

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation ePA- Dokumentenverwaltung

Version:	1. <del>78</del> .0
Revision:	<a href="#">328297369582</a>
Stand:	<del>19</del> -02. <a href="#">06</a> .2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_Dokumentenverwaltung

## Dokumentinformationen

### Änderungen zur Vorversion

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

### Dokumentenhistorie

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

1.4.1	26.06.20		Einarbeitung Änderungsliste P21.3	gematik
1.5.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
1.6.0	12.10.20		Einarbeitung der Scope-Themen aus R4.0.1, PDSG-Änderungen	gematik
1.7.0	19.02.21		Einarbeitung Änderungsliste P22.5	gematik
<a href="#">1.8.0</a>	<a href="#">02.06.21</a>		<a href="#">Einarbeitung Änderungsliste ePA Maintenance 21.1</a>	<a href="#">gematik</a>

## Inhaltsverzeichnis

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

4.2.3.1 Provide X-User Assertion [ITI-40] .....	28
4.2.3.2 Provide and Register Document Set-b [ITI-41] .....	29
4.2.3.3 Remove Documents [ITI-86] .....	30
4.2.3.4 Remove Metadata [ITI-62] .....	31
<b>4.3 Fehlerbehandlung in Schnittstellenoperationen .....</b>	<b>32</b>
<b>4.4 Vertrauenswürdige Ausführungsumgebung .....</b>	<b>33</b>
4.4.1 Verarbeitungskontext .....	34
4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld .....	35
4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes .....	36
4.4.4 Parallele Zugriffe .....	37
4.4.5 Konsistenz der Akte, Logging und Monitoring .....	37
4.4.6 Client-Verbindungen zum Verarbeitungskontext .....	37
<b>4.5 Anforderungen zur sicherheitstechnischen Validierung .....</b>	<b>39</b>
<b>4.6 Protokollierung .....</b>	<b>41</b>
4.6.1 Protokollierung von Berechtigungen .....	47
<b>5 Funktionsmerkmale .....</b>	<b>53</b>
<b>5.1 Dokumentenverwaltung .....</b>	<b>53</b>
5.1.1 Schnittstelle I_Document_Management .....	53
5.1.1.1 Operation I_Document_Management::CrossGatewayDocumentProvide ..	54
5.1.1.1.1 Umsetzung .....	55
5.1.1.2 Operation I_Document_Management::CrossGatewayQuery .....	57
5.1.1.2.1 Umsetzung .....	58
5.1.1.3 Operation I_Document_Management::RemoveDocuments (abgekündigt) ..	60
5.1.1.3.1 Umsetzung .....	61
5.1.1.4 Operation I_Document_Management::RemoveMetadata .....	61
5.1.1.4.1 Umsetzung .....	63
5.1.1.5 Operation I_Document_Management::CrossGatewayRetrieve .....	63
5.1.1.5.1 Umsetzung .....	64
5.1.1.6 Operation I_Document_Management::RestrictedUpdateDocumentSet ...	65
5.1.1.6.1 Umsetzung .....	66
5.1.2 Schnittstelle I_Document_Management_Insurant .....	67
5.1.2.1 Operation	
I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b .....	69
5.1.2.1.1 Umsetzung .....	71
5.1.2.2 Operation I_Document_Management_Insurant::RegistryStoredQuery ...	71
5.1.2.2.1 Umsetzung .....	73
5.1.2.3 Operation I_Document_Management_Insurant::RemoveMetadata .....	77
5.1.2.3.1 Umsetzung .....	78
5.1.2.4 Operation I_Document_Management_Insurant::RetrieveDocumentSet ...	79
5.1.2.4.1 Umsetzung .....	80
5.1.2.5 Operation	
I_Document_Management_Insurant::RestrictedUpdateDocumentSet .....	81
5.1.2.5.1 Umsetzung .....	83
5.1.3 Schnittstelle I_Document_Management_Insurance .....	84

5.1.3.1 Operation	
<i>I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b</i> .....	85
5.1.3.1.1 Umsetzung .....	87
5.1.4 Anforderungen an Sammlungstypen .....	88
<b>5.2 Aktenkontoverwaltung .....</b>	<b>89</b>
5.2.1 Schnittstelle <i>I_Account_Management_Insurant</i> .....	89
5.2.1.1 Operation <i>I_Account_Management_Insurant::SuspendAccount</i> .....	90
5.2.1.1.1 Umsetzung .....	91
5.2.1.2 Operation <i>I_Account_Management_Insurant::ResumeAccount</i> .....	93
5.2.1.2.1 Umsetzung .....	94
5.2.1.3 Operation <i>I_Account_Management_Insurant::GetAuditEvents</i> .....	97
5.2.1.3.1 Umsetzung .....	99
5.2.1.4 Operation <i>I_Account_Management_Insurant::GetSignedAuditEvents</i> .....	99
5.2.1.4.1 Umsetzung .....	100
<b>5.3 Umschlüsselung .....</b>	<b>101</b>
5.3.1 Übergreifende Anforderungen .....	102
5.3.2 Schnittstelle <i>I_Key_Management_Insurant</i> .....	106
5.3.2.1 <i>I_Key_Management_Insurant::StartKeyChange()</i> .....	106
5.3.2.1.1 Umsetzung .....	108
5.3.2.2 <i>I_Key_Management_Insurant::GetAllDocumentKeys()</i> .....	109
5.3.2.2.1 Umsetzung .....	111
5.3.2.3 Operation <i>I_Key_Management_Insurant::PutAllDocumentKeys()</i> .....	112
5.3.2.3.1 Umsetzung .....	113
5.3.2.4 Operation <i>I_Key_Management_Insurant::FinishKeyChange()</i> .....	114
5.3.2.4.1 Umsetzung .....	115
5.3.2.5 Protokollierung .....	116
<b>5.4 Zugriffskontrolle.....</b>	<b>117</b>
5.4.1 Grob-, mittel- und feingranulare Berechtigungen .....	117
5.4.2 Berufsgruppenspezifische Einschränkungen.....	118
5.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln.....	119
5.4.4 Vergabe von Zugriffsregeln.....	120
5.4.5 Funktionsprinzip Policy Administration .....	121
5.4.6 Anforderungen an die Zugriffskontrollprüfung.....	124
5.4.6.1 <i>Erstmaliges Öffnen eines Verarbeitungskontextes</i> .....	132
5.4.6.2 <i>Berechtigung für einen Versicherten</i> .....	133
5.4.6.3 <i>Berechtigung für einen Vertreter</i> .....	134
5.4.6.4 <i>Berechtigung für eine Leistungserbringerinstitution</i> .....	134
5.4.6.5 <i>Berechtigung für einen Kostenträger</i> .....	134
5.4.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4 .....	135
<b>5.5 Vertrauenswürdige Ausführung.....</b>	<b>137</b>
5.5.1 Schnittstelle <i>I_Document_Management_Connect</i> .....	137
5.5.1.1 Operation <i>I_Document_Management_Connect::OpenContext</i> .....	143
5.5.1.1.1 Umsetzung .....	144
5.5.1.2 Operation <i>I_Document_Management_Connect::CloseContext</i> .....	145
5.5.1.2.1 Umsetzung .....	146
5.5.2 Hardware-Merkmale .....	147
<b>5.6 Statische Akteninhalte.....</b>	<b>147</b>

<b>6 Informationsmodelle .....</b>	<b>149</b>
<b>7 Anhang A – Verzeichnisse .....</b>	<b>150</b>
7.1 Abkürzungen .....	150
7.2 Glossar .....	152
7.3 Abbildungsverzeichnis .....	152
7.4 Tabellenverzeichnis .....	152
7.5 Referenzierte Dokumente .....	156
7.5.1 Dokumente der gematik .....	156
7.5.2 Weitere Dokumente .....	157
<b>8 Anhang B – XACML 2.0 Profile für Policy Documents (für Upgrade von ePA 3.1.3) .....</b>	<b>161</b>
<b>8.1 Policy Document für einen Versicherten .....</b>	<b>161</b>
8.1.1 Base Policy .....	161
8.1.2 Permission Policy .....	164
<b>8.2 Policy Document für einen Vertreter .....</b>	<b>195</b>
8.2.1 Base Policy .....	195
8.2.2 Permission Policy .....	199
<b>8.3 Policy Document für eine Leistungserbringereinstitution .....</b>	<b>227</b>
8.3.1 Base Policy zum Zugriff auf Leistungserbringer Dokumente .....	227
8.3.2 Permission Policy zum Zugriff auf Leistungserbringer Dokumente .....	232
8.3.3 Permission Policy zum Zugriff auf Versicherten und Kostenträger Dokumente .....	258
<b>8.4 Policy Document für einen Kostenträger .....</b>	<b>282</b>
8.4.1 Base Policy .....	282
8.4.2 Permission Policy .....	285
<b>9 Anhang C – XACML 2.0 Profile für Policy Documents .....</b>	<b>289</b>
<b>9.1 Policy Document für einen Versicherten .....</b>	<b>289</b>
<b>9.2 Policy Document für einen Vertreter .....</b>	<b>292</b>
<b>9.3 Policy Document für eine Leistungserbringereinstitution .....</b>	<b>295</b>
<b>9.4 Policy Document für einen Kostenträger .....</b>	<b>315</b>
<b>9.5 Statische Permission Policies .....</b>	<b>319</b>
9.5.1 Grobgranulare Berechtigung: Stufe Normal .....	319
9.5.2 Grobgranulare Berechtigung: Stufe Erweitert .....	319
9.5.3 Mittelgranulare Berechtigung: Kategorie "care" .....	320
9.5.4 Mittelgranulare Berechtigung: Kategorie "childsrecord" .....	320
9.5.5 Mittelgranulare Berechtigung: Kategorie "dentalrecord" .....	321
9.5.6 Mittelgranulare Berechtigung: Kategorie "eab" .....	322
9.5.7 Mittelgranulare Berechtigung: Kategorie "eau" .....	322
9.5.8 Mittelgranulare Berechtigung: Kategorie "ega" .....	323
9.5.9 Mittelgranulare Berechtigung: Kategorie "emp" .....	323
9.5.10 Mittelgranulare Berechtigung: Kategorie "mothersrecord" .....	324
9.5.11 Mittelgranulare Berechtigung: Kategorie "nfd" .....	325
9.5.12 Mittelgranulare Berechtigung: Kategorie "other" .....	326

9.5.13 Mittelgranulare Berechtigung: Kategorie "patientdoc" .....	327
9.5.14 Mittelgranulare Berechtigung: Kategorie "prescription" .....	327
9.5.15 Mittelgranulare Berechtigung: Kategorie "receipt" .....	328
9.5.16 Mittelgranulare Berechtigung: Kategorie "vaccination" .....	329
9.5.17 Mittelgranulare Berechtigung: Kategorie "practitioner" .....	329
9.5.18 Mittelgranulare Berechtigung: Kategorie "hospital" .....	330
9.5.19 Mittelgranulare Berechtigung: Kategorie "laboratory" .....	331
9.5.20 Mittelgranulare Berechtigung: Kategorie "physiotherapy" .....	331
9.5.21 Mittelgranulare Berechtigung: Kategorie "psychotherapy" .....	332
9.5.22 Mittelgranulare Berechtigung: Kategorie "dermatology" .....	332
9.5.23 Mittelgranulare Berechtigung: Kategorie "gynaecology_urology" .....	333
9.5.24 Mittelgranulare Berechtigung: Kategorie "dentistry_oms" .....	334
9.5.25 Mittelgranulare Berechtigung: Kategorie "other_medical" .....	334
9.5.26 Mittelgranulare Berechtigung: Kategorie "other_non_medical" .....	335
<b>1 Einführung .....</b>	<b>12</b>
<b>1.1 Zielsetzung .....</b>	<b>12</b>
<b>1.2 Zielgruppe .....</b>	<b>12</b>
<b>1.3 Geltungsbereich .....</b>	<b>12</b>
<b>1.4 Abgrenzungen .....</b>	<b>12</b>
<b>1.5 Methodik .....</b>	<b>13</b>
<b>2 Systemkontext.....</b>	<b>14</b>
<b>3 Zerlegung der Komponente.....</b>	<b>15</b>
<b>4 Übergreifende Festlegungen .....</b>	<b>16</b>
<b>4.1 Namensräume .....</b>	<b>16</b>
<b>4.2 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von Dokumenten.....</b>	<b>17</b>
4.2.1 Anforderungen an IHE ITI-Akteure .....	17
4.2.1.1 APPC Content Consumer.....	19
4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren .....	19
4.2.1.1.2 Optionen des IHE ITI-Akteurs.....	19
4.2.1.2 RMU Update Responder.....	20
4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren .....	20
4.2.1.2.2 Optionen des IHE ITI-Akteurs.....	20
4.2.1.3 XCA Responding Gateway.....	21
4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren .....	21
4.2.1.3.2 Optionen des IHE ITI-Akteurs.....	21
4.2.1.4 XCDR Responding Gateway.....	21
4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren .....	21
4.2.1.4.2 Optionen des IHE ITI-Akteurs.....	22
4.2.1.5 XDS Document Registry .....	22
4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren .....	22
4.2.1.5.2 Optionen des IHE ITI-Akteurs.....	22

4.2.1.6 XDS Document Repository .....	23
4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren .....	23
4.2.1.6.2 Optionen des IHE ITI-Akteurs .....	23
4.2.1.7 XUA X-Service Provider .....	23
4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren .....	23
4.2.1.7.2 Optionen des IHE ITI-Akteurs .....	24
4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen.....	24
4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen .....	28
4.2.3.1 Provide X-User Assertion [ITI-40] .....	28
4.2.3.2 Provide and Register Document Set-b [ITI-41] .....	29
4.2.3.3 Remove Documents [ITI-86].....	30
4.2.3.4 Remove Metadata [ITI-62] .....	31
<b>4.3 Fehlerbehandlung in Schnittstellenoperationen .....</b>	<b>32</b>
<b>4.4 Vertrauenswürdige Ausführungsumgebung .....</b>	<b>33</b>
4.4.1 Verarbeitungskontext .....	34
4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld .....	35
4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes .....	36
4.4.4 Parallele Zugriffe.....	37
4.4.5 Konsistenz der Akte, Logging und Monitoring .....	37
4.4.6 Client-Verbindungen zum Verarbeitungskontext .....	37
<b>4.5 Anforderungen zur sicherheitstechnischen Validierung.....</b>	<b>39</b>
<b>4.6 Protokollierung.....</b>	<b>41</b>
4.6.1 Protokollierung von Berechtigungen.....	47
<b>5 Funktionsmerkmale .....</b>	<b>53</b>
<b>5.1 Dokumentenverwaltung .....</b>	<b>53</b>
5.1.1 Schnittstelle I Document Management.....	53
5.1.1.1 Operation I Document Management::CrossGatewayDocumentProvide ..	54
5.1.1.1.1 Umsetzung .....	55
5.1.1.2 Operation I Document Management::CrossGatewayQuery .....	57
5.1.1.2.1 Umsetzung .....	58
5.1.1.3 Operation I Document Management::RemoveDocuments (abgekündigt)	60
5.1.1.3.1 Umsetzung .....	61
5.1.1.4 Operation I Document Management::RemoveMetadata .....	61
5.1.1.4.1 Umsetzung .....	63
5.1.1.5 Operation I Document Management::CrossGatewayRetrieve .....	63
5.1.1.5.1 Umsetzung .....	64
5.1.1.6 Operation I Document Management::RestrictedUpdateDocumentSet (abgekündigt).....	65
5.1.1.6.1 Umsetzung .....	66
5.1.2 Schnittstelle I Document Management Insurant .....	67
5.1.2.1 Operation I Document Management Insurant::ProvideAndRegisterDocumentSet-b.....	69
5.1.2.1.1 Umsetzung .....	71
5.1.2.2 Operation I Document Management Insurant::RegistryStoredQuery....	71
5.1.2.2.1 Umsetzung .....	73

5.1.2.3 Operation I Document Management Insurant::RemoveDocuments (abgekündigt).....	75
5.1.2.4 Operation I Document Management Insurant::RemoveMetadata.....	77
5.1.2.4.1 Umsetzung .....	78
5.1.2.5 Operation I Document Management Insurant::RetrieveDocumentSet...	79
5.1.2.5.1 Umsetzung .....	80
5.1.2.6 Operation I Document Management Insurant::RestrictedUpdateDocumentSet.....	81
5.1.2.6.1 Umsetzung .....	83
5.1.3 Schnittstelle I Document Management Insurance .....	84
5.1.3.1 Operation I Document Management Insurance::ProvideAndRegisterDocumentSet-b.....	85
5.1.3.1.1 Umsetzung .....	87
5.1.4 Anforderungen an Sammlungstypen .....	88
<b>5.2 Aktenkontoverwaltung .....</b>	<b>89</b>
5.2.1 Schnittstelle I Account Management Insurant .....	89
5.2.1.1 Operation I Account Management Insurant::SuspendAccount.....	90
5.2.1.1.1 Umsetzung .....	91
5.2.1.2 Operation I Account Management Insurant::ResumeAccount.....	93
5.2.1.2.1 Umsetzung .....	94
5.2.1.3 Operation I Account Management Insurant::GetAuditEvents .....	97
5.2.1.3.1 Umsetzung .....	99
5.2.1.4 Operation I Account Management Insurant::GetSignedAuditEvents .....	99
5.2.1.4.1 Umsetzung .....	100
<b>5.3 Umschlüsselung .....</b>	<b>101</b>
5.3.1 Übergreifende Anforderungen .....	102
5.3.2 Schnittstelle I Key Management Insurant .....	106
5.3.2.1 I Key Management Insurant::StartKeyChange().....	106
5.3.2.1.1 Umsetzung .....	108
5.3.2.2 I Key Management Insurant::GetAllDocumentKeys().....	109
5.3.2.2.1 Umsetzung .....	111
5.3.2.3 Operation I Key Management Insurant::PutAllDocumentKeys().....	112
5.3.2.3.1 Umsetzung .....	113
5.3.2.4 Operation I Key Management Insurant::FinishKeyChange() .....	114
5.3.2.4.1 Umsetzung .....	115
5.3.2.5 Protokollierung.....	116
<b>5.4 Zugriffskontrolle.....</b>	<b>117</b>
5.4.1 Vergabe von Zugriffsrechten und Policy Administration.....	120
5.4.2 Anforderungen an die Zugriffskontrollprüfung.....	130
5.4.2.1 Erstmaliges Öffnen eines Verarbeitungskontextes .....	132
5.4.2.2 Berechtigung für einen Vertreter.....	133
5.4.2.3 Berechtigung für eine Leistungserbringerinstitution .....	134
5.4.2.4 Berechtigung für einen Kostenträger.....	134
5.4.3 Upgrade von ePA Release 3.1.3 auf ePA Release 4 .....	135
5.4.4 Simulierte Berechtigung.....	137
<b>5.5 Vertrauenswürdige Ausführung.....</b>	<b>137</b>
5.5.1 Schnittstelle I Document Management Connect.....	137

5.5.1.1 Operation I Document Management Connect::OpenContext .....	143
5.5.1.1.1 Umsetzung .....	144
5.5.1.2 Operation I Document Management Connect::CloseContext .....	145
5.5.1.2.1 Umsetzung .....	146
5.5.2 Hardware-Merkmale .....	147
<b>5.6 Statische Akteninhalte .....</b>	<b>147</b>
<b>6 Informationsmodelle .....</b>	<b>149</b>
<b>7 Anhang A – Verzeichnisse .....</b>	<b>150</b>
7.1 Abkürzungen .....	150
7.2 Glossar .....	152
7.3 Abbildungsverzeichnis .....	152
7.4 Tabellenverzeichnis .....	152
7.5 Referenzierte Dokumente .....	156
7.5.1 Dokumente der gematik .....	156
7.5.2 Weitere Dokumente .....	157
<b>8 Anhang B – XACML 2.0-Profile für Policy Documents (für Upgrade von ePA 3.1.3) .....</b>	<b>161</b>
8.1 Policy Document für einen Versicherten .....	161
8.1.1 Base Policy .....	161
8.1.2 Permission Policy .....	164
8.2 Policy Document für einen Vertreter .....	195
8.2.1 Base Policy .....	195
8.2.2 Permission Policy .....	199
8.3 Policy Document für eine Leistungserbringereinstitution .....	227
8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente .....	227
8.3.2 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente .....	232
8.3.3 Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente .....	258
8.4 Policy Document für einen Kostenträger .....	282
8.4.1 Base Policy .....	282
8.4.2 Permission Policy .....	285

---

## 1 Einführung

---

### 1.1 Zielsetzung

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

### 1.2 Zielgruppe

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

### 1.3 Geltungsbereich

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

#### Schutzrechts- /Patentrechtshinweis

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

### 1.4 Abgrenzungen

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

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

## 1.5 Methodik

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

### **<AFO-ID> - <Titel der Afo>**

Text / Beschreibung

[<=]

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

---

## 2 Systemkontext

---

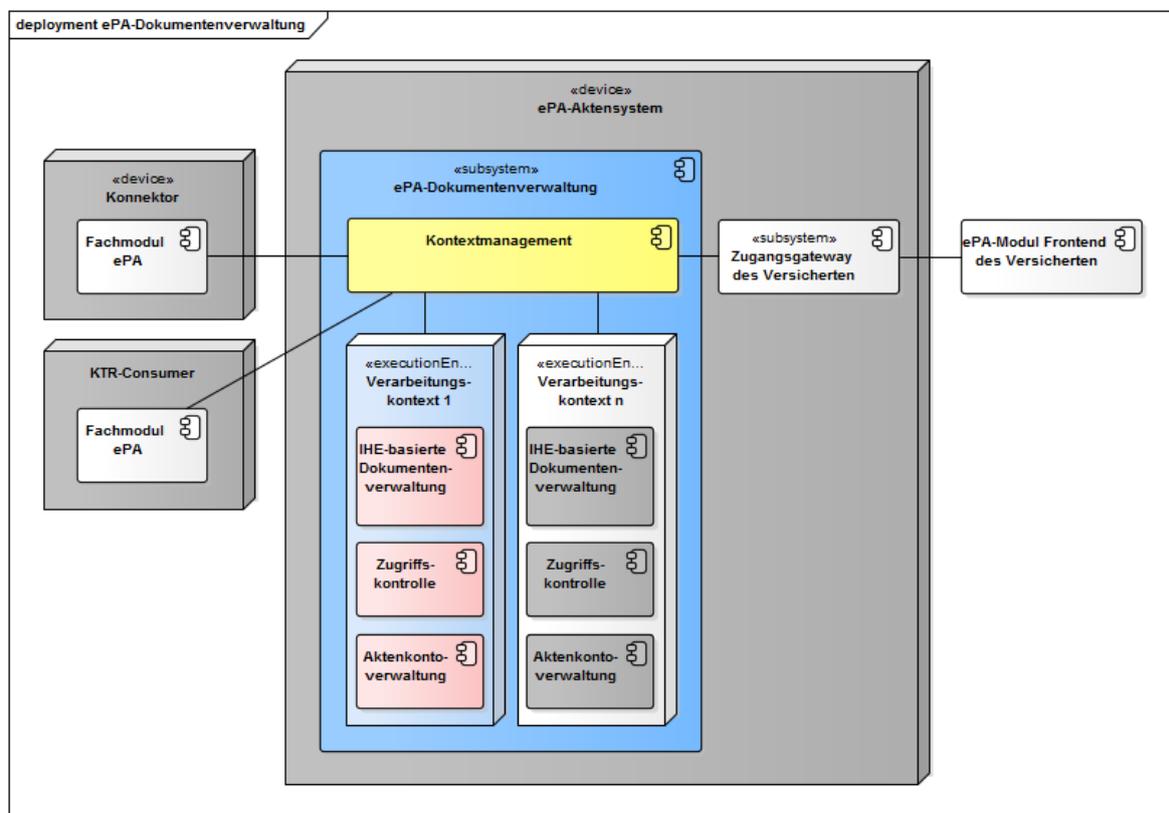
Die Komponente ePA-Dokumentenverwaltung des Produkttyps ePA-Aktensystem [gemSpec\_Aktensystem] dient dem sicheren Speichern und Auffinden von Dokumenten des Versicherten aus seiner persönlichen Akte durch berechnigte Nutzer. Diese sind der Versicherte selbst oder von ihm benannte Vertreter, Leistungserbringerinstitutionen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

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

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

### 3 Zerlegung der Komponente

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



**Abbildung 1: Komponentenzersetzung ePA-Dokumentenverwaltung**

## 4 Übergreifende Festlegungen

### **A\_15033 - Komponente ePA-Dokumentenverwaltung – Verwendung des SAML Token Profile 1.1 für Web Services Security bei SAML 2.0 Assertions**

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

### **A\_15035 - Komponente ePA-Dokumentenverwaltung – Verwendung von SOAP Message Security 1.1**

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

### **A\_15034 - Komponente ePA-Dokumentenverwaltung – Unterstützung von Profilen der Web Services Interoperability Organization (WS-I)**

Die Komponente ePA-Dokumentenverwaltung MUSS das WS-I Basic Profile V2.0 [WSIBP], das WS-I Basic Security Profile Version V1.1 [WSIBSP] sowie das WS-I Attachment Profile V1.0 [WSIAP] für die Kommunikation über Web Services berücksichtigen. [ <= ]

#### 4.1 Namensräume

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

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

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

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

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

*Hinweis: Alle spezifizierten Anforderungen der IHE ITI-Akteure in Abschnitt 4.2.1 definieren das zu implementierende Verhalten an den Außenschnittstellen I\_Document\_Management, I\_Document\_Management\_Insurance sowie I\_Document\_Management\_Insurant. Dies schließt keine zusätzlich implementierten IHE-Funktionalitäten innerhalb der ePA-Dokumentenverwaltung aus.*

### A\_17826 - Komponente ePA-Dokumentenverwaltung – Außenverhalten der IHE ITI-Implementierung

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

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

### 4.2.1 Anforderungen an IHE ITI-Akteure

#### A\_13805 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XCDR Responding Gateway

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

#### A\_13806 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XDS Document Registry

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

**A\_14727 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XDS Document Repository**

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

**A\_13807 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XCA Responding Gateway**

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

Die § 291a-konforme Protokollierung von Zugriffen erfolgt mit Mechanismen außerhalb des IHE ITI-TF. Eine technische Protokollierung via ATNA kann gemäß der Anforderung A\_17826 dennoch erfolgen.

**A\_13809 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs ATNA Audit Record Repository**

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

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

**A\_17166 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung der IHE ITI-Akteure ATNA Secure Node sowie ATNA Secure Application für Node Authentication**

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

[ <= ]

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

**A\_14654 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs CT Time Client**

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

**A\_14655-01 - Komponente ePA-Dokumentenverwaltung – Zeitsynchronisation über Zeitdienst in der TI**

Die Komponente ePA-Dokumentenverwaltung MUSS die Systemzeit über den Zeitdienst in der TI gemäß [gemSpec\_Net#6.2] synchronisieren. [ <= ]

**A\_14597 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XUA X-Service Provider**

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

**A\_14665 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Document Source**

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

**A\_14667 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Integrated Document Source/Repository**

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

[<=]

**A\_14668 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Document Consumer**

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

**A\_14666 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Patient Identity Source**

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

[<=]

**A\_14669 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS On-Demand Document Source**

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

[<=]

**A\_14782 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs APPC Content Consumer**

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

**A\_14950 - Komponente ePA-Dokumentenverwaltung – Keine Angabe einer Fehlerlokalisierung im RegistryError-Element**

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

[<=]

**A\_15081 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs RMU Update Responder**

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

#### 4.2.1.1 APPC Content Consumer

##### 4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren

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

##### 4.2.1.1.2 Optionen des IHE ITI-Akteurs

**A\_14787 - Komponente ePA-Dokumentenverwaltung – APPC Content Consumer ohne "View Option"-Option**

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

**A\_14788 - Komponente ePA-Dokumentenverwaltung – APPC Content Consumer mit "Structured Policy Processing Option"-Option**

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

**4.2.1.2 RMU Update Responder***4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren***A\_15093-01 - Komponente ePA-Dokumentenverwaltung – Gruppierung RMU Update Responder mit Document Registry und X-Service Provider**

~~A\_15093 – Komponente ePA-Dokumentenverwaltung – Gruppierung RMU Update Responder mit XCA Responding Gateway und X-Service Provider~~ Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS mit dem ~~XCA~~XDS-Akteur "~~Responding Gateway~~Document Registry" gemäß [IHE-ITI-RMU] sowie mit dem XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions verarbeiten.

[ $\leq$ ]

**A\_17571 - Komponente ePA-Dokumentenverwaltung – Gruppierung RMU Update Responder mit APPC Content Consumer**

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

*4.2.1.2.2 Optionen des IHE ITI-Akteurs***A\_15094 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "Forward Update"-Option**

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

[ $\leq$ ]

**~~A\_15095 – Komponente ePA-Dokumentenverwaltung – RMU Update Responder mit "XCA Persistence"-Option~~**

~~Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS die Option "XCA Persistence" unterstützen.~~

~~[ $\leq$ ]~~

**A\_15095-02 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "XCA Persistence"-Option**

~~A\_15096 – Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "XDS Persistence"-Option~~ Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF NICHT die Option "~~XDS~~XCA Persistence" unterstützen.

[ $\leq$ ]

**A\_15096-02 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder mit "XDS Persistence"-Option**

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

**A\_15097 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "XDS Version Persistence"-Option**

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

[ $\leq$ ]

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

### 4.2.1.3 XCA Responding Gateway

#### 4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren

##### **A\_14598 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit X-Service Provider**

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

##### **A\_14725 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit XDS Document Registry**

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

##### **A\_14726 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit XDS Document Repository**

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

##### **A\_14784 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit APPC Content Consumer**

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

#### 4.2.1.3.2 Optionen des IHE ITI-Akteurs

##### **A\_13819 - Komponente ePA-Dokumentenverwaltung – XCA Responding Gateway ohne "On-Demand Documents"-Option**

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

##### **A\_13820 - Komponente ePA-Dokumentenverwaltung – XCA Responding Gateway ohne "Persistence of Retrieved Documents"-Option**

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

### 4.2.1.4 XCDR Responding Gateway

#### 4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren

##### **A\_13648 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit X-Service Provider**

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

**A\_14723 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit XDS Document Registry**

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

**A\_14724 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit XDS Document Repository**

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

**A\_14783 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit APPC Content Consumer**

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

*4.2.1.4.2 Optionen des IHE ITI-Akteurs***A\_13650 - Komponente ePA-Dokumentenverwaltung – XCDR Responding Gateway ohne "Basic Patient Privacy Enforcement"-Option**

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

**4.2.1.5 XDS Document Registry***4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren***A\_14599 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS Document Registry mit X-Service Provider**

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

**A\_14785 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS Document Registry mit APPC Content Consumer**

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

*4.2.1.5.2 Optionen des IHE ITI-Akteurs***A\_14637 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "Asynchronous Web Services Exchange"-Option**

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

**A\_14638 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry mit "Reference ID"-Option**

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

**A\_14639 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "Patient Identity Feed"-Option**

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

[<=]

**A\_14640 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "Patient Identity Feed HL7v3"-Option**

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

[<=]

**A\_14641 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "On-Demand Documents"-Option**

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

[<=]

**A\_14642 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "Document Metadata Update"-Option**

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

#### 4.2.1.6 XDS Document Repository

##### 4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren

**A\_14600 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS Document Repository mit X-Service Provider**

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

**A\_14786 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS Document Repository mit APPC Content Consumer**

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

##### 4.2.1.6.2 Optionen des IHE ITI-Akteurs

**A\_14636 - Komponente ePA-Dokumentenverwaltung – XDS Document Repository ohne "Asynchronous Web Services Exchange"-Option**

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

#### 4.2.1.7 XUA X-Service Provider

##### 4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren

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

4.2.1.7.2 Optionen des IHE ITI-Akteurs

**A\_14612 - Komponente ePA-Dokumentenverwaltung – XUA X-Service Provider ohne "Subject-Role"-Option**

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

**A\_14613 - Komponente ePA-Dokumentenverwaltung – XUA X-Service Provider ohne "Authz-Consent"-Option**

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

**A\_14614 - Komponente ePA-Dokumentenverwaltung – XUA X-Service Provider ohne "PurposeOfUse"-Option**

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

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

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

**Tabelle 1: Tab\_Dokv\_10 - Kennzeichnung von Optionalitäten**

Code	Bedeutung
R	Required - Mit "R" gekennzeichnete IHE ITI-Akteure oder Optionen MÜSSEN implementiert oder gruppiert werden.
X	Mit "X" gekennzeichnete IHE ITI-Akteure oder Optionen DÜRFEN NICHT implementiert oder gruppiert werden.

**Tabelle 2: Tab\_Dokv\_11 - Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung**

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

		XCA Responding Gateway	R		
		XCDR Responding Gateway	R		
		XDS Document Registry	R		
		XDS Document Repository	R		
ATNA Audit Record Repository	X				
CT Time Client	X				
RMU Update Responder	R			Forward Update	X
				XCA Persistence	<del>R</del> X
				XDS Persistence	<del>X</del> R
				XDS Version Persistence	X
		APPC Content Consumer	R		
		<a href="#">XCA Responding Gateway Document Registry</a>	R		
		X-Service Provider	R		
XCDR Responding	R			Basic Patient Privacy Enforcement	X

Gateway		APPC Content Consumer	R		
		ATNA Secure Node oder Secure Application für Node Authentication	X		
		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		
		<del>RMU Update Responder</del>	<del>R</del>		
		XDS Document Registry	R		
		XDS Document Repository	R		
		XUA X-Service Provider	R		
XDS Document Consumer	X				
	R			Asynchronous Web Services Exchange	X

XDS Document Registry			Document Metadata Update	X
			On-Demand Documents	X
			Patient Identity Feed	X
			Patient Identity Feed HL7v3	X
			Reference ID	R
		APPC Content Consumer	R	
		ATNA Secure Node oder Secure Application für Node Authentication	X	
		X-Service Provider	R	
XDS Document Repository	R		Asynchronous Web Services Exchange	X
			APPC Content Consumer	R
			ATNA Secure Node oder Secure Application für Node Authentication	X
			X-Service Provider	R
XDS Document Source	X			
XDS Integrated Document Source / Repository	X			
XDS On-Demand Document Source	X			

XDS Patient Identity Source	X				
XUA X-Service Provider	R		Subject-Role	X	
			Authz-Consent	X	
			PurposeOfUse	X	
		XCDR Responding Gateway	R		
		RMU Update Responder	R		
		XCA Responding Gateway	R		
		XDS Document Registry	R		
XDS Document Repository	R				

### 4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen

#### A\_17832 - Komponente ePA-Dokumentenverwaltung – Unterstützung MTOM/XOP

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

#### 4.2.3.1 Provide X-User Assertion [ITI-40]

##### [A\\_14915-04A\\_14915-03](#) - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide X-User Assertion

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

- I\_Document\_Management::CrossGatewayDocumentProvide
- I\_Document\_Management::CrossGatewayQuery
- I\_Document\_Management::RemoveDocuments
- I\_Document\_Management::RemoveMetadata
- I\_Document\_Management::CrossGatewayRetrieve
- I\_Document\_Management::RestrictedUpdateDocumentSet
- I\_Document\_Management\_Insurance::ProvideAndRegisterDocumentSet-b
- I\_Document\_Management\_Insurant::RestrictedUpdateDocumentSet

- I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b
- I\_Document\_Management\_Insurant::RegistryStoredQuery
- I\_Document\_Management\_Insurant::RemoveDocuments
- I\_Document\_Management\_Insurant::RemoveMetadata
- I\_Document\_Management\_Insurant::RetrieveDocumentSet

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

#### **A\_14594-01A\_14594 - Komponente ePA-Dokumentenverwaltung – Validierung der Authentication Assertion**

Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" MUSS die X-User Assertion (Authentication Assertion) gemäß der Anforderung A\_13690 prüfen und die eingehende Nachricht mit Fehlercodes nach [WSS#12] sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls diese X-User Assertion nicht gültig ist. [ $\leq$ ]

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

##### **A\_14549-01A\_14549 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Provide and Register Document Set-b**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS ~~für die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden~~ Ausführung dieser Operation prüfen, ob für den zugreifenden Nutzer ein gültiges Policy Documents (Advanced Patient Privacy Consents) entsprechend Document vorliegt und ob er gemäß der Anforderung Rollenprüfung in A\_19303 schreibberechtigt ist. Liegt kein Policy Document vor oder ist er nicht schreibberechtigt, MUSS die Nachricht mit dem SOAP-Fault ACCESS\_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [ $\leq$ 14822 durchsetzen, bevor ein Registry-Datenobjekt registriert und ein Dokument gespeichert wird.

[ $\leq$ ]

##### **A\_15162-03A\_15162-02 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung bei Angabe von Document Entry Relationships in Metadaten**

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

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

[ $\leq$ ]

### **A\_14937 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße prüfen**

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

### **A\_14938-01A\_14938 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung der Metadaten aus ITI Document Sharing-Profilen durch XDS-Akteur "Document Repository"**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die `SubmissionSet-` sowie die `DocumentEntry-Metadaten` der eingehenden ~~Nachricht~~[Nachricht vor](#) einer Zugriffskontrolle gemäß Konformität zu den Nutzungsvorgaben in [gemSpec\_DM\_ePA#A\_14760] prüfen. Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError` quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind- [oder eine nachgelagerte Zugriffskontrollprüfung negativ ausfällt.](#) Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError-`Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht. [`<=`]

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

#### **A\_21186 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen der Metadaten bei Löschung von Dokumenten**

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

#### **A\_21187 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Remove Documents**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor ein Dokument oder mehrere Dokumente gelöscht werden. Bei einem Löschen von mehreren Dokumenten durch das ePA-Fachmodul können einzelne Dokumente durch den zwischenzeitlichen Entzug einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für das Löschen berechtigt sein. Widerspricht ein zu löschendes Dokument einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum betreffenden Dokument einen `XDSDocumentUniqueIdError`-Fehlercode enthalten und der Wert 4 des `EventOutcomeIndicators` im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein zu löschendes Dokument nicht mehr verfügbar, MUSS gemäß IHE TF ITI der Fehlercode `XDSDocumentUniqueIdError` zurückgegeben werden. [`<=`]

#### **A\_21245-02A\_21245 - Komponente ePA-Dokumentenverwaltung – Policy-Aktualisierung für Remove Documents**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS beim Löschen eines Dokuments über die Operation Remove Documents die `DocumentEntry.uniqueIdentryUUID` des Dokuments aus der Whitelist aller LEI-Policy-Dokumente (gemäß 9.3) löschen, welche die entsprechende `DocumentEntry.uniqueIdentryUUID` referenzieren.

[<=]

#### **4.2.3.4 Remove Metadata [ITI-62]**

##### **A\_14926-01 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen der Dokumente bei Remove Metadata**

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

##### **A\_20701 - Komponente ePA-Dokumentenverwaltung – Unwiderrufliches Löschen bei Remove Metadata**

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

##### **A\_21715 - Komponente ePA-Dokumentenverwaltung – Kein Löschen von "replaced"-Dokumenten im Status "Deprecated"**

Die Komponente ePA Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS sicherstellen, dass keine Löschanfrage eines ePA-Client auf Dokumenten mit dem `availabilityStatus = Deprecated` ausgeführt werden darf. [<=]

##### **A\_21714 - Komponente ePA-Dokumentenverwaltung – Löschen von strukturierten Dokumenten**

Die ePA-Dokumentenverwaltung MUSS sicherstellen, dass eine Löschanfrage eines ePA-FdV für strukturierte Dokumente der Sammlungstypen `mixed` als Löschen von Ordnern umgesetzt wird, wobei das Löschen einzelner Dokumente mit dem Status `approved` nicht zulässig ist. Falls das Löschen dieser Ordner erlaubt ist, impliziert es aktensystemseitig immer das Löschen zugehöriger `SubmissionSets`, `Associations` sowie zugeordneter Dokumente.

Die ePA-Dokumentenverwaltung MUSS sicherstellen, dass eine Löschanfrage eines Primärsystems auch einzelne Dokumente der Sammlungstypen `mixed`, `uniform` sowie `atomic` umfassen kann, wobei auch sämtliche Dokumente der jeweiligen Ordner gelöscht werden können.

Liegt eine Verletzung der Löschvorgaben vor, MUSS die Komponente ePA-Dokumentenverwaltung das Löschen ablehnen, die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und den `XDSRemoveDocumentsError`-Fehlercode mit der `UniqueID` des Policy Document zurückgeben.

[<=]

##### **A\_14670-02 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Remove Metadata**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor ein oder mehrere Dokumente oder Metadatenobjekte gelöscht werden. Bei einem Löschen von mehreren Dokumenten oder Metadatenobjekten durch das ePA-Fachmodul können einzelne Dokumente durch den zwischenzeitlichen Entzug einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für das Löschen berechtigt sein. Widerspricht ein zu löschendes Dokument einer

anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum betreffenden Dokument einen `XDSDocumentUniqueIdError`- Fehlercode enthalten und der Wert 4 des `EventOutcomeIndicators` im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein zu löschendes Dokument nicht mehr verfügbar, MUSS gemäß IHE TF ITI der Fehlercode `XDSDocumentUniqueIdError` zurückgegeben werden. [`<=`]

#### **A\_21246-01 - Komponente ePA-Dokumentenverwaltung – Policy-Dokument-Aktualisierung für Remove Metadata**

~~A\_21246 – Komponente ePA-Dokumentenverwaltung – Policy Aktualisierung für Remove Metadata~~ Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS beim Löschen eines Dokuments über die Operation Remove Metadata die `DocumentEntry.uniqueIdentryUUID` des Dokuments aus der Whitelist aller LEI-Policy-Dokumente (~~gemäß 9.3~~) löschen, welche die entsprechende `DocumentEntry.uniqueIdentryUUID` referenzieren. [`<=`]

~~Das Löschen eines Dokuments von der Whitelist geschieht über über das Entfernen aller <Resource> Elemente aus allen LEI-Policy-Dokumenten, für die gilt:~~

```
//PolicySet[@PolicySetId='urn:gematik:policy-set-id:permissions-access-group-hep:base']/Policy[@PolicySetId='urn:gematik:policy-id:permissions-access-group-hep:whitelist']/Rule/Target/Resources/Resource/ResourceMatch/AttributeValue {text()='xyz'}
```

~~wobei 'xyz' der DocumentEntry.uniqueId des gelöschten Dokuments entspricht.~~

Auch wenn eine LEI ausschließlich Leseberechtigung für ein einzelnes Dokument besessen hat und diese durch das Löschen entfällt, darf das Policy-Dokument Document nicht vollständig gelöscht werden, da die LEI damit auch die Schreibberechtigung in für die Akte des Versicherten verlieren würde, die mit einer Berechtigung immer grundsätzlich einhergeht einhergehen kann.

### 4.3 Fehlerbehandlung in Schnittstellenoperationen

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

#### **A\_15664 - Komponente ePA-Dokumentenverwaltung – Fehlername**

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

#### **A\_15665 - Komponente ePA-Dokumentenverwaltung – Fehlertext**

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

### A\_15666 - Komponente ePA-Dokumentenverwaltung – Fehlernummer

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

**Tabelle 3: Tab\_Dokv\_12 - Fehlercodes zu Fehlern gemäß Operationsdefinition**

Name	Fehlercode
INTERNAL_ERROR	7500
SYNTAX_ERROR	7510
ASSERTION_INVALID	7520
ACCESS_DENIED	7530
TEMP_UNAVAILABLE	7550
INVALID_AUT_KEY	7560

[<=]

## 4.4 Vertrauenswürdige Ausführungsumgebung

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

### A\_14472-01 - Komponente ePA-Dokumentenverwaltung – Umsetzung des Dokumentenmanagements in einer Vertrauenswürdigen Ausführungsumgebung (VAU)

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

### A\_18714-01 - Komponente ePA-Dokumentenverwaltung – Verhalten des Kontextmanagements bei ungeöffnetem Verarbeitungskontext

Das Kontextmanagement MUSS mit einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") antworten, wenn für eine Web-Service-Operation der Schnittstellen `I_Document_Management`, `I_Document_Management_Insurant`, `I_Document_Management_Insurance` sowie `I_Account_Management_Insurant` für den angemeldeten Nutzer kein Verarbeitungskontext geöffnet wurde.

[<=]

#### 4.4.1 Verarbeitungskontext

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

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

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

##### **A\_14557 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext der VAU**

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

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

##### **A\_14581 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung von außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten**

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

##### **A\_14582 - Komponente ePA-Dokumentenverwaltung – Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU**

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

##### **A\_14583 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung der Dokumentmetadaten und technischen Daten der VAU**

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

##### **A\_14566 - Komponente ePA-Dokumentenverwaltung – Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU**

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

#### 4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld

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

##### **A\_14558 - Komponente ePA-Dokumentenverwaltung – Isolation der VAU von Datenverarbeitungsprozessen des Anbieters**

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

##### **A\_14559 - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Software der VAU**

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

##### **A\_14560 - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Hardware der VAU**

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

##### **A\_14561 - Komponente ePA-Dokumentenverwaltung – Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU**

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

##### **A\_14562 - Komponente ePA-Dokumentenverwaltung – Kein physischer Zugang des Anbieters zu Systemen der VAU**

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

##### **A\_14563 - Komponente ePA-Dokumentenverwaltung – Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU**

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

##### **A\_14564 - Komponente ePA-Dokumentenverwaltung – Private Schlüssel von Dienstzertifikaten im HSM**

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

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

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

Die Prüftiefe des HSM MUSS dabei den in [gemSpec\_Aktensystem#A\_15156] angegebenen Standards entsprechen.

[<=]

#### **A\_14565 - Komponente ePA-Dokumentenverwaltung – HSM-Kryptographieschnittstelle verfügbar nur für Instanzen der VAU**

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

#### **A\_14567 - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal vom Client zum Verarbeitungskontext der VAU**

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

### **4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes**

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

#### **A\_14568 - Komponente ePA-Dokumentenverwaltung – Aktivierung des Verarbeitungskontextes der VAU**

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

#### **A\_15085 - Komponente ePA-Dokumentenverwaltung – Prüfung des Kontextschlüssels durch die VAU**

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

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

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

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

#### **A\_14570 - Komponente ePA-Dokumentenverwaltung – Keine Speicherung des Kontextschlüssels in der VAU**

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

#### **A\_15841 - Komponente ePA-Dokumentenverwaltung – Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes**

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

### **4.4.4 Parallele Zugriffe**

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

#### **A\_14571 - Komponente ePA-Dokumentenverwaltung – Parallele Zugriffe auf den Verarbeitungskontext der VAU**

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

#### **A\_14572 - Komponente ePA-Dokumentenverwaltung – Eindeutige VAU-Instanz für einen Verarbeitungskontext der VAU**

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

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

#### **A\_14573 - Komponente ePA-Dokumentenverwaltung – Konsistenter Systemzustand des Verarbeitungskontextes der VAU**

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

#### **A\_14574 - Komponente ePA-Dokumentenverwaltung – Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU**

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

### **4.4.6 Client-Verbindungen zum Verarbeitungskontext**

Um Verbindungen vom Fachmodul ePA nach [gemSpec\_FM\_ePA, gemSpec\_FM\_ePA\_KTR\_Consumer] und ePA-Frontend des Versicherten nach [gemSpec\_FdV\_ePA] zum Verarbeitungskontext des Aktenkontos zu ermöglichen, ist ein Kontextmanagement erforderlich. Das Kontextmanagement ist im Netzwerk der TI für das Fachmodul ePA und für das ePA-Frontend des Versicherten unter mindestens einer

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

#### **A\_14616 - Komponente ePA-Dokumentenverwaltung – Kontextmanagement der Vertrauenswürdigen Ausführungsumgebung**

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

#### **A\_14575 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontexte der VAU über gemeinsame Host-Adresse erreichbar**

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

#### **A\_14576-01 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom ePA-Frontend des Versicherten zum Verarbeitungskontextes der VAU über das Zugangsgateway**

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

#### **A\_15528 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom Fachmodul ePA zum Verarbeitungskontextes der VAU über das Kontextmanagement**

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

#### **A\_17834 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom Fachmodul ePA KTR-Consumer zum Verarbeitungskontextes der VAU über das Kontextmanagement**

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

#### **A\_14577-01 - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal zum Verarbeitungskontext der VAU auf Inhaltsebene**

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

#### **A\_14580 - Komponente ePA-Dokumentenverwaltung – Identität der Dokumentenverwaltung für das Fachmodul ePA und Fachmodul ePA KTR-Consumer**

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

**A\_15646-01 - Komponente ePA-Dokumentenverwaltung – Identität des Verarbeitungskontextes für Clients**

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

[<=]

**A\_15183 - Komponente ePA-Dokumentenverwaltung – Automatisierter Abbau des sicheren Kanals bei Inaktivität**

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS den sicheren Kanal zu einem Client nach 20 Minuten Inaktivität abbauen, sodass anschließend keine Zugriffe dieses Clients auf den Verarbeitungskontext mehr möglich sind, ohne dass eine neue Verbindung aufgebaut wird.[<=]

## 4.5 Anforderungen zur sicherheitstechnischen Validierung

**A\_15186 - Komponente ePA-Dokumentenverwaltung – Prüfung der Kombination von WS-Addressing Action und SOAP Body**

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

**A\_15585 - Komponente ePA-Dokumentenverwaltung – Gleichheit von SOAP Action und WS-Addressing Action**

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

**A\_14465-01 - Komponente ePA-Dokumentenverwaltung – XML Schema-Validierung für SOAP-Eingangsnachrichten**

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

**A\_14809 - Komponente ePA-Dokumentenverwaltung – Keine Verwendung des "xsi:schemaLocation"-Attributs**

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

**~~A\_13690-03A~~ ~~A\_13690-02~~ - Komponente ePA-Dokumentenverwaltung – SAML 2.0 Assertion-Validierung**

Die Komponente ePA-Dokumentenverwaltung MUSS die vorliegende Assertion einer grundsätzlichen XML Schema-Prüfung, einer Prüfung gemäß den Prüfvorschriften aus [gemSpec\_TBAuth#3.2] sowie einer Prüfung auf Übereinstimmung mit dem erforderlichen SAML 2.0 Assertion-Profil aus [gemSpec\_FM\_ePA#A\_14927, A\_15638], [gemSpec\_Authentisierung\_Vers#A\_14109, A\_15631], [gemSpec\_Autorisierung#A\_14491] oder [gemSpec\_FM\_ePA\_KTR\_Consumer#A\_17253,

A\_17254] unterziehen~~und~~. Die Verarbeitung der begleitenden Nachricht ~~abbrechen und MUSS abgebrochen werden, falls eine Übereinstimmung nicht festgestellt werden kann. Bei Nichtübereinstimmung einer Authentication Assertion MUSS die Verarbeitung gemäß [WSS#12] bzw. im Sonderfall der sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittiert werden. Bei Nichtübereinstimmung einer Authorization Assertion MUSS die Verarbeitung mit einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls eine Übereinstimmung nicht festgestellt werden kann. quittiert werden.~~

Insbesondere MUSS das in der SAML 2.0 Assertion enthaltende Signaturzertifikat mittels [gemSpec\_PKI\_018#TUC\_PKI\_018] mit den folgenden Parametern geprüft werden:

**Tabelle 4: Tab\_Dokv\_35 - Eingangsparameter für TUC\_PKI\_018**

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

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

Der Hinweis unter [gemSpec\_Autorisierung]#A\_17655 gilt auch im vorliegenden Prüfkontext, d.h. die dort beschriebene vereinfachte Prüfung kann für selbst ausgestellte Identitätsbestätigungen dementsprechend auch im Kontext der hier thematisierten Prüfung umgesetzt werden.

**A\_18990 - ePA-Dokumentenverwaltung – Beschränkung gültiger Identitätsbestätigungen**

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

**A\_17386-01 - Komponente ePA-Dokumentenverwaltung – Authentication Assertion-Validierung**

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

**A\_17387 - Komponente ePA-Dokumentenverwaltung – Authorization Assertion-Validierung**

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

[<=]

Dies kann durch eine aktuell gehaltene Konfiguration vertrauenswürdiger Zertifikate umgesetzt werden und ersetzt eine detaillierte Prüfung der Signaturzertifikate gem. [gemSpec\_TBAuth#A\_15557].

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

**A\_14735 - Komponente ePA-Dokumentenverwaltung – Verpflichtende Nutzung des "mustUnderstand"-Attributs im SOAP Security Header**

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

**A\_14810 - Komponente ePA-Dokumentenverwaltung – Erkennung von Denial-of-Service-Angriffen hinsichtlich dem Parsen von SOAP 1.2-Nachrichten**

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

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

[<=]

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

**A\_14811-01 - Komponente ePA-Dokumentenverwaltung – Ablehnung von SOAP 1.2-Nachrichten ohne UTF-8 Kodierung**

Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Nachrichten dahingehend prüfen, dass diese der Zeichenkodierung UTF-8 entsprechen, andernfalls die Operation einem geeigneten HTTP-Statuscode gemäß [RFC7231] ablehnen.[<=]

**A\_21200 - Komponente ePA-Dokumentenverwaltung und Clients – UTF-8 Kodierung von SOAP 1.2-Nachrichten**

Die Komponente ePA-Dokumentenverwaltung und deren Clients MÜSSEN sicherstellen, dass die XML-Inhalte der SOAP 1.2-Nachrichten, die sie senden, der Zeichenkodierung UTF-8 entsprechen.<=[<=]

Es ist zu beachten, dass sich die Anzeige der verwendeten Kodierung in der Nachricht unterscheiden kann, z.B. in Nachrichten, in denen MTOM verwendet wird.

## 4.6 Protokollierung

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

**A\_14813-03 - Komponente ePA-Dokumentenverwaltung – Protokollierung in der Komponente ePA-Dokumentenverwaltung**

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

- I\_Document\_Management::CrossGatewayDocumentProvide
- I\_Document\_Management::CrossGatewayQuery
- I\_Document\_Management::RemoveMetadata
- I\_Document\_Management::RemoveDocuments
- I\_Document\_Management::CrossGatewayRetrieve
- I\_Document\_Management::RestrictedUpdateDocumentSet
- I\_Document\_Management\_Insurance::ProvideAndRegisterDocumentSet-b
- I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b
- I\_Document\_Management\_Insurant::RestrictedUpdateDocumentSet
- I\_Document\_Management\_Insurant::RegistryStoredQuery
- I\_Document\_Management\_Insurant::RemoveMetadata
- I\_Document\_Management\_Insurant::RetrieveDocumentSet
- I\_Account\_Management\_Insurant::GetAuditEvents
- I\_Account\_Management\_Insurant::GetSignedAuditEvents
- I\_Account\_Management\_Insurant::SuspendAccount
- I\_Account\_Management\_Insurant::ResumeAccount
- I\_Key\_Management\_Insurant::StartKeyChange
- I\_Key\_Management\_Insurant::FinishKeyChange

je einen Eintrag im § 291a-Protokoll für den Versicherten gemäß [gemSpec\_DM\_ePA#A\_14471] mit folgenden vom Operationsaufruf abhängigen Parametern vornehmen: UserID, UserName, ObjectID, ObjectName und ObjectDetail. [ $\leq$ ]

**A\_14814 - Komponente ePA-Dokumentenverwaltung – Schutz vor Manipulation der Protokoll Daten**

Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die § 291a-Protokoll Daten gegen Veränderung und unberechtigtes Löschen geschützt sind. [ $\leq$ ]

**~~A\_20538-02A\_20538-01~~ - Komponente ePA-Dokumentenverwaltung – Parameter des § 291a-Protokolls**

Die Komponente ePA-Dokumentenverwaltung MUSS einen Protokolleintrag gemäß der Festlegung in [gemSpec\_DM\_ePA#A\_14471] mit folgenden Ergänzungen erzeugen:

**Tabelle 5: Tab\_Dokv\_13 - Parameter des § 291a-Protokolls**

Proto koll- param eter	Parameterwerte gemäß aufgerufener Operation

<p>UserID</p>	<p>Wert des AttributeStatements der übergebenen übergebenen AuthenticationAssertion in SAML:Assertion/SAML:AttributeStatement</p> <p><b>Variante a: Akteur des Aufrufs ist Versicherter bzw. Vertreter</b> (unveränderbare Anteil der KVNR des aufrufenden Versicherten bzw. Vertreters) XPath-Ausdruck zur "Subject ID" der im Operationsaufruf übergebenen Authentication Assertion:  <pre>//*[local-name()='Assertion' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion'][@Name='urn:gematik:subject:subject-id']/*[local-name()='AttributeValue']/*[local-name()='InstanceIdentifier']/data(@extension)</pre> </p> <p><b>Variante b: Akteur des Aufrufs ist LEI oder Kostenträger</b> (Telematik-ID der aufrufenden LEI oder Kostenträgers) XPath-Ausdruck zur "Organization ID" der im Operationsaufruf übergebenen Authentication Assertion:  <pre>//*[local-name()='Assertion' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion'][@Name='urn:gematik:subject:organization-id']/*[local-name()='AttributeValue']/*[local-name()='InstanceIdentifier']/data(@extension)</pre> </p>					
<p>UserName</p>	<p>XPath-Ausdruck zur Behauptung "name" (beinhaltet commonName aus dem X.509-Zertifikat), der im Operationsaufruf übergebenen Authentication Assertion:  <pre>//*[local-name()='Assertion' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion'][@Name='http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name']/*[local-name()='AttributeValue']</pre> </p>					
<p>Object ID</p>	<p>Der unveränderbare Anteil der KVNR des <code>extension</code>-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>Object Detail</p>	<p>Für alle Operationen gilt: Falls die Operation mit einem Fehler ASSERTION_INVALID aufgrund einer ungültigen übergebenen Authentication Assertion abbricht, MUSS ParticipantObjectDetail mit folgenden Wertepaaren (type/value) belegt werden:</p> <table border="1" data-bbox="304 1881 1391 1944"> <thead> <tr> <th data-bbox="304 1881 737 1944">type</th> <th data-bbox="737 1881 1391 1944">value</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>		type	value		
type	value					

ErrorInformation	"fehlgeschlagene Authentifizierung des Zugreifenden"
<p>Bei Zugriff über die Operationen:</p> <ul style="list-style-type: none"> <li>• <i>CrossGatewayDocumentProvide</i></li> <li>• <i>ProvideAndRegisterDocumentSet-b</i></li> <li>• <i>CrossGatewayRetrieve</i></li> <li>• <i>RetrieveDocumentSet</i></li> <li>• <i>RemoveMetadata</i></li> <li>• <i>RemoveDocuments</i></li> <li>• <i>RestrictedUpdateDocumentSet</i></li> </ul> <p>MUSS ParticipantObjectDetail beim Zugriff auf Dokumente mit folgenden Wertepaaren (type/value) belegt werden:</p>	
<b>type</b>	<b>value</b>
DocumentUniqueId	Wert von DocumentEntry.uniqueId
DocumentTitle	Wert von DocumentEntry.title
DocumentPracticeSetting	<p>Wert von DocumentEntry.practiceSettingCode, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3]. (Beispiel: „ALLG^^^&amp;1.3.6.1.4.1.19376.3.276.1.5.4&amp;ISO“, wobei ALLG für den Code und 1.3.6.1.4.1.19376.3.276.1.5.4 für das Code System steht.</p>
DocumentFormat	<p>Wert von DocumentEntry.formatCode, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3]., siehe oben.                      Wenn es sich beim Wert von DocumentEntry.formatCode um den Code urn:ihe:iti:xds:2017:mimeTypeSufficient (Code System 1.3.6.1.4.1.19376.1.2.3) handelt, MUSS stattdessen der Wert von DocumentEntry.mimeType hier eingetragen werden.</p> <p>Hinweis: Ein verarbeitendes System muss also, falls der hinterlegte Wert nicht dem Coded String-Format entspricht, den Wert als mimeType gemäß DocumentEntry.mimeType interpretieren.</p>

DocumentConfidentialityCode	Wert von DocumentEntry.confidentialityCode, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3], siehe oben. <a href="#">Wird mehr als ein Code dokumentiert, MUSS als Trennzeichen das Tildezeichen ('~') verwendet werden.</a>
und beim Zugriff auf Ordner mit den folgenden Wertepaaren (type/value) belegt werden:	
<b>type</b>	<b>value</b>
FolderCodeList	Wert von Folder.codeList, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3], siehe oben. Wird mehr als ein Code dokumentiert, MUSS als Trennzeichen das Tildezeichen ('~') verwendet werden.
FolderUniqueId	Wert von Folder.uniqueId
FolderTitle	Wert von Folder.title
FolderLastUpdateTime	Wert von Folder.lastUpdateTime

[<=]

**A\_21213 - Komponente ePA-Dokumentenverwaltung - Protokollierung von Suchparametern**

Die Komponente ePA-Dokumentenverwaltung MUSS beim Zugriff auf die Operationen I\_Document\_Management\_Insurant::RegistryStoredQuery sowie I\_Document\_Management::CrossGatewayQuery einen Protokolleintrag gemäß A\_20538-\* vornehmen und darüberhinaus ParticipantObjectDetail um folgende Wertepaaren (type/value) ergänzen:

Protokollparameter	Parameterwerte gemäß aufgerufener Operation	
Object-Detail	<b>type</b>	<b>value</b>
	ParameterQueryId	Der Wert MUSS der Parameter Query ID gemäß [IHE-ITI-TF3]#3.18.4.1.2.4 entsprechen.

Darüberhinaus MUSS jeder gesendete Suchparameter mit Parametername (type) und -wert (value) protokolliert werden. Dabei gelten folgenden Regeln für Werte, die per UND/ODER verknüpft sind (entsprechend [IHE-ITI-TF2a]#3.18.4.1.2.3.5):

- Falls innerhalb desselben <Slot> verschiedene <Value>-Elemente innerhalb der <ValueList> gesendet werden (ODER-Verknüpfung), MÜSSEN die Werte protokolliert werden, als wenn sie kommasepariert innerhalb eines einzelnen <Value>-Elements gesendet worden wären. Längenbeschränkungen des Query

Schemas auf dem <Value>-Element sind dabei für die entsprechende Transformation außer Kraft gesetzt.		
<ul style="list-style-type: none"> <li>Falls derselbe Parametername in mehreren Slots angefragt wird (UND-Verknüpfung), MUSS der Parametername mehrmals (jeweils einmal pro Slot) mit dem jeweils dazugehörigen Wert protokolliert werden.</li> </ul>		
Object-Detail	type	value
	Query Parameter Name (UUID-Format: "urn:uuid:...")	Parameterwert

## [&lt;=]

Die folgende Tabelle zeigt Beispiele für Parameternamen und -werte, wie sie als Teil des Protollierungseintrags für eine FindDocuments-Query ("ParameterQueryId"="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d") protokolliert werden würden. Etwaige weitere Parameter wie \$XDSDocumentEntryPatientId werden nicht gezeigt:

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

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

### **A\_20144 - Komponente ePA-Dokumentenverwaltung - Aufteilen von Protokolleinträgen für mehrere Dokumente**

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

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

### ~~A\_20708 - Komponente ePA-Dokumentenverwaltung - Protokollierung gelöschter Ordner für Dokumente des Sammlungstyp "mixed"~~

~~Die Komponente ePA-Dokumentenverwaltung MUSS beim Löschen eines Ordners gemäß A\_20579 einen Protokolleintrag gemäß A\_20538 \* vornehmen und dabei für die Parameter "User ID", "User Name" und "Object ID" die Werte wählen, die für die Protokollierung der Operation verwendet wurden, welche die Löschung des Ordners ausgelöst haben. [<=]~~

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

### **A\_21210 - Komponente ePA-Dokumentenverwaltung - Protokollierung von Metadaten ohne Inhalt**

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

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

DocumentTitle = ""

## **4.6.1 Protokollierung von Berechtigungen**

Falls Berechtigungen angepasst werden, muss die Dokumentenverwaltung noch weitere Details protokollieren, die es dem Versicherten ermöglichen, den Verlauf der Berechtigungsvergabe für einzelne Berechtigte nachzuvollziehen. ~~Dabei wird zwischen dem Einstellen, Aktualisieren und vollständigen Löschen von Berechtigungen unterschieden. Pro eingestelltes oder ersetztes Policy Document (vgl. A\_14998) muss ein Protokolleintrag erzeugt werden.~~

**A\_20564-03A\_20564-01 - Komponente ePA-Dokumentenverwaltung – Protokollierung neuer Berechtigungen**

Die Komponente ePA-Dokumentenverwaltung MUSS ~~bei~~ beim Registrieren von Zugriffen auf APPC durch ein neu registriertes Policy-Dokumente (Document gemäß emSpec[gemSpec\_DM\_ePA#A\_14961]) über die Transaktionen

- CrossGatewayDocumentProvide
- ProvideAndRegisterDocumentSet-b

das Protokoll gemäß A\_20538\* um die einen weiteren Eintrag mit den folgenden Details ergänzen, ~~sofern noch keine Berechtigung für den von der Policy betroffenen Berechtigten existiert:~~

Protokollparameter	Parameterwerte beim Einstellen <del>von</del> <u>eines</u> Policy-Dokumenten <u>Document</u>	
Object Detail	<b>type</b>	<b>value</b>
	PermAuthorized ID	Wert des <u>Attributs XPath-Ausdrucks des Policy Document</u> <code>/PolicySet/<del>PolicySet</del>[1]/Target/Subjects/Subject {1}/SubjectMatch/AttributeValue/InstanceIdentifier{<del>@/</del>@extension}</code>  <del>aus der eingestellten Policy (bei LEI und</del>  <u>Bei Leistungserbringerinstitutionen sowie Kostenträgern <del>die</del>st der Wert eine Telematik-ID, bei Vertretern <del>die</del>der unveränderliche Teil der KVNR).</u>
	PermAuthorized Name	Wert des <u>Attributs</u> <code>/PolicySet/<del>PolicySet</del>[1]/Target/Subjects/Subject {2}/SubjectMatch/AttributeValue{@text}</code>  <del>aus der eingestellten</del> <u>XPath-Ausdrucks des Policy (Document bei LEI und Leistungserbringerinstitutionen sowie Kostenträgern <del>der</del> substring-before(/PolicySet/Description/text (),' :')</u>  <u>Wert des XPath-Ausdrucks des Policy Document bei Vertretern</u> <code>/PolicySet/Description/text ()</code>  <u>Bei Leistungserbringerinstitutionen sowie Kostenträgern ist der Wert ein Organisationsname, bei Vertretern <del>der</del> X.509 Subject <u>ein</u> Name <del>der</del> eGK).</u>
<del>PermAccessLevel</del>	<del>Gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.</del>	

PermCategories	Gewährte mittelgranulare Rechte: Kommaseparierte Liste von <u>Kategorien</u> <u>Dokumenten</u> <u>kategorien</u> (technischer Identifier gemäß A_19303-*) <u>mitsamt der gewährten Vertraulichkeitsstufe: „normal“ oder „erweitert“</u> im Format " <u>Kategorie~Vertraulichkeitsstufe</u> " Als Trennzeichen fungiert das Tildezeichen ('~'). <u>Beispiel "care~normal, ega~erweitert"</u>
PermWhitelist	Explizit freigegebene Dokumente ( <u>feingranulare</u> <u>dokumentenspezifische</u> Berechtigung): kommaseparierte Liste <u>der uniqueIDs der freigegebenen</u> <u>Dokumente</u> aus <u>DocumentEntry.entryUUID</u>
PermBlacklist	Explizit gesperrte Dokumente ( <u>feingranulare</u> <u>oder</u> <u>Ordner</u> ( <u>dokumentenspezifische</u> Berechtigung): kommaseparierte Liste <u>der uniqueIDs der gesperrten</u> <u>Dokumente</u> aus <u>DocumentEntry.entryUUID</u> bzw. <u>Folder.entryUUID</u>

[<=]

Ein separater Eintrag für das Einstellen des Policy Document DARF NICHT angelegt werden. Das Erfassen von eingestellten Dokumenten in A\_20538 betrachtet keine Policy Documents. [<=]

**A\_20565-01 – Komponente ePA – Dokumentenverwaltung – Protokollierung aktualisierter Berechtigungen**

Die Komponente ePA – Dokumentenverwaltung MUSS beim Einstellen von APPC – Policy – Dokumenten (gemäß emSpec\_DM\_ePA#A\_14961) über die Transaktionen

- CrossGatewayDocumentProvide
- ProvideAndRegisterDocumentSet

das Protokoll gemäß A\_20538-\* um die folgenden Details ergänzen, sofern bereits eine Berechtigung für den betroffenen Berechtigten existiert, die durch die neue Berechtigung aktualisiert wird:

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

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

<del>PermBlackListRemoved</del>	<del>Ursprünglich explizit gesperrte Dokumente (feingranulare Berechtigung), die in der neuen Policy nicht mehr explizit gesperrt sind: kommaseparierte Liste der uniqueIDs der gesperrten Dokumente.</del>
<del>PermBlackList</del>	<del>Explizit gesperrte Dokumente (feingranulare Berechtigung) gemäß aktualisierter Berechtigung: kommaseparierte Liste der uniqueIDs der gesperrten Dokumente.</del>

[<=]

**A\_20566-02A\_20566-01 - Komponente ePA-Dokumentenverwaltung – Protokollierung gelöschter Berechtigungen**

Die Komponente ePA-Dokumentenverwaltung MUSS beim Löschen von APPC-Zugriffen (d.h. Löschen eines Policy-Dokumenten (Document gemäß emSpec[gemSpec\_DM\_ePA#A\_14961])) über die Transaktionen

- I\_Document\_Management\_Insurant::RemoveMetadata
- I\_Document\_Management\_Insurant::RemoveDocuments (abgekündigt)

das Protokoll gemäß A\_20538-\* um die einen weiteren Eintrag mit den folgenden Details ergänzen:

Protokollparameter	Parameterwerte beim Löschen <del>von</del> <u>eines Policy-Dokumenten Document</u>	
Object Detail	<b>type</b>	<b>value</b>
	PermAuthorizedID	Wert des <u>Attributs XPath-Ausdrucks des Policy Document</u> /PolicySet/ <u>PolicySet[1]</u> /Target/Subjects/Subject <u>[1]</u> /SubjectMatch/AttributeValue/InstanceIdentifier <u>[@extension]</u>  <u>-aus der eingestellten Policy (bei LEI und</u>  <u>Bei Leistungserbringerinstitutionen sowie Kostenträgern</u> <u>die ist der Wert eine Telematik-ID, bei Vertretern</u> <u>unveränderliche Teil der KVNR).</u>
	PermAuthorizedName	Wert des <u>Attributs</u>  /PolicySet/ <u>PolicySet[1]</u> /Target/Subjects/Subject <u>[2]</u> /SubjectMatch/AttributeValue <u>[@text]</u>  <u>-aus der eingestellten XPath-Ausdrucks des Policy</u> <u>(Document bei LEI</u> <u>und Leistungserbringerinstitutionen sowie</u> <u>Kostenträgern</u> <u>der</u> <u>substring-</u>

	<p><a href="#">before (/PolicySet/Description/text(), ':')</a></p> <p><u>Wert des XPath-Ausdrucks des Policy Document bei Vertretern</u> <a href="#">/PolicySet/Description/text()</a></p> <p><u>Bei Leistungserbringerinstitutionen sowie Kostenträgern ist der Wert ein Organisationsname, bei Vertretern der X.509-Subject ein Name der eGK).</u></p>
<del>PermAccessLevel</del>	<del>Ursprünglich gewährte grobgranulare Zugriffsstufe: „normal“ oder „erweitert“.</del>
<del>PermCategoriesRemoved</del>	<del>Ursprünglich gewährte mittelgranulare Rechte: „kommaseparierte Liste von Kategorien Dokumentenkategorien (technischer Identifier gemäß A_19303-*)“ mitsamt der gewährten Vertraulichkeitsstufe: „normal“ oder „erweitert“ im Format "Kategorie~Vertraulichkeitsstufe" Als Trennzeichen fungiert das Tildezeichen ('~'). Beispiel "care~normal, eqa~erweitert"</del>
<del>PermWhiteListRemoved</del>	<del>Ursprünglich explizit freigegebene Dokumente (feingranulare dokumentenspezifische Berechtigung): kommaseparierte Liste der uniqueIDs der freigegebenen Dokumente aus <a href="#">DocumentEntry.entryUUID</a></del>
<del>PermBlackListRemoved</del>	<del>Ursprünglich explizit gesperrte Dokumente (feingranulare oder Ordner (dokumentenspezifische Berechtigung): kommaseparierte Liste der uniqueIDs der gesperrten Dokumente aus <a href="#">DocumentEntry.entryUUID</a> bzw. <a href="#">Folder.entryUUID</a></del>

[<=]

## 5 Funktionsmerkmale

### 5.1 Dokumentenverwaltung

In diesem Abschnitt wird die Außenschnittstelle der IHE ITI-basierten Dokumentenverwaltung festgelegt. Einzelne Umsetzungsanforderungen suggerieren eine vermischte Verarbeitung von Funktionalitäten, welche bei IHE ITI originär getrennt von einer Document Registry und einem Document Repository (bzw. den Responding Gateways) durchgeführt werden. Da die Außenschnittstelle der ePA-Dokumentenverwaltung nicht zwischen Document Registry und Document Repository unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit differenzierten Pfaden siehe [gemSpec\_Aktensystem#A\_17969]), werden sonst bei IHE ITI explizite Operationen zwischen diesen Akteuren nicht gesondert dargestellt, sondern als interne Umsetzung angenommen. Die in einer Umsetzung geforderte Verarbeitung einer SOAP-Nachricht kann an IHE ITI-konforme Akteure ausgerichtet werden.

#### 5.1.1 Schnittstelle I\_Document\_Management

##### A\_14152-01 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I\_Document\_Management

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

**Tabelle 6: Tab\_Dokv\_14 - Schnittstelle I\_Document\_Management**

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

	Remove Metadata	Löschen von Dokumenten oder Ordern
	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
<b>WSDL</b>	DocumentManagementService.wsdl	
<b>XML Schema</b>	<ul style="list-style-type: none"> <li>• PRPA_IN201301UV02.xsd</li> <li>• PRPA_IN201302UV02.xsd</li> <li>• PRPA_IN201304UV02.xsd</li> <li>• MCCI_IN000002UV01.xsd</li> <li>• query.xsd</li> <li>• rs.xsd</li> <li>• lcm.xsd</li> <li>• rim.xsd</li> <li>• XDS.b_DocumentRepository.xsd</li> </ul>	

[<=]

### 5.1.1.1 Operation

#### **I\_Document\_Management::CrossGatewayDocumentProvide**

#### **A\_14153 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-Gateway Document Provide**

Die Komponente ePA-Dokumentenverwaltung MUSS

die Operation `I_Document_Management::CrossGatewayDocumentProvide` gemäß der folgenden Signatur implementieren:

**Tabelle 7: Tab\_Dokv\_15 - Operation Cross-Gateway Document Provide**

<b>Operation</b>	<b>I_Document_Management::CrossGatewayDocumentProvide</b>		
<b>Beschreibung</b>	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.		
<b>Formatvorgabe n</b>	SOAP Action: urn:ihe:iti:2015:CrossGatewayDocumentProvide		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>

<b>Cross-Gateway Document Provide Message</b>	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	n
<b>X-User Assertion</b>	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
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>Cross-Gateway Document Provide Response Message</b>	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	rs:RegistryResponse	n
<b>Technische Fehlermeldungen</b>			
<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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>MaxDocSizeExceeded</b>	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines der übermittelten Dokumente übersteigt 25 MByte.	
<b>MaxPkgSizeExceeded</b>	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

[&lt;=]

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

#### 5.1.1.1.1 Umsetzung

### **A\_15055 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung von gemischten Dokumentenpaketen mit Policy Documents**

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

Anforderung [gemSpec\_DM\_ePA#A\_14961] für Policy Documents (Advanced Patient Privacy Consents) enthalten sind.

[<=]

### [A\\_14941-05A\\_14941-03](#) - Komponente ePA-Dokumentenverwaltung – Keine Registrierung bei Angabe von Document Entry Relationships in Metadaten

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

- `urn:ihe:iti:2007:AssociationType:XFRM` (Transform)
- `urn:ihe:iti:2007:AssociationType:XFRM_RPLC` ([Transform and Replace with Transformation](#))
- `urn:ihe:iti:2007:AssociationType:signs` (Digital Signature)
- `urn:ihe:iti:2010:AssociationType:IsSnapshotOf` (Snapshot of On-Demand document entry)
- `urn:ihe:iti:20102007:AssociationType:APND` (Addendum)

[<=]

### [A\\_21713](#) - Komponente ePA-Dokumentenverwaltung – Kein Einstellen von Ordnern

Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS das Registrieren und Speichern von Metadaten und Dokument(en) über die Schnittstelle `I Document Management::CrossGatewayDocumentProvide` ablehnen und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder enthalten sind. Ausnahme: Folder der Kategorie `mothersrecord` und `childsrecord` in `Folder.codelist`. [[<=](#)]

### **A\_13838 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße prüfen**

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

[<=]

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

### [A\\_13798-01A\\_13798](#) - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung der Metadaten aus ITI Document Sharing-Profilen durch XCDR-Akteur "Responding Gateway"

Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS die `SubmissionSet`- sowie die `DocumentEntry`-Metadaten der eingehenden ~~Nachricht~~[Nachricht vor](#) einer Zugriffskontrolle gemäß der Konformität zu den Nutzungsvorgaben in [gemSpec\_DM\_ePA#A\_14760] prüfen. Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit

einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind- [oder eine nachgelagerte Zugriffskontrollprüfung negativ ausfällt](#). Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht.[<=]

**A\_13715 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-Gateway Document Provide**

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

**~~A\_13657-01A\_13657~~ - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Cross-Gateway Document Provide**

Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS ~~für die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden~~[Ausführung dieser Operation prüfen, ob für den zugreifenden Nutzer ein gültiges Policy Documents \(Advanced Patient Privacy Consents\) entsprechend Document vorliegt und ob er gemäß der Anforderung Rollenprüfung in A\\_19303 schreibberechtigt ist. Liegt kein Policy Document vor oder ist er nicht schreibberechtigt, MUSS die Nachricht mit dem SOAP-Fault ACCESS DENIED-Fehlercode sowie einem HTTP-Statuscode 403 \(Fehlermeldung "Access Denied"\) gemäß \[RFC7231\] quittiert werde.](#) ~~14822 durchsetzen, bevor ein Registry-Datenobjekt registriert und ein Dokument gespeichert wird~~.[<=]

**5.1.1.2 Operation I\_Document\_Management::CrossGatewayQuery**

**A\_14450 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-Gateway Query**

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

**Tabelle 7: Tab\_Dokv\_16 - Operation Cross-Gateway Query**

Operation	<code>I_Document_Management::CrossGatewayQuery</code>
<b>Beschreibung</b>	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.
<b>Formatvorgaben</b>	SOAP Action: urn:ihe:iti:2007:CrossGatewayQuery
<b>Eingangsparameter</b>	

Name	Beschreibung	Typ	opt.
<b>Cross-Gateway Query Message</b>	Eingangsnachricht zur Suche nach Metadaten zu XDS.b-Objekten	query:AdhocQueryRequest	n
<b>X-User Assertion</b>	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
<b>Ausgangsparameter</b>			
Name	Beschreibung	Typ	opt.
<b>Cross-Gateway Query Response Message</b>	Ausgangsnachricht zur Suche nach Metadaten zu XDS.b-Objekten	query:AdhocQueryResponse	n
<b>Technische Fehlermeldungen</b>			
<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	

## [&lt;=]

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

## 5.1.1.2.1 Umsetzung

**A\_14924-01 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe von Metadaten zu Policy Documents (Advanced Patient Privacy Consents) und damit verbundenen Associations/SubmissionSets**

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" DARF Metadaten zu Policy Documents (Advanced Patient Privacy Consents) gemäß der Anforderung [gemSpec\_DM\_ePA#A\_14961] und den damit verbundenen Associations und SubmissionSets NICHT zurückgeben bzw. MUSS diese aus der Antwortnachricht entfernen, falls diese den Anfragekriterien entsprechen.[<=]

**A\_14910 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-Gateway Query**

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

**A\_17184 - Komponente ePA-Dokumentenverwaltung – Suchanfragen über das Metadatenattribut DocumentEntry.title**

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

**A\_13585 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Cross-Gateway Query**

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor ein Registry-Datenobjekt zum Fachmodul ePA als XCA-Akteur "Initiating Gateway" zurückgegeben wird. Widerspricht die Suchergebnismenge ganz oder teilweise einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Suchergebnismenge dahingehend gefiltert werden, dass nur berechtigte Metadaten (d.h. Document Entries sowie Submission Sets) an den Document Consumer zurückgegeben werden. [`<=`]

**A\_18069 - Komponente ePA-Dokumentenverwaltung – Suche über Author Institution bei Cross-Gateway Query**

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

**A\_21131 - Komponente ePA-Dokumentenverwaltung – Rückgabe unscharfer Suchergebnisse für Cross-Gateway-Query**

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS bei der Ermittlung der Ergebnisse einer Cross-Gateway Query bei Auswertung der folgenden Queries und deren Suchparametern beim Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d.h. bezogen auf das jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht abweichende Ergebnisse zurückliefern können:

- Query "FindDocuments" und Query "FindDocumentsByTitle"
  - `$XDSDocumentEntryTitle`
  - `$XDSDocumentEntryAuthorInstitution`
  - `$XDSDocumentEntryAuthorPerson`
- Query "FindSubmissionSets"

- \$XDSSubmissionSetAuthorPerson

Dabei MUSS die Komponente ePA-Dokumentenverwaltung mindestens unscharfe Ergebnisse bezüglich Groß/Kleinschreibung unterstützen, also Groß/Kleinschreibung für die angegebenen Parameter der ausgewählten Query-Typen ignorieren.

[<=]

Das zur Ermittlung weiterer unscharfer Ergebnisse von der Dokumentenverwaltung einzusetzende Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu liefern, die ihm möglicherweise sonst wegen beispielsweise falscher Schreibweise eines Namens (z. B. "Meyer" vs. "Maier") vorenthalten worden wäre. Dabei sind Verfahren wie die Kölner Phonetik aber auch andere Mechanismen denkbar.

### 5.1.1.3 Operation I\_Document\_Management::RemoveDocuments (abgekündigt)

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

### A\_21183 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove Documents

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation I\_Document\_Management::RemoveDocuments gemäß der folgenden Signatur implementieren:

**Tabelle 8: Tab\_Dokv\_17 - Operation Remove Documents**

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

	Leistungserbringereinstitut ion		
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b> .
<b>Remove Documents Response Message</b>	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocumentsResponse_Message	n
<b>Technische Fehlermeldungen</b> <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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	

[<=]

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

#### 5.1.1.3.1 Umsetzung

#### **A\_21184 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Documents**

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

#### **5.1.1.4 Operation I\_Document\_Management::RemoveMetadata**

#### **A\_14489-02 - Komponente ePA-Dokumentenverwaltung – Signatur für RemoveMetadata**

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

**Tabelle 9: Tab\_Dokv\_17 - Operation RemoveMetadata**

<b>Operation</b>	<b>I_Document_Management::RemoveMetadata</b>
<b>Beschreibung</b>	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management::deleteDocuments</code> technisch um. Sie

	basiert auf den IHE ITI-Transaktionen "Remove Metadata" [ITI-62] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente, Ordner und/oder Associations eines Aktenkontos im ePA-Aktensystem zu löschen.		
<b>Formatvorgaben</b>	SOAP Action: urn:ihe:iti:2010>DeleteDocumentSet		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>Remove Documents Message</b>	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	xds>DeleteDocumentSet_Message	n
<b>X-User Assertion</b>	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>Remove Documents Response Message</b>	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	xds>DeleteDocumentSetResponse_Message	n
<b>Technische Fehlermeldungen</b>			
<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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	

[&lt;=]

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

5.1.1.4.1 Umsetzung

**A\_14908-02A\_14908-01 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Metadata**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS die Umsetzung der Operation `I_Document_Management::RemoveMetadata` gemäß der definierten Ablauflogik in [IHE-ITI-RMD#3.8662.4.1.2 und 3.8662.4.1.3 ] implementieren. [`<=`]

**A\_21710-01 - Komponente ePA-Dokumentenverwaltung – Kein Löschen von statischen Ordnern und Associations durch die LEI**

**A\_20633—Komponente ePA-Dokumentenverwaltung—Policy Enforcement für Remove Metadata**

Die Komponente ePA-Dokumentenverwaltung als `RMDXDS`-Akteur "Document Registry" MUSS ~~die registrierten und anwendbaren Zugriffsrichtliniensicherstellen, dass eine Löschanfrage einer Leistungserbringerinstitution grundsätzlich keine statischen Ordner und Associations aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Dokumentenverwaltung löschen darf.~~ Dies gilt nicht für nicht-statische Ordner, wie einen Mutterpass (`folderCode = mothersrecord`) oder Kinderuntersuchungsheft (`folderCode = childsrecord`). Die Komponente ePA-Dokumentenverwaltung MUSS bei Löschung eines Dokumentes die Assoziation zum Folder löschen. Anforderung A\_14822 durchsetzen, bevor ein Registry-Datenobjekt (und ein ggf. dazugehöriges Dokument) gelöscht wird. [`<=`]

**5.1.1.5 Operation `I_Document_Management::CrossGatewayRetrieve`**

**A\_14464 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-Gateway Retrieve**

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

**Tabelle 10: Tab\_Dokv\_18 - Operation Cross-Gateway Retrieve**

<b>Operation</b>	<b><code>I_Document_Management::CrossGatewayRetrieve</code></b>		
<b>Beschreibung</b>	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.		
<b>Formatvorgaben</b>	SOAP Action: urn:ihe:iti:2007:CrossGatewayRetrieve		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b>
<b>Cross-Gateway Retrieve Message</b>	Eingangsnachricht zum Abruf von Dokumenten	<code>xdsb:RetrieveDocumentSetRequest</code>	n

<b>X-User Assertion</b>	Authentication Assertion der authentifizierten Leistungserbringereinstitui	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b>
<b>Cross-Gateway Retrieve Response Message</b>	Ausgangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetResponse	n
<b>Technische Fehlermeldungen</b>			
<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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße der angefragten Dokumente übersteigt 250 MByte.	

[&lt;=]

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

#### 5.1.1.5.1 Umsetzung

##### **A\_14911 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-Gateway Retrieve**

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

##### **A\_16201 - Komponente ePA-Dokumentenverwaltung – Prüfung der zurückgegebenen Paketgröße**

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

[&lt;=]

##### **A\_14548-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Cross-Gateway Retrieve**

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

Anforderung A\_14822 durchsetzen, bevor ein Repository-Datenobjekt zum Fachmodul ePA als XCA-Akteur "Initiating Gateway" zurückgegeben wird. Bei einem Abruf von mehreren Dokumenten können einzelne Dokumente durch den zwischenzeitlichen Entzug einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für den Abruf berechtigt sein. Widerspricht ein abzurufendes Dokument einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum betreffenden Dokument einen `XSDocumentUniqueIdError`- Fehlercode enthalten (das Dokument wird nicht herausgegeben) und der Wert 4 des `EventOutcomeIndicators` im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein angefordertes Dokument nicht mehr verfügbar (d.h. es wurde gelöscht), MUSS gemäß IHE ITI der Fehlercode `XSDocumentUniqueIdError` zurückgegeben werden. [`<=`]

### 5.1.1.6 Operation

#### **I\_Document\_Management::RestrictedUpdateDocumentSet**

#### **(abgekündigt)**

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

#### **A\_21190 - Komponente ePA-Dokumentenverwaltung – Signatur für Restricted Update Document Set**

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

**Tabelle 11: Tab\_Dokv\_45 - Operation Restricted Update Document Set**

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

Name	Beschreibung	Typ	opt
<b>Update Responder Restricted Update Document Set</b>	Eingangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	lcm:SubmitObjectsRequest	n
<b>X-User Assertion</b>	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_149 27, A_15638]	n
<b>Ausgangsparameter</b>			
Name	Beschreibung	Typ	opt
<b>Update Responder Restricted Update Document Set Response</b>	Ausgangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	rs:RegistryResponse	n
<b>Technische Fehlermeldungen</b>			
<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	

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

#### 5.1.1.6.1 Umsetzung

### A\_21191 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Restricted Update Document Set

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF NICHT die Umsetzung der Operation `I_Document_Management::RestrictedUpdateDocumentSet` gemäß der

definierten Ablauflogik in [IHE-ITI-RMU#3.92.4.1.2 und 3.92.4.1.3] implementieren.  
[<=]

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

**A\_21192 - Komponente ePA-Dokumentenverwaltung – Fehler für Restricted Update Document Set**

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS beim Aufruf der Operation `I_Document_Management::RestrictedUpdateDocumentSet` immer den folgenden Fehler zurückliefern:

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

[<=]

**5.1.2 Schnittstelle I\_Document\_Management\_Insurant**

**A\_14478-01A\_14478 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I\_Document\_Management\_Insurant**

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

**Tabelle 12: Tab\_Dokv\_20 - Schnittstelle I\_Document\_Management\_Insurant**

Schnittstelle	I_Document_Management_Insurant	
<b>Version</b>	1.0.1	
<b>Namensraum</b>	urn:ihe:iti:xds-b:2007	
<b>Namensraumkürzel</b>	tns	
<b>Operationen</b>	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
	<a href="#">Remove Documents (abgekündigt)</a>	<a href="#">Löschen ein oder mehrerer Dokumente</a>
	<a href="#">Remove Metadata</a>	<a href="#">Löschen ein oder mehrerer Dokumente oder Folder</a>
	<a href="#">Restricted Update Document Set</a>	<a href="#">Aktualisierung von Metadaten (Kennzeichen)</a>
<b>WSDL</b>	<a href="#">DocumentManagementService.wsdl</a>	
<b>XML Schema</b>	<ul style="list-style-type: none"> <li>• <a href="#">PRPA_IN201301UV02.xsd</a></li> <li>• <a href="#">PRPA_IN201302UV02.xsd</a></li> <li>• <a href="#">PRPA_IN201304UV02.xsd</a></li> <li>• <a href="#">MCCI_IN000002UV01.xsd</a></li> <li>• <a href="#">query.xsd</a></li> <li>• <a href="#">rs.xsd</a></li> <li>• <a href="#">lcm.xsd</a></li> <li>• <a href="#">rim.xsd</a></li> <li>• <a href="#">XDS.b_DocumentRepository.xsd</a></li> </ul>	

[<=]

**A 14478 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I Document Management Insurant**

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

**Tabelle 13: Tab Dokv 20 - Schnittstelle I Document Management Insurant**

<b>Schnittstelle</b>	<b>I Document Management Insurant</b>	
<b>Version</b>	<a href="#">1.0.1</a>	
<b>Namensraum</b>	<a href="#">urn:ihe:iti:xds-b:2007</a>	
<b>Namensraumkürzel</b>	<a href="#">tns</a>	
<b>Operationen</b>	<b>Name</b>	<b>Beschreibung</b>
	<a href="#">Provide And Register DocumentSet-b</a>	<a href="#">Speichern und Registrieren ein oder mehrerer Dokumente in der Dokumentenverwaltung</a>

	<a href="#">Registry Stored Query</a>	<a href="#">Abfrage von Metadaten zu registrierten Dokumenten</a>
	<a href="#">Retrieve Document Set</a>	<a href="#">Anfrage von registrierten Dokumenten</a>
	Remove Documents	Löschen ein oder mehrerer Dokumente
<b>WSDL</b>	DocumentManagementService.wsdl	
<b>XML Schema</b>	<ul style="list-style-type: none"> <li>• PRPA_IN201301UV02.xsd</li> <li>• PRPA_IN201302UV02.xsd</li> <li>• PRPA_IN201304UV02.xsd</li> <li>• MCCI_IN000002UV01.xsd</li> <li>• query.xsd</li> <li>• rs.xsd</li> <li>• lcm.xsd</li> <li>• rim.xsd</li> <li>• XDS.b_DocumentRepository.xsd</li> </ul>	

[<=]

### 5.1.2.1 Operation

#### **I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b A\_14479 - Komponente ePA-Dokumentenverwaltung – Signatur für Provide And Register Document Set-b**

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b gemäß der folgenden Signatur implementieren:

**Tabelle 14: Tab\_Dokv\_21 - Operation Provide And Register Document Set-b**

<b>Operation</b>	<b>I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b</b>
<b>Beschreibung</b>	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.
<b>Formatvorgaben</b>	SOAP Action: urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b

<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b> .
<b>Provide And Register Document Set-b Message</b>	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	n
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b> .
<b>Provide And Register Document Set-b Response Message</b>	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	rs:RegistryResponse	n
<b>Technische Fehlermeldungen</b>			
<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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>MaxDocSizeExceeded</b>	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines einzelnen übermittelten Dokuments übersteigt 25 MByte.	
<b>MaxPkgSizeExceeded</b>	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

[&lt;=]

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

#### 5.1.2.1.1 Umsetzung

##### **A\_15056 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung von gemischten Dokumentenpaketen mit Policy Documents**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern in der Eingangsnachricht mehr als ein Dokument und Dokumenten-Metadaten gemäß der Anforderung [gemSpec\_DM\_ePA#A\_14961] für Policy Documents (Advanced Patient Privacy Consents) enthalten sind. [`<=`]

##### **A\_14912 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide And Register Document Set-b**

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

##### **A\_16442-01A\_16442 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] [sowie einem HTTP-Fehler 403 \(Fehlermeldung "Access Denied"\)](#) quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec\_Authentisierung\_Vers#A\_14109, A\_15631] entspricht. [`<=`]

##### **A\_21481-01 - Komponente ePA-Dokumentenverwaltung – Kein Einstellen von Ordnern und Associations**

[Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS das Registrieren und Speichern von Metadaten und Dokument\(en\) über die Schnittstelle `I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b\(\)` ablehnen und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder oder Associations enthalten sind. Ausnahme: nicht-statische Folder und Associations zu Kindern und Schwangerschaften \(Kategorien `childsrecord` und `mothersrecord`\).](#) [`<=`]

[Das Referenzieren bestehender Ordner ist davon nicht berührt, wie dies z. B. beim Einstellen von Dokumenten in Sammlungen der Fall ist \(z. B. Einstellen von Elternnotizen in die Sammlung Kinderuntersuchungsheft\).](#)

#### 5.1.2.2 Operation

##### **I\_Document\_Management\_Insurant::RegistryStoredQuery**

##### **A\_14480 - Komponente ePA-Dokumentenverwaltung – Signatur für Registry Stored Query**

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

Tabelle 15: Tab\_Dokv\_22 - Operation Registry Stored Query

<b>Operation</b>	<b>I_Document_Management_Insurant::RegistryStoredQuery</b>		
<b>Beschreibung</b>	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.		
<b>Formatvorgabe n</b>	SOAP Action: urn:ihe:iti:2007:RegistryStoredQuery		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b>
			.
<b>Registry Stored Query Message</b>	Eingangsnachricht zur Suche nach Metadaten zu XDS.b-Objekten	query:AdhocQueryRequest	n
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b>
			.
<b>Registry Stored Query Response Message</b>	Ausgangsnachricht zur Suche nach Metadaten zu XDS.b-Objekten	query:AdhocQueryResponse	n
<b>Technische Fehlermeldungen</b>			
<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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	

[<=]

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

#### 5.1.2.2.1 Umsetzung

##### **A\_14913 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Registry Stored Query**

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

Operation `I_Document_Management_Insurant::RegistryStoredQuery` gemäß der definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3 ] implementieren. [ $\leq$ ]

##### **A\_16436-02A\_16436 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] [sowie einem HTTP-Fehler 403 \(Fehlermeldung "Access Denied"\)](#) quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec\_Authentisierung\_Vers#A\_14109, A\_15631] entspricht.

[ $\leq$ ]

##### **A\_17185 - Komponente ePA-Dokumentenverwaltung – Suchanfragen über das Metadatenattribut DocumentEntry.title**

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

[ $\leq$ ]

##### **A\_14588 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Registry Stored Query**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor ein Registry-Datenobjekt zum ePA-Frontend des Versicherten (XDS-Akteur "Document Consumer") zurückgegeben wird.

[ $\leq$ ]

##### **A\_20532 - Komponente ePA-Dokumentenverwaltung – Zugriff auf SubmissionSets bei der Suche**

Die Komponente ePA-Dokumentenverwaltung MUSS einen Zugriff auf ein `SubmissionSet` im Rahmen der Operationen `I_Document_Management::CrossGatewayQuery` sowie `I_Document_Management_Insurant::RegistryStoredQuery` unterbinden, wenn der Zugreifende nicht mindestens für ein Dokument darin berechtigt ist.

[ $\leq$ ]

**A\_20533 - Komponente ePA-Dokumentenverwaltung – Zugriff auf Folder bei der Suche**

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

**A\_20534 - Komponente ePA-Dokumentenverwaltung – Zugriff auf Associations bei der Suche**

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

**A\_20535 - Komponente ePA-Dokumentenverwaltung – Fehlerbehandlung bei fehlender Berechtigung auf SubmissionSets, Folders und Associations bei der Suche**

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

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

[`<=`]

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

**A\_18070 - Komponente ePA-Dokumentenverwaltung – Suche über Author Institution bei Registry Stored Query**

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

**A\_21132 - Komponente ePA-Dokumentenverwaltung – Rückgabe unscharfer Suchergebnisse bei Registry Stored Query**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS bei der Ermittlung der Ergebnisse einer Registry Stored Query bei Auswertung der folgenden Queries und deren Suchparametern beim Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d.h. bezogen auf das jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht abweichende Ergebnisse zurückliefern können:

- Query "FindDocuments" und Query "FindDocumentsByTitle"
  - `$XDSDocumentEntryTitle`
  - `$XDSDocumentEntryAuthorInstitution`

- \$XDSDocumentEntryAuthorPersonuath
- Query "FindSubmissionSets"
- \$XDSSubmissionSetAuthorPerson

Dabei MUSS die Komponente ePA-Dokumentenverwaltung mindestens unscharfe Ergebnisse bezüglich Groß/Kleinschreibung unterstützen, also Groß/Kleinschreibung für die angegebenen Parameter der ausgewählten Query-Typen ignorieren.

[<=]

Das zur Ermittlung weiterer unscharfer Ergebnisse von der Dokumentenverwaltung einzusetzende Verfahren wird nicht vorgegeben. Ziel ist es, einem Client auch Treffer zu liefern, die ihm möglicherweise sonst wegen beispielsweise falscher Schreibweise eines Namens (z. B. "Meyer" vs. "Maier") vorenthalten worden wäre. Dabei sind Verfahren wie die Kölner Phonetik aber auch andere Mechanismen denkbar.

~~5.1.2.2.1.1 Suche mit simulierter Berechtigung~~

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

**5.1.2.3 Operation**

**I Document Management Insurant::RemoveDocuments (abgekündigt)**

Die Operation removeDocuments wird aus Kompatibilitätsgründen während der Migration von ePA 1 zu ePA 2 weiterhin optional angeboten. Die Operation removeMetadata löst die Operation removeDocuments ab.

**A 14488-02 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove Documents**

~~**A\_20224 – Komponente ePA-Dokumentenverwaltung – Suche mit simulierter Berechtigung: Anfrageformat**~~ Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS für alle Anfragen ("Stored Queries") den optionalen Parameter \$impersonatePolicy verarbeiten können. Die Komponente ePA-Dokumentenverwaltung prüft dazu die folgenden Bestimmungen KANN die Operation I Document Management Insurant::RemoveDocuments gemäß der folgenden Signatur implementieren:

- ~~• Der Parameter wird als Slot mit dem Namen impersonatePolicy kodiert. Tabelle 16: Tab Dokv 23 - Operation RemoveDocuments~~
- ~~• Der Parameter MUSS eine vollständige Base Policy für eine LEI (gemäß 9.3) oder eines Kostenträgers (gemäß 9.4) enthalten.~~
- ~~• Der Wert (die XML-Policy) MUSS Base64 kodiert im Datentyp string gemäß [IHE-ITI-TF3] abgelegt werden~~
- ~~• Der Parameter (sofern gesendet) MUSS immer die Multiplizität 1 besitzen.~~
- ~~• Wenn der Parameter nicht genutzt wird, dann DARF der entsprechende Slot nicht gesendet werden (d. h. es darf nicht stattdessen ein leerer Wert gesendet werden).~~

{<=>}

<u>Operation</u>	<u>I Document Management Insurant::RemoveDocuments</u>
------------------	--

<b>Beschreibung</b>	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I Document Management Insurant::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 im ePA-Aktensystem zu löschen.		
<b>Formatvorgaben</b>	SOAP Action: <code>urn:ihe:iti:2017:RemoveDocuments</code>		
<b><u>Eingangsparameter</u></b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b>
			▪
<b>Remove Documents Message</b>	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	<code>rmc:RemoveDocuments Message</code>	<u>n</u>
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec Authentisierung Vers#A 14 109, A 15631]	<u>n</u>
<b><u>Ausgangsparameter</u></b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b>
			▪
<b>Remove Documents Response Message</b>	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	<code>rmc:RemoveDocumentsResponse Message</code>	<u>n</u>
<b><u>Technische Fehlermeldungen</u></b> <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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	

--	--	--

[<=]

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

~~**A\_20227 – Komponente ePA-Dokumentenverwaltung – Suche mit simulierter Berechtigung: Umsetzung**~~

Die in A\_20224 definierte Suche MUSS wie folgt umgesetzt werden:

- ~~• Wenn die in A\_20224 genannten Bestimmungen nicht erfüllt sind, MUSS die Komponente ePA-Dokumentenverwaltung einen Fehler zurückgeben (ResponseStatusType:Failure).~~
- ~~• Ansonsten gelten folgende Bestimmungen:~~
  - ~~• Die Komponente ePA-Dokumentenverwaltung MUSS die im Base64-Format enthaltene Policy dekodieren.~~
  - ~~• Die Komponente ePA-Dokumentenverwaltung DARF das Policy-Dokument NICHT in der Dokumentenverwaltung hinterlegen. Sie wird also für andere Anfragen an die Schnittstellen der Dokumentenverwaltung nicht beachtet.~~
  - ~~• Die Komponente ePA-Dokumentenverwaltung DARF NICHT ein anderes (etwaig hinterlegtes) Base-Policy-Dokument für dieselbe LEI oder KTR im Rahmen dieser Suche beachten.~~
  - ~~• Die Komponente ePA-Dokumentenverwaltung MUSS die Klartextpolicy gemäß 5.4.6 behandeln und bei erfolgreicher Zugriffskontrollprüfung ("Permit") die Suche wie in 5.1.2.2 beschrieben unter Beachtung der Policy umsetzen.~~

~~**5.1.2.35.1.2.4 {<=}**~~

~~**5.1.2.45.1.2.5 Operation**~~

~~**I\_Document\_Management\_Insurant::RemoveMetadata**~~

~~**A\_14488-01 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove Metadata**~~

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

~~I\_Document\_Management\_Insurant::RemoveMetadata~~ gemäß der folgenden Signatur implementieren:

**Tabelle 17: Tab\_Dokv\_23 - Operation RemoveMetadata**

Operation	I_Document_Management_Insurant::RemoveMetadata
<b>Beschreibung</b>	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::deleteDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove Metadata" [ITI-62] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente im ePA-Aktensystem zu löschen.

<b>Formatvorgabe n</b>	SOAP Action: urn:ihe:iti:2010>DeleteDocumentSet		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b> .
<b>Remove Metadata Message</b>	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	xds>DeleteDocumentSet_Message	n
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b> .
<b>Remove Metadata Response Message</b>	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	xds>DeleteDocumentSetResponse_Message	n
<b>Technische Fehlermeldungen</b>			
<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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	

## [&lt;=]

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

[5.1.2.4.15.1.2.5.1 Umsetzung](#)

### [A\\_14909-03A\\_14909-01](#) - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Metadata

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document RepositoryRegistry" MUSS die Umsetzung der

Operation `I_Document_Management_Insurant::RemoveMetadata` gemäß der definierten Ablauflogik in [IHE-ITI-RMD#3.8662.4.1.2 und 3.8662.4.1.3 ] implementieren. [`<=`]

**A\_16437-03A\_16437-01 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document [RepositoryRegistry](#)" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] [sowie einem HTTP-Fehler 403 \(Fehlermeldung "Access Denied"\)](#) quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec\_Authentisierung\_Vers#A\_14109, A\_15631] entspricht. [`<=`]

**A\_21696-01 - Komponente ePA-Dokumentenverwaltung – Kein Löschen von statischen Ordnern und Associations durch FdV**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS sicherstellen, dass eine Löschanfrage eines ePA-FdV grundsätzlich keine statischen Ordner und Associations aus der Dokumentenverwaltung löschen darf. Dies gilt nicht für nicht-statische Ordner, wie einen Mutterpass (folderCode = mothersrecord) oder Kinderuntersuchungsheft (folderCode = childsrecord). Die Komponente ePA-Dokumentenverwaltung MUSS bei Löschung eines Dokumentes die Assoziation zum Folder löschen.

[`<=`]

**5.1.2.55.1.2.6 Operation**

**`I_Document_Management_Insurant::RetrieveDocumentSet`**

**A\_14481 - Komponente ePA-Dokumentenverwaltung – Signatur für Retrieve Document Set**

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

**Tabelle 18: Tab\_Dokv\_24 - Operation Retrieve Document Set**

<b>Operation</b>	<b><code>I_Document_Management_Insurant::RetrieveDocumentSet</code></b>		
<b>Beschreibung</b>	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management_Insurant::getDocuments</code> 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.		
<b>Formatvorgaben</b>	SOAP Action: urn:ihe:iti:2007:RetrieveDocumentSet		
<b><i>Eingangsparameter</i></b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b> .

<b>Retrieve Document Set Message</b>	Eingangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetRequest	n
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b>
<b>Retrieve Document Set Response Message</b>	Ausgangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetResponse	n
<b>Technische Fehlermeldungen</b>			
<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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>MaxPkgSizeExceeded</b>	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße der angefragten Dokumente übersteigt 250 MByte.	

[&lt;=]

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

#### [5.1.2.5-15.1.2.6.1](#) Umsetzung

### **A\_14914 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Retrieve Document Set**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Umsetzung der

Operation `I_Document_Management_Insurant::RetrieveDocumentSet` gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3] und [IHE-ITI-TF2b#3.43.4.2.2 und 3.43.4.2.3] implementieren. [<=]

**A\_16443-01A\_16443 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] [sowie einem HTTP-Fehler 403 \(Fehlermeldung "Access Denied"\)](#) quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec\_Authentisierung\_Vers#A\_14109, A\_15631] entspricht.  
[<=]

**A\_16200 - Komponente ePA-Dokumentenverwaltung – Prüfung der zurückgegebenen Paketgröße**

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

**A\_14589 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Retrieve Document Set**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor ein Repository-Datenobjekt zum ePA-Frontend des Versicherten als XDS-Akteur "Document Consumer" zurückgegeben wird. Ist ein abzurufendes Dokument nicht mehr verfügbar, MUSS gemäß IHE TF ITI der FehlercodeXSDSDocumentUniqueIdError zurückgegeben werden.

[<=]

**5-1-2-65.1.2.7 Operation**

**I\_Document\_Management\_Insurant::RestrictedUpdateDocumentSet**

**A\_15057-02A\_15057-01 - Komponente ePA-Dokumentenverwaltung – Signatur für Restricted Update Document Set**

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation I\_Document\_Management\_Insurant::RestrictedUpdateDocumentSet gemäß der folgenden Signatur implementieren:

**Tabelle 19: Tab\_Dokv\_19 - Operation RestrictedUpdateDocumentSet**

Operation	I_Document_Management_Insurant::RestrictedUpdateDocumentSet
<b>Beschreibung</b>	<p>Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::updateMetadata technisch um. Sie basiert auf den IHE ITI-Transaktionen "Restricted Update Document Set" [ITI-92] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, Metadaten zu Dokumenten zu ändern.</p> <p>Für Änderungen an der Vertraulichkeitsstufe von Dokumenten werden im documentEntry.confidentialityCode die Werte "normal", "restricted" oder "very restricted" mit derupdateMetadata Operation umgesetzt. Andere Änderungen sind mit dieser Operation nicht möglich.</p>

<b>Formatvorgaben</b>	SOAP Action: urn:ihe:iti:2018:RestrictedUpdateDocumentSet		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>Update Responder Restricted Update Document Set</b>	Eingangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	lcm:SubmitObjectsRequest	n
<b>X-User Assertion</b>	Authentication Assertion <u>der-des</u> authentifizierten <u>Leistungserbringerinstitution</u> <u>Ver</u> <u>sicherten</u> <u>oder</u> <u>des</u> <u>Vertreters</u>	<a href="#">SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]</a> <a href="#">SAML 2.0 Assertion gemäß gemSpec Authentisierung Vers# A_14109, A_15631</a>	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>Update Responder Restricted Update Document Set Response</b>	Ausgangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	rs:RegistryResponse	n
<b>Technische Fehlermeldungen</b>			
<i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] bzw. [IHE-ITI-RMU#4.2.4], und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			

**[<=]**

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

### 5.1.2.6.15.1.2.7.1 Umsetzung

#### **A\_15082 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung der Metadaten aus ITI Document Sharing-Profilen durch RMU-Akteur "Update Responder"**

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS die übermittelten `DocumentEntry`-Metadaten der eingehenden Nachricht dahingehend prüfen, dass gegenüber den Bestandsdaten das Metadatenattribut `documentEntry.confidentialityCode` konform zu den Nutzungsvorgaben in [gemSpec\_DM\_ePA#A\_14760] geändert ist. Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS das Aktualisieren dieses Metadatenattributs ablehnen und mit einem `XDSRepositoryMetadataError` quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. [≤]

#### **A\_15083-01 - Komponente ePA-Dokumentenverwaltung – Prüfung auf ausschließliche Aktualisierung des Metadatenattributs `documentEntry.confidentialityCode`**

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

#### **~~A\_15061-02A\_15061-01~~ - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Restricted Update Document Set**

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

- ~~Ein neues `SubmissionSet`~~
- ~~Einen `DocumentEntry`, der identisch mit dem zu aktualisierenden `DocumentEntry` identisch ist (inklusive `entryUUID`) und sich nur im `confidentialityCode` unterscheidet~~
- ~~Eine SS-DE HasMember-Association, die das `SubmissionSet` mit dem geschickten `DocumentEntry` verbindet~~
- ~~Die „lid“ (`logicalID`) DARF NICHT gesendet werden.~~

- [Der Slot "PreviousVersion" MUSS immer mit dem Wert "1" gesendet werden.](#)
- Der Slot „associationPropagation“ MUSS auf „no“ gesetzt werden.

Die Komponente ePA-Dokumentenverwaltung DARF die gesendete Association und das neue SubmissionSet NICHT dauerhaft speichern.

[<=]

**[A\\_21533 - Komponente ePA-Dokumentenverwaltung – Kein Anlegen von Versionen für Restricted Update Document Set](#)**

[Die Dokumentenverwaltung DARF eine echte Versionierung NICHT umsetzen, d. h sie DARF den alten DocumentEntry NICHT speichern. Insbesondere DARF die Dokumentenverwaltung DocumentEntry.version NICHT anlegen und verwalten. \[<=\]](#)

[Entsprechend besitzt der Wert standardmäßig gemäß \[IHE-ITI-RMU\] immer den impliziten Wert 1.](#)

**[A\\_21783 - Komponente ePA-Dokumentenverwaltung - Vererbung der Vertraulichkeitsstufe](#)**

[Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS den neu gesetzten documentEntry.confidentialityCode ebenfalls auf alle mit dem geänderten Dokument assoziierten Dokumente setzen. \[<=\]{<=<=}](#)

**A\_15080-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Restricted Update Document Set**

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor Metadaten einer oder mehrerer Dokumente aktualisiert werden. Beim Aktualisieren der Metadaten durch das ePA-Frontend des Versicherten können einzelne Dokumente bzw. Metadaten durch den zwischenzeitlichen Entzug einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für die Aktualisierung berechtigt sein. Widerspricht ein Dokument bzw. die damit assoziierten Metadaten einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum betreffenden Dokument einenXSDDocumentUniqueIdError-Fehlercode enthalten und der Wert 4 des EventOutcomeIndicators im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein zu aktualisierendes Dokument bzw. Metadaten nicht mehr verfügbar, MUSS gemäß IHE TF ITI der Fehlercode XSDDocumentUniqueIdError zurückgegeben werden.

[<=]

**5.1.3 Schnittstelle I\_Document\_Management\_Insurance**

**A\_17438 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I\_Document\_Management\_Insurance**

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

**Tabelle 20: Tab\_Dokv\_36 - Schnittstelle I\_Document\_Management\_Insurance**

Schnittstelle	I_Document_Management_Insurance
<b>Version</b>	1.0.1

<b>Namensraum</b>	urn:ihe:iti:xds-b:2007	
<b>Namensraumkürzel</b>	tns	
<b>Operationen</b>	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente in der Dokumentenverwaltung
<b>WSDL</b>	DocumentManagementService.wsdl	
<b>XML Schema</b>	<ul style="list-style-type: none"> <li>• PRPA_IN201301UV02.xsd</li> <li>• PRPA_IN201302UV02.xsd</li> <li>• PRPA_IN201304UV02.xsd</li> <li>• MCCI_IN000002UV01.xsd</li> <li>• query.xsd</li> <li>• rs.xsd</li> <li>• lcm.xsd</li> <li>• rim.xsd</li> <li>• XDS.b_DocumentRepository.xsd</li> </ul>	

[&lt;=]

### 5.1.3.1 Operation

#### **I\_Document\_Management\_Insurance::ProvideAndRegisterDocumentSet-b**

#### **A\_17439 - Komponente ePA-Dokumentenverwaltung – Signatur für Provide And Register Document Set-b**

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

I\_Document\_Management\_Insurance::ProvideAndRegisterDocumentSet-b gemäß der folgenden Signatur implementieren:

**Tabelle 21: Tab\_Dokv\_37 - Operation Provide And Register Document Set-b**

<b>Operation</b>	<b>I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b</b>
<b>Beschreibung</b>	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.

<b>Formatvorgaben</b>	SOAP Action: urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b> .
<b>Provide And Register Document Set-b Message</b>	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	n
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Kostenträgers	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA_KTR_Consumer #A_17253, A_17254]	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b> .
<b>Provide And Register Document Set-b Response Message</b>	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	rs:RegistryResponse	n
<b>Technische Fehlermeldungen</b>			
<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>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>MaxDocSizeExceeded</b>	Die max. Dokumentgröße wurde überschritten.	Die Größe mindestens eines einzelnen übermittelten Dokuments übersteigt 25 MByte.	
<b>MaxPkgSizeExceeded</b>	Die max. Paketgröße	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

	wurde überschritten.	
--	----------------------	--

[<=]

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

#### 5.1.3.1.1 Umsetzung

##### **A\_17443 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide And Register Document Set-b**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Umsetzung der

Operation `I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b` gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3 ] und [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3 ] implementieren.

[<=]

##### **A\_17444-01A\_17444 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] [sowie einem HTTP-Fehler 403 \(Fehlermeldung "Access Denied"\)](#) quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec\_FM\_ePA\_KTR\_Consumer#A\_17253, A\_17254] entspricht. [<=]

##### **A\_21482 - Komponente ePA-Dokumentenverwaltung – Kein Einstellen von Ordnern**

[Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS das Registrieren und Speichern von Metadaten und Dokument\(en\) über die Schnittstelle `I\_Document\_Management\_Insurance::ProvideAndRegisterDocumentSet-b\(\)` ablehnen und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder enthalten sind.](#)

[<=]

## 5.1.4 Anforderungen an Sammlungstypen

### ~~A\_20578 – Komponente ePA-Dokumentenverwaltung – Einstellen von Dokumenten in Sammlungen des Typs "mixed"~~

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

### ~~A\_20707-02 - Komponente ePA-Dokumentenverwaltung – Keine unpassenden Dokumente in nicht-statische Ordner~~

~~A\_20627 – Komponente ePA-Dokumentenverwaltung – Kein Ordner für Sammlungstyp "mixed" ohne entsprechendes strukturiertes Dokument~~  
 Die Komponente ePA-Dokumentenverwaltung MUSS das ~~Anlegen eines Folders für den Verwaltungstyp "mixed" mit dem Fehler `XDSRegistryMetadataError` unterbinden, wenn Einstellen von Dokumenten in nicht in derselben Operation auch mindestens ein entsprechendes Sammlungstyp-spezifisches strukturiertes Dokument (-statische Ordner gemäß [gemSpec\\_DM\\_ePA#A\\_20577](#)) eingestellt wird und die Operation mit dem Fehler `ACCESS_DENIED` abbrechen, wenn der Zugreifende nicht die Berechtigung besitzt, den Ordner und alle für den vorgesehenen Ordner mitgesendeten Dokumente anzulegen. [~~≤~~]~~

### ~~A\_20707 – Komponente ePA-Dokumentenverwaltung – Keine unpassenden Dokumente in Ordner für Sammlungstyp "mixed"~~

~~Die Komponente ePA-Dokumentenverwaltung MUSS das Einstellen von Dokumenten in einen Ordner für Sammlungstyp "mixed" mit dem Fehler `ACCESS_DENIED` abbrechen, wenn das Dokument nicht einem dem entsprechende Sammlungstyp zugeordneten strukturierten Dokumententyp (gemäß [gemSpec\\_DM\\_ePA#A\\_20577](#)) entspricht. [~~≤~~]~~

### ~~A\_20579-01 - Komponente ePA-Dokumentenverwaltung – Löschen von Ordnern~~

~~A\_20579 – Komponente ePA-Dokumentenverwaltung – Löschen von Ordnern des Sammlungstyp "mixed"~~  
 Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS beim Löschen des letzten Dokuments aus `Requests`, die darauf abzielen, einen statischen Folder direkt zu löschen, mit einem `XDSRegistryMetadataError` ablehnen. [~~≤~~ Ordner für Sammlungstyp "mixed" sicherstellen, dass der Ordner automatisch durch die "Document Registry" mitgelöscht wird. [~~≤~~]

### ~~A\_20581-01~~ ~~A\_20581 - Komponente ePA-Dokumentenverwaltung – Löschen von Dokumenten aus Sammlungen der Typen "mixed" und "uniform"~~

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

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

## 5.2 Aktenkontoverwaltung

### 5.2.1 Schnittstelle I\_Account\_Management\_Insurant

Diese Schnittstelle setzt einen Teil der in [gemSysL\_ePA] definierten Schnittstelle I\_Account\_Management\_Insurant technisch um. Die Operationen der Schnittstelle werden vom Verarbeitungskontext über den sicheren Kanal zum ePA-Frontend des Versicherten bereitgestellt.

#### A\_14804-01 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I\_Account\_Management\_Insurant

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

**Tabelle 22: Tab\_Dokv\_25 - Schnittstelle I\_Account\_Management\_Insurant**

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

[<=]

### 5.2.1.1 Operation I\_Account\_Management\_Insurant::SuspendAccount

#### A\_14805 - Komponente ePA-Dokumentenverwaltung – Signatur für

#### I\_Account\_Management\_Insurant::SuspendAccount

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

I\_Account\_Management\_Insurant::SuspendAccount gemäß der folgenden Signatur implementieren:

**Tabelle 23: Tab\_Dokv\_26 - Operation Suspend Account**

Operation	I_Account_Management_Insurant::SuspendAccount		
<b>Beschreibung</b>	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.		
<b>Formatvorgaben</b>	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/SuspendAccount		
<b>Eingangsparameter</b>			
Name	Beschreibung	Typ	opt.
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten als Inhaber der Akte	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109, A_15631]	n
<b>Ausgangsparameter</b>			
<b>Package URL</b>	URL, über die das erzeugte Exportpaket vom neuen Anbieter ePA-Aktensystem geladen werden kann	URL mit Prozentkodierung	n
<b>Technische Fehlermeldungen</b>			
Name	Fehlertext	Details	

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

[&lt;=]

#### 5.2.1.1.1 Umsetzung

##### **A\_15530-02 - Komponente ePA-Dokumentenverwaltung – I\_Account\_Management\_Insurant über sicheren Kanal**

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

Die folgende Anforderung bewirkt, dass nur der Versicherte als Inhaber einer Akte im Zustand "DISMISSED" ~~die Operation~~ oder "START MIGRATION" die Operation `I_Account_Management_Insurant::SuspendAccount` ausführen kann.

##### **A\_15062-03A\_15062 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Suspend Account**

Die Komponente ePA-Dokumentenverwaltung MUSS ~~für die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor die Ausführung dieser~~ Operation `I_Account_Management_Insurant::SuspendAccount` ~~ausgeführt wird. Bei einer negativen Autorisierungsentscheidung prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist und ob der RecordState der KeyChain des Versicherten den Wert DISMISSED, START MIGRATION oder SUSPENDED besitzt. Liegt dieser Fall nicht vor,~~ MUSS die Nachricht mit dem SOAP-Fault ACCESS\_DENIED-Fehlercode ~~sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231]~~ quittiert werden.

[&lt;=]

### A\_21753-01 - Komponente ePA-Dokumentenverwaltung – Erneuter Aufruf von SuspendAccount

Erfolgt der Aufruf von `SuspendAccount`, wenn die Erstellung des Exportpakets noch aktiv ist oder erfolgreich beendet wurde (Aufruf von `SuspendAccount` ist schon zuvor erfolgt.), MUSS die Komponente ePA-Dokumentenverwaltung die gleiche PackageURL wie beim ursprünglichen Aufruf von `SuspendAccount` als Ergebnis liefern. Die ePA-Dokumentenverwaltung unterbricht die ggfs. noch aktive Erstellung des Exportpakets nicht, sondern führt diese fort. [ <= ]

### **A\_14885-01 - Komponente ePA-Dokumentenverwaltung – Exportpaket des Aktenkontos erstellen**

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

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

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

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

- die ZIP-Datei außerhalb des Verarbeitungskontextes persistieren,
- die ZIP-Datei im Zuge des Exports mit dem `ContextKey` gemäß [gemSpec\_Krypt#GS-A\_5016] verschlüsseln, so dass sichergestellt ist, dass nur entsprechend verschlüsselte Daten außerhalb des Verarbeitungskontextes auftreten können,
- die § 291a-Protokolldaten innerhalb der ZIP-Datei unter dem Dateinamen `PROTO291.XML` mit der folgenden Struktur
 

```
<?xml version="1.0" encoding="UTF-8" xmlns=""?>
<AuditMessagesxmlns:phrext="http://ws.gematik.de/fa/phrext/v1.0">
  <AuditMessages>
    <phrext:AuditMessage>...</phrext:AuditMessage>
    <phrext:AuditMessage>...</phrext:AuditMessage>
  </AuditMessages>
```

 abgelegt werden, sowie
- die ZIP-Datei zum Abruf für berechtigte andere Anbieter ePA-Aktensystem verfügbar machen.

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

### **A\_15012 - Komponente ePA-Dokumentenverwaltung – Korrektheit des Exportpakets sicherstellen**

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

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

**A\_15005 - Komponente ePA-Dokumentenverwaltung – Kein Aktenzugriff während des Exports der Daten**

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

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

Da der Anbieterwechsel als ein zusammenhängender Vorgang aus Sicht des ePA-Frontend des Versicherten ablaufen soll, der Export und anschließende Import je nach Größe des Exportpakets jedoch einige Zeit in Anspruch nehmen können, soll der Vorgang im Backend asynchron ablaufen können. Die folgende Anforderung regelt dies für den Export. Die Anforderung A\_15623 im nächsten Abschnitt regelt die asynchrone Verarbeitung des Imports.

**A\_15622 - Komponente ePA-Dokumentenverwaltung – Asynchroner Export**

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

**A\_16076 - Komponente ePA-Dokumentenverwaltung – Frist für Bereitstellung des Exportpakets**

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

**5.2.1.2 Operation I\_Account\_Management\_Insurant::ResumeAccount**

**A\_14807 - Komponente ePA-Dokumentenverwaltung – Signatur für I\_Account\_Management\_Insurant::ResumeAccount**

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

**Tabelle 24: Tab\_Dokv\_27 - Operation Resume Account**

Operation	<code>I_Account_Management_Insurant::ResumeAccount</code>
<b>Beschreibung</b>	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Account_Management_Insurant::ResumeAccount</code> technisch um. Mit dieser Operation wird das Paket mit den Daten aus der Akte eines Versicherten beim vorhergehenden Anbieter ePA-Aktensystem bezogen und importiert.
<b>Formatvorgaben</b>	SOAP Action: <code>http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.</code>

	0/ResumeAccount		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>Package URL</b>	URL, über die das vom vorhergehenden Anbieter ePA-Aktensystem erzeugte Exportpaket geladen werden kann	URL mit Prozentkodierung	n
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten des Versicherten als Inhaber der Akte	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers# A_14109, A_15631]	n
<b>Technische Fehlermeldungen</b>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>INTERNAL_ERROR</b>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
<b>ASSERTION_INVALID</b>	Die übergebene Authentication Assertion ist ungültig.	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
<b>SYNTAX_ERROR</b>	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
<b>ACCESS_DENIED</b>	Der Zugriff für diese Operation konnte nicht gewährt werden.		

[&lt;=]

#### 5.2.1.2.1 Umsetzung

Die Ausführung der Operation `I_Account_Management_Insurant::ResumeAccount` setzt voraus, dass der Versicherte mittels seines ePA-Frontend des Versicherten einen sicheren Kanal zum Verarbeitungskontext aufgebaut hat und diesen mittels der Operation `I_Document_Management_Connect::OpenContext` kryptographisch aktiviert hat. Darüber hinaus muss die Operation `I_Account_Management_Insurant::ResumeAccount` aufgerufen werden, bevor weitere Operationen am Verarbeitungskontext ausgeführt

werden können. Sie muss mit Fehler terminieren, wenn sie für ein Aktenkonto bereits vorher erfolgreich ausgeführt wurde.

#### **A\_15526-01A\_15526 - Komponente ePA-Dokumentenverwaltung – Voraussetzungen für die Ausführung von Resume Account**

Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Operation `I_Account_Management_Insurant::ResumeAccount` nur ausgeführt wird, wenn die Akte des Versicherten im Zustand REGISTERED FOR MIGRATION oder DL IN PROGRESS ist und aktuell kein Datenimport aktiv ist (resumeAccount läuft bereits). [~~=der Verarbeitungskontext eines für einen Anbieterwechsel mit Übernahme der Aktendaten registriertes Aktenkonto erstmalig durch den Versicherten geöffnet wurde.~~] [~~=~~]

#### **A\_15568-02A\_15568 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Resume Account**

Die Komponente ePA-Dokumentenverwaltung MUSS für die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor die Ausführung dieser Operation `I_Account_Management_Insurant::ResumeAccount` ~~ausgeführt wird. Bei einer negativen Autorisierungsentscheidungsprüfung, ob der zugreifende Nutzer der Akteninhaber selbst ist und für seine OwnerKVNR ein AuthorizationKey existiert . Liegt dieser Fall nicht vor,~~ MUSS die Nachricht mit dem `SOAP-Fault ACCESS_DENIED`-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [~~=~~]

#### **A\_15013-01A\_15013 - ePA-Aktensystem – Download des Exportpakets**

Das ePA-Aktensystem MUSS nach Eingang des Requests `I_Account_Management_Insurant::ResumeAccount` das mittels des Aufrufparameters `PackageURL` referenzierte Exportpaket beim vorhergehenden Anbieter ePA-Aktensystem des Versicherten abrufen und für den Import durch den Verarbeitungskontext der ePA-Dokumentenverwaltung verfügbar machen sowie den Zustand RecordState der KeyChain des Versicherten auf den Wert DL IN PROGRESS setzen. [~~=~~;~~=~~]

#### **A\_21752 - ePA-Aktensystem – Erfolgreicher Download des Exportpakets**

Das ePA-Aktensystem MUSS nach erfolgreichem Download und Inegritätsprüfung des Exportpakets den Zustand RecordState der KeyChain des Versicherten auf den Wert READY FOR IMPORT setzen und die Verarbeitung mit dem Import des Exportpakets fortsetzen. Ist die Integritätsprüfung nicht erfolgreich, ist der Zustand RecordState der KeyChain des Versicherten auf den Wert REGISTERED FOR MIGRATION zu setzen und der Verarbeitungs-kontext zu schließen sowie der Versicherten über das Fehlschlagen des Downloads zu informieren. [~~=~~]

#### **A\_14905-01A\_14905 - Komponente ePA-Dokumentenverwaltung – Import des Exportpakets des vorhergehenden Aktenkontos**

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

- das Exportpaket mittels des `ContextKey` entschlüsseln und
- die Struktur des Exportpakets auf Übereinstimmung mit den Festlegungen aus Anforderung A\_14885 prüfen.

~~[<=]~~ Kann das Exportpaket nicht entschlüsselt werden oder ist die Struktur des Exportpakets fehlerhaft ist der Zustand RecordState der KeyChain des Versicherten auf den Wert REGISTERED FOR MIGRATION zu setzen und der Verarbeitungs-kontext zu

[schließen sowie der Versicherten über das Fehlschlagen des Imports zu informieren.](#)  
[<=]

#### **A\_15596 - Komponente ePA-Dokumentenverwaltung – Ersetzen der Home Community ID**

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

#### **A\_15623 - Komponente ePA-Dokumentenverwaltung – Asynchroner Import**

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

I\_Account\_Management\_Insurant::ResumeAccount unmittelbar nach dem Aufruf an den Client zurückgeben, unabhängig davon, wie lange der Erhalt und Import des Exportpakets dauert.[<=]

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

I\_Account\_Management\_Insurant::ResumeAccount beim neuen Anbieter ausgelöst hat.

#### **A\_15624 - Komponente ePA-Dokumentenverwaltung – Abfrage auf Verfügbarkeit des Exportpakets**

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

#### **A\_15625 - Komponente ePA-Dokumentenverwaltung – Kein Aktenzugriff während des Imports der Daten**

Die Komponente ePA-Dokumentenverwaltung MUSS während der Ausführung der Operation I\_Account\_Management\_Insurant::ResumeAccount für ein Aktenkonto alle Operationen mit Fehlermeldung "Aktenkonto aufgrund einer andauernden Datenmigration vorübergehend nicht erreichbar" ablehnen.[<=]

#### **A\_16077 - Komponente ePA-Dokumentenverwaltung – Frist für den Import des Exportpakets**

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

[<=]

#### **A\_17845 - Komponente ePA-Dokumentenverwaltung – Offener Verarbeitungskontext während der Verarbeitung des Exportpakets**

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS den für die Operation I\_Account\_Management\_Insurant::ResumeAccount geöffneten Verarbeitungskontext so lange geöffnet lassen, bis der Abruf des Exportpakets beim alten Anbieter erfolgt ist und die Verarbeitung der Daten des Exportpakets durch diesen

Verarbeitungskontext abgeschlossen ist, jedoch maximal drei Tage, falls kein Exportpaket abgerufen werden kann.

[<=]

Wird der Kontext nach dem Download geschlossen (Absturz, Wartungsarbeiten o.Ä.) muss der eigentliche Import des Exportpakets unmittelbar nach dem nächsten openContext erfolgen.

**A 21754 - Komponente ePA-Dokumentenverwaltung – Aktivierung Import des Exportpakets**

Befindet sich der RecordState der KeyChain des Versicherten im Zustand READY\_FOR\_IMPORT und ist kein Importvorgang aktiv MUSS die Komponente ePA-Dokumentenverwaltung beim Öffnen des Verarbeitungskontexts den Import des bereits heruntergeladenen Migrationspakets anstoßen und alle folgenden Operationsaufrufe entsprechend A 15625 mit der Fehlermeldung "Aktenkonto aufgrund einer andauernden Datenmigration vorübergehend nicht erreichbar" ablehnen. [<=]

**A 21241-01A-21241 - Komponente ePA-Dokumentenverwaltung - Zustandswechsel nach erfolgreichem Import des Exportpakets**

Die Komponente Dokumentenverwaltung MUSS nach dem erfolgreichem Import des Exportpakets durch die Dokumentenverwaltung in der Komponente Autorisierung den Zustand RecordState der KeyChain des Versicherten von REGISTEREDREADY\_FOR\_MIGRATIONIMPORT auf den Wert ACTIVATED setzen, wenn die initiale Schlüssel hinterlegung für den Versicherten bereits erfolgte. [<=]

**5.2.1.3 Operation I\_Account\_Management\_Insurant::GetAuditEvents**

**A 14490-06A-14490-04 - Komponente ePA-Dokumentenverwaltung – Signatur für Get Audit Events**

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation I\_Account\_Management\_Insurant::GetAuditEvents gemäß der folgenden Signatur implementieren:

**Tabelle 25: Tab\_Dokv\_28 - Operation Get Audit Events**

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

<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
<del>AuditLog-PageSize</del>	Umsetzung gemäß [gemSpecAktensystem#gemSpecAktensystem#5.2.1.1]	Integer (> 0)	y
<del>AuditLog-PageNumber</del>	Umsetzung gemäß [gemSpecAktensystem#gemSpecAktensystem#5.2.1.1]	Integer (> 0)	y
<del>AuditLog-LastDay</del>	Umsetzung gemäß [gemSpecAktensystem#gemSpecAktensystem#5.2.1.1]	YYYY-MM-DD	y
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<del>AuditEventList-AuditMessage</del>	Liste der Zugriffsprotokolleinträge	<del>php::</del> AuditMessage [0..*]	n
<del>AuditLog-PageSize</del>	Umsetzung gemäß [gemSpecAktensystem#gemSpecAktensystem#5.2.1.1]	Integer (> 0)	y
<del>AuditLog-PageNumber</del>	Umsetzung gemäß [gemSpecAktensystem#gemSpecAktensystem#5.2.1.1]	Integer (> 0)	y
<del>AuditLog-TotalPages</del>	Umsetzung gemäß [gemSpecAktensystem#gemSpecAktensystem#5.2.1.1]	Integer (>= 0)	y
<del>AuditLog-TotalEntries</del>	Umsetzung gemäß [gemSpecAktensystem#gemSpecAktensystem#5.2.1.1]	Integer (>= 0)	y
<b>Technische Fehlermeldungen</b>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>INTERNAL_ERROR</b>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	

<b>ASSERTION_INVALID</b>	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig
<b>SYNTAX_ERROR</b>	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.
<b>ACCESS_DENIED</b>	Der Zugriff für diese Operation konnte nicht gewährt werden.	

[&lt;=]

### 5.2.1.3.1 Umsetzung

#### ~~A\_15229-03A\_15229-02~~ - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Get Audit Events

Die Komponente ePA-Dokumentenverwaltung MUSS ~~für die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden~~Ausführung dieser Operation prüfen, ob für den zugreifenden Nutzer ein gültiges Policy Document vorliegt. ~~Liegt kein Policy Document vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS\_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [<=Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor eine Audit Event List zum ePA-Frontend des Versicherten zurückgegeben wird.~~

[&lt;=]

#### A\_15583 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Get Audit Events

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

### 5.2.1.4 Operation

#### I\_Account\_Management\_Insurant::GetSignedAuditEvents

#### ~~A\_21110-01A\_21110~~ - Komponente ePA-Dokumentenverwaltung – Signatur für Get Signed Audit Events

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

**Tabelle 26: Tab\_Dokv\_44 - Operation Get Signed Audit Events**

Operation	<code>I_Account_Management_Insurant::GetSignedAuditEvents</code>
<b>Beschreibung</b>	Mit dieser Operation erhält der Versicherte bzw. sein berechtigter Vertreter eine signierte Liste aller in der Dokumentenverwaltung vorliegenden Protokolleinträge des Versicherten.
<b>Formatvorgabe n</b>	SOAP Action: <code>http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/GetSignedAuditEvents</code>
<b>Eingangsparemeter</b>	

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

[&lt;=]

#### 5.2.1.4.1 Umsetzung

##### **~~A 21111-01A-21111~~ - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Get Signed Audit Events**

Die Komponente ePA-Dokumentenverwaltung MUSS ~~für die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden~~Ausführung dieser Operation prüfen, ob für den zugreifenden Nutzer ein gültiges Policy Document vorliegt. Liegt kein Policy Document vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS\_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [<=Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822 durchsetzen, bevor eine Signed Audit Event List zum ePA-Frontend des Versicherten zurückgegeben wird.**[<=]**

### A 21112-01A-21112 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Get Signed Audit Events

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

Es wird das gesamte ~~PDF~~-Dokument bzw. die Dokumente signiert. Beim Anlegen des PDF-Dokuments muss Platz für die Signatur vorgesehen werden Das Format soll dem von Audit Events entsprechen.

## 5.3 Umschlüsselung

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

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

Der Vorgang der Umschlüsselung wird über die folgenden Operationen gesteuert:

- I\_Key\_Management\_Insurant::StartKeyChange()
- I\_Key\_Management\_Insurant::GetAllDocumentKeys()
- I\_Key\_Management\_Insurant::PutAllDocumentKeys()
- I\_Key\_Management\_Insurant::FinishKeyChange()

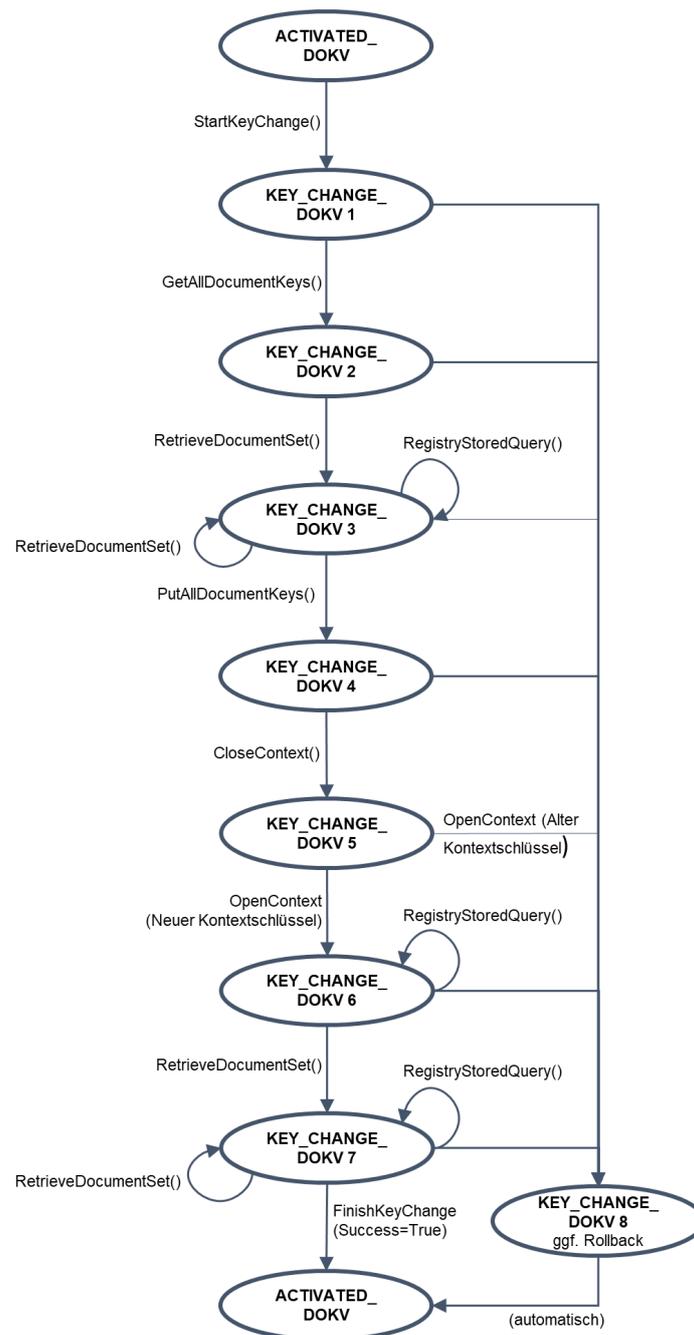
Die Dokumentenverwaltung befindet sich nach erfolgreicher Einleitung der Umschlüsselung (StartKeyChange()) im logischen Zustand "KEY\_CHANGE\_DOKV". Sie ist dabei für alle Teilnehmer außer den Versicherten sowie für alle Operationen, die nicht die Umschlüsselung betreffen, gesperrt.

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

### 5.3.1 Übergreifende Anforderungen

#### **A\_20466-01A\_20466 - Komponente ePA-Dokumentenverwaltung – Erlaubte Zustandsübergänge für Zustand KEY\_CHANGE\_DOKV**

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



**Abbildung 2: Zustandsübergänge Schlüsselwechsel**

Erläuterungen:

- Die abgebildeten Operationen stehen als Kurzform für die folgenden Operationen der Dokumentenverwaltung:
  - StartKeyChange(): I\_Key\_Management\_Insurant::StartKeyChange()
  - GetAllDocumentKeys(): I\_Key\_Management\_Insurant::GetAllDocumentKeys()

- `PutAllDocumentKeys()`:  
`I_Key_Management_Insurant::PutAllDocumentKeys()`
- `FinishKeyChange()`: `I_Key_Management_Insurant::FinishKeyChange()`
- `OpenContext()`: `I_Document_Management_Connect::OpenContext()`
- `CloseContext()`: `I_Document_Management_Connect::CloseContext()`
- `RetrieveDocumentSet()`:  
`I_Document_Management_Insurant::RetrieveDocumentSet()`
- `CloseContext()` (gefolgt von `OpenContext()` ([Neuer Kontextschlüssel](#))) DARF zusätzlich auch in Kombination in den Zuständen [Normalbetrieb](#) sowie `KEY_CHANGE_DOKV 1, 2, 53, 6` und `67` ausgeführt werden. In dem Fall ist der Zustand nach `OpenContext()` identisch mit dem vor `CloseContext()`, d.h. sie verändern den internen Zustand der Dokumentenverwaltung nicht. Die entsprechenden Zustandsübergänge sind nur aus Gründen der Übersichtlichkeit nicht im Diagramm enthalten.
- Der Zustände "KEY\_CHANGE\_DOKV" (mit und ohne angehängte Ziffer) und "ACTIVATED\_DOKV" entsprechen nicht direkt den Zuständen "Key\_Change" bzw. "Activated" des Aktensystems.
- Der Zustand "ACTIVATED\_DOKV" beschreibt den normalen Betriebszustand der Akte, in dem Versicherte bzw. berechnigte weitere Parteien (LEI, KTR) über die jeweilige Schnittstelle auf Dokumente zugreifen können.

#### [<=]

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

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

#### **A\_20729 - Komponente ePA-Dokumentenverwaltung – Start der Umschlüsselung nur in Zustand Activated**

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

#### **A\_20726 - Komponente ePA-Dokumentenverwaltung – Verbotene Operationen außerhalb Status KEY\_CHANGE\_DOKV**

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

#### **A\_20727-01A\_20727 - Komponente ePA-Dokumentenverwaltung – Validierung der Authentication Assertion**

Die Komponente ePA-Dokumentenverwaltung MUSS in allen Eingangsnachrichten der Schnittstelle `I_Key_Management_Insurant` analog eines XUA-Akteur "X-Service Provider" die mitgelieferte X-User Assertion (Authentication Assertion) gemäß der Anforderung A\_13690 prüfen und die eingehende Nachricht mit Fehlercodes nach [WSS#12] [sowie einem HTTP-Fehler 403 \(Fehlermeldung "Access Denied"\)](#) quittieren, falls diese X-User Assertion nicht gültig ist. [**<=**]

Die Authentication Assertion wird als Teil des SOAP Headers mitgeschickt.

#### **A\_20444 - Komponente ePA-Dokumentenverwaltung – Format phr:KeyList für Zustand KEY\_CHANGE\_DOKV**

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

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

Dabei gelten folgende Anforderungen:

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

Einzelne Operationen schränken das angegebene Format ggf. noch weiter ein. [`<=`]

#### **A\_20446 - Komponente ePA-Dokumentenverwaltung – Gültigkeit des Kontextschlüssels für Zustand KEY\_CHANGE\_DOKV**

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

[`<=`]

#### **A\_20468 - Komponente ePA-Dokumentenverwaltung – Login mit altem Kontextschlüssel im Zustand KEY\_CHANGE\_DOKV**

Die Komponente ePA-Dokumentenverwaltung MUSS bei einem Login des Versicherten mithilfe des alten Kontextschlüssels, falls sie sich im Zustand KEY\_CHANGE\_DOKV befindet, ein Rollback gemäß A\_20447\* durchführen und den [Zustand KEY\\_ZustandKEY\\_CHANGE\\_DOKV](#) nach [ACTIVATED\\_DOKV](#) verlassen. [`<=`]

#### **A\_20735 - Komponente ePA-Dokumentenverwaltung – Exklusiver Versichertenzugriff im Zustand KEY\_CHANGE\_DOKV**

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

[`<=`]

#### **[A\\_20442-01A\\_20442](#) - Komponente ePA-Dokumentenverwaltung – Timeout für Zustand KEY\_CHANGE\_DOKV**

Die Komponente ePA-Dokumentenverwaltung MUSS im Status KEY\_CHANGE\_DOKV nach Erreichen des Zeitpunkts `in-RollbackTime` ([Parameter Zeitpunkt 24 Stunden nach Aufruf](#)

von `StartKeyChange()` zum frühestmöglichen Zeitpunkt ein Rollback gemäß [A\\_20447-01A-20447-ML-118312 - Komponente ePA-Dokumentenverwaltung – Rollback für Zustand KEY\\_CHANGE\\_DOKV](#) durchführen. Wenn der Versicherte bei Erreichen von `RollbackTime` noch eingeloggt ist, MUSS die Komponente ePA-Dokumentenverwaltung die Sitzung des Versicherten beenden und eine etwaig ausstehende Operation mit einem Fehler abrechnen. [`<=`]

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

**[A\\_20447-01A-20447 - Komponente ePA-Dokumentenverwaltung – Rollback für Zustand KEY\\_CHANGE\\_DOKV](#)**

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

- [Aufruf `finishKeyChange\(FALSE\)` in der Autorisierungskomponente](#)
- Löschen [des aller Daten, die mit dem neuen Kontextschlüssel verschlüsselt wurden](#)
- [Reaktivierung aller mit dem alten Kontextschlüssel verschlüsselten Daten](#)
- Wiederherstellen bzw. Reaktivierung aller mit dem alten Aktenschlüssel verschlüsselten Dokumentenschlüssel
- Löschen von allen mit dem neuen Aktenschlüssel verschlüsselten Dokumentenschlüssel
- ~~Löschen des neuen Aktenschlüssels~~
- Verlassen des Status `KEY_CHANGE_DOKV` in den Zustand `ACTIVATED_DOKV`

[`<=`]

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

### 5.3.2 Schnittstelle `I_Key_Management_Insurant`

#### 5.3.2.1 `I_Key_Management_Insurant::StartKeyChange()`

**[A\\_20467-01A-20467 - Komponente ePA-Dokumentenverwaltung – Signatur für `I\_Key\_Management\_Insurant::StartKeyChange\(\)`](#)**

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

**Tabelle 27: `Tab_Dokv_38` - Operation `I_Key_Management_Insurant::StartKeyChange()`**

Operation	<code>I_Key_Management_Insurant::StartKeyChange</code>
<b>Beschreibung</b>	Diese Operation setzt die Operation <code>I_Account_Management_Insurant::StartKeyChange</code> technisch um. Mit dieser Operation kann der Versicherte den Prozess der

	Umschlüsselung initiieren.		
<b>Formatvorgaben</b>	SOAP Action: http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/StartKeyChange		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhabers)	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
<b>ContextKey</b>	Neuer Kontextschlüssel	ContextKey	n
<b>RollbackTime</b>	Zeitpunkt (UTC-Zeit), an dem ein Rollback durchgeführt werden muss, sofern bis dahin nicht explizit finishKeyChange() aufgerufen wurde.	<del>Signierte xsd:dateTime, base64-kodiert</del>	<del>n</del>
<b>Ausgangsparameter</b>			
<b>AuthorizedIDList</b>	Liste mit IDs aller zurzeit berechtigten Akteure	phr:AuthorizedIDList	n
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>Technische Fehlermeldungen</b>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>INTERNAL_ERROR</b>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	

<b>ASSERTION_INV ALID</b>	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig
<b>SYNTAX_ERROR</b>	Fehlerhafte Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.
<b>ACCESS_DENIED</b>	Der Zugriff für diese Operation konnte nicht gewährt werden.	

[&lt;=]

### 5.3.2.1.1 Umsetzung

#### **A\_20495 - Komponente ePA-Dokumentenverwaltung – Format von phr:AuthorizedIDList**

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

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

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

#### **A\_20738-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Start Key Change**

~~**A\_20738 – Komponente ePA-Dokumentenverwaltung – Policy Enforcement für StartKeyChange()**~~ Die Komponente ePA-Dokumentenverwaltung MUSS für die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822\_01 durchsetzen vor Ausführen der Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS\_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [~~StartKeyChange()~~].

[&lt;=]

### A\_20757 - Komponente ePA-Dokumentenverwaltung – Prüfung des ContextKey-Parameters

Die Komponente ePA-Dokumentenverwaltung MUSS prüfen, ob der im Parameter "ContextKey" mitgelieferten neue Kontextschlüssel den Strukturvorgaben gemäß [gemSpec\_Krypt#A\_1800415705] entspricht und ansonsten den Fehler "ACCESS\_DENIED" zurückgeben.

[<=]

### ~~A\_20530 – Komponente ePA-Dokumentenverwaltung – Prüfung des RollbackTime-Parameters~~

~~Die Komponente ePA-Dokumentenverwaltung MUSS die RollbackTime Base64-dekodieren, das Format gemäß xsd:dateTime sowie die Signatur des Eingangsparameters "RollbackTime" prüfen. Für die Signaturprüfung MUSS die Komponente ePA-Dokumentenverwaltung auch prüfen, ob das zugehörige Signaturzertifikat zeitlich gültig ist, nicht gesperrt wurde und nach dem Zertifikatsprofil C.FD.SIG auf die Identität der Komponente Autorisierung in seiner fachlichen Rolle oid\_epa\_authz gemäß [gemSpec\_OID] ausgestellt wurde. Falls Signatur oder Zertifikat fehlerhaft sind oder die RollbackTime mehr als 24 Stunden in der Zukunft liegt, MUSS die Komponente ePA-Dokumentenverwaltung den Fehler "ACCESS\_DENIED" zurückgeben.~~

~~[<=]~~

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

### A\_20422 - Komponente ePA-Dokumentenverwaltung – Beenden bestehender Sitzungen bei StartKeyChange()

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

### A\_21618 - Komponente ePA-Dokumentenverwaltung – Aufruf von StartKeyChange() der Autorisierungskomponente

Die Komponente ePA-Dokumentenverwaltung MUSS unmittelbar nach dem Aufruf von StartKeyChange() ihrerseits die Operation StartKeyChange() der Autorisierungskomponente aufrufen. [<=]

### 5.3.2.2 I\_Key\_Management\_Insurant::GetAllDocumentKeys()

#### A\_20443 - Komponente ePA-Dokumentenverwaltung – Signatur für I\_Key\_Management\_Insurant::GetAllDocumentKeys()

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation I\_Key\_Management\_Insurant::GetAllDocumentKeys gemäß der folgenden Signatur implementieren:

**Tabelle 28: Tab\_Dokv\_39 - Operation I\_Key\_Management\_Insurant::GetAllDocumentKeys()**

Operation	I_Key_Management_Insurant::GetAllDocumentKeys
<b>Beschreibung</b>	Diese Operation setzt die Operation I_Key_Management_Insurant::GetAllDocumentKeys technisch um. Mit dieser Operation kann der Versicherte alle mit dem

	Aktenschlüssel verschlüsselte Dokumentenschlüssel abrufen.		
<b>Formatvorgabe n</b>	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/GetAllDocumentKeys		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhabers)	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
<b>OkDate</b>	Zeitpunkt, an dem die Komponente Autorisierung PutForReplacement() erfolgreich ausgeführt hat.	Signierte xsd:dateTime, base64-kodiert	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>DocumentKeyList</b>	Liste aller Document Keys, jeweils verschlüsselt mit altem Aktenschlüssel	phr:KeyList	n
<b>Technische Fehlermeldungen</b>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>INTERNAL_ERROR</b>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
<b>ASSERTION_INVALID</b>	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
<b>SYNTAX_ERROR</b>	Fehlerhafte Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	

<b>ACCESS_DENIED</b>	Der Zugriff für diese Operation konnte nicht gewährt werden.	
----------------------	--	--

[&lt;=]

### 5.3.2.2.1 Umsetzung

#### **A\_20452-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Get All Document Keys**

~~**A\_20452 – Komponente ePA-Dokumentenverwaltung – Policy Enforcement für GetAllDocumentKeys()** Die Komponente ePA-Dokumentenverwaltung MUSS für die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822-01 durchsetzen vor Ausführen der Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS\_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [<=GetAllDocumentKeys()]~~

[&lt;=]

#### **A\_20425 - Komponente ePA-Dokumentenverwaltung – Rückgabe aller verschlüsselter Dokumentenschlüssel**

Die Komponente ePA-Dokumentenverwaltung MUSS als Rückgabewert von GetAllDocumentKeys() alle jeweils mit dem Aktenschlüssel verschlüsselten Dokumentenschlüssel über eine XML-Struktur (phr:KeyList) gemäß A\_20444 zurückgeben. Die Komponente ePA-Dokumentenverwaltung MUSS dabei die alten verschlüsselten Dokumentenschlüssel für den Fall eines späteren Rollbacks und zum Abgleich für die Operation PutAllDocumentKeys() sichern.

[&lt;=]

#### **A\_20528 - Komponente ePA-Dokumentenverwaltung – Prüfung des OkDate-Parameters**

Die Komponente ePA-Dokumentenverwaltung MUSS den Eingangsparameter "OkDate" Base64-dekodieren, das Format gemäß xsd:dateTime sowie die Signatur prüfen und sicherstellen, dass OkDate einen Zeitpunkt in der Vergangenheit bezeichnet, der nicht mehr als 24 Stunden zurückliegt. Zur Signaturprüfung MUSS die Komponente ePA-Dokumentenverwaltung auch prüfen, ob das zugehörige Signaturzertifikat zeitlich gültig ist, nicht gesperrt wurde und nach dem Zertifikatsprofil C.FD.SIG auf die Identität der Komponente Autorisierung in seiner fachlichen Rolle oid\_epa\_authz gemäß [gemSpec\_OID] ausgestellt wurde. Falls Signatur oder Zertifikat fehlerhaft sind, MUSS die Komponente ePA-Dokumentenverwaltung den Fehler "ACCESS\_DENIED" zurückgeben und ein Rollback gemäß A\_20447-\* durchführen.

[&lt;=]

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

### 5.3.2.3 Operation I\_Key\_Management\_Insurant::PutAllDocumentKeys()

#### A\_20436-01 - Komponente ePA-Dokumentenverwaltung – Signatur für I\_Key\_Management\_Insurant::PutAllDocumentKeys()

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

I\_Key\_Management\_Insurant::PutAllDocumentKeys gemäß der folgenden Signatur implementieren:

**Tabelle 29: Tab\_Dokv\_40 - Operation I\_Key\_Management\_Insurant::PutAllDocumentKeys()**

<b>Operation</b>	I_Account_Management_Insurant::PutAllDocumentKeys		
<b>Beschreibung</b>	Diese Operation setzt die Operation I_Key_Management_Insurant::PutAllDocumentKeys technisch um. Mit dieser Operation kann der Versicherte den Prozess des Schlüsselwechsels einleiten.		
<b>Formatvorgaben</b>	SOAP Action: http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/PutAllDocumentKeys		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b>
			.
<b>X-User Assertion</b>	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhabers)	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109, A_15631]	n
<b>DocumentKeyList</b>	Liste aller Document Keys, jeweils verschlüsselt mit neuem Aktenschlüssel	phr:KeyList	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt</b>
			.
<b>Technische Fehlermeldungen</b>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	

<b>INTERNAL_ERROR</b>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik
<b>ASSERTION_INVALID</b>	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig
<b>SYNTAX_ERROR</b>	Fehlerhafte Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.
<b>ACCESS_DENIED</b>	Der Zugriff für diese Operation konnte nicht gewährt werden.	

[<=]

#### 5.3.2.3.1 Umsetzung

##### **A\_20453-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Put All Document Keys**

~~**A\_20453 – Komponente ePA-Dokumentenverwaltung – Policy Enforcement für PutAllDocumentKeys()** Die Komponente ePA-Dokumentenverwaltung MUSS für die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A\_14822\_01 durchsetzen vor Ausführen der Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS\_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [~~PutAllDocumentKeys()~~.~~

[<=]

##### **A\_20448 - Komponente ePA-Dokumentenverwaltung – Hochladen aller verschlüsselter Dokumentenschlüssel**

Die Komponente ePA-Dokumentenverwaltung MUSS als Eingabeparameter von PutAllDocumentKeys() alle mit dem neuen Aktenschlüssel verschlüsselten Dokumentenschlüssel über eine XML-Struktur (phr:KeyList) gemäß A\_20444 einstellen. Die Komponente ePA-Dokumentenverwaltung MUSS dabei sicherstellen, dass Schlüssel für dieselben Dokumente hochgeladen werden, wie sie beim vorhergehenden Aufruf von GetAllDocumentKeys() von der Dokumentenverwaltung übertragen wurde.

[<=]

##### **A\_20758 - Komponente ePA-Dokumentenverwaltung – Prüfung des DocumentKeyList-Parameters**

Die Komponente ePA-Dokumentenverwaltung MUSS prüfen, ob die im Parameter "DocumentKeyList" gesendeten Daten den Strukturvorgaben gemäß A\_20495-20447-\* entspricht und ansonsten den Fehler "ACCESS\_DENIED" zurückgeben.

[<=]

### A\_20730 - Komponente ePA-Dokumentenverwaltung – Rollback bei fehlgeschlagenem PutAllDocumentKeys()

Die Komponente ePA-Dokumentenverwaltung MUSS, falls die Operation `PutAllDocumentKeys()` fehlschlägt, einen Fehler zurückgeben und ein Rollback gemäß A\_20447-\* durchführen.

[<=]

### 5.3.2.4 Operation I\_Key\_Management\_Insurant::FinishKeyChange()

#### A\_20449 - Komponente ePA-Dokumentenverwaltung – Signatur für I\_Key\_Management\_Insurant::FinishKeyChange()

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

**Tabelle 30: Tab\_Dokv\_41 -**

#### Operation I\_Account\_Management\_Insurant::FinishKeyChange()

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

<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>Technische Fehlermeldungen</b>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>INTERNAL_ERROR</b>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
<b>ASSERTION_INVALID</b>	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
<b>SYNTAX_ERROR</b>	Fehlerhafte Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
<b>ACCESS_DENIED</b>	Der Zugriff für diese Operation konnte nicht gewährt werden.		

[&lt;=]

#### 5.3.2.4.1 Umsetzung

##### **A\_20454-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Finish Key Change**

~~**A\_20454 – Komponente ePA-Dokumentenverwaltung – Policy Enforcement für FinishKeyChange()**~~ Die Komponente ePA-Dokumentenverwaltung MUSS ~~für~~ die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung ~~A\_14822\_01~~ durchsetzen vor Ausführen der Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS\_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [~~<=~~]

##### **A\_21620 - Komponente ePA-Dokumentenverwaltung – Aufruf von FinishKeyChange() der Autorisierungskomponente**

Die Komponente ePA-Dokumentenverwaltung MUSS unmittelbar nach dem Aufruf von `FinishKeyChange()` ihrerseits die Operation `FinishKeyChange()` der Autorisierungskomponente aufrufen und dabei den gleichen Wert des Parameters `Success` verwenden. [~~<=~~]

[&lt;=]

### A\_20450 - Komponente ePA-Dokumentenverwaltung – Erfolgreicher Abschluss des Schlüsselwechsels

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

### A\_21141 - Komponente ePA-Dokumentenverwaltung – Protokollierung erfolgreicher Abschluss des Schlüsselwechsels

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

### A\_20451 - Komponente ePA-Dokumentenverwaltung – Erfolgloser Abschluss des Schlüsselwechsels

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

## 5.3.2.5 Protokollierung

### A\_20470-01 - Komponente ePA-Dokumentenverwaltung - Protokollierungszusatz für Status `KEY_CHANGE_DOKV`

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

**Tabelle 31: Tab\_Dokv\_42 - Zusätzliche Parameter des § 291a-Protokolls für die Umschlüsselung**

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

[`<=`]

### A\_20473-02 - Komponente ePA-Dokumentenverwaltung - Protokollierungszusatz für Status Rollback im Status `KEY_CHANGE_DOKV`

Die Komponente ePA-Dokumentenverwaltung MUSS im Falle eines Rollbacks gemäß `A_20447-*` der Protokollierung gemäß `gemSpec_DM_ePA#A_14505` einen Protokolleintrag (`Event.code=PHR-860`) hinzufügen und dabei den folgenden Parameter hinzufügen:

**Tabelle 32: Tab\_Dokv\_43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung**

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

[&lt;=]

### A\_21157 - Komponente ePA-Dokumentenverwaltung - Protokollierungszusatz für Verwaltungsprotokolleintrag für Aufruf der Operation `FinishKeyChange`

Die Komponente ePA-Dokumentenverwaltung MUSS im Falle des Aufrufs von `FinishKeyChange` bei der Protokollierung gemäß `gemSpec_DM_ePA#A_14505` einen Protokolleintrag (`Event.code=PHR-840`) hinzufügen und dabei den folgenden Parameter hinzufügen:

**Tabelle 33: Tab\_Dokv\_43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung**

Protokollparameter	Parameterwerte gemäß aufgerufener Operation	
ObjectDetail	Das Element <code>ParticipantObjectDetail</code> muss zusätzlich mit folgendem Wertepaar ( <code>type/value</code> ) belegt werden:	
	type	value
	Details	Der Wert ist abhängig vom Aufrufparameter <code>Success</code> der Operation <code>FinishKeyChange</code> . <b>Success = 1:</b> "Umschlüsselung erfolgreich beenden" <b>Success = 0:</b> "Umschlüsselung abbrechen"

[&lt;=]

## 5.4 Zugriffskontrolle

### 5.4.1 ~~Grob-, mittel- und feingranulare Berechtigungen~~

Die Zugriffskontrolle ~~mus sicherstellen~~ stellt sicher, dass nur solche Zugriffe zugelassen werden, die vom Versicherten ~~berechtigt~~ oder seinen Vertreter autorisiert wurden. Zur ~~Berechtigungsvergabe~~ Autorisierung an Leistungserbringerinstitutionen (LEI) sowie Kostenträgern stehen ~~dem Versicherten~~ dazu grundsätzlich ~~drei Ansätze~~ verschiedene Granularitäten zur Verfügung:

#### 1. ~~Grobgranulare Berechtigung (Vertraulichkeitsstufen)~~

~~Allen Dokumenten wird in der Akte eine von drei Vertraulichkeitsstufen zugeordnet ("Streng vertraulich", "Vertraulich" oder "Normal") und jedem Berechtigten eine von zwei Zugriffsrechten ("Normal" oder "Erweitert"). LEI mit Zugriffsrecht "Normal" dürfen auf die Dokumente in Vertraulichkeitsstufe "Normal" zugreifen, jene mit Zugriffsrecht "Erweitert" zusätzlich auf die mit "Vertraulich" gekennzeichneten Dokumente. Dokumente in der Stufe "Streng vertraulich". Dies sind nur für den Versicherten sichtbar (Ausnahme: "Whitelisting", siehe unten).~~

#### Mittelgranulare Berechtigung (Kategorien)

Ein Versicherter kann Dokumente aus zum einen oder mehreren vorgegebenen Dokumentenkategorien (z. B. Arztbriefe) freigeben. Die dadurch getätigte Dokumentenauswahl wird mit dem grobgranularen Zugriffsrecht (siehe 1.) des Berechtigten kombiniert. Das heißt, dass eine auf Arztbriefe berechtigte LEI je nach Zugriffsrecht entweder nur die als "Normal" eingestuften Arztbriefe sehen kann oder auch die als "Vertraulich" gekennzeichneten. Mittelgranulare Berechtigungen schränken die grobgranular vergebene Berechtigungen ggf. ein, erweitern sie aber niemals. Die Metadaten eines Dokuments bzw. ihre Zugehörigkeit zu einem Ordner entscheiden darüber, welchen Kategorien (mindestens einer, potentiell mehreren) ein Dokument zugeordnet ist (siehe auch A\_19388 in gemSpec\_DM\_ePA). die (1) kategoriebasierte Autorisierung und zum anderen die (2) dokumentenspezifische Autorisierung.

#### 2. ~~Feingranulare Berechtigung (White und Blacklist)~~

~~Der Versicherte kann einer LEI den Zugriff auf einzelne Dokumente gewähren ("Whitelisting") oder entziehen ("Blacklisting"). Die Vergabe von feingranularen Berechtigungen ist immer unabhängig von den vergebenen mittel- und grobgranularen Berechtigungen. Steht also ein Dokument auf White- oder Blacklist, spielen etwaige entgegenstehende grob- und feingranulare Berechtigungen bei der Zugriffsentscheidung auf dieses Dokument keine Rolle.~~

### 5.4.2 Berufsruppenspezifische Einschränkungen

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

1. Beispielsweise haben Die **kategoriebasierte Autorisierung** schränkt den Zugang Dritter über berufsruppenspezifische Vorgaben gemäß § 341 PDSG Absatz 2 ein. Dazu gibt es festgelegte Dokumentenkategorien, welche mit spezifischen Zugriffsrechten der grundlegenden Zugriffsoperationen (CRUD - create, read, update, delete) wirken (vgl. Tab Dokv\_030 - Zugriffsunterbindungsregeln in A\_19303). Diese Zugriffsrechte wirken ausnahmslos, d.h. auch bei einer etwaigen weiteren Autorisierung einer dokumentenspezifischen Autorisierung (siehe 2.) gelten diese Regeln ebenso. Beispiele sind:

- a. Apotheker grundsätzlich haben keinen Zugriff auf das Zahnbonusheft (Kategorie der Dokumentenkategorie "dentalrecord") des Versicherten (siehe Tab\_Dokv\_030 - Zugriffsunterbindungsregeln).).
- b. Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen, ändern oder noch löschen.

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

Eine Übersicht über die unterschiedenen Berufsgruppen und die ihnen möglichen Berechtigungen finden sich in [Tab\_Dokv\_030—Zugriffsunterbindungsregeln].

### 5.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln

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

1. Dynamische Berechtigungsfreigaben (wie z. B. die Entscheidung, welche LEI überhaupt vom Versicherten berechtigt werden, in welcher Stufe, welchen Kategorien und mit welchen Ausnahmen) werden vom über "Policies" in die Dokumentenverwaltung eingestellt oder auch gelöscht.
1. Unabänderliche Regeln (wie die gesetzlich motivierten Vorgaben für Berufsgruppen) werden über entsprechende AFOs realisiert, insbesondere A\_19303. Es ist natürlich umsetzender Software möglich, auch diese Regeln über interne Policies durchzusetzen.

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

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

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

Mittelgranulare Berechtigungen (kategoriebasiert) werden über verschiedene Metadaten(kombinationen) umgesetzt. Die Details sind A\_19388 (gemSpec\_DM\_ePA) oder auch direkt den Policies in Anhang C zu entnehmen.

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

Jede Einstellung eines Dokuments wird von der ePA-Dokumentenverwaltung mit einer automatischen Zuordnung zu einem statischen Ordner, welcher die Dokumentenkategorie repräsentiert, erweitert. Diese statischen Ordner sind initial bei jedem Aktenkonto eines Versicherten existent. Die serverseitige Zuordnung in diese Ordner erfolgt anhand der XDS-Metadaten in Kombination mit der Nutzergruppe des Einstellers, welche aus der Authentication Assertion erkennbar ist (die Nutzergruppe ist dem Signaturzertifikat zu entnehmen). Die Regeln für diese Zuordnung sind in [gemSpec\_DM\_ePA#A\_20577] festgelegt.

Das bedeutet weiterhin, dass das Anlegen von Ordnern durch ePA-Clients nicht erlaubt ist, um eine zweifelsfreie Freigabe auf Grundlage der Dokumentenkategorien zu gewährleisten. Es gibt zwei Ausnahmen bei den medizinischen Informationsobjekten (MIOs), welche ebenso einer Dokumentenkategorie unterliegen und jeweils einem Ordner zugeordnet werden müssen. Diese sind der Mutterpass sowie das Kinderuntersuchungsheft. Bei mehreren Kindern können auch mehrere Ordner zu diesen Pässen in einer ePA existieren. Eine zweifelsfreie Zuordnung in der ePA-Dokumentenverwaltung wäre daher nicht gegeben, sodass hier ePA-Clients die Ordner zeitgleich mit der

Dokumentenregistrierung anlegen müssen. Eine vorherige Abfrage der Ordner mit den speziellen folderCodes ist allerdings zu empfehlen.

Weiterhin kann die Auswahl einer Dokumentenkategorie durch den Versicherten oder seinen Vertreter durch eine sensiblere Vertraulichkeit eingeschränkt werden. Es ist von Vorteil, die Vertraulichkeit eines Dokuments an dieser Stelle näher zu beschreiben: Einstellende Akteure können einem Dokument eine der drei Vertraulichkeitsstufen "streng vertraulich", "vertraulich" oder "normal" zuordnen. Grundsätzlich sind eingestellte Dokumente mit der Vertraulichkeitsstufe "streng vertraulich" nicht autorisierbar, d.h. sie sind nur vom Versicherten oder seinen Vertreter einsehbar. Wenn eine Autorisierung und damit Freigabe dieses sensiblen Dokuments dennoch erwünscht ist, muss auch eine weniger sensible Vertraulichkeitsstufe ("vertraulich" oder "normal") zuvor zugeordnet werden.

Die beiden anderen Stufen "vertraulich" oder "normal" müssen mit einer Dokumentenkategorie kombiniert werden. Eine pauschale Berechtigung auf "normale" Dokumente beinhaltet im Detail auch implizit die Auswahl und Zustimmung aller Dokumentenkategorien. Während einer Ad-hoc-Berechtigung kann aufgrund der Einschränkungen des Kartenterminals zu ein oder mehreren ausgewählten Dokumentenkategorien nur eine Vertraulichkeit für die Freigabe durch den Versicherten bestätigt werden. Auf Seite des ePA-FdV könnte hingegen pro freigegebene Kategorie entweder die Vertraulichkeitsstufe "vertraulich", "normal" als auch beide Stufen in einer Autorisierung ausgesprochen werden.

Einer Leistungserbringerinstitution, welcher lediglich ein ausschließlicher Zugriff auf Dokumente mit der Vertraulichkeitsstufe "normal" vergeben wurde, wird unter dem Begriff "einfaches Zugriffsrecht" subsumiert. Hingegen bedeutet die Autorisierung auf Dokumente mit den Vertraulichkeitsstufen "normal" und "vertraulich" ein "erweitertes Zugriffsrecht".

2. Die **dokumentenspezifische Autorisierung** bietet dem Versicherten oder seinen Vertreter mit ePA-FdV die Möglichkeit, Dokumente auf einer Whitelist ("gewährender Zugriff") oder Blacklist ("verbietender Zugriff") zu setzen. Ein Dokument (genauer gesagt die DocumentEntry.entryUUID auf Policy-Ebene) darf auf diesen Listen nicht gleichzeitig stehen. Auch sind diese Dokumente aufgrund der Zuordnungsregeln beim Einstellen indirekt immer einer Kategorie zugeordnet. Es ist hier aber möglich, feingranularer, d.h. auf Dokumentenebene Zugriffe für Leistungserbringerinstitutionen auszusprechen. Aufgrund der zuvor angesprochen Sonderbehandlung von Mutterpass und Kinderuntersuchungsheft, ist es darüber hinaus möglich, einen bestimmten Pass von potentiell mehreren Pässen auf eine Blacklist zu setzen, um einen Zugriff, der pauschal über die Dokumentenkategorie "mothersrecord" bzw. "childsrecord" gewährt wurde, zu untersagen. Auf einer Whitelist sind hingegen lediglich Dokumente und keine Ordner aufgelistet. Ordner sind hiervon ausgeschlossen da hierfür konzeptionell die Dokumentenkategorie zu verwenden ist.

#### **5-4-45.4.1 Vergabe von Zugriffsregeln Zugriffsrechten und Policy Administration**

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

~~Darüberhinaus~~ Darüber hinaus können ~~LEI~~Leistungserbringerinstitutionen über eine ~~Ad-hoc~~Ad-hoc-Berechtigung beim ~~LEI~~Leistungserbringer vor Ort ~~groß- und mittelgranularkategoriebasiert~~ berechtigt werden. Die zeitliche Gültigkeit der erteilten Zugriffsrechte wird vom Versicherten festgelegt. Sie wird zeitlich befristet oder unbefristet vergeben.

### **5.4.5 Funktionsprinzip ~~Policy Administration~~**

Die Berechtigungsvergabe ~~an Leistungserbringerinstitutionen und Vertreter des Versicherten~~ erfolgt durch das Einstellen ~~von~~eines Policy Documents als XDS-Dokument (siehe nachstehende Abbildung). ~~Diese Dokumente werden in den Abschnitten 3).~~ Vorgaben bzgl. der Struktur sowie der aktensystemseitigen Verarbeitung sind im Abschnitt 5.4.6.2 bis 5.4.6.5 für die ePA-Fachanwendung definiert und festgelegt. Die Policy Documents setzen ferner das Zugriffskontrollmodell Attribute-based Access Control (ABAC) um. Die Registrierung dieser sogenannten Advanced Patient Privacy Consents (APPC) erfolgt als unverschlüsselte Dokumente (jedoch über die sichere Verbindung zwischen dem Fachmodul ePA bzw. dem ePA-Frontend des Versicherten und dem Verarbeitungskontext) durch Nutzung der IHE ITI-Transaktionen "Cross-Gateway Document Provide" [ITI-80] sowie "Provide And Register Document Set-b" [ITI-41]. Die interne Datenhaltung bzgl. der ~~Policy Documents (Advanced Patient Privacy Consents) Policies~~ ist nicht vorgegeben, allerdings müssen diese Policy Documents Policies über die Standard-Abfrageschnittstelle über die Operation ~~+~~ der Operationen Registry Stored Query [ITI-18] und Retrieve Document\_Management\_Insurant::RegistryStoredQuery Set [ITI-43] dem ePA-Frontend des Versicherten zugänglich gemacht werden. Dazu werden die DocumentEntry-Metadaten gemäß der Anforderung [gemSpec\_DM\_ePA#A\_14961] vorgegeben.

Die grundlegende Zugriffsstrategie ist "Opting-in", sodass ein gewährendes Zugriffsrecht nur durch Registrierung eines neuen Policy ~~Documents~~Document vergeben werden kann. Ein Policy Document drückt die grundsätzliche Autorisierung eines Leistungserbringers oder Kostenträgers durch den Versicherten oder seinen Vertreter aus. Es formuliert KEINE erlaubten Operationen im Detail (wie in ePA1), sondern legitimiert potentielle Lese- und Löschzugriffe entsprechend der Zugriffsunterbindungsregeln (vgl. A 20736). Das Zugriffsrecht zum Einstellen oder Ersetzen eines (med.) Dokuments durch einen Zugriffsberechtigten ergibt sich indirekt durch die Existenz eines gültigen Policy Document für diesen Zugriffsberechtigten.

#### **A 15173-04 - Komponente ePA-Dokumentenverwaltung – Zugriffsstrategie "Opting-in" mit "Access Deny" als Standardeinstellung**

Die Komponente ePA-Dokumentenverwaltung MUSS jeden Zugriff verweigern, der nicht auf der Grundlage definierter Policy Documents (Advanced Patient Privacy Consents) in Kombination mit der entsprechenden Operation gemäß A 19303, A 19997, A 19998 oder A 20736 explizit erlaubt ist. [ $\leq$ ]

Eine inhaltliche Änderung eines Policy ~~Documents~~Document ist nicht vorgesehen. Stattdessen soll durch den Client ein zu einem Berechtigten ein vorhandenes Policy Document gelöscht und ein neues registriert werden. Wurde ein vorhandenes Policy Document, das demselben Berechtigten zuzuordnen ist ~~(d.h. xaaml:SubjectMatch, xaaml:ResourceMatch sind identisch),~~ durch den Client nicht explizit gelöscht, wird ~~dieses~~diese von der ePA-Dokumentenverwaltung automatisch gelöscht bzw. überschrieben, während das neue Policy Document eingestellt

wird. [Eine Übereinstimmung liegt vor, wenn xacml:SubjectMatch, xacml:ResourceMatch identisch sind.](#)

#### **A\_14998 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen vom Policy Document bei neuem Policy Document mit demselben Berechtigten**

Die Komponente ePA-Dokumentenverwaltung MUSS über die Operationen

I\_Document\_Management::CrossGatewayDocumentProvide sowie

I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b eine Prüfung

auf ein bereits registriertes Policy Document (Advanced Patient Privacy Consent) mit

demselben Berechtigten sowie der Aktenidentität (d.h. xacml:SubjectMatch und

xacml:ResourceMatch sind identisch) durchführen und bei Existenz dieses

Policy Documents (Advanced Patient Privacy Consent) dieses samt IHE ITI-XDS-

Metadaten löschen, bevor ein neues Policy Document gespeichert wird.

[<=]

[Weitere Anforderungen zum Umgang mit Policies sind die folgenden:](#)

#### **~~A\_14892-04A~~ ~~14892-02~~ - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen ungültiger Policy Documents**

Die Komponente ePA-Dokumentenverwaltung ~~SOLL~~**MUSS** Policy Documents (Advanced

Patient Privacy Consents) und zugehörige IHE ITI-XDS-Metadaten löschen, wenn diese

Policy Documents ihre zeitliche Gültigkeit verlieren. [<=]

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

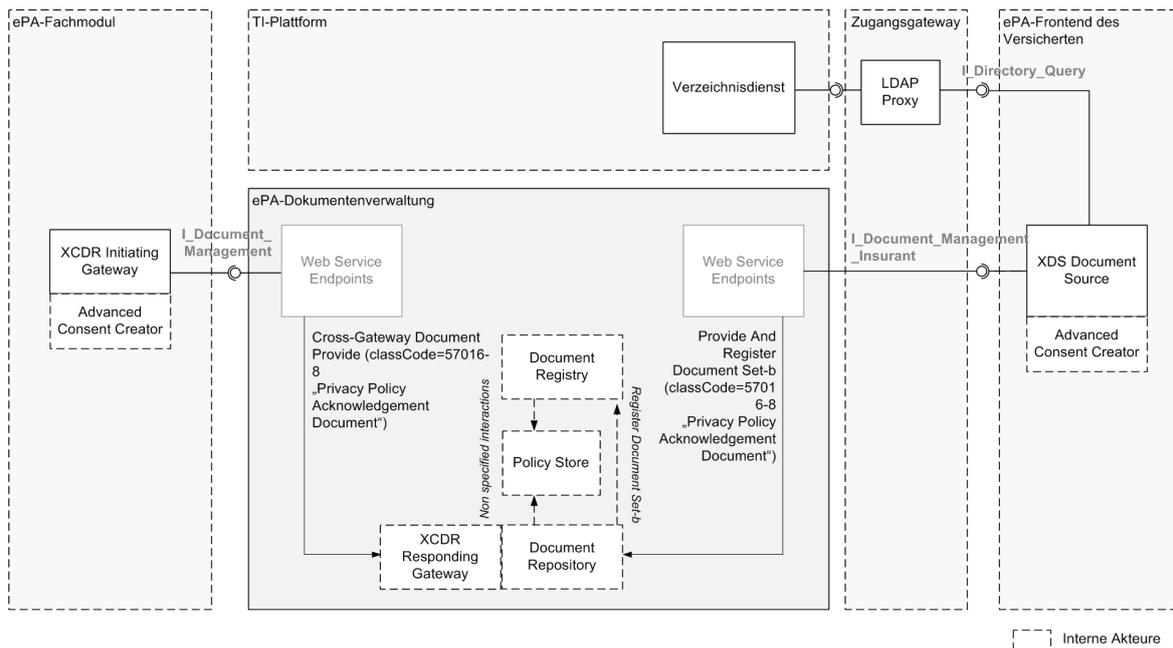
#### **A\_14895 - Komponente ePA-Dokumentenverwaltung – Schutz vor Manipulation der Policy Documents**

Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Policy

Documents (Advanced Patient Privacy Consents) gegen Veränderung und unberechtigtes

Löschen geschützt sind.

[<=]



**Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen**

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

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



["urn:ihe:iti:ser:2016:patient-id"](#) nicht mit der Identität der Akte (d.h. die des Akteninhabers) übereinstimmt.

- **A\_19303-03—Komponente ePA-Dokumentenverwaltung—Zugriffsunterbindungsregeln**  
Prüfung des Einstellers  
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung des Policy Document Die\_abbrechen, wenn die in der Nachricht enthaltene SAML 2.0 Assertion (Authentication Assertion / X-User Assertion) nicht dem Versicherten oder einem seiner Vertreter zugeordnet ist (d.h. das root-Attribut des InstanceIdentifier-Elements innerhalb des SubjectMatch-Elements muss mit der OID "1.2.276.0.76.4.8" eine KVNR kennzeichnen).
- Keine Verwendung des "xsi:schemaLocation"-Attributs  
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung des Policy Document abbrechen, wenn ein xsi:schemaLocation-Attribut gemäß [XMLSchema#2.6.3] enthalten ist.
- Verstöße gegen Policy-Struktur und -Inhalte  
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung des Policy Document abbrechen, wenn sie Verstöße gegen die Vorgaben aus [gemSpec DM ePA#A 14961] erkennt.

[<=]

#### **A 14933-02 - Komponente ePA-Dokumentenverwaltung – XML Schema-Validierung eines Policy Document**

Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Document dieses einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen. Ist ein Policy Document nicht wohlgeformt oder gültig, MUSS die Komponente ePA-Dokumentenverwaltung die Registrierung des Policy Document ablehnen, die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und den InvalidDocumentContent-Fehlercode mit der UniqueID des Policy Document zurückgeben. [<=]

#### **A 21647 - Komponente ePA-Dokumentenverwaltung – Keine Elemente eines MIO in Whitelist und Blacklist mit Ausnahme der Kinderordner in Kategorien 3 und 4 für Blacklist**

Die Komponente ePA-Dokumentenverwaltung DARF medizinische Informationsobjekte (d.h. MIOs der Dokumentenkategorien 2, 3, 4, 5 oder 10) NICHT mit ihrer Folder.entryUUID in der Blacklist oder Whitelist einer Policy akzeptieren, wobei es jedoch erlaubt ist, in MIOs der Kategorie 3 und 4 die auf einzelne Kinder bezogenen Ordner auf eine Blacklist zu setzen. Policy Documents MÜSSEN abgelehnt werden, die Teilelemente von MIOs der Dokumentenkategorien 2, 3, 4, 5 oder 10 auf die Whitelist oder Blacklist einer Policy setzen. Liegt eine Verletzung vor, MUSS die Komponente ePA-Dokumentenverwaltung die Registrierung des Policy Document ablehnen, die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und den InvalidDocumentContent-Fehlercode mit der UniqueID des Policy Document zurückgeben. [<=]

#### **A 21650 - Komponente ePA-Dokumentenverwaltung – Ein Dokument darf nicht gleichzeitig auf Black- und Whitelist stehen.**

Die Komponente ePA-Dokumentenverwaltung MUSS unterbinden, dass Dokumente in demselben Policy Document gleichzeitig auf der Blacklist und der Whitelist aufgeführt werden. Liegt eine Verletzung vor, MUSS die Komponente ePA-Dokumentenverwaltung die Registrierung des Policy Document ablehnen, die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und den InvalidDocumentContent-Fehlercode mit der UniqueID des Policy Document zurückgeben. [<=]

**A 21695 - Komponente ePA-Dokumentenverwaltung – Ablehnung einer zu registrierenden Policy bei Verletzung der Zugriffsunterbindungsregeln**

Die Komponente ePA-Dokumentenverwaltung MUSS anhand der ProfessionOID sowie die Telematik-ID der zu registrierenden Policy prüfen, ob eine Verletzung der Zugriffsunterbindungsregeln vorliegt. Liegt eine Verletzung vor, MUSS die Komponente ePA-Dokumentenverwaltung die Registrierung des Policy Document ablehnen, die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und den InvalidDocumentContent-Fehlercode mit der UniqueID des Policy Document zurückgeben. Eine Ausnahme bei dieser Prüfvorgabe ist eine Vertreter-Berechtigung. [ $\leq$ ]

**A 19303-05 - Komponente ePA-Dokumentenverwaltung – Zugriffsunterbindungsregeln**

Die Komponente ePA-Dokumentenverwaltung MUSS alle in der Tabelle Tab\_Dokv\_030 - Zugriffsunterbindungsregeln aufgeführten ZugriffsunterbindungsregelnRegeln durchsetzen. ~~Die Komponente ePA-Dokumentenverwaltung MUSS~~ sowie beim Aufruf einer der Operationen der Schnittstelle I\_Document\_Management die übergebene ~~AuthenticationAssertion~~ Authentication Assertion dahingehend prüfen, ob die ProfessionOID der ZertifikatsExtensionZertifikats-Extension Admission gemäß [gemSpec\_PKI#Anhang A] im Signaturzertifikat C.HCI.OSIG (/saml2:Assertion/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate) für die Operation, ausgeführt auf eine bestimmte Dokumentenkategorie, zugriffsberechtigt ist. Das Ausführen von Operationen auf Dokumentenkategorien, die nicht explizit erlaubt sind, muss verhindert werden ("Access Deny"). Ferner MUSS auch das Registrieren von Policy Documents durch die Komponente ePA-Dokumentenverwaltung verhindert werden, wenn inhaltlich die Zugriffsunterbindungsregeln verletzt werden (vgl. A 21695).

**Tabelle 34: Tab\_Dokv\_030 - Zugriffsunterbindungsregeln**

Dokumentenkategorie gemäß § 341 PDSG Absatz 2		Zugriffsrecht										
Nr.	Technischer Identifizier	Arzt	ZArzt	Apo	Psych	Pflege	Heba	Phy s	GD	AM	KT R	Ver
1a1	practitioner	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
1a2	hospital	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
1a3	laboratory	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
1a4	physiotherapy	CRU D	CRU D	R	CRU D	R	R	CRU D	CRU D	R	-	RDM
1a5	psychotherapy	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM

1a6	dermatology	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
1a7	gynaecology_u rology	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
1a8	dentistry_oms	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
1a9	other_medical	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
1a10	other_non_me dical	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
1b	emp	CRU D	CRU D	CRU D	CRU D	R	R	R	CRU D	R	-	RDM
1c	nfd	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
1d	eab	CRU D	CRU D	R	CRU D	R	R	R	CRU D	R	-	RDM
2	dentalrecord	CRU D	CRU D	-	CRU D	R	-	-	CRU D	R	-	RDM
3	childsrecord	CRU D	CRU D	R	CRU D	R	CRU D	R	CRU D	R	-	RDM
4	mothersrecord	CRU D	CRU D	R	CRU D	R	CRU D	R	CRU D	R	-	RDM
5	vaccination	CRU D	CRU D	CRU D	CRU D	R	R	-	CRU D	CRU D	-	RDM
6	patientdoc	RD	RD	R	RD	R	R	R	RD	R	-	CRU DM
7	ega	RD	RD	R	RD	R	R	R	RD	R	-	CRU DM
8	receipt	RD	RD	RD	RD	R	R	R	RD	R	CU	RDM
10	care	CRU D	CRU D	R	CRU D	CRU D	R	R	CRU D	R	-	RDM
11	prescription	CRU D	CRU D	CRU D	CRU D	R	R	R	CRU D	R	-	RDM

12	eau	CRU D	CRU D	-	CRU D	-	-	-	CRU D	R	-	RDM
13	other	CRU D	CRU D	-	CRU D	-	-	-	CRU D	R	-	RDM

Legende der [Zugriffsrechte](#) CRUD, Zuordnung zur Operation:

- C (create)  $\Rightarrow$  = I\_Document\_Management::CrossGatewayDocumentProvide, I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b, I\_Document\_Management\_Insurance::ProvideAndRegisterDocumentSet-b;
- R (read)  $\Rightarrow$  = I\_Document\_Management::CrossGatewayQuery, I\_Document\_Management::CrossGatewayRetrieve, I\_Document\_Management\_Insurant::CrossGatewayQuery, I\_Document\_Management\_Insurant::CrossGatewayRetrieve;
- U (update)  $\Rightarrow$  = Document Replacement (über urn:ihe:iti:2007:AssociationType:~~XFRM~~-RPLC) via Operationen I\_Document\_Management::CrossGatewayDocumentProvide, I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b, I\_Document\_Management\_Insurance::ProvideAndRegisterDocumentSet-b;
- D (delete)  $\Rightarrow$  = I\_Document\_Management::RemoveMetadata, I\_Document\_Management::RemoveDocuments, [I\\_Document\\_Management\\_Insurant::RemoveDocuments](#), I\_Document\_Management\_Insurant::RemoveMetadata;
- M (metadata update)  $\Rightarrow$  = I\_Document\_Management\_Insurant::RestrictedUpdateDocumentSet;
- "-" = keine Zugriffsrechte;

Legende der Institutionen, Zuordnung zur ProfessionOID:

- Arzt  $\Rightarrow$  = oid\_praxis\_arzt, oid\_krankenhaus, oid\_institution-vorsorge-reha, oid\_sanitaetsdienst-bundeswehr;
- ZArzt  $\Rightarrow$  = oid\_zahnarztpraxis;
- Apo  $\Rightarrow$  = oid\_öffentliche\_apotheke;
- Psych  $\Rightarrow$  = oid\_praxis\_psychotherapeut;
- Pflege  $\Rightarrow$  = oid\_institution-pflege;
- Heba  $\Rightarrow$  = oid\_institution-geburtshilfe;
- Phys  $\Rightarrow$  = oid\_praxis-physiotherapeut;
- GD  $\Rightarrow$  = oid\_institution-oegd;
- AM  $\Rightarrow$  = oid\_institution-arbeitsmedizin;
- KTR  $\Rightarrow$  = oid\_epa\_ktr;

Legende Zugriffsberechtigte, Zuordnung über KVNR:

- Ver  $\Rightarrow$  = Versicherter/Vertreter;

[\[<=>\] Dokumente können ausnahmsweise zwei Kategorien angehören. Die Elternnotiz des Kinderuntersuchungsheftes gehört sowohl der Kategorie "patientdoc" als auch "childsrecord" an, da die Elternnotiz über das ePA-FdV durch den Versicherten oder seinen Vertreter eingestellt werden darf. \[<=\]](#)

### **A\_21211 - Komponente ePA-Dokumentenverwaltung - Änderungen von Zugriffsunterbindungsregeln nicht erlauben**

Die Komponente ePA-Dokumentenverwaltung MUSS durch technische Maßnahmen sicherstellen, dass Änderungen von Tab\_Dokv\_030 - Zugriffsunterbindungsregeln ausgeschlossen sind.

[<=]

### ~~A\_15173-03 - Komponente ePA-Dokumentenverwaltung - Zugriffsstrategie "Opting-in" mit "Access-Deny" als StandardEinstellung~~

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

~~A\_19303, A\_19997, A\_19998 oder A\_20736 explizit erlaubt ist. [<=]~~

### A\_20736-02 - Komponente ePA-Dokumentenverwaltung - Generelles schreibendes Zugriffsrecht für Leistungserbringerinstitutionen oder Kostenträger

**A\_20736 - Komponente ePA-Dokumentenverwaltung - Generelles schreibendes Zugriffsrecht für LEI** Die Komponente ePA-Dokumentenverwaltung MUSS einen schreibenden Zugriff ("C>Create" und "U"Update") gemäß Tabeller Zugriffsunterbindungsregeln in A\_19303) für eine per bei einem vorliegenden und gültigen Policy Document gemäß 9.3- A\_15442 für berechnigte LEI zulassen, selbst wenn die Policy diesen nicht ausdrücklich erlaubt. Wenn A\_19303 der LEI als Angehöriger einer bestimmten Berufsgruppe allgemein Zugriff auf die gewählte Dokumentenkategorie untersagt (d.h. bzw. A\_17460 für die Kategorie generell weder "C" noch "U" erlaubt), MUSS der Zugriff jedoch weiterhin abgelehnt werden.

[<=]

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

Aus diesem Grund ist der Bereich "Actions", der die erlaubten Operationen üblicherweise in APPC-Policy-Dokumenten beschreibt dort nicht gesetzt, um die APPC-Dokumente übersichtlich zu halten. Stattdessen werden die gemäß Berufsgruppe zur Verfügung stehenden Operationen in Tab\_Dokv\_030 (via A\_15173-02) festgelegt und geprüft.

Eine Ausnahme ist die generelle Erlaubnis für grundsätzlich berechnigte LEI (d.h. solche, für die eine wie auch immer geartete Policy eingestellt wurde), Dokumente in die Akte einzustellen, sofern sie für die gewählte Dokumentenkategorie generell das Zugriffsrecht "C" oder "U" gemäß Tab\_Dokv\_030 besitzen.

Beispiel: Ein gemäß APPC-Policy-Dokument berechnigter Kostenträger darf nur Dokumente der Kategorie 8 zugreifen, und zwar nach Tabelle ausschließlich mittels CU-Operation (create, update),

d.h. I-Document-Management::CrossGatewayDocumentProvide. Ein Zugriff auf andere Dokumentenkategorien würde durch das APPC-Policy-Dokument verhindert, ein Zugriff durch andere Operationen (bspw. ein Löschen via I- zulassen).

Liegt beim Vorliegen eines gültigen Policy Document-Management::RemoveMetadata) durch Tab\_Dokv\_030.

Beispiel 2: Ein Leistungserbringer ist nur auf ein einziges Dokument berechtigt (ein Whitelist-Eintrag). Es ist also weder ein grobgranulares noch ein mittelgranulares Zugriffsrecht vergeben worden. Der Leistungserbringer darf damit nur auf dieses eine Dokument lesend ("R") und ggf. löschend ("D") zugreifen, darf aber gemäß A\_20736 alle Dokumente einstellen, für deren Kategorie er nach Tab\_Dokv\_030 die Berechtigung "C" oder "U" besitzt. Letzteres Recht ist ihm auch nicht zu entziehen (außer über den kompletten Entzug der Berechtigung über Löschen der Policy).

Policy Documents trotzdem eine Verletzung der Zugriffsunterbindungsregeln bei Einstellung eines Dokuments in eine nicht zulässige Dokumentenkategorie vor, MUSS die Nachricht, welche dieser Autorisierungsprüfung zugrunde liegt, mit einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [ $\leq$ ]

die Berechtigung für klassifizierte Nutzer steuern (d.h. für den Versicherten, seine Vertreter, für Leistungserbringerinstitutionen sowie Kostenträger), referenzieren jeweils eine oder mehrere statische, akteninterne XACML 2.0 Policy (Permission Policies). Diese statischen Policies müssen für die Zugriffs kontrollprüfung innerhalb des Verarbeitungskontextes verfügbar sein und verlassen die ePA-Dokumentenverwaltung nicht. XACML 2.0 Policies, welche interne Permission Policies referenzieren, heißen im Folgenden Base Policies:

#### 5.4.2 Anforderungen an die Zugriffs kontrollprüfung

##### **A\_19997-01 - Zugriff durch Versicherten auf Schnittstelle**

##### **I\_Account\_Management\_Insurant und I\_Key\_Management\_Insurant**

Die Komponente ePA-Dokumentenverwaltung MUSS dem Versicherten über A\_15173-02 hinaus den Zugriff auf die Operationen der Schnittstellen I\_Account\_Management\_Insurant und I\_Key\_Management\_Insurant erlauben. [ $\leq$ ]

##### **A\_19998-01 - Zugriff durch Vertreter auf Operation**

##### **I\_Account\_Management\_Insurant::GetAuditEvents und GetSignedAuditEvents**

Die Komponente ePA-Dokumentenverwaltung MUSS einem berechtigten Vertreter des Versicherten über A\_15173-02 hinaus den Zugriff auf die Operation

I\_Account\_Management\_Insurant::GetAuditEvents() und

I\_Account\_Management\_Insurant::GetSignedAuditEvents() erlauben.

[ $\leq$ ]

##### ~~**A\_14933-01 - Komponente ePA-Dokumentenverwaltung - XML Schema-Validierung eines Policy Documents**~~

~~Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Documents (Advanced Patient Privacy Consents) dieses einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen. Ist ein Policy Document nicht wohlgeformt oder gültig, MUSS die Komponente ePA-Dokumentenverwaltung die Nachricht mit einem HTTP-Statuscode 200 oder 400 gemäß [RFC7231] quittieren und einen geeigneten Fehler in der IHE-Antwortnachricht zurückgeben. [ $\leq$ ]~~

##### ~~**A\_15536-02 - Komponente ePA-Dokumentenverwaltung - Prüfungen bei Registrierung eines Policy Documents**~~

~~Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Documents (Advanced Patient Privacy Consents) folgende inhaltlichen Prüfungen durchführen und im Fehlerfall die Nachricht mit einem HTTP-Statuscode 200 oder 400~~

gemäß [RFC7231] quittieren und einen geeigneten Fehler in der IHE Antwortnachricht zurückgeben:

- ~~Prüfung der XACML 2.0 Policy Konformität~~  
Die Komponente ePA Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn das Profil der vorliegenden XACML 2.0 Policy nicht mit den Anforderungen aus den Abschnitten 5.4.6.2 bis 5.4.6.5 übereinstimmt.
- ~~Prüfung der Aktenidentität~~  
Die Komponente ePA Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn das Resource Element mit der Attribut ID "urn:ihe:iti:ser:2016:patient-id" nicht mit der Identität der Akte aus dem internen Policy Document mit der Policy Set ID "urn:gematik:policy-set-id:insurant" übereinstimmt.
- ~~**A\_14822-02** Prüfung des Einstellers~~  
Die Komponente ePA Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn die in der Nachricht enthaltene SAML 2.0 Assertion (Authentication Assertion / X-User Assertion) nicht dem Versicherten oder einem seiner Vertreter zugeordnet ist (d.h. das root Attribut des InstanceIdentifier Elements innerhalb des SubjectMatch Elements muss mit der OID "1.2.276.0.76.4.8" eine KVNR kennzeichnen).
- ~~Keine Verwendung des "xsi:schemaLocation" Attributs~~  
Die Komponente ePA Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn ein xsi:schemaLocation Attribut gemäß [XMLSchema#2.6.3] enthalten ist. - **Komponente ePA-Dokumentenverwaltung - Attribute für Anfrage einer Autorisierungsentscheidung**
- ~~Verstöße gegen Policy Struktur und Inhalte~~  
Die Komponente ePA Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn sie Verstöße gegen die Vorgaben aus [gemSpec\_DM\_ePA#A\_14961] verstößt.

[<=>]

**A\_14822-01 Komponente ePA Dokumentenverwaltung Attribute für Anfrage einer Autorisierungsentscheidung** Die Komponente ePA-Dokumentenverwaltung MUSS das "Policy Pull"-Muster gemäß [IHE-ITI-ACWP] umsetzen und die folgenden Daten für eine Berechtigungsprüfung extrahieren sowie eine Autorisierungsanfrage gegen die vorhandenen Policy Documents Die Komponente ePA Dokumentenverwaltung MUSS das "Policy Pull"-Muster gemäß [IHE-ITI-ACWP] umsetzen und die folgenden Daten für eine Berechtigungsprüfung extrahieren sowie eine Autorisierungsanfrage gegen die vorhandenen Policy Documents (Advanced Patient Privacy Consents) stellen, um die autorisierte Verarbeitung eines Dokuments sicherzustellen:

- Subject ID oder XSPA Organization ID der Authentication Assertion / X-User Assertion
- unveränderbarer Teil der KVNR aus der Eingangsnachricht oder serverseitig mit Hilfe von Anfrageparametern beschafft (Aktenidentität)
- ~~wsa:Action Element aus der Eingangsnachricht~~
- ggf. Metadaten des DocumentEntry (u.a. confidentialityCode), des dazugehörigen SubmissionSets und etwaiger verbundener Ordner

[<=>]

### ~~A\_20217—Komponente ePA Dokumentenverwaltung—APPC Erweiterung für SubmissionSet.authorRole~~

Die Komponente ePA Dokumentenverwaltung MUSS das XACML Attribute "~~urn:gematik:ig:document-entry:related-submission-set:author-role~~" wie folgt unterstützen:

XACML Target Section	Resource
XACML Attribute ID	<del>urn:gematik:ig:document-entry:related-submission-set:author-role</del>
XACML Data Type	<del>urn:hl7-org:v3#CV</del>
XACML MatchID	<del>urn:hl7-org:v3:function:CV-equal</del>
XACML Attribute Value Content	<del>Use CX.4.2 as codeSystem and CX.1 as extension</del>
XACML Beispiel	<pre> &lt;Resource&gt;   &lt;ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal"&gt;     &lt;AttributeValue DataType="urn:hl7-org:v3#CV"&gt;       &lt;CodedValue code="102" codeSystem="1.3.6.1.4.1.19376.3.276.1.5.13"/&gt;     &lt;/AttributeValue&gt;     &lt;ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-entry:related-submission-set:author-role" DataType="urn:hl7-org:v3#CV"/&gt;   &lt;/ResourceMatch&gt; &lt;/Resource&gt; </pre>

[<=]

### ~~A\_16195—Komponente ePA Dokumentenverwaltung—UTF-8 Kodierung eines Policy Documents~~

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

#### ~~5.4.6.15.4.2.1~~ **Erstmaliges Öffnen eines Verarbeitungskontextes**

Beim erstmaligen Öffnen des Verarbeitungskontextes eines neu registrierten Aktenkontos durch den Versicherten muss dieser erkennen, dass er erstmalig geöffnet wird und die Aktenzustände "Registered" und "Registered for Migration" gemäß [\[gemSpec Aktensystem#6.1.1\]](#) unterscheiden. Darüber hinaus ist der Verarbeitungskontext für den Versicherten [gemäß der Anforderung A\\_15250](#) zu personalisieren. Die für die Personalisierung und die Unterscheidung der Aktenzustände erforderliche Konfiguration des Verarbeitungskontextes für das Aktenkonto erfolgt über die Authorization Assertion.

**A\_15603 - Komponente ePA-Dokumentenverwaltung – Nur Resume Account bei erforderlicher Datenübernahme möglich**

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

**5.4.6.2 Berechtigung für einen Versicherten****~~A\_15437-01 – Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Versicherten~~**

~~Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in Tab\_Dokv\_500 in Anhang C durchsetzen. [`<=`]~~

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

**~~A\_15250 – Komponente ePA-Dokumentenverwaltung – Aktivierung des Policy Documents "urn:gematik:policy-set-id:insurant"~~**

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

Die Festlegung des Zeitpunkts der Personalisierung ~~in der vorstehenden Anforderung~~ verhindert die Personalisierung eines Verarbeitungskontexts für den Fall, dass für ein mit der Option "Registered for Migration" registriertes Aktenkonto der Verarbeitungskontext geöffnet wird, ohne dass unmittelbar anschließend die Operation `I_Account_Management_Insurant::ResumeAccount` aufgerufen wird. Der Verarbeitungskontext verbleibt damit in seinem initialen (d.h. ungenutzten) Zustand, so dass der Vorgang konsistent neu gestartet werden kann.

**5.4.6.35.4.2.2 Berechtigung für einen Vertreter****~~A\_15440-02 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Document zur Berechtigung eines Vertreters~~**

~~**5.4.6.4 A\_15178 – Komponente ePA-Dokumentenverwaltung – Unveränderliches Policy Document "urn:gematik:policy-set-id:insurant" Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-id:insurant" nach ihrer Aktivierung**~~

### ~~kontinuierlich und dauerhaft unverändert für die Zugriffskontrollprüfung wirksam ist. [ <= ] Berechtigung für einen Vertreter~~

~~**A\_15440-01 – Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Vertreters**~~  
 Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten übermittelte XACML 2.0 Policy auf Konformität als ~~übermitteltes~~ Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in ~~Tab\_Dokv\_501 in Anhang C der Policy-Definition~~ [gemSpec\_ePA\_Policy\_Vertreter] prüfen. [ <= ]

### ~~**A\_15441-01 – Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Vertreters mit erlaubten Operationen**~~

Die Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in ~~Tab\_Dokv\_501 in Anhang C~~ erstellen und durchsetzen. [ <= ]

### **A\_15180 - Komponente ePA-Dokumentenverwaltung – Prüfung auf weitere, unerlaubte Vertreterberechtigungen**

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

### **5.4.6.55.4.2.3 Berechtigung für eine Leistungserbringerinstitution**

#### **A\_15442-03 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Document zur Berechtigung einer Leistungserbringerinstitution**

~~**A\_15442-02 – Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung einer Leistungserbringerinstitution**~~  
 Die Komponente ePA-Dokumentenverwaltung MUSS ~~eine~~ein vom ePA-Frontend des Versicherten bzw. vom Fachmodul ePA übermittelte XACML 2.0 Policy auf Konformität als ~~übermitteltes~~ Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt ~~von Tab\_Dokv\_502 der Policy-Definition~~ in ~~Anhang C~~ [gemSpec\_ePA\_Policy\_LEI] prüfen. [ <= ]

### **5.4.6.65.4.2.4 Berechtigung für einen Kostenträger**

#### **A\_17460-02 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Document zur Berechtigung eines Kostenträgers**

~~**A\_17460-01 – Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Kostenträgers**~~  
 Die Komponente ePA-Dokumentenverwaltung MUSS ~~eine~~ein vom ePA-Frontend des Versicherten übermittelte XACML 2.0 Policy auf Konformität als ~~übermitteltes~~ Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in ~~Tab\_Dokv\_503 der Policy Definition~~ in ~~Anhang C~~ [gemSpec\_ePA\_Policy\_KTR] prüfen. [ <= ]

### 5.4.75.4.3 Upgrade von ePA Release 3.1.3 auf ePA Release 4

Bei einem Upgrade von ePA Release 3.1.3 auf Release 4 ändert sich das Berechtigungssystem. Deshalb müssen zum einen Dokumentenmetadaten ([d.h. confidentialityCode](#)) und zum anderen die Berechtigungsregeln selbst ([APPC-Policy-Dokumente Documents](#)) angepasst werden. Davon sind nicht nur neue Dokumente betroffen, sondern es müssen auch bestehende Metadaten und ~~Policies~~[das jeweilige Policy Document](#) angepasst werden.

Im Ergebnis akzeptiert die ePA-Dokumentenverwaltung in Release 4 alte [Policy-Dokumente Documents](#) und Dokumente mit alten confidentialityCodes (beides gemäß ~~gemäß~~ ePA Release 3.1.3), liefert nach außen jedoch beides nur nach neuen Vorgaben (~~gemäß~~ Release 4) zurück. Dieses Verhalten soll es ~~auch~~ (insbesondere) Primärsystemen nach alter Spezifikation erlauben, mit einem aktuellen [ePA-Aktensystem](#) zu kommunizieren.

#### A\_20039-01 - Komponente ePA-Dokumentenverwaltung – Transformation eines Policy Document

##### ~~A\_20039 – Komponente ePA-Dokumentenverwaltung – Transformation von~~

~~Policy Dokumenten hin zu neuerer Version~~ Die Komponente ePA-Dokumentenverwaltung MUSS ~~sämtliche XACML 2.0 Policies gemäß~~ [das Policy Document des anfragenden Berechtigten transformieren. Die Policy-Definition in Anhang B umwandeln in XACML 2.0 \(ePA1-Policies\) MUSS in eine Policy-Definition aus \[gemSpec ePA Policy LEI\], \[gemSpec ePA Policy KTR\] sowie \[gemSpec ePA Policy Vertreter\] \(ePA2-Policies gemäß Anhang C, \) umgewandelt werden, sobald](#)

[eine XACML 2.0 Policy gemäß Anhang B eingestellt die Zugriffsberechtigung des Anfragenden geprüft](#) wird. [ $\leq$ ]

7

- ~~• ein Zugriffsversuch auf eine XACML 2.0 Policy gemäß Anhang B erfolgt.~~

[ $\leq$ ] Während die Transformation ~~der~~ [des Policy-Dokumente Document](#) stattfindet, und solange sie nicht abgeschlossen ist, werden weitere Zugriffsversuche mit der Fehlermeldung "Aktenkonto vorübergehend nicht erreichbar" abgelehnt.

#### A\_20049-03A\_20049-02 - Komponente ePA-Dokumentenverwaltung – Regeln für die Policy-Transformation

Bei der Transformation ~~der XACML 2.0 des~~ [Policy Document](#) ohne die Versionsangabe @Version ([ePA1-Policies](#)) MUSS ~~dieses~~ vom Client ~~eingestellten Base~~ und ggf. ~~vorhandene Permission Policies durch eine entsprechende XACML 2.0 eingestellte~~ [Policy Document durch ein Policy Document mit Versionsangabe @Version \(ePA2-Policy\) gemäß der Policy-Definitionen in \[gemSpec ePA Policy LEI\], \[gemSpec ePA Policy KTR\] sowie \[gemSpec ePA Policy Vertreter\]](#) ersetzt werden. Bei der Transformation gelten folgende Vorgaben:

- Das Ablaufdatum MUSS übernommen werden.
- Bei LEI-, KTR- und Vertreter-Base-Policydokumenten Policies muss der Name der Institution bzw. des Vertreters aus `//PolicySet/Target/Subjects[2]/SubjectMatch/AttributeValue` stattdessen nach `//PolicySet/Description` übernommen werden (**Hinweis:** das Element `Subjects[2]`) wird durch die `Description` abgelöst). Bei einer LEI- und KTR-Base-Policy muss nach dem Namen der Ersetzung Institution gefolgt von einem Doppelpunkt die ProfessionOID angehängt werden. Diese ist aus der

~~XACML 2.0 Policies ohne Versionsangabe (alt) durch XACML 2.0 Policies mit Versionsangabe (neu) Authentication Assertion zu extrahieren.~~

- Bei der Transformation einer LEI-Base-Policy MÜSSEN folgende Zugriffsregeln in einer Policy-Definitionen aus [gemSpec\_ePA\_Policy\_LEI] umgesetzt werden (Zugriffsrecht alt wird zu Zugriffsrecht neu):
- ~~alt: LEI, neu: alt: LEI, neu:~~ Anhand der ProfessionOID gemäß A 19303 die maximal zulässigen Dokumentenkategorien der Liste practitioner, hospital, laboratory, physiotherapy, psychotherapy, dermatology, gynaecology\_urology, dentistry\_oms, other\_medical, other\_non\_medical, emp, nfd, eab;
- alt: PAT, neu: patientdoc;
- alt: KTR, neu: receipt;
- neu: Die ~~Vertrauensstufe~~Vertraulichkeitsstufe "normal" (~~grobgranulare Berechtigung~~) wird vorgegeben MUSS in der Policy gesetzt werden.
- Bei der Transformation einer KTR-Base-Policy MUSS ein Policy Document gemäß [gemSpec\_ePA\_Policy\_KTR] angelegt werden. [<=]
- Bei der Transformation einer Vertreter-Base-Policy MUSS ein Policy Document gemäß [gemSpec\_ePA\_Policy\_Vertreter] angelegt werden.
- Etwaige Dokumente MÜSSEN gemäß A 19388 den Ordnern entsprechend der Dokumentenkategorie zugewiesen werden.

–

[<=]

#### **A\_20046-03A\_20046 - Komponente ePA-Dokumentenverwaltung – Transformation des confidentialityCodes bei eingestellten Dokumenten**

Die Komponente ePA-Dokumentenverwaltung MUSS mit dem Update auf ePA 2.0 bei allen Dokumenten eines Versicherten, bei denen der confidentialityCode auf "PAT" gesetzt ist, diese Dokumente dem Folder "patientdoc" (gemäß A 19388, Tab\_DM Dokumentenkategorien, Zeile Nr. 6) zuordnen. Die Komponente ePA-Dokumentenverwaltung MUSS bei allen Dokumenten eines Versicherten, bei denen der confidentialityCode "PAT", "LEI", "LEÄ" oder "KTR" gesetzt ist, diesen Eintrag löschen und stattdessen den confidentialityCode "normal" setzen. Diese Transformation MUSS durch die Komponente ePA-Dokumentenverwaltung nach dem ersten erfolgreichen Öffnen der Akte des Versicherten (Operation I\_Document\_Management\_Connect::OpenContext()) und nachfolgend beim Einstellen jedes DocumentEntry, der noch alte confidentialityCodes enthält, durchgeführt werden.

[<=]

Damit soll die Transformation zum frühestmöglichen Zeitpunkt durch die ePA\_Dokumentenverwaltung durchgeführt werden.

#### **A\_20050-01 - Komponente ePA-Dokumentenverwaltung – Abbildung von Suchanfragen nach confidentialityCodes und deren Ergebnisse**

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

- alt: LEI, neu: practitioner, hospital, laboratory, physiotherapy, psychotherapy, dermatology, gynaecology\_urology, dentistry\_oms, other\_medical, other\_non\_medical, emp, nfd, eab;
- alt: PAT, neu: patientdoc;
- alt: KTR, neu: receipt;

#### [<=]

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

### 5.4.4 Simulierte Berechtigung

#### **A 21705 - Komponente ePA-Dokumentenverwaltung – Simulation der lesbaren Dokumente für eine Leistungserbringerinstitution**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS ein Policy Document anhand der XDS-Metadaten gemäß

[gemSpec DM ePA#A 14961] verarbeiten. Ist anhand der Metadaten

SubmissionSet.contentTypeCode = "simulatedAuthorization" erkennbar, dass es eine

simulierte Berechtigungsanfrage eines ePA-FdVs ist, MUSS die Komponente ePA-

Dokumentenverwaltung mögliche Dokumente identifizieren, welche durch dieses Policy

Document durch die Leistungserbringerinstitution lesbar sind oder bei potentieller

Registrierung lesbar wären. Das Policy Document DARF NICHT dauerhaft

gespeichert werden. Weiterhin MUSS der Submission Request mit einem

InvalidDocumentContent-Fehlercode sowie HTTP-Statuscode 200 beantwortet

werden. Pro identifiziertes Dokument MUSS ein RegistryError-Element mit der UniqueID

des Dokuments (codeContext) und des InvalidDocumentContent-Fehlercode (code)

zurückgegeben werden. [<=]

## 5.5 Vertrauenswürdige Ausführung

### 5.5.1 Schnittstelle I\_Document\_Management\_Connect

Diese Schnittstelle setzt die in [gemSysL\_ePA] definierte Schnittstelle I\_Document\_Management\_Connect technisch um. Die logische OperationI\_Document\_Management\_Connect::ConnectToContext aus [gemSysL\_ePA] wird durch den Verbindungsaufbau der Clients zum Verarbeitungskontext der ePA-Dokumentenverwaltung umgesetzt. Die Client-Verbindungen vom Fachmodul ePA zu der Schnittstelle sowie vom ePA-Frontend des Versicherten zu der Schnittstelle werden über HTTP hergestellt. Die Schnittstelle ermöglicht beiden Clients den Aufbau eines sicheren Kanals auf Inhaltsebene zum Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung (VAU), die Aktivierung des Verarbeitungskontextes mittels Übergabe des Kontextschlüssels sowie die Beendigung ihrer Client-Verbindung. Das Fachmodul ePA baut zum Kontextmanagement je Aktensession eine TLS-Verbindung auf. Die Verbindung des ePA-Frontends des Versicherten zum Kontextmanagement erfolgt mittels Weiterleitung der HTTP Requests und HTTP Responses durch das Zugangsgateway, welches auch einen HTTP Header zur Identifikation der Sitzung setzt.

Das Protokoll für den Verbindungsaufbau zwischen Clients und dem Verarbeitungskontext folgt den Spezifikationen in [gemSpec\_Krypt#3.15] und [gemSpec\_Krypt#6]. Zur Prüfung der Autorisierung des Clients durch das Kontextmanagement wird das dort

beschriebene Protokoll um zwei zusätzliche Schlüssel-Wert-Paare ergänzt, die die Authorization Assertion im HTTP Body in der VAUClientHello-Nachricht und optional einen Sitzungsbezeichner im HTTP Header übermitteln.

#### **A\_15587 - Komponente ePA-Dokumentenverwaltung – Implementierung des sicheren Verbindungsprotokolls**

Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS für die Schnittstelle `I_Document_Management_Connect` das Kommunikationsprotokoll gemäß den Vorgaben aus [gemSpec\_Krypt#3.15] und [gemSpec\_Krypt#6] umsetzen.  
[<=]

#### **A\_15592-03 - Komponente ePA-Dokumentenverwaltung – Erweiterung des sicheren Verbindungsprotokolls**

Ein Client (d.h. ePA-Fachmodul, ePA-Frontend des Versicherten, Fachmodul ePA KTR-Consumer) MUSS bei der Erzeugung der VAUClientHello-Nachricht (vgl. [A\\_16883-01](#)) im Datenfeld `AuthorizationAssertion` die Base64-kodierte Authorization Assertion eintragen.

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

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

#### **A\_14631-02 - Komponente ePA-Dokumentenverwaltung – HTTP-Schnittstelle I\_Document\_Management\_Connect**

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

#### **A\_15540 - Komponente ePA-Dokumentenverwaltung – TLS-Schnittstelle I\_Document\_Management\_Connect**

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die Schnittstelle `I_Document_Management_Connect` für TLS-Verbindungen des Fachmoduls ePA sowie des Fachmoduls ePA KTR-Consumer verfügbar machen.  
[=<]

#### **A\_15588 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext bei Bedarf verfügbar machen**

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

#### **[A\\_14633-03](#)~~A\_14633-02~~ - Komponente ePA-Dokumentenverwaltung – Vermittlung der Verbindung zwischen Client und Verarbeitungskontext**

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

- die Base64-dekodierte Authorization Assertion der VAUClientHello-Nachricht auf Gültigkeit gemäß Anforderung [A\\_13690](#) sowie auf den gültigen Berechtigungstyp (`AuthorizationType = "DOCUMENT_AUTHORIZATION"`) oder "ACCOUNT\_AUTHORIZATION" prüfen und bei ungültiger Authorization Assertion den Verbindungsaufbau abbrechen und mit dem HTTP-Fehler 403 antworten,
- den Record Identifier des Verarbeitungskontextes über den Wert des Attributs `Resource ID` aus der Authorization Assertion der VAUClientHello-Nachricht ermitteln,

- für Clients vom Typ ePA-Frontend des Versicherten die Verbindung auf der Grundlage des vom Zugangsgateway gesetzten HTTP Header-Feldes `Session` registrieren,
- für Clients vom Typ Fachmodul ePA die Verbindung auf Grundlage der TLS-Sitzung (Session-ID) oder auf Grundlage der KeyID des VAU-Kanals [`gemSpec_Krypt`] (mit der Ausnahme, dass im Rahmen des Handshakes `VAUClientHelloDataHash` zur Zuordnung des Verarbeitungskontext verwendet wird), registrieren,
- während der Dauer der Sitzung alle eingehenden Requests auf der Grundlage der registrierten Verbindung an den Zielverarbeitungskontext weiterleiten sowie
- nach dem Ende der Sitzung, aufgrund eines Timeouts bzw. aufgrund einer Beendigung durch den Nutzer, die Registrierung der Verbindung löschen.

[<=]

**A\_21746-01 - Komponente ePA-Dokumentenverwaltung – Zulässige Operationen bei Betreiberwechselautorisierung**

Die ePA-Dokumentenverwaltung MUSS die folgenden Prüfungen durchführen, wenn die Autorisierung mit einer Betreiberwechselautorisierung (`AuthorizationType` der `Authorization Assertion = "ACCOUNT AUTHORIZATION"`) erfolgt ist:

- In den Zuständen `START MIGRATION` und `SUSPENDED` des Aktensystems des authentifizierten Nutzers ist als auszuführende Operation nur `suspendAccount` möglich.
- In den Zuständen `REGISTERED FOR MIGRATION` und `DL IN PROGRESS` des Aktensystems des authentifizierten Nutzers ist als auszuführende Operation nur `resumeAccount` möglich.
- Im Zustand `READY FOR IMPORT` des Aktensystems des authentifizierten Nutzers darf kein Operationsaufruf erfolgen. Lediglich beim Öffnen des Verarbeitungskontext darf der Import des bereits heruntergeladenen Migrationspakets erfolgen.

Sofern keine dieser Bedingungen erfüllt ist, MUSS die aufgerufene Operation mit dem Fehler `ACCESS DENIED` beendet werden.[<=]

**A\_20580 - Komponente ePA-Dokumentenverwaltung – TLS Session Resumption mittels Session-ID nutzen**

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

[<=]

**A\_14617-02 - Komponente ePA-Dokumentenverwaltung – Ablauf des Verbindungsaufbaus**

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

**Tabelle 35: Tab\_Dokv\_29 - Ablauf Operation Hello**

Nr.	Sub-Komponente	Beschreibung
-----	----------------	--------------

	(Client)	(Senden des HTTP Request mit VAUClientHello-Nachricht)
1	Kontextmanagement	Prüfen der Authorization Assertion der VAUClientHello-Nachricht auf Gültigkeit gemäß Anforderung A_13690 und Abbruch des Verbindungsaufbaus mit HTTP-Fehler 403 (Fehlermeldung "Access Denied") bei ungültiger Authorization Assertion.
2	Kontextmanagement	Extrahieren des Record Identifiers über den Wert des Attributs XSPA Resource ID aus der Authorization Assertion
3	Kontextmanagement	Prüfen, ob ein Verarbeitungskontext für den Record Identifier bereits initialisiert ist und Starten eines Verarbeitungskontextes, falls dies nicht der Fall ist
4	Kontextmanagement	Registrieren der Verbindung zwischen dem Client und dem Verarbeitungskontext für den Record Identifier für die Vermittlung des folgenden Nachrichtenaustauschs
5	Kontextmanagement	Weiterleiten der VAUClientHello-Nachricht an den Verarbeitungskontext für den Record Identifier
6	Verarbeitungskontext	Registrieren der Authorization Assertion der VAUClientHello-Nachricht und Erzeugen der VAUServerHello-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
7	Verarbeitungskontext	Senden der VAUServerHello-Nachricht
8	Kontextmanagement	Weiterleiten der VAUServerHello-Nachricht an den Client
9	Verarbeitungskontext	Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
	(Client)	(Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6])
	(Client)	(Erzeugen und Senden der VAUClientSigFin-Nachricht)
10	Kontextmanagement	Weiterleiten der VAUClientSigFin-Nachricht an den Verarbeitungskontext für den RecordIdentifier Record Identifier
11	Verarbeitungskontext	Prüfen auf Identität des authentifizierten Nutzers (Subject::Subject-id bzw. Subject::Organization-id der Authorization Assertion entspricht der KVNR bzw. Telematik-ID des übergebenen Zertifikats der Client-

		Authentisierung gemäß [gemSpec_Krypt#A_17070]) Im Fehlerfall MUSS der Verbindungsaufbau abgebrochen und mit einer VAUServerError-Nachricht beantwortet werden.
12	Verarbeitungskontext	Erzeugen der VAUServerErrorFin-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
13	Kontextmanagement	Weiterleiten der VAUServerErrorFin-Nachricht an den Client

[<=]

Der abgeleitete Sitzungsschlüssel wird anschließend vom Client und vom Verarbeitungskontext gemäß [gemSpec\_Krypt#3.15] und [gemSpec\_Krypt#6] genutzt, um alle fachlichen Eingangs- und Ausgangsnachrichten zu ver- und entschlüsseln.

### **A 14545-05A\_14545-03 - Komponente ePA-Dokumentenverwaltung – Operationen des Dokumenten-, Konto- und Schlüsselmanagements nur über sicheren Kanal**

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

- I\_Document\_Management::CrossGatewayDocumentProvide
- I\_Document\_Management::CrossGatewayQuery
- I\_Document\_Management::RemoveMetadata
- I\_Document\_Management::RemoveDocuments
- I\_Document\_Management::CrossGatewayRetrieve
- I\_Document\_Management::RestrictedUpdateDocumentSet
- I\_Document\_Management\_Insurance::ProvideAndRegisterDocumentSet-b
- I\_Document\_Management\_Insurant::ProvideAndRegisterDocumentSet-b
- I\_Document\_Management\_Insurant::RestrictedUpdateDocumentSet
- I\_Document\_Management\_Insurant::RegistryStoredQuery
- I\_Document\_Management\_Insurant::RemoveDocuments
- I\_Document\_Management\_Insurant::RemoveMetadata
- I\_Document\_Management\_Insurant::RetrieveDocumentSet
- I\_Account\_Management\_Insurant::GetAuditEvents
- I\_Account\_Management\_Insurant::GetSignedAuditEvents
- I\_Account\_Management\_Insurant::SuspendAccount
- I\_Account\_Management\_Insurant::ResumeAccount
- I\_Key\_Management\_Insurant::StartKeyChange
- I\_Key\_Management\_Insurant::GetAllDocumentKeys

- I\_Key\_Management\_Insurant::PutAllDocumentKeys
- I\_Key\_Management\_Insurant::FinishKeyChange
- I\_Document\_Management\_Connect::OpenContext
- I\_Document\_Management\_Connect::CloseContext

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

**A\_14645-01 - Komponente ePA-Dokumentenverwaltung – Nutzung des sicheren Kanals zwischen ePA-Frontend des Versicherten bzw. Fachmodul ePA, Fachmodul ePA KTR-Consumer und Verarbeitungskontext**

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

**A\_14457 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I\_Document\_Management\_Connect**

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

**Tabelle 36: 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		

<b>XML Schema</b>	DocumentManagementConnectService.xsd
-------------------	--------------------------------------

[&lt;=]

### 5.5.1.1 Operation **I\_Document\_Management\_Connect::OpenContext**

#### **A\_14426 - Komponente ePA-Dokumentenverwaltung – Signatur für**

#### **I\_Document\_Management\_Connect::OpenContext**

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

`I_Document_Management_Connect::OpenContext` gemäß der folgenden Signatur implementieren:

**Tabelle 37: Tab\_Dokv\_31 - Operation OpenContext**

<b>Operation</b>	<b>I_Document_Management_Connect::OpenContext</b>		
<b>Beschreibung</b>	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management_Connect::OpenContext</code> technisch um. Mit dieser Operation wird der Kontextschlüssel an den Verarbeitungskontext übergeben.		
<b>Formatvorgabe n</b>	SOAP Action: <code>http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0/OpenContext</code>		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
<b>ContextKey</b>	Der Kontextschlüssel	<code>ContextKey</code>	n
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
-	-	-	-
<b>Technische Fehlermeldungen</b>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>INTERNAL_ERROR</b>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
<b>INVALID_AUTH_KEY</b>	Der Kontextschlüssel ist ungültig.	Wenn der Vergleich mit einem bereits im Verarbeitungskontext	

		vorhandenen Kontextsschlüssel keine Übereinstimmung ergibt, oder das Entschlüsseln von Kontextdaten fehlschlägt
<b>SYNTAX_ERROR</b>	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.

[<=]

### 5.5.1.1.1 Umsetzung

#### **A\_14687-01 - Komponente ePA-Dokumentenverwaltung – Ablauf der Operation Open Context**

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

`I_Document_Management_Connect::OpenContext` so umsetzen, dass nach einem Aufruf der Operation durch einen Client, d.h. durch ein ePA-Frontend des Versicherten, ein Fachmodul ePA oder ein Fachmodul ePA KTR-Consumer, der folgende Ablauf in angegebener Reihenfolge (1 - 6) ausgeführt wird:

**Tabelle 38: Tab\_Dokv\_32 - Ablauf der Operation Open Context**

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden der <code>OpenContextRequest</code> -Nachricht über den sicheren Kanal zwischen Client und Verarbeitungskontext)
1	Kontextmanagement	Weiterleiten der <code>OpenContextRequest</code> -Nachricht an den Verarbeitungskontext gemäß den vorgehaltenen Zuordnungsdaten (siehe Anforderung A_14633)
2	Verarbeitungskontext	Entnahme des im Eingangsparameter <code>ContextKey</code> enthaltenen Kontextschlüssels
3	Verarbeitungskontext	Falls bereits eine Sitzung mit einem Nutzer besteht, Prüfung des neu erhaltenen Kontextschlüssels auf Übereinstimmung mit dem aus der bestehenden Sitzung bereits registrierten Kontextschlüssel und Abbruch mit Fehlermeldung <code>INVALID_AUT_KEY</code> bei Nichtübereinstimmung
4	Verarbeitungskontext	Falls nicht bereits eine Sitzung mit einem Nutzer besteht, Laden der benötigten Kontextdaten aus dem Speichersystem, Entschlüsseln mit dem erhaltenen Kontextschlüssel und Abbruch mit Fehlermeldung <code>INVALID_AUT_KEY</code> , falls die Entschlüsselung der Kontextdaten fehlschlägt.  Sind keine Kontextdaten mit dem Verarbeitungskontext assoziiert (d.h. erstmaliges Öffnen) MUSS der

		Kontextschlüssel in der Sitzung verwendet werden, um die neu erzeugten Kontextdaten zu verschlüsseln. In diesem beschriebenen Fall wird die Verarbeitung nicht mit der Fehlermeldung INVALID_AUT_KEY abgebrochen.
5	Verarbeitungskontext	Senden der <code>OpenContextResponse</code> -Nachricht
6	Kontextmanagement	Weiterleiten der <code>OpenContextResponse</code> -Nachricht an den Client

[<=]

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

### 5.5.1.2 Operation `I_Document_Management_Connect::CloseContext`

#### A\_14462 - Komponente ePA-Dokumentenverwaltung – Signatur für `I_Document_Management_Connect::CloseContext`

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

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

**Tabelle 39: Tab\_Dokv\_33 - Operation Close Context**

Operation	<code>I_Document_Management_Connect::CloseContext</code>		
<b>Beschreibung</b>	Diese Operation setzt die in [gemSysL_ePA] in definierte Operation <code>I_Document_Management_Connect::CloseContext</code> technisch um. Mit dieser Operation wird die Verbindung zum Verarbeitungskontext beendet. Der Verarbeitungskontext kann geschlossen werden, falls nicht eine andere Verbindung noch besteht.		
<b>Formatvorgaben</b>	SOAP Action: <code>http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0/CloseContext</code>		
<b>Eingangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>
-	-	-	-
<b>Ausgangsparameter</b>			
<b>Name</b>	<b>Beschreibung</b>	<b>Typ</b>	<b>opt.</b>

-	-	-	-
<b>Technische Fehlermeldungen</b>			
<b>Name</b>	<b>Fehlertext</b>	<b>Details</b>	
<b>INTERNAL_ERROR</b>	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	

[&lt;=]

## 5.5.1.2.1 Umsetzung

**A\_14707-02 - Komponente ePA-Dokumentenverwaltung – Ablauf der Operation Close Context**

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

**Tabelle 40: Tab\_Dokv\_34 - Ablauf Operation CloseContext**

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden der <code>CloseContextRequest</code> -Nachricht über den sicheren Kanal zwischen Client und Verarbeitungskontext)
1	Kontextmanagement	Weiterleiten der <code>CloseContextRequest</code> -Nachricht an den Verarbeitungskontext gemäß den vorgehaltenen Zuordnungsdaten (siehe Anforderung A_14633)
2	Verarbeitungskontext	Senden der <code>CloseContextResponse</code> -Nachricht
3	Kontextmanagement	Weiterleiten der <code>CloseContextResponse</code> -Nachricht an den Client
4	Verarbeitungskontext	Prüfen, ob mindestens eine weitere Sitzung existiert, ignorieren der <code>CloseContextRequest</code> -Nachricht, falls dies der Fall ist und Abbruch der Operation
5	Verarbeitungskontext	Falls keine weitere Sitzung existiert, persistieren geänderter Kontextdaten und Beenden des Verarbeitungskontextes
6	Kontextmanagement	Löschen der Verbindungszuordnung zwischen Client und Verarbeitungskontext

[&lt;=]

## 5.5.2 Hardware-Merkmale

Die Vertrauenswürdige Ausführungsumgebung setzt die Nutzung eines HSM zur Speicherung und Anwendung der privaten Schlüssel von Dienstzertifikaten und Schlüsselpaaren gemäß Anforderung A\_14564 voraus.

## 5.6 Statische Akteninhalte

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

### ~~A\_20191-01A\_20191~~ - Komponente ePA-Dokumentenverwaltung – Anlegen von statischen Ordnern

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

~~I\_Document\_Managemet\_Connect::OpenContext()~~) ~~folgende Kategorienordner aus A\_19388-\* und gemSpec\_DM#20190-\* unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in gemSpec\_DM\_ePA#A\_14760-01 (Belegung der restlichen Metadatenfelder) für den Versicherten anlegen. Alle Kategorienordner mit jeweils einem Ordner pro Kategorie, mit Ausnahme der Kategorien 3 (childsrecord) und 4 (mothersrecord), die nicht von der ePA-Dokumentenverwaltung erstellt werden. Hinweis: Die Clientsysteme erstellen jeweils einen Ordner pro Kind, mit Folder.title für den Namen des Kindes. Alle statischen Ordner sind nach dem Anlegen initial leer.~~

~~[<=]~~

~~die folgenden Ordner für den Versicherten anlegen:~~

- ~~• Kategorienordner, jeweils einen pro Kategorie 1a\* gemäß gemSpec\_DM\_ePA#A\_20190-01 gemSpec\_DM\_ePA#A\_20190 (Belegung Folder.codeList) unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in gemSpec\_DM\_ePA#A\_14760-01 (Belegung der restlichen Metadatenfelder).~~

~~Alle statischen Ordner sind nach dem Anlegen initial leer.~~ ~~[<=]~~

### ~~A\_20214~~ — Komponente ePA-Dokumentenverwaltung — Anlegen von Permission Policies

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

~~I\_Document\_Managemet\_Connect::OpenContext()) alle in Abschnitt 9.5 aufgeführten Permission Policies für den Versicherten anlegen.~~ ~~[<=]~~

### ~~A\_20215~~ — Komponente ePA-Dokumentenverwaltung — Keine Herausgabe von Permission Policies

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

### ~~A\_20216-02A\_20216~~ - Komponente ePA-Dokumentenverwaltung – Unveränderlichkeit von statischen Akteninhalten

Die Komponente ePA-Dokumentenverwaltung DARF die Metadaten eines statischen Aktenobjekts nach Abschnitt 5.6 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen. Dabei gelten folgende Ausnahmen:

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

- Während des Aktenumzugs MUSS bei einem Import eines Exportpakets (mitsamt der Ordner und zugehörigen Assoziationen) der statische Akteninhalt überschrieben werden.

[<=]

---

## 6 Informationsmodelle

---

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

## 7 Anhang A – Verzeichnisse

### 7.1 Abkürzungen

Kürzel	Erläuterung
<a href="#">AdV</a>	<a href="#">Anwendungen des Versicherten</a>
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BPPC	Basic Patient Privacy Consents
<a href="#">CRUD</a>	<a href="#">Create Read Update Delete</a>
<a href="#">ePA-FdV</a>	<a href="#">ePA-Frontend des Versicherten</a>
<a href="#">ePA-FdV AdV</a>	<a href="#">ePA-Frontend des Versicherten im KTR-AdV-Terminal</a>
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
<a href="#">KTR</a>	<a href="#">Kostenträger</a>
<a href="#">MIO</a>	<a href="#">Medizinisches Informationsobjekt</a>

MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
<a href="#">PDSG</a>	<a href="#">Patientendaten-Schutz-Gesetz</a>
PHR	Personal Health Record
RMU	Restricted Metadata Update Profile
SAML	Security Assertion Markup Language
TLS	Transport Layer Security
UUID	Universally Unique Identifier
VAU	Vertrauenswürdige Ausführungsumgebung
W3C	World Wide Web Consortium
WS-I	Web-Services Interoperability Consortium
XCA	Cross-Community Access Profile
XDR	Cross-Enterprise Document Reliable Interchange Profile
XDS	Cross-Enterprise Document Sharing ProfileGetAllDocumentKeys
XCDR	Cross-Community Document Reliable Interchange Profile
XACML	eXtensible Access Control Markup Language

XDW	Cross-Enterprise Document Workflow Profile
XOP	XML-binary Optimized Packaging
XSPA	Cross-Enterprise Security and Privacy Authorization Profile
XUA	Cross-Enterprise User Assertion Profile

## 7.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

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

## 7.3 Abbildungsverzeichnis

Abbildung 1: Komponentenzerlegung ePA-Dokumentenverwaltung .....	15
Abbildung 2: Zustandsübergänge Schlüsselwechsel .....	103
Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen .....	123
Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen .....	124

## 7.4 Tabellenverzeichnis

<del>Tabelle 1: Tab_Dokv_10 – Kennzeichnung von Optionalitäten .....</del>	<del>24</del>
<del>Tabelle 2: Tab_Dokv_11 – Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung .....</del>	<del>24</del>
<del>Tabelle 3: Tab_Dokv_12 – Fehlercodes zu Fehlern gemäß Operationsdefinition .....</del>	<del>33</del>
<del>Tabelle 4: Tab_Dokv_35 – Eingangsparameter für TUC_PKI_018 .....</del>	<del>40</del>
<del>Tabelle 5: Tab_Dokv_13 – Parameter des § 291a-Protokolls .....</del>	<del>42</del>
<del>Tabelle 6: Tab_Dokv_14 – Schnittstelle I_Document_Management .....</del>	<del>53</del>
<del>Tabelle 7: Tab_Dokv_16 – Operation Cross-Gateway Query .....</del>	<del>57</del>

Tabelle 8: Tab_Dokv_17— Operation Remove Documents .....	60
Tabelle 9: Tab_Dokv_17— Operation RemoveMetadata .....	61
Tabelle 10: Tab_Dokv_18— Operation Cross Gateway Retrieve .....	63
Tabelle 11: Tab_Dokv_45— Operation Restricted Update Document Set .....	65
Tabelle 12: Tab_Dokv_20— Schnittstelle I_Document_Management_Insurant .....	67
Tabelle 13: Tab_Dokv_21— Operation Provide And Register Document Set b .....	69
Tabelle 14: Tab_Dokv_22— Operation Registry Stored Query.....	72
Tabelle 15: Tab_Dokv_23— Operation RemoveMetadata .....	77
Tabelle 16: Tab_Dokv_24— Operation Retrieve Document Set .....	79
Tabelle 17: Tab_Dokv_19— Operation RestrictedUpdateDocumentSet .....	81
Tabelle 18: Tab_Dokv_36— Schnittstelle I_Document_Management_Insurance .....	84
Tabelle 19: Tab_Dokv_37— Operation Provide And Register Document Set b .....	85
Tabelle 20: Tab_Dokv_25— Schnittstelle I_Account_Management_Insurant .....	89
Tabelle 21: Tab_Dokv_26— Operation Suspend Account .....	90
Tabelle 22: Tab_Dokv_27— Operation Resume Account .....	93
Tabelle 23: Tab_Dokv_28— Operation Get Audit Events .....	97
Tabelle 24: Tab_Dokv_44— Operation Get Signed Audit Events.....	99
Tabelle 25: Tab_Dokv_38— Operation I_Key_Management_Insurant::StartKeyChange() .....	106
Tabelle 26: Tab_Dokv_39— Operation I_Key_Management_Insurant::GetAllDocumentKeys() .....	109
Tabelle 27: Tab_Dokv_40— Operation I_Key_Management_Insurant::PutAllDocumentKeys() .....	112
Tabelle 28: Tab_Dokv_41— Operation I_Account_Management_Insurant::FinishKeyChange().....	114
Tabelle 29: Tab_Dokv_42— Zusätzliche Parameter des § 291a-Protokolls für die Umschlüsselung .....	116
Tabelle 30: Tab_Dokv_43— Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung .....	117
Tabelle 31: Tab_Dokv_43— Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung .....	117
Tabelle 32: Tab_Dokv_030— Zugriffsunterbindungsregeln .....	126
Tabelle 33: Tab_Dokv_29— Ablauf Operation Hello .....	139
Tabelle 34: Tab_Dokv_30— Schnittstelle I_Document_Management_Connect .....	142
Tabelle 35: Tab_Dokv_31— Operation OpenContext .....	143
Tabelle 36: Tab_Dokv_32— Ablauf der Operation Open Context .....	144
Tabelle 37: Tab_Dokv_33— Operation Close Context .....	145
Tabelle 38: Tab_Dokv_34— Ablauf Operation CloseContext .....	146
Tabelle 39: Tab_Dokv_99— Kennzeichnung von Optionalitäten in XACML 2.0 Policies .	161

Tabelle 40: Tab_Dokv_100— XACML 2.0 Policy für einen Versicherten (Base Policy)...	161
Tabelle 41: Tab_Dokv_101— XACML 2.0 Policy mit erlaubten Operationen für einen Versicherten (Permission Policy).....	164
Tabelle 42: Tab_Dokv_200— XACML 2.0 Policy für einen Vertreter (Base Policy).....	195
Tabelle 43: Tab_Dokv_201— XACML 2.0 Policy mit erlaubten Operationen für einen Vertreter (Permission Policy).....	199
Tabelle 44: Tabelle : Tab_Dokv_300-01— XACML 2.0 Policy für eine Leistungserbringerinstitution (Base Policy).....	227
Tabelle 45: Tab_Dokv_301— XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer Dokumente (Permission Policy).....	232
Tabelle 46: Tab_Dokv_302— XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten und Kostenträger Dokumente (Permission Policy).....	258
Tabelle 47: Tab_Dokv_400— XACML 2.0 Policy für einen Kostenträger (Base Policy) ..	282
Tabelle 48: Tab_Dokv_401— XACML 2.0 Policy mit erlaubten Operationen für einen Kostenträger (Permission Policy) .....	285
Tabelle 49: Tab_Dokv_99— Kennzeichnung von Optionalitäten in XACML 2.0 Policies .	289
Tabelle 50: Tab_Dokv_500— XACML 2.0 Policy für einen Versicherten.....	289
Tabelle 51: Tab_Dokv_501— XACML 2.0 Policy für einen Vertreter.....	292
Tabelle 52: Tab_Dokv_502— XACML 2.0 Policy für eine Leistungserbringerinstitution .	295
Tabelle 53: Tab_Dokv_503— XACML 2.0 Policy für einen Kostenträger .....	315
Tabelle 1: Tab Dokv 10 - Kennzeichnung von Optionalitäten .....	24
Tabelle 2: Tab Dokv 11 - Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung.....	24
Tabelle 3: Tab Dokv 12 - Fehlercodes zu Fehlern gemäß Operationsdefinition.....	33
Tabelle 4: Tab Dokv 35 - Eingangsparameter für TUC PKI 018.....	40
Tabelle 5: Tab Dokv 13 - Parameter des § 291a-Protokolls .....	42
Tabelle 6: Tab Dokv 14 - Schnittstelle I Document Management.....	53
Tabelle 7: Tab Dokv 16 - Operation Cross-Gateway Query.....	57
Tabelle 8: Tab Dokv 17 - Operation Remove Documents .....	60
Tabelle 9: Tab Dokv 17 - Operation RemoveMetadata .....	61
Tabelle 10: Tab Dokv 18 - Operation Cross-Gateway Retrieve.....	63
Tabelle 11: Tab Dokv 45 - Operation Restricted Update Document Set .....	65
Tabelle 12: Tab Dokv 20 - Schnittstelle I Document Management Insurant.....	67
Tabelle 13: Tab Dokv 20 - Schnittstelle I Document Management Insurant.....	68
Tabelle 14: Tab Dokv 21 - Operation Provide And Register Document Set-b .....	69
Tabelle 15: Tab Dokv 22 - Operation Registry Stored Query.....	72
Tabelle 16: Tab Dokv 23 - Operation RemoveDocuments.....	75

<a href="#">Tabelle 17: Tab Dokv 23 - Operation RemoveMetadata .....</a>	77
<a href="#">Tabelle 18: Tab Dokv 24 - Operation Retrieve Document Set .....</a>	79
<a href="#">Tabelle 19: Tab Dokv 19 - Operation RestrictedUpdateDocumentSet .....</a>	81
<a href="#">Tabelle 20: Tab Dokv 36 - Schnittstelle I Document Management Insurance .....</a>	84
<a href="#">Tabelle 21: Tab Dokv 37 - Operation Provide And Register Document Set-b .....</a>	85
<a href="#">Tabelle 22: Tab Dokv 25 - Schnittstelle I Account Management Insurant .....</a>	89
<a href="#">Tabelle 23: Tab Dokv 26 - Operation Suspend Account .....</a>	90
<a href="#">Tabelle 24: Tab Dokv 27 - Operation Resume Account .....</a>	93
<a href="#">Tabelle 25: Tab Dokv 28 - Operation Get Audit Events .....</a>	97
<a href="#">Tabelle 26: Tab Dokv 44 - Operation Get Signed Audit Events.....</a>	99
<a href="#">Tabelle 27: Tab Dokv 38 - Operation I Key Management Insurant::StartKeyChange() .....</a>	106
<a href="#">Tabelle 28: Tab Dokv 39 - Operation I Key Management Insurant::GetAllDocumentKeys() .....</a>	109
<a href="#">Tabelle 29: Tab Dokv 40 - Operation I Key Management Insurant::PutAllDocumentKeys() .....</a>	112
<a href="#">Tabelle 30: Tab Dokv 41 - Operation I Account Management Insurant::FinishKeyChange().....</a>	114
<a href="#">Tabelle 31: Tab Dokv 42 - Zusätzliche Parameter des § 291a-Protokolls für die Umschlüsselung .....</a>	116
<a href="#">Tabelle 32: Tab Dokv 43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung .....</a>	117
<a href="#">Tabelle 33: Tab Dokv 43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung .....</a>	117
<a href="#">Tabelle 34: Tab Dokv 030 - Zugriffsunterbindungsregeln .....</a>	126
<a href="#">Tabelle 35: Tab Dokv 29 - Ablauf Operation Hello.....</a>	139
<a href="#">Tabelle 36: Tab Dokv 30 - Schnittstelle I Document Management Connect .....</a>	142
<a href="#">Tabelle 37: Tab Dokv 31 - Operation OpenContext .....</a>	143
<a href="#">Tabelle 38: Tab Dokv 32 - Ablauf der Operation Open Context .....</a>	144
<a href="#">Tabelle 39: Tab Dokv 33 - Operation Close Context .....</a>	145
<a href="#">Tabelle 40: Tab Dokv 34 - Ablauf Operation CloseContext .....</a>	146
<a href="#">Tabelle 41: Tab Dokv 99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies .</a>	161
<a href="#">Tabelle 42: Tab Dokv 100 - XACML 2.0 Policy für einen Versicherten (Base Policy)...</a>	161
<a href="#">Tabelle 43: Tab Dokv 101 - XACML 2.0 Policy mit erlaubten Operationen für einen Versicherten (Permission Policy).....</a>	164
<a href="#">Tabelle 44: Tab Dokv 200 - XACML 2.0 Policy für einen Vertreter (Base Policy).....</a>	195
<a href="#">Tabelle 45: Tab Dokv 201 - XACML 2.0 Policy mit erlaubten Operationen für einen Vertreter (Permission Policy).....</a>	199
<a href="#">Tabelle 46 Tabelle : Tab Dokv 300-01 - XACML 2.0 Policy für eine Leistungserbringereinstitution (Base Policy) .....</a>	227

[Tabelle 47: Tab Dokv 301 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente \(Permission Policy\) .....](#) 232

[Tabelle 48: Tab Dokv 302 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-Dokumente \(Permission Policy\) .....](#) 258

[Tabelle 49: Tab Dokv 400 - XACML 2.0 Policy für einen Kostenträger \(Base Policy\) ..](#) 282

[Tabelle 50: Tab Dokv 401 - XACML 2.0 Policy mit erlaubten Operationen für einen Kostenträger \(Permission Policy\) .....](#) 285

## 7.5 Referenzierte Dokumente

### 7.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemSpec_Aktensystem]	gematik: Spezifikation ePA-Aktensystem
[gemSpec_Authentisierung_Vers]	gematik: Spezifikation Authentisierung des Versicherten ePA
[gemSpec_Autorisierung]	gematik: Spezifikation Autorisierung ePA
[gemSpec_DM_ePA]	gematik: Datenmodell ePA
[gemSpec_FdV_ePA]	gematik: Spezifikation ePA-Frontend des Versicherten
[gemSpec_FM_ePA]	gematik: Spezifikation Fachmodul ePA
[gemSpec_FM_ePA_KTR_Consumer]	gematik: Spezifikation Fachmodul ePA im KTR-Consumer

[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
<a href="#">[gemSpec_ePA_Policy_LEI]</a>	gematik: XACML Policy Definition für Leistungserbringerinstitutionen "hcp-policy-definition.xml", <a href="https://github.com/gematik/api-ePA">https://github.com/gematik/api-ePA</a>
<a href="#">[gemSpec_ePA_Policy_KTR]</a>	gematik: XACML Policy Definition für Kostenträger "insurance-policy-definition.xml", <a href="https://github.com/gematik/api-ePA">https://github.com/gematik/api-ePA</a>
<a href="#">[gemSpec_ePA_Policy_Vertreter]</a>	gematik: XACML Policy Definition für Vertreter "representative-policy-definition.xml", <a href="https://github.com/gematik/api-ePA">https://github.com/gematik/api-ePA</a>
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_TBAuth]	gematik: Spezifikation Tokenbasierte Authentisierung
[gemSysL_ePA]	gematik: Systemspezifisches Konzept ePA

## 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, <a href="http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf">http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf</a>
[IHE-ITI-APPC]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Advanced Patient Privacy Consents (APPC), Revision 1.2 – Trial Implementation, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf</a>
[IHE-ITI-RMD]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.2 – Trial Implementation, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf</a>

	<a href="#">I_Suppl_RMD.pdf</a>
[IHE-ITI-RMU]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.1 – Trial Implementation, <a href="https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf">https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf</a>
[IHE-ITI-TF1]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Integration Profiles, Revision 15.0, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf</a>
[IHE-ITI-TF2a]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2a (ITI TF-2a) – Transactions Part A, Revision 15.0, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf</a>
[IHE-ITI-TF2b]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf</a>
[IHE-ITI-TF2x]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2x) – Volume 2 Appendices, Revision 15.1, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf</a>
[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, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf</a>
[IHE-ITI-XCDR]	IHE International (2017): IHE IT Infrastructure (ITI) Technical Framework Supplement, Cross-Community Document Reliable Interchange (XCDR), Revision 1.4 – Trial Implementation, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf</a>
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, <a href="https://www.w3.org/TR/soap12-mtom/">https://www.w3.org/TR/soap12-mtom/</a>

[OWASP-IP]	Open Web Application Security Project (OWASP) (2017): Input Validation Cheat Sheet, <a href="https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet">https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet</a>
[OWASP-SAML]	Open Web Application Security Project (OWASP) (2017): SAML Security Cheat Sheet, <a href="https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet">https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet</a>
[OWASP-WSS]	Open Web Application Security Project (OWASP) (2017): Web Service Security Cheat Sheet, <a href="https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet">https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet</a>
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, <a href="http://tools.ietf.org/html/rfc2119">http://tools.ietf.org/html/rfc2119</a>
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231, <a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a>
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), <a href="https://www.w3.org/TR/soap12-part1/">https://www.w3.org/TR/soap12-part1/</a>
[WSA]	OASIS (2004): Web Services Addressing (WS-Addressing), <a href="https://www.w3.org/Submission/ws-addressing/">https://www.w3.org/Submission/ws-addressing/</a>
[WSIAP]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, <a href="http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html">http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html</a>
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), <a href="http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html">http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html</a>
[WSIBSP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, <a href="http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html">http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html</a>
[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004),

	<a href="http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf">http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf</a>
[WSS-SAML]	OASIS (2006): Web Services Security: SAML Token Profile 1.1, <a href="https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLSecurityProfile.pdf">https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLSecurityProfile.pdf</a>
[XACML]	OASIS (2005): eXtensible Access Control Markup Language (XACML) Version 2.0, <a href="https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf">https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf</a>
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, <a href="http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/">http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/</a>

## 8 Anhang B – XACML 2.0-Profile für Policy Documents (für Upgrade von ePA 3.1.3)

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

**Tabelle 41: Tab\_Dokv\_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies**

Code	Bedeutung
R	Required - Mit "R" gekennzeichnete Element-, Attribut- oder Textknoten MÜSSEN verwendet werden.
O	Optional - Mit "O" gekennzeichnete Element-, Attribut- oder Textknoten KÖNNEN verwendet werden.
X	Mit "X" gekennzeichnete Element-, Attribut- oder Textknoten DÜRFEN NICHT verwendet werden.

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

### 8.1 Policy Document für einen Versicherten

#### 8.1.1 Base Policy

**Tabelle 42: 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	
	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.
<b>&lt;!-- KVNR als Aktenidentifikator --&gt;</b>				
		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.

### 8.1.2 Permission Policy

**Tabelle 43: Tab\_Dokv\_101 - XACML 2.0 Policy mit erlaubten Operationen für einen Versicherten (Permission Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Optional	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	

<b>&lt;!-- 'CrossGatewayDocumentProvide' --&gt;</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:2015: CrossGatewayDocumentPro vide" MUSS gesetzt werden.
			ActionAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- 'ProvideAndRegisterDocumentSet-b' --&gt;</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	
<b>&lt;!-- Registry Stored Query 'FindDocuments' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'FindSubmissionSets' --&gt;</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: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:f26abbc-b- 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.
<b>&lt;!-- Registry Stored Query 'GetAll' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'GetDocuments' --&gt;</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: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: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.
<b>&lt;!-- Registry Stored Query 'GetAssociations' --&gt;</b>						
				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.
<b>&lt;!-- Registry Stored Query 'GetDocumentsAndAssociations' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'GetSubmissionSets' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'GetSubmissionSetAndContents' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'GetRelatedDocuments' --&gt;</b>						
				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.
<b>&lt;!-- Registry Stored Query 'FindDocumentsByReferenceId' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'FindDocumentsByTitle' --&gt;</b>							
		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.
<b>&lt;!-- RemoveDocuments --&gt;</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: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.
<b>&lt;!-- RetrieveDocumentSet --&gt;</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: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.
<b>&lt;!-- GetAuditEvents --&gt;</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 "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.
<b>&lt;!-- ResumeAccount --&gt;</b>						
				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.
<b>&lt;!-- SuspendAccount --&gt;</b>					
		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.

## 8.2 Policy Document für einen Vertreter

### 8.2.1 Base Policy

Tabelle 44: 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	
<b>&lt;!-- Vertreter (repräsentiert durch seine KVNR) --&gt;</b>		
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-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.
<b>&lt;!-- KVNR als Aktenidentifikator --&gt;</b>				
		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.

### 8.2.2 Permission Policy

**Tabelle 45: Tab\_Dokv\_201 - XACML 2.0 Policy mit erlaubten Operationen für einen Vertreter (Permission Policy)**

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

	Target	R	Das Element MUSS leer bleiben.
	Policy	R	
	@PolicyId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@RuleCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target	R	
	Resources	R	
	Resource	R	
	ResourceMatch	R	
	@MatchId	R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
	AttributeValue	R	
	@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.

					CodedValue	R	
					@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
					@code	R	Der Wert "PAT" MUSS gesetzt werden.
					@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
					@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
					@displayName	O	Der Wert "Dokument eines Versicherten" MUSS gesetzt werden.
					ResourceAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
					@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
					@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
					Actions	R	

<b>&lt;!-- 'CrossGatewayDocumentProvide' --&gt;</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: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.
<b>&lt;!-- 'ProvideAndRegisterDocumentSet-b' --&gt;</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	
<b>&lt;!-- Registry Stored Query 'FindDocuments' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'FindSubmissionSets' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'GetAll' --&gt;</b>						
				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.
<b>&lt;!-- Registry Stored Query 'GetDocuments' --&gt;</b>						

				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.
<b>&lt;!-- Registry Stored Query 'GetAssociations' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'GetDocumentsAndAssociations' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'GetSubmissionSets' --&gt;</b>						
				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.
<b>&lt;!-- Registry Stored Query 'GetSubmissionSetAndContents' --&gt;</b>						

				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.
<b>&lt;!-- Registry Stored Query 'GetRelatedDocuments' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'FindDocumentsByReferenceId' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'FindDocumentsByTitle' --&gt;</b>							
		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.
<b>&lt;!-- RemoveDocuments --&gt;</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: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.
<b>&lt;!-- RetrieveDocumentSet --&gt;</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: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.
<b>&lt;!-- GetAuditEvents --&gt;</b>					

			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.

## 8.3 Policy Document für eine Leistungserbringerinstitution

### 8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente

**Tabelle 46 Tabelle : Tab\_Dokv\_300-01 - XACML 2.0 Policy für eine 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	
<b>&lt;!-- Leistungserbringerinstitution (repräsentiert durch ihre Telematik-ID) --&gt;</b>		
Subjects	R	
Subject	R	
SubjectMatch	R	

		@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
		AttributeValue	R	
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		InstanceIdentifier	R	
		@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
		@root	R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
		@extension	R	Als Wert MUSS die Telematik-ID gesetzt werden.
		SubjectAttributeDesignator	R	
		@AttributeId	R	Der Wert "urn:gematik:subject:organization-id" MUSS gesetzt werden.
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
		Subject	R	
		SubjectMatch	R	
		@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
		AttributeValue	R	

		@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
		text()	R	Als Wert MUSS der Name der Leistungserbringerinstitution gesetzt werden.
		SubjectAttributeDesignator	R	
		@AttributeId	R	Der Wert "urn:oasis:names:tc:xspa:1.0:subject:organization" MUSS gesetzt werden.
		@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<b>&lt;!-- KVNR als Aktenidentifikator --&gt;</b>				
		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:hl7-org:v3#II" MUSS gesetzt werden.
<b>&lt;!-- Gültigkeitszeitraum des Policy Documents --&gt;</b>					
			Environments	R	
			Environment	R	
			EnvironmentMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:date- <del>less</del> greater-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"> <li>• "urn:gematik:policy-set-id:permissions-access-group-hcp"</li> <li>• "urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents"</li> <li>• "urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents"</li> </ul>
--------	---	---

### 8.3.2 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente

Tabelle 47: Tab\_Dokv\_301 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente (Permission Policy)

Element-, Attribut- oder Textknoten gemäß [XACML]	Op t.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-

									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 "LEI" MUSS gesetzt werden.
					@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
					@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
					@displayName	O	Der Wert "Dokument einer 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	
<b>&lt;!-- 'CrossGatewayDocumentProvide' --&gt;</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:2015:CrossGatewayDocumentProvide" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				Rule	R	
				@RuleId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
				@Effect	R	Der Wert "Permit" MUSS gesetzt werden.

Policy				R	
	@PolicyId			R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@RuleCombiningAlgId			R	Der Wert "urn:oasis:names:tc:xcml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
Target				R	
	Resources			R	
	Resource			R	
	ResourceMatch			R	
			@MatchId	R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
			AttributeValue	R	
			@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
			CodedValue	R	
			@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.

					@code	R	Der Wert "LEI" MUSS gesetzt werden.
					@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
					@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
					@displayName	R	Der Wert "Dokument einer Leistungserbringerinstitution" MUSS gesetzt werden.
				ResourceAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti: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.
				Resource		R	
				ResourceMatch		R	
					@MatchId	R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
				AttributeValue		R	

				@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
				CodedValue	R	
				@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
				@code	R	Der Wert "LEÄ" MUSS gesetzt werden.
				@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
				@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
				@displayName	R	Der Wert "Leistungserbringeräquivalentes Dokument eines Versicherten oder Kostenträgers" MUSS gesetzt werden.
				ResourceAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
				@MustBePresent		Der Wert "true" MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'FindDocuments' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'FindSubmissionSets' --&gt;</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:Cr

						ossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbcl9" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery: queryId" MUSS gesetzt werden.

				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetAll' --&gt;</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:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				ActionMatch	R	

				@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:10b545ea- 725c-446d-9b95- 8aeb444eddf3" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetDocuments' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'GetAssociations' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'GetDocumentsAndAssociations' --&gt;</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/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
			text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
			ActionAttributeDesignator	R	
			@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
			ActionMatch	R	
			@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
			AttributeValue	R	
			@DataType	R	Der Wert "http://www.w3.org/2

						001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R Der Wert "urn:uuid:bab9529a-4a10-40b3-a01f-f68a615d247a" MUSS gesetzt werden.
				ActionAttributeDesignator		R
					@AttributeId	R Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetSubmissionSets' --&gt;</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: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/2

						001/XMLSchema#anyURI " MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetSubmissionSetAndContents' --&gt;</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/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0:action: action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:

						xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:e8e3cb2c- e39c-46b9-99e4- c12f57260b83" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetRelatedDocuments' --&gt;</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: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.
<b>&lt;!-- Registry Stored Query 'FindDocumentsByReferenceId' --&gt;</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: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:12941a89- e02e-4be5-967c- ce4bfc8fe492" MUSS gesetzt werden.	
				ActionAttributeDesignator					R	
					@AttributeId			R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.	
					@DataType			R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.	
<b>&lt;!-- Registry Stored Query 'FindDocumentsByTitle' --&gt;</b>										
			Acti on						R	
			Action Match						R	

				@MatchId			R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue			R	
					@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()		R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator			R	
					@AttributeId		R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
			Action Match				R	
				@MatchId			R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue			R	
					@DataType		R	Der Wert "http://www.w3.org/2

								001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()			R Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
				ActionAttribut eDesignator				R
					@AttributeId			R Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType			R Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- RemoveDocuments --&gt;</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: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.
<b>&lt;!-- CrossGatewayRetrieve --&gt;</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/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayRetrieve" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.

		@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
	Rule		R	
	@RuleId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@Effect		R	Der Wert "Permit" MUSS gesetzt werden.

### 8.3.3 Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente

**Tabelle 48: Tab\_Dokv\_302 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-Dokumente (Permission Policy)**

Element-, Attribut- oder Textknoten gemäß [XACML]	Optional	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	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.  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.
	@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target	R	Das Element MUSS leer bleiben.
	Policy	R	
	@PolicyId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@RuleCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target	R	
	Resources	R	
	Resource	R	
	ResourceMatch	R	

				@MatchId	R	Der Wert "urn:hl7-org:v3:function:CV-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
				CodedValue	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@code	R	<p>Der Wert "KTR" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden                      (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents").</p> <p>Der Wert "PAT" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden                      (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents").</p>
				@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.

					@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
					@displayName	O	<p>Der Wert "Dokument eines Kostenträgers" aus MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden                  (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents").</p> <p>Der Wert "Dokument eines Versicherten" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden                  (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents").</p>
				ResourceAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti: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	
<b>&lt;!-- Registry Stored Query 'FindDocuments' --&gt;</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:CrossGatewayQuery" MUSS gesetzt werden.
			ActionAttributeDesignator		R	
			@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
			@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			ActionMatch		R	
			@MatchId		R	Der Wert "urn:oasis:names:tc:x

						acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:14d4debf- 8f97-4251-9a74- a90016b0af0d" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'FindSubmissionSets' --&gt;</b>						
				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	

				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbc1a9" MUSS gesetzt werden.
				ActionAttributeDesignator	R	

				@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetAll' --&gt;</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:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.	
					ActionMatch		R	
					@MatchId		R	Der Wert "urn:oasis:names:tc: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:10b545ea- 725c-446d-9b95- 8aeb444eddf3" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
					@AttributeId		R	Der Wert "urn:ihe:iti:2016:Reg istryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetDocuments' --&gt;</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:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:5c4f972b- d56b-40ac-a5fc- c8ca9b40b9d4" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetAssociations' --&gt;</b>							
				Action		R	
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20



						acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:bab9529a- 4a10-40b3-a01f- f68a615d247a" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:2016:Reg istryStoredQuery: queryId" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetSubmissionSets' --&gt;</b>						
				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue	R	

				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
			ActionAttributeDesignator		R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			ActionMatch		R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
			AttributeValue		R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "urn:uuid:51224314- 5390-4169-9b91- b1980040715a" MUSS gesetzt werden.
			ActionAttributeDesignator		R	

				@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'GetSubmissionSetAndContents' --&gt;</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:CrossGatewayQuery" MUSS gesetzt werden.
			ActionAttributeDesignator		R	
			@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
			@DataType		R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch		R
					@MatchId		R Der Wert "urn:oasis:names:tc: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: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.
<b>&lt;!-- Registry Stored Query 'GetRelatedDocuments' --&gt;</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:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:d90e5407- b356-4d91-a89f- 873917b4b0e6" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<b>&lt;!-- Registry Stored Query 'FindDocumentsByReferenceId' --&gt;</b>							
				Action		R	
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:12941a89-e02e-4be5-967c-ce4bfc8fe492" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20



				Actio nMat ch				R	
					@MatchId			R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeVal ue			R	
						@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
						text()		R	Der Wert "urn:uuid:ab474085- 82b5-402d-8115- 3f37cb1e2405" MUSS gesetzt werden.
					ActionAttrib uteDesignat or			R	
						@AttributeI d		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.
<b>&lt;!-- CrossGatewayRetrieve --&gt;</b>									
				Action				R	
				ActionMatch				R	
					@MatchId			R	Der Wert "urn:oasis:names:tc:x



					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.
<b>&lt;!-- RestrictedUpdateDocumentSet --&gt;</b>								
					Action		R	
					ActionMatch		R	
					@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURIEqual" 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.

## 8.4 Policy Document für einen Kostenträger

### 8.4.1 Base Policy

**Tabelle 49: 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	
<b>&lt;!-- Kostenträger (repräsentiert durch ihre Telematik-ID) --&gt;</b>		
Subjects	R	
Subject	R	
SubjectMatch	R	
@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
AttributeValue	R	
@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
InstanceIdentifier	R	
@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
@root	R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
@extension	R	Als Wert MUSS die Telematik-ID gesetzt werden.
SubjectAttributeDesignator	R	

		@AttributeId	R	Der Wert " urn:gematik:subject:organization-id" MUSS gesetzt werden.
		@DataType	R	Der Wert "urn: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#stri ng" MUSS gesetzt werden.
		text()	R	Als Wert MUSS der Name des Kostenträgers gesetzt werden.
		SubjectAttributeDesignator	R	
		@AttributeId	R	Der Wert "urn:oasis:names:tc:xspa:1.0: subject:organization" MUSS gesetzt werden.
		@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#stri ng" MUSS gesetzt werden.
<b>&lt;!-- KVNR als Aktenidentifikator --&gt;</b>				
		Resources	R	
		Resource	R	

		ResourceMatch	R	
		@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
		AttributeValue	R	
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		InstanceIdentifier	R	
		@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
		@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
		@extension	R	Als Wert MUSS der unveränderbare Teil der KVN (10 Stellen) gesetzt werden.
		ResourceAttributeDesignator	R	
		@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		PolicySetIdReference	R	
		text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurance" MUSS gesetzt werden.

### 8.4.2 Permission Policy

**Tabelle 50: Tab\_Dokv\_401 - XACML 2.0 Policy mit erlaubten Operationen für einen 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: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: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	
<b>&lt;!-- 'ProvideAndRegisterDocumentSet-b' --&gt;</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.

## 9-Anhang C – XACML 2.0 Profile für Policy Documents

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

**Tabelle 49: Tab\_Dokv\_99 – Kennzeichnung von Optionalitäten in XACML 2.0 Policies**

Code	Bedeutung
R	Required – Mit "R" gekennzeichnete Element, Attribut oder Textknoten MÜSSEN verwendet werden.
O	Optional – Mit "O" gekennzeichnete Element, Attribut oder Textknoten KÖNNEN verwendet werden.
X	Mit "X" gekennzeichnete Element, Attribut oder Textknoten DÜRFEN NICHT verwendet werden.

Beispiele zu den folgenden XACML 2.0 Profilen können dem beiliegenden Dokumentenpaket entnommen werden:

### 9.1 Policy Document für einen Versicherten

**Tabelle 50: Tab\_Dokv\_500 – XACML 2.0 Policy für einen Versicherten**

Element, Attribut oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:insurant" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
@Version	R	Der Wert "4.0" MUSS gesetzt werden

Target	R	
<del>←!→Versicherter (repräsentiert durch seine KVNR)→</del>		
Subjects-	R	
Subject-	R	
SubjectMatch-	R	
@MatchId	R	Der Wert " <del>urn:h17-org:v3:function:II=equal</del> " MUSS gesetzt werden.
AttributeValue	R	
@DataType	R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.
InstanceIdentifier	R	
@xmlns	R	Der Wert " <del>urn:h17-org:v3</del> " MUSS gesetzt werden.
@root	R	Der Wert " <del>1.2.276.0.76.4.8</del> " MUSS gesetzt werden.
@extension	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
SubjectAttributeDesignator-	R	
@AttributeId	R	Der Wert " <del>urn:gematik:subject:subject-id</del> " MUSS gesetzt werden.

		@DataType	R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.
		@MustBePresent	R	Der Wert " <del>true</del> " MUSS gesetzt werden.
<b>←!— KVNR als Aktenidentifikator —!→</b>				
		Resources	R	
		Resource	R	
		ResourceMatch	R	
		@MatchId	R	Der Wert " <del>urn:h17-org:v3:function:II=equal</del> " MUSS gesetzt werden.
		AttributeValue	R	
		@DataType	R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.
		InstanceIdentifier	R	
		@xmlns	R	Der Wert " <del>urn:h17-org:v3</del> " MUSS gesetzt werden.
		@root	R	Der Wert " <del>1.2.276.0.76.4.8</del> " MUSS gesetzt werden.
		@extension	R	Als Wert MUSS den unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
		ResourceAttributeDesignator	R	

			@AttributeId	R	Der Wert " <del>urn:ihe:iti:ser:2016:patient-id</del> " MUSS gesetzt werden.
			@DataType	R	Der Wert " <del>urn:hl7-org:v3#II</del> " MUSS gesetzt werden.
		text()		R	Der Wert " <del>urn:gematik:policy-set-id:permissions-access-group-insurant</del> " MUSS gesetzt sein.

## 9.2 Policy Document für einen Vertreter

Tabelle 51: ~~Tab\_Dokv\_501~~ – XACML 2.0 Policy für einen Vertreter

Element , Attribut oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert " <del>urn:gematik:policy-set-id:permissions-access-group-representative:base</del> " MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert " <del>urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides</del> " MUSS gesetzt werden.
@Version	R	Der Wert "4.0.2" MUSS gesetzt werden.
Description	R	Der Common Name des X.509 Subject Name der eGK MUSS gesetzt werden, um die Lesbarkeit für den Versicherten im ePA-





					@AttributeId	R	Der Wert <del>"urn:ihe:iti:ser:2016:patient-id"</del> MUSS gesetzt werden.
					@DataType	R	Der Wert <del>"urn:hl7-org:v3#II"</del> MUSS gesetzt werden.

### 9.3 Policy Document für eine Leistungserbringerinstitution

Tabelle 52: Tab\_Dokv\_502 – XACML 2.0 Policy für eine Leistungserbringerinstitution

Element, Attribut oder Textknoten gemäß [XACML]			⊙ p t r	Nutzungsvorgabe
PolicySet			R	
@PolicySetId			R	Der Wert <del>"urn:gematik:policy-set-id:permissions-access-group-hep:base"</del> MUSS gesetzt werden.
@PolicyCombiningAlgorithmId			R	Der Wert <del>"urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides"</del> MUSS gesetzt werden.
@Version			R	Der Wert "4.0.2" MUSS gesetzt werden.
Description			R	Als Wert MUSS der Name der Leistungserbringerinstitution gesetzt werden, um die Lesbarkeit für

									den Versicherten im ePA-Frontend des Versicherten zu erhöhen, d.h. wem er ein Zugriffsrecht eingeräumt hat.
	Target								R Das Element MUSS leer bleiben.
	Policy Set								R
	@PolicySetId								R Der Wert <del>"urn:gematik:policy-set-id:permissions-access-group-hep:container"</del> MUSS gesetzt werden.
	@PolicyCombiningAlgorithmId								R Der Wert <del>"urn:oasis:names:tc:acml:1.0:policy-combining-algorithm:deny-overrides"</del> MUSS gesetzt werden.
	@Version								R Der Wert "4.0" MUSS gesetzt werden.
	Target								R
	<b>&lt;!--Leistungserbringerinstitution (repräsentiert durch ihre Telematik-ID)--&gt;</b>								
									R
									R
									R

						@MatchId	R	Der Wert " <del>urn:h17-org:v3:function:II-equal</del> " MUSS gesetzt werden.
						AttributeValue	R	
						@DataTyp e	R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.
						InstanceIdentifier	R	
						@xmlns	R	Der Wert " <del>urn:h17-org:v3</del> " 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 der zu berechtigenden LEI gesetzt werden.
						SubjectAttributeDesignator	R	
						@AttributeId	R	Der Wert " <del>urn:gematik:subject:organization-id</del> " MUSS gesetzt werden.
						@DataTyp e	R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.
						@MustBePresent	R	Der Wert " <del>true</del> " MUSS gesetzt werden.
						<b>←!—KVNR als Aktenidentifikator—!→</b>		
						Resources	R	

					Resource		R	
					ResourceMatch		R	
					@MatchId		R	Der Wert " <del>urn:h17-org:v3:function:II-equal</del> " MUSS gesetzt werden.
					AttributeValue		R	
					@Dat aTyp e		R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.
					Insta nceId entifi er		R	
						@x ml ns	R	Der Wert " <del>urn:h17-org:v3</del> " MUSS gesetzt werden.
						@f oo t	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
						@e xte nsi on	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
					ResourceAttrib uteDesignator		R	
					@Attr ibuteI d		R	Der Wert " <del>urn:ihe:iti:ser:2016:patient-id</del> " MUSS gesetzt werden.
					@Dat aTyp e		R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.

		<b>←!—Gültigkeitszeitraum des Policy Documents—→</b>					
		Environments					R
		Environment					R
		EnvironmentMatch					R
					@MatchId	R	Der Wert " <del>urn:oasis:names:tc:xacml:1.0: function:date-less-than-or-equal</del> " MUSS gesetzt werden.
					AttributeValue	R	
					@DateType	R	Der Wert " <del>http://www.w3.org/2001/XMLSchema#date</del> " MUSS gesetzt werden.
					text()	R	Der Wert muss dem Tag der Ausstellung (Format YYYY-MM-DD nach ISO 8601:2004 in UTC) des Policy Documents entsprechen.
					EnvironmentAttributeDesignator	R	
					@AttributeId	R	Der Wert " <del>urn:oasis:names:tc:xacml:1.0: environment:current-date</del> " MUSS gesetzt werden.
					@DateType	R	Der Wert " <del>http://www.w3.org/2001/XMLSchema#date</del> " MUSS gesetzt werden.

						EnvironmentMatch		R	
						@MatchId		R	Der Wert " <del>urn:oasis:names:tc:xaaml:1.0:environment:current-date-greater-than</del> " MUSS gesetzt werden.
						AttributeValue		R	
						@Date		R	Der Wert " <del>http://www.w3.org/2001/XMLSchema#date</del> " MUSS gesetzt werden.
						text()		R	Der Wert muss dem Enddatum (Format YYYY-MM-DD nach ISO 8601:2004 in UTC) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen:  <ul style="list-style-type: none"> <li>• "<del>heute</del>" + frei wählbare Anzahl Tage (maximal heute + 100 Jahre)</li> </ul>
						EnvironmentAttributeDesignator		R	
						@AttributeId		R	Der Wert " <del>urn:oasis:names:tc:xaaml:1.0:environment:current-date</del> " MUSS gesetzt werden.
						@Date		R	Der Wert " <del>http://www.w3.org/2001/XMLSchema#date</del> " MUSS gesetzt werden.
<p><b>← Der folgende Teil setzt folgende Auswertungsmechanik um: Permit, wenn</b></p>									

<b>(Vertrauensstufe AND Kategorie erlaubt AND not Blacklisted) OR Whitelist. Ansonsten Deny →</b>										
Policy Set									R	
	@PolicySetId								R	Der Wert <del>"urn:gematik:policy-set-id:permissions-access-group-hep:all-permissions"</del> MUSS gesetzt werden.
	@PolicyCombiningAlgorithmId								R	Der Wert <del>"urn:oasis:names:tc:xacl:1.0:policy-combining-algorithm:permit-overrides"</del> MUSS gesetzt werden.
	@Version								R	Der Wert "4.0" MUSS gesetzt werden.
	Target								R	Der Wert MUSS leer bleiben.
<b>← Feingranulare Berechtigung: Whitelist →</b>										
	PolicyIdReference								R	Der Wert <del>"urn:gematik:policy-id:permissions-access-group-hep:whitelist"</del> MUSS gesetzt werden.
<b>← Vertrauensstufe AND Kategorie erlaubt AND not Blacklisted →</b>										
	Policy Set								R	
		@PolicySetId							R	Der Wert <del>"urn:gematik:policy-set-id:permissions-</del>

											<del>access-group- hep:base:check-wo- whitelist" MUSS gesetzt werden.</del>	
			@PolicyCombiningAlgorithmId							R	Der Wert " <del>urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.</del>	
			@Version							R	Der Wert " <del>4.0" MUSS gesetzt werden.</del>	
			Target							R	Der Wert MUSS leer bleiben.	
			PolicyIdReference							R	Der Wert " <del>urn:gematik:policy-set-id:permissions-access-group-hep:levels" MUSS gesetzt werden.</del>	
			PolicyIdReference							R	Der Wert " <del>urn:gematik:policy-set-id:permissions-access-group-hep:categories" MUSS gesetzt werden.</del>	
			PolicyIdReference							R	Der Wert " <del>urn:gematik:policy-set-id:permissions-access-group-hep:blacklist" MUSS gesetzt werden.</del>	
		<b>←-Default Policy, die immer Deny zurückgibt-→</b>										
		Policy								R		
			@PolicyId							R	Der Wert " <del>urn:gematik:policy-id:permissions-</del>	



		<del>mbiningAlgorithmId</del>									<del>xacml:1.0:policy-combining-algorithm:permit-overrides</del> MUSS gesetzt werden.
		<del>@Version</del>								R	Der Wert "4.0" MUSS gesetzt werden.
		<del>Target</del>								R	Der Wert MUSS leer bleiben.
		<del>← Grobgranulare Berechtigung "normal" (immer vorhanden) →</del>									
		<del>PolicyIdReference</del>								R	Der Wert " <del>urn:gematik:policy-id:permissions-access-group-hep:levels:normal</del> " MUSS gesetzt werden.
		<del>← Grobgranulare Berechtigung "erweitert" (nur bei Bedarf vorhanden) →</del>									
		<del>PolicyIdReference</del>								⊖	Das Element MUSS genau dann vorhanden sein, wenn "erweiterte Berechtigung" erteilt werden soll, und dann den Wert " <del>urn:gematik:policy-id:permissions-access-group-hep:levels:extended</del> " besitzen.
		<del>← Default Policy, die immer Deny zurückgibt →</del>									
		<del>PolicyIdReference</del>								R	Der Wert " <del>urn:gematik:policy-id:permissions-access-group-hep:base:default-deny</del> " MUSS gesetzt sein.

<b>←Setzen der mittelgranularen Berechtigung→</b>										
Policy Set									R	
	@PolicySetId								R	Der Wert <del>"urn:gematik:policy-set-id:permissions-access-group-hep:categories"</del> MUSS gesetzt werden.
	@PolicyCombiningAlgorithmId								R	Der Wert <del>"urn:oasis:names:tc:xaaml:1.0:policy-combining-algorithm:permit-overrides"</del> MUSS gesetzt werden.
	@Version								R	Der Wert "4.0" MUSS gesetzt werden.
	Target								R	Der Wert MUSS leer bleiben.
<b>←Setzen der Berechtigung auf Kategorie "emp"→</b>										
	PolicyIdReference								⊖	Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "emp" erteilt werden soll, und dann den Wert <del>"urn:gematik:policy-id:permissions-access-group-hep:categories:emp"</del> besitzen.
<b>←Setzen der Berechtigung auf Kategorie "nfd"→</b>										
	PolicyIdReference								⊖	Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf

										<p>Kategorie "<del>nfd</del>" erteilt werden soll, und dann den Wert <del>"urn:gematik:policy-id:permissions-access-group-hep:categories:nfd" besitzen.</del></p>
<p><b>← Setzen der Berechtigung auf Kategorie "eab" →</b></p>										
		Policy IdReferene								<p>⊖ Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "<del>eab</del>" erteilt werden soll, und dann den Wert <del>"urn:gematik:policy-id:permissions-access-group-hep:categories:eab" besitzen.</del></p>
<p><b>← Setzen der Berechtigung auf Kategorie "dentalrecord" →</b></p>										
		Policy IdReferene								<p>⊖ Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "<del>dentalrecord</del>" erteilt werden soll, und dann den Wert <del>"urn:gematik:policy-id:permissions-access-group-hep:categories:dentalrecord" besitzen.</del></p>
<p><b>← Setzen der Berechtigung auf Kategorie "childsrecord" →</b></p>										
		Policy IdReferene								<p>⊖ Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "<del>childsrecord</del>" erteilt werden soll, und dann</p>

										den Wert "urn:gematik:policy-id:permissions-access-group-hep:categories:childrecord" besitzen.
		<b>← Setzen der Berechtigung auf Kategorie "mothersrecord" →</b>								
		Policy IdReferene								⊖ Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "mothersrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hep:categories:mothersrecord" besitzen.
		<b>← Setzen der Berechtigung auf Kategorie "vaccination" →</b>								
		Policy IdReferene								⊖ Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "vaccination" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hep:categories:vaccination" besitzen.
		<b>← Setzen der Berechtigung auf Kategorie "patientdoc" →</b>								
		Policy IdReferene								⊖ Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "patientdoc" erteilt werden soll, und dann den Wert "urn:gematik:policy-

										<del>id:permissions-access-group-hep:categories:patientdoe" besitzen.</del>
		<b>← Setzen der Berechtigung auf Kategorie "ega" →</b>								
		Policy IdReferene								⊖ Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "ega" erteilt werden soll, und dann den Wert <del>"urn:gematik:policy-id:permissions-access-group-hep:categories:ega" besitzen.</del>
		<b>← Setzen der Berechtigung auf Kategorie "receipt" →</b>								
		Policy IdReferene								⊖ Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "receipt" erteilt werden soll, und dann den Wert <del>"urn:gematik:policy-id:permissions-access-group-hep:categories:receipt" besitzen.</del>
		<b>← Setzen der Berechtigung auf Kategorie "care" →</b>								
		Policy IdReferene								⊖ Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "care" erteilt werden soll, und dann den Wert <del>"urn:gematik:policy-id:permissions-access-group-hep:categories:care" besitzen.</del>

		<b>←Setzen der Berechtigung auf Kategorie "prescription"→</b>							
	Policy IdReference							⊖ Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "prescription" erteilt werden soll, und dann den Wert <code>"urn:gematik:policy-id:permissions-access-group-hep:categories:prescription"</code> besitzen.	
		<b>←Setzen der Berechtigung auf Kategorie "eau"→</b>							
	Policy IdReference							⊖ Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "eau" erteilt werden soll, und dann den Wert <code>"urn:gematik:policy-id:permissions-access-group-hep:categories:eau"</code> besitzen.	
		<b>←Setzen der Berechtigung auf Kategorie "other"→</b>							
	Policy IdReference							⊖ Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "other" erteilt werden soll, und dann den Wert <code>"urn:gematik:policy-id:permissions-access-group-hep:categories:other"</code> besitzen.	
		<b>←Setzen der Berechtigung für Kategorien practitioner, hospital, laboratory, physiotherapy, psychotherapy, dermatolo</b>							

		<del>gy, gynaecology_urology, dentistry_oms, other_medical und other_non_medical</del> →								
		Policy IdReferene e								<p>⊖ Das Element MUSS genau dann vorhanden sein, wenn auf eine der Kategorien <del>category = {practitioner hospital laboratory physiotherapy psychotherapy dermatology, gynaecology_urology dentistry_oms other_medical other_non_medical}</del> <b>berechtigt werden soll, und dann den Wert</b>  <del>"urn:gematik:policy-id:permissions-access-group-hep:categories:&lt;category&gt;"</del> <b>besitzen.</b></p> <p><b>Beispiel: Der Wert</b>  <del>"urn:gematik:policy-id:permissions-access-group-hep:categories:other_medical"</del> <b>berechtigt auf die Kategorie "other_medical".</b></p> <p>Das Element wird für jede zu berechtigende Kategorie (mit jeweils der Kategorie entsprechenden Wert) wiederholt.</p>
		<b>← Default Policy, die immer Deny zurückgibt</b>								
		Policy IdReferene e								<p>R Der Wert  <del>"urn:gematik:policy-id:permissions-access-group-hep:base:default-deny"</del> <b>MUSS gesetzt sein.</b></p>

<del>← Setzen der feingranularen Berechtigung: Blacklist →</del>									
Policy							R		
		<del>@PolicyId</del>					R	<del>Der Wert "urn:gematik:policy-id:permissions-access-group-hep:blacklist" MUSS gesetzt werden.</del>	
		<del>@RuleCombiningAlgorithmId</del>					R	<del>Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.</del>	
		Target					R		
		Rule					R		
			<del>@RuleId</del>					R	<del>Der Wert "urn:gematik:rule-id:permissions-access-group-hep:blacklist" MUSS gesetzt sein.</del>
			<del>@Effect</del>				R	<del>Der Wert "Deny" MUSS gesetzt werden.</del>	
			Target				R		
				Resources				⊖	Das Element MUSS genau dann vorhanden sein, wenn mindestens ein Dokument auf die Blacklist gesetzt werden soll.
					<del>-Resource</del>		R	Das Element MUSS genau ein mal für jedes Dokument vorhanden	

										sein, dass auf die Blacklist gesetzt werden soll.	
										R	
						Resourcemathe				R	
						@MatheId				R	Der Wert " <code>urn:oasis:names:tc:xaeml:1.0:function:string-equal</code> " MUSS gesetzt werden.
						Attribut eValue				R	Der Wert MUSS dem Wert der <code>DocumentEntry.uniqueId</code> des Dokuments entsprechen, das auf die Blacklist gesetzt werden soll.
							@DataTyp e			R	Der Wert " <code>http://www.w3.org/2001/XMLSchema#string</code> " MUSS gesetzt werden.
						ResourceAttributeDesignator				R	
							@AttributeId			R	Der Wert " <code>urn:oasis:names:tc:xaeml:1.0:resource:resource-id</code> " MUSS gesetzt werden.
							@DataTyp e			R	Der Wert " <code>http://www.w3.org/2001/XMLSchema#string</code> " MUSS gesetzt werden.
						← Default Rule, das immer Permit zurückgibt →					

		Rule							R	
			@RuleId						R	Der Wert "urn:gematik:rule-id:permissions-access-group-hep:blacklist:default-permit" MUSS gesetzt werden.
			@Effect						R	Der Wert "Permit" MUSS gesetzt werden.
<b>← Setzen der feingranularen Berechtigung: Whitelist →</b>										
		Policy							R	
			@PolicyId						R	Der Wert "urn:gematik:policy-id:permissions-access-group-hep:whitelist" MUSS gesetzt werden.
			@RuleCombiningAlgorithmId						R	Der Wert "urn:oasis:names:tc:xacl:1.0:rule-combining-algorithm:permit-overrides" MUSS gesetzt werden.
		Target							R	
		Rule							R	
			@RuleId						R	Der Wert "urn:gematik:rule-id:permissions-access-group-hep:whitelist" MUSS gesetzt sein.
			@Effect						R	Der Wert "Permit" MUSS gesetzt werden.

			Target						R	
				Resources					O	Das Element MUSS genau dann vorhanden sein, wenn mindestens ein Dokument auf die Whitelist gesetzt werden soll.
				-Resource					R	Das Element MUSS genau ein mal für jedes Dokument vorhanden sein, dass auf die Whitelist gesetzt werden soll.
				ResourceMatch					R	
						@MatchId			R	Der Wert "urn:oasis:names:tc:acml:1.0:function:string-equal" MUSS gesetzt werden.
						AttributeValue			R	Der Wert MUSS dem Wert der DocumentEntry.uniqueId des Dokuments entsprechen, das auf die Whitelist gesetzt werden soll.  Der Wert DARF NICHT gleichzeitig in //Policy/Rule[@PolicyId="urn:gematik:policy-id:permissions-access-group-hep:blacklist']/Target/Resources/Resource/ResourceMatch/AttributeValue enthalten sein (Dokument ist nie gleichzeitig auf Black- und Whitelist gelistet).

							@DataTyp e	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.	
						ResourceAttributeDesignator		R		
							@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:resource:resource-id" MUSS gesetzt werden.	
							@DataTyp e	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.	
		<b>← Default Rule, das immer Deny zurückgibt →</b>								
		Rule						R		
			@RuleId					R	Der Wert "urn:gematik:rule-id:permissions-access-group-hep:whitelist:default-deny" MUSS gesetzt werden.	
			@Effect					R	Der Wert "Deny" MUSS gesetzt werden.	

### 9.4 Policy Document für einen Kostenträger

Tabelle 53: Tab\_Dokv\_503 – XACML 2.0 Policy für einen Kostenträger

Element-, Attribut- oder Textknoten gemäß [XACML]	Op t.	Nutzungsvorgabe
PolicySet	R	

	@PolicySetId		R	Der Wert " <del>urn:gematik:policy-set-id:permissions-access-group-ctr:base</del> " MUSS gesetzt sein.
	@PolicyCombiningAlgId		R	Der Wert " <del>urn:oasis:names:tc:xacml:1.1.0:policy-combining-algorithm:permit-overrides</del> " MUSS gesetzt werden.
	@Version		R	Der Wert "4.0.2" MUSS gesetzt werden.
	Description		R	Als Wert MUSS der Name des Kostenträgers gesetzt werden.
	Target		R	
	<del>←! Kostenträger (repräsentiert durch seine Telematik ID) →</del>			
	Subjects		R	
	Subject		R	
	SubjectMatch		R	
		@MatchId	R	Der Wert " <del>urn:h17-org:v3:function:II-equal</del> " MUSS gesetzt werden.
		AttributeValue	R	
		@DataType	R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.
		InstanceIdentifier	R	

				@xmlns	R	Der Wert " <del>urn:h17-org:v3</del> " MUSS gesetzt werden.
				@root	R	Der Wert " <del>1.2.276.0.76.4.188</del> " MUSS gesetzt werden.
				@extension	R	Als Wert MUSS die Telematik-ID gesetzt werden.
			SubjectAttributeDesignator		R	
				@AttributeId	R	Der Wert " <del>urn:gematik:subject:organization-id</del> " MUSS gesetzt werden.
				@DataType	R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.
				@MustBePresent	R	Der Wert " <del>true</del> " MUSS gesetzt werden.
<b>←! KVNR als Aktenidentifikator →</b>						
			Resources		R	
			Resource		R	
			ResourceMatch		R	
			@MatchId		R	Der Wert " <del>urn:h17-org:v3:function:II-equal</del> " MUSS gesetzt werden.
			AttributeValue		R	
			@DataType		R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.

				InstanceIdentifier		R	
					@xmlns	R	Der Wert " <del>urn:h17-org:v3</del> " MUSS gesetzt werden.
					@root	R	Der Wert " <del>1.2.276.0.76.4.8</del> " MUSS gesetzt werden.
					@extension	R	Als Wert MUSS der unveränderbare Teil der KVN-R (10 Stellen) gesetzt werden.
				ResourceAttributeDesignator		R	
					@AttributeId	R	Der Wert " <del>urn:ihe:iti:ser:2016:patient-id</del> " MUSS gesetzt werden.
					@DataType	R	Der Wert " <del>urn:h17-org:v3#II</del> " MUSS gesetzt werden.
<b>←!-Prüfung der Berechtigungskategorien-!→</b>							
<b>←-Setzen der Berechtigung auf Kategorie "receipt"-&gt;</b>							
				PolicyIdReference		-R	Der Wert " <del>urn:gematik:policy-id:permissions-access-group-hep:categories:receipt</del> " MUSS gesetzt werden.
<b>←-Setzen der Berechtigung auf Kategorie "ega"-&gt;</b>							
				PolicyIdReference		-R	Der Wert " <del>urn:gematik:policy-id:permissions-access-group-hep:categories:ega</del> " MUSS gesetzt werden.

## 9.5 Statische Permission Policies

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

### 9.5.1 Grobgranulare Berechtigung: Stufe Normal

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
  overrides" PolicyId="urn:gematik:policy-id:permissions-access-group-
  hcp:levels:normal" Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:levels:normal"
  Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="N"
              codeSystem="2.16.840.1.113883.5.25" displayName="normal"/>
            </AttributeValue>
            <ResourceAttributeDesignator
              AttributeId="urn:ihe:iti:appc:2016:confidentiality-code" DataType="urn:hl7-
              org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
  hcp:levels:normal:default-deny" Effect="Deny"/>
</Policy>
```

### 9.5.2 Grobgranulare Berechtigung: Stufe Erweitert

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy
  xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
  overrides"
  PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:levels:extended"
  Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:levels:extended"
  Effect="Permit">
    <Target>
      <Resources>
        <Resource>
```

```

-----<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
-----<AttributeValue DataType="urn:hl7-org:v3#CV">
-----<CodedValue xmlns="urn:hl7-org:v3" code="R"
codeSystem="2.16.840.1.113883.5.25" displayName="restricted"/>
-----</AttributeValue>
-----<ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:confidentiality-code" DataType="urn:hl7-
org:v3#CV"/>
-----</ResourceMatch>
-----</Resource>
-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:levels:extended:default-deny" Effect="Deny"/>
-----</Policy>

```

### 9.5.3 Mittelgranulare Berechtigung: Kategorie "care"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:care"
xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" RuleCombiningAlgId="urn:oasi
s:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" Version="4.0">
-----<Target/>
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:care"
Effect="Permit">
-----<Target>
-----<Resources>
-----<Resource>
-----<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
-----<AttributeValue DataType="urn:hl7-org:v3#CV">
-----<CodedValue xmlns="urn:hl7-org:v3" code="PFL"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.5"/>
-----</AttributeValue>
-----<ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:practice-setting-code"
DataType="urn:hl7-org:v3#CV"/>
-----</ResourceMatch>
-----</Resource>
-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:care:default-deny" Effect="Deny"/>
-----</Policy>

```

### 9.5.4 Mittelgranulare Berechtigung: Kategorie "childsrecord"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:childsrecord" xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"

```

```

RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides" Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hgp:categories:childsrecord" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3"
code="urn:gematik:ig:Kinderuntersuchungsheft:r4.0"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:related-folder:code"
DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hgp:categories:childsrecord:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.5 Mittelgranulare Berechtigung: Kategorie "dentalrecord"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hgp:categories:dentalrecord" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:deny-overrides" Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hgp:categories:dentalrecord" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3"
code="urn:gematik:ig:Zahnbonusheft:r4.0"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:format-code" DataType="urn:hl7-
org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->

```

```

——<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:dentalrecord:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.6 Mittelgranulare Berechtigung: Kategorie "eab"

```

<?xml version="1.0" encoding="UTF-8"?>
<!-- Mittelgranular: Kategorie "eArztbrief" -->
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:eab"
xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides" Version="4.0">
——<Target/>
——<Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:eab"
Effect="Permit">
——<Target>
——<Resources>
——<Resource>
——<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
——<AttributeValue DataType="urn:hl7-org:v3#CV">
——<CodedValue xmlns="urn:hl7-org:v3"
code="urn:gematik:ig:Arztbrief:r3.1"
——<codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
——</AttributeValue>
——<ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:format-
code"
——<DataType="
urn:hl7-org:v3#CV"/>
——</ResourceMatch>
——</Resource>
——</Resources>
——</Target>
——</Rule>
——<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
——<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:eab:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.7 Mittelgranulare Berechtigung: Kategorie "eau"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:eau"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides" Version="4.0">
——<Target/>
——<Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:eau"
Effect="Permit">
——<Target>
——<Resources>
——<Resource>
——<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
——<AttributeValue DataType="urn:hl7-org:v3#CV">

```

```

-----<CodedValue xmlns="urn:hl7-org:v3"
code="urn:gematik:ig:Arbeitsunfähigkeitsbescheinigung:r4.0"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
-----</AttributeValue>
-----<ResourceAttributeDesignator
AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
org:v3#CV"/>
-----</ResourceMatch>
-----</Resource>
-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:eau:default-deny" Effect="Deny"/>
-----</Policy>

```

### 9.5.8 Mittelgranulare Berechtigung: Kategorie "ega"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:ega"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides" Version="4.0">
-----<Target/>
-----<!-- Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:ega"
Effect="Permit">
-----<Target>
-----<Resources>
-----<Resource>
-----<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
-----<AttributeValue DataType="urn:hl7-org:v3#CV">
-----<CodedValue xmlns="urn:hl7-org:v3" code="ega"
codeSystem="TODO"/>
-----</AttributeValue>
-----<ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
-----</ResourceMatch>
-----</Resource>
-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:ega:default_deny" Effect="Deny"/>
-----</Policy>

```

### 9.5.9 Mittelgranulare Berechtigung: Kategorie "emp"

```

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

```

```

RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides" Version="4.0">
  <Target/>
  <RuleRuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:emp"
Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatchMatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValueDataType="urn:hl7-org:v3#CV">
              <CodedValuexmlns="urn:hl7-org:v3"
code="urn:gematik:ig:Medikationsplan:r3.1"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
            </AttributeValue>
            <ResourceAttributeDesignatorAttributeId="urn:ihe:iti:appc:2016:docum
ent-entry:format-code" DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <RuleRuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:emp:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.10 Mittelgranulare Berechtigung: Kategorie "mothersrecord"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:mothersrecord"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides" Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:mothersrecord" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3"
code="urn:gematik:ig:Mutterpass:r4.0" codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:related-folder:code"
DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-

```

```

hcp:categories:mothersrecord:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.11 Mittelgranulare Berechtigung: Kategorie "nfd"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:nfd"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides" Version="4.0">
  <Target/>
  <!-- Notfalldatensatz -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:nfd:nfd" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3"
code="urn:gematik:ig:Notfalldatensatz:r3.1"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:format-code" DataType="urn:hl7-
org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Persönliche Erklärung -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:nfd:pe"
Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3"
code="urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:format-code" DataType="urn:hl7-
org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:nfd:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.12 Mittelgranulare Berechtigung: Kategorie "other"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-hcp:categories:other"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
  <!-- practiceSettingCode = 1.3.6.1.4.1.19376.3.276.1.5.4 (ärztlich) -->
  <Target>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-
equal">
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
            <CodedValue codeSystem="1.3.6.1.4.1.19376.3.276.1.5.4"/>
          </AttributeValue>
          <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:practice-setting-code"
DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
        </ResourceMatch>
      </Resource>
    </Resources>
  </Target>
  <!-- typeCode = ABRE, PATI oder SCHR -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:other:type-code" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="ABRE"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:type-code" DataType="urn:hl7-
org:v3#CV" MustBePresent="true"/>
          </ResourceMatch>
        </Resource>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="PATI"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:type-code" DataType="urn:hl7-
org:v3#CV" MustBePresent="true"/>
          </ResourceMatch>
        </Resource>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="SCHR"

```

```

codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
</AttributeValue>
</ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:type-code" DataType="urn:hl7-
org:v3#CV" MustBePresent="true"/>
</ResourceMatch>
</Resource>
</Resources>
</Target>
</Rule>
<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:other:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.13 Mittelgranulare Berechtigung: Kategorie "patientdoc"

```

<?xmlversion="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:patientdoc" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:deny-overrides" Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:patientdoc" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue code="102"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.13"/>
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-submission-set:author-role" DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:patientdoc:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.14 Mittelgranulare Berechtigung: Kategorie "prescription"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:prescription" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:deny-overrides" Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:prescription" Effect="Permit">
    <Target>

```

```

</Resources>
</Resource>
<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
  <AttributeValue DataType="urn:hl7-org:v3#CV">
    <CodedValue xmlns="urn:hl7-org:v3"
code="urn:gematik:ig:VerordnungsdatensatzMedikation:r4.0"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
  </AttributeValue>
  <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:apcc:2016:document-entry:format-code" DataType="urn:hl7-
org:v3#CV"/>
</ResourceMatch>
</Resource>
</Resources>
</Target>
</Rule>
<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:prescription:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.15 Mittelgranulare Berechtigung: Kategorie "receipt"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:receipt" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:deny-overrides" Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:receipt"
Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="VER"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.3"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:apcc:2016:document-entry:healthcare-facility-type-code"
DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="ABRE"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.9"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:apcc:2016:document-entry:type-code" DataType="urn:hl7-
org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>

```

```

—————</Resources>
—————</Target>
—————</Rule>
—————<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann —>
—————<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:receipt:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.16 Mittelgranulare Berechtigung: Kategorie "vaccination"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:vaccination" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:deny-overrides" Version="4.0">
  <Target/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:vaccination" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3"
code="urn:gematik:ig:Impfausweis:r4.0"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
            </AttributeValue>
            <ResourceAttributeDesignator
AttributeId="urn:ihe:iti:appc:2016:document-entry:format-code" DataType="urn:hl7-
org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann —>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:vaccination:default-deny" Effect="Deny"/>
</Policy>

```

### 9.5.17 Mittelgranulare Berechtigung: Kategorie "practitioner"

```

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

```

```

-----<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
-----<AttributeValue DataType="urn:hl7-org:v3#CV">
-----<CodedValue xmlns="urn:hl7-org:v3" code="practitioner"
codeSystem="TODO"/>
-----</AttributeValue>
-----<ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
-----</ResourceMatch>
-----</Resource>
-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:practitioner:default-deny" Effect="Deny">
-----<Target/>
-----</Rule>
-----</Policy>

```

### 9.5.18 Mittelgranulare Berechtigung: Kategorie "hospital"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:hospital" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:permit-overrides" Version="4.0">
-----<Target/>
-----<!-- Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:hospital" Effect="Permit">
-----<Target>
-----<Resources>
-----<Resource>
-----<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
-----<AttributeValue DataType="urn:hl7-org:v3#CV">
-----<CodedValue xmlns="urn:hl7-org:v3" code="hospital"
codeSystem="TODO"/>
-----</AttributeValue>
-----<ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
-----</ResourceMatch>
-----</Resource>
-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:hospital:default-deny" Effect="Deny">
-----<Target/>
-----</Rule>
-----</Policy>

```

### 9.5.19 Mittelgranulare Berechtigung: Kategorie "laboratory"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hep:categories:laboratory" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-
combining-algorithm:permit-overrides" Version="4.0">
  <Target/>
  <!-- Prüfung, ob folder.codeList den Code "laboratory" enthält (TODO: Code System
hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hep:categories:laboratory" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="laboratory"
codeSystem="TODO"/>
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hep:categories:laboratory:default-deny" Effect="Deny">
    <Target/>
  </Rule>
</Policy>

```

### 9.5.20 Mittelgranulare Berechtigung: Kategorie "physiotherapy"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hep:categories:physiotherapy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
  <Target/>
  <!-- Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hep:categories:physiotherapy" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="physiotherapy"
codeSystem="TODO"/>
            </AttributeValue>

```

```

-----<ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related_folder:codeList" DataType="urn:hl7-org:v3#CV"/>
-----</ResourceMatch>
-----</Resource>
-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:physiotherapy:default-deny" Effect="Deny">
-----<Target/>
-----</Rule>
-----</Policy>

```

### 9.5.21 Mittelgranulare Berechtigung: Kategorie "psychotherapy"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:psychotherapy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
-----<Target/>
-----<!-- Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:psychotherapy" Effect="Permit">
-----<Target>
-----<Resources>
-----<Resource>
-----<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
-----<AttributeValue DataType="urn:hl7-org:v3#CV">
-----<CodedValue xmlns="urn:hl7-org:v3" code="psychotherapy"
codeSystem="TODO"/>
-----</AttributeValue>
-----<ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related_folder:codeList" DataType="urn:hl7-org:v3#CV"/>
-----</ResourceMatch>
-----</Resource>
-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:psychotherapy:default-deny" Effect="Deny">
-----<Target/>
-----</Rule>
-----</Policy>

```

### 9.5.22 Mittelgranulare Berechtigung: Kategorie "dermatology"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:dermatology" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-

```

```

combining-algorithm:permit-overrides" Version="4.0">
  <Target/>
  <!-- Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:dermatology" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="dermatology"
codeSystem="TODO"/>
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:dermatology:default-deny" Effect="Deny">
    <Target/>
  </Rule>
</Policy>

```

### 9.5.23 Mittelgranulare Berechtigung: Kategorie "gynaecology\_urology"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:gynaecology_urology"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
  <Target/>
  <!-- Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:gynaecology_urology" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="gynaecology_urology"
codeSystem="TODO"/>
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>

```

```

-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:gynaecology_urology:default-deny" Effect="Deny">
-----<Target/>
-----</Rule>
-----</Policy>

```

### 9.5.24 Mittelgranulare Berechtigung: Kategorie "dentistry\_oms"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:dentistry_oms"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
-----<Target/>
-----<!-- Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:dentistry_oms" Effect="Permit">
-----<Target>
-----<Resources>
-----<Resource>
-----<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
-----<AttributeValue DataType="urn:hl7-org:v3#CV">
-----<CodedValue xmlns="urn:hl7-org:v3" code="dentistry_oms"
codeSystem="TODO"/>
-----</AttributeValue>
-----<ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
-----</ResourceMatch>
-----</Resource>
-----</Resources>
-----</Target>
-----</Rule>
-----<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
-----<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:dentistry_oms:default-deny" Effect="Deny">
-----<Target/>
-----</Rule>
-----</Policy>

```

### 9.5.25 Mittelgranulare Berechtigung: Kategorie "other\_medical"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:other_medical"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
-----<Target/>
-----<!-- Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System

```

hier und unten ergänzen) →

```

<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:other_medical" Effect="Permit">
  <Target>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
          <AttributeValue DataType="urn:hl7-org:v3#CV">
            <CodedValue xmlns="urn:hl7-org:v3" code="other_medical"
codeSystem="TODO"/>
          </AttributeValue>
          <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related_folder:codeList" DataType="urn:hl7-org:v3#CV"/>
        </ResourceMatch>
      </Resource>
    </Resources>
  </Target>
</Rule>
<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
<Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:other_medical:default-deny" Effect="Deny">
  <Target/>
</Rule>
</Policy>

```

### 9.5.26 Mittelgranulare Berechtigung: Kategorie "other\_non\_medical"

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:other_non_medical"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
  <Target/>
  <!-- Prüfung, ob folder.codeList den Code "other_non_medical" enthält (TODO: Code
System hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:other_non_medical" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="other_non_medical"
codeSystem="TODO"/>
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related_folder:codeList" DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>

```

```
—<!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->  
—<Rule RuleId="urn:gematik:rule-id:permissions-access-group-  
hcp:categories:other_non_medical:default-deny" Effect="Deny">  
—<Target/>  
—</Rule>  
</Policy>
```