telematik-ID im Signaturzertifikat muss identisch mit der Telematik-ID in der
 1125 Identitätsbestätigung sein. [\leq]
 1126
 1127 [Der Hinweis unter \[gemSpec_Autorisierung\]#A_17655](#) gilt auch im vorliegenden
 1128 Prüfkontext, d.h. die dort beschriebene vereinfachte Prüfung kann für selbst ausgestellte
 1129 Identitätsbestätigungen dementsprechend auch im Kontext der hier thematisierten
 1130 Prüfung umgesetzt werden.

1131 **A_18990 - ePA-Dokumentenverwaltung – Beschränkung gültiger**
 1132 **Identitätsbestätigungen**

1133 Die Komponente ePA-Dokumentenverwaltung DARF in Aufrufen aus Richtung der
 1134 Komponente Zugangsgateway KEINE Identitätsbestätigung akzeptieren, die nicht durch
 1135 die Komponente Authentisierung (Versicherter) erstellt wurde. [\leq]

1136 **A_17386-01A_17386 - Komponente ePA-Dokumentenverwaltung –**
 1137 **Authentication Assertion-Validierung**

1138 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass Authentication
 1139 Assertions nur akzeptiert werden, wenn das zugehörige Signaturzertifikat zeitlich gültig
 1140 ist, nicht gesperrt wurde und [entweder](#) nach dem Zertifikatsprofil C.FD.SIG auf die
 1141 Identität der Komponente Authentisierung Versicherter [oder aber nach dem](#)
 1142 [Zertifikatsprofil C.HCI.OSIG auf die Identität einer SM-B](#) ausgestellt wurde.
 1143 [\leq]

1144 **A_17387 - Komponente ePA-Dokumentenverwaltung – Authorization Assertion-**
1145 **Validierung**

1146 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass Authorization
1147 Assertions nur akzeptiert werden, wenn das zugehörige Signaturzertifikat zeitlich gültig
1148 ist, nicht gesperrt wurde und nach dem Zertifikatsprofil C.FD.SIG auf die Identität der
1149 Komponente Autorisierung ausgestellt wurde.

1150 [`<=`]

1151 Dies kann durch eine aktuell gehaltene Konfiguration vertrauenswürdiger Zertifikate
1152 umgesetzt werden und ersetzt eine detaillierte Prüfung der Signaturzertifikate gem.
1153 [`gemSpec_TBAuth#A_15557`].

1154 Weitere Hinweise zur Validierung von SAML 2.0 Assertions können [`OWASP-SAML`]
1155 entnommen werden.

1156 **A_14735 - Komponente ePA-Dokumentenverwaltung – Verpflichtende Nutzung**
1157 **des "mustUnderstand"-Attributs im SOAP Security Header**

1158 Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Nachrichten mit SAML 2.0
1159 Assertions im SOAP Security Header mit einem HTTP-Statuscode 400 gemäß [`RFC7231`]
1160 quittieren, sofern das SOAP 1.2 `mustUnderstand`-Attribut im SOAP Security Header nicht
1161 angegeben ist oder den Wert `false` bzw. 0 hat ([`SOAP12#5.2.3`] [`WSS#5`]). [`<=`]

1162 **A_14810 - Komponente ePA-Dokumentenverwaltung – Erkennung von Denial-**
1163 **of-Service-Angriffen hinsichtlich dem Parsen von SOAP 1.2-Nachrichten**

1164 Die Komponente ePA-Dokumentenverwaltung MUSS die folgenden Angriffstypen in
1165 eingehenden SOAP 1.2-Nachrichten erkennen und mit einem HTTP-Statuscode 400
1166 gemäß [`RFC7231`] quittieren:

- 1167 • XML Injection
- 1168 • XPath Query Tampering
- 1169 • XML External Entity Injection

1170 [`<=`]

1171 Weitere Hinweise zur Erkennung von Denial-of-Service-Angriffen können [`OWASP-WSS`]
1172 und [`OWASP-IP`] entnommen werden.

1173 **A_14811 - Komponente ePA-Dokumentenverwaltung – Ablehnung von SOAP**
1174 **1.2-Nachrichten ohne UTF-8 Kodierung**

1175 Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Nachrichten mit
1176 einem HTTP-Statuscode 406 gemäß [`RFC7231`] quittieren, sofern die Zeichenkodierung
1177 im HTTP Header nicht UTF-8 benannt (`Content-Type: charset=utf-8`). [`<=`]

1178 **4.6 Protokollierung**

1179 Die Anforderungen an die Protokollierung für die Komponente ePA-
1180 Dokumentenverwaltung leiten sich aus dem Konzept der Protokollierung
1181 aus [`gemSysL_ePA#2.5.5`] ab.

1182 **A_14813 - Komponente ePA-Dokumentenverwaltung – Protokollierung in der**
1183 **Komponente ePA-Dokumentenverwaltung**

1184 Die Komponente ePA-Dokumentenverwaltung MUSS beim Aufruf einer der folgenden
1185 Operationen

- 1186 • `I_Document_Management::CrossGatewayDocumentProvide`
- 1187 • `I_Document_Management::CrossGatewayQuery`

- 1188 • I_Document_Management::RemoveDocuments
- 1189 • I_Document_Management::CrossGatewayRetrieve
- 1190 • I_Document_Management::RestrictedUpdateDocumentSet
- 1191 • I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- 1192 • I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- 1193 • I_Document_Management_Insurant::RegistryStoredQuery
- 1194 • I_Document_Management_Insurant::RemoveDocuments
- 1195 • I_Document_Management_Insurant::RetrieveDocumentSet
- 1196 • I_Account_Management_Insurant::GetAuditEvents
- 1197 • I_Account_Management_Insurant::SuspendAccount
- 1198 • I_Account_Management_Insurant::ResumeAccount

1199 je einen Eintrag im § 291a-Protokoll für den Versicherten
 1200 gemäß [gemSpec_DM_ePA#A_14471] mit folgenden vom Operationsaufruf abhängigen
 1201 Parametern vornehmen: UserID, UserName, ObjectID, und ObjectName.
 1202 [`<=`]

1203 **A_14816-01 - Komponente ePA-Dokumentenverwaltung – Parameter des §**
 1204 **291a-Protokolls**

1205 Die Komponente ePA-Dokumentenverwaltung MUSS einen Protokolleintrag gemäß der
 1206 Festlegung in [gemSpec_DM_ePA#A_14471] wie folgt erzeugen:
 1207

1208 **Tabelle 5: Tab_Dokv_13 - Parameter des § 291a-Protokolls**

Protokollparameter	Parameterwerte gemäß aufgerufener Operation
User-ID	Bei Aufrufen einer Operation der Schnittstellen <i>I_Document_Management, I_Document_Management_Insurance</i> sowie <i>I_Document_Management_Insurant</i> : XPath-Ausdruck zur " Subject ID" der im Operationsaufruf übergebenen Authentication Assertion: <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	Bei Aufrufen einer Operation der Schnittstellen <i>I_Document_Management</i> : XPath-Ausdruck zur "XSPA Organization" der im Operationsaufruf übergebenen Authentication Assertion: <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- </pre>

	<pre>name()='AttributeValue']/text() [normalize-space()]</pre> <p><i>I_Document_Management_Insurance und I_Document_Management_Insurant:</i> XPath-Ausdruck zum SAML Subject der im Operationsaufruf übergebenen Authentication Assertion: <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></p>
Object-ID	<p>Der unveränderbare Anteil der KVNR des extension-Attributs aus dem InsurantId-Element des RecordIdentifier-Elements oder die documentEntry.patientId des entsprechenden Operationsaufrufs</p> <p><i>Hinweis: Bei Aufruf von Operationen ohne diesen Parameter wird der Wert im Protokolleintrag nicht belegt.</i></p> <p>Bei Zugriffen auf Dokumente über die Transaktionen CrossGatewayDocumentProvide, ProvideAndRegisterDocumentSet-b, CrossGatewayRetrieve, RetrieveDocumentSet, RemoveDocuments, RestrictedUpdateDocument MUSS die Document Unique ID im Element ParticipantObjectDetail hinterlegt werden. Als Attribut type MUSS der Wert DocumentUniqueId und als Attribut value der Wert der Document Unique ID verwendet werden.</p>
Object Name	<p>Bei Zugriffen auf Dokumente über die Transaktionen CrossGatewayDocumentProvide, ProvideAndRegisterDocumentSet-b, CrossGatewayRetrieve, RetrieveDocumentSet, RemoveDocuments, RestrictedUpdateDocument MUSS der Document Title im Element ParticipantObjectDetail hinterlegt werden. Als Attribut type MUSS der Wert DocumentTitle und als Attribut value der Wert der Document Title verwendet werden.</p>
Device-ID	<p>Der Parameter DeviceID wird im Protokolleintrag nicht belegt.</p>

1209 [**<=**]

1210 **A_14814 - Komponente ePA-Dokumentenverwaltung – Schutz vor Manipulation**
 1211 **der Protokolldaten**

1212 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die § 291a-
 1213 Protokolldaten gegen Veränderung und unberechtigtes Löschen geschützt sind.**[<=]**

1214 **A_15184 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen**
 1215 **alter § 291a-Protokolldaten**

1216 Die Komponente ePA-Dokumentenverwaltung MUSS für jeden bekannten
 1217 RecordIdentifier Protokolleinträge des § 291a-Protokolls - außer den 50 jüngsten
 1218 Einträgen - am Ende des auf ihre Generierung folgenden Kalenderjahres löschen, sobald
 1219 die VAU erstmalig nach dem Stichtag aktiviert wird.**[<=]**

1220

1221

5 Funktionsmerkmale

1222 5.1 Dokumentenverwaltung

1223 In diesem Abschnitt wird die Außenschnittstelle der IHE ITI-basierten
 1224 Dokumentenverwaltung festgelegt. Einzelne Umsetzungsanforderungen suggerieren eine
 1225 vermischte Verarbeitung von Funktionalitäten, welche bei IHE ITI originär getrennt von
 1226 einer Document Registry und einem Document Repository (bzw. den Responding
 1227 Gateways) durchgeführt werden. Da die Außenschnittstelle der ePA-
 1228 Dokumentenverwaltung nicht zwischen Document Registry und Document Repository
 1229 unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit differenzierten Pfaden
 1230 siehe [gemSpec_Aktensystem#A_17969]), werden sonst bei IHE ITI explizite
 1231 Operationen zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne
 1232 Umsetzung angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-
 1233 Nachricht kann an IHE ITI-konforme Akteure ausgerichtet werden.

1234 5.1.1 Schnittstelle I_Document_Management

1235 A_14152 - Komponente ePA-Dokumentenverwaltung – Implementierung der 1236 Schnittstelle I_Document_Management

1237 Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle
 1238 definierte Web-Service-Schnittstelle implementieren.

1239 **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 	

1240 [\leq]

1241 **5.1.1.1 Operation**

1242 **I_Document_Management::CrossGatewayDocumentProvide**

1243 **A_14153 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-Gateway Document Provide**

1244 Die Komponente ePA-Dokumentenverwaltung MUSS

1245 die Operation `I_Document_Management::CrossGatewayDocumentProvide` gemäß der

1246 folgenden Signatur implementieren:

1248 **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 <code>I_Document_Management::putDocuments</code> 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_Ver#A_14109, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Cross-Gateway Document Provide Response Message	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	rs:RegistryResponse	n
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	
MaxDocSizeExceeded	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines der übermittelten Dokumente übersteigt 25 MByte.	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

1249 [\leq]

1250 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1251 Transaktionen "Cross-Gateway Document Provide" [ITI-80] und "Provide X-User
1252 Assertion" [ITI-40] sind [IHE-ITI-XCDR], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-
1253 TF2x] zu entnehmen.

1254 5.1.1.1.1 Umsetzung

1255 **A_15055 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung von**
1256 **gemischten Dokumentenpaketen mit Policy Documents**

1257 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1258 MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und
1259 mit einem XDSRepositoryMetadataError-Fehlercode quittieren, sofern in der
1260 Eingangsnachricht mehr als ein Dokument und Dokumenten-Metadaten gemäß der

1261 Anforderung [gemSpec_DM_ePA#A_14961] für Policy Documents (Advanced Patient
1262 Privacy Consents) enthalten sind.
1263 [`<=`]

1264 **A_14941 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung bei**
1265 **Angabe von Document Entry Relationships in Metadaten**

1266 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1267 MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und
1268 mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern die Metadaten die
1269 folgenden Association Types nach [IHE-ITI-TF3#4.2.2] enthalten:
1270

- 1271 • `urn:ihe:iti:2007:AssociationType:RPLC` (Replace)
- 1272 • `urn:ihe:iti:2007:AssociationType:XFRM` (Transform)
- 1273 • `urn:ihe:iti:2007:AssociationType:APND` (Addendum)
- 1274 • `urn:ihe:iti:2007:AssociationType:XFRM_RPLC` (Replace with Transformation)
- 1275 • `urn:ihe:iti:2007:AssociationType:signs` (Digital Signature)
- 1276 • `urn:ihe:iti:2010:AssociationType:IsSnapshotOf` (Snapshot of On-Demand
1277 document entry)

1278 [`<=`]

1279 **A_13838 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße**
1280 **prüfen**

1281 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1282 MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das SubmissionSet
1283 verarbeitet wird. Die Verarbeitung MUSS abgelehnt werden und mit einem mit
1284 einem `MaxDocSizeExceeded`-bzw. `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-
1285 TF3#4.2.4] quittieren, wenn die Gesamtgröße aller übermittelten Dokumente 250 MByte
1286 übersteigt oder die Größe mindestens eines einzelnen übermittelten Dokuments 25
1287 MByte übersteigt.
1288 [`<=`]

1289 Das bedeutet, dass Dokumente bis zu einer Größe von 25 MB = 25 * (1024)² Byte in
1290 die ePA hochgeladen werden. Grundlage für die Berechnung der Dokumentengröße ist
1291 das Dokument ohne Verschlüsselung durch den Dokumentenschlüssel und ohne
1292 Transportcodierung. Größere Dokumente können nicht hochgeladen werden.

1293 **A_13798 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung**
1294 **der Metadaten aus ITI Document Sharing-Profilen durch XCDR-Akteur**
1295 **"Responding Gateway"**

1296 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
1297 MUSS die SubmissionSet- sowie die DocumentEntry-Metadaten der eingehenden
1298 Nachricht vor einer Zugriffskontrolle gemäß der Konformität zu den Nutzungsvorgaben in
1299 [gemSpec_DM_ePA#A_14760] prüfen. Die Komponente ePA-Dokumentenverwaltung
1300 als XCDR-Akteur "Responding Gateway" MUSS das Registrieren und Speichern von
1301 Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`-
1302 Fehlercode quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben
1303 sind. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-
1304 Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben
1305 entspricht. [`<=`]

1306 **A_13715 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-Gateway Document Provide**

1307 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
 1308 MUSS die Umsetzung der
 1309 Operation `I_Document_Management::CrossGatewayDocumentProvide` bzw. die
 1310 Verarbeitung des übermittelten Submission Sets gemäß den definierten Ablauflogiken
 1311 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
 1312 3.80.4.2.3] implementieren.[<=]

1314 **A_13657 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Cross-Gateway Document Provide**

1315 Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway"
 1316 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
 1317 Policy Documents (Advanced Patient Privacy Consents) entsprechend der
 1318 Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt registriert und ein
 1319 Dokument gespeichert wird.[<=]

1321 **5.1.1.2 Operation I_Document_Management::CrossGatewayQuery**

1322 **A_14450 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-Gateway Query**

1323 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 1324 `I_Document_Management::CrossGatewayQuery` gemäß der folgenden Signatur
 1325 implementieren:

1327 **Tabelle 7: Tab_Dokv_16 - Operation Cross-Gateway Query**

Operation	<code>I_Document_Management::CrossGatewayQuery</code>		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management::find</code> 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	<code>query:AdhocQueryRequest</code>	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n

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

1328
1329

[<=]

1330 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1331 Transaktionen "Cross-Gateway Document Query" [ITI-38] und "Provide X-User Assertion"
1332 [ITI-40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1333 entnehmen.

1334 **5.1.1.2.1 Umsetzung**

1335 **A_14924 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe von**
1336 **Metadaten zu Policy Documents (Advanced Patient Privacy Consents)**

1337 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
1338 DARF Metadaten zu Policy Documents (Advanced Patient Privacy Consents) gemäß der
1339 Anforderung [gemSpec_DM_ePA#A_14961] NICHT zurückgeben bzw. MUSS diese aus
1340 der Antwortnachricht entfernen, falls diese den Anfragekriterien entsprechen.

1341 [<=]

1342 Die folgende XACML 2.0 Policy repräsentiert die o.g. Anforderung technisch:

```

1343 <?xml version="1.0" encoding="UTF-8"?>
1344 <Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
1345   PolicyId="urn:uuid:6e84f679-5f36-4861-bfb5-607aef021fff"
1346   RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
1347 algorithm:deny-overrides">
1348   <Target>
1349     <Resources>
1350       <Resource>
1351         <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
1352           <AttributeValue DataType="urn:hl7-org:v3#CV">
1353             <CodedValue xmlns="urn:hl7-org:v3" code="57016-8"
1354               codeSystem="1.2.276.0.76.11.32"/>
1355           </AttributeValue>
1356           <ResourceAttributeDesignator
1357             AttributeId="urn:ihe:iti:appc:2016:document-entry:class-code"
1358             DataType="urn:hl7-org:v3#CV" MustBePresent="true"/>
1359         </ResourceMatch>
1360       </Resource>

```

```

1361     </Resources>
1362     </Target>
1363     <Rule RuleId="urn:uuid:bb42d632-c70c-447d-94aa-011f2c9561f4"
1364     Effect="Deny"/>
1365 </Policy>
1366

```

1367 **A_14939 - Komponente ePA-Dokumentenverwaltung – Keine Anfragen auf**

1368 **Ordern**

1369 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
 1370 DARF die folgenden Anfragetypen aufgrund des in ePA-Fachanwendung nicht
 1371 verwendeten IHE ITI-Ordnerkonzepts NICHT unterstützen und MUSS die Anfrage mit
 1372 einem XDSUnknownStoredQuery-Fehlercode quittieren:

- 1373 • FindFolders (Query ID: urn:uuid:958f3006-baad-4929-a4de-ff1114824431)
- 1374 • GetFolders (Query ID:urn:uuid:5737b14c-8a1a-4539-b659-e03a34a5e1e4)
- 1375 • GetFolderAndContents (Query ID:urn:uuid:b909a503-523d-4517-8acf-
- 1376 8e5834dfc4c7)
- 1377 • GetFoldersForDocument (Query ID:urn:uuid:10cae35a-c7f9-4cf5-b61e-
- 1378 fc3278ffb578)

1379 [**<=**]

1380 **A_14910 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-**

1381 **Gateway Query**

1382 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
 1383 MUSS die Umsetzung der Operation `I_Document_Management::CrossGatewayQuery`
 1384 gemäß der definierten Ablauflogik in [IHE-ITI-TF2b#3.38.4.1.2 und 3.38.4.1.3]
 1385 implementieren. [**<=**]

1386 **A_17184 - Komponente ePA-Dokumentenverwaltung – Suchanfragen über das**

1387 **Metadatenattribut DocumentEntry.title**

1388 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
 1389 MUSS einen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID
 1390 "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben
 1391 Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-
 1392 ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter
 1393 `$XDSDocumentEntryTitle` unterstützen, sodass eine Suchergebnismenge über das
 1394 Attribut `XDSDocumentEntry.title` eingeschränkt werden kann. Weiterhin MUSS dieselbe
 1395 Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den
 1396 Parameter `$XDSDocumentEntryAuthorPerson`. Das `wsa:Action`-Element MUSS den Wert
 1397 "urn:ihe:iti:2007:CrossGatewayQuery" besitzen. [**<=**]

1398 **A_13585 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**

1399 **Cross-Gateway Query**

1400 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
 1401 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
 1402 Policy Documents (Advanced Patient Privacy Consents) entsprechend der
 1403 Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt zum Fachmodul ePA
 1404 als XCA-Akteur "Initiating Gateway" zurückgegeben wird. Widerspricht die
 1405 Suchergebnismenge ganz oder teilweise einer anwendbaren Zugriffsrichtlinie aus zur
 1406 Verfügung stehenden Policy Documents, so MUSS die Suchergebnismenge dahingehend
 1407 gefiltert werden, dass nur berechtigte Metadaten (d.h. Document Entries sowie
 1408 Submission Sets) an den Document Consumer zurückgegeben werden. [**<=**]

1409 **A_18069 - Komponente ePA-Dokumentenverwaltung – Suche über Author**
 1410 **Institution bei Cross-Gateway Query**
 1411 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
 1412 MUSS für den Anfragetyp "FindDocumentsByTitle" den weiteren optionalen Parameter
 1413 \$XDSDocumentEntryAuthorInstitution verarbeiten können, sodass eine
 1414 Suchergebnismenge über den authorInstitution-Slot der XDSDocumentEntry.author-
 1415 Classification (Wertemenge des authorInstitution-Sub-Attributs) eingeschränkt werden
 1416 kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein,
 1417 wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson.[<=]

1418 **5.1.1.3 Operation I_Document_Management::RemoveDocuments**
 1419 **A_14489 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove**
 1420 **Documents**

1421 Die Komponente ePA-Dokumentenverwaltung MUSS
 1422 die Operation `I_Document_Management::RemoveDocuments` gemäß der folgenden
 1423 Signatur implementieren:

1424 **Tabelle 8: Tab_Dokv_17 - Operation Remove Documents**

Operation		I_Document_Management::RemoveDocuments	
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management::deleteDocuments</code> technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove Documents" [ITI-86] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente eines Aktenkontos im ePA-Aktensystem zu löschen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2017:RemoveDocuments		
Eingangsparameter			
Name	Beschreibung	Typ	opt
Remove Documents Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	<code>rmd:RemoveDocuments_Message</code>	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringereinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt

Remove Documents Response Message	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocumentsResponse_Message	n
<p>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></p>			
Name	Fehlertext	Details	

1425 [**<=**]

1426 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
 1427 Transaktionen "RemoveDocuments" [ITI-86] und "Provide X-User Assertion" [ITI-
 1428 40] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

1429 *5.1.1.3.1 Umsetzung*

1430 **A_14908 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove**
 1431 **Documents**

1432 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
 1433 MUSS die Umsetzung der Operation `I_Document_Management::RemoveDocuments` gemäß
 1434 der definierten Ablauflogik in [IHE-ITI-RMD#3.86.4.1.2 und 3.86.4.1.3]
 1435 implementieren. [**<=**]

1436 **5.1.1.4 Operation I_Document_Management::CrossGatewayRetrieve**

1437 **A_14464 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-**
 1438 **Gateway Retrieve**

1439 Die Komponente ePA-Dokumentenverwaltung MUSS
 1440 die Operation `I_Document_Management::CrossGatewayRetrieve` gemäß der folgenden
 1441 Signatur implementieren:

1442 **Tabelle 9: Tab_Dokv_18 - Operation Cross-Gateway Retrieve**

Operation	I_Document_Management::CrossGatewayRetrieve
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	opt
Cross-Gateway Retrieve Message	Eingangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetRequest	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 Retrieve 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.	

1443 [\leq]

1444 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1445 Transaktionen "Cross-Gateway Document Retrieve" [ITI-39] und "Provide X-User
1446 Assertion" [ITI-40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-
1447 TF2x] zu entnehmen.

1448 *5.1.1.4.1 Umsetzung*

1449 **A_14911 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-
1450 Gateway Retrieve**

1451 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
1452 MUSS die Umsetzung der Operation `I_Document_Management::CrossGatewayRetrieve`
1453 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.39.4.1.2 und 3.39.4.1.3] und
1454 [IHE-ITI-TF2b#3.39.4.2.2 und 3.39.4.2.3] implementieren. [\leq]

1455 **A_16201 - Komponente ePA-Dokumentenverwaltung – Prüfung der
1456 zurückgegebenen Paketgröße**

1457 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
1458 MUSS anhand der übergebenen DocumentUniqueIDs die Gesamtgröße ermitteln und bei
1459 Überschreitung von 250 MByte die Verarbeitung ablehnen und die Nachricht mit

1460 einem `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.
 1461 [`<=`]

1462 **A_14548-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement**
 1463 **für Cross-Gateway Retrieve**

1464 Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway"
 1465 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
 1466 Policy Documents (Advanced Patient Privacy Consents) entsprechend der
 1467 Anforderung A_14822 durchsetzen, bevor ein Repository-Datenobjekt zum Fachmodul
 1468 ePA als XCA-Akteur "Initiating Gateway" zurückgegeben wird. Bei einem Abruf von
 1469 mehreren Dokumenten können einzelne Dokumente durch den zwischenzeitlichen Entzug
 1470 einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für den Abruf
 1471 berechtigt sein. Widerspricht ein abzurufendes Dokument einer anwendbaren
 1472 Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die
 1473 Antwortnachricht zum betreffenden Dokument einen `XSDDocumentUniqueIdError`-
 1474 Fehlercode enthalten (das Dokument wird nicht herausgegeben) und der Wert 4 des
 1475 `EventOutcomeIndicators` im Protokollierungseintrag des § 291a-Protokolls gesetzt
 1476 werden. Ist ein angefordertes Dokument nicht mehr verfügbar (d.h. es wurde gelöscht),
 1477 MUSS gemäß IHE ITI der Fehlercode `XSDDocumentUniqueIdError` zurückgegeben
 1478 werden.[`<=`]

1479 **5.1.1.5 Operation**

1480 **I_Document_Management::RestrictedUpdateDocumentSet**

1481 **A_15057 - Komponente ePA-Dokumentenverwaltung – Signatur für Restricted**
 1482 **Update Document Set**

1483 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 1484 `I_Document_Management::RestrictedUpdateDocument Set` gemäß der folgenden
 1485 Signatur implementieren:

1486 **Tabelle 10: Tab_Dokv_19 - Operation Restricted Update Document Set**

Operation	I_Document_Management::RestrictedUpdateDocumentSet
-----------	--

<p>Beschreibung</p>	<p>Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_PHR_Management::updateMetadata</code> technisch um. Sie basiert auf den IHE ITI-Transaktionen "Restricted Update Document Set" [ITI-92] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, Metadaten zu Dokumenten zu ändern.</p> <p>Für die Kenntlichmachung von Dokumenten eines Versicherten oder eines Kostenträgers mit leistungserbringeräquivalenter Relevanz ermöglicht die ePA-Fachanwendung Mitarbeitern einer Leistungserbringerinstitution, Dokumente, die durch einen Versicherten (oder dessen Vertreter) bereitgestellt wurden, anderen berechtigten Leistungserbringerinstitutionen zur Verfügung zu stellen. Dies setzt voraus, dass die entsprechende Leistungserbringerinstitution Zugriff auf die Dokumente eines Versicherten oder die des Kostenträgers hat, um die Sensibilität ändern zu können.</p> <p>Im Detail werden durch einen Versicherten eingestellte Dokumente mit dem Metadatenattribut <code>documentEntry.confidentialityCode</code> "PAT" (Dokument eines Versicherten) gekennzeichnet. Dokumente, welche ein Kostenträger eingestellt hat, werden ferner mit dem Metadatenattribut <code>documentEntry.confidentialityCode</code> "KTR" (Dokument eines Kostenträgers) gekennzeichnet. Durch eine Leistungserbringerinstitution eingestellte Dokumente werden mit dem Metadatenattribut <code>documentEntry.confidentialityCode</code> "LEI" (Dokument einer Leistungserbringerinstitution) gekennzeichnet.</p> <p>Um ein Dokument als leistungserbringeräquivalent zu kennzeichnen, muss der Mitarbeiter einer Leistungserbringerinstitution auch Zugriff auf Dokumente mit dem Metadatenattribut <code>documentEntry.confidentialityCode</code> "PAT" (Dokument eines Versicherten) oder "KTR" (Dokument eines Kostenträgers) haben (vgl. <code>RegistryStoredQuery</code>). Die besagte Kennzeichnung erfolgt durch das Hinzufügen eines weiteren Confidentiality Codes "LEÄ" (Leistungserbringeräquivalentes Dokument eines Versicherten oder Kostenträgers). Dieses Kennzeichen kann nach demselben Mechanismus wieder entfernt werden.</p>		
<p>Formatvorgabe n</p>	<p>SOAP Action: urn:ihe:iti:2018:RestrictedUpdateDocumentSet</p>		
<p>Eingangsparameter</p>			
<p>Name</p>	<p>Beschreibung</p>	<p>Typ</p>	<p>opt</p>

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_14927, 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			
<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	

1487
1488

[<=]

1489 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1490 Transaktionen "RestrictedUpdateDocumentSet" [ITI-92] und "Provide X-User Assertion"
1491 [ITI-40] sind [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1492 entnehmen.

1493 *5.1.1.5.1 Umsetzung*

1494 **A_15082 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung**
1495 **der Metadaten aus ITI Document Sharing-Profilen durch RMU-Akteur "Update**
1496 **Responder"**

1497 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
1498 die übermittelten DocumentEntry-Metadaten der eingehenden Nachricht dahingehend
1499 prüfen, dass gegenüber den Bestandsdaten das
1500 Metadatenattribut `documentEntry.confidentialityCode` konform zu den
1501 Nutzungsvorgaben in [gemSpec_DM_ePA#A_14760] geändert ist. Die Komponente ePA-

1502 Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS das Aktualisieren
1503 dieses Metadatenattributs ablehnen und mit einem `XDSRepositoryMetadataError`
1504 quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind.[<=]

1505 **A_15083 - Komponente ePA-Dokumentenverwaltung – Prüfung auf**
1506 **ausschließliche Aktualisierung des Metadatenattributs**
1507 **`documentEntry.confidentialityCode`**

1508 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
1509 die übermittelten `DocumentEntry`-Metadaten der eingehenden Nachricht dahingehend
1510 prüfen, dass gegenüber den Bestandsdaten ausschließlich das
1511 Metadatenattribut `documentEntry.confidentialityCode` geändert werden soll . Es ist
1512 nur das Hinzufügen oder Entfernen des Confidentiality Codes "LEÄ"
1513 (Leistungserbringeräquivalentes Dokument eines Versicherten oder
1514 Kostenträgers) erlaubt. Wenn andere Aktualisierungen für die übermittelten
1515 Metadatenattribute in der Eingangsnachricht enthalten sind, MUSS die Komponente ePA-
1516 Dokumentenverwaltung als RMU-Akteur "Update Responder" die Weiterverarbeitung
1517 abbrechen und die Nachricht mit einem `LocalPolicyRestrictionError`-Fehlercode
1518 quittieren.

1519
1520 [<=]

1521 **A_15061 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für**
1522 **`Restricted Update Document Set`**

1523 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
1524 die Umsetzung der Operation `I_Document_Management::RestrictedUpdateDocumentSet`
1525 gemäß der definierten Ablauflogik in [IHE-ITI-RMU#3.92.4.1.2 und 3.92.4.1.3]
1526 implementieren.[<=]

1527 **A_15080-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement**
1528 **für `Restricted Update Document Set`**

1529 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS
1530 die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy
1531 Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822
1532 durchsetzen, bevor Metadaten einer oder mehrerer Dokumente aktualisiert werden. Beim
1533 Aktualisieren der Metadaten durch das ePA-Fachmodul können einzelne Dokumente bzw.
1534 Metadaten durch den zwischenzeitlichen Entzug einer Berechtigung durch den
1535 Versicherten oder Ablauf nicht mehr für die Aktualisierung berechtigt sein. Widerspricht
1536 ein Dokument bzw. die damit assoziierten Metadaten einer anwendbaren Zugriffsrichtlinie
1537 aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum
1538 betreffenden Dokument einen `XSDSDocumentUniqueIdError`-Fehlercode enthalten und der
1539 Wert 4 des `EventOutcomeIndicators` im Protokollierungseintrag des § 291a-Protokolls
1540 gesetzt werden. Ist ein zu aktualisierendes Dokument bzw. Metadaten nicht mehr
1541 verfügbar, MUSS gemäß IHE TF ITI der Fehlercode `XSDSDocumentUniqueIdError`
1542 zurückgegeben werden.

1543 [<=]

1544 **5.1.2 Schnittstelle `I_Document_Management_Insurant`**

1545 **A_14478 - Komponente ePA-Dokumentenverwaltung – Implementierung der**
1546 **Schnittstelle `I_Document_Management_Insurant`**

1547 Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle
1548 definierte Web-Service-Schnittstelle implementieren.

1549 **Tabelle 11: 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 	

1550
1551 [**<=**]

1552 **5.1.2.1 Operation**
 1553 **I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b**
 1554 **A_14479 - Komponente ePA-Dokumentenverwaltung – Signatur für Provide And**
 1555 **Register Document Set-b**
 1556 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 1557 I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b gemäß der
 1558 folgenden Signatur implementieren:

1559 **Tabelle 12: 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.

1560
1561
1562

[<=]

1563 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1564 Transaktionen "Provide And Register Document Set-b" [ITI-41] und "Provide X-User
1565 Assertion" [ITI-40] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1566 entnehmen.

1567 *5.1.2.1.1 Umsetzung*

1568 **A_15056 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung von**
1569 **gemischten Dokumentenpaketen mit Policy Documents**

1570 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1571 MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und
1572 mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern in der
1573 Eingangsnachricht mehr als ein Dokument und Dokumenten-Metadaten gemäß der
1574 Anforderung [gemSpec_DM_ePA#A_14961] für Policy Documents (Advanced Patient
1575 Privacy Consents) enthalten sind. [<=]

1576 **A_14912 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide**
1577 **And Register Document Set-b**

1578 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1579 MUSS die Umsetzung der
1580 Operation `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b`
1581 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3] und
1582 [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3] implementieren. [<=]

1583 **A_16442 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender**
1584 **X-User Assertion**

1585 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1586 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12]
1587 quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
1588 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
1589 [<=]

- 1590 **5.1.2.2 Operation**
- 1591 **I_Document_Management_Insurant::RegistryStoredQuery**
- 1592 **A_14480 - Komponente ePA-Dokumentenverwaltung – Signatur für Registry**
- 1593 **Stored Query**
- 1594 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
- 1595 I_Document_Management_Insurant::RegistryStoredQuery gemäß der folgenden
- 1596 Signatur implementieren:
- 1597 **Tabelle 13: Tab_Dokv_22 - Operation Registry Stored Query**

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

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

1598
1599

[<=]

1600 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1601 Transaktionen "Registry Stored Query" [ITI-18] und "Provide X-User Assertion" [ITI-
1602 40] sind [IHE-ITI-TF2a], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1603 entnehmen.

1604 *5.1.2.2.1 Umsetzung*

1605 **A_14835 - Komponente ePA-Dokumentenverwaltung – Keine Anfragen auf**
1606 **Ordern**

1607 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF
1608 die folgenden Anfragetypen aufgrund des in ePA nicht verwendeten IHE ITI-
1609 Ordnerkonzepts NICHT unterstützen und MUSS die Anfrage mit
1610 einem XDSUnknownStoredQuery-Fehlercode quittieren:

- 1611 • FindFolders (Query ID: urn:uuid:958f3006-baad-4929-a4de-ff1114824431)
- 1612 • GetFolders (Query ID:urn:uuid:5737b14c-8a1a-4539-b659-e03a34a5e1e4)
- 1613 • GetFolderAndContents (Query ID:urn:uuid:b909a503-523d-4517-8acf-
1614 8e5834dfc4c7)
- 1615 • GetFoldersForDocument (Query ID:urn:uuid:10cae35a-c7f9-4cf5-b61e-
1616 fc3278ffb578)

1617 [<=]

1618 **A_14913 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Registry**
1619 **Stored Query**

1620 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1621 die Umsetzung der
1622 Operation `I_Document_Management_Insurant::RegistryStoredQuery` gemäß der
1623 definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3]
1624 implementieren.[<=]

1625 **A_16436 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender**
1626 **X-User Assertion**

1627 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1628 die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren, falls
1629 die X-User Assertion nicht dem SAML 2.0 Assertion Profil
1630 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.

1631 [<=]

1632 **A_17185 - Komponente ePA-Dokumentenverwaltung – Suchanfragen über das**
1633 **Metadatenattribut DocumentEntry.title**

1634 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
1635 einen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID
1636 "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben

1637 Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-
 1638 ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter
 1639 \$XDSDocumentEntryTitle unterstützen, sodass eine Suchergebnismenge über das
 1640 Attribut XDSDocumentEntry.title eingeschränkt werden kann. Weiterhin MUSS dieselbe
 1641 Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den
 1642 Parameter \$XDSDocumentEntryAuthorPerson. Daswsa:Action-Element MUSS den Wert
 1643 "urn:ihe:iti:2007:RegistryStoredQuery" besitzen.
 1644 [`<=`]

1645 **A_14588 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
 1646 **Registry Stored Query**

1647 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
 1648 die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy
 1649 Documents (Advanced Patient Privacy Consents) entsprechend der
 1650 Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt zum ePA-Frontend
 1651 des Versicherten (XDS-Akteur "Document Consumer") zurückgegeben wird.
 1652

1653 [`<=`]

1654 **A_18070 - Komponente ePA-Dokumentenverwaltung – Suche über Author**
 1655 **Institution bei Registry Stored Query**

1656 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS
 1657 für den Anfragetyp "FindDocumentsByTitle" den weiteren optionalen Parameter
 1658 \$XDSDocumentEntryAuthorInstitution verarbeiten können, sodass eine
 1659 Suchergebnismenge über den authorInstitution-Slot der XDSDocumentEntry.author-
 1660 Classification (Wertemenge des authorInstitution-Sub-Attributs) eingeschränkt werden
 1661 kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein,
 1662 wie für Suchanfragen über den Parameter \$XDSDocumentEntryAuthorPerson.[`<=`]

1663 **5.1.2.3 Operation**

1664 **I_Document_Management_Insurant::RemoveDocuments**

1665 **A_14488 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove**
 1666 **Documents**

1667 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 1668 I_Document_Management_Insurant::RemoveDocuments gemäß der folgenden Signatur
 1669 implementieren:

1670 **Tabelle 14: Tab_Dokv_23 - Operation RemoveDocuments**

Operation	I_Document_Management_Insurant::RemoveDocuments
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 Documents" [ITI-86] 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:RemoveDocuments
Eingangsparameter	

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

1671
1672

[<=]

1673 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1674 Transaktionen "RemoveDocuments" [ITI-86] und Provide X-User Assertion [ITI-
1675 40] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

1676 *5.1.2.3.1 Umsetzung*

1677 **A_14909 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove**
1678 **Documents**

1679 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1680 MUSS die Umsetzung der
1681 Operation `I_Document_Management_Insurant::RemoveDocuments` gemäß der definierten
1682 Ablauflogik in [IHE-ITI-RMD#3.86.4.1.2 und 3.86.4.1.3] implementieren.[<=]

1683 **A_16437 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender**
 1684 **X-User Assertion**
 1685 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
 1686 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren,
 1687 falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
 1688 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
 1689 [\leq]

1690 **5.1.2.4 Operation**

1691 **I_Document_Management_Insurant::RetrieveDocumentSet**

1692 **A_14481 - Komponente ePA-Dokumentenverwaltung – Signatur für Retrieve**
 1693 **Document Set**

1694 Die Komponente ePA-Dokumentenverwaltung MUSS
 1695 die Operation I_Document_Management_Insurant::RetrieveDocumentSet gemäß der
 1696 folgenden Signatur implementieren:

1697 **Tabelle 15: 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 authentifizierte n 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.	

1698
1699

[<=]

1700 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1701 Transaktionen "RetrieveDocumentSet" [ITI-43] und "Provide X-User Assertion" [ITI-
1702 40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1703 entnehmen.

1704 *5.1.2.4.1 Umsetzung*

1705 **A_14914 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Retrieve**
1706 **Document Set**

1707 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1708 MUSS die Umsetzung der
1709 Operation `I_Document_Management_Insurant::RetrieveDocumentSet` gemäß den
1710 definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3] und [IHE-ITI-
1711 TF2b#3.43.4.2.2 und 3.43.4.2.3] implementieren.[<=]

1712 **A_16443 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender**
1713 **X-User Assertion**

1714 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1715 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren,
1716 falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
1717 gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
1718 [<=]

1719 **A_16200 - Komponente ePA-Dokumentenverwaltung – Prüfung der**
1720 **zurückgegebenen Paketgröße**

1721 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1722 MUSS anhand der übergebenen DocumentUniqueIDs die Gesamtgröße ermitteln und bei
1723 Überschreitung von 250 MByte die Verarbeitung ablehnen und die Nachricht mit
1724 einem `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.
1725 [<=]

1726 **A_14589 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
 1727 **Retrieve Document Set**
 1728 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
 1729 MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden
 1730 Policy Documents (Advanced Patient Privacy Consents) entsprechend der
 1731 Anforderung A_14822 durchsetzen, bevor ein Repository-Datenobjekt zum ePA-Frontend
 1732 des Versicherten als XDS-Akteur "Document Consumer" zurückgegeben wird. Ist ein
 1733 abzurufendes Dokument nicht mehr verfügbar, MUSS gemäß IHE TF ITI der
 1734 Fehlercode `XDSDocumentUniqueIdError` zurückgegeben werden.
 1735
 1736 [**<=**]

1737 **5.1.3 Schnittstelle I_Document_Management_Insurance**

1738 **A_17438 - Komponente ePA-Dokumentenverwaltung – Implementierung der**
 1739 **Schnittstelle I_Document_Management_Insurance**
 1740 Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle
 1741 definierte Web-Service-Schnittstelle implementieren.

1742 **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 	

1743
 1744 [**<=**]

1745 **5.1.3.1 Operation**
 1746 **I_Document_Management_Insurance::ProvideAndRegisterDocumentSet**
 1747 **-b**

1748 **A_17439 - Komponente ePA-Dokumentenverwaltung – Signatur für Provide And**
 1749 **Register Document Set-b**

1750 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

1751 I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b gemäß der
 1752 folgenden Signatur implementieren:

1753 **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 <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. Dokumentgröße 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.	

1754
1755

[<=]

1756 Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-
1757 Transaktionen "Provide And Register Document Set-b" [ITI-41] und "Provide X-User
1758 Assertion" [ITI-40] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu
1759 entnehmen.

1760 *5.1.3.1.1 Umsetzung*

1761 **A_17443 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide**
1762 **And Register Document Set-b**

1763 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1764 MUSS die Umsetzung der
1765 Operation `I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b`
1766 gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3] und
1767 [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3] implementieren.

1768 [<=]

1769 **A_17444 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender**
1770 **X-User Assertion**

1771 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository"
1772 MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren,
1773 falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil
1774 gemäß [gemSpec_FM_ePA_KTR_Consumer#A_17253, A_17254] entspricht. [<=]

1775 **5.2 Aktenkontoverwaltung**

1776 **5.2.1 Schnittstelle I_Account_Management_Insurant**

1777 Diese Schnittstelle setzt einen Teil der in [gemSysL_ePA] definierten Schnittstelle
 1778 I_Account_Management_Insurant technisch um. Die Operationen der Schnittstelle
 1779 werden vom Verarbeitungskontext über den sicheren Kanal zum ePA-Modul Frontend des
 1780 Versicherten bereitgestellt.

1781 **A_14804 - Komponente ePA-Dokumentenverwaltung – Implementierung der**
 1782 **Schnittstelle I_Account_Management_Insurant**

1783 Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle
 1784 definierte Web-Service-Schnittstelle implementieren.

1785 **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	

1786 [**<=**]

1787 **5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount**

1788 **A_14805 - Komponente ePA-Dokumentenverwaltung – Signatur für**
 1789 **I_Account_Management_Insurant::SuspendAccount**

1790 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 1791 I_Account_Management_Insurant::SuspendAccount gemäß der folgenden Signatur
 1792 implementieren:

1793 **Tabelle 19: Tab_Dokv_26 - Operation Suspend Account**

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

1794 [`<=`]

1795 *5.2.1.1.1 Umsetzung*

1796 **A_15530 - Komponente ePA-Dokumentenverwaltung –**
 1797 **I_Account_Management_Insurant über sicheren Kanal**

1798 Die Komponente ePA-Dokumentenverwaltung MUSS die von ihr angebotenen
 1799 Operationen der Schnittstelle `I_Account_Management_Insurant` ausschließlich über den
 1800 sicheren Kanal zum ePA-Modul Frontend des Versicherten verfügbar machen. [`<=`]

1801 Die folgende Anforderung bewirkt, dass nur der Versicherte als Inhaber einer Akte im
 1802 Zustand "DISMISSED" die
 1803 Operation `I_Account_Management_Insurant::SuspendAccount` ausführen kann.

1804 **A_15062 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
 1805 **Suspend Account**

1806 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
 1807 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
 1808 Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor die
 1809 Operation `I_Account_Management_Insurant::SuspendAccount` ausgeführt wird. Bei
 1810 einer negativen Autorisierungsentscheidung MUSS die Nachricht mit dem
 1811 `ACCESS_DENIED`-Fehlercode quittiert werden. [`<=`]

1812 **A_14885 - Komponente ePA-Dokumentenverwaltung – Exportpaket des**
 1813 **Aktenkontos erstellen**

1814 Die Komponente ePA-Dokumentenverwaltung MUSS bei der Ausführung der Operation
 1815 `I_Account_Management_Insurant::SuspendAccount` für das Aktenkonto

- 1816 • sämtliche Dokumente einschließlich Policy Documents (Advanced Patient Privacy
- 1817 Consents) des XCDR Responding Gateway bzw. XDS Document Repository,
- 1818 • sämtliche Metadaten der XCA Responding Gateway bzw. XDS Document Registry,
- 1819 • sämtliche § 291a-Protokolldaten,

1820 gemäß den strukturellen Vorgaben in [IHE-ITI-TF2b] zur Transaktion *IHE ITI Cross-*
 1821 *Enterprise Document Media Interchange (XDM) - Distribute Document Set on Media [ITI-*
 1822 *32]*, in eine ZIP-Datei exportieren.

1823 Die Komponente ePA-Dokumentenverwaltung MUSS dabei abweichend von den Vorgaben
 1824 aus [ITI-32],
 1825

- 1826 • die ZIP-Datei außerhalb des Verarbeitungskontextes persistieren,

1827 • die ZIP-Datei im Zuge des Exports mit dem `ContextKey` gemäß
1828 `[gemSpec_Krypt#GS-A_5016]` verschlüsseln, so dass sichergestellt ist, dass nur
1829 entsprechend verschlüsselte Daten außerhalb des Verarbeitungskontextes
1830 auftreten können sowie

1831 • die ZIP-Datei zum Abruf für berechtigte andere Anbieter ePA-Aktensystem
1832 verfügbar machen.

1833 Der Verarbeitungskontext MUSS solange geöffnet bleiben, bis die ZIP-Datei erstellt
1834 worden ist. [`<=`]

1835 **A_15012 - Komponente ePA-Dokumentenverwaltung – Korrektheit des** 1836 **Exportpakets sicherstellen**

1837 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS mit
1838 technischen Mitteln die Integrität der Daten und Datenstrukturen des Exportpakets
1839 während der Erstellung, Bereitstellung und Übermittlung an einen neuen Anbieter ePA-
1840 Aktensystem schützen, um damit ein Scheitern des Imports bei einem neuen Anbieter
1841 ePA-Aktensystem aufgrund eines fehlerhaften oder beschädigten
1842 Exportpakets auszuschließen. [`<=`]

1843 Die Herausgabe des Exportpakets an den neuen Anbieter des Versicherten ist über
1844 Anforderungen in `[gemSpec_Aktensystem#6.1.4]` geregelt.

1845 **A_15005 - Komponente ePA-Dokumentenverwaltung – Kein Aktenzugriff** 1846 **während des Exports der Daten**

1847 Die Komponente ePA-Dokumentenverwaltung MUSS während der Ausführung der
1848 Operation `I_Account_Management_Insurant::SuspendAccount` für ein Aktenkonto alle
1849 Operationen mit der Fehlermeldung "Aktenkonto vorübergehend nicht erreichbar"
1850 ablehnen. [`<=`]

1851 Für das ePA-Modul Frontend des Versicherten endet die Operation
1852 `I_Account_Management_Insurant::SuspendAccount` mit dem Erhalt der Download-URL
1853 für das Exportpaket. Bis zur vollständigen Übertragung des Exportpakets an den neuen
1854 Anbieter bleibt der vorherige Anbieter jedoch für die Daten des Versicherten
1855 verantwortlich.

1856 Da der Anbieterwechsel als ein zusammenhängender Vorgang aus Sicht des ePA-Moduls
1857 Frontend des Versicherten ablaufen soll, der Export und anschließende Import je nach
1858 Größe des Exportpakets jedoch einige Zeit in Anspruch nehmen können, soll der Vorgang
1859 im Backend asynchron ablaufen können. Die folgende Anforderung regelt dies für den
1860 Export. Die Anforderung `A_15623` im nächsten Abschnitt regelt die asynchrone
1861 Verarbeitung des Imports.

1862 **A_15622 - Komponente ePA-Dokumentenverwaltung – Asynchroner Export**

1863 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die URL
1864 des Exportpakets bestimmen und unmittelbar danach die Antwort auf den Aufruf der
1865 Operation `I_Account_Management_Insurant::SuspendAccount` an den Client
1866 zurückgeben, unabhängig davon, wie lange die Erstellung und Bereitstellung des
1867 Exportpakets dauert. [`<=`]

1868 **A_16076 - Komponente ePA-Dokumentenverwaltung – Frist für Bereitstellung** 1869 **des Exportpakets**

1870 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS das
1871 Exportpaket innerhalb von drei Werktagen für den Download durch den neuen Anbieter
1872 bereitstellen. [`<=`]

1873 **5.2.1.2 Operation I_Account_Management_Insurant::ResumeAccount**

1874 **A_14807 - Komponente ePA-Dokumentenverwaltung – Signatur für**

1875 **I_Account_Management_Insurant::ResumeAccount**

1876 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

1877 I_Account_Management_Insurant::ResumeAccount gemäß der folgenden Signatur

1878 implementieren:

1879 **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.	

1880 [**<=**]

1881 *5.2.1.2.1 Umsetzung*

1882 Die Ausführung der Operation `I_Account_Management_Insurant::ResumeAccount` setzt
 1883 voraus, dass der Versicherte mittels seines ePA-Moduls Frontend des Versicherten einen
 1884 sicheren Kanal zum Verarbeitungskontext aufgebaut hat und diesen mittels der Operation
 1885 `I_Document_Management_Connect::OpenContext` kryptographisch aktiviert hat. Darüber
 1886 hinaus muss die Operation `I_Account_Management_Insurant::ResumeAccount`
 1887 aufgerufen werden, bevor weitere Operationen am Verarbeitungskontext ausgeführt
 1888 werden können. Sie muss mit Fehler terminieren, wenn sie für ein Aktenkonto bereits
 1889 vorher erfolgreich ausgeführt wurde.

1890 **A_15526 - Komponente ePA-Dokumentenverwaltung – Voraussetzungen für die**
 1891 **Ausführung von Resume Account**

1892 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Operation
 1893 `I_Account_Management_Insurant::ResumeAccount` nur ausgeführt wird, wenn der
 1894 Verarbeitungskontext eines für einen Anbieterwechsel mit Übernahme der Akten Daten
 1895 registriertes Aktenkonto erstmalig durch den Versicherten geöffnet wurde. [**<=**]

1896 **A_15568 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für**
 1897 **Resume Account**

1898 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
 1899 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
 1900 Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor die
 1901 Operation `I_Account_Management_Insurant::ResumeAccount` ausgeführt wird. Bei einer
 1902 negativen Autorisierungsentscheidung MUSS die Nachricht mit dem `ACCESS_DENIED-`
 1903 Fehlercode quittiert werden. [**<=**]

1904 **A_15013 - ePA-Aktensystem – Download des Exportpakets**

1905 Das ePA-Aktensystem MUSS nach Eingang des Requests
 1906 `I_Account_Management_Insurant::ResumeAccount` das mittels des Aufrufparameters
 1907 `PackageURL` referenzierte Exportpaket beim vorhergehenden Anbieter ePA-Aktensystem
 1908 des Versicherten abrufen und für den Import durch den Verarbeitungskontext der ePA-
 1909 Dokumentenverwaltung verfügbar machen. [**<=**]

1910 **A_14905 - Komponente ePA-Dokumentenverwaltung – Import des Exportpakets**
 1911 **des vorhergehenden Aktenkontos**

1912 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS das vom
 1913 vorhergehenden Anbieter ePA-Aktensystem des Versicherten bezogene Exportpaket, vom
 1914 vorhergehenden Anbieter herunterladen sobald es dort verfügbar ist und in das neue
 1915 Aktenkonto importieren und dazu:

- 1916 • das Exportpaket mittels des `ContextKey` entschlüsseln und
- 1917 • die Struktur des Exportpakets auf Übereinstimmung mit den Festlegungen aus
- 1918 Anforderung A_14885 prüfen.

1919 [**<=**]

- 1920 **A_15596 - Komponente ePA-Dokumentenverwaltung – Ersetzen der Home**
1921 **Community ID**
1922 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS beim
1923 Import eines Exportpakets in sämtlichen Metadatensätzen den anbieterspezifischen Wert
1924 in den Feldern DocumentEntry.homeCommunityId und SubmissionSet.homeCommunityId
1925 sowie DocumentEntry.repositoryUniqueId mit der neuen Home Community ID
1926 aktualisieren.[<=]
- 1927 **A_15623 - Komponente ePA-Dokumentenverwaltung – Asynchroner Import**
1928 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die
1929 Antwort auf den Aufruf der Operation
1930 I_Account_Management_Insurant::ResumeAccount unmittelbar nach dem Aufruf an den
1931 Client zurückgeben, unabhängig davon, wie lange der Erhalt und Import des
1932 Exportpakets dauert.[<=]
- 1933 Die folgende Anforderung stellt sicher, dass der neue Anbieter des Aktenkontos
1934 ausreichend lange auf die Bereitstellung des Exportpakets durch den alten Anbieter
1935 wartet, da die Bereitstellung je nach Größe des Exportpakets eine gewisse Zeit in
1936 Anspruch nehmen kann. Der Versicherte kann mit dem neuen Aktenkonto nicht
1937 interagieren, bis der Import abgeschlossen ist. Das ePA-Modul Frontend des Versicherten
1938 muss jedoch nicht auf den Abschluss warten, weil der Vorgang auf Ebene der Dienste
1939 asynchron abgeschlossen ist, nachdem der Versicherte ihn mittels des Aufrufs der
1940 Operation I_Account_Management_Insurant::SuspendAccount beim alten Anbieter und
1941 dem direkt anschließenden Aufruf der Operation
1942 I_Account_Management_Insurant::ResumeAccount beim neuen Anbieter ausgelöst hat.
- 1943 **A_15624 - Komponente ePA-Dokumentenverwaltung – Abfrage auf**
1944 **Verfügbarkeit des Exportpakets**
1945 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS nach dem
1946 Aufruf der Operation I_Account_Management_Insurant::ResumeAccount bei unmittelbar
1947 vorgesehenem Abruf des Exportpakets bis zum Erfolgsfall periodisch prüfen,
1948 jedoch maximal für einen Zeitraum von drei Werktagen, ob ein Exportpaket unter der
1949 vom Client übergebenen URL bereitsteht.[<=]
- 1950 **A_15625 - Komponente ePA-Dokumentenverwaltung – Kein Aktenzugriff**
1951 **während des Imports der Daten**
1952 Die Komponente ePA-Dokumentenverwaltung MUSS während der Ausführung der
1953 Operation I_Account_Management_Insurant::ResumeAccount für ein Aktenkonto alle
1954 Operationen mit Fehlermeldung "Aktenkonto aufgrund einer andauernden
1955 Datenmigration vorübergehend nicht erreichbar" ablehnen.[<=]
- 1956 **A_16077 - Komponente ePA-Dokumentenverwaltung – Frist für den Import des**
1957 **Exportpakets**
1958 Die Komponente ePA-Dokumentenverwaltung MUSS den Import eines Exportpakets
1959 innerhalb von drei Werktagen nach Beginn des Downloads vom vorherigen Anbieter
1960 abschließen.
1961 [<=]
- 1962 **A_17845 - Komponente ePA-Dokumentenverwaltung – Offener**
1963 **Verarbeitungskontext während der Verarbeitung des Exportpakets**
1964 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS den für die
1965 Operation I_Account_Management_Insurant::ResumeAccount geöffneten
1966 Verarbeitungskontext so lange geöffnet lassen, bis der Abruf des Exportpakets beim alten
1967 Anbieter erfolgt ist und die Verarbeitung der Daten des Exportpakets durch diesen
1968 Verarbeitungskontext abgeschlossen ist, jedoch maximal drei Tage, falls kein
1969 Exportpaket abgerufen werden kann.
1970 [<=]

1971 **5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents**
 1972 **A_14490-01 - Komponente ePA-Dokumentenverwaltung – Signatur für Get**
 1973 **Audit Events**

1974 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 1975 I_Account_Management_Insurant::GetAuditEvents gemäß der folgenden Signatur
 1976 implementieren:

1977 **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.	

1978 [`<=`]

1979

1980 *5.2.1.3.1 Umsetzung*

1981 **A_15229 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für
1982 Get Audit Events**

1983 Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren
1984 Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient
1985 Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor eine Audit
1986 Event List zum ePA-Modul Frontend des Versicherten zurückgegeben wird.
1987

1988 [`<=`]

1989 **A_15583 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Get Audit
1990 Events**

1991 Die Komponente ePA-Dokumentenverwaltung MUSS die Liste der § 291a-
1992 Protokolleinträge als Liste `phr:AuditMessage` zurückgeben. [`<=`]

1993 **5.3 Zugriffskontrolle**

1994 Die Zugriffskontrolle basiert auf drei Zugriffsgruppen, welche Dokumente in die
1995 elektronische Patientenakte eines Versicherten einstellen. Diese Zugriffsgruppen müssen
1996 den einzustellenden Dokumenten jeweils ein vorbestimmtes, nicht änderbares
1997 Kennzeichen zuordnen, was ihre Zugriffsgruppe repräsentiert. Diese Gruppen sind:

- 1998 • Zugriffsgruppe der Leistungserbringerinstitutionen, wobei der Leistungserbringer
1999 dieses Dokument einstellt
- 2000 • Zugriffsgruppe des Versicherten, wobei der Versicherte (oder sein berechtigter
2001 Vertreter) dieses Dokument einstellt
- 2002 • Zugriffsgruppe des Kostenträgers, wobei der Kostenträger dieses Dokument
2003 einstellt

2004 Einer Leistungserbringerinstitution werden im Rahmen der Autorisierung durch den
2005 Versicherten bzw. seines Vertreters Zugriffsrechte auf Dokumente mit diesen
2006 Zugriffsgruppen gewährt. Dies kann in beliebiger Kombination entweder ad-hoc beim
2007 Arztbesuch oder über das ePA-Modul Frontend des Versicherten erfolgen. Von einem
2008 Versicherten bzw. seinen Vertreter vergebene Zugriffsrechte an eine
2009 Leistungserbringerinstitution auf die Dokumente der Zugriffsgruppe des Versicherten

2010 oder des Kostenträgers beinhalten das Lesen und Löschen von Dokumenten. Weiterhin
2011 haben Mitarbeiter von Leistungserbringerinstitutionen die Möglichkeit, ein
2012 Dokument gesondert als leistungserbringeräquivalent zu kennzeichnen, was das
2013 Aktualisieren der Dokumentmetadaten erfordert – siehe unten.

2014 Kostenträger können Dokumente lediglich einstellen, d.h. sie können Dokumente weder
2015 lesen, ändern oder löschen. Sie brauchen zum Einstellen allerdings technisch bedingt ein
2016 Zugriffsrecht, welches durch einen Versicherten vergeben werden kann.

2017 Weiterhin können Mitarbeiter aus Leistungserbringerinstitutionen – sofern ein
2018 Zugriffsrecht besteht – die Sichtbarkeit bzw. den Zugriff auf Dokumente, die der
2019 Zugriffsgruppe der Versicherten oder Kostenträger zugeordnet sind, erweitern. Das
2020 bedeutet, ein einzelnes Dokument, welches von einem Versicherten oder einem
2021 Kostenträger eingestellt wurde, kann von einem Leistungserbringer als
2022 "leistungserbringeräquivalent" gekennzeichnet werden, wenn es für die Behandlung eines
2023 Patienten relevant erscheint und auch andere Leistungserbringer darauf Zugriff erhalten
2024 sollen. Dies ermöglicht, dass Leistungserbringer ohne Zugriff auf Dokumente des
2025 Versicherten oder auf die eingestellten Dokumente eines Kostenträgers dennoch
2026 behandlungsrelevante Dokumente einsehen können (nur lesender Zugriff). Der
2027 Zugriffsgruppe der Leistungserbringerinstitutionen werden daher implizit auch
2028 Zugriffsrechte auf Dokumente mit diesem Kennzeichen eingeräumt. Dieses Kennzeichen
2029 kann jederzeit wieder von einem Mitarbeiter einer Leistungserbringerinstitution entfernt
2030 werden. All diese Zugriffsszenarien haben keinen Einfluss auf das omnipräsente Lese-
2031 und Löschrecht auf Dokumente des Versicherten. Das bedeutet, dass der Versicherte
2032 bzw. sein Vertreter alle Dokumente aus allen Zugriffsgruppen lesen oder löschen kann.

2033 Die benannten Zugriffskonstellationen werden über sogenannte Confidentiality Codes an
2034 den IHE XDS-Dokumentmetadaten realisiert. Jedem Code, genauer gesagt jeder
2035 Zugriffsumgebung, werden XACML Policies [XACML] nach den inhaltlichen Vorgaben
2036 von [IHE-ITI-APPC] zugeordnet, welche die erlaubten Zugriffe auf die Dokumente in einer
2037 bestimmten Konstellation von IHE ITI-Transaktionen steuern. Diese Codes, welche der
2038 OID 1.2.276.0.76.5.491 und dem Code System Name "ePA-Vertraulichkeit"
2039 zugeordnet sind, sind die folgenden:

- 2040 • Code = "LEI", Display Name = "Dokument einer
2041 Leistungserbringerinstitution"
- 2042 • Code = "KTR", Display Name = "Dokument eines Kostenträgers"
- 2043 • Code = "PAT", Display Name = "Dokument eines Versicherten"

2044 Darüber hinaus kann ein weiterer Code zur gesonderten Kennzeichnung eines
2045 leistungserbringeräquivalenten Dokuments bei einem bestehenden Dokument
2046 hinzugefügt oder später auch wieder entfernt werden, welches bereits einen
2047 Confidentiality Code = "PAT" oder "KTR" hat:

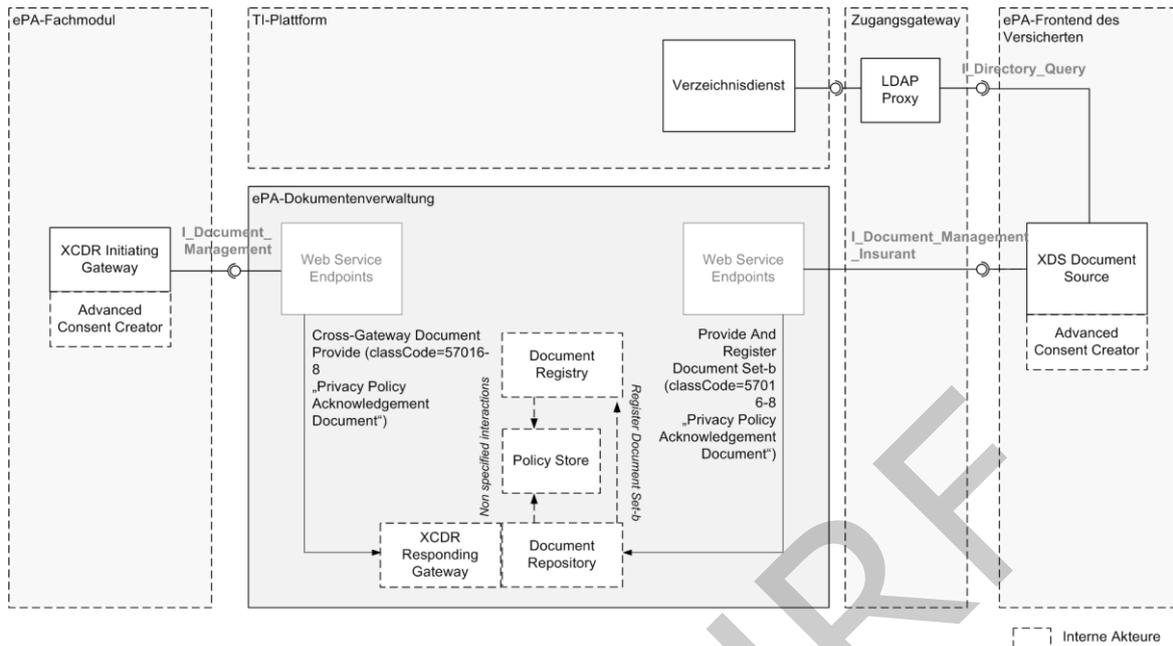
- 2048 • Code = "LEÄ", Display Name="Leistungserbringeräquivalentes Dokument
2049 eines Versicherten oder Kostenträgers"

2050 Diesen Code bzw. dieses Kennzeichen darf, wie oben beschrieben, ausschließlich ein
2051 Mitarbeiter einer Leistungserbringerinstitution vergeben oder entfernen.

2052 **5.3.1 Funktionsprinzip Policy Administration**

2053 Die Berechtigungsvergabe an Leistungserbringerinstitutionen und Vertreter des
2054 Versicherten erfolgt durch das Einstellen von Policy Documents (siehe nachstehende
2055 Abbildung). Diese Dokumente werden in den Abschnitten 5.3.2.2 bis 5.3.2.5 für die ePA-

- 2056 Fachanwendung definiert und setzen ferner das Zugriffskontrollmodell Attribute-based
2057 Access Control (ABAC) um.
- 2058 Die Registrierung dieser sogenannten Advanced Patient Privacy Consents erfolgt als
2059 unverschlüsselte Dokumente (jedoch über die sichere Verbindung zwischen dem
2060 Fachmodul ePA bzw. dem ePA-Modul Frontend des Versicherten und dem
2061 Verarbeitungskontext) durch Nutzung der IHE ITI-Transaktionen "Cross-Gateway
2062 Document Provide" [ITI-80] sowie "Provide And Register Document Set-b" [ITI-41]. Die
2063 interne Datenhaltung bzgl. der Policy Documents (Advanced Patient Privacy Consents) ist
2064 nicht vorgegeben, allerdings müssen diese Policy Documents über die Standard-
2065 Abfrageschnittstelle über
2066 die Operation `I_Document_Management_Insurant::RegistryStoredQuery` dem ePA-
2067 Modul Frontend des Versicherten zugänglich gemacht werden. Dazu werden die
2068 DocumentEntry-Metadaten gemäß der Anforderung [gemSpec_DM_ePA#A_14961]
2069 vorgegeben.
- 2070
- 2071 Die grundlegende Zugriffsstrategie ist "opting-in", sodass ein gewährendes Zugriffsrecht
2072 nur durch Registrierung eines neuen Policy Documents vergeben werden kann. Eine
2073 inhaltliche Änderung eines Policy Documents ist nicht vorgesehen. Stattdessen soll durch
2074 den Client ein zu einem Berechtigten vorhandenes Policy Document gelöscht und ein
2075 neues registriert werden. Wurde ein vorhandenes Policy Document, das demselben
2076 Berechtigten zuzuordnen ist (d.h. `xacml:SubjectMatch` und `xacml:ResourceMatch` sind
2077 identisch), durch den Client nicht gelöscht, wird dieses von der ePA-
2078 Dokumentenverwaltung automatisch gelöscht, während das neue Policy Document
2079 eingestellt wird.
- 2080 **A_14998 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen**
2081 **vom Policy Document bei neuem Policy Document mit demselben Berechtigten**
2082 Die Komponente ePA-Dokumentenverwaltung MUSS über die Operationen
2083 `I_Document_Management::CrossGatewayDocumentProvide` sowie
2084 `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b` eine Prüfung
2085 auf ein bereits registriertes Policy Document (Advanced Patient Privacy Consent) mit
2086 demselben Berechtigten sowie der Aktenidentität (d.h. `xacml:SubjectMatch` und
2087 `xacml:ResourceMatch` sind identisch) durchführen und bei Existenz dieses
2088 Policy Documents (Advanced Patient Privacy Consent) dieses samt IHE ITI-XDS-
2089 Metadaten löschen, bevor ein neues Policy Document gespeichert wird.
2090 [`<=`]
- 2091 **A_14892 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen**
2092 **ungültiger Policy Documents**
2093 Die Komponente ePA-Dokumentenverwaltung SOLL Policy Documents (Advanced Patient
2094 Privacy Consents) und zugehörige IHE ITI-XDS-Metadaten löschen, wenn diese Policy
2095 Documents ihre zeitliche Gültigkeit verlieren.
2096 [`<=`]
- 2097 Der durch die vorstehende Anforderung motivierte Vorgang kann nur ausgeführt werden,
2098 wenn der Verarbeitungskontext für das Aktenkonto durch einen berechtigten Nutzer
2099 aktiviert wurde.
- 2100 **A_14895 - Komponente ePA-Dokumentenverwaltung – Schutz vor Manipulation**
2101 **der Policy Documents**
2102 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Policy
2103 Documents (Advanced Patient Privacy Consents) gegen Veränderung und unberechtigtes
2104 Löschen geschützt sind.
2105 [`<=`]



2106

2107

Abbildung 2: Schematische Darstellung zur Vergabe von Berechtigungen

2108

2109 *Hinweis: Die vorstehende Abbildung verdeutlicht, wie Berechtigungen über die*
 2110 *entsprechenden IHE ITI-Transaktionen vergeben werden. Der Transaktion "Cross-*
 2111 *Gateway Document Provide" liegt genau genommen keine IHE ITI-konforme Nachricht*
 2112 *des Primärsystems zum Einstellen des Policy Documents durch den Versicherten*
 2113 *zugrunde. Stattdessen wird diese Transaktion durch die Web-Service-Operation*
 2114 *"RequestFacilityAuthorization" gemäß [gemSpec FM ePA#7.2.1.2](#) ausgelöst, sodass sich*
 2115 *die Verwendung der Transaktion "Cross-Gateway Document Provide" eigentlich verbietet.*
 2116 *Aus Praktikabilitätsgründen ist jedoch keine separate Schnittstelle mit der Transaktion*
 2117 *"Provide And Register Document Set-b" für die*
 2118 *Schnittstelle I_Document_Management zum Einstellen eines Policy Documents gegenüber*
 2119 *der ePA-Dokumentenverwaltung definiert.*

2120 Der Entzug von Berechtigungen erfolgt über das Löschen von ausgewählten Policy
 2121 Documents durch Ausführung der
 2122 Operation `I_Document_Management_Insurant::RemoveDocuments`, wie die folgende
 2123 Abbildung verdeutlicht.

2124

2153 **A_15536 - Komponente ePA-Dokumentenverwaltung – Prüfungen bei**
2154 **Registrierung eines Policy Documents**

2155 Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy
2156 Documents (Advanced Patient Privacy Consents) folgende inhaltlichen Prüfungen
2157 durchführen und im Fehlerfall die Nachricht mit einem HTTP-Statuscode 400 gemäß
2158 [RFC7231] quittieren:

- 2159 • *Prüfung der XACML 2.0 Policy-Konformität*
2160 Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML
2161 2.0 Policy abbrechen, wenn das Profil der vorliegenden XACML 2.0 Policy nicht mit
2162 den Anforderungen aus den Abschnitten 5.3.2.2 bis 5.3.2.5 übereinstimmt. Dabei
2163 MUSS die Verwendung der PolicySetIdReference(n) zur intendierten Berechtigung
2164 passen. Das heißt, eine XACML 2.0 Policy für die Berechtigung eines
2165 Kostenträgers darf beispielsweise nur die PolicySetIdReference mit dem Wert
2166 "urn:gematik:policy-set-id:permissions-access-group-insurance"
2167 verwenden.
- 2168 • *Prüfung der Aktenidentität*
2169 Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML
2170 2.0 Policy abbrechen, wenn das Resource-Element mit der Attribut-ID
2171 "urn:ihe:iti:ser:2016:patient-id" nicht mit der Identität der Akte aus dem
2172 internen Policy Document mit der Policy Set ID "urn:gematik:policy-set-
2173 id:insurant" übereinstimmt.
- 2174 • *Prüfung des Einstellers*
2175 Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML
2176 2.0 Policy abbrechen, wenn die in der Nachricht enthaltene SAML 2.0 Assertion
2177 (Authentication Assertion / X-User Assertion) nicht dem Versicherten oder einem
2178 seiner Vertreter zugeordnet ist (d.h. das root-Attribut des InstanceIdentifier-
2179 Elements innerhalb des SubjectMatch-Elements muss mit der OID
2180 "1.2.276.0.76.4.8" eine KVNR kennzeichnen).
- 2181 • *Keine Verwendung des "xsi:schemaLocation"-Attributs*
2182 Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML
2183 2.0 Policy abbrechen, wenn ein xsi:schemaLocation-Attribut gemäß
2184 [XMLSchema#2.6.3] enthalten ist.

2185 [\leq]

2186 **A_14822 - Komponente ePA-Dokumentenverwaltung – Attribute für Anfrage**
2187 **einer Autorisierungsentscheidung**

2188 Die Komponente ePA-Dokumentenverwaltung MUSS das "Policy Pull"-Muster gemäß
2189 [IHE-ITI-ACWP] umsetzen und die folgenden Daten für eine Berechtigungsprüfung
2190 extrahieren sowie eine Autorisierungsanfrage gegen die vorhandenen Policy Documents
2191 (Advanced Patient Privacy Consents) stellen, um die autorisierte Verarbeitung eines
2192 Dokuments sicherzustellen:

- 2193 • Subject ID oder XSPA Organization ID der Authentication Assertion / X-User
2194 Assertion
- 2195 • unveränderbarer Teil der KVNR aus der Eingangsnachricht oder serverseitig mit
2196 Hilfe von Anfrageparametern beschafft (Aktenidentität)
- 2197 • wsa:Action-Element aus der Eingangsnachricht
- 2198 • ggf. Confidentiality Code des Dokuments

2199 [\leq]

2200 **A_16195 - Komponente ePA-Dokumentenverwaltung – UTF-8-Kodierung eines**
2201 **Policy Documents**
2202 Die Komponente ePA-Dokumentenverwaltung MUSS ausschließlich UTF-8-kodierte Policy
2203 Documents verarbeiten.[<=]

2204 **5.3.2.1 Erstmaliges Öffnen eines Verarbeitungskontextes**

2205 Beim erstmaligen Öffnen des Verarbeitungskontextes eines neu registrierten Aktenkontos
2206 durch den Versicherten muss dieser erkennen, dass er erstmalig geöffnet wird und die
2207 Aktenzustände "Registered" und "Registered for Migration"
2208 gemäß [\[gemSpec Aktensystem#6.1.1\]](#) unterscheiden. Darüber hinaus ist der
2209 Verarbeitungskontext für den Versicherten gemäß der Anforderung A_15250 zu
2210 personalisieren. Die für die Personalisierung und die Unterscheidung der Aktenzustände
2211 erforderliche Konfiguration des Verarbeitungskontextes für das Aktenkonto erfolgt über
2212 die Authorization Assertion.

2213 **A_15603 - Komponente ePA-Dokumentenverwaltung – Nur Resume Account** 2214 **bei erforderlicher Datenübernahme möglich**

2215 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass ausschließlich die
2216 Operation `I_Account_Management_Insurant::ResumeAccount` ausgeführt werden kann,
2217 wenn der Verarbeitungskontext erstmalig vom Versicherten geöffnet wurde und eine
2218 Übernahme von Daten aus dem Aktenkonto des Versicherten bei einem vorherigen
2219 Anbieter erforderlich ist, d.h. das Aktenkonto mit der Option "Registered for Migration"
2220 registriert wurde.[<=]

2221 **5.3.2.2 Berechtigung für einen Versicherten**

2222 **A_15437 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum** 2223 **Inhalt eines Policy Documents zur Berechtigung eines Versicherten**

2224 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS eine
2225 XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-
2226 ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_100 in
2227 [Anhang B](#) durchsetzen (Base Policy).
2228 [<=]

2229 Um dem Versicherten Zugriff auf seine Akte zu gewähren, wird die Akte im Zuge ihrer
2230 Erstbenutzung durch den Versicherten personalisiert und ein Versicherten-Policy-
2231 Document erstellt bzw. aktiviert.

2232 **A_15250 - Komponente ePA-Dokumentenverwaltung – Aktivierung des Policy** 2233 **Documents "urn:gematik:policy-set-id:insurant"**

2234 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS eine
2235 Personalisierung durchführen. Dazu MUSS die Komponente ePA-Dokumentenverwaltung
2236 das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set
2237 ID "urn:gematik:policy-set-id:insurant" aktivieren und anschließend die darin
2238 festgelegten Regeln bei Zugriffsanfragen durchsetzen. Der Verarbeitungskontext der
2239 Komponente ePA-Dokumentenverwaltung MUSS die Personalisierung im Zuge des ersten
2240 Aufrufs einer fachlichen Operation durchführen und das Policy Document unmittelbar auf
2241 die fachliche Operation anwenden, die die Personalisierung ausgelöst hat. Der Aufruf
2242 der Operation `I_Document_Management_Connect::OpenContext` zur kryptographischen
2243 Aktivierung gilt in diesem Zusammenhang nicht als fachliche Operation.[<=]

2244 Die Festlegung des Zeitpunkts der Personalisierung in der vorstehenden Anforderung
2245 verhindert die Personalisierung eines Verarbeitungskontexts für den Fall, dass für ein mit
2246 der Option "Registered for Migration" registriertes Aktenkonto der Verarbeitungskontext
2247 geöffnet wird, ohne dass unmittelbar anschließend die

2248 OperationI_Account_Management_Insurant::ResumeAccount aufgerufen wird. Der
2249 Verarbeitungskontext verbleibt damit in seinem initialen (d.h. ungenutzten) Zustand, so
2250 dass der Vorgang konsistent neu gestartet werden kann.

2251 **A_15178 - Komponente ePA-Dokumentenverwaltung – Unveränderliches Policy**
2252 **Document "urn:gematik:policy-set-id:insurant"**

2253 Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass das Policy
2254 Document (Advanced Patient Privacy Consent) mit der Policy Set
2255 ID "urn:gematik:policy-set-id:insurant" nach ihrer Aktivierung kontinuierlich und
2256 dauerhaft unverändert für die Zugriffskontrollprüfung wirksam ist.[<=]

2257 **A_15230 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum**
2258 **Inhalt eines Policy Documents zur Berechtigung eines Versicherten mit**
2259 **erlaubten Operationen**

2260 Die Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy
2261 Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter
2262 Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_101 in Anhang B
2263 erstellen und durchsetzen (Permission Policy).
2264 [<=]

2265 **A_15616-01 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe**
2266 **des Policy Documents "urn:gematik:policy-set-id:permissions-access-group-**
2267 **insurant"**

2268 Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced
2269 Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-
2270 id:permissions-access-group-insurant" über Suchoperationen NICHT dem ePA-
2271 Frontend des Versicherten zur Verfügung stellen. Ferner DARF es NICHT heruntergeladen
2272 werden können.[<=]

2273 **5.3.2.3 Berechtigung für einen Vertreter**

2274 **A_15440 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum**
2275 **Inhalt eines Policy Documents zur Berechtigung eines Vertreters**

2276 Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des
2277 Versicherten übermittelte XACML 2.0 Policy auf Konformität als Policy Document
2278 (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der
2279 Anforderungen an den Inhalt in Tab_Dokv_200 in Anhang B (Base Policy) prüfen.
2280 [<=]

2281 **A_15441 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum**
2282 **Inhalt eines Policy Documents zur Berechtigung eines Vertreters mit erlaubten**
2283 **Operationen**

2284 Die Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy
2285 Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter
2286 Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_201 in Anhang B
2287 erstellen und durchsetzen (Permission Policy).
2288 [<=]

2289 **A_15240 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe des**
2290 **Policy Documents "urn:gematik:policy-set-id:permissions-access-group-**
2291 **representative"**

2292 Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced
2293 Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-
2294 id:permissions-access-group-representative" über Suchoperationen NICHT dem
2295 ePA-Frontend des Versicherten zur Verfügung stellen. Ferner DARF es NICHT
2296 heruntergeladen werden können.
2297 [<=]

2298 Ein Vertreter darf keine weiteren Vertreter, sondern ausschließlich
 2299 Leistungserbringerinstitutionen, berechtigen.

2300 **A_15180 - Komponente ePA-Dokumentenverwaltung – Prüfung auf weitere,**
 2301 **unerlaubte Vertreiberberechtigungen**

2302 Die Komponente ePA-Dokumentenverwaltung MUSS ein von einem Vertreter
 2303 übermitteltes Policy Document (Advanced Patient Privacy Consent) ablehnen, falls das
 2304 XACML 2.0 Subject nicht das Attribut "urn:gematik:subject:organization-id" enthält.
 2305 [`<=`]

2306 **5.3.2.4 Berechtigung für eine Leistungserbringerinstitution**

2307 **A_15442-01 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben**
 2308 **zum Inhalt eines Policy Documents zur Berechtigung einer**
 2309 **Leistungserbringerinstitution**

2310 Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des
 2311 Versicherten bzw. vom Fachmodul ePA übermittelte XACML 2.0 Policy auf Konformität als
 2312 Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter
 2313 Berücksichtigung der Anforderungen an den Inhalt in Tab_Dokv_300-01 prüfen.

2314 **Tabelle 22: Tab_Dokv_300-01 - XACML 2.0 Policy für eine**
 2315 **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: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 Telematik-ID 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 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.
		InstanceIdentifier	R	
		@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
		@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
		@extension	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
		ResourceAttributeDesignator	R	
		@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
<!-- Gültigkeitszeitraum des Policy Documents -->				
		Environments	R	
		Environment	R	

		EnvironmentMatch	R	
		@MatchId	R	Der Wert "urn:oasis:names:tc: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"

2316

2317 [\leq]

2318

2319 **A_15519 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum**
 2320 **Inhalt eines Policy Documents zur Berechtigung einer**
 2321 **Leistungserbringerinstitution mit erlaubten Operationen**

2322 Die Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy
 2323 Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter
 2324 Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_301 in Anhang B
 2325 erstellen und durchsetzen (Permission Policy).

2326 [\leq]

- 2327 **A_15242 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe des**
2328 **Policy Documents "urn:gematik:policy-set-id:permissions-access-group-hcp"**
2329 Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced
2330 Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-
2331 id:permissions-access-group-hcp" über Suchoperationen NICHT dem ePA-Frontend
2332 des Versicherten zur Verfügung stellen. Ferner DARF es NICHT heruntergeladen werden
2333 können.[<=]
- 2334 **A_15243 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe des**
2335 **Policy Documents "urn:gematik:policy-set-id:permissions-access-group-hcp-**
2336 **insurance-documents"**
2337 Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced
2338 Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-
2339 id:permissions-access-group-hcp-insurance-documents" über Suchoperationen
2340 NICHT dem ePA-Frontend des Versicherten zur Verfügung stellen. Ferner DARF es NICHT
2341 heruntergeladen werden können.[<=]
- 2342 **A_17459 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe des**
2343 **Policy Documents "urn:gematik:policy-set-id:permissions-access-group-hcp-**
2344 **insurant-documents"**
2345 Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced
2346 Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-
2347 id:permissions-access-group-hcp-insurant-documents" über Suchoperationen
2348 NICHT dem ePA-Frontend des Versicherten zur Verfügung stellen. Ferner DARF es NICHT
2349 heruntergeladen werden können.[<=]
- 2350 **5.3.2.5 Berechtigung für einen Kostenträger**
- 2351 **A_17460 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum**
2352 **Inhalt eines Policy Documents zur Berechtigung eines Kostenträgers**
2353 Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des
2354 Versicherten übermittelte XACML 2.0 Policy auf Konformität als Policy Document
2355 (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der
2356 Anforderungen an den Inhalt in Tab_Dokv_400 in Anhang.B. (Base Policy) prüfen.[<=]
- 2357 **A_17461 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum**
2358 **Inhalt eines Policy Documents zur Berechtigung eines Kostenträgers mit**
2359 **erlaubten Operationen**
2360 Die Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy
2361 Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter
2362 Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_401 in Anhang.B
2363 erstellen und durchsetzen (Permission Policy).[<=]
- 2364 **A_17462 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe des**
2365 **Policy Documents "urn:gematik:policy-set-id:permissions-access-group-**
2366 **insurance"**
2367 Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced
2368 Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-
2369 id:permissions-access-group-insurance" über Suchoperationen NICHT dem ePA-
2370 Frontend des Versicherten zur Verfügung stellen. Ferner DARF es NICHT heruntergeladen
2371 werden können.[<=]

2372 **5.4 Vertrauenswürdige Ausführung**2373 **5.4.1 Schnittstelle I_Document_Management_Connect**

2374 Diese Schnittstelle setzt die in [gemSysL_ePA] definierte
2375 Schnittstelle `I_Document_Management_Connect` technisch um. Die logische
2376 `OperationI_Document_Management_Connect::ConnectToContext` aus [gemSysL_ePA]
2377 wird durch den Verbindungsaufbau der Clients zum Verarbeitungskontext der ePA-
2378 Dokumentenverwaltung umgesetzt. Die Client-Verbindungen vom Fachmodul ePA zu der
2379 Schnittstelle sowie vom ePA-Modul Frontend des Versicherten zu der Schnittstelle werden
2380 über HTTP hergestellt. Die Schnittstelle ermöglicht beiden Clients den Aufbau eines
2381 sicheren Kanals auf Inhaltsebene zum Verarbeitungskontext der Vertrauenswürdigen
2382 Ausführungsumgebung (VAU), die Aktivierung des Verarbeitungskontextes mittels
2383 Übergabe des Kontextschlüssels sowie die Beendigung ihrer Client-Verbindung. Das
2384 Fachmodul ePA baut zum Kontextmanagement eine TLS-Verbindung auf. Die Verbindung
2385 des ePA-Moduls Frontend des Versicherten zum Kontextmanagement erfolgt mittels
2386 Weiterleitung der HTTP Requests und HTTP Responses durch das Zugangsgateway,
2387 welches auch einen HTTP Header zur Identifikation der Sitzung setzt.

2388 Das Protokoll für den Verbindungsaufbau zwischen Clients und dem Verarbeitungskontext
2389 folgt den Spezifikationen in [gemSpec_Krypt#3.15] und [\[gemSpec_Krypt#6\]](#). Zur
2390 Prüfung der Autorisierung des Clients durch das Kontextmanagement wird das dort
2391 beschriebene Protokoll um zwei zusätzliche Schlüssel-Wert-Paare ergänzt, die die
2392 Authorization Assertion im HTTP Body in der `VAUClientHello`-Nachricht und optional
2393 einen Sitzungsbezeichner im HTTP Header übermitteln.

2394 **A_15587 - Komponente ePA-Dokumentenverwaltung – Implementierung des**
2395 **sicheren Verbindungsprotokolls**

2396 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS für die
2397 Schnittstelle `I_Document_Management_Connect` das Kommunikationsprotokoll gemäß den
2398 Vorgaben aus [gemSpec_Krypt#3.15] und [\[gemSpec_Krypt#6\]](#) umsetzen.
2399 [`<=`]

2400 **A_15592-01 - Komponente ePA-Dokumentenverwaltung – Erweiterung des**
2401 **sicheren Verbindungsprotokolls**

2402 Ein Client (d.h. ePA-Fachmodul, ePA-Modul Frontend des Versicherten, Fachmodul ePA KTR-
2403 Consumer) MUSS bei der Erzeugung der `VAUClientHello`-Nachricht (vgl. [A_16883-01](#)) im
2404 ~~„Authorization-Assertion“~~-Datenfeld `AuthorizationAssertion` die Base64-kodierte Authorization -
2405 Assertion eintragen.

2406
2407 Weiterhin MUSS der Verarbeitungskontext der Komponente ePA-
2408 Dokumentenverwaltung ein optionales Schlüssel-Wert-Paar zur Übermittlung eines
2409 Sitzungsbezeichners an das Kontextmanagement im HTTP-Request-Header prüfen und
2410 akzeptieren. Das Schlüssel-Wert-Paar hat die Form

2411 `Session: ...Sitzungsbezeichner vom Zugangsgateway... [<=]`

2412 **A_14631 - Komponente ePA-Dokumentenverwaltung – HTTP-Schnittstelle**
2413 **I_Document_Management_Connect**

2414 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die
2415 Schnittstelle `I_Document_Management_Connect` für über das Zugangsgateway vermittelte
2416 HTTP-Verbindungen des ePA-Moduls Frontends des Versicherten verfügbar machen. [`<=`]

2417 **A_15540 - Komponente ePA-Dokumentenverwaltung – TLS-Schnittstelle**
2418 **I_Document_Management_Connect**

2419 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die
2420 Schnittstelle `I_Document_Management_Connect` für TLS-Verbindungen des Fachmoduls

2421 ePA sowie des Fachmoduls ePA KTR-Consumer verfügbar machen.
 2422 [`<=`]

2423 **A_15588 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext**
 2424 **bei Bedarf verfügbar machen**

2425 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS
 2426 Verarbeitungskontexte bedarfsgesteuert für autorisierte Nutzer verfügbar machen. [`<=`]

2427 **A_14633 - Komponente ePA-Dokumentenverwaltung – Vermittlung der**
 2428 **Verbindung zwischen Client und Verarbeitungskontext**

2429 Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die
 2430 Verbindung zwischen Client, d.h. dem ePA-Modul Frontend des Versicherten bzw. dem
 2431 Fachmodul ePA oder Fachmodul ePA KTR-Consumer, und Verarbeitungskontext
 2432 vermitteln und dabei

- 2433 • die Base64-dekodierte Authorization Assertion der `VAUClientHello`-Nachricht auf
 2434 Gültigkeit gemäß Anforderung A_13690 sowie auf den gültigen Berechtigungstyp
 2435 (`AuthorizationType = "DOCUMENT_AUTHORIZATION"`) prüfen und bei ungültiger
 2436 Authorization Assertion den Verbindungsaufbau abbrechen und mit dem HTTP-
 2437 Fehler 403 antworten,
- 2438 • den Record Identifier des Verarbeitungskontextes über den Wert des Attributs
 2439 `Resource ID` aus der Authorization Assertion der `VAUClientHello`-Nachricht
 2440 ermitteln,
- 2441 • für Clients vom Typ ePA-Modul Frontend des Versicherten die Verbindung auf der
 2442 Grundlage des vom Zugangsgateway gesetzten HTTP Header-
 2443 Feldes `Session` registrieren,
- 2444 • für Clients vom Typ Fachmodul ePA die Verbindung auf Grundlage der TLS-Sitzung
 2445 registrieren,
- 2446 • während der Dauer der Sitzung alle eingehenden Requests auf der Grundlage der
 2447 registrierten Verbindung an den Zielverarbeitungskontext weiterleiten sowie
- 2448 • nach dem Ende der Sitzung, aufgrund eines Timeouts bzw. aufgrund einer
 2449 Beendigung durch den Nutzer, die Registrierung der Verbindung löschen.

2450 [`<=`]

2451 **A_14617-01A_14617 - Komponente ePA-Dokumentenverwaltung – Ablauf des**
 2452 **Verbindungsaufbaus**

2453 Die Komponente ePA-Dokumentenverwaltung MUSS den Verbindungsaufbau von Clients,
 2454 d.h. von einem ePA-Modul Frontend des Versicherten oder einem Fachmodul so
 2455 umsetzen, dass der folgende Ablauf in angegebener Reihenfolge ausgeführt wird,
 2456 nachdem ein HTTP Request mit einer `VAUClientHello`-Nachricht von einem Client
 2457 empfangen wurde:

2458 **Tabelle 23: Tab_Dokv_29 - Ablauf Operation Hello**

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden des HTTP Request mit <code>VAUClientHello</code> -Nachricht)
1	Kontextmanagement	Prüfen der Authorization Assertion der <code>VAUClientHello</code> -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 <code>XSPA Resource ID</code> 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 <code>VAUClientHello</code> -Nachricht an den Verarbeitungskontext für den Record Identifier
6	Verarbeitungskontext	Registrieren der Authorization Assertion der <code>VAUClientHello</code> -Nachricht und Erzeugen der <code>VAUServerHello</code> -Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
7	Verarbeitungskontext	Senden der <code>VAUServerHello</code> -Nachricht
8	Kontextmanagement	Weiterleiten der <code>VAUServerHello</code> -Nachricht an den Client
9	Verarbeitungskontext	Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
	(Client)	(Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6])

	(Client)	(Erzeugen und Senden der VAUClientSigFin-Nachricht)
10	Kontextmanagement	<p>Weiterleiten der VAUClientSigFin-Nachricht an den Verarbeitungskontext für den RecordIdentifier Record Identifier</p> <p>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])</p> <p>Im Fehlerfall MUSS der Verbindungsaufbau abgebrochen und mit einer VAUServerError-Nachricht beantwortet werden.</p>
11	Kontextmanagement Verarbeitungskontext	<p>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])</p> <p>Im Fehlerfall MUSS der Verbindungsaufbau abgebrochen und mit einer VAUServerError-Nachricht beantwortet werden. Weiterleiten der VAUClientSigFin-Nachricht an den Verarbeitungskontext für den RecordIdentifier Record Identifier</p>
12	Verarbeitungskontext	Erzeugen der VAUServerFin-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
13	Kontextmanagement	Weiterleiten der VAUServerFin-Nachricht an den Client

2459 [**<=**]

2460 Der abgeleitete Sitzungsschlüssel wird anschließend vom Client und vom
 2461 Verarbeitungskontext gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6] genutzt,
 2462 um alle fachlichen Eingangs- und Ausgangsnachrichten zu ver- und entschlüsseln.

2463 **A_14545 - Komponente ePA-Dokumentenverwaltung – Operationen des**
 2464 **Dokumentenmanagements nur über sicheren Kanal nutzbar**

2465 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die
 2466 folgenden Operationen ausschließlich über den sicheren Kanal zwischen dem ePA-Modul
 2467 Frontend des Versicherten bzw. dem Fachmodul ePA und dem Verarbeitungskontext
 2468 verfügbar machen:

- 2469 • `I_Document_Management::CrossGatewayDocumentProvide`
- 2470 • `I_Document_Management::CrossGatewayQuery`
- 2471 • `I_Document_Management::RemoveDocuments`
- 2472 • `I_Document_Management::CrossGatewayRetrieve`
- 2473 • `I_Document_Management::RestrictedUpdateDocumentSet`
- 2474 • `I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b`
- 2475 • `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b`
- 2476 • `I_Document_Management_Insurant::RegistryStoredQuery`
- 2477 • `I_Document_Management_Insurant::RemoveDocuments`
- 2478 • `I_Document_Management_Insurant::RetrieveDocumentSet`
- 2479 • `I_Account_Management_Insurant::GetAuditEvents`
- 2480 • `I_Account_Management_Insurant::SuspendAccount`
- 2481 • `I_Account_Management_Insurant::ResumeAccount`
- 2482 • `I_Document_Management_Connect::OpenContext`
- 2483 • `I_Document_Management_Connect::CloseContext`

2484 Weiterhin MUSS der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung
 2485 bei sämtlichen genannten Operationen (bis auf Open Context und Close Context) prüfen,
 2486 ob das Subjekt der übergebenen Authentication Assertion mit dem der registrierten
 2487 Authorization Assertion übereinstimmt und im Fehlerfall eine `VAUServerError`-Nachricht
 2488 mit HTTP-Fehler 403 (Fehlermeldung "Access Denied") gemäß [gemSpec_Krypt#6.9]
 2489 returnieren. [`<=`]

2490 **A_14645 - Komponente ePA-Dokumentenverwaltung – Nutzung des sicheren**
 2491 **Kanals zwischen ePA-Modul Frontend des Versicherten bzw. Fachmodul ePA,**
 2492 **Fachmodul ePA KTR-Consumer und Verarbeitungskontext**

2493 Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS den mit
 2494 dem ePA-Modul Frontend des Versicherten bzw. mit dem Fachmodul ePA sowie dem
 2495 Fachmodul ePA KTR-Consumer gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
 2496 ausgehandelten Sitzungsschlüssel verwenden, um alle Eingangsnachrichten zu
 2497 entschlüsseln und alle Ausgangsnachrichten zu verschlüsseln. [`<=`]

2498
 2499 **A_14457 - Komponente ePA-Dokumentenverwaltung – Implementierung der**
 2500 **Schnittstelle `I_Document_Management_Connect`**

2501 Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle
 2502 definierte Web-Service-Schnittstelle implementieren.

2503 **Tabelle 24: 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	

2504 [**<=**]

2505 **5.4.1.1 Operation I_Document_Management_Connect::OpenContext**

2506 **A_14426 - Komponente ePA-Dokumentenverwaltung – Signatur für**

2507 **I_Document_Management_Connect::OpenContext**

2508 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

2509 I_Document_Management_Connect::OpenContext gemäß der folgenden Signatur

2510 implementieren:

2511 **Tabelle 25: Tab_Dokv_31 - Operation OpenContext**

Operation	I_Document_Management_Connect::OpenContext
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Connect::OpenContext technisch um. Mit dieser Operation wird der Kontextschlüssel an den Verarbeitungskontext übergeben.
Formatvorgabe n	SOAP Action: http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0/OpenContext
Eingangsparameter	

Name	Beschreibung	Typ	opt.
ContextKey	Der Kontextschlüssel	ContextKey	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
-	-	-	-
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
INVALID_AUTH_KEY	Der Kontextschlüssel ist ungültig.	Wenn der Vergleich mit einem bereits im Verarbeitungskontext vorhandenen Kontextschlüssel keine Übereinstimmung ergibt, oder das Entschlüsseln von Kontextdaten fehlschlägt	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	

2512 [\leq]

2513 5.4.1.1.1 Umsetzung

2514 **A_14687 - Komponente ePA-Dokumentenverwaltung – Ablauf der Operation**
 2515 **Open Context**

2516 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
 2517 `I_Document_Management_Connect::OpenContext` so umsetzen, dass nach einem Aufruf
 2518 der Operation durch einen Client, d.h. durch ein ePA-Modul Frontend des Versicherten,
 2519 ein Fachmodul ePA oder ein Fachmodul ePA KTR-Consumer, der folgende Ablauf in
 2520 angegebener Reihenfolge (1 - 6) ausgeführt wird:

2521 **Tabelle 26: Tab_Dokv_32 - Ablauf der Operation Open Context**

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden der <code>OpenContextRequest</code> -Nachricht über den sicheren Kanal zwischen Client und Verarbeitungskontext)

1	Kontextmanagement	Weiterleiten der <code>OpenContextRequest</code> -Nachricht an den Verarbeitungskontext gemäß den vorgehaltenen Zuordnungsdaten (siehe Anforderung A_14633)
2	Verarbeitungskontext	Entnahme des im Eingangsparameter <code>ContextKey</code> enthaltenen Kontextschlüssels
3	Verarbeitungskontext	Falls bereits eine Sitzung mit einem Nutzer besteht, Prüfung des neu erhaltenen Kontextschlüssels auf Übereinstimmung mit dem aus der bestehenden Sitzung bereits registrierten Kontextschlüssel und Abbruch mit Fehlermeldung <code>INVALID_AUT_KEY</code> bei Nichtübereinstimmung
4	Verarbeitungskontext	Falls nicht bereits eine Sitzung mit einem Nutzer besteht, Laden der benötigten Kontextdaten aus dem Speichersystem, Entschlüsseln mit dem erhaltenen Kontextschlüssel und Abbruch mit Fehlermeldung <code>INVALID_AUT_KEY</code> , falls die Entschlüsselung der Kontextdaten fehlschlägt. Sind keine Kontextdaten mit dem Verarbeitungskontext assoziiert (d.h. erstmaliges Öffnen) MUSS der Kontextschlüssel in der Sitzung verwendet werden, um die neu erzeugten Kontextdaten zu verschlüsseln. In diesem beschriebenen Fall wird die Verarbeitung nicht mit der Fehlermeldung <code>INVALID_AUT_KEY</code> abgebrochen.
5	Verarbeitungskontext	Senden der <code>OpenContextResponse</code> -Nachricht
6	Kontextmanagement	Weiterleiten der <code>OpenContextResponse</code> -Nachricht an den Client

2522 [`<=`]

2523 Der Verarbeitungskontext ist anschließend für die Verarbeitung von fachlichen
2524 Operationen bereit.

2525 **5.4.1.2 Operation `I_Document_Management_Connect::CloseContext`**

2526 **A_14462 - Komponente ePA-Dokumentenverwaltung – Signatur für**

2527 **`I_Document_Management_Connect::CloseContext`**

2528 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

2529 `I_Document_Management_Connect::CloseContext` gemäß der folgenden Signatur

2530 implementieren:

2531 **Tabelle 27: 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	

2532 [**<=**]

2533 *5.4.1.2.1 Umsetzung*

2534 **A_14707 - Komponente ePA-Dokumentenverwaltung – Ablauf der Operation**
2535 **Close Context**

2536 Die Komponente ePA-Dokumentenverwaltung MUSS die Operation
2537 I_Document_Management_Connect::CloseContext so umsetzen, dass nach einem Aufruf
2538 der Operation durch einen Client, d. h. durch ein ePA-Modul Frontend des Versicherten,
2539 ein Fachmodul ePA oder ein Fachmodul ePA KTR-Consumer, der folgende Ablauf in
2540 angegebener Reihenfolge (1 - 6) ausgeführt wird:

2541 **Tabelle 28: Tab_Dokv_34 - Ablauf Operation OpenContext**

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

2542 [\leq]

2543 **5.4.2 Hardware-Merkmale**

2544 Die Vertrauenswürdige Ausführungsumgebung setzt die Nutzung eines HSM zur
 2545 Speicherung und Anwendung der privaten Schlüssel von Dienstzertifikaten und
 2546 Schlüsselpaaren gemäß Anforderung A_14564 voraus.

6 Informationsmodelle

2547

2548 Ein gesondertes Informationsmodell der durch den Produkttypen verarbeiteten Daten
2549 wird nicht benötigt.

ENTWURF

2550

7 Anhang A – Verzeichnisse2551 **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 Profile
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

2552 **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.

2553 Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung
 2554 gestellt.

2555 **7.3 Abbildungsverzeichnis**

2556 ~~Abbildung 1: Komponentenerlegung ePA-Dokumentenverwaltung 13~~

2557 ~~Abbildung 2: Schematische Darstellung zur Vergabe von Berechtigungen 77~~

2558 ~~Abbildung 3: Schematische Darstellung zum Entzug von Berechtigungen 78~~

2559 ~~Abbildung 1: Komponentenerlegung ePA-Dokumentenverwaltung 13~~

2560 ~~Abbildung 2: Schematische Darstellung zur Vergabe von Berechtigungen 77~~

2561 ~~Abbildung 3: Schematische Darstellung zum Entzug von Berechtigungen 78~~

2562 |

2563 **7.4 Tabellenverzeichnis**

2564 ~~Tabelle 1: Tab_Dokv_10 – Kennzeichnung von Optionalitäten 22~~

2565 ~~Tabelle 2: Tab_Dokv_11 – Übersicht über gruppierte IHE ITI-Akteure und Optionen an den~~

2566 ~~Außerschnittstellen der ePA-Dokumentenverwaltung 22~~

2567 ~~Tabelle 3: Tab_Dokv_12 – Fehlercodes zu Fehlern gemäß Operationsdefinition 29~~

2568 ~~Tabelle 4: Tab_Dokv_35 – Eingangsparameter für TUC_PKI_018 36~~

2569 ~~Tabelle 5: Tab_Dokv_13 – Parameter des § 291a-Protokolls 38~~

2570 ~~Tabelle 6: Tab_Dokv_14 – Schnittstelle I_Document_Management 40~~

2571 ~~Tabelle 7: Tab_Dokv_16 – Operation Cross-Gateway Query 44~~

2572 ~~Tabelle 8: Tab_Dokv_17 – Operation Remove Documents 47~~

2573 ~~Tabelle 9: Tab_Dokv_18 – Operation Cross-Gateway Retrieve 48~~

2574 ~~Tabelle 10: Tab_Dokv_19 – Operation Restricted Update Document Set 50~~

2575 ~~Tabelle 11: Tab_Dokv_20 – Schnittstelle I_Document_Management_Insurant 54~~

2576 ~~Tabelle 12: Tab_Dokv_21 – Operation Provide And Register Document Set b 55~~

2577 ~~Tabelle 13: Tab_Dokv_22 – Operation Registry Stored Query 57~~

2578 ~~Tabelle 14: Tab_Dokv_23 – Operation Remove Documents 59~~

2579 ~~Tabelle 15: Tab_Dokv_24 – Operation Retrieve Document Set 61~~

2580	Tabelle 16: Tab_Dokv_36 – Schnittstelle I_Document_Management_Insurance	63
2581	Tabelle 17: Tab_Dokv_37 – Operation Provide And Register Document Set b	64
2582	Tabelle 18: Tab_Dokv_25 – Schnittstelle I_Account_Management_Insurant	66
2583	Tabelle 19: Tab_Dokv_26 – Operation Suspend Account	67
2584	Tabelle 20: Tab_Dokv_27 – Operation Resume Account	70
2585	Tabelle 21: Tab_Dokv_28 – Operation Get Audit Events	73
2586	Tabelle 22: Tab_Dokv_300_01 – XACML 2.0 Policy für eine	
2587	Leistungserbringerinstitution (Base Policy)	82
2588	Tabelle 23: Tab_Dokv_29 – Ablauf Operation Hello	89
2589	Tabelle 24: Tab_Dokv_30 – Schnittstelle I_Document_Management_Connect	93
2590	Tabelle 25: Tab_Dokv_31 – Operation OpenContext	93
2591	Tabelle 26: Tab_Dokv_32 – Ablauf der Operation Open Context	94
2592	Tabelle 27: Tab_Dokv_33 – Operation Close Context	96
2593	Tabelle 28: Tab_Dokv_34 – Ablauf Operation OpenContext	96
2594	Tabelle 29: Tab_Dokv_99 – Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	108
2595	Tabelle 30: Tab_Dokv_100 – XACML 2.0 Policy für einen Versicherten (Base Policy) ...	108
2596	Tabelle 31: Tab_Dokv_101 – XACML 2.0 Policy mit erlaubten Operationen für einen	
2597	Versicherten (Permission Policy)	111
2598	Tabelle 32: Tab_Dokv_200 – XACML 2.0 Policy für einen Vertreter (Base Policy)	142
2599	Tabelle 33: Tab_Dokv_201 – XACML 2.0 Policy mit erlaubten Operationen für einen	
2600	Vertreter (Permission Policy)	146
2601	Tabelle 34: Tab_Dokv_301 – XACML 2.0 Policy mit erlaubten Operationen für eine	
2602	Leistungserbringerinstitution zum Zugriff auf Leistungserbringer Dokumente	
2603	(Permission Policy)	174
2604	Tabelle 35: Tab_Dokv_302 – XACML 2.0 Policy mit erlaubten Operationen für eine	
2605	Leistungserbringerinstitution zum Zugriff auf Versicherten und Kostenträger	
2606	Dokumente (Permission Policy)	200
2607	Tabelle 36: Tab_Dokv_400 – XACML 2.0 Policy für einen Kostenträger (Base Policy) ..	224
2608	Tabelle 37: Tab_Dokv_401 – XACML 2.0 Policy mit erlaubten Operationen für einen	
2609	Kostenträger (Permission Policy)	227
2610	Tabelle 1: Tab_Dokv_10 - Kennzeichnung von Optionalitäten	22
2611	Tabelle 2: Tab_Dokv_11 - Übersicht über gruppierte IHE ITI-Akteure und Optionen an den	
2612	Außenschnittstellen der ePA-Dokumentenverwaltung	22
2613	Tabelle 3: Tab_Dokv_12 - Fehlercodes zu Fehlern gemäß Operationsdefinition	29
2614	Tabelle 4: Tab_Dokv_35 - Eingangsparameter für TUC_PKI_018	36
2615	Tabelle 5: Tab_Dokv_13 - Parameter des § 291a-Protokolls	38
2616	Tabelle 6: Tab_Dokv_14 - Schnittstelle I_Document_Management	40
2617	Tabelle 7: Tab_Dokv_16 - Operation Cross-Gateway Query	44
2618	Tabelle 8: Tab_Dokv_17 - Operation Remove Documents	47

2619	Tabelle 9: Tab_Dokv_18 - Operation Cross-Gateway Retrieve.....	48
2620	Tabelle 10: Tab_Dokv_19 - Operation Restricted Update Document Set	50
2621	Tabelle 11: Tab_Dokv_20 - Schnittstelle I_Document_Management_Insurant	54
2622	Tabelle 12: Tab_Dokv_21 - Operation Provide And Register Document Set-b	55
2623	Tabelle 13: Tab_Dokv_22 - Operation Registry Stored Query.....	57
2624	Tabelle 14: Tab_Dokv_23 - Operation RemoveDocuments.....	59
2625	Tabelle 15: Tab_Dokv_24 - Operation Retrieve Document Set	61
2626	Tabelle 16: Tab_Dokv_36 - Schnittstelle I_Document_Management_Insurance	63
2627	Tabelle 17: Tab_Dokv_37 - Operation Provide And Register Document Set-b	64
2628	Tabelle 18: Tab_Dokv_25 - Schnittstelle I_Account_Management_Insurant	66
2629	Tabelle 19: Tab_Dokv_26 - Operation Suspend Account	67
2630	Tabelle 20: Tab_Dokv_27 - Operation Resume Account	70
2631	Tabelle 21: Tab_Dokv_28 - Operation Get Audit Events.....	73
2632	Tabelle 22: Tab_Dokv_300-01 - XACML 2.0 Policy für eine	
2633	Leistungserbringerinstitution (Base Policy)	82
2634	Tabelle 23: Tab_Dokv_29 - Ablauf Operation Hello.....	89
2635	Tabelle 24: Tab_Dokv_30 - Schnittstelle I_Document_Management_Connect	93
2636	Tabelle 25: Tab_Dokv_31 - Operation OpenContext	93
2637	Tabelle 26: Tab_Dokv_32 - Ablauf der Operation Open Context	94
2638	Tabelle 27: Tab_Dokv_33 - Operation Close Context	96
2639	Tabelle 28: Tab_Dokv_34 - Ablauf Operation OpenContext.....	96
2640	Tabelle 29: Tab_Dokv_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies .	108
2641	Tabelle 30: Tab_Dokv_100 - XACML 2.0 Policy für einen Versicherten (Base Policy) ...	108
2642	Tabelle 31: Tab_Dokv_101 - XACML 2.0 Policy mit erlaubten Operationen für einen	
2643	Versicherten (Permission Policy).....	111
2644	Tabelle 32: Tab_Dokv_200 - XACML 2.0 Policy für einen Vertreter (Base Policy).....	142
2645	Tabelle 33: Tab_Dokv_201 - XACML 2.0 Policy mit erlaubten Operationen für einen	
2646	Vertreter (Permission Policy).....	146
2647	Tabelle 34: Tab_Dokv_301 - XACML 2.0 Policy mit erlaubten Operationen für eine	
2648	Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente	
2649	(Permission Policy)	174
2650	Tabelle 35: Tab_Dokv_302 - XACML 2.0 Policy mit erlaubten Operationen für eine	
2651	Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-	
2652	Dokumente (Permission Policy)	200
2653	Tabelle 36: Tab_Dokv_400 - XACML 2.0 Policy für einen Kostenträger (Base Policy) ..	224
2654	Tabelle 37: Tab_Dokv_401 - XACML 2.0 Policy mit erlaubten Operationen für einen	
2655	Kostenträger (Permission Policy)	227
2656		

2657 **7.5 Referenzierte Dokumente**2658 **7.5.1 Dokumente der gematik**

2659 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 2660 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der
 2661 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
 2662 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und
 2663 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
 2664 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer ist in der
 2665 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die
 2666 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

2667 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/deliverables/workinggroup.aspx?wg=basicprofile
[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-SAMLSecurityProfile.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/

2668 8 Anhang B – XACML 2.0-Profile für Policy Documents

2669 Die folgende Notation wird zur Kennzeichnung von Optionalitäten (Opt.) in den XACML
2670 2.0 Policies verwendet:

2671 **Tabelle 29: 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.

2672

2673 Beispiele zu den folgenden XACML 2.0-Profilen der Base Policies können dem
2674 beiliegenden Dokumentenpaket entnommen werden.

2675 8.1 Policy Document für einen Versicherten

2676 8.1.1 Base Policy

2677 **Tabelle 30: Tab_Dokv_100 - XACML 2.0 Policy für einen Versicherten (Base Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:insurant" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.

Target	R	Das Element MUSS leer bleiben.
<!-- Versicherter (repräsentiert durch seine KVNR) -->		
Subjects	R	
Subject	R	
SubjectMatch	R	
@MatchId	R	Der Wert "urn: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 der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
SubjectAttributeDesignator	R	
@AttributeId	R	Der Wert "urn:gematik:subject:subject-id" MUSS gesetzt werden.

	@DataType	R	Der Wert "urn:h17-org:v3#II" MUSS gesetzt werden.
	@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
<!-- KVNR 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 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:h17-org:v3#II" MUSS gesetzt werden.
	PolicySetIdReference	R	
	text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurant" MUSS gesetzt werden.

2678 **8.1.2 Permission Policy**

2679 **Tabelle 31: Tab_Dokv_101 - XACML 2.0 Policy mit erlaubten Operationen für einen**
 2680 **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: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: 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:xac ml: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: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:uuid:e8e3cb2c- e39c-46b9-99e4- c12f57260b83" MUSS gesetzt werden.
			ActionAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis- tryStoredQuery: queryId" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetRelatedDocuments' -->					
			Action	R	
			ActionMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc:xac- ml:1.0: function:anyURI-equal" MUSS gesetzt werden.

			AttributeValue	R	
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
			ActionAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			ActionMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue	R	
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

			text()	R	Der Wert "urn:uuid:d90e5407-b356-4d91-a89f-873917b4b0e6" MUSS gesetzt werden.
			ActionAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByReferenceId' -->					
			Action	R	
			ActionMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue	R	
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

					gesetzt werden.
			ActionAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
			ActionMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue	R	
			@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
			text()	R	Der Wert "urn:uuid:12941a89- e02e-4be5-967c- ce4bfc8fe492" MUSS gesetzt werden.
			ActionAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis- tryStoredQuery:"

							queryId" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByTitle' -->							
		Act ion				R	
		Action Match				R	
			@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue			R	
				@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
			ActionAttributeDesignator			R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:

								action:action-id" MUSS gesetzt werden.
				@Data Type			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
		Action Match					R	
			@MatchId				R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue				R	
				@Data Type			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()			R	Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
			ActionAttributeDesignator				R	
				@AttributeId			R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.

			@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: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:xac ml: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.

2681 **8.2 Policy Document für einen Vertreter**

2682 **8.2.1 Base Policy**

2683 **Tabelle 32: Tab_Dokv_200 - XACML 2.0 Policy für einen Vertreter (Base Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt .	Nutzungsvorgabe
---	-------	-----------------

PolicySet	R	
@PolicySetId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
Target	R	Das Element MUSS leer bleiben.
<!-- Vertreter (repräsentiert durch seine KVNR) -->		
Subjects	R	
Subject	R	
SubjectMatch	R	
@MatchId	R	Der Wert "urn: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 der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
	SubjectAttributeDesignator	R	
	@AttributeId	R	Der Wert "urn:gematik:subject:subject-id" MUSS gesetzt werden.
	@DataType	R	Der Wert "urn:h17-org:v3#II" MUSS gesetzt werden.
	@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
	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: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 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:h17-org:v3#II" MUSS gesetzt werden.
	PolicySetIdReference	R	
	text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-representative" MUSS gesetzt werden.

2684 **8.2.2 Permission Policy**

2685 **Tabelle 33: Tab_Dokv_201 - XACML 2.0 Policy mit erlaubten Operationen für einen**
 2686 **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: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.
<!-- '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: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:xa cml:1.0: action:action-id" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
			ActionMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue	R	
			@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
			text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbc1a9" MUSS gesetzt werden.
			ActionAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regi stryStoredQuery:

					queryId" MUSS gesetzt werden.
				@DataType	R Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAll' -->					
				Action	R
				ActionMatch	R
				@MatchId	R Der Wert "urn:oasis:names:tc: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: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:bab9529a- 4a10-40b3-a01f- f68a615d247a" 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 '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:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue		R	
			@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			text()		R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS gesetzt werden.
			ActionAttributeDesignator		R	
			@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:

								action:action-id" MUSS gesetzt werden.
				@Data Type			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
		Action Match					R	
			@MatchId				R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
			AttributeValue				R	
				@Data Type			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()			R	Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
			ActionAttributeDesignator				R	
				@AttributeId			R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.

			@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.

2687 **8.3 Policy Document für eine Leistungserbringerinstitution**

2688 **8.3.1 Permission Policy zum Zugriff auf Leistungserbringer-**
2689 **Dokumente**

2690

2691 **Tabelle 34: Tab_Dokv_301 - XACML 2.0 Policy mit erlaubten Operationen für eine**
2692 **Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente**
2693 **(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-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

				@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
				@displayName	O	Der Wert "Dokument einer Leistungserbringereinstitution" 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/2

						001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2015: CrossGatewayDocument Provide" 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.
				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	
		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 Leistungserbringerinst

				@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:appc: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/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: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: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:f26abbc- 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/2 001/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/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: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: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: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/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:a7ae438b- 4bc2-4642-93e9- be891f7bb155" 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 '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: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: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: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: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: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:

				@Data Type		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.
			ActionAttribut eDesignator			R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
				@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
		Action Match				R	
			@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
		AttributeValue				R	
				@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				text()		R	Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
			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/2 001/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.

2694 **8.3.2 Permission Policy zum Zugriff auf Versicherten- und**
 2695 **Kostenträger-Dokumente**

2696 **Tabelle 35: Tab_Dokv_302 - XACML 2.0 Policy mit erlaubten Operationen für eine**
 2697 **Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-**
 2698 **Dokumente (Permission Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Optional	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	<p>Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents" MUSS gesetzt werden, sofern dieses Policy Set den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden.</p> <p>Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents" MUSS gesetzt werden, sofern dieses Policy Set den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden.</p>

	@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	<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	Der Wert "Dokument eines Kostenträgers" aus MUSS gesetzt werden, sofern diese Policy den Zugriff auf

						<p>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:h17-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: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: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:f26abbcb-ac74-4422-8a30-edb644bbcl1a9" 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/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: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/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: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: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: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: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/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/20

					01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSetAndContents' -->					
			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: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: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: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: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

			@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: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: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:CrossGatewayRetrieve" 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.
<!-- RemoveDocuments -->							
		Ac tio n				R	
			Actio nMat ch			R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeVal ue	R	
					@Data Type	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2017:Rem oveDocuments" 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.

2699 **8.4 Policy Document für einen Kostenträger**

2700

2701 **8.4.1 Base Policy**

2702 **Tabelle 36: 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: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 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#string" MUSS gesetzt werden.
<!-- KVNR 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 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:h17-org:v3#II" MUSS gesetzt werden.
	PolicySetIdReference	R	
	text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurance" MUSS gesetzt werden.

2703 **8.4.2 Permission Policy**

2704 **Tabelle 37: Tab_Dokv_401 - XACML 2.0 Policy mit erlaubten Operationen für einen**
 2705 **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:appc: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.

2706

2707

ENTWURF