

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation ePA- Dokumentenverwaltung

Version:	1. 6 7.0
Revision:	294776328297
Stand:	12.11.2020 19.02.2021
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 -> 5.1.2.2.1 A_13585 von ehemals 4.2.3.3 -> 5.1.1.2.1 A_14585 von ehemals 4.2.3.4 -> 5.1.1.4.1 A_14589 von ehemals 4.2.3.7 -> 5.1.2.4.1 A_13657 von ehemals 4.2.3.7 -> 5.1.1.1.1 A_14052 von ehemals 4.2.3.7 -> 5.1.1.1.1 A_13656 von ehemals 4.2.3.7 -> 5.1.1.1.1 A_15080 von ehemals 4.2.3.10 -> 5.1.1.5.1</p> <p>Umgekehrt wurden übergreifende Afos nach Kapitel 4 verschoben und Afo-Duplikate storniert</p> <p>A_14926 von 5.1.2.3.1 -> 4.2.3.4 A_15162 von 5.1.2.1.1 -> 4.2.3.3 A_14937 von 5.1.2.1.1 -> 4.2.3.3 A_14938 von 5.1.2.1.1 -> 4.2.3.3</p>	gematik
1.2.0	28.06.19		Einarbeitung Änderungsliste P19.1	gematik
1.3.0	02.10.19		Einarbeitung Änderungsliste P20.1/2	gematik
1.4.0	02.03.20		Einarbeitung Änderungsliste P21.1	gematik

1.4.1	26.06.20		Einarbeitung Änderungsliste P21.3	gematik
1.5.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
1.6.0	12. 11 10.20		Einarbeitung der Scope-Themen aus R4.0.1, PDSG-Änderungen	gematik
1.7.0	19.02.21		Einarbeitung Änderungsliste P22.5	gematik

Inhaltsverzeichnis

1 Einführung	13
1.1 Zielsetzung	13
1.2 Zielgruppe	13
1.3 Geltungsbereich	13
1.4 Abgrenzungen	13
1.5 Methodik	14
2 Systemkontext	15
3 Zerlegung der Komponente	16
4 Übergreifende Festlegungen	18
4.1 Namensräume	18
4.2 Nutzung von IHE IT Infrastructure Profilen für Speicherung und Abruf von Dokumenten	19
4.2.1 Anforderungen an IHE ITI-Akteure	19
4.2.1.1 APPC Content Consumer	21
4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren	21
4.2.1.1.2 Optionen des IHE ITI-Akteurs	21
4.2.1.2 RMU Update Responder	22
4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren	22
4.2.1.2.2 Optionen des IHE ITI-Akteurs	22
4.2.1.3 XCA Responding Gateway	23
4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
4.2.1.3.2 Optionen des IHE ITI-Akteurs	23
4.2.1.4 XCDR Responding Gateway	23
4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
4.2.1.4.2 Optionen des IHE ITI-Akteurs	24
4.2.1.5 XDS Document Registry	24
4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren	24
4.2.1.5.2 Optionen des IHE ITI-Akteurs	24
4.2.1.6 XDS Document Repository	25
4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren	25
4.2.1.6.2 Optionen des IHE ITI-Akteurs	25
4.2.1.7 XUA X-Service Provider	25
4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren	25
4.2.1.7.2 Optionen des IHE ITI-Akteurs	25
4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen	26
4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen	30

4.2.3.1 Provide X-User Assertion [ITI-40].....	30
4.2.3.2 Provide and Register Document Set-b [ITI-41].....	31
4.2.3.3 Remove Metadata [ITI-62].....	32
4.3 Fehlerbehandlung in Schnittstellenoperationen	33
4.4 Vertrauenswürdige Ausführungsumgebung	34
4.4.1 Verarbeitungskontext	35
4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	36
4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes	37
4.4.4 Parallele Zugriffe.....	38
4.4.5 Konsistenz der Akte, Logging und Monitoring.....	39
4.4.6 Client Verbindungen zum Verarbeitungskontext.....	39
4.5 Anforderungen zur sicherheitstechnischen Validierung.....	40
4.6 Protokollierung.....	43
4.6.1 Protokollierung von Berechtigungen	50
5 Funktionsmerkmale	55
5.1 Dokumentenverwaltung	55
5.1.1 Schnittstelle I_Document_Management	55
5.1.1.1 Operation I_Document_Management::CrossGatewayDocumentProvide ...	56
5.1.1.1.1 Umsetzung	57
5.1.1.2 Operation I_Document_Management::CrossGatewayQuery	59
5.1.1.2.1 Umsetzung	60
5.1.1.3 Operation I_Document_Management::RemoveMetadata	64
5.1.1.3.1 Umsetzung	65
5.1.1.4 Operation I_Document_Management::CrossGatewayRetrieve	65
5.1.1.4.1 Umsetzung	67
5.1.2 Schnittstelle I_Document_Management_Insurant.....	70
5.1.2.1 Operation	
I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b.....	71
5.1.2.1.1 Umsetzung	72
5.1.2.2 Operation I_Document_Management_Insurant::RegistryStoredQuery.....	73
5.1.2.2.1 Umsetzung	74
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	82
5.1.3 Schnittstelle I_Document_Management_Insurance.....	83
5.1.3.1 Operation	
I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b	84
5.1.3.1.1 Umsetzung	86
5.1.4 Anforderungen an Sammlungstypen	86
5.2 Aktenkontoverwaltung	87
5.2.1 Schnittstelle I_Account_Management_Insurant.....	87

5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount.....	88
5.2.1.1.1 Umsetzung.....	90
5.2.1.2 Operation I_Account_Management_Insurant::ResumeAccount.....	91
5.2.1.2.1 Umsetzung.....	93
5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents.....	95
5.2.1.3.1 Umsetzung.....	97
5.3 Umschlüsselung.....	98
5.3.1 Übergreifende Anforderungen.....	99
5.3.2 Schnittstelle I_Key_Management_Insurant.....	104
5.3.2.1 I_Key_Management_Insurant::StartKeyChange().....	104
5.3.2.1.1 Umsetzung.....	106
5.3.2.2 I_Key_Management_Insurant::GetAllDocumentKeys().....	107
5.3.2.2.1 Umsetzung.....	108
5.3.2.3 Operation I_Key_Management_Insurant::PutAllDocumentKeys().....	109
5.3.2.3.1 Umsetzung.....	111
5.3.2.4 Operation I_Key_Management_Insurant::FinishKeyChange().....	111
5.3.2.4.1 Umsetzung.....	113
5.3.2.5 Protokollierung.....	113
5.4 Zugriffskontrolle.....	115
5.4.1 Grob-, mittel- und feingranulare Berechtigungen.....	115
5.4.2 Berufsgruppenspezifische Einschränkungen.....	116
5.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln.....	116
5.4.4 Vergabe von Zugriffsregeln.....	117
5.4.5 Funktionsprinzip Policy Administration.....	117
5.4.6 Anforderungen an die Zugriffskontrollprüfung.....	121
5.4.6.1 Erstmaliges Öffnen eines Verarbeitungskontextes.....	127
5.4.6.2 Berechtigung für einen Versicherten.....	127
5.4.6.3 Berechtigung für einen Vertreter.....	128
5.4.6.4 Berechtigung für eine Leistungserbringerinstitution.....	129
5.4.6.5 Berechtigung für einen Kostenträger.....	129
5.4.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4.....	129
5.5 Vertrauenswürdige Ausführung.....	131
5.5.1 Schnittstelle I_Document_Management_Connect.....	131
5.5.1.1 Operation I_Document_Management_Connect::OpenContext.....	136
5.5.1.1.1 Umsetzung.....	137
5.5.1.2 Operation I_Document_Management_Connect::CloseContext.....	138
5.5.1.2.1 Umsetzung.....	139
5.5.2 Hardware-Merkmale.....	140
5.6 Statische Akteninhalte.....	140
6 Informationsmodelle.....	142
7 Anhang A Verzeichnisse.....	143
7.1 Abkürzungen.....	143
7.2 Glossar.....	145
7.3 Abbildungsverzeichnis.....	145

7.4 Tabellenverzeichnis	145
7.5 Referenzierte Dokumente	149
7.5.1 Dokumente der gematik	149
7.5.2 Weitere Dokumente	150
8 Anhang B XACML 2.0 Profile für Policy Documents (für Upgrade von ePA 3.1.3)	154
8.1 Policy Document für einen Versicherten	154
8.1.1 Base Policy	154
8.1.2 Permission Policy	157
8.2 Policy Document für einen Vertreter	188
8.2.1 Base Policy	188
8.2.2 Permission Policy	192
8.3 Policy Document für eine Leistungserbringereinstitution	220
8.3.1 Base Policy zum Zugriff auf Leistungserbringer Dokumente	220
8.3.2 Permission Policy zum Zugriff auf Leistungserbringer Dokumente	225
8.3.3 Permission Policy zum Zugriff auf Versicherten und Kostenträger Dokumente	251
8.4 Policy Document für einen Kostenträger	275
8.4.1 Base Policy	275
8.4.2 Permission Policy	278
9 Anhang C XACML 2.0 Profile für Policy Documents	282
9.1 Policy Document für einen Versicherten	282
9.2 Policy Document für einen Vertreter	285
9.3 Policy Document für eine Leistungserbringereinstitution	289
9.4 Policy Document für einen Kostenträger	310
9.5 Statische Permission Policies	315
9.5.1 Grobgranulare Berechtigung: Stufe Normal	315
9.5.2 Grobgranulare Berechtigung: Stufe Erweitert	316
9.5.3 Mittelgranulare Berechtigung: Kategorie "care"	316
9.5.4 Mittelgranulare Berechtigung: Kategorie "childsrecord"	317
9.5.5 Mittelgranulare Berechtigung: Kategorie "dentalrecord"	317
9.5.6 Mittelgranulare Berechtigung: Kategorie "eab"	318
9.5.7 Mittelgranulare Berechtigung: Kategorie "eau"	319
9.5.8 Mittelgranulare Berechtigung: Kategorie "ega"	319
9.5.9 Mittelgranulare Berechtigung: Kategorie "emp"	320
9.5.10 Mittelgranulare Berechtigung: Kategorie "mothersrecord"	320
9.5.11 Mittelgranulare Berechtigung: Kategorie "nfd"	321
9.5.12 Mittelgranulare Berechtigung: Kategorie "other"	322
9.5.13 Mittelgranulare Berechtigung: Kategorie "patientdoc"	323
9.5.14 Mittelgranulare Berechtigung: Kategorie "prescription"	324
9.5.15 Mittelgranulare Berechtigung: Kategorie "receipt"	324
9.5.16 Mittelgranulare Berechtigung: Kategorie "vaccination"	325
9.5.17 Mittelgranulare Berechtigung: Kategorie "practitioner"	326
9.5.18 Mittelgranulare Berechtigung: Kategorie "hospital"	326
9.5.19 Mittelgranulare Berechtigung: Kategorie "laboratory"	327
9.5.20 Mittelgranulare Berechtigung: Kategorie "physiotherapy"	328
9.5.21 Mittelgranulare Berechtigung: Kategorie "psychotherapy"	328

9.5.22 Mittelgranulare Berechtigung: Kategorie "dermatology"	329
9.5.23 Mittelgranulare Berechtigung: Kategorie "gynaecology_urology"	329
9.5.24 Mittelgranulare Berechtigung: Kategorie "dentistry_oms"	330
9.5.25 Mittelgranulare Berechtigung: Kategorie "other_medical"	331
9.5.26 Mittelgranulare Berechtigung: Kategorie "other_non_medical"	331
1 Einführung	13
1.1 Zielsetzung	13
1.2 Zielgruppe	13
1.3 Geltungsbereich	13
1.4 Abgrenzungen	13
1.5 Methodik	14
2 Systemkontext.....	15
3 Zerlegung der Komponente.....	16
4 Übergreifende Festlegungen	18
4.1 Namensräume	18
4.2 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von Dokumenten	19
4.2.1 Anforderungen an IHE ITI-Akteure	19
4.2.1.1 <i>APPC Content Consumer</i>	21
4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren	21
4.2.1.1.2 Optionen des IHE ITI-Akteurs	21
4.2.1.2 <i>RMU Update Responder</i>	22
4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren	22
4.2.1.2.2 Optionen des IHE ITI-Akteurs	22
4.2.1.3 <i>XCA Responding Gateway</i>	23
4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
4.2.1.3.2 Optionen des IHE ITI-Akteurs	23
4.2.1.4 <i>XCDR Responding Gateway</i>	23
4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
4.2.1.4.2 Optionen des IHE ITI-Akteurs	24
4.2.1.5 <i>XDS Document Registry</i>	24
4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren	24
4.2.1.5.2 Optionen des IHE ITI-Akteurs	24
4.2.1.6 <i>XDS Document Repository</i>	25
4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren	25
4.2.1.6.2 Optionen des IHE ITI-Akteurs	25
4.2.1.7 <i>XUA X-Service Provider</i>	25
4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren	25
4.2.1.7.2 Optionen des IHE ITI-Akteurs	25

4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen	26
4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen	30
4.2.3.1 <i>Provide X-User Assertion [ITI-40]</i>	30
4.2.3.2 <i>Provide and Register Document Set-b [ITI-41]</i>	31
4.2.3.3 <i>Remove Documents [ITI-86]</i>	32
4.2.3.4 <i>Remove Metadata [ITI-62]</i>	32
4.3 Fehlerbehandlung in Schnittstellenoperationen	33
4.4 Vertrauenswürdige Ausführungsumgebung	34
4.4.1 Verarbeitungskontext	35
4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld	36
4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes	37
4.4.4 Parallele Zugriffe	38
4.4.5 Konsistenz der Akte, Logging und Monitoring	39
4.4.6 Client-Verbindungen zum Verarbeitungskontext	39
4.5 Anforderungen zur sicherheitstechnischen Validierung	40
4.6 Protokollierung	43
4.6.1 Protokollierung von Berechtigungen	50
5 Funktionsmerkmale	55
5.1 Dokumentenverwaltung	55
5.1.1 Schnittstelle I_Document_Management	55
5.1.1.1 <i>Operation I_Document_Management::CrossGatewayDocumentProvide</i> ...	56
5.1.1.1.1 Umsetzung	57
5.1.1.2 <i>Operation I_Document_Management::CrossGatewayQuery</i>	59
5.1.1.2.1 Umsetzung	60
5.1.1.3 <i>Operation I_Document_Management::RemoveDocuments (abgekündigt)</i> ..	62
5.1.1.3.1 Umsetzung	63
5.1.1.4 <i>Operation I_Document_Management::RemoveMetadata</i>	64
5.1.1.4.1 Umsetzung	65
5.1.1.5 <i>Operation I_Document_Management::CrossGatewayRetrieve</i>	65
5.1.1.5.1 Umsetzung	67
5.1.1.6 <i>Operation I_Document_Management::RestrictedUpdateDocumentSet</i>	67
5.1.1.6.1 Umsetzung	69
5.1.2 Schnittstelle I_Document_Management_Insurant	70
5.1.2.1 <i>Operation</i> <i>I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b</i>	71
5.1.2.1.1 Umsetzung	72
5.1.2.2 <i>Operation I_Document_Management_Insurant::RegistryStoredQuery</i>	73
5.1.2.2.1 Umsetzung	74
5.1.2.3 <i>Operation I_Document_Management_Insurant::RemoveMetadata</i>	77
5.1.2.3.1 Umsetzung	78
5.1.2.4 <i>Operation I_Document_Management_Insurant::RetrieveDocumentSet</i> ...	79
5.1.2.4.1 Umsetzung	80
5.1.2.5 <i>Operation</i> <i>I_Document_Management_Insurant::RestrictedUpdateDocumentSet</i>	81
5.1.2.5.1 Umsetzung	82

5.1.3 Schnittstelle I_Document_Management_Insurance.....	83
5.1.3.1 Operation	
I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b	84
5.1.3.1.1 Umsetzung	86
5.1.4 Anforderungen an Sammlungstypen	86
5.2 Aktenkontoverwaltung	87
5.2.1 Schnittstelle I_Account_Management_Insurant.....	87
5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount.....	88
5.2.1.1.1 Umsetzung	90
5.2.1.2 Operation I_Account_Management_Insurant::ResumeAccount.....	91
5.2.1.2.1 Umsetzung	93
5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents	95
5.2.1.3.1 Umsetzung	97
5.2.1.4 Operation I_Account_Management_Insurant::GetSignedAuditEvents	97
5.2.1.4.1 Umsetzung	98
5.3 Umschlüsselung	98
5.3.1 Übergreifende Anforderungen	99
5.3.2 Schnittstelle I_Key_Management_Insurant.....	104
5.3.2.1 I_Key_Management_Insurant::StartKeyChange()	104
5.3.2.1.1 Umsetzung	106
5.3.2.2 I_Key_Management_Insurant::GetAllDocumentKeys()	107
5.3.2.2.1 Umsetzung	108
5.3.2.3 Operation I_Key_Management_Insurant::PutAllDocumentKeys()	109
5.3.2.3.1 Umsetzung	111
5.3.2.4 Operation I_Key_Management_Insurant::FinishKeyChange()	111
5.3.2.4.1 Umsetzung	113
5.3.2.5 Protokollierung.....	113
5.4 Zugriffskontrolle.....	115
5.4.1 Grob-, mittel- und feingranulare Berechtigungen	115
5.4.2 Berufsgruppenspezifische Einschränkungen	116
5.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln	116
5.4.4 Vergabe von Zugriffsregeln	117
5.4.5 Funktionsprinzip Policy Administration	117
5.4.6 Anforderungen an die Zugriffskontrollprüfung	121
5.4.6.1 Erstmaliges Öffnen eines Verarbeitungskontextes.....	127
5.4.6.2 Berechtigung für einen Versicherten	127
5.4.6.3 Berechtigung für einen Vertreter	128
5.4.6.4 Berechtigung für eine Leistungserbringerinstitution	129
5.4.6.5 Berechtigung für einen Kostenträger.....	129
5.4.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4	129
5.5 Vertrauenswürdige Ausführung.....	131
5.5.1 Schnittstelle I_Document_Management_Connect	131
5.5.1.1 Operation I_Document_Management_Connect::OpenContext	136
5.5.1.1.1 Umsetzung	137
5.5.1.2 Operation I_Document_Management_Connect::CloseContext	138
5.5.1.2.1 Umsetzung	139
5.5.2 Hardware-Merkmale	140

5.6 Statische Akteninhalte.....	140
6 Informationsmodelle	142
7 Anhang A – Verzeichnisse	143
7.1 Abkürzungen	143
7.2 Glossar	145
7.3 Abbildungsverzeichnis.....	145
7.4 Tabellenverzeichnis	145
7.5 Referenzierte Dokumente	149
7.5.1 Dokumente der gematik.....	149
7.5.2 Weitere Dokumente.....	150
8 Anhang B – XACML 2.0-Profile für Policy Documents (für Upgrade von ePA 3.1.3)	154
8.1 Policy Document für einen Versicherten	154
8.1.1 Base Policy	154
8.1.2 Permission Policy	157
8.2 Policy Document für einen Vertreter	188
8.2.1 Base Policy	188
8.2.2 Permission Policy	192
8.3 Policy Document für eine Leistungserbringerinstitution	220
8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente	220
8.3.2 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente	225
8.3.3 Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente	251
8.4 Policy Document für einen Kostenträger	275
8.4.1 Base Policy	275
8.4.2 Permission Policy	278
9 Anhang C– XACML 2.0-Profile für Policy Documents	282
9.1 Policy Document für einen Versicherten	282
9.2 Policy Document für einen Vertreter	285
9.3 Policy Document für eine Leistungserbringerinstitution	289
9.4 Policy Document für einen Kostenträger	310
9.5 Statische Permission Policies	315
9.5.1 Grobgranulare Berechtigung: Stufe Normal	315
9.5.2 Grobgranulare Berechtigung: Stufe Erweitert.....	316
9.5.3 Mittelgranulare Berechtigung: Kategorie "care"	316
9.5.4 Mittelgranulare Berechtigung: Kategorie "childsrecord"	317
9.5.5 Mittelgranulare Berechtigung: Kategorie "dentalrecord"	317
9.5.6 Mittelgranulare Berechtigung: Kategorie "eab"	318
9.5.7 Mittelgranulare Berechtigung: Kategorie "eau"	319
9.5.8 Mittelgranulare Berechtigung: Kategorie "ega"	319
9.5.9 Mittelgranulare Berechtigung: Kategorie "emp"	320
9.5.10 Mittelgranulare Berechtigung: Kategorie "mothersrecord"	320

9.5.11 Mittelgranulare Berechtigung: Kategorie "nfd"	321
9.5.12 Mittelgranulare Berechtigung: Kategorie "other"	322
9.5.13 Mittelgranulare Berechtigung: Kategorie "patientdoc"	323
9.5.14 Mittelgranulare Berechtigung: Kategorie "prescription"	324
9.5.15 Mittelgranulare Berechtigung: Kategorie "receipt"	324
9.5.16 Mittelgranulare Berechtigung: Kategorie "vaccination"	325
9.5.17 Mittelgranulare Berechtigung: Kategorie "practitioner"	326
9.5.18 Mittelgranulare Berechtigung: Kategorie "hospital"	326
9.5.19 Mittelgranulare Berechtigung: Kategorie "laboratory"	327
9.5.20 Mittelgranulare Berechtigung: Kategorie "physiotherapy"	328
9.5.21 Mittelgranulare Berechtigung: Kategorie "psychotherapy"	328
9.5.22 Mittelgranulare Berechtigung: Kategorie "dermatology"	329
9.5.23 Mittelgranulare Berechtigung: Kategorie "gynaecology_urology"	329
9.5.24 Mittelgranulare Berechtigung: Kategorie "dentistry_oms"	330
9.5.25 Mittelgranulare Berechtigung: Kategorie "other_medical"	331
9.5.26 Mittelgranulare Berechtigung: Kategorie "other_non_medical"	331

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.

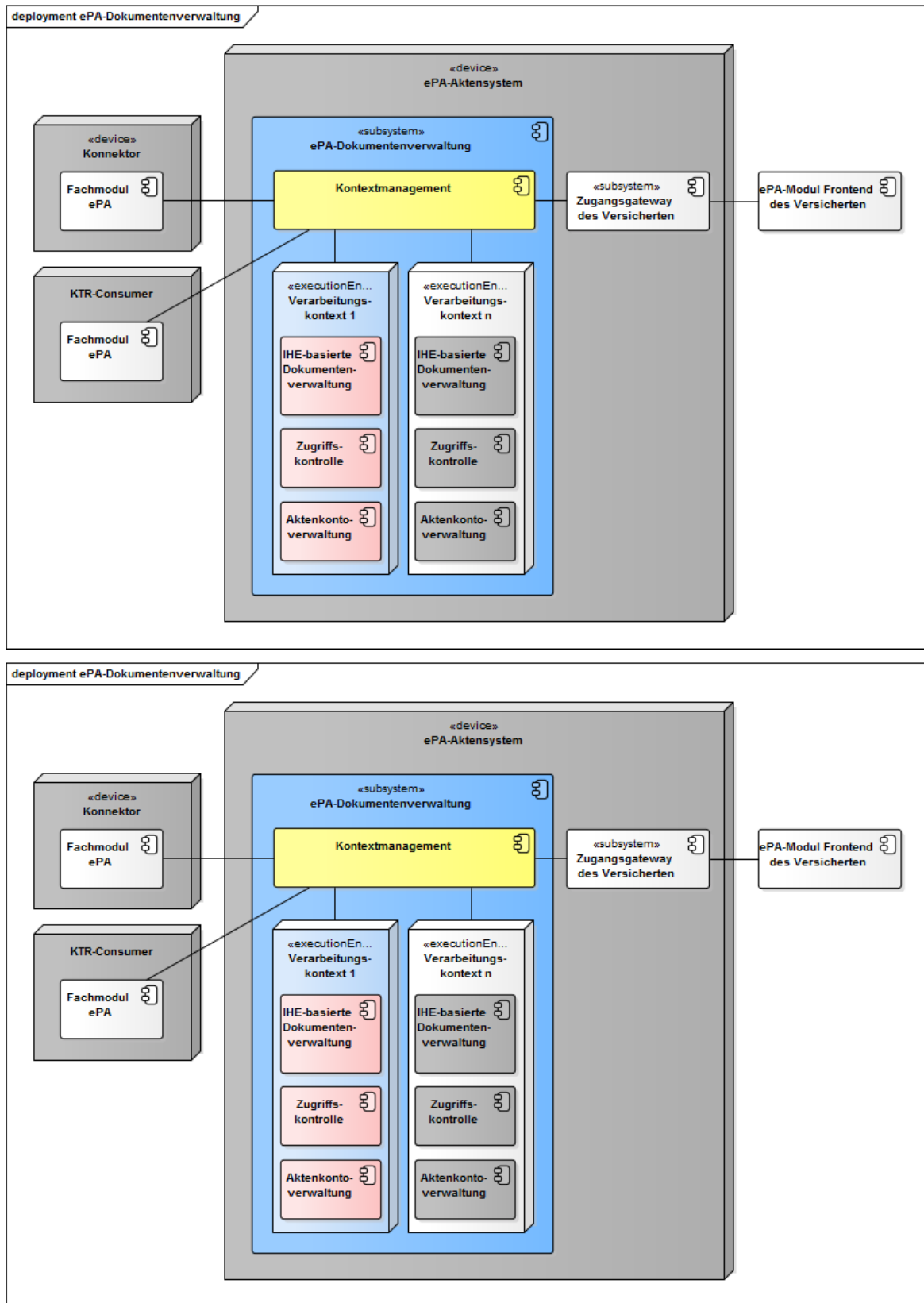


Abbildung 1: Komponentenzерlegung ePA-Dokumentenverwaltung

4 Übergreifende Festlegungen

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

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

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

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

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

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

4.1 Namensräume

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

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

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

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

In diesem Abschnitt werden Anforderungen und Einschränkungen an relevante IHE ITI-Akteure und -Transaktionen der Komponente ePA-Dokumentenverwaltung gestellt, um die geforderte IHE ITI-Semantik zum ePA-Aktensystem zu bewahren. Werden IHE ITI-Akteure mit weiteren Sub-Akteuren gruppiert, so werden die Anforderungen der Sub-Akteure zum gruppierten Akteur übernommen. Eine Übersicht und Herleitung der IHE ITI-Akteure ist [\[gemSpec_DM_ePA#2.1.3\]](#) zu entnehmen. In Abschnitt 4.2.2 wird ein zusammenfassender Überblick über die 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_14655-01A_14655 - Komponente ePA-Dokumentenverwaltung – Zeitsynchronisation über Zeitdienst in der TI

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

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

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

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

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

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

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

[<=]

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

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

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

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

[<=]

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

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

[<=]

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

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

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

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

[<=]

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

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

4.2.1.1 APPC Content Consumer*4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren*

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

*4.2.1.1.2 Optionen des IHE ITI-Akteurs***A_14787 - Komponente ePA-Dokumentenverwaltung – APPC Content Consumer ohne "View Option"-Option**

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

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. [≤]

4.2.1.2 RMU Update Responder

4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren

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

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

[≤]

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. [≤]

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.

[≤]

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.

[≤]

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

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

[≤]

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.

[≤]

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	R
			XDS Persistence	X
			XDS Version Persistence	X
		APPC Content Consumer	R	
		XCA Responding Gateway	R	
		X-Service Provider	R	
XCDR Responding Gateway	R		Basic Patient Privacy Enforcement	X
		APPC Content Consumer	R	
		ATNA Secure Node oder Secure Application für Node	X	

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

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

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

4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen

A_17832 - Komponente ePA-Dokumentenverwaltung – Unterstützung MTOM/XOP

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

4.2.3.1 Provide X-User Assertion [ITI-40]

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

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

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

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

A_14594 - Komponente ePA-Dokumentenverwaltung – Validierung der Authentication Assertion

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

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

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

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

[<=]

A_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` (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)

[<=]

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

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

4.2.3.3 Remove Documents [ITI-86]

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

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

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

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

A_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.uniqueId` des Dokuments aus der Whitelist aller LEI-Policy-Dokumente (gemäß 9.3) löschen, welche die entsprechende `DocumentEntry.uniqueId` referenzieren. [`<=`]

4.2.3.3.4 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. [\leq]

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

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

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.uniqueId` des Dokuments aus der Whitelist aller LEI-Policy-Dokumente (gemäß 9.3) löschen, welche die entsprechende `DocumentEntry.uniqueId` referenzieren. [\leq]

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-hcp:base']/Policy[@PolicySetId='urn:gematik:policy-id:permissions-access-group-hcp: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 nicht vollständig gelöscht werden, da die LEI damit auch die Schreibberechtigung in die Akte des Versicherten verlieren würde, die mit einer Berechtigung immer grundsätzlich einhergeht.

4.3 Fehlerbehandlung in Schnittstellenoperationen

Bei Fehlern in der internen Verarbeitung oder fachlichen Fehlern in der Nutzung der von der Komponente ePA-Dokumentenverwaltung bereitgestellten Schnittstellen werden Operationsaufrufe von Nicht-IHE-Operationen mit gematik-Fehlermeldungen gemäß der Definition in [gemSpec_OM] beantwortet. Die Fehlermeldungen werden als SOAP-Fault

gemäß [TelematikError.xsd] strukturiert. Abweichend von den Festlegungen in [gemSpec_OM] [des](#) sind zu meldende Fehler wie folgt mit Informationen zu füllen.

A_15664 - Komponente ePA-Dokumentenverwaltung – Fehlername

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

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 Vertrauenswürdigen Ausführungsumgebung.

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

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

A_14557 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext der VAU

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[≤]

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

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

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

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

4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes

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

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

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln gewährleisten, dass schützenswerte Nutzdaten im Verarbeitungskontext erst nach Aktivierung – mittels Übergabe des korrekten *Kontextschlüssels* an den

Verarbeitungskontext durch den Client eines berechtigten Nutzers – entschlüsselt und verarbeitet werden können. [≤]

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

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

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

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

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

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

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

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS sämtliche aktenbezogenen Daten (Nutzdaten, Konfigurationsdaten und Schlüsselmateriale) 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. [\leq]

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

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

[\leq]

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

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

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

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

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

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

[\leq]

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

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

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. [\leq]

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_13690-02 - 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 gemäß [WSS#12] bzw. im Sonderfall der Authorization Assertion mit einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls eine Übereinstimmung nicht festgestellt werden kann.

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

Tabelle 4: Tab_Dokv_35 - Eingangsparameter für TUC_PKI_018

Parameter	Belegung
	SAML 2.0 Assertion des Fachmodul ePA
Zertifikat	Signaturzertifikat
PolicyList	oid_smc_b_osig
intendedKeyUsage	nonRepudiation
intendedExtendedKeyUsage	(leer)
OCSP-Graceperiod	60 Minuten

Offline-Modus	nein
Prüfmodus	OCSP

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

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

A_18990 - ePA-Dokumentenverwaltung – Beschränkung gültiger Identitätsbestätigungen

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

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. [\leq]

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.

[\leq]

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]). [\leq]

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

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

- XML Injection
- XPath Query Tampering

- XML External Entity Injection

[<=]

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

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

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

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

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

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

4.6 Protokollierung

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

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

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

- I_Document_Management::CrossGatewayDocumentProvide
- I_Document_Management::CrossGatewayQuery
- I_Document_Management::RemoveMetadata
- I_Document_Management::RemoveDocuments
- I_Document_Management::CrossGatewayRetrieve
- I_Document_Management::RestrictedUpdateDocumentSet
- I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::RestrictedUpdateDocumentSet
- I_Document_Management_Insurant::RegistryStoredQuery
- I_Document_Management_Insurant::RemoveMetadata
- I_Document_Management_Insurant::RetrieveDocumentSet
- I_Account_Management_Insurant::GetAuditEvents
- I_Account_Management_Insurant::GetSignedAuditEvents

- `I_Account_Management_Insurant::SuspendAccount`
- `I_Account_Management_Insurant::ResumeAccount`
- `I_Key_Management_Insurant::StartKeyChange`
- ~~`I_Key_Management_Insurant::GetAllDocumentKeys`~~
- ~~`I_Key_Management_Insurant::PutAllDocumentKeys`~~
- ~~`I_Key_Management_Insurant::FinishKeyChange`~~

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

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

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

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

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

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

Protokollparameter	Parameterwerte gemäß aufgerufener Operation
--------------------	---

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

	<p>• <i>I_Document_Management_Insurant</i></p> <p>XPath-Ausdruck zum SAML-Subject der im Operationsaufruf übergebenen Authentication Assertion:</p> <pre>//*[local-name()='Assertion' and namespace-uri()='urn:oasis:names:tc:SAML:2.0:assertion']/*[local-name()='Subject']/*[local-name()='NameID']/text()[normalize-space()='']</pre>				
Object- ID	<p>Der unveränderbare Anteil der KVNR des <code>extension</code>-Attributs aus dem <code>InsurantId</code>-Element des <code>RecordIdentifier</code>-Elements oder die <code>DocumentEntry.patientId</code> des entsprechenden Operationsaufrufs</p> <p><i>Hinweis: Bei Aufruf von Operationen ohne diesen Parameter wird der Wert im Protokolleintrag nicht belegt.</i></p>				
Object Detail ObjectD etail	<p>Bei Zugriff über für alle Operationen gilt: Falls die Transaktionen-Operation mit einem Fehler ASSERTION_INVALID aufgrund einer ungültigen übergebenen Authentication Assertion abbricht,</p> <p>• <i>CrossGatewayDocumentProvide</i></p> <p>• <i>ProvideAndRegisterDocumentSet-b</i></p> <p>• <i>CrossGatewayRetrieve</i></p> <p>• <i>RetrieveDocumentSet</i></p> <p>• <i>RemoveMetadata</i></p> <p>• <i>RestrictedUpdateDocumentSet</i></p> <p>MUSS <code>ParticipantObjectDetail</code> beim Zugriff auf Dokumente mit folgenden Wertepaaren (<code>type/value</code>) belegt werden:</p> <table> <tr> <th>type</th><th>value</th></tr> <tr> <td>ErrorInformation</td><td>"fehlgeschlagene Authentifizierung des Zugreifenden"</td></tr> </table> <p>Bei Zugriff über die Operationen:</p> <ul style="list-style-type: none"> • <i>CrossGatewayDocumentProvide</i> • <i>ProvideAndRegisterDocumentSet-b</i> • <i>CrossGatewayRetrieve</i> • <i>RetrieveDocumentSet</i> • <i>RemoveMetadata</i> • <i>RemoveDocuments</i> • <i>RestrictedUpdateDocumentSet</i> 	type	value	ErrorInformation	"fehlgeschlagene Authentifizierung des Zugreifenden"
type	value				
ErrorInformation	"fehlgeschlagene Authentifizierung des Zugreifenden"				

MUSS ParticipantObjectDetail beim Zugriff auf Dokumente mit folgenden Wertepaaren (type/value) belegt werden:	
type	value
DocumentUniqueId	Wert von DocumentEntry.uniqueId
DocumentTitle	Wert von DocumentEntry.title
DocumentPracticeSetting	Wert von DocumentEntry.practiceSettingCode, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3]. (Beispiel: „ALLG^^^&1.3.6.1.4.1.19376.3.276.1.5.4&ISO“, wobei ALLG für den Code und 1.3.6.1.4.1.19376.3.276.1.5.4 für das Code System steht.
DocumentFormat	<p>Wert von DocumentEntry.formatCode, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3]., siehe oben.</p> <p>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.
und beim Zugriff auf Ordner mit den folgenden Wertepaaren (type/value) belegt werden:	
type	value
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	type	value
	ParameterQueryId	Der Wert MUSS der Parameter Query ID gemäß [IHE-ITI-TF3]#3.18.4.1.2.4 entsprechen.
<p>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):</p> <ul style="list-style-type: none"> 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. 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. 		
Object-Detail	type	value
	Query Parameter Name (UUID-Format: "urn:uuid:...")	Parameterwert

[<=]

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
Queryparameter auf einzelnen Wert (Code):	
"\$XDSDocumentEntryFormatCode"	"('urn:gematik:ig:Arztbrief:r3.1^^1.3.6.1.4.1.19376.3.276.1.5.6')"
Query auf zwei ODER-verknüpfte Werte:	
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')"
Query auf zwei UND-verknüpfte Werte	
Zwei Einträge für denselben Parameter: 1. "\$XDSDocumentEntryEventCodeList" 2. "\$XDSDocumentEntryEventCodeList"	1. "('H3^^1.3.6.1.4.1.19376.3.276.1.5.15')" 2. "('E100^^1.3.6.1.4.1.19376.3.276.1.5.16')"

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 Metadatums 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.

A_20564-01A_20564 - Komponente ePA-Dokumentenverwaltung – Protokollierung neuer Berechtigungen

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

- CrossGatewayDocumentProvide
- ProvideAndRegisterDocumentSet-b

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

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

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

[<=]

A_20565-01A-~~20565~~ - Komponente ePA-Dokumentenverwaltung – Protokollierung aktualisierter Berechtigungen

Die Komponente ePA-Dokumentenverwaltung MUSS beim Einstellen von APPC-Policy-Dokumenten (gemäß emSpec_DM_ePA#A_14961) über die Transaktionen

- CrossGatewayDocumentProvide
- ProvideAndRegisterDocumentSet

das Protokoll gemäß A_20538-* um die folgenden Details ergänzen, sofern bereits eine Berechtigung für den betroffenen Berechtigten existiert, die durch die neue Berechtigung aktualisiert wird:

Protokollparameter	Parameterwerte beim Aktualisieren von Policy-Dokumenten	
	type	value

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

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

[<=]

A_20566-01A_20566 - Komponente ePA-Dokumentenverwaltung – Protokollierung gelöschter Berechtigungen

Die Komponente ePA-Dokumentenverwaltung MUSS beim Löschen von APPC-Policy-Dokumenten (gemäß emSpec_DM_ePA#A_14961) über die Transaktionen

- I_Document_Management_Insurant::RemoveMetadata

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

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

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

[<=]

5 Funktionsmerkmale

5.1 Dokumentenverwaltung

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

5.1.1 Schnittstelle I_Document_Management

A_14152-01A_14152 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management

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

Tabelle 6: Tab_Dokv_14 - Schnittstelle I_Document_Management

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

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

[<=]

5.1.1.1 Operation

I_Document_Management::CrossGatewayDocumentProvide

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

Die Komponente ePA-Dokumentenverwaltung MUSS

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

Tabelle 7: Tab_Dokv_15 - Operation Cross-Gateway Document Provide

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

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

[<=]

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_14941-03 - 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` (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:2010:AssociationType:APND` (Addendum)

[<=]

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 MB = $25 * (1024)^2$ 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 - 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 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. 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 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Cross-Gateway Document Provide

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

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

[<=]

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

~~A_14924 – Komponente ePA-Dokumentenverwaltung – Keine Herausgabe von Metadaten zu Policy Documents (Advanced Patient Privacy Consents)~~ 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.

[<=]

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

```

<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  PolicyId="urn:uuid:6e84f679-5f36-4861-bfb5-607aef021fff"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
  <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="57016-8"
              codeSystem="1.2.276.0.76.11.32"/>
          </AttributeValue>
          <ResourceAttributeDesignator
            AttributeId="urn:ihe:iti:appe:2016:document-entry:class-code"
            DataType="urn:hl7-org:v3#CV" MustBePresent="true"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Policy>

```



```

</Resources>
</Target>
<Rule RuleId="urn:uuid:bb42d632-e70e-447d-94aa-011f2e9561f4"
Effect="Deny"/>
</Policy>

```

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

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

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

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

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

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt zum Fachmodul ePA als XCA-Akteur "Initiating Gateway" zurückgegeben wird. Widerspricht die Suchergebnismenge ganz oder teilweise einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Suchergebnismenge dahingehend gefiltert werden, dass nur berechnete 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 `$XDSDocumentEntryAuthorInstitution` verarbeiten können, sodass eine Suchergebnismenge über den `authorInstitution`-Slot der `XDSDocumentEntry.author-Classification` (Wertemenge des `authorInstitution`-Sub-Attributs) eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter `$XDSDocumentEntryAuthorPerson`. [`<=`]

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	<code>I_Document_Management::RemoveDocuments</code>
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_Document_Management::deleteDocuments</code> technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove Documents" [ITI-86] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente eines Aktenkontos im ePA-Aktensystem zu löschen.
Formatvorgaben	SOAP Action: <code>urn:ihe:iti:2017:RemoveDocuments</code>
Eingangsparameter	

Name	Beschreibung	Typ	opt
Remove Documents Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocuments_Message	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt
Remove Documents Response Message	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocumentsResponse_Message	n
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	

[<=]

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.

[<=]

5.1.1.35.1.1.4 Operation I_Document_Management::RemoveMetadata

A_14489-02A_14489-01 - Komponente ePA-Dokumentenverwaltung – Signatur für RemoveMetadata

Die Komponente ePA-Dokumentenverwaltung MUSS

die Operation I_Document_Management::RemoveMetadata gemäß der folgenden Signatur implementieren:

Tabelle 9: Tab_Dokv_17 - Operation RemoveMetadata

Operation	I_Document_Management::RemoveMetadata		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management::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, Ordner und/oder Associations eines Aktenkontos im ePA-Aktensystem zu löschen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2010>DeleteDocumentSet		
Eingangsparameter			
Name	Beschreibung	Typ	optional
Remove Documents Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	xds>DeleteDocumentSet_Message	nein
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringereinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	nein
Ausgangsparameter			
Name	Beschreibung	Typ	optional
Remove Documents Response Message	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	xds>DeleteDocumentSetResponse_Message	nein
Technische Fehlermeldungen			
Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.			

Name	Fehlertext	Details

[<=]

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

~~5.1.1.3~~ 5.1.1.4.1 Umsetzung

A_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#3.86.4.1.2 und 3.86.4.1.3] implementieren.[<=]

~~A_20713 – Komponente ePA-Dokumentenverwaltung – Remove Metadata mit uniqueIds (Übergangsphase)~~

~~Falls in der Anfragenachricht zu `I_Document_Management::RemoveMetadata` im Feld `/RemoveObjectsRequest/ObjectRefList/ObjectRef[@id]` anstelle einer `entryUUID` eine `uniqueId` gesendet wird, MUSS die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" die Operation gemäß A_14908-01 durchführen, als wenn stattdessen dort die `DocumentEntry.entryUUID` des Dokuments hinterlegt wäre, dessen `DocumentEntry.uniqueId` der gesendeten `uniqueId` entspricht.[<=]~~

A_20633 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Remove Metadata

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

~~5.1.1.4~~ 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

Operation	<code>I_Document_Management::CrossGatewayRetrieve</code>

Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management::getDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Cross-Gateway Retrieve" [ITI-39] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente aus dem ePA-Aktensystem abzufragen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:CrossGatewayRetrieve		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Cross-Gateway Retrieve Message	Eingangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetRequest	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Cross-Gateway Retrieve Response Message	Ausgangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetResponse	n
Technische Fehlermeldungen			
<i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße der angefragten Dokumente übersteigt 250 MByte.	

[<=]

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.

5.1.1.4.15.1.1.5.1 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. [\leq]

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. [\leq]

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 `XSDDocumentUniqueIdError`-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 `XSDDocumentUniqueIdError` zurückgegeben werden. [\leq]

5.1.1.6 Operation

I_Document_Management::RestrictedUpdateDocumentSet

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

A_21190 - Komponente ePA-Dokumentenverwaltung – Signatur für Restricted Update Document Set

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

Tabelle 11: Tab_Dokv_45 - Operation Restricted Update Document Set

Operation	<code>I_Document_Management::RestrictedUpdateDocumentSet</code>
-----------	---

Beschreibung	<p>Diese Operation setzt die in [gemSysL_ePA] definierte Operation <code>I_PHR_Management::updateMetadata</code> technisch um. Sie basiert auf den IHE ITI-Transaktionen "Restricted Update Document Set" [ITI-92] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, Metadaten zu Dokumenten zu ändern.</p> <p>Die Operation wurde in früheren ePA-Releases dazu genutzt, Dokumente von Versicherten oder Kostenträger als "leistungserbringeräquivalent" zu kennzeichnen oder eine entsprechende Kennzeichnung zu entfernen. Da eine entsprechende Kennzeichnung nicht mehr möglich ist, liefert der Aufruf der Operation nun in jedem Fall einen Fehler zurück.</p>		
Formatvorgabe n	SOAP Action: urn:ihe:iti:2018:RestrictedUpdateDocumentSet		
Eingangsparameter			
Name	Beschreibung	Typ	opt .
Update Responder Restricted Update Document Set	Eingangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	lcm:SubmitObjectsRequest	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_149 27, A_15638]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt .
Update Responder Restricted Update Document Set Response	Ausgangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	rs:RegistryResponse	n
Technische Fehlermeldungen <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 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management_Insurant

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

Tabelle 12: Tab_Dokv_20 - Schnittstelle I_Document_Management_Insurant

Schnittstelle	I_Document_Management_Insurant	
Version	1.0.1	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente in der Dokumentenverwaltung
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Documents	Löschen ein oder mehrerer Dokumente
WSDL	DocumentManagementService.wsdl	
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd 	

[<=]

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 13: Tab_Dokv_21 - Operation Provide And Register Document Set-b

Operation	I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::putDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Provide And Register Document Set-b" [ITI-41] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente mitsamt Metadaten im ePA-Aktensystem dauerhaft zu speichern.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Provide And Register Document Set-b Message	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	n
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers# A_14109, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Provide And Register Document Set-b Response Message	Ausgangsnachricht zum Registrieren und Speichern ein	rs:RegistryResponse	n

	oder mehrerer Dokumente		
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	
MaxDocSizeExceeded	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines einzelnen übermittelten Dokuments übersteigt 25 MByte.	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

[<=]

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

5.1.2.1.1 Umsetzung

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

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

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

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

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

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12]

quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht. [\leq]

5.1.2.2 Operation

I_Document_Management_Insurant::RegistryStoredQuery

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

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

I_Document_Management_Insurant::RegistryStoredQuery gemäß der folgenden Signatur implementieren:

Tabelle 14: Tab_Dokv_22 - Operation Registry Stored Query

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

Technische Fehlermeldungen

Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.

Name	Fehlertext	Details

[<=]

Weitere Details zur Ausgestaltung dieser Operation in Bezug zu den zugehörigen IHE ITI-Transaktionen "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. **[<=]**

A_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] quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.

[<=]**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 `$XDSDocumentEntryTitle` unterstützen, sodass eine Suchergebnismenge über das Attribut `XDSDocumentEntry.title` eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter `$XDSDocumentEntryAuthorPerson`. Das `wsa:Action-Element` MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery" besitzen.

[<=]**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.

[<=]

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.

[<=]

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.author-Classification` (Wertemenge des authorInstitution-Sub-Attributs) eingeschränkt werden

kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter `$XDSDocumentEntryAuthorPerson.[<=]`

~~Die folgende Anforderung ermöglicht~~

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".

~~5.1.2.2.1.11.1.1.1.1.1.1 Suche mit simulierter Berechtigung~~

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

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

- Der Parameter wird als Slot mit dem Namen `impersonatePolicy` kodiert.
- Der Parameter MUSS eine vollständige Base Policy für eine LEI (gemäß [9.3](#)) oder eines Kostenträgers (gemäß [9.4](#)) enthalten.
- Der Wert (die XML-Policy) MUSS Base64-kodiert im Datentyp `String` gemäß [IHE-ITI-TF3] abgelegt werden
- Der Parameter (sofern gesendet) MUSS immer die Multiplizität 1 besitzen.

- Wenn der Parameter nicht genutzt wird, dann DARF der entsprechende Slot nicht gesendet werden (d. h. es darf nicht stattdessen ein leerer Wert gesendet werden).

[<=]

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

Die in A_20224 definierte Suche MUSS wie folgt umgesetzt werden:

- Wenn die in A_20224 genannten Bestimmungen nicht erfüllt sind, MUSS die Komponente ePA-Dokumentenverwaltung einen Fehler zurückgeben (`ResponseStatusType:Failure`).
- Ansonsten gelten folgende Bestimmungen:
 - Die Komponente ePA-Dokumentenverwaltung MUSS die im Base64-Format enthaltene Policy dekodieren.
 - Die Komponente ePA-Dokumentenverwaltung DARF das Policy-Dokument NICHT in der Dokumentenverwaltung hinterlegen. Sie wird also für andere Anfragen an die Schnittstellen der Dokumentenverwaltung nicht beachtet.
 - Die Komponente ePA-Dokumentenverwaltung DARF NICHT ein anderes (etwaig hinterlegtes) Base Policy Dokument für dieselbe LEI oder KTR im Rahmen dieser Suche beachten.
 - Die Komponente ePA-Dokumentenverwaltung MUSS die Klartextpolicy gemäß 5.4.6 behandeln und bei erfolgreicher Zugriffskontrollprüfung ("Permit") die Suche wie in 5.1.2.2 beschrieben unter Beachtung der Policy umsetzen.

[<=]

5.1.2.3 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 15: Tab_Dokv_23 - Operation RemoveMetadata

Operation	I_Document_Management_Insurant::RemoveMetadata
Beschreibung	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 Metadata" [ITI-62] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente im ePA-Aktensystem zu löschen.
Formatvorgabe n	SOAP Action: urn:ihe:iti:2010:DeleteDocumentSet
Eingangsparameter	

Name	Beschreibung	Typ	opt .
Remove Metadata Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	xds:DeleteDocumentSet_Message	n
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt .
Remove Metadata Response Message	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	xds:DeleteDocumentSetResponse_Message	n
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	

[<=]

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.

5.1.2.3.1 Umsetzung

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

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

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

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

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

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

Tabelle 16: Tab_Dokv_24 - Operation Retrieve Document Set

Operation	I_Document_Management_Insurant::RetrieveDocumentSet		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::getDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Retrieve Document Set" [ITI-43] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente aus dem ePA-Aktensystem abzufragen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:RetrieveDocumentSet		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Retrieve Document Set Message	Eingangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetRequest	n
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
Ausgangsparameter			

Name	Beschreibung	Typ	opt
Retrieve Document Set Response Message	Ausgangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetResponse	n
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße der angefragten Dokumente übersteigt 250 MByte.	

[<=]

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.

5.1.2.4.1 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 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion

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

[<=]

A_16200 - Komponente ePA-Dokumentenverwaltung – Prüfung der zurückgegebenen Paketgröße

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

[<=]

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

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

[<=]

5.1.2.5 Operation

I_Document_Management_Insurant::RestrictedUpdateDocumentSet

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

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

Tabelle 17: Tab_Dokv_19 - Operation RestrictedUpdateDocumentSet

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

X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringereinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Update Responder Restricted Update Document Set Response	Ausgangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	rs:RegistryResponse	n
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			

[<=]

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.

5.1.2.5.1 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_15061-01 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Restricted Update Document Set

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

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

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

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

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

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

[<=]

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 18: Tab_Dokv_36 - Schnittstelle I_Document_Management_Insurance

Schnittstelle	I_Document_Management_Insurance	
Version	1.0.1	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente in der Dokumentenverwaltung
WSDL	DocumentManagementService.wsdl	
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd 	

[<=]

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 19: Tab_Dokv_37 - Operation Provide And Register Document Set-b

Operation	I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
-----------	---

Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurance::putDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Provide And Register Document Set-b" [ITI-41] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente mitsamt Metadaten im ePA-Aktensystem dauerhaft zu speichern.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b		
Eingangsparameter			
Name	Beschreibung	Typ	optional
Provide And Register Document Set-b Message	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	nein
X-User Assertion	Authentication Assertion des authentifizierten Kostenträgers	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA_KTR_Consumer #A_17253, A_17254]	nein
Ausgangsparameter			
Name	Beschreibung	Typ	optional
Provide And Register Document Set-b Response Message	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	rs:RegistryResponse	nein
Technische Fehlermeldungen			
<i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	

MaxDocSizeExceeded	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines einzelnen übermittelten Dokuments übersteigt 25 MByte.
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.

[<=]

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

5.1.3.1.1 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 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion

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

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_20627 - Komponente ePA-Dokumentenverwaltung – Kein Ordner für Sammlungstyp "mixed" ohne entsprechendes strukturiertes Dokument

Die Komponente ePA-Dokumentenverwaltung MUSS das Anlegen eines Folders für den Verwaltungstyp "mixed" mit dem Fehler `XDSRegistryMetadataError` unterbinden, wenn nicht in derselben Operation auch mindestens ein entsprechendes Sammlungstyp-spezifisches strukturiertes Dokument (gemäß [gemSpec_DM_ePA#A_20577](#)) eingestellt

wird und die Operation mit dem Fehler ACCESS_DENIED abbrechen, wenn der Zugreifende nicht die Berechtigung besitzt, den Ordner und alle für den vorgesehenen Ordner mitgesendeten Dokumente anzulegen.

[<=]

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

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

[<=]

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

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

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

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

[<=]

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

5.2 Aktenkontoverwaltung

5.2.1 Schnittstelle I_Account_Management_Insurant

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

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

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

Tabelle 20: Tab_Dokv_25 - Schnittstelle I_Account_Management_Insurant

Schnittstelle	I_Account_Management_Insurant
Version	1.0.1

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

[<=]

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 21: Tab_Dokv_26 - Operation Suspend Account

Operation	I_Account_Management_Insurant::SuspendAccount
Beschreibung	<p>Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Account_Management_Insurant::SuspendAccount technisch um.</p> <p>Mit dieser Operation werden die Daten aus der Akte eines Versicherten bei einem Anbieter ePA-Aktensystem in ein für andere Anbieter ePA-Aktensystem verarbeitbares Paket konsolidiert.</p>
Formatvorgaben	<p>SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/SuspendAccount</p>

Eingangsparameter			
Name	Beschreibung	Typ	opt.
X-User Assertion	Authentication Assertion des authentifizierten Versicherten als Inhaber der Akte	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109, A_15631]	n
Ausgangsparameter			
Package URL	URL, über die das erzeugte Exportpaket vom neuen Anbieter ePA-Aktensystem geladen werden kann	URL mit Prozentkodierung	n
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig.	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
TEMP_UNAVAILABLE	Aktenkonto aufgrund einer andauernden Datenmigration vorübergehend nicht erreichbar	Dies sollte nur auftreten, wenn ein Anbieterwechsel angestoßen, aber noch nicht abgeschlossen wurde.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.	Der Nutzer hat nicht die erforderliche Berechtigung.	

[<=]

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 `I_Account_Management_Insurant::SuspendAccount` ausführen kann.

A_15062 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Suspend Account

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

A_14885-01A_14885 - Komponente ePA-Dokumentenverwaltung – Exportpaket des Aktenkontos erstellen

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

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

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

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

- die ZIP-Datei außerhalb des Verarbeitungskontextes persistieren,
- die ZIP-Datei im Zuge des Exports mit dem `ContextKey` gemäß [gemSpec_Krypt#GS-A_5016] verschlüsseln, so dass sichergestellt ist, dass nur entsprechend verschlüsselte Daten außerhalb des Verarbeitungskontextes auftreten können ~~sowie~~,
- die § 291a-Protokolldaten innerhalb der ZIP-Datei unter dem Dateinamen **PROTO291.XML** mit der folgenden Struktur

```
<?xml version="1.0" encoding="UTF-8"
xmlns: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 berechnigte 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 22: Tab_Dokv_27 - Operation Resume Account

Operation	I_Account_Management_Insurant::ResumeAccount		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Account_Management_Insurant::ResumeAccount technisch um. Mit dieser Operation wird das Paket mit den Daten aus der Akte eines Versicherten beim vorhergehenden Anbieter ePA-Aktensystem bezogen und importiert.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/ResumeAccount		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Package URL	URL, über die das vom vorhergehenden Anbieter ePA-Aktensystem erzeugte Exportpaket geladen werden kann	URL mit Prozentkodierung	n
X-User Assertion	Authentication Assertion des authentifizierten des Versicherten als Inhaber der Akte	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers# A_14109, A_15631]	n
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig.	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	

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

[<=]

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 - 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 der Verarbeitungskontext eines für einen Anbieterwechsel mit Übernahme der Aktendaten registriertes Aktenkonto erstmalig durch den Versicherten geöffnet wurde.[<=]

A_15568 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Resume Account

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

A_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.[<=]

A_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.

[<=]

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. [\leq]

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. [\leq]

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. [\leq]

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

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

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

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

[\leq]

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

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS den für die Operation `I_Account_Management_Insurant::ResumeAccount` geöffneten

Verarbeitungskontext so lange geöffnet lassen, bis der Abruf des Exportpakets beim alten Anbieter erfolgt ist und die Verarbeitung der Daten des Exportpakets durch diesen Verarbeitungskontext abgeschlossen ist, jedoch maximal drei Tage, falls kein Exportpaket abgerufen werden kann.

[\leq]

A_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 `REGISTERED_FOR_MIGRATION` 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_14490-04A_14490-03~~ - Komponente ePA-Dokumentenverwaltung – Signatur für Get Audit Events

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

Tabelle 23: Tab_Dokv_28 - Operation Get Audit Events

Operation	I_Account_Management_Insurant::GetAuditEvents		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Account_Management_Insurant::GetAuditEvents technisch um. Mit dieser Operation kann der Versicherte bzw. sein berechtigter Vertreter das § 291a-Zugriffsprotokoll eines Aktenkontos herunterladen.		
Formatvorgabe n	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/GetAuditEvents		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
AuditLog-PageSize	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (> 0)	y
AuditLog-PageNumber	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (> 0)	y
AuditLog-LastDay	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	YYYY-MM-DD	y

Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Audit Event List	Liste der Zugriffsprotokolleinträge	phr:AuditMessage	n
AuditLog- PageSize	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (> 0)	y
AuditLog- PageNumber	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (> 0)	y
AuditLog- TotalPages	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (>= 0)	y
AuditLog- TotalEntries	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (>= 0)	y
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.		

[<=]

5.2.1.3.1 Umsetzung

A_15229-02 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Get Audit Events

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

[<=]

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

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

5.2.1.4 Operation

I_Account_Management_Insurant::GetSignedAuditEvents**A_21110 - Komponente ePA-Dokumentenverwaltung – Signatur für Get Signed Audit Events**

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

Tabelle 24: Tab_Dokv_44 - Operation Get Signed Audit Events

Operation	I_Account_Management_Insurant::GetSignedAuditEvents		
Beschreibung	Mit dieser Operation erhält der Versicherte bzw. sein berechtigter Vertreter eine signierte Liste aller in der Dokumentenverwaltung vorliegenden Protokolleinträge des Versicherten.		
Formatvorgabe n	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/GetSignedAuditEvents		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.

Signed Audit Event List	Signierte Liste der Zugriffsprotokolleinträge	Signiertes PDF/A-Dokument	n
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.		

[<=]

5.2.1.4.1 Umsetzung

A_21111 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Get Signed Audit Events

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

A_21112 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Get Signed Audit Events

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

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

5.3 Umschlüsselung

Die ePA-Dokumentenverwaltung verwaltet verschlüsselte Dokumente: Die Dokumente selbst sind mit einem dokumentenspezifischen Dokumentenschlüssel verschlüsselt, der

wiederum mit dem Aktenschlüssel verschlüsselt wird und so verpackt dem Dokument beigelegt wird. Die Dokumentenmetadaten, das Protokoll des Versicherten sowie die Policy-Dokumente werden zudem über einen Kontextschlüssel gesichert. Akten- und Kontextschlüssel sind für die gesamte Akte des Versicherten gültig.

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

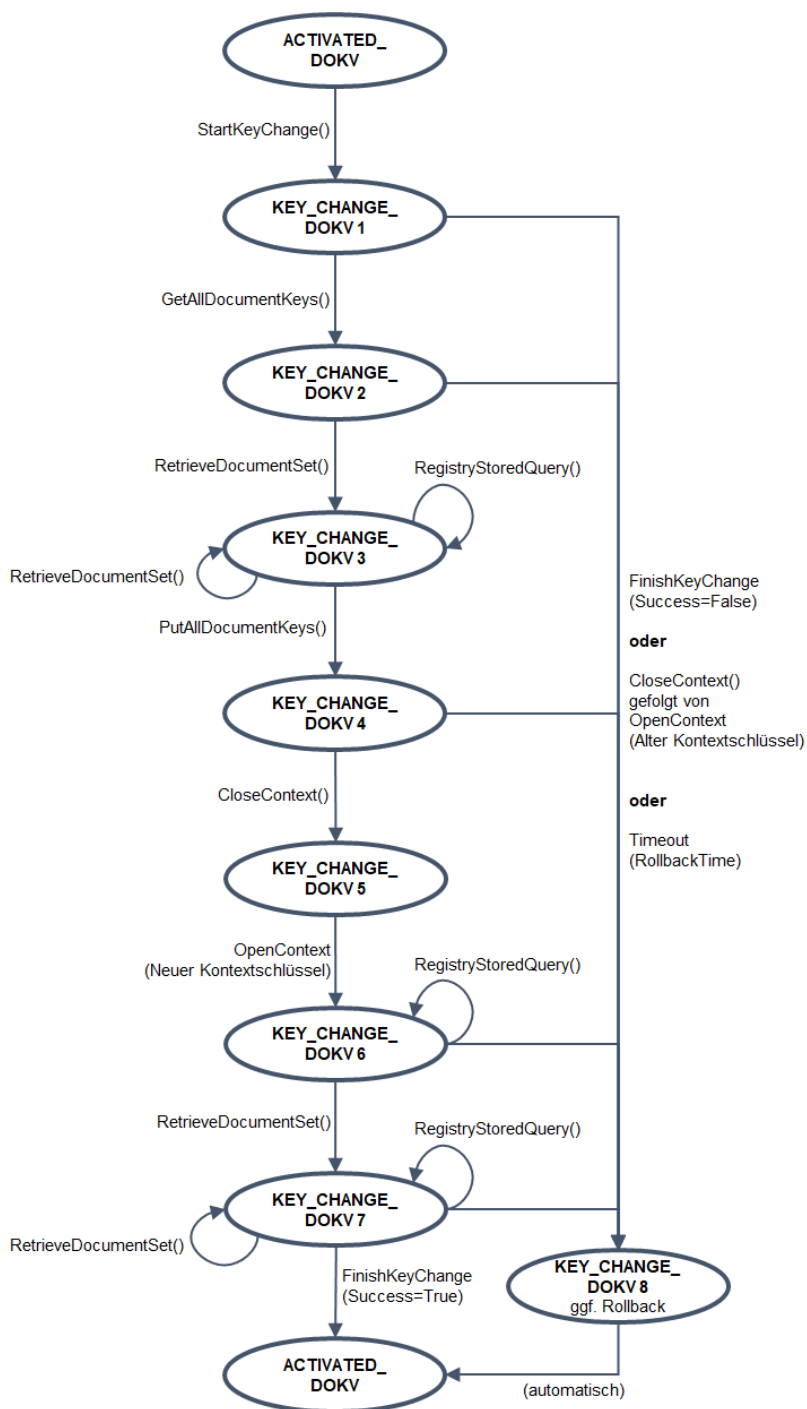
Die Dokumentenverwaltung befindet sich nach erfolgreicher Einleitung der Umschlüsselung (StartKeyChange()) im logischen Zustand "KEY_CHANGE_DOKV". Sie ist dabei für alle Teilnehmer außer den Versicherten sowie für alle Operationen, die nicht die Umschlüsselung betreffen, gesperrt.

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 - 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.



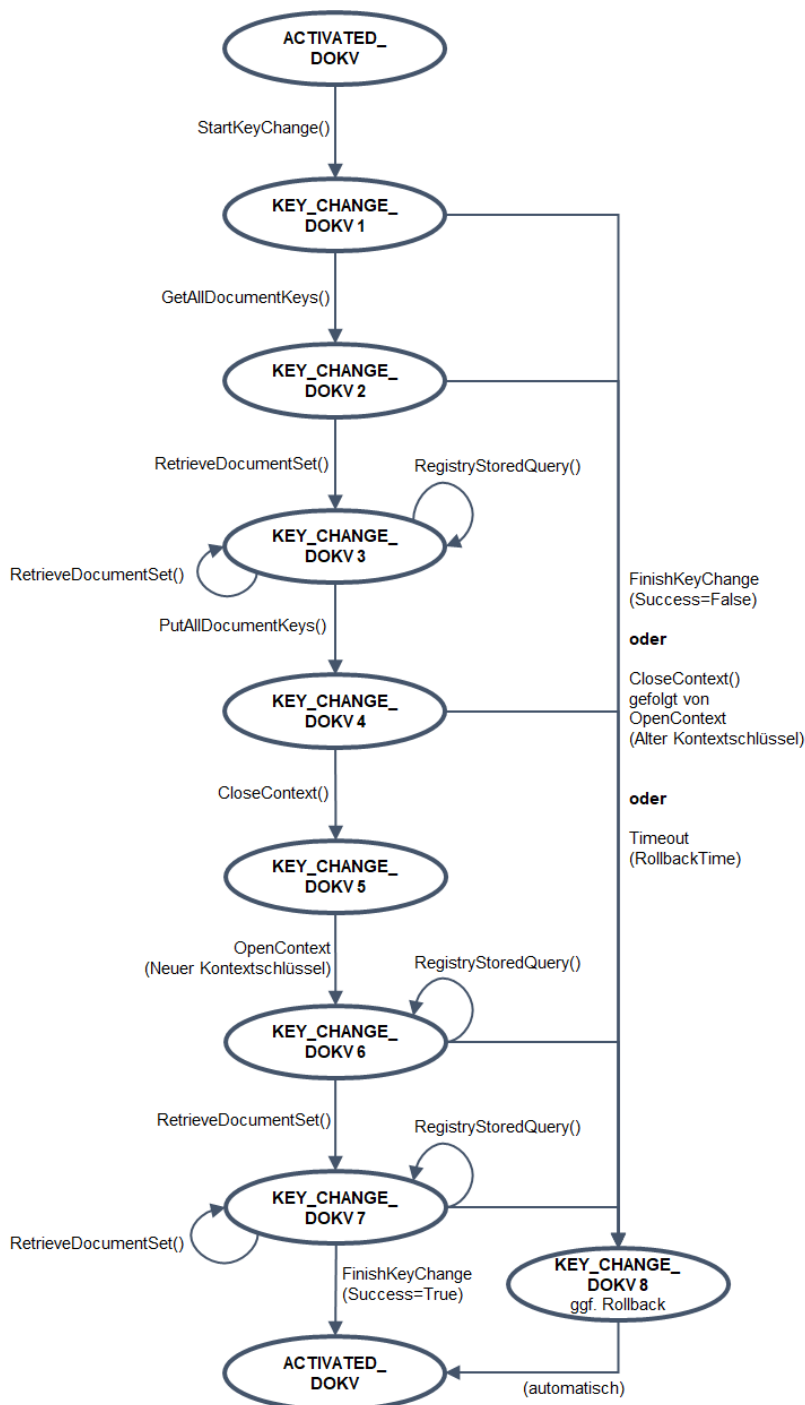


Abbildung 2: Zustandsübergänge Schlüsselwechsel

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

[<=]

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

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

A_20729 - Komponente ePA-Dokumentenverwaltung – Start der Umschlüsselung nur in Zustand Activated

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

A_20726 - Komponente ePA-Dokumentenverwaltung – Verbotene Operationen außerhalb Status KEY_CHANGE_DOKV

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

A_20727 - Komponente ePA-Dokumentenverwaltung – Validierung der Authentication Assertion

Die Komponente ePA-Dokumentenverwaltung MUSS in allen Eingangsnachrichten der Schnittstelle `I_Key_Management_Insurant` analog eines XUA-Akteur "X-Service Provider" die mitgelieferte X-User Assertion (Authentication Assertion) gemäß der Anforderung A_13690 prüfen und die eingehende Nachricht mit Fehlercodes nach [WSS#12] quittieren, falls diese X-User Assertion nicht gültig ist. [<=]

Die Authentication Assertion wird als Teil des SOAP Headers mitgeschickt.

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

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

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

Dabei gelten folgende Anforderungen:

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

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

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

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

[<=]

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

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

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

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

A_20442 - Komponente ePA-Dokumentenverwaltung – Timeout für Zustand KEY_CHANGE_DOKV

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

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

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

A_20447 - Komponente ePA-Dokumentenverwaltung – Rollback für Zustand KEY_CHANGE_DOKV

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

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

[`<=`]

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

5.3.2 Schnittstelle I_Key_Management_Insurant

5.3.2.1 I_Key_Management_Insurant::StartKeyChange()

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

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

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

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

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

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

[<=]

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

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

[<=]

A_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_18004](#) 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_20728 - Komponente ePA-Dokumentenverwaltung - Verwendung des Parameters ContextKey~~

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

~~[<=]~~

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

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

5.3.2.2 I_Key_Management_Insurant::GetAllDocumentKeys()

A_20443 - Komponente ePA-Dokumentenverwaltung - Signatur für I_Key_Management_Insurant::GetAllDocumentKeys()

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

Tabelle 26: Tab_Dokv_39 - Operation I_Key_Management_Insurant::GetAllDocumentKeys()

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

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

[<=]

5.3.2.2.1 Umsetzung

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

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

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

[<=]

A_20425 - Komponente ePA-Dokumentenverwaltung – Rückgabe aller verschlüsselter Dokumentenschlüssel

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

[<=]

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

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

[<=]

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

5.3.2.3 Operation I_Key_Management_Insurant::PutAllDocumentKeys()

A_20436-01A_20436 - Komponente ePA-Dokumentenverwaltung – Signatur für I_Key_Management_Insurant::PutAllDocumentKeys()

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

Tabelle 27: Tab_Dokv_40 -

Operation I_Key_Management_Insurant::PutAllDocumentKeys()

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

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

[<=]

5.3.2.3.1 Umsetzung

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

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

[<=]

A_20448 - Komponente ePA-Dokumentenverwaltung – Hochladen aller verschlüsselter Dokumentenschlüssel

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

[<=]

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

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

[<=]

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

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

[<=]

5.3.2.4 Operation I_Key_Management_Insurant::FinishKeyChange()

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

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

Tabelle 28: Tab_Dokv_41 -

Operation I_Account_Management_Insurant::FinishKeyChange()

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

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

[<=]

5.3.2.4.1 Umsetzung

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

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

[<=]

A_20450 - Komponente ePA-Dokumentenverwaltung – Erfolgreicher Abschluss des Schlüsselwechsels

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

A_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. [<=]

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

5.3.2.5 Protokollierung

A_20470-01 - Komponente ePA-Dokumentenverwaltung - Protokollierungszusatz für Status `KEY_CHANGE_DOKV`

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

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

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

[<=]

A_20473-02 - Komponente ePA-Dokumentenverwaltung - Protokollierungszusatz für Status Rollback im Status KEY_CHANGE_DOKV

~~A_20473-01 - Protokollierungszusatz für Status Rollback im Status KEY_CHANGE_DOKV~~ Die Komponente ePA-Dokumentenverwaltung MUSS im Falle eines Rollbacks gemäß A_20447 der Protokollierung gemäß A_20538 gemSpec_DM_ePA#A_14505 einen Protokolleintrag (Event.code=PHR-860) hinzufügen und dabei den folgenden Parameter hinzufügen:

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

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

[<=]

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

Protokoll-parameter	Parameterwerte gemäß aufgerufener Operation
ObjectDetail	Das Element ParticipantObjectDetail muss zusätzlich mit folgendem Wertepaar (type/value) belegt werden :

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

[<=]

5.4 Zugriffskontrolle

5.4.1 Grob-, mittel- und feingranulare Berechtigungen

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

1. Grobgranulare Berechtigung (Vertraulichkeitsstufen)
Allen Dokumenten wird in der Akte eine von drei Vertraulichkeitsstufen zugeordnet ("Streng vertraulich", "Vertraulich" oder "Normal") und jedem Berechtigten eine von zwei Zugriffsrechten ("Normal" oder "Erweitert"). LEI mit Zugriffsrecht "Normal" dürfen auf die Dokumente in Vertraulichkeitsstufe "Normal" zugreifen, jene mit Zugriffsrecht "Erweitert" zusätzlich auf die mit "Vertraulich" gekennzeichneten Dokumente. Dokumente in der Stufe "Streng vertraulich" sind nur für den Versicherten sichtbar (Ausnahme: "Whitelisting", siehe unten).
2. Mittelgranulare Berechtigung (Kategorien)
Ein Versicherter kann Dokumente aus einen oder mehreren vorgegebenen Dokumentenkategorien (z. B. Arztbriefe) freigeben. Die dadurch getätigte Dokumentenauswahl wird mit dem grobgranularen Zugriffsrecht (siehe 1.) des Berechtigten kombiniert. Das heißt, dass eine auf Arztbriefe berechtigte LEI je nach Zugriffsrecht entweder nur die als "Normal" 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).
3. Feingranulare Berechtigung (White- und Blacklist)
Der Versicherte kann einer LEI den Zugriff auf einzelne Dokumente gewähren ("Whitelisting") oder entziehen ("Blacklisting"). Die Vergabe von feingranularen 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 Berufsgruppenspezifische Einschränkungen

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

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

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

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

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

5.4.3 Grundsätzliche Umsetzung der Berechtigungsregeln

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

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

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

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

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

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

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

5.4.4 Vergabe von Zugriffsregeln

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

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

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

5.4.5 Funktionsprinzip Policy Administration

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

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

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

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

Die Komponente ePA-Dokumentenverwaltung MUSS über die Operationen

`I_Document_Management::CrossGatewayDocumentProvide` sowie

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

Metadaten löschen, bevor ein neues Policy Document gespeichert wird.

[<=]

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

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

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.

[<=]

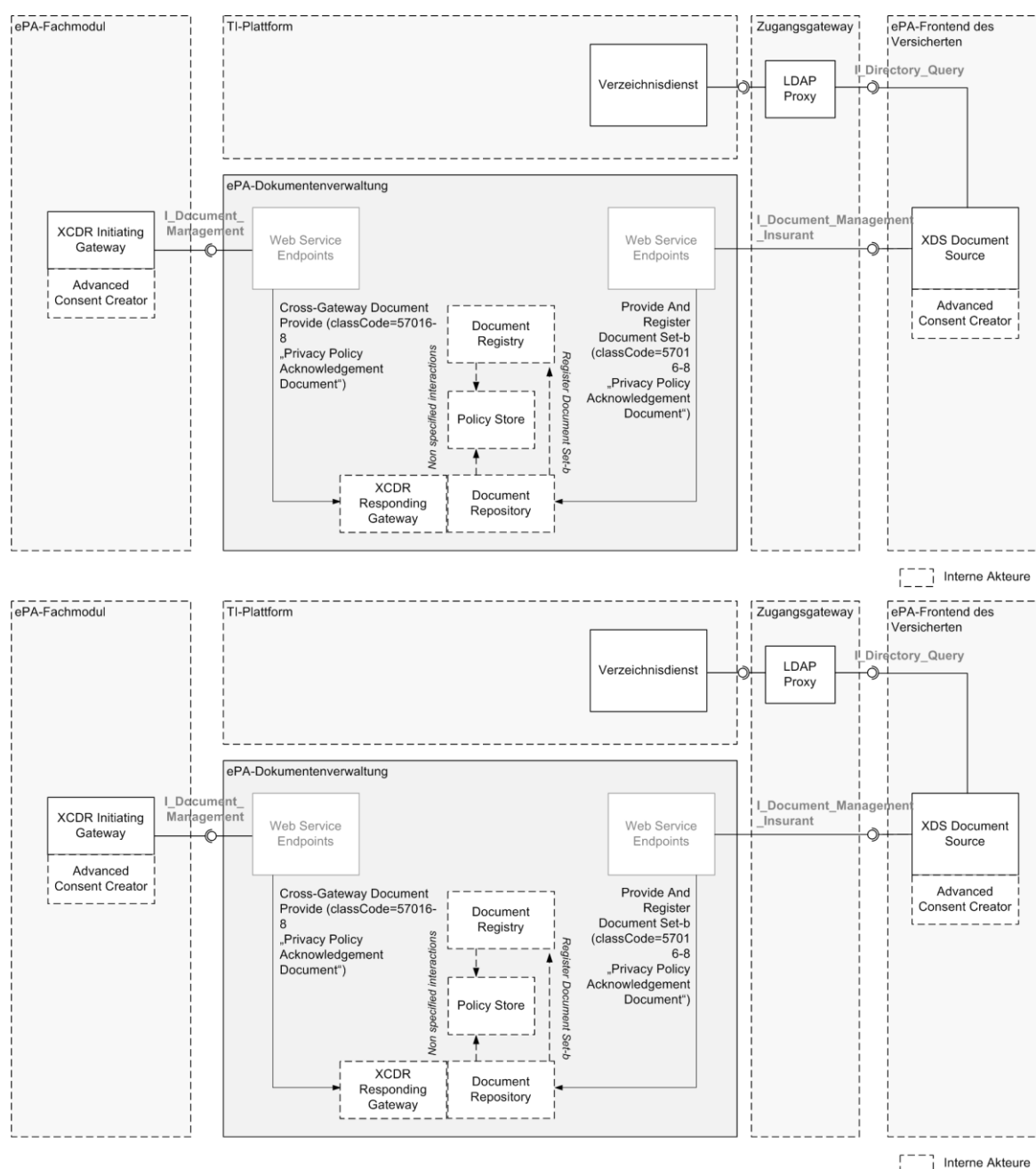


Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen

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

Schnittstelle I_Document_Management zum Einstellen eines Policy Documents 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.

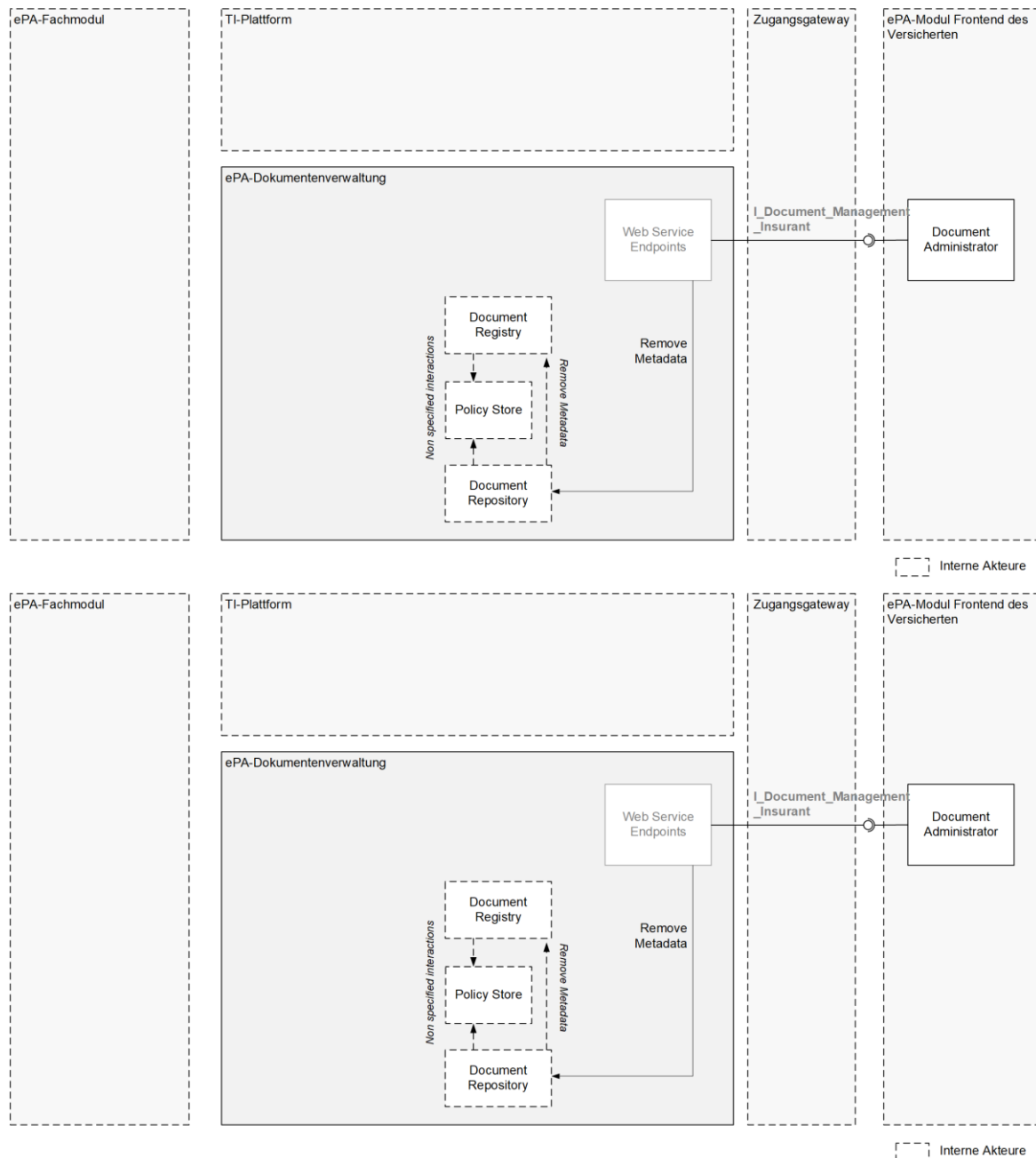


Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen

5.4.6 Anforderungen an die Zugriffskontrollprüfung

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

A_19303-03 - Komponente ePA-Dokumentenverwaltung – Zugriffsunterbindungsregeln

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

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

Tabelle 32: Tab_Dokv_030 - Zugriffsunterbindungsregeln

Dokumentenkategorie gemäß § 341 PDSG Absatz 2		Zugriffsrecht											
Nr.	Technischer Identifier	Arzt	ZArzt	Apo	Psych	Pfleger	Heb	Phy	GD	AM	KT	Ver	
1a1	practitioner	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RØRDM	
1a2	hospital	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RØRDM	
1a3	laboratory	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RØRDM	
1a4	physiotherapy	CR UD	CR UD	R	CR UD	R	R	CR UD	CR UD	R	-	RØRDM	
1a5	psychotherapy	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RØRDM	
1a6	dermatology	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RØRDM	

1a7	gynaecology_urology	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDRDM
1a8	dentistry_oms	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDRDM
1a9	other_medical	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDRDM
1a10	other_non_medical	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDRDM
1b	emp	CR UD	CR UD	CR UD	CR UD	R	R	R	CR UD	R	-	RDRDM
1c	nfd	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDRDM
1d	eab	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDRDM
2	dentalrecord	CR UD	CR UD	-	CR UD	R	-	-	CR UD	R	-	RDRDM
3	childsrecord	CR UD	CR UD	R	CR UD	R	CR UD	R	CR UD	R	-	RDRDM
4	mothersrecord	CR UD	CR UD	R	CR UD	R	CR UD	R	CR UD	R	-	RDRDM
5	vaccination	CR UD	CR UD	CR UD	CR UD	R	R	-	CR UD	CR UD	-	RDRDM
6	patientdoc	RD	RD	R	RD	R	R	R	RD	R	-	CRUDCR UDM
7	ega	RD	RD	R	RD	R	R	R	RD	R	-	CRUDCR UDM
8	receipt	RD	RD	RD	RD	R	R	R	RD	R	CU	RDRDM
10	care	CR UD	CR UD	R	CR UD	CR UD	R	R	CR UD	R	-	RDRDM
11	prescription	CR UD	CR UD	CR UD	CR UD	R	R	R	CR UD	R	-	RDRDM
12	eau	CR UD	CR UD	-	CR UD	-	-	-	CR UD	R	-	RDRDM

13	other	CR UD	CR UD	-	CR UD	-	-	-	CR UD	R	-	RDRDM
----	-------	----------	----------	---	----------	---	---	---	----------	---	---	-------

Legende der Zugriffsrecht CRUD, Zuordnung zur Operation:

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

Legende der Institutionen, Zuordnung zur ProfessionOID:

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

Legende Zugriffsberechtigte, Zuordnung über KVN:

- Ver=Versicherter/Vertreter;

[<=]

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 - Komponente ePA-Dokumentenverwaltung – Generelles schreibendes Zugriffsrecht für LEI

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

[<=]

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

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

Eine Ausnahme ist die generelle Erlaubnis für grundsätzlich berechnete LEI (d.h. solche, für die eine wie auch immer geartete Policy eingestellt wurde), Dokumente in die Akte einzustellen, sofern sie für die gewählte Dokumentenkategorie generell das Zugriffsrecht "C" oder "U" gemäß Tab_Dokv_030 besitzen.

Beispiel: Ein gemäß APPC-Policy-Dokument berechtigter Kostenträger darf nur Dokumente der Kategorie 8 zugreifen, und zwar nach Tabelle ausschließlich mittels CU-Operation (create, update),

d.h. I_Document_Management::CrossGatewayDocumentProvide. Ein Zugriff auf andere Dokumentenkategorien würde durch das APPC-Policy-Dokument verhindert, ein Zugriff durch andere Operationen (bspw. ein Löschen via I_Document_Management::RemoveMetadata) durch Tab_Dokv_030.

Beispiel 2: Ein Leistungserbringer ist nur auf ein einziges Dokument berechtigt (ein Whitelist-Eintrag). Es ist also weder ein grobgranulares noch ein mittelgranulares Zugriffsrecht vergeben worden. Der Leistungserbringer darf damit nur auf dieses eine Dokument lesend ("R") und ggf. löschend ("D") zugreifen, darf aber gemäß A_20736 alle Dokumente einstellen, für deren Kategorie er nach Tab_Dokv_030 die Berechtigung "C" oder "U" besitzt. Letzteres Recht ist ihm auch nicht zu entziehen (außer über den kompletten Entzug der Berechtigung über Löschen der Policy).

Policy Documents, welche die Berechtigung für klassifizierte Nutzer steuern (d.h. für den Versicherten, seine Vertreter, für Leistungserbringerinstitutionen sowie Kostenträger), referenzieren jeweils eine oder mehrere statische, akteninterne XACML 2.0 Policy (Permission Policies). Diese statischen Policies müssen für die Zugriffskontrollprüfung innerhalb des Verarbeitungskontextes verfügbar sein und verlassen die ePA-Dokumentenverwaltung nicht. XACML 2.0 Policies, welche interne Permission Policies referenzieren, heißen im Folgenden Base Policies.

A_19997-01 - Zugriff durch Versicherten auf Schnittstelle

I_Account_Management_Insurant und I_Key_Management_Insurant

Die Komponente ePA-Dokumentenverwaltung MUSS dem Versicherten über A_15173-02 hinaus den Zugriff auf die Operationen der Schnittstellen I_Account_Management_Insurant und I_Key_Management_Insurant erlauben. [\leq]

A_19998-01 - Zugriff durch Vertreter auf Operation

I_Account_Management_Insurant::GetAuditEvents und GetSignedAuditEvents

~~A_19998-01~~ - Zugriff durch Vertreter auf Operation

~~I_Account_Management_Insurant::GetAuditEvents~~ Die Komponente ePA-Dokumentenverwaltung MUSS einem berechtigten Vertreter des Versicherten über A_15173-02 hinaus den Zugriff auf die Operation

~~I_Account_Management_Insurant::GetAuditEvents()~~ und

~~I_Account_Management_Insurant::GetSignedAuditEvents()~~ erlauben.

[\leq]

~~A_14933-01~~A_14933 - Komponente ePA-Dokumentenverwaltung – XML

Schema-Validierung eines Policy Documents

Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Documents (Advanced Patient Privacy Consents) dieses einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen. Ist ein Policy Document nicht wohlgeformt oder gültig, MUSS die Komponente ePA-Dokumentenverwaltung die Nachricht mit einem HTTP-Statuscode 200 oder 400 gemäß [RFC7231] quittieren und einen geeigneten Fehler in der IHE-Antwortnachricht zurückgeben. [\leq]

~~A_15536-02~~A_15536-01 - Komponente ePA-Dokumentenverwaltung –

Prüfungen bei Registrierung eines Policy Documents

Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Documents (Advanced Patient Privacy Consents) folgende inhaltlichen Prüfungen durchführen und im Fehlerfall die Nachricht mit einem HTTP-Statuscode 200 oder 400 gemäß [RFC7231] quittieren und einen geeigneten Fehler in der IHE-Antwortnachricht zurückgeben:

- *Prüfung der XACML 2.0 Policy-Konformität*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn das Profil der vorliegenden XACML 2.0 Policy nicht mit den Anforderungen aus den Abschnitten 5.4.6.2 bis 5.4.6.5 übereinstimmt.
- *Prüfung der Aktenidentität*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn das Resource-Element mit der Attribut-ID "urn:ihe:iti:ser:2016:patient-id" nicht mit der Identität der Akte aus dem internen Policy Document mit der Policy Set ID "urn:gematik:policy-set-id:insurant" übereinstimmt.
- *Prüfung des Einstellers*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML

2.0 Policy abbrechen, wenn die in der Nachricht enthaltene SAML 2.0 Assertion (Authentication Assertion / X-User Assertion) nicht dem Versicherten oder einem seiner Vertreter zugeordnet ist (d.h. das `root`-Attribut des `InstanceIdentifier`-Elements innerhalb des `SubjectMatch`-Elements muss mit der OID "1.2.276.0.76.4.8" eine 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.
- *Verstöße gegen Policy-Struktur und -Inhalte*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn sie Verstöße gegen die Vorgaben aus [gemSpec_DM_ePA#A_14961] verstößt.

[<=]

A_14822-01 - Komponente ePA-Dokumentenverwaltung – Attribute für Anfrage einer Autorisierungsentscheidung

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

- Subject ID oder XSPA Organization ID der Authentication Assertion / X-User Assertion
- unveränderbarer Teil der KVNR aus der Eingangsnachricht oder serverseitig mit Hilfe von Anfrageparametern beschafft (Aktenidentität)
- `wsa:Action`-Element aus der Eingangsnachricht
- ggf. Metadaten des DocumentEntry (u.a. `confidentialityCode`), des dazugehörigen SubmissionSets und etwaiger verbundener Ordner

[<=]

A_20217 - Komponente ePA-Dokumentenverwaltung – APPC Erweiterung für SubmissionSet.authorRole

Die Komponente ePA-Dokumentenverwaltung MUSS das XACML-Attribute "urn:gematik:ig:document-entry:related-submission-set:author-role" wie folgt unterstützen:

XACML Target Section	Resource
XACML Attribute ID	urn:gematik:ig:document-entry:related-submission-set:author-role
XACML Data Type	urn:hl7-org:v3#CV

XACML MatchID	urn:hl7-org:v3:function:CV-equal
XACML Attribute Value Content	Use CX.4.2 as codeSystem and CX.1 as extension
XACML Beispiel	<pre> <Resource> <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal"> <AttributeValue DataType="urn:hl7-org:v3#CV"> <CodedValue code="102" codeSystem="1.3.6.1.4.1.19376.3.276.1.5.13"/> </AttributeValue> <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-entry:related-submission- set:author-role" DataType="urn:hl7-org:v3#CV"/> </ResourceMatch> </Resource> </pre>

[<=]

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

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

5.4.6.1 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 Akstensystem#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.

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. [≤]

5.4.6.3 Berechtigung für einen Vertreter

A_15440-01 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Vertreters

Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten übermittelte XACML 2.0 Policy auf Konformität als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in Tab_Dokv_501 in Anhang C prüfen. [≤]

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 Vertreiberberechtigungen

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.

[<=]

5.4.6.4 Berechtigung für eine Leistungserbringerinstitution**A_15442-02 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung einer Leistungserbringerinstitution**

Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten bzw. vom Fachmodul ePA übermittelte XACML 2.0 Policy auf Konformität als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt von Tab_Dokv_502 in Anhang C prüfen.

[<=]

5.4.6.5 Berechtigung für einen Kostenträger**A_17460-01 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Kostenträgers**

Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten übermittelte XACML 2.0 Policy auf Konformität als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in Tab_Dokv_503 in Anhang C prüfen.[<=]

5.4.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4

Bei einem Upgrade von ePA Release 3.1.3 auf Release 4 ändert sich das Berechtigungssystem. Deshalb müssen zum einen Dokumentenmetadaten (confidentialityCode) und zum anderen die Berechtigungsregeln selbst (APPC Policy-Dokumente) angepasst werden. Davon sind nicht nur neue Dokumente betroffen, sondern es müssen auch bestehende Metadaten und Policies angepasst werden.

Im Ergebnis akzeptiert die ePA-Dokumentenverwaltung in Release 4 alte Policy-Dokumente und Dokumente mit alten confidentialityCodes (beides gemäß (gemäß ePA Release 3.1.3), liefert nach außen jedoch beides nur nach neuen Vorgaben (Release 4) zurück. Dieses Verhalten soll es auch (insbesondere) Primärsystemen nach alter Spezifikation erlauben, mit einem aktuellen Aktensystem zu kommunizieren.

A_20039 - Komponente ePA-Dokumentenverwaltung – Transformation von Policy-Dokumenten hin zu neuerer Version

Die Komponente ePA-Dokumentenverwaltung MUSS sämtliche XACML 2.0 Policies gemäß Anhang B umwandeln in XACML 2.0 Policies gemäß Anhang C, sobald

- eine XACML 2.0 Policy gemäß Anhang B eingestellt wird,
- ein Zugriffsversuch auf eine XACML 2.0 Policy gemäß Anhang B erfolgt.

[<=]

Während die Transformation der Policy-Dokumente stattfindet, und solange sie nicht abgeschlossen ist, werden weitere Zugriffsversuche mit der Fehlermeldung "Aktenkonto vorübergehend nicht erreichbar" abgelehnt.

A_20049-02A_20049-01 - Komponente ePA-Dokumentenverwaltung – Regeln für die Policy-Transformation

Bei der Transformation der XACML 2.0 Policy ohne die Versionsangabe @Version MUSS die vom Client eingestellten Base- und ggf. vorhandene Permission Policies durch eine entsprechende XACML 2.0 Policy mit Versionsangabe @Version ersetzt werden. Bei der Transformation gelten folgende Vorgaben:

- Das Ablaufdatum MUSS übernommen werden.
- Bei LEI, KTR- und Vertreter-Base-Policydokumenten muss der Name der Institution bzw. des Vertreters `aus//PolicySet/Target/Subjects[2]/SubjectMatch/AttributeValue` stattdessen nach `//PolicySet/Description` übernommen werden (das Element `Subjects[2]`) wird durch die `Description` abgelöst).
- Bei der Ersetzung der XACML 2.0 Policies ohne Versionsangabe (alt) durch XACML 2.0 Policies mit Versionsangabe (neu) MÜSSEN folgende Zugriffsregeln umgesetzt werden (Zugriffsrecht alt wird zu Zugriffsrecht neu):
 - alt: LEI, neu: `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 "normal" (grobgranulare Berechtigung) wird vergeben

[<=]

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

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

[<=]

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

A_20050-01 - 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.

5.5 Vertrauenswürdige Ausführung

5.5.1 Schnittstelle I_Document_Management_Connect

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

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

A_15587 - Komponente ePA-Dokumentenverwaltung – Implementierung des sicheren Verbindungsprotokolls

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

[<=]

A_15592-03 - Komponente ePA-Dokumentenverwaltung – Erweiterung des sicheren Verbindungsprotokolls

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

Weiterhin MUSS der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung ein optionales Schlüssel-Wert-Paar zur Übermittlung eines

Sitzungsbezeichners an das Kontextmanagement im HTTP-Request-Header prüfen und akzeptieren. Das Schlüssel-Wert-Paar hat die Form

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

A_14631-02 - Komponente ePA-Dokumentenverwaltung – HTTP-Schnittstelle

I_Document_Management_Connect

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

A_15540 - Komponente ePA-Dokumentenverwaltung – TLS-Schnittstelle

I_Document_Management_Connect

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die Schnittstelle `I_Document_Management_Connect` für TLS-Verbindungen des Fachmoduls 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_14633-02 - 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"`) 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_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 33: Tab_Dokv_29 - Ablauf Operation Hello

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden des HTTP Request mit <code>VAUClientHello</code> -Nachricht)
1	Kontextmanagement	Prüfen der Authorization Assertion der <code>VAUClientHello</code> -Nachricht auf Gültigkeit gemäß Anforderung A_13690 und Abbruch des Verbindungsaufbaus mit HTTP-Fehler 403 (Fehlermeldung "Access Denied") bei ungültiger Authorization Assertion.
2	Kontextmanagement	Extrahieren des Record Identifiers über den Wert des Attributs <code>XSPA Resource ID</code> aus der Authorization Assertion
3	Kontextmanagement	Prüfen, ob ein Verarbeitungskontext für den Record Identifier bereits initialisiert ist und Starten eines Verarbeitungskontextes, falls dies nicht der Fall ist
4	Kontextmanagement	Registrieren der Verbindung zwischen dem Client und dem Verarbeitungskontext für den Record Identifier für die Vermittlung des folgenden Nachrichtenaustauschs
5	Kontextmanagement	Weiterleiten der <code>VAUClientHello</code> -Nachricht an den Verarbeitungskontext für den Record Identifier
6	Verarbeitungskontext	Registrieren der Authorization Assertion der <code>VAUClientHello</code> -Nachricht und Erzeugen der <code>VAUServerHello</code> -Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
7	Verarbeitungskontext	Senden der <code>VAUServerHello</code> -Nachricht
8	Kontextmanagement	Weiterleiten der <code>VAUServerHello</code> -Nachricht an den Client

9	Verarbeitungskontext	Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
	(Client)	(Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6])
	(Client)	(Erzeugen und Senden der VAUClientSigFin-Nachricht)
10	Kontextmanagement	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 KVN- 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 VAUServerFin-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
13	Kontextmanagement	Weiterleiten der VAUServerFin-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_14545-03A_14545-02 - 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::CrossGatewayRetrieveRemoveDocuments
- I_Document_Management::CrossGatewayRetrieve
- I_Document_Management::RestrictedUpdateDocumentSet
- I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::RestrictedUpdateDocumentSet

- `I_Document_Management_Insurant::RegistryStoredQuery`
- `I_Document_Management_Insurant::RemoveMetadata`
- `I_Document_Management_Insurant::RetrieveDocumentSet`
- `I_Account_Management_Insurant::GetAuditEvents`
- `I_Account_Management_Insurant::GetSignedAuditEvents`
- `I_Account_Management_Insurant::SuspendAccount`
- `I_Account_Management_Insurant::ResumeAccount`
- `I_Key_Management_Insurant::StartKeyChange`
- `I_Key_Management_Insurant::GetAllDocumentKeys`
- `I_Key_Management_Insurant::PutAllDocumentKeys`
- `I_Key_Management_Insurant::FinishKeyChange`
- `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. [\leq]

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. [\leq]

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 34: Tab_Dokv_30 - Schnittstelle `I_Document_Management_Connect`

Schnittstelle	<code>I_Document_Management_Connect</code>
Version	1.0.1
Namensraum	<code>http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0</code>

Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Open Context	Übergabe des Kontextschlüssels vom Client an den Verarbeitungskontext der Akte
	Close Context	Beendigung der Client-Verbindung und ggf. Beendigung des Verarbeitungskontextes der Akte
WSDL	DocumentManagementConnectService.wsdl	
XML Schema	DocumentManagementConnectService.xsd	

[<=]

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 35: Tab_Dokv_31 - Operation OpenContext

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

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

[<=]

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 36: Tab_Dokv_32 - Ablauf der Operation Open Context

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden der <code>OpenContextRequest</code> -Nachricht über den sicheren Kanal zwischen Client und Verarbeitungskontext)
1	Kontextmanagement	Weiterleiten der <code>OpenContextRequest</code> -Nachricht an den Verarbeitungskontext gemäß den vorgehaltenen Zuordnungsdaten (siehe Anforderung A_14633)
2	Verarbeitungskontext	Entnahme des im Eingangsparameter <code>ContextKey</code> enthaltenen Kontextschlüssels
3	Verarbeitungskontext	Falls bereits eine Sitzung mit einem Nutzer besteht, Prüfung des neu erhaltenen Kontextschlüssels auf

		Übereinstimmung mit dem aus der bestehenden Sitzung bereits registrierten Kontextschlüssel und Abbruch mit Fehlermeldung INVALID_AUT_KEY bei Nichtübereinstimmung
4	Verarbeitungskontext	<p>Falls nicht bereits eine Sitzung mit einem Nutzer besteht, Laden der benötigten Kontextdaten aus dem Speichersystem, Entschlüsseln mit dem erhaltenen Kontextschlüssel und Abbruch mit Fehlermeldung INVALID_AUT_KEY, falls die Entschlüsselung der Kontextdaten fehlschlägt.</p> <p>Sind keine Kontextdaten mit dem Verarbeitungskontext assoziiert (d.h. erstmaliges Öffnen) MUSS der Kontextschlüssel in der Sitzung verwendet werden, um die neu erzeugten Kontextdaten zu verschlüsseln. In diesem beschriebenen Fall wird die Verarbeitung nicht mit der Fehlermeldung INVALID_AUT_KEY abgebrochen.</p>
5	Verarbeitungskontext	Senden der OpenContextResponse-Nachricht
6	Kontextmanagement	Weiterleiten der OpenContextResponse-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 37: Tab_Dokv_33 - Operation Close Context

Operation	I_Document_Management_Connect::CloseContext
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] in definierte Operation I_Document_Management_Connect::CloseContext technisch um. Mit dieser Operation wird die Verbindung zum Verarbeitungskontext beendet. Der Verarbeitungskontext kann geschlossen werden, falls nicht eine andere Verbindung noch besteht.

Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0/CloseContext		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
-	-	-	-
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
-	-	-	-
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	

[<=]

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 38: Tab_Dokv_34 - Ablauf Operation CloseContext

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden der <code>CloseContextRequest</code> -Nachricht über den sicheren Kanal zwischen Client und Verarbeitungskontext)
1	Kontextmanagement	Weiterleiten der <code>CloseContextRequest</code> -Nachricht an den Verarbeitungskontext gemäß den vorgehaltenen Zuordnungsdaten (siehe Anforderung A_14633)
2	Verarbeitungskontext	Senden der <code>CloseContextResponse</code> -Nachricht

3	Kontextmanagement	Weiterleiten der <code>CloseContextResponse</code> -Nachricht an den Client
4	Verarbeitungskontext	Prüfen, ob mindestens eine weitere Sitzung existiert, ignorieren der <code>CloseContextRequest</code> -Nachricht, falls dies der Fall ist und Abbruch der Operation
5	Verarbeitungskontext	Falls keine weitere Sitzung existiert, persistieren geänderter Kontextdaten und Beenden des Verarbeitungskontextes
6	Kontextmanagement	Löschen der Verbindungszuordnung zwischen Client und Verarbeitungskontext

[<=]

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 - 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()`) 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. [\leq]

A_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`

[\leq]

`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].

6 Informationsmodelle

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

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

Kürzel	Erläuterung
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BPPC	Basic Patient Privacy Consents
HL7	Health Level Seven
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IHE ITI TF	IHE IT Infrastructure Technical Framework
MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
PHR	Personal Health Record

RMU	Restricted Metadata Update Profile
SAML	Security Assertion Markup Language
TLS	Transport Layer Security
UUID	Universally Unique Identifier
VAU	Vertrauenswürdige Ausführungsumgebung
W3C	World Wide Web Consortium
WS-I	Web-Services Interoperability Consortium
XCA	Cross-Community Access Profile
XDR	Cross-Enterprise Document Reliable Interchange Profile
XDS	Cross-Enterprise Document Sharing ProfileGetAllDocumentKeys
XCDR	Cross-Community Document Reliable Interchange Profile
XACML	eXtensible Access Control Markup Language
XDW	Cross-Enterprise Document Workflow Profile
XOP	XML-binary Optimized Packaging
XSPA	Cross-Enterprise Security and Privacy Authorization Profile
XUA	Cross-Enterprise User Assertion Profile

7.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

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

7.3 Abbildungsverzeichnis

Abbildung 1: Komponentenzerlegung ePA-Dokumentenverwaltung	17
Abbildung 2: Zustandsübergänge Schlüsselwechsel	101
Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen	119
Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen	120
Abbildung 1: Komponentenzerlegung ePA-Dokumentenverwaltung	17
Abbildung 2: Zustandsübergänge Schlüsselwechsel	101
Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen	119
Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen	120

7.4 Tabellenverzeichnis

Tabelle 1: Tab_Dokv_10 – Kennzeichnung von Optionalitäten	26
Tabelle 2: Tab_Dokv_11 – Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung	26
Tabelle 3: Tab_Dokv_12 – Fehlercodes zu Fehlern gemäß Operationsdefinition	34
Tabelle 4: Tab_Dokv_35 – Eingangsparameter für TUC_PKI_018	41
Tabelle 5: Tab_Dokv_13 – Parameter des § 291a-Protokolls	44
Tabelle 6: Tab_Dokv_14 – Schnittstelle I_Document_Management	55
Tabelle 7: Tab_Dokv_16 – Operation Cross-Gateway-Query	59
Tabelle 8: Tab_Dokv_17 – Operation RemoveMetadata	64
Tabelle 9: Tab_Dokv_18 – Operation Cross-Gateway-Retrieve	65
Tabelle 10: Tab_Dokv_20 – Schnittstelle I_Document_Management_Insurant	70
Tabelle 11: Tab_Dokv_21 – Operation Provide And Register Document Set-b	71
Tabelle 12: Tab_Dokv_22 – Operation Registry Stored-Query	73
Tabelle 13: Tab_Dokv_23 – Operation RemoveMetadata	77

Tabelle 14: Tab_Dokv_24—Operation Retrieve Document Set	79
Tabelle 15: Tab_Dokv_19—Operation RestrictedUpdateDocumentSet	81
Tabelle 16: Tab_Dokv_36—Schnittstelle I_Document_Management_Insurance	84
Tabelle 17: Tab_Dokv_37—Operation Provide And Register Document Set b	84
Tabelle 18: Tab_Dokv_25—Schnittstelle I_Account_Management_Insurant	87
Tabelle 19: Tab_Dokv_26—Operation Suspend Account	88
Tabelle 20: Tab_Dokv_27—Operation Resume Account	92
Tabelle 21: Tab_Dokv_28—Operation Get Audit Events	95
Tabelle 22: Tab_Dokv_38—Operation I_Key_Management_Insurant::StartKeyChange()	104
Tabelle 23: Tab_Dokv_39— Operation I_Key_Management_Insurant::GetAllDocumentKeys()	107
Tabelle 24: Tab_Dokv_40— Operation I_Key_Management_Insurant::PutAllDocumentKeys()	109
Tabelle 25: Tab_Dokv_41— Operation I_Account_Management_Insurant::FinishKeyChange()	111
Tabelle 26: Tab_Dokv_42—Zusätzliche Parameter des § 291a Protokolls für die Umschlüsselung	114
Tabelle 27: Tab_Dokv_43—Zusätzliche Parameter des § 291a Protokolls für ein Rollback im Rahmen der Umschlüsselung	114
Tabelle 28: Tab_Dokv_030—Zugriffsunterbindungsregeln	121
Tabelle 29: Tab_Dokv_29—Ablauf Operation Hello	133
Tabelle 30: Tab_Dokv_30—Schnittstelle I_Document_Management_Connect	135
Tabelle 31: Tab_Dokv_31—Operation OpenContext	136
Tabelle 32: Tab_Dokv_32—Ablauf der Operation Open Context	137
Tabelle 33: Tab_Dokv_33—Operation Close Context	138
Tabelle 34: Tab_Dokv_34—Ablauf Operation CloseContext	139
Tabelle 35: Tab_Dokv_99—Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	154
Tabelle 36: Tab_Dokv_100—XACML 2.0 Policy für einen Versicherten (Base Policy)	154
Tabelle 37: Tab_Dokv_101—XACML 2.0 Policy mit erlaubten Operationen für einen Versicherten (Permission Policy)	157
Tabelle 38: Tab_Dokv_200—XACML 2.0 Policy für einen Vertreter (Base Policy)	188
Tabelle 39: Tab_Dokv_201—XACML 2.0 Policy mit erlaubten Operationen für einen Vertreter (Permission Policy)	192
Tabelle 40: Tabelle : Tab_Dokv_300-01—XACML 2.0 Policy für eine Leistungserbringerinstitution (Base Policy)	220
Tabelle 41: Tab_Dokv_301—XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer Dokumente (Permission Policy)	225

Tabelle 42: Tab_Dokv_302 – XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-Dokumente (Permission Policy)	251
Tabelle 43: Tab_Dokv_400 – XACML 2.0 Policy für einen Kostenträger (Base Policy) ...	275
Tabelle 44: Tab_Dokv_401 – XACML 2.0 Policy mit erlaubten Operationen für einen Kostenträger (Permission Policy)	278
Tabelle 45: Tab_Dokv_99 – Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	282
Tabelle 46: Tab_Dokv_500 – XACML 2.0 Policy für einen Versicherten	282
Tabelle 47: Tab_Dokv_501 – XACML 2.0 Policy für einen Vertreter	285
Tabelle 48: Tab_Dokv_502 – XACML 2.0 Policy für eine Leistungserbringerinstitution ..	289
Tabelle 49: Tab_Dokv_503 – XACML 2.0 Policy für einen Kostenträger	310
Tabelle 1: Tab_Dokv_10 - Kennzeichnung von Optionalitäten	26
Tabelle 2: Tab_Dokv_11 - Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung	26
Tabelle 3: Tab_Dokv_12 - Fehlercodes zu Fehlern gemäß Operationsdefinition	34
Tabelle 4: Tab_Dokv_35 - Eingangsparameter für TUC_PKI_018	41
Tabelle 5: Tab_Dokv_13 - Parameter des § 291a-Protokolls	44
Tabelle 6: Tab_Dokv_14 - Schnittstelle I_Document_Management	55
Tabelle 7: Tab_Dokv_16 - Operation Cross-Gateway Query	59
Tabelle 8: Tab_Dokv_17 - Operation Remove Documents	62
Tabelle 9: Tab_Dokv_17 - Operation RemoveMetadata	64
Tabelle 10: Tab_Dokv_18 - Operation Cross-Gateway Retrieve	65
Tabelle 11: Tab_Dokv_45 - Operation Restricted Update Document Set	67
Tabelle 12: Tab_Dokv_20 - Schnittstelle I_Document_Management_Insurant	70
Tabelle 13: Tab_Dokv_21 - Operation Provide And Register Document Set-b	71
Tabelle 14: Tab_Dokv_22 - Operation Registry Stored Query	73
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	84
Tabelle 20: Tab_Dokv_25 - Schnittstelle I_Account_Management_Insurant	87
Tabelle 21: Tab_Dokv_26 - Operation Suspend Account	88
Tabelle 22: Tab_Dokv_27 - Operation Resume Account	92
Tabelle 23: Tab_Dokv_28 - Operation Get Audit Events	95
Tabelle 24: Tab_Dokv_44 - Operation Get Signed Audit Events	97
Tabelle 25: Tab_Dokv_38 - Operation I_Key_Management_Insurant::StartKeyChange()	104

Tabelle 26: Tab_Dokv_39 - Operation I_Key_Management_Insurant::GetAllDocumentKeys()	107
Tabelle 27: Tab_Dokv_40 - Operation I_Key_Management_Insurant::PutAllDocumentKeys().....	109
Tabelle 28: Tab_Dokv_41 - Operation I_Account_Management_Insurant::FinishKeyChange()	111
Tabelle 29: Tab_Dokv_42 - Zusätzliche Parameter des § 291a-Protokolls für die Umschlüsselung	114
Tabelle 30: Tab_Dokv_43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung	114
Tabelle 31: Tab_Dokv_43 - Zusätzliche Parameter des § 291a-Protokolls für ein Rollback im Rahmen der Umschlüsselung	114
Tabelle 32: Tab_Dokv_030 - Zugriffsunterbindungsregeln	121
Tabelle 33: Tab_Dokv_29 - Ablauf Operation Hello	133
Tabelle 34: Tab_Dokv_30 - Schnittstelle I_Document_Management_Connect	135
Tabelle 35: Tab_Dokv_31 - Operation OpenContext.....	136
Tabelle 36: Tab_Dokv_32 - Ablauf der Operation Open Context	137
Tabelle 37: Tab_Dokv_33 - Operation Close Context.....	138
Tabelle 38: Tab_Dokv_34 - Ablauf Operation CloseContext.....	139
Tabelle 39: Tab_Dokv_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	154
Tabelle 40: Tab_Dokv_100 - XACML 2.0 Policy für einen Versicherten (Base Policy)	154
Tabelle 41: Tab_Dokv_101 - XACML 2.0 Policy mit erlaubten Operationen für einen Versicherten (Permission Policy)	157
Tabelle 42: Tab_Dokv_200 - XACML 2.0 Policy für einen Vertreter (Base Policy)	188
Tabelle 43: Tab_Dokv_201 - XACML 2.0 Policy mit erlaubten Operationen für einen Vertreter (Permission Policy)	192
Tabelle 44 Tabelle : Tab_Dokv_300-01 - XACML 2.0 Policy für eine Leistungserbringerinstitution (Base Policy)	220
Tabelle 45: Tab_Dokv_301 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente (Permission Policy)	225
Tabelle 46: Tab_Dokv_302 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger- Dokumente (Permission Policy)	251
Tabelle 47: Tab_Dokv_400 - XACML 2.0 Policy für einen Kostenträger (Base Policy) ...	275
Tabelle 48: Tab_Dokv_401 - XACML 2.0 Policy mit erlaubten Operationen für einen Kostenträger (Permission Policy)	278
Tabelle 49: Tab_Dokv_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	282
Tabelle 50: Tab_Dokv_500 - XACML 2.0 Policy für einen Versicherten	282
Tabelle 51: Tab_Dokv_501 - XACML 2.0 Policy für einen Vertreter	285
Tabelle 52: Tab_Dokv_502 - XACML 2.0 Policy für eine Leistungserbringerinstitution ..	289

Tabelle 53: Tab_Dokv_503 - XACML 2.0 Policy für einen Kostenträger	310
--	-----

7.5 Referenzierte Dokumente

7.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemSpec_Aktensystem]	gematik: Spezifikation ePA-Aktensystem
[gemSpec_Authentisierung_Vers]	gematik: Spezifikation Authentisierung des Versicherten ePA
[gemSpec_Autorisierung]	gematik: Spezifikation Autorisierung ePA
[gemSpec_DM_ePA]	gematik: Datenmodell ePA
[gemSpec_FdV_ePA]	gematik: Spezifikation ePA-Frontend des Versicherten
[gemSpec_FM_ePA]	gematik: Spezifikation Fachmodul ePA
[gemSpec_FM_ePA_KTR_Consumer]	gematik: Spezifikation Fachmodul ePA im KTR-Consumer
[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_TBAuth]	gematik: Spezifikation Tokenbasierte Authentisierung

[gemSysL_ePA]

gematik: Systemspezifisches Konzept ePA

7.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-ACWP]	IHE International (2009): IHE IT Infrastructure White Paper Access Control, Revision 1.3, http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf
[IHE-ITI-APPC]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Advanced Patient Privacy Consents (APPC), Revision 1.2 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf
[IHE-ITI-RMD]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.2 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-RMU]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.1 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf
[IHE-ITI-TF1]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Integration Profiles, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
[IHE-ITI-TF2a]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2a (ITI TF-2a) – Transactions Part A, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf

[IHE-ITI-TF2b]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf
[IHE-ITI-TF2x]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2x) – Volume 2 Appendices, Revision 15.1, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf
[IHE-ITI-TF3]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Transaction Specifications and Content Specifications, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf
[IHE-ITI-XCDR]	IHE International (2017): IHE IT Infrastructure (ITI) Technical Framework Supplement, Cross-Community Document Reliable Interchange (XCDR), Revision 1.4 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[OWASP-IP]	Open Web Application Security Project (OWASP) (2017): Input Validation Cheat Sheet, https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet
[OWASP-SAML]	Open Web Application Security Project (OWASP) (2017): SAML Security Cheat Sheet, https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet
[OWASP-WSS]	Open Web Application Security Project (OWASP) (2017): Web Service Security Cheat Sheet, https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet

[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, http://tools.ietf.org/html/rfc2119
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231, https://tools.ietf.org/html/rfc7231
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), https://www.w3.org/TR/soap12-part1/
[WSA]	OASIS (2004): Web Services Addressing (WS-Addressing), https://www.w3.org/Submission/ws-addressing/
[WSIA P]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html
[WSIB P]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[WSIB SP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html
[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
[WSS-SAML]	OASIS (2006): Web Services Security: SAML Token Profile 1.1, https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLSecurityProfile.pdf

	SAMLTokenProfile.pdf
[XACML]	OASIS (2005): eXtensible Access Control Markup Language (XACML) Version 2.0, https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/ http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/

8 Anhang B – XACML 2.0-Profiles für Policy Documents (für Upgrade von ePA 3.1.3)

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

Tabelle 39: Tab_Dokv_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies

Code	Bedeutung
R	Required - Mit "R" gekennzeichnete Element-, Attribut- oder Textknoten MÜSSEN verwendet werden.
O	Optional - Mit "O" gekennzeichnete Element-, Attribut- oder Textknoten KÖNNEN verwendet werden.
X	Mit "X" gekennzeichnete Element-, Attribut- oder Textknoten DÜRFEN NICHT verwendet werden.

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

8.1 Policy Document für einen Versicherten

8.1.1 Base Policy

Tabelle 40: Tab_Dokv_100 - XACML 2.0 Policy für einen Versicherten (Base Policy)

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

		Target	R	Das Element MUSS leer bleiben.
←! Versicherter (repräsentiert durch seine KVNR) →				
		Subjects	R	
		Subject	R	
		SubjectMatch	R	
		@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
		AttributeValue	R	
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		InstanceIdentifier	R	
		@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
		@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
		@extension	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
		SubjectAttributeDesignator	R	
		@AttributeId	R	Der Wert "urn:gematik:subject:subject-id" MUSS gesetzt werden.

				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
<!-- KVN R als Aktenidentifikator -->						
				Resources	R	
				Resource	R	
				ResourceMatch	R	
				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS den unveränderbare Teil der KVN R (10 Stellen) gesetzt werden.
				ResourceAttributeDesignator	R	

				@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				PolicySetIdReference	R	
				text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurant" MUSS gesetzt werden.

8.1.2 Permission Policy

Tabelle 41: Tab_Dokv_101 - XACML 2.0 Policy mit erlaubten Operationen für einen Versicherten (Permission Policy)

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

Policy						R	
	@PolicyId					R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@RuleCombiningAlgId					R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target					R	
	Resources					R	
	Resource					R	
		ResourceMatch				R	
				@MatchId	R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.	
				AttributeValue	R		
					@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
					CodedValue	R	

						@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
						@code	R	Der Wert "PAT" MUSS gesetzt werden.
						@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	O	Der Wert "Dokument eines Versicherten" MUSS gesetzt werden.
					ResourceAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:ihe:iti:appc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
					Actions		R	

<!-- 'CrossGatewayDocumentProvide' -->									
				Action			R		
				ActionMatch			R		
					@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue			R	
						@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.	
						text()	R	Der Wert "urn:ihe:iti:2015: CrossGatewayDocumentPro vide" MUSS gesetzt werden.	
				ActionAttributeDesignator			R		
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.	
						@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.	
<!-- 'ProvideAndRegisterDocumentSet-b' -->									

				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007: ProvideAndRegisterDocum entSet-b" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
				Rule		R	
				@RuleId		R	Es MUSS ein URN- kodierter, global eindeutiger Identifikator

						gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
			@Effect		R	Der Wert "Permit" MUSS gesetzt werden.
			Policy		R	
			@PolicyId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
			@RuleCombiningAlgId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
			Target		R	
			Actions		R	
<!-- Registry Stored Query 'FindDocuments' -->						
			Action		R	
			ActionMatch		R	
			@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.

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

						text()	R	Der Wert "urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindSubmissionSets' -->								
					Action		R	
					ActionMatch		R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue		R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbc1a9" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis tryStoredQuery:

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

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocuments' -->							

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

							function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:5c4f972b- d56b-40ac-a5fc- c8ca9b40b9d4" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis- tryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAssociations' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xac- ml:1.0: function:anyURI-equal" MUSS gesetzt werden.

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

						text()	R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocumentsAndAssociations' -->								
					Action		R	
					ActionMatch		R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue		R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:bab9529a- 4a10-40b3-a01f- f68a615d247a" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis tryStoredQuery:

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

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:51224314-5390-4169-9b91-b1980040715a" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSetAndContents' -->							

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

							function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:e8e3cb2c- e39c-46b9-99e4- c12f57260b83" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regis- tryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetRelatedDocuments' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xac- ml:1.0: function:anyURI-equal" MUSS gesetzt werden.

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

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

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

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

						@Data Type			R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RemoveDocuments -->										
					Action				R	
					ActionMatch				R	
						@MatchId			R	Der Wert "urn:oasis:names:tc:xac ml:1.0: function:anyURI-equal" MUSS gesetzt werden.
						AttributeValue			R	
						@DataType			R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS gesetzt werden.
						text()			R	Der Wert "urn:ihe:iti:2017:Remov eDocuments" MUSS gesetzt werden.
					ActionAttributeDesignator				R	
						@AttributeId			R	Der Wert "urn:oasis:names:tc:xac ml:1.0: action:action-id" MUSS gesetzt werden.
						@DataType			R	Der Wert "http://www.w3.org/2001 /XMLSchema#anyURI" MUSS

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

					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "http://ws.gematik.de/f d/phr/ I_Account_Management_In surant/v1.0/ GetAuditEvents" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action- id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/ XMLSchema#anyURI" MUSS gesetzt werden.
<!-- ResumeAccount -->							
					Action	R	

					ActionMatch	R	
					@MatchId	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/ResumeAccount" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					Rule	R	
					@RuleId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B]

									vergeben werden.
					@Effect			R	Der Wert "Permit" MUSS gesetzt werden.
<!-- SuspendAccount -->									
					Policy			R	
					@PolicyId			R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
					@RuleCombiningAlgId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
					Target			R	
					Resources			R	
					Resource			R	
					ResourceMatch			R	
					@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
					AttributeValue			R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
					text()	R	Der Wert "DISMISSED" MUSS gesetzt werden.
				ResourceAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:gematik:fa:phr:1.0:status:status-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
				Actions		R	
				Action		R	
				ActionMatch		R	
					@MatchId	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

						text()	R	Der Wert "http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/SuspendAccount" MUSS gesetzt werden.
						ActionAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						Rule	R	
						@RuleId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
						@Effect	R	Der Wert "Permit" MUSS gesetzt werden.

8.2 Policy Document für einen Vertreter

8.2.1 Base Policy

Tabelle 42: Tab_Dokv_200 - XACML 2.0 Policy für einen Vertreter (Base Policy)

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

PolicySet			R	
@PolicySetId			R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
@PolicyCombiningAlgId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
Target			R	Das Element MUSS leer bleiben.
<!-- Vertreter (repräsentiert durch seine KVN) -->				
Subjects			R	
Subject			R	
SubjectMatch			R	
@MatchId			R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
AttributeValue			R	
@DataType			R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
InstanceIdentifier			R	
@xmlns			R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.

					@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
					@extension	R	Als Wert MUSS der unveränderbare Teil der KVN (10 Stellen) gesetzt werden.
					SubjectAttributeDesignator	R	
					@AttributeId	R	Der Wert " urn:gematik:subject:subject-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
					@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
					Subject	R	
					SubjectMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:string-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
					text()	R	Der Common Name des X.509 Subject Name der eGK MUSS gesetzt werden, um die Lesbarkeit für den Versicherten im ePA- Frontend des Versicherten zu erhöhen, d.h. wem er ein Zugriffsrecht eingeräumt hat.

				SubjectAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:subject:subject" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVNR als Aktenidentifikator -->						
				Resources	R	
				Resource	R	
				ResourceMatch	R	
				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.

				ResourceAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				PolicySetIdReference	R	
				text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-representative" MUSS gesetzt werden.

8.2.2 Permission Policy

Tabelle 43: Tab_Dokv_201 - XACML 2.0 Policy mit erlaubten Operationen für einen Vertreter (Permission Policy)

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

				Target		R	Das Element MUSS leer bleiben.
				Policy		R	
				@PolicyId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
				@RuleCombiningAlgId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
				Target		R	
				Resources		R	
				Resource		R	
				ResourceMatch		R	
				@MatchId		R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.

						CodedValue	R	
						@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
						@code	R	Der Wert "PAT" MUSS gesetzt werden.
						@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	O	Der Wert "Dokument eines Versicherten" MUSS gesetzt werden.
					ResourceAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
					Actions		R	

<!-- 'CrossGatewayDocumentProvide' -->									
				Action			R		
				ActionMatch			R		
					@MatchId			R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue			R	
						@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.	
						text()	R	Der Wert "urn:ihe:iti:2015: CrossGatewayDocumentPr ovide" MUSS gesetzt werden.	
				ActionAttributeDesignator			R		
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.	
						@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.	
<!-- 'ProvideAndRegisterDocumentSet-b' -->									

				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				Rule		R	
				@RuleId		R	Es MUSS ein URN- kodierter, global eindeutiger Identifikator

						gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
			@Effect		R	Der Wert "Permit" MUSS gesetzt werden.
			Policy		R	
			@PolicyId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
			@RuleCombiningAlgId		R	Der Wert "urn:oasis:names:tc:xcml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
			Target		R	
			Actions		R	
<!-- Registry Stored Query 'FindDocuments' -->						
			Action		R	
			ActionMatch		R	
			@MatchId		R	Der Wert "urn:oasis:names:tc: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:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

						text()	R	Der Wert "urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d" MUSS gesetzt werden.
						ActionAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindSubmissionSets' -->								
						Action	R	
						ActionMatch	R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
						AttributeValue	R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbc1a9" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regi stryStoredQuery:

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

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocuments' -->							

					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Regi stryStoredQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0:

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

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

						text()	R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" MUSS gesetzt werden.
						ActionAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocumentsAndAssociations' -->								
						Action	R	
						ActionMatch	R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
						AttributeValue	R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:RegistryStoredQuery" MUSS

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:bab9529a- 4a10-40b3-a01f- f68a615d247a" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regi stryStoredQuery:

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

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:51224314-5390-4169-9b91-b1980040715a" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSetAndContents' -->							

					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Regi stryStoredQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0:

[illegible]

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

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

							gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:12941a89- e02e-4be5-967c- ce4bfc8fe492" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Regi stryStoredQuery:

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

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

						@DataType			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RemoveDocuments -->										
				Action					R	
				ActionMatch					R	
					@MatchId				R	Der Wert "urn:oasis:names:tc: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:2017:RemoveDocuments" 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.
<!-- RetrieveDocumentSet -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:RetrieveDocumentSet" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- GetAuditEvents -->							

				Action	R	
				ActionMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
				text()	R	Der Wert "http://ws.gematik.de/ fd/phr/ I_Account_Management_I nsurant/v1.0/ GetAuditEvents" MUSS gesetzt werden.
				ActionAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
				@RuleId	R	Es MUSS ein URN- kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus

				[IHE-ITI-TF2x#Appendix B] vergeben werden.
		@Effect	R	Der Wert "Permit" MUSS gesetzt werden.

8.3 Policy Document für eine Leistungserbringerinstitution

8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente

Tabelle 44 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	Das Element MUSS leer bleiben.
<!-- Leistungserbringerinstitution (repräsentiert durch ihre Telematik-ID) -->		
Subjects	R	
Subject	R	
SubjectMatch	R	

				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS die Telematik-ID gesetzt werden.
				SubjectAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:gematik:subject:organization-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Subject	R	
				SubjectMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
				AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
					text()	R	Als Wert MUSS der Name der Leistungserbringerinstitution gesetzt werden.
					SubjectAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xspa:1.0:subject:organization" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVNDR als Aktenidentifikator -->							
					Resources	R	
					Resource	R	
					ResourceMatch	R	
					@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
					InstanceIdentifier	R	
					@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
					@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.

					@extension	R	Als Wert MUSS der unveränderbare Teil der KVN (10 Stellen) gesetzt werden.
					ResourceAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
<!-- Gültigkeitszeitraum des Policy Documents -->							
					Environments	R	
					Environment	R	
					EnvironmentMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:date-less-than-or-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
					text()	R	Der Wert muss dem Tag der Ausstellung (Format YYYY-MM-DD nach ISO 8601:2004) des Policy Documents entsprechen.
					EnvironmentAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.

				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				EnvironmentMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:date-greater-than" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				text()	R	Der Wert muss dem Enddatum (Format YYYY-MM-DD nach ISO 8601:2004) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen: "heute" + frei eintragbare Anzahl Tage in der Spanne von 1 bis 540
				EnvironmentAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				PolicySetIdReference	R	

text()	R	<p>Die Policy Set ID Reference steuert, ob Leistungserbringerinstitutionen Zugriff auf durch Leistungserbringer (permissions-access-group-hcp), Versicherte und Vertreter (permissions-access-group-hcp-insurant-documents) sowie Kostenträger (permissions-access-group-hcp-insurance-documents) eingestellte Dokumente erhalten sollen oder nicht. Das Hinzufügen einer betreffenden Policy Set ID Reference gewährt der Leistungserbringerinstitution Zugriffsrechte.</p> <p>Es muss mindestens ein und maximal drei der folgenden Werte gesetzt werden:</p> <ul style="list-style-type: none"> • "urn:gematik:policy-set-id:permissions-access-group-hcp" • "urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents" • "urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents"
--------	---	---

8.3.2 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente

Tabelle 45: Tab_Dokv_301 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente (Permission Policy)

Element-, Attribut- oder Textknoten gemäß [XACML]	Op t.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-

[illegible]

						CodedValue	R	
						@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
						@code	R	Der Wert "LEI" MUSS gesetzt werden.
						@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	O	Der Wert "Dokument einer Leistungserbringerinstitution" MUSS gesetzt werden.
					ResourceAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Actions			R	
<!-- 'CrossGatewayDocumentProvide' -->								
				Action			R	

					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2015:CrossGatewayDocumentProvide" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					Rule	R	
					@RuleId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
					@Effect	R	Der Wert "Permit" MUSS gesetzt werden.

Policy							R	
	@PolicyId						R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@RuleCombiningAlgId						R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target						R	
	Resources						R	
	Resource						R	
		ResourceMatch					R	
				@MatchId			R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
				AttributeValue			R	
					@DataType		R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
					CodedValue		R	
						@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.

						@code	R	Der Wert "LEI" MUSS gesetzt werden.
						@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	R	Der Wert "Dokument einer Leistungserbringerinstitution" MUSS gesetzt werden.
				ResourceAttributeDesignator			R	
						@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Resource			R	
				ResourceMatch			R	
						@MatchId	R	Der Wert "urn:h17-org:v3:function:CV-equal" MUSS gesetzt werden.
				AttributeValue			R	

						@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
						CodedValue	R	
						@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
						@code	R	Der Wert "LEÄ" MUSS gesetzt werden.
						@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	R	Der Wert "Leistungserbringeräquivalentes Dokument eines Versicherten oder Kostenträgers" MUSS gesetzt werden.
					ResourceAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:h17-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent		Der Wert "true" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocuments' -->								
					Action		R	

					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d" " MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" " MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
<!-- Registry Stored Query 'FindSubmissionSets' -->							
			Action			R	
			ActionMatch			R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" " MUSS gesetzt werden.
			AttributeValue			R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:Cr

							ossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbcla9" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery: queryId" MUSS gesetzt werden.

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAll' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				ActionMatch		R	

					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:10b545ea- 725c-446d-9b95- 8aeb444eddf3" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocuments' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.

					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:5c4f972b-d56b-40ac-a5fc-c8ca9b40b9d4" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAssociations' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" " MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" " MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" " MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocumentsAndAssociations' -->							
				Action		R	
				ActionMatch		R	

					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2

							001/XMLSchema#anyURI " MUSS gesetzt werden.
						text()	R Der Wert "urn:uuid:bab9529a-4a10-40b3-a01f-f68a615d247a" MUSS gesetzt werden.
					ActionAttributeDesignator		R
						@AttributeId	R Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType	R Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSets' -->							
				Action			R
				ActionMatch			R
					@MatchId		R Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue		R
						@DataType	R Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:51224314- 5390-4169-9b91- b1980040715a" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2

							001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSetAndContents' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc: xacml:1.0:action: action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:

							xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:e8e3cb2c- e39c-46b9-99e4- c12f57260b83" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetRelatedDocuments' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:d90e5407-b356-4d91-a89f-873917b4b0e6" MUSS gesetzt werden.
				ActionAttributeDesignator		R	

					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByReferenceId' -->							
				Action		R	
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2

									001/XMLSchema#anyURI " MUSS gesetzt werden.
				ActionMatch				R	
					@MatchId			R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue			R	
						@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
						text()		R	Der Wert "urn:uuid:12941a89- e02e-4be5-967c- ce4bfc8fe492" MUSS gesetzt werden.
				ActionAttributeDesignator				R	
						@AttributeId		R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
						@DataType		R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByTitle' -->									
			Acti on					R	
			Action Match					R	

					@MatchId				R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue				R	
						@Data Type			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.
						@Data Type			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	
						@Data Type			R	Der Wert "http://www.w3.org/2

									001/XMLSchema#anyURI " MUSS gesetzt werden.
						text()		R	Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
					ActionAttribut eDesignator			R	
						@AttributeId		R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RemoveDocuments -->									
					Action			R	
					ActionMatch			R	
						@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue			R	
						@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()		R	Der Wert "urn:ihe:iti:2017:RemoveDocuments" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- CrossGatewayRetrieve -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:Cr ossGatewayRetrieve" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				Rule		R	
				@RuleId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
				@Effect		R	Der Wert "Permit" MUSS gesetzt werden.

8.3.3 Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente

Tabelle 46: Tab_Dokv_302 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-Dokumente (Permission Policy)

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

						documents" MUSS gesetzt werden, sofern dieses Policy Set den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden.
				@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
				Target	R	Das Element MUSS leer bleiben.
				Policy	R	
				@PolicyId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
				@RuleCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
				Target	R	
				Resources	R	
				Resource	R	
				ResourceMatch	R	

					@MatchId	R	Der Wert "urn:hl7-org:v3:function:CV-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
					CodedValue	R	
					@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
					@code	R	<p>Der Wert "KTR" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents").</p> <p>Der Wert "PAT" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents").</p>
					@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.

						@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
						@displayName	O	<p>Der Wert "Dokument eines Kostenträgers" aus MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden</p> <p>(@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents").</p> <p>Der Wert "Dokument eines Versicherten" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden</p> <p>(@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents").</p>
					ResourceAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
						@DataType	R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.

				Actions		R	
<!-- Registry Stored Query 'FindDocuments' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				text()		R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
				@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
				@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:x

							acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:14d4debf- 8f97-4251-9a74- a90016b0af0d" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindSubmissionSets' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue		R	

						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch		R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue		R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:uuid:f26abbcb- ac74-4422-8a30- edb644bbcla9" MUSS gesetzt werden.
					ActionAttributeDesignator		R	

						@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAll' -->								
				Action			R	
				ActionMatch			R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
						AttributeValue	R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator			R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:10b545ea- 725c-446d-9b95- 8aeb444eddf3" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Reg istryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocuments' -->							
					Action	R	
					ActionMatch	R	

					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R Der Wert "urn:uuid:5c4f972b- d56b-40ac-a5fc- c8ca9b40b9d4" MUSS gesetzt werden.
					ActionAttributeDesignator		R
						@AttributeId	R Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
						@DataType	R Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAssociations' -->							
					Action		R
					ActionMatch		R
						@MatchId	R Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue		R
						@DataType	R Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20

								01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetDocumentsAndAssociations' -->								
				Action			R	
				ActionMatch			R	
				@MatchId			R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
				AttributeValue			R	
					@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()		R	Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator			R	
					@AttributeId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
				ActionMatch			R	
				@MatchId			R	Der Wert "urn:oasis:names:tc:x

							acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:bab9529a- 4a10-40b3-a01f- f68a615d247a" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:Reg istryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSets' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	

						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch		R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue		R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:uuid:51224314- 5390-4169-9b91- b1980040715a" MUSS gesetzt werden.
					ActionAttributeDesignator		R	

						@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetSubmissionSetAndContents' -->								
					Action		R	
					ActionMatch		R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue		R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/20

								01/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch		R	
					@MatchId		R	Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue		R	
					@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
					text()		R	Der Wert "urn:uuid:e8e3cb2c- e39c-46b9-99e4- c12f57260b83" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
					@AttributeId		R	Der Wert "urn:ihe:iti:2016:Reg istryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType		R	Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetRelatedDocuments' -->								
					Action		R	
					ActionMatch		R	

					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/20

							01/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R Der Wert "urn:uuid:d90e5407- b356-4d91-a89f- 873917b4b0e6" MUSS gesetzt werden.
					ActionAttributeDesignator		R
						@AttributeId	R Der Wert "urn:ihe:iti:2016: RegistryStoredQuery:q ueryId" MUSS gesetzt werden.
						@DataType	R Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByReferenceId' -->							
					Action		R
					ActionMatch		R
						@MatchId	R Der Wert "urn:oasis:names:tc:x acml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue		R
						@DataType	R Der Wert "http://www.w3.org/20 01/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R Der Wert "urn:ihe:iti:2007:Cro ssGatewayQuery" MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:12941a89-e02e-4be5-967c-ce4bfc8fe492" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/20

									01/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByTitle' -->									
				Action					R
				ActionMatch					R
					@MatchId				R
					AttributeValue				R
						@DataType			R
						text()			R
					ActionAttributeDesignator				R
						@AttributeId			R
						@DataType			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:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
					ActionAttributeDesignator				R	
						@AttributeId			R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- CrossGatewayRetrieve -->										
				Action					R	
				ActionMatch					R	
					@MatchId				R	Der Wert "urn:oasis:names:tc:x

[illegible]

						AttributeValue		R	
						@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()		R	Der Wert "urn:ihe:iti:2017:RemoveDocuments" MUSS gesetzt werden.
						ActionAttributeDesignator		R	
						@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
						@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RestrictedUpdateDocumentSet -->									
					Action			R	
					ActionMatch			R	
						@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue			R	
						@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.

						text()	R	Der Wert "urn:ihe:iti:2018:RestrictedUpdateDocumentSet" MUSS gesetzt werden.
						ActionAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					Rule		R	
					@RuleId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
					@Effect		R	Der Wert "Permit" MUSS gesetzt werden.

8.4 Policy Document für einen Kostenträger

8.4.1 Base Policy

Tabelle 47: Tab_Dokv_400 - XACML 2.0 Policy für einen Kostenträger (Base Policy)

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

@PolicySetId		R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
@PolicyCombiningAlgId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
Target		R	Das Element MUSS leer bleiben.
<!-- Kostenträger (repräsentiert durch ihre Betriebsnummer) Telematik-ID) -->			
	Subjects	R	
	Subject	R	
	SubjectMatch	R	
	@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
	AttributeValue	R	
	@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
	InstanceIdentifier	R	
	@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
	@root	R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
	@extension	R	Als Wert MUSS die Betriebsnummer 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#stri ng" MUSS gesetzt werden.
				text()	R	Als Wert MUSS der Name des Kostenträgers gesetzt werden.
				SubjectAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xspa:1.0: subject:organization" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#stri ng" MUSS gesetzt werden.
<!-- KVNR als Aktenidentifikator -->						
				Resources	R	
				Resource	R	

				ResourceMatch	R	
				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS der unveränderbare Teil der 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 48: 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:hl7-org:v3:function:CV-equal" MUSS gesetzt werden.
	AttributeValue		R	
	@DataType		R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.

							CodedValue	R	
							@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
							@code	R	Der Wert "KTR" MUSS gesetzt werden.
							@codeSystem	R	Der Wert "1.2.276.0.76.5.491 " MUSS gesetzt werden.
							@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
							@displayName	O	Der Wert "Dokument eines Kostenträgers" MUSS gesetzt werden.
							ResourceAttributeDesignator	R	
							@AttributeId	R	Der Wert "urn:ihe:iti:apcc:2016:confidentiality-code" MUSS gesetzt werden.
							@DataType	R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
							@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
							Actions	R	
<!-- 'ProvideAndRegisterDocumentSet-b' -->									
							Action	R	
							ActionMatch	R	
							@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
							AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					Rule	R	
					@RuleId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
					@Effect	R	Der Wert "Permit" MUSS gesetzt werden.

9 Anhang C– XACML 2.0-Profiles für Policy Documents

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

Tabelle 49: Tab_Dokv_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies

Code	Bedeutung
R	Required - Mit "R" gekennzeichnete Element-, Attribut- oder Textknoten MÜSSEN verwendet werden.
O	Optional - Mit "O" gekennzeichnete Element-, Attribut- oder Textknoten KÖNNEN verwendet werden.
X	Mit "X" gekennzeichnete Element-, Attribut- oder Textknoten DÜRFEN NICHT verwendet werden.

Beispiele zu den folgenden XACML 2.0-Profilen können dem beiliegenden Dokumentenpaket entnommen werden.

9.1 Policy Document für einen Versicherten

Tabelle 50: Tab_Dokv_500 - XACML 2.0 Policy für einen Versicherten

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:insurant" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
@Version	R	Der Wert "4.0" MUSS gesetzt werden

Target				R	Das Element MUSS leer bleiben.
<!-- Versicherter (repräsentiert durch seine KVN R) -->					
	Subjects			R	
		Subject		R	
		SubjectMatch		R	
			@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
			AttributeValue	R	
			@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
			InstanceIdentifier	R	
			@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
			@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
			@extension	R	Als Wert MUSS der unveränderbare Teil der KVN R (10 Stellen) gesetzt werden.
		SubjectAttributeDesignator		R	
			@AttributeId	R	Der Wert "urn:gematik:subject:subject-id" MUSS gesetzt werden.

				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
<!-- KVN R als Aktenidentifikator -->						
				Resources	R	
				Resource	R	
				ResourceMatch	R	
				@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS den unveränderbare Teil der KVN R (10 Stellen) gesetzt werden.
				ResourceAttributeDesignator	R	

				@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurant" MUSS gesetzt sein.

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 "urn:gematik:policy-set-id:permissions-access-group-representative:base" MUSS gesetzt werden.
			@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
			@Version	R	Der Wert "4.0.2" 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-

						Frontend des Versicherten zu erhöhen, d.h. wem er ein Zugriffsrecht eingeräumt hat.
	Target			R		Das Element MUSS leer bleiben.
<!-- Vertreter (repräsentiert durch seine KVNR) -->						
	Subjects			R		
	Subject			R		
	SubjectMatch			R		
	@MatchId			R		Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
	AttributeValue			R		
	@DataType			R		Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
	InstanceIdentifier			R		
	@xmlns			R		Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
	@root			R		Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
	@extension			R		Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
	SubjectAttributeDesignator			R		

				@AttributeId	R	Der Wert " urn:gematik:subject:subject-id" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
				@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Subject	R	
				SubjectMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xaeml: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:xaeml:1.0: subject:subject" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string " MUSS gesetzt werden.

<!-- KVN-R als Aktenidentifikator -->				
		Resources	R	
		Resource	R	
		ResourceMatch	R	
		@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
		AttributeValue	R	
		@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
		InstanceIdentifier	R	
		@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
		@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
		@extension	R	Als Wert MUSS der unveränderbare Teil der KVN-R (10 Stellen) gesetzt werden.
		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.
--	--	--	--	--	--	--	-----------	---	---

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]			Opt.	Nutzungsvorgabe
PolicySet			R	
	@PolicySetId		R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:base" MUSS gesetzt werden.
	@PolicyCombiningAlgorithmId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	@Version		R	Der Wert "4.0.2" 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.
	PolicySet								R	
		@PolicySetId							R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:container" MUSS gesetzt werden.
		@PolicyCombiningAlgorithmId							R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
		@Version							R	Der Wert "4.0" MUSS gesetzt werden.
		Target							R	
		<!-- Leistungserbringerinstitution (repräsentiert durch ihre Telematik-ID) -->								
			Subjects						R	
			Subject						R	
				SubjectMatch					R	
					@MatchId				R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.

						AttributeValue		R	
						@DataTyp e		R	Der Wert "urn:h17- org:v3#II" MUSS gesetzt werden.
						InstanceId entifier		R	
							@xml ns	R	Der Wert "urn:h17- org:v3" MUSS gesetzt werden.
							@roo t	R	Der Wert "1.2.276.0.76.4.1 88" MUSS gesetzt werden.
							@ext ensio n	R	Als Wert MUSS die Telematik-ID der zu berechtigenden LEI gesetzt werden.
						SubjectAttribu teDesignator		R	
						@Attribute Id		R	Der Wert " urn:gematik:subj ect:organization- id" MUSS gesetzt werden.
						@DataTyp e		R	Der Wert "urn:h17- org:v3#II" MUSS gesetzt werden.
						@MustBePr esent		R	Der Wert "true" MUSS gesetzt werden.
						Subject		R	
						SubjectMatch		R	
						@MatchId		R	Der Wert " urn:oasis:names:tc:xaeml:1.0:

[illegible]

						InstanceIdentifier		R
							@xmlns	R Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
							@root	R Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
							@extension	R Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
						ResourceAttributeDesignator		R
							@AttributeId	R Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
							@DataType	R Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
	<!-- Gültigkeitszeitraum des Policy Documents -->							
		Environments						R
			Environment					R
				EnvironmentMatch				R
						@MatchId		R Der Wert "urn:oasis:names:tc:xacml:1.0:function:date-less-than-or-equal" MUSS gesetzt werden.
						AttributeValue		R

						@Dat aType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
						text()	R	Der Wert muss dem Tag der Ausstellung (Format YYYY-MM-DD nach ISO 8601:2004 in UTC) des Policy Documents entsprechen.
					EnvironmentAttri buteDesignator		R	
						@Attri buteId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: environment:current- date" MUSS gesetzt werden.
						@Dat aType	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	
						@Dat aType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
						text()	R	Der Wert muss dem Enddatum (Format YYYY- MM-DD nach ISO 8601:2004 in UTC) aus der folgenden Festlegungen ab der

									Ausstellung des Policy Documents entsprechen: <ul style="list-style-type: none"> • "heute" + frei wählbare Anzahl Tage in der Spanne von 1 bis 540 oder • "(maximal heute " + 100 Jahre)
						EnvironmentAttributeDesignator			R
						@AttributeId			R Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.
						@Data Type			R Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
<-- Entweder Der folgende Teil setzt folgende Auswertungsmechanik um: Permit , wenn (Vertrauensstufe AND Kategorie erlaubt AND notBlacklisted) ODER OR Whitelist. Wenn JA, dann Permit , Ansonsten Deny -->									
PolicySet									R
	@PolicySetId								R Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:all-permissions" MUSS gesetzt werden.
	@PolicyCombiningAlgorithmId								R Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides" MUSS gesetzt werden.

	@Version							R	Der Wert "4.0" MUSS gesetzt werden.
	Target							R	Der Wert MUSS leer bleiben.
	<-- Feingranulare Berechtigung: Whitelist -->								
	PolicyIdReference							R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:whitelist" MUSS gesetzt werden.
	<-- Vertrauensstufe AND Kategorie erlaubt AND not Blacklisted -->								
	PolicySet							R	
		@PolicySetId						R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:base:check-wo-whitelist" MUSS gesetzt werden.
		@PolicyCombiningAlgorithmId						R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
		@Version						R	Der Wert "4.0" MUSS gesetzt werden.
		Target						R	Der Wert MUSS leer bleiben.
		PolicyIdReference						R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:levels" MUSS

								gesetzt werden.
		PolicyIdReference						R Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:categories" MUSS gesetzt werden.
		PolicyIdReference						R Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp:blacklist" MUSS gesetzt werden.
	<--Default Policy, die immer Deny zurückgibt -->							
	Policy							R
		@PolicyId						R Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:base:default-deny" MUSS gesetzt werden.
		@RuleCombiningAlgorithmId						R Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
		Target						R Der Wert MUSS leer bleiben.
		Rule						R
			@RuleId					R Der Wert "urn:gematik:rule-id:permissions-access-group-hcp:base:default-deny" MUSS gesetzt werden.

			@Ef fect						R Der Wert "Deny" MUSS gesetzt werden.
<-- Setzen der grobgranularen Berechtigung -->									
Pol ic yS et									R
	@Polic ySetId								R Der Wert "urn:gematik:policy- set-id:permissions- access-group- hcp:levels" MUSS gesetzt werden.
	@Polic yComb iningAl gId								R Der Wert "urn:oasis:names:tc:xa cml:1.0: policy-combining- algorithm:permit- overrides" MUSS gesetzt werden.
	@Versi on								R Der Wert "4.0" MUSS gesetzt werden.
	Target								R Der Wert MUSS leer bleiben.
<-- Grobgranulare Berechtigung "normal" (immer vorhanden) -->									
	PolicyI dRefer ence								R Der Wert "urn:gematik:policy- id:permissions-access- group- hcp:levels:normal" MUSS gesetzt werden.

	<-- Grobgranulare Berechtigung "erweitert" (nur bei Bedarf vorhanden) -->							
	PolicyIdReference							C Das Element MUSS genau dann vorhanden sein, wenn "erweiterte Berechtigung" erteilt werden soll, und dann den Wert <code>"urn:gematik:policy-id:permissions-access-group-hcp:levels:extended"</code> besitzen.
	<-- Default Policy, die immer Deny zurückgibt -->							
	PolicyIdReference							R Der Wert <code>"urn:gematik:policy-id:permissions-access-group-hcp:base:default-deny"</code> MUSS gesetzt sein.
	<-- Setzen der mittelgranularen Berechtigung -->							
	PolicySet							R
	@PolicySetId							R Der Wert <code>"urn:gematik:policy-set-id:permissions-access-group-hcp:categories"</code> MUSS gesetzt werden.
	@PolicyCombiningAlgorithmId							R Der Wert <code>"urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides"</code> MUSS gesetzt werden.

	@Version							R	Der Wert "4.0" MUSS gesetzt werden.
	Target							R	Der Wert MUSS leer bleiben.
	<--Setzen der Berechtigung auf Kategorie "emp" -->								
	PolicyIdReference							C	Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "emp" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:emp" besitzen.
	<--Setzen der Berechtigung auf Kategorie "nfd" -->								
	PolicyIdReference							C	Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "nfd" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:nfd" besitzen.
	<--Setzen der Berechtigung auf Kategorie "eab" -->								
	PolicyIdReference							C	Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "eab" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:eab" besitzen.

	<-- Setzen der Berechtigung auf Kategorie "dentalrecord" -->							
	PolicyIdReference							C Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "dentalrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:dentalrecord" besitzen.
	<-- Setzen der Berechtigung auf Kategorie "childsrecord" -->							
	PolicyIdReference							C Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "childsrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:childsrecord" besitzen.
	<-- Setzen der Berechtigung auf Kategorie "mothersrecord" -->							
	PolicyIdReference							C Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "mothersrecord" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:mothersrecord" besitzen.
	<-- Setzen der Berechtigung auf Kategorie "vaccination" -->							

	PolicyIdReference							C 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-hcp:categories:vaccination" besitzen.
	<-- Setzen der Berechtigung auf Kategorie "patientdoc" -->							
	PolicyIdReference							C Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "patientdoc" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:patientdoc" besitzen.
	<-- Setzen der Berechtigung auf Kategorie "ega" -->							
	PolicyIdReference							C Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "ega" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:ega" besitzen.
	<-- Setzen der Berechtigung auf Kategorie "receipt" -->							
	PolicyIdReference							C Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "receipt" erteilt werden soll, und dann den Wert "urn:gematik:policy-

									id:permissions-access-group-hcp:categories:receipt " besitzen.
	<-- Setzen der Berechtigung auf Kategorie "care" -->								
	PolicyIdReference								C Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "care" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:care" besitzen.
	<-- Setzen der Berechtigung auf Kategorie "prescription" -->								
	PolicyIdReference								C Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "prescription" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:prescription" besitzen.
	<-- Setzen der Berechtigung auf Kategorie "eau" -->								
	PolicyIdReference								C Das Element MUSS nur dann vorhanden sein, wenn die Berechtigung auf Kategorie "eau" erteilt werden soll, und dann den Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:eau" besitzen.

	<-- Setzen der Berechtigung auf Kategorie "other" -->							
	PolicyIdReference							<p>C Das Element MUSS genau dann vorhanden sein, wenn die Berechtigung auf Kategorie "other" erteilt werden soll, und dann den Wert</p> <pre>"urn:gematik:policy-id:permissions-access-group-hcp:categories:other"</pre> <p>besitzen.</p>
	<-- Setzen der Berechtigung für Kategorien practitioner, hospital, laboratory, physiotherapy, psychotherapy, dermatology, gynaecology_urology, dentistry_oms, other_medical und other_non_medical -->							
	PolicyIdReference							<p>C Das Element MUSS genau dann vorhanden sein, wenn auf eine der Kategorien category = {practitioner hospital laboratory physiotherapy psychotherapy dermatology, gynaecology_urology dentistry_oms other_medical other_non_medical} berechtigt werden soll, und dann den Wert</p> <pre>"urn:gematik:policy-id:permissions-access-group-hcp:categories:<category>"</pre> <p>besitzen.</p> <p>Beispiel: Der Wert</p> <pre>"urn:gematik:policy-id:permissions-access-group-hcp:categories:other_medical"</pre> <p>berechtigt auf die Kategorie "other_medical".</p> <p>Das Element wird für jede zu berechtigende</p>

								Kategorie (mit jeweils der Kategorie entsprechenden Wert) wiederholt.
	<-- Default Policy, die immer Deny zurückgibt							
	PolicyIdReference							R Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:base:default-deny" MUSS gesetzt sein.
	<-- Setzen der feingranularen Berechtigung: Blacklist -->							
Policy								R
	@PolicyId							R Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:blacklist" MUSS gesetzt werden.
	@RuleCombiningAlgorithmId							R Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target							R
	Rule							R
		@RuleId						R Der Wert "urn:gematik:rule-id:permissions-access-group-hcp:blacklist" MUSS gesetzt sein.
		@Effect						R Der Wert "Deny" MUSS gesetzt werden.

			Target				R	
				Resources			C	Das Element MUSS genau dann vorhanden sein, wenn mindestens ein Dokument auf die Blacklist gesetzt werden soll.
				Resource			R	Das Element MUSS genau ein mal für jedes Dokument vorhanden sein, dass auf die Blacklist gesetzt werden soll.
							R	
				ResourceMatch			R	
					@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
					Attribute Value		R	Der Wert MUSS dem Wert der <code>DocumentEntry.uniqueId</code> des Dokuments entsprechen, das auf die Blacklist gesetzt werden soll.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
					ResourceAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:resource:resou

									rce-id" MUSS gesetzt werden.
						@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
	<-- Default Rule, das immer Permit zurückgibt -->								
	Rule							R	
		@Rule Id						R	Der Wert "urn:gematik:rule-id:permissions-access-group-hcp:blacklist:default-permit" MUSS gesetzt werden.
		@Effect t						R	Der Wert "Permit" MUSS gesetzt werden.
	<--Setzen der feingranularen Berechtigung: Whitelist -->								
	Policy							R	
	@Policy Id							R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:whitelist" MUSS gesetzt werden.
	@Rule Combining Algorithm Id							R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides" MUSS gesetzt werden.
	Target							R	

	Rule							R	
		@Rule Id						R	Der Wert "urn:gematik:rule- id:permissions-access- group-hcp:whitelist" MUSS gesetzt sein.
		@Effect t						R	Der Wert "Permit" MUSS gesetzt werden.
		Target						R	
			Resources					C	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	
					@MatchI d			R	Der Wert "urn:oasis:names:tc:xa cml:1.0: function:string-equal" MUSS gesetzt werden.
					Attribute Value			R	Der Wert MUSS dem Wert der <code>DocumentEntry.uniqueId</code> des Dokuments entsprechen, das auf die Whitelist gesetzt werden soll. Der Wert DARF NICHT gleichzeitig in <code>//Policy/Rule[@Policy Id=- 'urn:gematik:policy- id:permissions-access- group- hcp:blacklist']/Target</code>

									/Resources/Resource/ResourceMatch/AttributeValue enthalten sein (Dokument ist nie gleichzeitig auf Black- und Whitelist gelistet).
						@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
						ResourceAttributeDesignator		R	
						@Attribute Id		R	Der Wert "urn:oasis:names:tc:xacml:1.0:resource:resource-id" MUSS gesetzt werden.
						@Data Type		R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
	<-- Default Rule, das immer Deny zurückgibt -->								
	Rule							R	
		@Rule Id						R	Der Wert "urn:gematik:rule-id:permissions-access-group-hcp:whitelist:default-deny" MUSS gesetzt werden.
		@Effect						R	Der Wert "Deny" MUSS gesetzt werden.

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]		Opt	Nutzungsvorgabe
PolicySet		R	
@PolicySetId		R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-ktr:base" MUSS gesetzt sein.
@PolicyCombiningAlgId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:permit-overrides" MUSS gesetzt werden.
@Version		R	Der Wert "4.0.2" MUSS gesetzt werden.
Description Target		R	Das Element MUSS leer bleiben. Als Wert MUSS der Name des Kostenträgers gesetzt werden.
Target		R	
<!-- Kostenträger (repräsentiert durch ihre Betriebsnummer)seine Telematik-ID) -->			
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: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 BetriebsnummerTelematik-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:xaaml:1.0+function:string-equal" MUSS gesetzt werden.
						AttributeValue	R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.

						text()	R	Als Wert MUSS der Name der Leistungserbringerinstitution gesetzt werden.
						SubjectAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xspa:1.0:subject:organization" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVN als Aktenidentifikator -->								
					Resources		R	
					Resource		R	
					ResourceMatch		R	
					@MatchId		R	Der Wert "urn: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 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:h17-org:v3#II" MUSS gesetzt werden.
←! Gültigkeitszeitraum des Policy Documents →							
					Environments	R	
					Environment	R	
					EnvironmentMatch	R	
					@MatchId	R	Der Wert " urn:oasis:names:tc:xacml:1.0:function:date-less-than-or-equal " MUSS gesetzt werden.
					AttributeValue	R	
					@Datatype	R	Der Wert " http://www.w3.org/2001/XMLSchema#date " MUSS gesetzt werden.
					text()	R	Der Wert muss dem Tag der Ausstellung (Format YYYY-MM-DD nach ISO-8601:2004 in UTC)
					EnvironmentAttributeDesignator	R	
					@AttributeId	R	Der Wert " urn:oasis:names:tc:xacml:1.0: "

							environment:current-date " MUSS gesetzt werden.
					@DataTy pe	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				EnvironmentMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xaeml:1.0: function:date-greater-than" MUSS gesetzt werden.
				AttributeValue		R	
					@DataTy pe	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
					text()	R	Der Wert muss dem Enddatum (Format YYYY-MM-DD nach ISO 8601:2004 in UTC) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen: <ul style="list-style-type: none"> • "heute" + frei wählbare Anzahl Tage in der Spanne von 1 bis 540 oder • "heute " + 100 Jahre
				EnvironmentAttributeDes ignator		R	
					@Attribut eId	R	Der Wert "urn:oasis:names:tc:xaeml:1.0: environment:current-date" MUSS gesetzt werden.
					@DataTy pe	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.

<!-- Prüfung der Berechtigungskategorien -->		
<-- Setzen der Berechtigung auf Kategorie "receipt" -->		
PolicyIdReference	R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:receipt" MUSS gesetzt werden.
<-- Setzen der Berechtigung auf Kategorie "ega" -->		
PolicyIdReference	R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp:categories:ega" MUSS gesetzt werden.

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>
  </Policy>
```

```

    </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:apcc: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:apcc: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-
hcp: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:apcc: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: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-

```

```

hcp: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-
hcp: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: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: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:apcc:2016:document-entry:format-
code"
urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>

```

DataType="

```

    </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/>
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-hcp:categories:emp"
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:Medikationsplan:r3.1"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.6"/>
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:ihe:iti:apcc: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 -->
  <Rule RuleId="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:apcc: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:apcc: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: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: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:apcc: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:apcc: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:apcc: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:apcc: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"?>
<PolicyPolicyId="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/>
    <RuleRuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:patientdoc" Effect="Permit">
        <Target>
            <Resources>
                <Resource>
                    <ResourceMatchMatchId="urn:hl7-org:v3:function:CV-equal">
                        <AttributeValueDataType="urn:hl7-org:v3#CV">
                            <CodedValuecode="102"
codeSystem="1.3.6.1.4.1.19376.3.276.1.5.13"/>

```

```

        </AttributeValue>
        <ResourceAttributeDesignatorAttributeId="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 -->
<RuleRuleId="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>
<!-- 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:apcc:2016:document-entry:format-code" DataType="urn:hl7-
org:v3#CV"/>
          </ResourceMatch>

```

```

        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:vaccination:default-deny" Effect="Deny"/>
</Policy>

```

9.5.17 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
        <Resource>
          <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-
hcp: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-
hcp: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-
hcp: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-
hcp:categories:physiotherapy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
  <Target/>
  <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:physiotherapy" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="physiotherapy"
codeSystem="TODO"/>
            </AttributeValue>
            <ResourceAttributeDesignator AttributeId="urn:gematik:ig:document-
entry:related-folder:codeList" DataType="urn:hl7-org:v3#CV"/>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <!-- Default Rule: Deny, wenn kein "Permit" oben erreicht werden kann -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:physiotherapy:default-deny" Effect="Deny">
    <Target/>
  </Rule>
</Policy>
```

9.5.21 Mittelgranulare Berechtigung: Kategorie "psychotherapy"

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="urn:gematik:policy-id:permissions-access-group-
hcp:categories:psychotherapy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-
overrides" Version="4.0">
  <Target/>
  <!--Prüfung, ob folder.codeList den Code "practitioner" enthält (TODO: Code System
hier und unten ergänzen) -->
  <Rule RuleId="urn:gematik:rule-id:permissions-access-group-
hcp:categories:psychotherapy" Effect="Permit">
    <Target>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
            <AttributeValue DataType="urn:hl7-org:v3#CV">
              <CodedValue xmlns="urn:hl7-org:v3" code="psychotherapy"
codeSystem="TODO"/>
            </AttributeValue>
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
</Policy>
```

```

        </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>
  <!-- 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>
</Policy>

```

```

        </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>

```