

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation ePA- Dokumentenverwaltung

Version:	1. 51 .152.0
Revision:	485752529994
Stand:	17.08 01.12.2022
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	12.10.20		Einarbeitung der Scope-Themen aus R4.0.1, PDSG-Änderungen	gematik
1.7.0	19.02.21		Einarbeitung Änderungsliste P22.5	gematik
1.8.0	02.06.21		Einarbeitung Änderungsliste ePA_Maintenance_21.1	gematik
1.9.0	09.07.21		Einarbeitung Anpassung IOP-WS (ePA_Maintenance_21.2)	gematik
1.10.0	30.09.21		Einarbeitung Änderungsliste ePA_Maintenance_21.3	gematik
1.11.0	31.01.22		Einarbeitung Änderungsliste ePA_Maintenance_21.4 und ePA_Maintenance_21.5	gematik
1.11.1	10.02.22		Anpassung zu ePA_Maintenance_21.5 (C_10981 - Änderung letzter Satz A_19303-07)	gematik
1.11.2	31.03.22		Einarbeitung Änderungsliste ePA_Maintenance_22.1	gematik
1.50.0	13.04.22		ePA-Stufe 2.5: gemF_ePA_DiGA_Anbindung, gemF_ePA_FDZ_Anbindung	gematik
1.50.1	23.05.22		Rücknahme C_11009 (Änderungsliste ePA_Maintenance_22.1), Korrektur Titel in [gemSpec_ePA_Policy_DiGA]	gematik
1.51.0	25.07.22		Änderungsliste ePA_Maintenance_22.2, redaktionell: diskriminierungsfreie Sprache (Black-/Whitelist in Deny-/Allowlist)	gematik
1.51.1	17.08.22		Anpassung zur Einarbeitung Änderungsliste ePA_Maintenance_22.2 nach weiteren Abstimmungen	gematik

1.52.0	01.12.22		Einarbeitung Änderungsliste ePA_Maintenance_22.3	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	17
4.1 Namensräume	17
4.2 Nutzung von IHE IT Infrastructure Profilen für Speicherung und Abruf von Dokumenten	18
4.2.1 Anforderungen an IHE ITI-Akteure	18
4.2.1.1 APPC Content Consumer	20
4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren	20
4.2.1.1.2 Optionen des IHE ITI-Akteurs	20
4.2.1.2 RMU Update Responder	21
4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren	21
4.2.1.2.2 Optionen des IHE ITI-Akteurs	21
4.2.1.3 XCA Responding Gateway	22
4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren	22
4.2.1.3.2 Optionen des IHE ITI-Akteurs	22
4.2.1.4 XCDR Responding Gateway	22
4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren	22
4.2.1.4.2 Optionen des IHE ITI-Akteurs	23
4.2.1.5 XDS Document Registry	23
4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
4.2.1.5.2 Optionen des IHE ITI-Akteurs	23
4.2.1.6 XDS Document Repository	24
4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren	24
4.2.1.6.2 Optionen des IHE ITI-Akteurs	24
4.2.1.7 XUA X-Service Provider	24
4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren	24
4.2.1.7.2 Optionen des IHE ITI-Akteurs	24
4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen	25
4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen	29

4.2.3.1 Provide X-User Assertion [ITI-40].....	29
4.2.3.2 Provide and Register Document Set-b [ITI-41].....	30
4.2.3.3 Remove Documents [ITI-86].....	31
4.2.3.4 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	38
4.4.4 Parallele Zugriffe.....	39
4.4.5 Konsistenz der Akte, Logging und Monitoring.....	39
4.4.6 Client Verbindungen zum Verarbeitungskontext.....	39
4.5 Anforderungen zur sicherheitstechnischen Validierung.....	41
4.6 Protokollierung.....	43
4.6.1 Protokollierung von Berechtigungen	49
4.7 Liste der freigegebenen Dokumente für Forschungszwecke	52
5 Funktionsmerkmale	53
5.1 Dokumentenverwaltung	53
5.1.1 Schnittstelle I_Document_Management	53
5.1.1.1 Operation I_Document_Management::CrossGatewayDocumentProvide ...	54
5.1.1.1.1 Umsetzung	56
5.1.1.2 Operation I_Document_Management::CrossGatewayQuery	58
5.1.1.2.1 Umsetzung	59
5.1.1.3 Operation I_Document_Management::RemoveDocuments (abgekündigt).....	61
5.1.1.3.1 Umsetzung	63
5.1.1.4 Operation I_Document_Management::RemoveMetadata	63
5.1.1.4.1 Umsetzung	64
5.1.1.5 Operation I_Document_Management::CrossGatewayRetrieve	65
5.1.1.5.1 Umsetzung	66
5.1.1.6 Operation I_Document_Management::RestrictedUpdateDocumentSet (abgekündigt).....	66
5.1.1.6.1 Umsetzung	68
5.1.2 Schnittstelle I_Document_Management_Insurant.....	69
5.1.2.1 Operation I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b.....	70
5.1.2.1.1 Umsetzung	71
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::RemoveDocuments (abgekündigt).....	75
5.1.2.4 Operation I_Document_Management_Insurant::RemoveMetadata.....	77
5.1.2.4.1 Umsetzung	78
5.1.2.5 Operation I_Document_Management_Insurant::RetrieveDocumentSet ...	78
5.1.2.5.1 Umsetzung	80

5.1.2.6 Operation	
<i>I_Document_Management_Insurant::RestrictedUpdateDocumentSet</i>	80
5.1.2.6.1 Umsetzung	82
5.1.3 Schnittstelle <i>I_Document_Management_Insurance</i>	84
5.1.3.1 Operation	
<i>I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b</i>	85
5.1.3.1.1 Umsetzung	86
5.1.4 Anforderungen an Sammlungstypen	87
5.2 Aktenkontoverwaltung	88
5.2.1 Schnittstelle <i>I_Account_Management_Insurant</i>	88
5.2.1.1 Operation <i>I_Account_Management_Insurant::SuspendAccount</i>	89
5.2.1.1.1 Umsetzung	90
5.2.1.2 Operation <i>I_Account_Management_Insurant::ResumeAccount</i>	93
5.2.1.2.1 Umsetzung	94
5.2.1.3 Operation <i>I_Account_Management_Insurant::GetAuditEvents</i>	97
5.2.1.3.1 Umsetzung	99
5.2.1.4 Operation <i>I_Account_Management_Insurant::GetSignedAuditEvents</i>	99
5.2.1.4.1 Umsetzung	101
5.3 Umschlüsselung	101
5.3.1 Übergreifende Anforderungen	102
5.3.2 Schnittstelle <i>I_Key_Management_Insurant</i>	107
5.3.2.1 <i>I_Key_Management_Insurant::StartKeyChange()</i>	107
5.3.2.1.1 Umsetzung	109
5.3.2.2 <i>I_Key_Management_Insurant::GetAllDocumentKeys()</i>	110
5.3.2.2.1 Umsetzung	111
5.3.2.3 Operation <i>I_Key_Management_Insurant::PutAllDocumentKeys()</i>	112
5.3.2.3.1 Umsetzung	113
5.3.2.4 Operation <i>I_Key_Management_Insurant::FinishKeyChange()</i>	114
5.3.2.4.1 Umsetzung	115
5.3.2.5 Protokollierung	116
5.4 Zugriffskontrolle	116
5.4.1 Vergabe von Zugriffsrechten und Policy Administration	118
5.4.2 Anforderungen an die Zugriffskontrollprüfung	127
5.4.2.1 Erstmaliges Öffnen eines Verarbeitungskontextes	128
5.4.2.2 Berechtigung für einen Vertreter	128
5.4.2.3 Berechtigung für eine Leistungserbringerinstitution	129
5.4.2.4 Berechtigung für einen Kostenträger	129
5.4.2.5 Berechtigung für eine DiGA	129
5.4.3 Upgrade von ePA 1 auf ePA 2	130
5.4.4 Simulierte Berechtigung	132
5.5 Vertrauenswürdige Ausführung	132
5.5.1 Schnittstelle <i>I_Document_Management_Connect</i>	132
5.5.1.1 Operation <i>I_Document_Management_Connect::OpenContext</i>	138
5.5.1.1.1 Umsetzung	139
5.5.1.2 Operation <i>I_Document_Management_Connect::CloseContext</i>	140
5.5.1.2.1 Umsetzung	141
5.5.2 Hardware-Merkmale	142

5.6 Statische Akteninhalte	142
6 Informationsmodelle	143
7 Anhang A – Verzeichnisse	144
7.1 Abkürzungen	144
7.2 Glossar	146
7.3 Abbildungsverzeichnis	146
7.4 Tabellenverzeichnis	147
7.5 Referenzierte Dokumente	150
7.5.1 Dokumente der gematik	150
7.5.2 Weitere Dokumente	151
8 Anhang B – XACML 2.0 Profile für Policy Documents (für Upgrade von ePA 3.1.3)	155
8.1 Policy Document für einen Versicherten	155
8.1.1 Base Policy	155
8.1.2 Permission Policy	158
8.2 Policy Document für einen Vertreter	189
8.2.1 Base Policy	189
8.2.2 Permission Policy	193
8.3 Policy Document für eine Leistungserbringerinstitution	221
8.3.1 Base Policy zum Zugriff auf Leistungserbringer Dokumente	221
8.3.2 Permission Policy zum Zugriff auf Leistungserbringer Dokumente	226
8.3.3 Permission Policy zum Zugriff auf Versicherten und Kostenträger Dokumente	250
8.4 Policy Document für einen Kostenträger	272
8.4.1 Base Policy	272
8.4.2 Permission Policy	275
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	17
4.1 Namensräume	17
4.2 Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von Dokumenten	18

4.2.1 Anforderungen an IHE ITI-Akteure	18
4.2.1.1 <i>APPC Content Consumer</i>	20
4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren	20
4.2.1.1.2 Optionen des IHE ITI-Akteurs	20
4.2.1.2 <i>RMU Update Responder</i>	21
4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren	21
4.2.1.2.2 Optionen des IHE ITI-Akteurs	21
4.2.1.3 <i>XCA Responding Gateway</i>	22
4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren	22
4.2.1.3.2 Optionen des IHE ITI-Akteurs	22
4.2.1.4 <i>XCDR Responding Gateway</i>	22
4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren	22
4.2.1.4.2 Optionen des IHE ITI-Akteurs	23
4.2.1.5 <i>XDS Document Registry</i>	23
4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren	23
4.2.1.5.2 Optionen des IHE ITI-Akteurs	23
4.2.1.6 <i>XDS Document Repository</i>	24
4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren	24
4.2.1.6.2 Optionen des IHE ITI-Akteurs	24
4.2.1.7 <i>XUA X-Service Provider</i>	24
4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren	24
4.2.1.7.2 Optionen des IHE ITI-Akteurs	24
4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen	25
4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen	29
4.2.3.1 <i>Provide X-User Assertion [ITI-40]</i>	29
4.2.3.2 <i>Provide and Register Document Set-b [ITI-41]</i>	30
4.2.3.3 <i>Remove Documents [ITI-86]</i>	31
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	38
4.4.4 Parallele Zugriffe	39
4.4.5 Konsistenz der Akte, Logging und Monitoring	39
4.4.6 Client-Verbindungen zum Verarbeitungskontext	39
4.5 Anforderungen zur sicherheitstechnischen Validierung	41
4.6 Protokollierung	43
4.6.1 Protokollierung von Berechtigungen	49
4.7 Liste der freigegebenen Dokumente für Forschungszwecke	52
5 Funktionsmerkmale	53
5.1 Dokumentenverwaltung	53
5.1.1 Schnittstelle I_Document_Management	53

5.1.1.1 Operation <i>I_Document_Management::CrossGatewayDocumentProvide</i> ...	54
5.1.1.1.1 Umsetzung	56
5.1.1.2 Operation <i>I_Document_Management::CrossGatewayQuery</i>	58
5.1.1.2.1 Umsetzung	59
5.1.1.3 Operation <i>I_Document_Management::RemoveDocuments (abgekündigt)</i> ..	61
5.1.1.3.1 Umsetzung	63
5.1.1.4 Operation <i>I_Document_Management::RemoveMetadata</i>	63
5.1.1.4.1 Umsetzung	64
5.1.1.5 Operation <i>I_Document_Management::CrossGatewayRetrieve</i>	65
5.1.1.5.1 Umsetzung	66
5.1.1.6 Operation <i>I_Document_Management::RestrictedUpdateDocumentSet</i> (abgekündigt)	66
5.1.1.6.1 Umsetzung	68
5.1.2 Schnittstelle <i>I_Document_Management_Insurant</i>	69
5.1.2.1 Operation <i>I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b</i>	70
5.1.2.1.1 Umsetzung	71
5.1.2.2 Operation <i>I_Document_Management_Insurant::RegistryStoredQuery</i>	73
5.1.2.2.1 Umsetzung	74
5.1.2.3 Operation <i>I_Document_Management_Insurant::RemoveDocuments</i> (abgekündigt)	75
5.1.2.4 Operation <i>I_Document_Management_Insurant::RemoveMetadata</i>	77
5.1.2.4.1 Umsetzung	78
5.1.2.5 Operation <i>I_Document_Management_Insurant::RetrieveDocumentSet</i> ...	78
5.1.2.5.1 Umsetzung	80
5.1.2.6 Operation <i>I_Document_Management_Insurant::RestrictedUpdateDocumentSet</i>	80
5.1.2.6.1 Umsetzung	82
5.1.3 Schnittstelle <i>I_Document_Management_Insurance</i>	84
5.1.3.1 Operation <i>I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b</i>	85
5.1.3.1.1 Umsetzung	86
5.1.4 Anforderungen an Sammlungstypen	87
5.2 Aktenkontoverwaltung	88
5.2.1 Schnittstelle <i>I_Account_Management_Insurant</i>	88
5.2.1.1 Operation <i>I_Account_Management_Insurant::SuspendAccount</i>	89
5.2.1.1.1 Umsetzung	90
5.2.1.2 Operation <i>I_Account_Management_Insurant::ResumeAccount</i>	93
5.2.1.2.1 Umsetzung	94
5.2.1.3 Operation <i>I_Account_Management_Insurant::GetAuditEvents</i>	97
5.2.1.3.1 Umsetzung	99
5.2.1.4 Operation <i>I_Account_Management_Insurant::GetSignedAuditEvents</i>	99
5.2.1.4.1 Umsetzung	101
5.3 Umschlüsselung	101
5.3.1 Übergreifende Anforderungen	102
5.3.2 Schnittstelle <i>I_Key_Management_Insurant</i>	107

5.3.2.1 <i>I_Key_Management_Insurant::StartKeyChange()</i>	107
5.3.2.1.1 Umsetzung	109
5.3.2.2 <i>I_Key_Management_Insurant::GetAllDocumentKeys()</i>	110
5.3.2.2.1 Umsetzung	111
5.3.2.3 <i>Operation I_Key_Management_Insurant::PutAllDocumentKeys()</i>	112
5.3.2.3.1 Umsetzung	113
5.3.2.4 <i>Operation I_Key_Management_Insurant::FinishKeyChange()</i>	114
5.3.2.4.1 Umsetzung	115
5.3.2.5 <i>Protokollierung</i>	116
5.4 Zugriffskontrolle	116
5.4.1 Vergabe von Zugriffsrechten und Policy Administration	118
5.4.2 Anforderungen an die Zugriffskontrollprüfung	127
5.4.2.1 <i>Erstmaliges Öffnen eines Verarbeitungskontextes</i>	128
5.4.2.2 <i>Berechtigung für einen Vertreter</i>	128
5.4.2.3 <i>Berechtigung für eine Leistungserbringerinstitution</i>	129
5.4.2.4 <i>Berechtigung für einen Kostenträger</i>	129
5.4.2.5 <i>Berechtigung für eine DiGA</i>	129
5.4.3 Upgrade von ePA 1 auf ePA 2	130
5.4.4 Simulierte Berechtigung	132
5.5 Vertrauenswürdige Ausführung	132
5.5.1 Schnittstelle <i>I_Document_Management_Connect</i>	132
5.5.1.1 <i>Operation I_Document_Management_Connect::OpenContext</i>	138
5.5.1.1.1 Umsetzung	139
5.5.1.2 <i>Operation I_Document_Management_Connect::CloseContext</i>	140
5.5.1.2.1 Umsetzung	141
5.5.2 Hardware-Merkmale	142
5.6 Statische Akteninhalte	142
6 Informationsmodelle	143
7 Anhang A – Verzeichnisse	144
7.1 Abkürzungen	144
7.2 Glossar	146
7.3 Abbildungsverzeichnis	146
7.4 Tabellenverzeichnis	147
7.5 Referenzierte Dokumente	150
7.5.1 Dokumente der gematik	150
7.5.2 Weitere Dokumente	151
8 Anhang B – XACML 2.0-Profile für Policy Documents (für Upgrade von ePA 3.1.3)	155
8.1 Policy Document für einen Versicherten	155
8.1.1 Base Policy	155
8.1.2 Permission Policy	158
8.2 Policy Document für einen Vertreter	189
8.2.1 Base Policy	189

8.2.2 Permission Policy	193
8.3 Policy Document für eine Leistungserbringerinstitution	221
8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente	221
8.3.2 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente	226
8.3.3 Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente	250
8.4 Policy Document für einen Kostenträger	272
8.4.1 Base Policy	272
8.4.2 Permission Policy	275

1 Einführung

1.1 Zielsetzung

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

1.2 Zielgruppe

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

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzungen

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

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

1.5 Methodik

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

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

2 Systemkontext

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

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

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

3 Zerlegung der Komponente

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

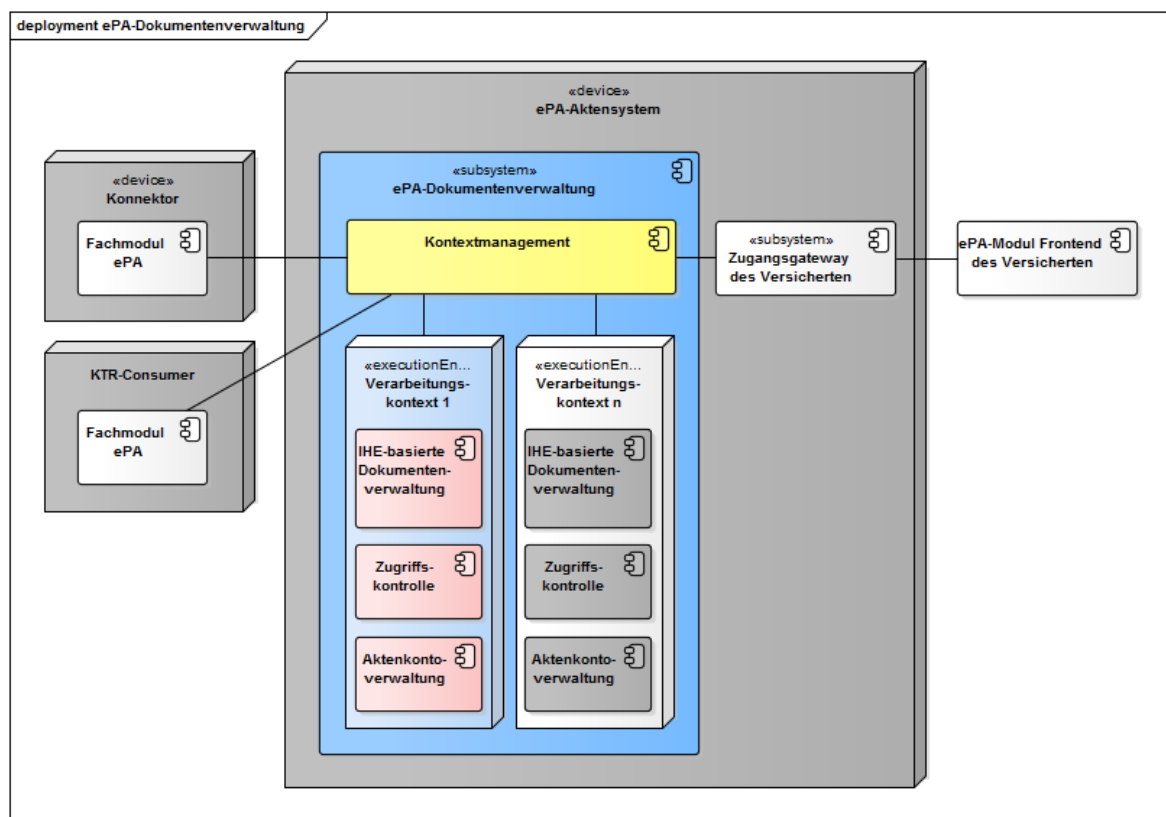


Abbildung 1: Komponentenzersetzung ePA-Dokumentenverwaltung

4 Übergreifende Festlegungen

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

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

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

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

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

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

4.1 Namensräume

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

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

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

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

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

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

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

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

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

4.2.1 Anforderungen an IHE ITI-Akteure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Die Komponente ePA-Dokumentenverwaltung MUSS die Systemzeit über den Zeitdienst in der TI gemäß [gemSpec_Net#6.2] synchronisieren. [≤]

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

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

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

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

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

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

[<=]

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

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

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

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

[<=]

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

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

[<=]

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

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

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

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

[<=]

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

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

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

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

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

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

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

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

4.2.1.2 RMU Update Responder

4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_15093-01 - Komponente ePA-Dokumentenverwaltung – Gruppierung RMU Update Responder mit Document Registry und X-Service Provider

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

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

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

A_15096-02 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder mit "XDS Persistence"-Option

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

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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	X
			XDS Persistence	R
			XDS Version Persistence	X
		APPC Content Consumer	R	
		Document Registry	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 Authentication	X	

		XDS Document Registry	R		
		XDS Document Repository	R		
		XUA X-Service Provider	R		
XCA Responding Gateway	R			On-Demand Documents	X
				Persistence of Retrieved Documents	X
		APPC Content Consumer	R		
		ATNA Secure Node oder Secure Application für Node Authentication	X		
		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_14915-04 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide X-User Assertion

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

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

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

A_14594-01 - Komponente ePA-Dokumentenverwaltung – Validierung der Authentication Assertion

Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" MUSS die X-User Assertion (Authentication Assertion) gemäß der Anforderung A_13690-* prüfen und die eingehende Nachricht mit Fehlercodes nach [WSS#12] sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls diese X-User Assertion nicht gültig ist. [≤]

4.2.3.2 Provide and Register Document Set-b [ITI-41]**A_14549-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Provide and Register Document Set-b**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS für die Ausführung dieser Operation prüfen, ob für den zugreifenden Nutzer ein gültiges Policy Document vorliegt und ob er gemäß der Rollenprüfung in A_19303-* schreibberechtigt ist. Liegt kein Policy Document vor oder ist er nicht schreibberechtigt, MUSS die Nachricht mit dem SOAP-Fault ACCESS_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden.

[≤]

A_15162-05 - 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 andere Association Types nach [IHE-ITI-TF3#4.2.2.2] als die Folgenden enthalten:

- urn:ihe:iti:2007:AssociationType:RPLC (Replace)
- urn:ihe:iti:2007:AssociationType:APND (Append)

[≤]

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_14938-02 - Komponente ePA-Dokumentenverwaltung – 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. [`<=`]

A_21505 - Komponente ePA-Dokumentenverwaltung – Zugriffsrechte DiGA-Hersteller

Die Komponente ePA-Dokumentenverwaltung MUSS alle IHE-ITI-Transaktionen von DiGA-Herstellern ablehnen, die nicht als Einstellen von Dokumenten in `I_Document_Management::CrossGatewayDocumentProvide` gemäß "Cross-Gateway Document Provide" [ITI-80] erfolgen. [`<=`]

A_23123 - Komponente ePA-Dokumentenverwaltung – APND-Assoziation mit existierendem Dokument oder Dokument aus SubmissionSet

Die Komponente ePA-Dokumentenverwaltung MUSS bei APND-Assoziationen sowohl Verknüpfungen auf ein existierendes Dokument im Status "Approved" als auch auf ein Dokument aus dem übergebenen SubmissionSet ermöglichen. [`<=`]

A_23124 - Komponente ePA-Dokumentenverwaltung – Addendum nur mit einem Dokument verknüpfen

Die Komponente ePA-Dokumentenverwaltung DARF ein Addendum NICHT mit mehr als einem Dokument verknüpfen. [`<=`]

A_23125 - Komponente ePA-Dokumentenverwaltung – Kein automatisches "Deprecated" des Addendums

Die Komponente ePA-Dokumentenverwaltung DARF abweichend von [IHE-ITI-TF3#4.2.2.2.3] einem Addendum NICHT den `availabilityStatus` = `Deprecated` zuweisen, wenn das verknüpfte Dokument den `availabilityStatus` `Deprecated` erhält. [`<=`]

4.2.3.3 Remove Documents [ITI-86]

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

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

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

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

A_21245-02 - 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.entryUUID des Dokuments aus der Allowlist aller LEI-Policy-Dokumente löschen, welche die entsprechende DocumentEntry.entryUUID referenzieren. [<=]

4.2.3.4 Remove Metadata [ITI-62]**A_14926-02 - 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 über RPLC assoziierten Dokumente im "Document Repository" löschen. [<=]

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

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

A_21715 - Komponente ePA-Dokumentenverwaltung – Kein Löschen von "replaced"-Dokumenten im Status "Deprecated"

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

A_21714-01 - Komponente ePA-Dokumentenverwaltung – Löschen von strukturierten Dokumenten durch ein ePA-FdV

Die ePA-Dokumentenverwaltung MUSS Löschanfragen eines dynamischen Ordners eines ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente enthalten sind. Das Löschen dieses Ordners impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittiert und der XDSRegistryError-Fehlercode zurückgegeben werden. Werden einzelne strukturierte Dokumente der statischen Ordner vom Typ "vaccination" und "dentalrecord" gelöscht, MUSS die ePA-Dokumentenverwaltung diese Anfrage ebenso mit der o.g. Vorgabe ablehnen. [<=]

A_21817-01 - Komponente ePA-Dokumentenverwaltung – Löschen von strukturierten Dokumenten durch ein Primärsystem

Die ePA-Dokumentenverwaltung MUSS Löschanfragen eines dynamischen Ordners eines Primärsystems ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente enthalten sind. Das Löschen dieses Ordners impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die Nachricht mit XDSRegistryError-Fehlercode zurückgegeben werden. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert "Anfragenachricht darf ausschließlich uniqueID für Folder beinhalten" belegt werden. [<=]

A_14670-04 - 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 `XDSUnreferencedObjectException`-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-ITI-RMD] der Fehlercode `XDSUnreferencedObjectException` zurückgegeben werden. [`<=`]

A_21246-01 - Komponente ePA-Dokumentenverwaltung – Policy-Dokument-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.entryUUID` des Dokuments aus der Allowlist aller LEI-Policy-Dokumente löschen, welche die entsprechende `DocumentEntry.entryUUID` referenzieren. [`<=`]

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

4.3 Fehlerbehandlung in Schnittstellenoperationen

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

A_15664 - Komponente ePA-Dokumentenverwaltung – Fehlername

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

A_15665 - Komponente ePA-Dokumentenverwaltung – Fehlertext

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

A_15666-02 - 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
CERTIFICATE_INVALID	7570
STARTKEYCHANGE_ACTIVE	7580

[<=]

A_22516-01 - Komponente ePA-Dokumentenverwaltung - Alternative Verwendung von XDSRegistryMetadataError anstelle von XDSRepositoryMetadataError

In den Anforderungen A_15162, A_14938, A_15055, A_14941, A_13798, A_15056, A_15082 und A_23098-* KANN alternativ zum Fehler "XDSRepositoryMetadataError" der Fehler "XDSRegistryMetadataError" verwendet werden.[<=]

A_23148 - Komponente ePA-Dokumentenverwaltung – Festlegung zu http-Statuscode bei IHE-Responses

Falls keine anderen Festlegungen in [gemSpec_Dokumentenverwaltung] getroffen wurden, SOLL die Komponente ePA-Dokumentenverwaltung für den Fall, dass eine IHE-Response in der HTTP-Response enthalten ist, den http-Statuscode 200 zurückgeben. Das gilt auch, wenn die IHE-Response einen IHE-Fehler überträgt.[<=]

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_14583-01 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung der Dokumentmetadaten und technischen Daten der VAU

Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS für die Verschlüsselung

- aller Dokumentmetadaten und Policy Documents des Versicherten sowie eigener technischer Daten den Kontextschlüssel des Aktenkontos verwenden,
- des § 291a-Protokolls des Versicherten den Kontextschlüssel des Aktenkontos oder einen aktenkontoindividuellen Protokollschlüssel verwenden.

[<=]

A_22618 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung der Protokolle mit Protokollschlüssel

Falls für die verschlüsselte Persistierung der Protokolle in der Dokumentenverwaltung anstelle des Kontextschlüssels des Aktenkontos ein separater Protokollschlüssel verwendet wird, MUSS die Komponente ePA-Dokumentenverwaltung sicherstellen, dass der Protokollschlüssel

- spezifisch für das Aktenkonto ist (d.h. unterschiedliche Aktenkonten haben unterschiedliche Protokollschlüssel),
- im Klartext ausschließlich innerhalb der VAU verarbeitet wird,
- für die Persistierung mit dem Kontextschlüssel des Aktenkontos verschlüsselt wird (d.h. außerhalb der VAU liegt der Protokollschlüssel ausschließlich mit dem Kontextschlüssel verschlüsselt vor),
- mindestens jährlich gewechselt wird und
- gelöscht wird, wenn keine Protokolle mehr mit dem Protokollschlüssel im Aktenkonto verschlüsselt sind.

Der jährliche Wechsel des Protokollschlüssels und das Löschen der veralteten Protokollschlüssel soll beim ersten Öffnen der Akte (openContext) nach Ablauf der jeweiligen Frist erfolgen.

[<=]

Darüber hinaus sind die folgenden – bereits dem Aktensystem zugeordneten – Anforderungen auch für den Protokollschlüssel zu erfüllen:

- GS-A_4367 Zufallszahlengenerator und
- GS-A_4368 Schlüsselerzeugung.

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 schadhaft auf die Verarbeitungen eines anderen Verarbeitungskontextes einwirken können.[<=]

4.4.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld

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

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

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

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

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

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

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

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

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

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

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

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

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

A_14564-01 - 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),
- TI-Fachdienst-Identität ID.FD.ENC zur Ver- und Entschlüsselung für den Verarbeitungskontext,

- TI-Fachdienst-Identität ID.FD.SIG zur Content-Signatur für den Verarbeitungskontext.

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

[<=]

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

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

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

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

4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes

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

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

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

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

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

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

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

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

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

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

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

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

4.4.4 Parallele Zugriffe

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

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

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

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

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

4.4.5 Konsistenz der Akte, Logging und Monitoring

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

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

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

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

4.4.6 Client-Verbindungen zum Verarbeitungskontext

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

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

A_14616 - Komponente ePA-Dokumentenverwaltung – Kontextmanagement der Vertrauenswürdigen Ausführungsumgebung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[<=]

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

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

4.5 Anforderungen zur sicherheitstechnischen Validierung

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

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

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

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

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

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

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

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

A_13690-03 - 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. Die Verarbeitung der begleitenden Nachricht MUSS abgebrochen werden, falls eine Übereinstimmung nicht festgestellt werden kann. Bei Nichtübereinstimmung einer Authentication Assertion MUSS die Verarbeitung gemäß [WSS#12] sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittiert werden. Bei Nichtübereinstimmung einer Authorization Assertion MUSS die Verarbeitung mit einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittiert werden.

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

Tabelle 4: Tab_Dokv_35 - Eingangsparameter für TUC_PKI_018

Parameter	Belegung
	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. [≤]

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

A_18990 - ePA-Dokumentenverwaltung – Beschränkung gültiger Identitätsbestätigungen

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

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

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

A_17387 - Komponente ePA-Dokumentenverwaltung – Authorization Assertion-Validierung

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

[<=]

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

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

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

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

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

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

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

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

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

4.6 Protokollierung

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

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

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

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

- I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::RestrictedUpdateDocumentSet
- I_Document_Management_Insurant::RegistryStoredQuery
- I_Document_Management_Insurant::RemoveMetadata
- I_Document_Management_Insurant::RetrieveDocumentSet
- I_Account_Management_Insurant::GetAuditEvents
- I_Account_Management_Insurant::GetSignedAuditEvents
- I_Account_Management_Insurant::SuspendAccount
- I_Account_Management_Insurant::ResumeAccount
- I_Key_Management_Insurant::StartKeyChange
- I_Key_Management_Insurant::FinishKeyChange

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

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_20538-02 - Komponente ePA-Dokumentenverwaltung – Parameter des § 291a-Protokolls

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

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

Proto koll- param eter	Parameterwerte gemäß aufgerufener Operation

UserID	<p>Wert des AttributeStatements der 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: //*[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)</p> <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: //*[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)</p>			
UserName	<p>XPath-Ausdruck zur Behauptung "name" (beinhaltet commonName aus dem X.509-Zertifikat), der im Operationsaufruf übergebenen Authentication Assertion: //*[local-name()='Assertion' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion']//*[local-name()='Attribute' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion'][@Name='http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name']/*[local-name()='AttributeValue']</p>			
Object ID	<p>Der unveränderbare Anteil der KVNR des extension-Attributs aus dem InsurantId-Element des RecordIdentifier-Elements oder die DocumentEntry.patientId des entsprechenden Operationsaufrufs</p> <p><i>Hinweis: Bei Aufruf von Operationen ohne diesen Parameter wird der Wert im Protokolleintrag nicht belegt.</i></p>			
Object Detail	<p>Für alle Operationen gilt: Falls die Operation mit einem Fehler ASSERTION_INVALID aufgrund einer ungültigen übergebenen Authentication Assertion abbricht, MUSS ParticipantObjectDetail mit folgenden Wertepaaren (type/value) belegt werden:</p> <table><tr><td>type</td><td>value</td></tr></table>		type	value
type	value			

ErrorInformation	"fehlgeschlagene Authentifizierung des Zugreifenden"
<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> <p>MUSS ParticipantObjectDetail beim Zugriff auf Dokumente mit folgenden Wertepaaren (type/value) belegt werden :</p>	
type	value
DocumentUniqueId	Wert von <code>DocumentEntry.uniqueId</code>
DocumentTitle	Wert von <code>DocumentEntry.title</code>
DocumentPracticeSetting	<p>Wert von <code>DocumentEntry.practiceSettingCode</code>, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3]. (Beispiel: „ALLG^^^&1.3.6.1.4.1.19376.3.276.1.5.4&ISO“, wobei ALLG für den Code und 1.3.6.1.4.1.19376.3.276.1.5.4 für das Code System steht.</p>
DocumentFormat	<p>Wert von <code>DocumentEntry.formatCode</code>, kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3]., siehe oben.</p> <p>Wenn es sich beim Wert von <code>DocumentEntry.formatCode</code> um den Code <code>urn:ihe:iti:xds:2017:mimeTypeSufficient</code> (Code System 1.3.6.1.4.1.19376.1.2.3) handelt, MUSS stattdessen der Wert von <code>DocumentEntry.mimeType</code> hier eingetragen werden.</p> <p>Hinweis: Ein verarbeitendes System muss also, falls der hinterlegte Wert nicht dem Coded String-Format entspricht, den Wert als mimeType gemäß <code>DocumentEntry.mimeType</code> interpretieren.</p>

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

[<=]

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.

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

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

<p>Schemas auf dem <Value>-Element sind dabei für die entsprechende Transformation außer Kraft gesetzt.</p> <ul style="list-style-type: none"> 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. "('H3^1.3.6.1.4.1.19376.3.276.1.5.15')
1. "\$XDSDocumentEntryEventCodeList"	2. "('E100^1.3.6.1.4.1.19376.3.276.1.5.16')"
2. "\$XDSDocumentEntryEventCodeList"	

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

A_20144-01 - Komponente ePA-Dokumentenverwaltung - Aufteilen von Protokolleinträgen für mehrere Dokumente

Bei Operationen, welche die Protokollierung von Details mehrerer Dokumente erfordern, KANN 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_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 Metadatoms als "" protokollieren. [≤]

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

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. Pro eingestelltes oder ersetztes Policy Document (vgl. A_14998) muss ein Protokolleintrag erzeugt werden.

A_20564-04 - Komponente ePA-Dokumentenverwaltung – Protokollierung neuer Berechtigungen

Die Komponente ePA-Dokumentenverwaltung MUSS beim Registrieren von Zugriffen durch ein neu registriertes Policy Document gemäß [gemSpec_DM_ePA#A_14961-*] über die Transaktionen

- CrossGatewayDocumentProvide
- ProvideAndRegisterDocumentSet-b

das Protokoll gemäß A_20538-* um einen weiteren Eintrag mit den folgenden Details ergänzen:

Protokollparameter	Parameterwerte beim Einstellen eines Policy Document	
Object Detail	type	value
	PermAuthorized ID	Wert des XPath-Ausdrucks des Policy Document /PolicySet/Target/Subjects/Subject /SubjectMatch/AttributeValue/InstanceIdentifier/@extension Bei Leistungserbringerinstitutionen sowie

		Kostenträgern ist der Wert eine Telematik-ID, bei Vertretern der unveränderliche Teil der KVNDR.
	PermAuthorized Name	<p>Wert des XPath-Ausdrucks des Policy Document bei Leistungserbringerinstitutionen sowie Kostenträgern <code>substring-before(/PolicySet/Description/text(), ':')</code></p> <p>Wert des XPath-Ausdrucks des Policy Document bei Vertretern <code>/PolicySet/Description/text()</code></p> <p>Bei Leistungserbringerinstitutionen sowie Kostenträgern ist der Wert ein Organisationsname, bei Vertretern ein Name.</p>
	PermCategories	Kommaseparierte Liste von Dokumentenkategorien (technischer Identifier gemäß -*) mitsamt der gewährten Vertraulichkeitsstufe: „normal“ oder „erweitert“ im Format "Kategorie~Vertraulichkeitsstufe" Als Trennzeichen fungiert das Tildezeichen ('~') . Beispiel "care~normal, ega~erweitert"
	PermWhitelist	Explizit freigegebene Dokumente oder Ordner (dokumentenspezifische Berechtigung): kommaseparierte Liste aus <code>DocumentEntry.entryUUID</code> bzw. <code>Folder.entryUUID</code>
	PermBlacklist	Explizit gesperrte Dokumente oder Ordner (dokumentenspezifische Berechtigung): kommaseparierte Liste aus <code>DocumentEntry.entryUUID</code> bzw. <code>Folder.entryUUID</code>

Ein separater Eintrag für das Einstellen des Policy Document DARF NICHT angelegt werden. Das Erfassen von eingestellten Dokumenten in A_20538-* betrachtet keine Policy Documents. [\leq]

A_20566-03 - Komponente ePA-Dokumentenverwaltung – Protokollierung gelöschter Berechtigungen

Die Komponente ePA-Dokumentenverwaltung MUSS beim Löschen von Zugriffen (d.h. Löschen eines Policy Document gemäß [gemSpec_DM_ePA#A_14961-*]) über die Transaktionen

- `I_Document_Management_Insurant::RemoveMetadata`
- `I_Document_Management_Insurant::RemoveDocuments` (abgekündigt)

das Protokoll gemäß A_20538-* um einen weiteren Eintrag mit den folgenden Details ergänzen:

Protokollparameter	Parameterwerte beim Löschen eines Policy Document	
Object Detail	type	value
	PermAuthorizedID	<p>Wert des XPath-Ausdrucks des Policy Document <code>/PolicySet/Target/Subjects/Subject/SubjectMatch/AttributeValue/InstanceIdentifier/@extension</code></p> <p>Bei Leistungserbringerinstitutionen sowie Kostenträgern ist der Wert eine Telematik-ID, bei Vertretern der unveränderliche Teil der KVNR.</p>
	PermAuthorizedName	<p>Wert des XPath-Ausdrucks des Policy Document bei Leistungserbringerinstitutionen sowie Kostenträgern <code>substring-before(/PolicySet/Description/text(),':')</code> Wert des XPath-Ausdrucks des Policy Document bei Vertretern <code>/PolicySet/Description/text()</code> Bei Leistungserbringerinstitutionen sowie Kostenträgern ist der Wert ein Organisationsname, bei Vertretern ein Name.</p>
	PermCategoriesRemoved	<p>Ursprünglich gewährte, kommaseparierte Liste von Dokumentenkategorien (technischer Identifier gemäß A_19303-*) mitsamt der gewährten Vertraulichkeitsstufe: „normal“ oder „erweitert“ im Format "Kategorie~Vertraulichkeitsstufe" Als Trennzeichen fungiert das Tildezeichen ('~') . Beispiel "care~normal, ega~erweitert"</p>
	PermWhiteListRemoved	<p>Ursprünglich explizit freigegebene Dokumente oder Ordner (dokumentenspezifische Berechtigung): kommaseparierte Liste aus DocumentEntry.entryUUID bzw. Folder.entryUUID</p>
	PermBlackListRemoved	<p>Ursprünglich explizit gesperrte Dokumente oder Ordner (dokumentenspezifische Berechtigung): kommaseparierte Liste aus DocumentEntry.entryUUID bzw. Folder.entryUUID</p>

[<=]

4.7 Liste der freigegebenen Dokumente für Forschungszwecke

Der Versicherte muss die Freigabe von Dokumenten für Forschungszwecke jederzeit widerrufen können (auch von bereits aus der Akte gelöschten Dokumenten). Daher müssen die für den Widerruf benötigten Informationen für den Versicherten stets verfügbar sein. Leistungserbringer hingegen sollen dieses Dokument nicht einsehen können.

A_22671 - Komponente ePA-Dokumentenverwaltung: Keine Freigabe der Liste freigegebener Dokumente für Forschungszwecke für Leistungserbringerinstitutionen

Die Dokumentenverwaltung MUSS sicherstellen, dass die Liste der freigegebenen Dokumente (Aufzeichnungsliste) nicht für Leistungserbringerinstitutionen freigegeben werden kann.[<=]

Eine Dokumentenfreigabe/-widerruf kann durch den Versicherten oder einen Vertreter erfolgen. Konkurrierende Vorgänge können potentiell in einer fehlerhaft befüllten Liste freigegebener Dokumente für Forschungszwecke (Aufzeichnungsliste) resultieren. Zur Vermeidung dieser Situation ist daher die exklusive Nutzung der Aufzeichnungsliste durch einen Freigebenden notwendig.

A_22672 - Komponente ePA-Dokumentenverwaltung: Exklusiver Zugriff auf die Liste der freigegebenen Dokumente für Forschungszwecke

Die Dokumentenverwaltung MUSS sicherstellen, dass ein Zugriff eines konkreten ePA-FdV auf die Liste der freigegebenen Dokumente für die Dauer seiner Aktensitzung exklusiv bleibt und die simultane Nutzung der Liste durch weitere ePA-FdV ausgeschlossen ist.[<=]

5 Funktionsmerkmale

5.1 Dokumentenverwaltung

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

5.1.1 Schnittstelle I_Document_Management

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

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

Tabelle 6: Tab_Dokv_14 - Schnittstelle I_Document_Management

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

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

[<=]

5.1.1.1 Operation

I_Document_Management::CrossGatewayDocumentProvide

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.

A_14153-02A_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, einer DiGA, 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_14941-06 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung bei Angabe von Document Entry Relationships in Metadaten

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

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

[<=]

A_21713-02 - Komponente ePA-Dokumentenverwaltung – Kein Einstellen von Ordnern

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

A_13838 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße prüfen

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

[<=]

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

A_13798-01 - Komponente ePA-Dokumentenverwaltung – 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 oder eine nachgelagerte Zugriffskontrollprüfung negativ ausfällt. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht. [`<=`]

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

Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS die Umsetzung der Operation `I_Document_Management::CrossGatewayDocumentProvide` bzw. die Verarbeitung des übermittelten Submission Sets gemäß den definierten Ablauflogiken in [IHE-ITI-XCDR#3.80.4.1.2 und 3.80.4.1.3] und [IHE-ITI-XCDR#3.80.4.2.2 und 3.80.4.2.3] implementieren. [`<=`]

A_13657-02 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Cross-Gateway Document Provide

Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS für die Ausführung dieser Operation prüfen, ob für den zugreifenden Nutzer ein gültiges Policy Document vorliegt und ob er gemäß der Rollenprüfung in A_19303-* schreibberechtigt ist. Liegt kein Policy Document vor oder ist er nicht schreibberechtigt MUSS die Komponente ePA-Dokumentenverwaltung das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-Fehlercode `DocumentAccessNotAuthorized` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die UUID (`DocumentEntry.entryUUID`) des identifizierten Dokuments angegeben werden. [`<=`]

A_21512-01 - Komponente ePA-Dokumentenverwaltung – dynamisches Anlegen von DiGA-Ordern

Falls eine gültige Policy für eine konkrete DiGA vorliegt, MUSS die Komponente ePA-Dokumentenverwaltung beim Einstellen eines Dokumentes in die Akte des Versicherten (`Operation I_Document_Management::CrossGatewayDocumentProvide()`) sicherstellen, dass genau ein Ordner für den Versicherten mit den folgenden Eigenschaften durch die Komponente ePA-Dokumentenverwaltung angelegt ist:

- DiGA-Ordner der Kategorie 9 gemäß `gemSpec_DM_ePA#A_19388` (Belegung `Folder.codeList`) unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in `gemSpec_DM_ePA#14760` (Belegung der restlichen Metadatenfelder).
- `Folder.title` wird mit dem Namen der DiGA `<name>` belegt, welcher in `PolicySet/description` des Policy-Files der DiGA enthalten ist.
- `Folder.comment` wird belegt mit dem Wert `urn:gematik:diga:<telematikID>`.

Eine konkrete DiGA wird identifiziert durch die TelematikID und ist als DiGA durch die `professionOID` gekennzeichnet.

[`<=`]

Mit A_21512-* ist gewährleistet, dass eine berechnete DiGA immer Dokumente einstellen kann, die durch die Komponente Dokumentenverwaltung in dem für diese DiGA vorgesehenen DiGA-Ordner abgelegt werden.

A_22994 - Komponente ePA-Dokumentenverwaltung - automatische Folder-Zuordnung für DiGA

Die Komponente ePA-Dokumentenverwaltung MUSS beim Einstellen eines DiGA-Dokumentes in die Akte des Versicherten (Operation `I_Document_Management::CrossGatewayDocumentProvide()`) sicherstellen, dass das DiGA-Dokument in den durch die TelematikID referenzierten DiGA-Ordner abgelegt wird. Die TelematikID des zu adressierenden Ordners entspricht der im Request enthaltenen Identität des authentifizierten Nutzers. [\leq]

A_23240 - Komponente ePA-Dokumentenverwaltung – Kostenträger akzeptiert

~~A_23043 – Automatische Befüllung leerer Dokumententitel~~ Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" KANN als Eingangsparameter X-User Assertion auch einen authentisierten Kostenträger akzeptieren. MUSS ~~documentEntry.title mit dem auf den reinen Dateinamen reduzierten Wert von documentEntry.URI (d.h. ohne Pfadangaben) befüllen, falls ein Client ein Dokument einstellt, ohne documentEntry.title befüllt zu haben.~~ [\leq]

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 <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 "Cross-Gateway Document Query" [ITI-38] und "Provide X-User Assertion" [ITI-40] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5.1.1.2.1 Umsetzung

A_14924-01 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe von Metadaten zu Policy Documents (Advanced Patient Privacy Consents) und damit verbundenen Associations/SubmissionSets

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" DARF Metadaten zu Policy Documents (Advanced Patient Privacy Consents) gemäß der Anforderung [gemSpec_DM_ePA#A_14961-*] und den damit verbundenen Associations und SubmissionSets NICHT zurückgeben bzw. MUSS diese aus der Antwortnachricht entfernen, falls diese den Anfragekriterien entsprechen. [<=]

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

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

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

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

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

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

A_20532-01 - 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` unterbinden, wenn der Zugreifende nicht mindestens für ein Dokument darin berechtigt ist. [≤]

A_20533-01 - 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` unterbinden, wenn der Zugreifende nicht für mindestens ein Dokument darin oder aber den Folder selbst berechtigt ist. [≤]

A_20534-02 - 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` unterbinden, wenn der Zugreifende nicht für beide Endpunkte der Association (DocumentEntries, SubmissionSets, Folder) berechtigt ist. [≤]

A_20535-01 - 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 sich verhalten, als wäre das Objekt 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_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	I_Document_Management::RemoveDocuments		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management::deleteDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove Documents" [ITI-86] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente eines Aktenkontos im ePA-Aktensystem zu löschen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2017:RemoveDocuments		
Eingangsparameter			
Name	Beschreibung	Typ	optional
Remove Documents Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocuments_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	rmd:RemoveDocumentsResponse_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 "RemoveDocuments" [ITI-86] und "Provide X-User Assertion" [ITI-40] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

5.1.1.3.1 Umsetzung

A_21184 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Documents

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

5.1.1.4 Operation `I_Document_Management::RemoveMetadata`

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

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

Tabelle 9: Tab_Dokv_17 - Operation RemoveMetadata

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	opt.
Remove Documents Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	xds>DeleteDocumentSet_Message	n

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

[<=]

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

5.1.1.4.1 Umsetzung

A_14908-02 - 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#3.62.4.1.2 und 3.62.4.1.3] implementieren.[<=]

A_21710-01 - Komponente ePA-Dokumentenverwaltung – Kein Löschen von statischen Ordnern und Associations durch die LEI

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

5.1.1.5 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	I_Document_Management::CrossGatewayRetrieve		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management::getDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Cross-Gateway Retrieve" [ITI-39] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente aus dem ePA-Aktensystem abzufragen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:CrossGatewayRetrieve		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Cross-Gateway Retrieve Message	Eingangsnachricht zum Abruf von Dokumenten	xdsb:RetrieveDocumentSetRequest	n
X-User Assertion	Authentication Assertion der authentifizierten 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			
Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.			
Name	Fehlertext	Details	

MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße der angefragten Dokumente übersteigt 250 MByte.
--------------------	--	---

[<=]

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

5.1.1.5.1 Umsetzung

A_14911 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-Gateway Retrieve

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

A_16201 - Komponente ePA-Dokumentenverwaltung – Prüfung der zurückgegebenen Paketgröße

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

[<=]

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.[<=]

5.1.1.6 Operation

I_Document_Management::RestrictedUpdateDocumentSet (abgekündigt)

Die Operation `I_Document_Management::RestrictedUpdateDocumentSet` wird aus Kompatibilitätsgründen weiterhin angeboten. Ziel ist es, diese Operation in späteren Releases nicht mehr zu unterstützen. Die Operation liefert bei jedem Aufruf einen

wohldefinierten Fehler zurück, da die früher (ePA bis Release 3.1.3) ausgelöste Funktionalität nicht mehr durch ePA ab Release 4 unterstützt wird.

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

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

I_Document_Management::RestrictedUpdateDocument Set gemäß der folgenden Signatur implementieren:

Tabelle 11: Tab_Dokv_45 - Operation Restricted Update Document Set

Operation	I_Document_Management::RestrictedUpdateDocumentSet		
Beschreibung	<p>Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_PHR_Management::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>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_14478-01 - 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 (abgekündigt)	Löschen ein oder mehrerer Dokumente
	Remove Metadata	Löschen ein oder mehrerer Dokumente oder Folder
	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
-------------------	---

[<=]

5.1.2.1 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	optional
Provide And Register Document Set-b Message	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	no

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

[<=]

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_16442-01 - 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] sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109-*, A_15631] entspricht.[<=]

A_21481-04 - Komponente ePA-Dokumentenverwaltung – Kein Einstellen von Ordnern und Associations

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS das Registrieren und Speichern von Metadaten und Dokument(en) über die Schnittstelle `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b()` ablehnen und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder oder andere als die folgenden Associationen

- SS-DE
- SS-HM
- FD-DE
- RPLC
- APND

enthalten sind.[<=]

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

A_22400 - Komponente ePA-Dokumentenverwaltung - Ablehnung Upload bei abweichenden confidentialityCode

Uploads, die als Resultat einen uneinheitlichen `documentEntry.confidentialityCode` in einer RPLC-Kette oder einer mixed- oder uniform-Sammlung hätten, MÜSSEN mit `XDSRegistryMetadataError` abgelehnt werden.[<=]

A_23144 - Komponente ePA-Dokumentenverwaltung: Automatische Ablage von Dokumenten im Ordner "technical"

Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass Dokumente mit einem `formatCode` mit der `codeSystem` OID "2.25.154081344090540725127779452347992051720", unabhängig von weiteren Metadaten, im statischen Ordner "technical" abgelegt werden.[<=]

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_16436-02 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109-*, A_15631] entspricht.

[<=]

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_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. [<=]

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.

5.1.2.3 Operation

I_Document_Management_Insurant::RemoveDocuments (abgekündigt)

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

A_21818 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove Documents

Die Komponente ePA-Dokumentenverwaltung KANN die Operation I_Document_Management_Insurant::RemoveDocuments gemäß der folgenden Signatur implementieren:

Tabelle 15: Tab_Dokv_23 - Operation RemoveDocuments

Operation	I_Document_Management_Insurant::RemoveDocuments		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurant::deleteDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Remove Documents" [ITI-86] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente im ePA-Aktensystem zu löschen.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2017:RemoveDocuments		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Remove Documents Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocuments_Message	n
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109-*, A_15631]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Remove Documents Response Message	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	rmd:RemoveDocumentsResponse_Message	n
Technische Fehlermeldungen			
Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.			
Name	Fehlertext	Details	

[<=]

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

5.1.2.4 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 16: Tab_Dokv_23 - Operation RemoveMetadata

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

5.1.2.4.1 Umsetzung**A_14909-03 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Metadata**

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS die Umsetzung der Operation `I_Document_Management_Insurant::RemoveMetadata` gemäß der definierten Ablauflogik in [IHE-ITI-RMD#3.62.4.1.2 und 3.62.4.1.3] implementieren.[<=]

A_16437-03 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109-*, A_15631] entspricht.

[<=]

A_21696-01 - Komponente ePA-Dokumentenverwaltung – Kein Löschen von statischen Ordnern und Associations durch FdV

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

5.1.2.5 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 17: 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			
Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.			
Name	Fehlertext	Details	
MaxPkgSizeExceeded	Die max. Paketgröße	Die Gesamtgröße der angefragten Dokumente übersteigt 250 MByte.	

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

[<=]

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

5.1.2.5.1 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_16443-01 - 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] sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109-*, A_15631] entspricht.[<=]

A_16200 - Komponente ePA-Dokumentenverwaltung – Prüfung der zurückgegebenen Paketgröße

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

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

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

[<=]

5.1.2.6 Operation

I_Document_Management_Insurant::RestrictedUpdateDocumentSet

A_15057-03 - 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 18: 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 zulässig. Deshalb darf von den übermittelten Metadaten nur der geänderte documentEntry.confidentialityCode im Aktensystem gespeichert werden. Beim Aufruf der Operation muss von den Metadaten im Request nur die EntryUUID sowie die Berechtigung geprüft werden.</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 des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109-*, A_15631]	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] bzw. [IHE-ITI-RMU#4.2.4], und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			

[<=]

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

5.1.2.6.1 Umsetzung

A_15082 - Komponente ePA-Dokumentenverwaltung – 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_15083-03 - 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" diese ignorieren und ausschließlich die Aktualisierung des Confidentiality Codes durchführen. Sind im Confidentiality Code neben den Werten "normal", "restricted" oder "very restricted" andere Werte angegeben (z.B.: "PAT" oder "LEI"), sind diese ebenfalls zu ignorieren. Wenn in der Eingangsnachricht keine Aktualisierung für das Metadatenattribut Confidentiality Code enthalten ist, ist die Weiterverarbeitung abubrechen und die Nachricht mit einem `LocalPolicyRestrictionError`-Fehlercode zu quittieren.

[<=]

A_15061-02 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Restricted Update Document Set

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

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

- Ein neues `SubmissionSet`
- Einen `DocumentEntry`, der identisch mit dem zu aktualisierenden `DocumentEntry` identisch ist (inklusive `entryUUID`) und sich nur im `confidentialityCode` unterscheidet
- Eine SS-DE HasMember-Association, die das `SubmissionSet` mit dem geschickten `DocumentEntry` verbindet
- Die „lid“ (`logicalID`) DARF NICHT gesendet werden.
- Der Slot "PreviousVersion" MUSS immer mit dem Wert "1" gesendet werden.
- Der Slot „associationPropagation“ MUSS auf „no“ gesetzt werden.

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

[<=]

A_21533 - Komponente ePA-Dokumentenverwaltung – Kein Anlegen von Versionen für Restricted Update Document Set

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

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

A_21783-01 - Komponente ePA-Dokumentenverwaltung - Vererbung der Vertraulichkeitsstufe

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS den neu gesetzten `documentEntry.confidentialityCode` ebenfalls auf alle mit dem geänderten Dokument assoziierten Dokumente setzen. Als assoziierte Dokumente sind im Sinne dieser Anforderung sowohl Dokumente einer RPLC-Kette als auch Dokumente einer mixed- oder uniform-Sammlung zu betrachten.

[<=]

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 `XDSDocumentUniqueIdError`-Fehlercode enthalten und der Wert 4 des

EventOutcomeIndicators im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein zu aktualisierendes Dokument bzw. Metadaten nicht mehr verfügbar, MUSS gemäß IHE TF ITI der Fehlercode XSDDocumentUniqueIdError zurückgegeben werden.

[<=]

5.1.3 Schnittstelle I_Document_Management_Insurance

A_17438 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management_Insurance

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

Tabelle 19: 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 20: Tab_Dokv_37 - Operation Provide And Register Document Set-b

Operation	I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Document_Management_Insurance::putDocuments technisch um. Sie basiert auf den IHE ITI-Transaktionen "Provide And Register Document Set-b" [ITI-41] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente mitsamt Metadaten im ePA-Aktensystem dauerhaft zu speichern.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b		
Eingangsparameter			
Name	Beschreibung	Typ	opt.
Provide And Register Document Set-b Message	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	xdsb:ProvideAndRegisterDocumentSetRequest	n
X-User Assertion	Authentication Assertion des authentifizierten Kostenträgers	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA_KTR_Consumer #A_17253, A_17254]	n
Ausgangsparameter			
Name	Beschreibung	Typ	opt.

Provide And Register Document Set-b Response Message	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	rs:RegistryResponse	n
Technische Fehlermeldungen <i>Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.</i>			
Name	Fehlertext	Details	
MaxDocSizeExceeded	Die max. 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_17444-01 - 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] sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_FM_ePA_KTR_Consumer#A_17253, A_17254] entspricht.[<=]

A_21482 - Komponente ePA-Dokumentenverwaltung – Kein Einstellen von Ordnern

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

[<=]

5.1.4 Anforderungen an Sammlungstypen

A_20707-04 - Komponente ePA-Dokumentenverwaltung – Keine unpassenden Dokumente in nicht-statische Ordner

Falls das Dokument nicht den Vorgaben der Metadaten für strukturierte Dokumente gemäß `[gemSpec_IG_ePA]` entspricht, MUSS die Komponente ePA-Dokumentenverwaltung das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-Fehlercode `BadFolderAssociation` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die UUID (`DocumentEntry.entryUUID`) des identifizierten Dokuments angegeben werden.[<=]

A_20579-01 - Komponente ePA-Dokumentenverwaltung – Löschen von Ordnern

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS Requests, die darauf abzielen, einen statischen Folder direkt zu löschen, mit einem `XDSRegistryMetadataError` ablehnen.[<=]

A_20581-02 - 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 die Operation mit dem Fehler `ReferencesExistsException` abgebrochen wird, mit folgender Ausnahme: Das Löschen einer Elternnotiz im Kinderuntersuchungsheft ist erlaubt.

[<=]

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

A_23098-01A_23098 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung bei zeitlicher Ungültigkeit von strukturierten Dokumenten

Die Komponente ePA-Dokumentenverwaltung ~~als XDS-Akteur "Document Registry"~~ MUSS beim Einstellen eines strukturierten Dokuments sicherstellen, dass die Vorgaben gemäß `[gemSpec_IG_ePA]` hinsichtlich der zeitlichen Gültigkeit erfüllt werden und andernfalls das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `XDSRepositoryMetadataError`-Elements der Text „Version of submitted ~~MI~~ structured document is ~~no longer~~ not supported“ zurückgegeben werden.[<=]

Hinweis: Die zeitliche Gültigkeit ergibt sich aus den Attributen "validFrom" und (optional) "clientReadOnlyFromDate" der Vorgaben in `[gemSpec_IG_ePA]`.

5.2 Aktenkontoverwaltung

5.2.1 Schnittstelle I_Account_Management_Insurant

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

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

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

Tabelle 21: 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_14805-01 - 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 22: Tab_Dokv_26 - Operation Suspend Account

Operation	I_Account_Management_Insurant::SuspendAccount		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation I_Account_Management_Insurant::SuspendAccount technisch um. Mit dieser Operation werden die Daten aus der Akte eines Versicherten bei einem Anbieter ePA-Aktensystem in ein für andere Anbieter ePA-Aktensystem verarbeitbares Paket konsolidiert.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/SuspendAccount		
Eingangsparameter			
Name	Beschreibung	Typ	optional
X-User Assertion	Authentication Assertion des authentifizierten Versicherten als Inhaber der Akte	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109-*, A_15631]	nein
Provider ENC-Certificate	Verschlüsselungszertifikat des ePA-Aktensystembetreibers, der vom neuen ePA-Anbieter zum Betrieb der Akte des Versicherten beauftragt ist	X.509 Zertifikat	nein
Ausgangsparameter			
Package URL	URL, über die das erzeugte Exportpaket vom neuen Anbieter ePA-	URL mit Prozentkodierung	nein

	Aktensystem geladen werden kann		
Technische Fehlermeldungen			
Name	Fehlertext	Details	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig.	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
CERTIFICATE_INVALID	Das übergebene Provider ENC-Certificate ist ungültig	Das ENC-Zertifikat 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" oder "START_MIGRATION" die Operation `I_Account_Management_Insurant::SuspendAccount` ausführen kann.

A_15062-03 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Suspend Account

Die Komponente ePA-Dokumentenverwaltung MUSS für die Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist und ob der RecordState der KeyChain des Versicherten den Wert DISMISSED, START_MIGRATION oder SUSPENDED

besitzt. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden.

[<=]

A_21753-01 - Komponente ePA-Dokumentenverwaltung – Erneuter Aufruf von SuspendAccount

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

A_14885-07 - 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],

- den ursprünglichen Inhalt von DocumentEntry.URI in das Metadatum DocumentEntry.originalURI kopieren. DocumentEntry.originalURI wird ausschließlich im Rahmen des Aktenumzugs verwendet (d.h. kein Metadatum von XDS-Registry) und wie die anderen Metadaten auch in METADATA.XML übertragen.
- für Dokumente ohne DocumentEntry.title dieses Metadatum mit dem auf den reinen Dateinamen reduzierten Wert (d.h. ohne Pfadangaben) von documentEntry.URI befüllen und in METADATA.XML übernehmen,
- die Komprimierung der ZIP-Datei mit den die Kompressionsalgorithmen no-Compression (0) oder Deflate (8) entsprechend der Spezifikation <https://pkware.cachefly.net/webdocs/casestudies/APPNOTE.TXT> durchführen,
- die ZIP-Datei außerhalb des Verarbeitungskontextes persistieren,
- die ZIP-Datei im Zuge des Exports gemäß Referenzimplementierung [RefImpl_Exportpaket] verschlüsseln, so dass sichergestellt ist, dass nur entsprechend verschlüsselte Daten außerhalb des Verarbeitungskontextes auftreten können,
- die § 291a-Protokolldaten innerhalb der ZIP-Datei unter dem Dateinamen PROTO291.XML mit der folgenden Struktur

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

```
0">
  <phrext:AuditMessage>...</phrext:AuditMessage>
  <phrext:AuditMessage>...</phrext:AuditMessage>
</AuditMessages>
```

abgelegt werden,

- ungültige/veraltete Policy-Files verwerfen/nicht übernehmen (z.B. Policies, die die einzelne Dokumente eines MIOs von statischen Ordnern der Typen uniform und mixed deny-/allowlisten), 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 und gemäß Referenzimplementierung [RefImpl_Exportpaket] signiert und verschlüsselt 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_21838 - Komponente ePA-Dokumentenverwaltung – Prüfung Provider ENC Zertifikat

Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS das übergebene Provider ENC-Certificate mittels `TUC_PKI_018` (OCSP-Graceperiod=12h, PolicyList={ oid_epa_vau }) prüfen und ungültige Zertifikate mit der Fehlermeldung "CERTIFICATE_INVALID " ablehnen. [<=]

A_15622-01 - 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. Am Ende der URL des Exportpakets MUSS der „Export-Paket-Name“ stehen, der gemäß Referenzimplementierung [RefImpl_Exportpaket] erstellt wurde. [\leq]

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. [\leq]

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 23: 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	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers# A_14109-*, A_15631]	n

	Versicherten als Inhaber der Akte		
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_15526-01 - Komponente ePA-Dokumentenverwaltung – Voraussetzungen für die Ausführung von Resume Account

Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Operation `I_Account_Management_Insurant::ResumeAccount` nur ausgeführt wird, wenn die Akte des Versicherten im Zustand `REGISTERED_FOR_MIGRATION` oder `DL_IN_PROGRESS` ist und aktuell kein Datenimport aktiv ist (`resumeAccount` läuft bereits).[<=]

A_15568-02 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Resume Account

Die Komponente ePA-Dokumentenverwaltung MUSS für die Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist und für seine OwnerKVNR ein `AuthorizationKey` existiert. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault `ACCESS_DENIED`-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden.[<=]

A_15013-01 - ePA-Aktensystem – Download des Exportpakets

Das ePA-Aktensystem MUSS nach Eingang des Requests

`I_Account_Management_Insurant::ResumeAccount` das mittels des Aufrufparameters `PackageURL` referenzierte Exportpaket beim vorhergehenden Anbieter ePA-Aktensystem des Versicherten abrufen und für den Import durch den Verarbeitungskontext der ePA-Dokumentenverwaltung verfügbar machen sowie den Zustand `RecordState` der `KeyChain` des Versicherten auf den Wert `DL_IN_PROGRESS` setzen. [`<=`]

A_21752 - ePA-Aktensystem – Erfolgreicher Download des Exportpakets

Das ePA-Aktensystem MUSS nach erfolgreichem Download und Integritätsprüfung des Exportpakets den Zustand `RecordState` der `KeyChain` des Versicherten auf den Wert `READY_FOR_IMPORT` setzen und die Verarbeitung mit dem Import des Exportpakets fortsetzen. Ist die Integritätsprüfung nicht erfolgreich, ist der Zustand `RecordState` der `KeyChain` des Versicherten auf den Wert `REGISTERED_FOR_MIGRATION` zu setzen und der Verarbeitungskontext zu schließen sowie der Versicherten über das Fehlschlagen des Downloads zu informieren. [`<=`]

A_14905-03 - 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 gemäß Referenzimplementierung [`RefImpl_Exportpaket`] importieren und dazu:

- das Exportpaket mittels des privaten ENC-VAU-Schlüssels des neuen Betreibers und des `ContextKey` entschlüsseln,
- die Signatur der VAU des alten Betreibers prüfen und
- die Struktur des Exportpakets auf Übereinstimmung mit den Festlegungen aus Anforderung A_14885 prüfen.
- falls `DocumentEntry.originalURI` in `METADATA.XML` vorhanden ist, wird für jedes Dokument eines `SubmissionSet` der Inhalt von `DocumentEntry.URI` durch den Inhalt von `DocumentEntry.originalURI` aus `METADATA.XML` ersetzt. (Hinweis: `DocumentEntry.originalURI` darf nicht als eigenständiges Metadatum in die Registry übernommen werden, da es lediglich dem Transport des Originalwertes von `DocumentEntry.URI` aus dem alten Aktensystem dient.)

Kann das Exportpaket nicht entschlüsselt werden oder ist die Struktur des Exportpakets fehlerhaft ist der Zustand `RecordState` der `KeyChain` des Versicherten auf den Wert `REGISTERED_FOR_MIGRATION` zu setzen und der Verarbeitungskontext zu schließen sowie den Versicherten über das Fehlschlagen des Imports zu informieren. [`<=`]

A_15596-01 - 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`, `SubmissionSet.homeCommunityId`, `Folder.homeCommunityId` und `DocumentEntry.repositoryUniqueId` mit der neuen Home Community ID aktualisieren. [`<=`]

A_15623 - Komponente ePA-Dokumentenverwaltung – Asynchroner Import

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

`I_Account_Management_Insurant::ResumeAccount` unmittelbar nach dem Aufruf an den

Client zurückgeben, unabhängig davon, wie lange der Erhalt und Import des Exportpakets dauert. [`<=`]

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

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

A_15624-01 - 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 oder Abbruch periodisch prüfen, jedoch maximal für einen Zeitraum von drei Tagen, ob ein Exportpaket unter der vom Client übergebenen URL bereitsteht. [`<=`]

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

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

A_16077-02 - Komponente ePA-Dokumentenverwaltung – Frist für den Import des Exportpakets

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

[`<=`]

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

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

[`<=`]

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

A_21754 - Komponente ePA-Dokumentenverwaltung – Aktivierung Import des Exportpakets

Befindet sich der `RecordState` der `KeyChain` des Versicherten im Zustand `READY_FOR_IMPORT` und ist kein Importvorgang aktiv MUSS die Komponente ePA-Dokumentenverwaltung beim Öffnen des Verarbeitungskontexts den Import des bereits heruntergeladenen Migrationspakets anstoßen und alle folgenden Operationsaufrufe

entsprechend A_15625 mit der Fehlermeldung "Aktenkonto aufgrund einer andauernden Datenmigration vorübergehend nicht erreichbar" ablehnen. [≤]

A_21241-01 - 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 ZustandRecordState der KeyChain des Versicherten von READY_FOR_IMPORT auf den Wert ACTIVATED setzen, wenn die initiale Schlüsselhinterlegung für den Versicherten bereits erfolgte. [≤]

5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents

A_14490-08 - 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 24: 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
PageSize	Umsetzung gemäß [gemSpec_Aktensystem#5.2.1.1]	Integer (> 0)	y
PageNumber	Umsetzung gemäß [gemSpec_Aktensystem#5.2.1.1]	Integer (> 0)	y

LastDay	Umsetzung gemäß [gemSpec_Aktensystem # 5.2.1.1]	YYYY-MM-DD oder YYYY-MM-DDThh:mm:ssZ	y
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
AuditMessage	Liste der Zugriffsprotokolleinträge	AuditMessage [0..*]	n
PageSize	Umsetzung gemäß [gemSpec_Aktensystem # 5.2.1.1]	Integer (> 0)	y
PageNumber	Umsetzung gemäß [gemSpec_Aktensystem # 5.2.1.1]	Integer (> 0)	y
TotalPages	Umsetzung gemäß [gemSpec_Aktensystem # 5.2.1.1]	Integer (>= 0)	y
TotalEntries	Umsetzung gemäß [gemSpec_Aktensystem # 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_15229-03 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Get Audit Events

Die Komponente ePA-Dokumentenverwaltung MUSS für die Ausführung dieser Operation prüfen, ob für den zugreifenden Nutzer ein gültiges Policy Document vorliegt. Liegt kein Policy Document vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [\leq]

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. [\leq]

5.2.1.4 Operation

I_Account_Management_Insurant::GetSignedAuditEvents

A_21110-04 - 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 25: 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
PageSize	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (> 0)	y

PageNumber	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (> 0)	y
LastDay	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	YYYY-MM-DD oder YYYY-MM-DDThh:mm:ssZ	y
Ausgangsparameter			
Name	Beschreibung	Typ	opt.
Signed Audit Event List	Signierte Liste (Teilliste bei Verwendung der Paging-Parameter) der Zugriffsprotokolleinträge	Signiertes Dokument	n
PageSize	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (> 0)	y
PageNumber	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (> 0)	y
TotalPages	Umsetzung gemäß [gemSpecAktensystem #5.2.1.1]	Integer (>= 0)	y
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.	
----------------------	--	--

[<=]

5.2.1.4.1 Umsetzung

A_21111-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Get Signed Audit Events

Die Komponente ePA-Dokumentenverwaltung MUSS für die Ausführung dieser Operation prüfen, ob für den zugreifenden Nutzer ein gültiges Policy Document vorliegt. Liegt kein Policy Document vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [<=]

A_21112-01 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Get Signed Audit Events

Die Komponente ePA-Dokumentenverwaltung MUSS die Liste der § 291a-Protokolleinträge als signiertes 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 Dokument bzw. die Dokumente signiert. Das Format soll dem von Audit Events entsprechen.

5.3 Umschlüsselung

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

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

Der Vorgang der Umschlüsselung wird über die folgenden Operationen gesteuert:

- I_Key_Management_Insurant::StartKeyChange()
- I_Key_Management_Insurant::GetAllDocumentKeys()
- I_Key_Management_Insurant::PutAllDocumentKeys()
- I_Key_Management_Insurant::FinishKeyChange()

Die Dokumentenverwaltung befindet sich nach erfolgreicher Einleitung der Umschlüsselung (StartKeyChange()) im logischen Zustand "KEY_CHANGE_DOKV". Sie ist

dabei für alle Teilnehmer außer den Versicherten sowie für alle Operationen, die nicht die Umschlüsselung betreffen, gesperrt.

Die Umschlüsselung wird vom Client mittels FinishKeyChange() abgeschlossen und die Dokumentenverwaltung über diesen Aufruf über Erfolg oder Misserfolg aus Sicht des Clients informiert. Im Falle eines Misserfolgs startet die Dokumentenverwaltung ein Rollback, in dem alle umgeschlüsselten Dokumentenschlüssel wieder durch die alte 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_20466-02 - Komponente ePA-Dokumentenverwaltung – Erlaubte Zustandsübergänge für Zustand KEY_CHANGE_DOKV

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

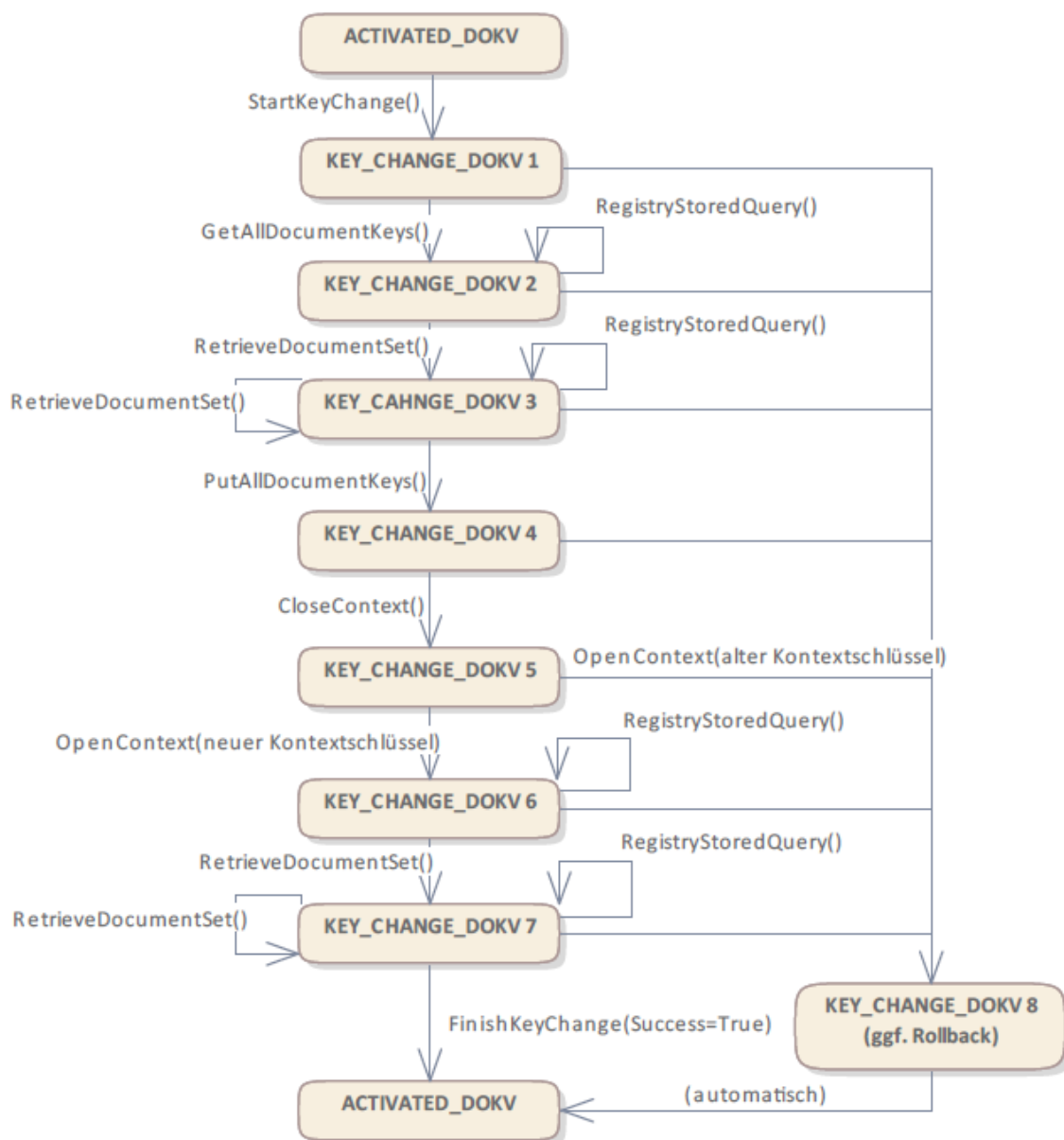


Abbildung 2: Zustandsübergänge Schlüsselwechsel

Erläuterungen:

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

- `FinishKeyChange(): I_Key_Management_Insurant::FinishKeyChange()`
- `OpenContext(): I_Document_Management_Connect::OpenContext()`
- `CloseContext(): I_Document_Management_Connect::CloseContext()`
- `RetrieveDocumentSet(): I_Document_Management_Insurant::RetrieveDocumentSet()`
- `CloseContext()` (gefolgt von `OpenContext(Neuer Kontextschlüssel)`) DARF zusätzlich auch in Kombination in den Zuständen `KEY_CHANGE_DOKV 1, 2, 3, 6` und `7` 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 über die jeweilige Schnittstelle auf Dokumente zugreifen können.
- Ein Rollback muss dann ausgeführt werden, wenn ein Fehler eine erfolgreiche Beendigung des Umschlüsselungsprozesses verhindert. Kann das ePA-FdV auf den Fehler so reagieren, dass der Umschlüsselungsprozess dennoch erfolgreich weitergeführt werden kann, ist kein Rollback nötig. Neben den in A_20468, A_20442, A_20730 und A_20451 beschriebenen Konstellationen bei denen durch das Aktensystem ein Rollback durchgeführt wird, muss auch in folgenden Situationen ein Rollback erfolgen, sofern das ePA-FdV darauf nicht geeignet reagieren kann:
 - Ablehnen einer Operation, die nicht zu den definierten Zustandsübergängen laut A_20466-01 passt und eine erfolgreiche Beendigung des Umschlüsselungsprozesses verhindern,
 - verschiedene Fehler in `GetAllDocumentKeys` sowie
 - verschiedene Fehler in `FinishKeyChange(TRUE)`.

[<=]

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_23001 - Komponente ePA-Dokumentenverwaltung – Spezielles CloseContext während der Umschlüsselung

Im Aktensystemzustand KEY_CHANGE MUSS die Komponente ePA-Dokumentenverwaltung bei der Operation CloseContext nur den VAU-Kontext schließen. Die VAU-Verbindung zwischen dem Client und dem Verarbeitungskontext MUSS erhalten bleiben. Somit wird sichergestellt, dass nach dem CloseContext (KEY_CHANGE_DOKV4) und vor dem OpenContext (KEY_CHANGE_DOKV5) keine neue VAU Verbindung aufgebaut wird und somit keine weitere Interaktion des Versicherten (wie z.B. PIN-Eingabe) während der Umschlüsselung erforderlich ist. [≤]

A_20726-01 - Komponente ePA-Dokumentenverwaltung – Verbotene Operationen außerhalb Status KEY_CHANGE_DOKV

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

A_20727-01 - Komponente ePA-Dokumentenverwaltung – Validierung der Authentication Assertion

Die Komponente ePA-Dokumentenverwaltung MUSS in allen Eingangsnachrichten der Schnittstelle I_Key_Management_Insurant analog eines XUA-Akteur "X-Service Provider" die mitgelieferte X-User Assertion (Authentication Assertion) gemäß der Anforderung A_13690-* prüfen und die eingehende Nachricht mit Fehlercodes nach [WSS#12] sowie einem HTTP-Fehler 403 (Fehlermeldung "Access Denied") quittieren, falls diese X-User Assertion nicht gültig ist. [≤]

Die Authentication Assertion wird als Teil des SOAP Headers mitgeschickt.

A_20444-03 - 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 in [KeyManagementService] festgelegte Format verwenden.

Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
<phr:DocumentKeyList xmlns:phr="http://ws.gematik.de/fd/phr/I_Key_Management/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:DocumentKeyList>
```

Dabei gelten folgende Anforderungen:

- Das Element <xenc:EncryptedData> MUSS wie in [gemSpec_DM_ePA#14977](#) angegeben gefüllt sein

- Abweichend davon MUSS das Element `<xenc:CipherData>` mit leerem Elementwert gesendet werden.
- Das Element `<ds:KeyInfo>` MUSS ausschließlich mit dem Child-Element 'KeyName' belegt 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_20735-01 - 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()`) mit dem Fehlercode `TEMP_UNAVAILABLE` 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 oder das FdV abgestürzt ist.

Das Aktensystem kann die erneute Anmeldung eines abgestürzten FdV daran erkennen, dass sie über das Gerät des Versicherten mit der gleichen Device-ID erfolgt.

[`<=`]

A_23003 - Komponente ePA-Dokumentenverwaltung – Protokollierung der Abrufe der Test-Dokumente bei der Umschlüsselung

Sofern kein Protokollierungsschlüssel verwendet wird, MUSS die Komponente ePA-Dokumentenverwaltung bei der Protokollierung der Umschlüsselung in „ObjectDetail“ der Protokolleinträge für den Abruf der Test-Dokumente vor `CloseContext` folgende Information aufnehmen:

„Um die korrekte Durchführung der Umschlüsselung sicherzustellen, wird auf dieses Dokument im Rahmen der Umschlüsselung zweimal zugegriffen. Wird die Umschlüsselung im Fehlerfall abgebrochen, erfolgt ggf. nur ein Zugriff“. [`<=`]

A_20442-01 - Komponente ePA-Dokumentenverwaltung – Timeout für Zustand KEY_CHANGE_DOKV

Die Komponente ePA-Dokumentenverwaltung MUSS im Status `KEY_CHANGE_DOKV` nach Erreichen des Zeitpunkts `RollbackTime` (Zeitpunkt 24 Stunden nach Aufruf von `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_20447-01 - Komponente ePA-Dokumentenverwaltung – Rollback für Zustand KEY_CHANGE_DOKV

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

- Aufruf `finishKeyChange(FALSE)` in der Autorisierungskomponente
- Löschen aller Daten, die mit dem neuen Kontextschlüssel verschlüsselt wurden
- Reaktivierung aller mit dem alten Kontextschlüssel verschlüsselten Daten
- Wiederherstellen bzw. Reaktivierung aller mit dem alten Aktenschlüssel verschlüsselten Dokumentenschlüssel
- Löschen von allen mit dem neuen Aktenschlüssel verschlüsselten Dokumentenschlüssel
- 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_20467-01 - Komponente ePA-Dokumentenverwaltung – Signatur für I_Key_Management_Insurant::StartKeyChange()

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

Tabelle 26: Tab_Dokv_38 - Operation I_Key_Management_Insurant::StartKeyChange()

Operation	I_Key_Management_Insurant::StartKeyChange		
Beschreibung	Diese Operation setzt die Operation I_Key_Management_Insurant::StartKeyChange technisch um. Mit dieser Operation kann der Versicherte den Prozess der Umschlüsselung initiieren.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/StartKeyChange		
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
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 Fehlerh after 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_22999 - Komponente ePA-Dokumentenverwaltung – Asynchrone Umsetzung von StartKeyChange

Die Komponente ePA-Dokumentenverwaltung KANN die Operation StartKeyChange bzgl. Kontextumschlüsselung und ggfs. Dokumentenschlüsselextraktion asynchron ausführen. [≤]

A_23000 - Komponente ePA-Dokumentenverwaltung – Fehlermeldung STARTKEYCHANGE_ACTIVE bei nicht abgeschlossenen asynchronen Operationen

Bei asynchroner Umsetzung der Operation StartKeyChange MÜSSEN die nachfolgenden Operationen GetAllDocumentKeys und ggfs. CloseContext die Fehlermeldung STARTKEYCHANGE_ACTIVE liefern, solange die asynchronen Operationen noch nicht abgeschlossen sind. [≤]

A_20495-01 - Komponente ePA-Dokumentenverwaltung – Format von phr:AuthorizedIDList

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

```
<phr:AuthorizedIDList xmlns:phr="http://ws.gematik.de/fd/phr/I_Key_Management/v1.0" >
  <!--ID des Berechtigten, jeweils eines für jeden Berechtigten-->
  <phr:AuthorizedID>
    <!-- KVNR (bei Versicherten) oder Telematik ID (bei Leistungserbringern und Kostenträgern) des Berechtigten -->
    <ID> ... </ID>
    <!-- Typ: "KVNR" oder "TelematikID"-->
    <Type> ... </Type>
  </phr:AuthorizedID>
</phr:AuthorizedIDList>
[≤]
```

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

A_20738-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Start Key Change

Die Komponente ePA-Dokumentenverwaltung MUSS für die Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [≤]

A_20757-01 - 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_15705] entspricht und ansonsten den Fehler "SYNTAX_ERROR" zurückgeben. [≤]

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

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

A_21618 - Komponente ePA-Dokumentenverwaltung – Aufruf von StartKeyChange() der Autorisierungskomponente

Die Komponente ePA-Dokumentenverwaltung MUSS unmittelbar nach dem Aufruf von `StartKeyChange()` ihrerseits die Operation `StartKeyChange()` der Autorisierungskomponente aufrufen. [`<=`]

5.3.2.2 I_Key_Management_Insurant::GetAllDocumentKeys()

A_20443-01 - 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 27: 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.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Key_Management_Insurant/v1.0/GetAllDocumentKeys		
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
Ausgangsparameter			

Name	Beschreibung	Typ	opt
DocumentKeyList	Liste aller Document Keys, jeweils verschlüsselt mit altem Aktenschlüssel	phr:KeyList	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.		

[<=]

5.3.2.2.1 Umsetzung

A_20452-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Get All Document Keys

Die Komponente ePA-Dokumentenverwaltung MUSS für die Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden.[<=]

A_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.

[<=]

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

5.3.2.3 Operation I_Key_Management_Insurant::PutAllDocumentKeys()

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

Die Komponente ePA-Dokumentenverwaltung MUSS die Operation

I_Key_Management_Insurant::PutAllDocumentKeys gemäß der folgenden Signatur implementieren:

Tabelle 28: Tab_Dokv_40 - Operation I_Key_Management_Insurant::PutAllDocumentKeys()

Operation	I_Key_Management_Insurant::PutAllDocumentKeys		
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	optional
X-User Assertion	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhaber s)	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109-*, A_15631]	nein
DocumentKeyList	Liste aller Document Keys, jeweils verschlüsselt mit neuem Aktenschlüssel	phr:KeyList	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 Fehlerhafter 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_20453-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Put All Document Keys

Die Komponente ePA-Dokumentenverwaltung MUSS für die Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [≤]

A_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_20758-01 - Komponente ePA-Dokumentenverwaltung – Prüfung des DocumentKeyList-Parameters

Die Komponente ePA-Dokumentenverwaltung MUSS prüfen, ob die im Parameter "DocumentKeyList" gesendeten Daten den Strukturvorgaben gemäß A_20444-* entspricht und ansonsten den Fehler "SYNTAX_ERROR" 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 29: Tab_Dokv_41 - Operation I_Key_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	opt.
X-User Assertion	Authentication Assertion des authentifizierten Versicherten (Aktenkonteninhabers)	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers #A_14109-*, A_15631]	n
Success	Beschreibt, ob die Umschlüsselung aus Sicht des Clients erfolgreich (true) oder nicht erfolgreich (false) beendet werden soll.	xs:boolean	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 Fehlerh after 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_20454-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Finish Key Change

Die Komponente ePA-Dokumentenverwaltung MUSS für die Ausführung dieser Operation prüfen, ob der zugreifende Nutzer der Akteninhaber selbst ist. Liegt dieser Fall nicht vor, MUSS die Nachricht mit dem SOAP-Fault ACCESS_DENIED-Fehlercode sowie einem HTTP-Statuscode 403 (Fehlermeldung "Access Denied") gemäß [RFC7231] quittiert werden. [<=]

A_21620 - Komponente ePA-Dokumentenverwaltung – Aufruf von FinishKeyChange() der Autorisierungskomponente

Die Komponente ePA-Dokumentenverwaltung MUSS unmittelbar nach dem Aufruf von `FinishKeyChange()` ihrerseits die Operation `FinishKeyChange()` der Autorisierungskomponente aufrufen und dabei den gleichen Wert des Parameters `Success` verwenden. [<=]

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#-*]` mit `EventID.code` `PHR-870` protokollieren.
[<=]

A_20451 - Komponente ePA-Dokumentenverwaltung – Erfolgreicher Abschluss des Schlüsselwechsels

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

5.3.2.5 Protokollierung

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

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

Tabelle 30: Tab_Dokv_42 - Zusätzliche Parameter des § 291a-Protokolls für die Umschlüsselung

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

[<=]

5.4 Zugriffskontrolle

Die Zugriffskontrolle stellt sicher, dass nur solche Zugriffe zugelassen werden, die vom Versicherten oder seinen Vertreter autorisiert wurden. Zur Autorisierung an Leistungserbringerinstitutionen (LEI) sowie Kostenträgern stehen dazu grundsätzlich verschiedene Granularitäten zur Verfügung. Dies sind zum einen die (1) kategorienbasierte Autorisierung und zum anderen die (2) dokumentenspezifische Autorisierung.

1. Die **kategorienbasierte Autorisierung** schränkt den Zugang Dritter über berufsgruppenspezifische Vorgaben gemäß § 341 PDSG Absatz 2 ein. Dazu gibt es festgelegte Dokumentenkategorien, welche mit spezifischen Zugriffsrechten der grundlegenden Zugriffsoperationen (CRUD - create, read, update, delete) wirken (vgl. Tab_Dokv_030 - Zugriffsunterbindungsregeln in A_19303-*). Diese Zugriffsrechte wirken ausnahmslos, d.h. auch bei einer etwaigen weiteren Autorisierung einer dokumentenspezifischen Autorisierung (siehe 2.) gelten diese Regeln ebenso. Beispiele sind:

- a. Apotheker haben keinen Zugriff auf das Zahnbonusheft der Dokumentenkategorie "dentalrecord").
- b. Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen noch löschen.

Jede Einstellung eines Dokuments (Ausnahme: Mutterpass und Kinderuntersuchungsheft) wird von der ePA-Dokumentenverwaltung mit einer automatischen Zuordnung zu einem statischen Ordner, welcher die Dokumentenkategorie repräsentiert, erweitert. Diese statischen Ordner sind initial bei jedem Aktenkonto eines Versicherten existent. Die serverseitige Zuordnung in diese Ordner erfolgt anhand der XDS-Metadaten in Kombination mit der Nutzergruppe des Einstellers, welche aus der Authentication Assertion erkennbar ist (die Nutzergruppe ist dem Signaturzertifikat zu entnehmen). Die Regeln für diese Zuordnung sind in [gemSpec_DM_ePA#A_20577-*] festgelegt.

Das bedeutet weiterhin, dass das Anlegen von Ordnern durch ePA-Clients nicht erlaubt ist, um eine zweifelsfreie Freigabe auf Grundlage der Dokumentenkategorien zu gewährleisten. Es gibt zwei Ausnahmen bei den medizinischen Informationsobjekten (MIOs), welche ebenso einer Dokumentenkategorie unterliegen und jeweils einem Ordner zugeordnet werden müssen. Diese sind der Mutterpass sowie das Kinderuntersuchungsheft. Bei mehreren Kindern können auch mehrere Ordner zu diesen Pässen in einer ePA existieren. Eine zweifelsfreie Zuordnung in der ePA-Dokumentenverwaltung wäre daher nicht gegeben, sodass hier ePA-Clients die Ordner zeitgleich mit der Dokumentenregistrierung anlegen müssen. Eine vorherige Abfrage der Ordner mit den speziellen folderCodes ist allerdings zu empfehlen.

Weiterhin kann die Auswahl einer Dokumentenkategorie durch den Versicherten oder seinen Vertreter durch eine sensiblere Vertraulichkeit eingeschränkt werden. Es ist von Vorteil, die Vertraulichkeit eines Dokuments an dieser Stelle näher zu beschreiben: Einstellende Akteure können einem Dokument eine der drei Vertraulichkeitsstufen "streng vertraulich", "vertraulich" oder "normal" zuordnen. Eingestellte Dokumente mit der Vertraulichkeitsstufe "streng vertraulich" sind zunächst nicht über potentiell vorhandene Autorisierungen für Dritte zugänglich. Wenn eine Autorisierung und damit Freigabe dieses sensiblen Dokuments erwünscht ist, muss dieses Dokument über eine dokumentenspezifische Autorisierung in Form einer Allowlist autorisiert werden.

Die beiden anderen Stufen "vertraulich" oder "normal" müssen mit einer Dokumentenkategorie kombiniert werden. Eine pauschale Berechtigung auf "normale" Dokumente beinhaltet im Detail auch implizit die Auswahl und Zustimmung aller Dokumentenkategorien. Während einer Ad-hoc-Berechtigung kann aufgrund der Einschränkungen des Kartenterminals zu ein oder mehreren ausgewählten Dokumentenkategorien nur eine Vertraulichkeit für die Freigabe durch den Versicherten bestätigt werden. Auf Seite des ePA-FdV könnte hingegen pro freigegebene Kategorie entweder die Vertraulichkeitsstufe "vertraulich", "normal" als auch beide Stufen in einer Autorisierung ausgesprochen werden. Einer Leistungserbringerinstitution, welcher lediglich ein ausschließlicher Zugriff auf Dokumente mit der Vertraulichkeitsstufe "normal" vergeben wurde, wird unter dem Begriff "einfaches Zugriffsrecht" subsumiert. Hingegen bedeutet die Autorisierung auf Dokumente mit den Vertraulichkeitsstufen "normal" und "vertraulich" ein "erweitertes Zugriffsrecht".

2. Die **dokumentenspezifische Autorisierung** bietet dem Versicherten oder seinen Vertreter mit ePA-FdV die Möglichkeit, Dokumente bzw. Ordner (gemeint sind dynamische Ordner) auf einer Allowlist ("gewährender Zugriff") oder Denylist

("verbotender Zugriff") zu setzen. Ein Dokument bzw. Ordner (genauer gesagt die `DocumentEntry.entryUUID` bzw. `Folder.entryUUID` auf Policy-Ebene) darf auf diesen Listen nicht gleichzeitig stehen. Auch sind diese Dokumente und Ordner aufgrund der Zuordnungsregeln beim Einstellen indirekt immer einer Kategorie zugeordnet. Es ist hier aber möglich, feingranularer, d.h. auf Dokumentenebene Zugriffe für Leistungserbringerinstitutionen auszusprechen.

Bei dynamischen Ordnern der Kategorie `"mothersrecord"` bzw. `"childsrecord"` gibt es die Besonderheit, dass ein konkreter Ordner auf Allow-/Denylist gesetzt werden kann. Dadurch wird automatisch auf das darin enthaltene MIO und weitere Dokumente der Zugriff erteilt bzw. verweigert. Weitere Dokumente aus diesen Ordnern, die nicht zu den MIOs gehören, können über die `DocumentEntry.entryUUID` auf Allow-/Denylist gesetzt werden.

5.4.1 Vergabe von Zugriffsrechten und Policy Administration

Der Versicherte und sein Vertreter können Berechtigungen aller Art (d.h. kategorienbasiert als auch dokumentenspezifisch) entweder über das ePA-FdV oder am KTR-AdV-Terminal in der Kostenträgerumgebung mittels dort zur Verfügung stehender ePA-FdV AdV vergeben. Darüber hinaus können Leistungserbringerinstitutionen über eine Ad-hoc-Berechtigung beim Leistungserbringer vor Ort kategorienbasiert berechtigt werden. Die zeitliche Gültigkeit der erteilten Zugriffsrechte wird vom Versicherten festgelegt. Sie wird zeitlich befristet oder unbefristet vergeben.

Die Berechtigungsvergabe erfolgt durch das Einstellen eines Policy Documents als XDS-Dokument (siehe nachstehende Abbildung 3). Vorgaben bzgl. der Struktur sowie der aktensystemseitigen Verarbeitung sind im Abschnitt 5.4.2 festgelegt. Die Policy Documents setzen ferner das Zugriffskontrollmodell Attribute-based Access Control (ABAC) um. Die Registrierung dieser sogenannten Advanced Patient Privacy Consents (APPC) erfolgt als unverschlüsselte Dokumente (jedoch über die sichere Verbindung zwischen dem Fachmodul ePA bzw. dem ePA-Frontend des Versicherten und dem Verarbeitungskontext) durch Nutzung der IHE ITI-Transaktionen "Cross-Gateway Document Provide" [ITI-80] sowie "Provide And Register Document Set-b" [ITI-41]. Die interne Datenhaltung bzgl. der Policies ist nicht vorgegeben, allerdings müssen diese Policies über die Standard-Abfrageschnittstelle der Operationen Registry Stored Query [ITI-18] und Retrieve Document Set [ITI-43] dem ePA-Frontend des Versicherten zugänglich gemacht werden. Dazu werden die `DocumentEntry`-Metadaten gemäß der Anforderung `[gemSpec_DM_ePA#A_14961-*)]` vorgegeben.

Die grundlegende Zugriffsstrategie ist "Opting-in", sodass ein gewährendes Zugriffsrecht nur durch Registrierung eines neuen Policy Document vergeben werden kann. Ein Policy Document drückt die grundsätzliche Autorisierung eines Leistungserbringers oder Kostenträgers durch den Versicherten oder seinen Vertreter aus. Es formuliert KEINE erlaubten Operationen im Detail (wie in ePA1), sondern legitimiert potentielle Lese- und Löschzugriffe entsprechend der Zugriffsunterbindungsregeln (vgl. A_20736-*). Das Zugriffsrecht zum Einstellen oder Ersetzen eines (med.) Dokuments durch einen Zugriffsberechtigten ergibt sich indirekt durch die Existenz eines gültigen Policy Document für diesen Zugriffsberechtigten.

A_15173-04 - Komponente ePA-Dokumentenverwaltung – Zugriffsstrategie "Opting-in" mit "Access Deny" als Standardeinstellung

Die Komponente ePA-Dokumentenverwaltung MUSS jeden Zugriff verweigern, der nicht auf der Grundlage definierter Policy Documents (Advanced Patient Privacy Consents) in Kombination mit der entsprechenden Operation gemäß A_19303-*, A_19997-*, A_19998-* oder A_20736-* explizit erlaubt ist. [\leq]

Eine inhaltliche Änderung eines Policy Document ist nicht vorgesehen. Stattdessen soll durch den Client ein zu einem Berechtigten ein vorhandenes Policy Document gelöscht und ein neues registriert werden. Wurde ein vorhandenes Policy Document, das demselben Berechtigten zuzuordnen ist, durch den Client nicht explizit gelöscht, wird diese von der ePA-Dokumentenverwaltung automatisch gelöscht bzw. überschrieben, während das neue Policy Document eingestellt wird. Eine Übereinstimmung liegt vor, wenn `xacml:SubjectMatch`, `xacml:ResourceMatch` identisch sind.

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

Die Komponente ePA-Dokumentenverwaltung MUSS über die Operationen

`I_Document_Management::CrossGatewayDocumentProvide` sowie

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

[<=]

Weitere Anforderungen zum Umgang mit Policies sind die folgenden:

A_14892-04 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen ungültiger Policy Documents

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

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

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

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

[<=]

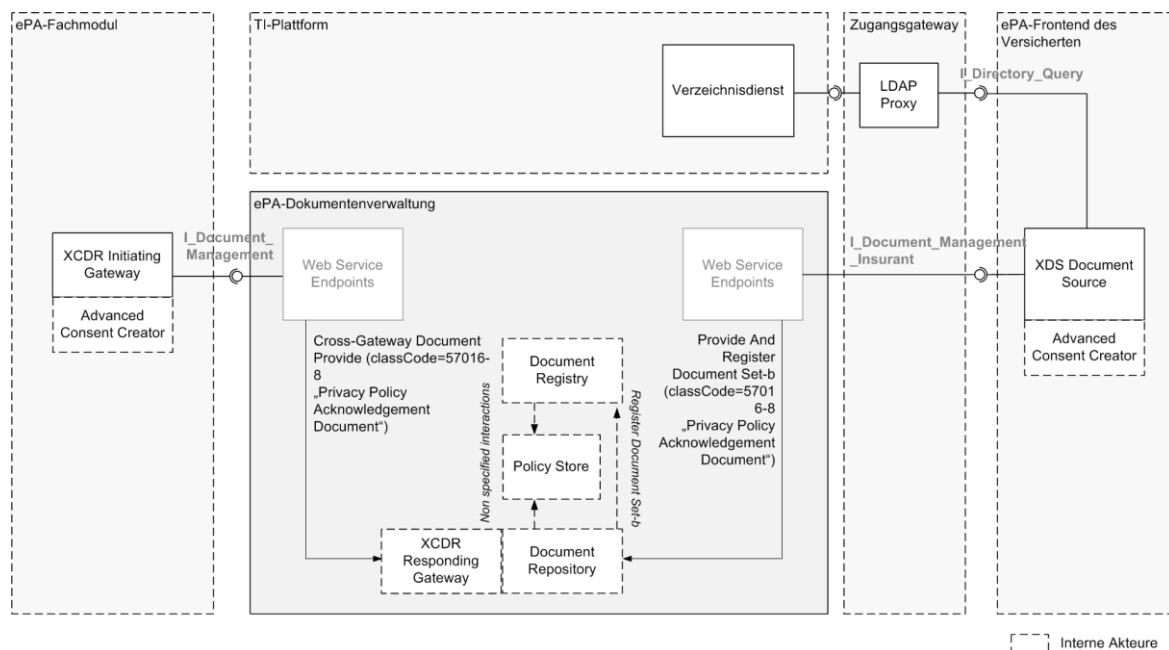


Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen

Hinweis: Die vorstehende Abbildung verdeutlicht, wie Berechtigungen über die entsprechenden IHE ITI-Transaktionen vergeben werden. Der Transaktion "Cross-Gateway Document Provide" liegt genaugenommen keine IHE ITI-konforme Nachricht des Primärsystems zum Einstellen des Policy Document 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 Document gegenüber der ePÄ-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.

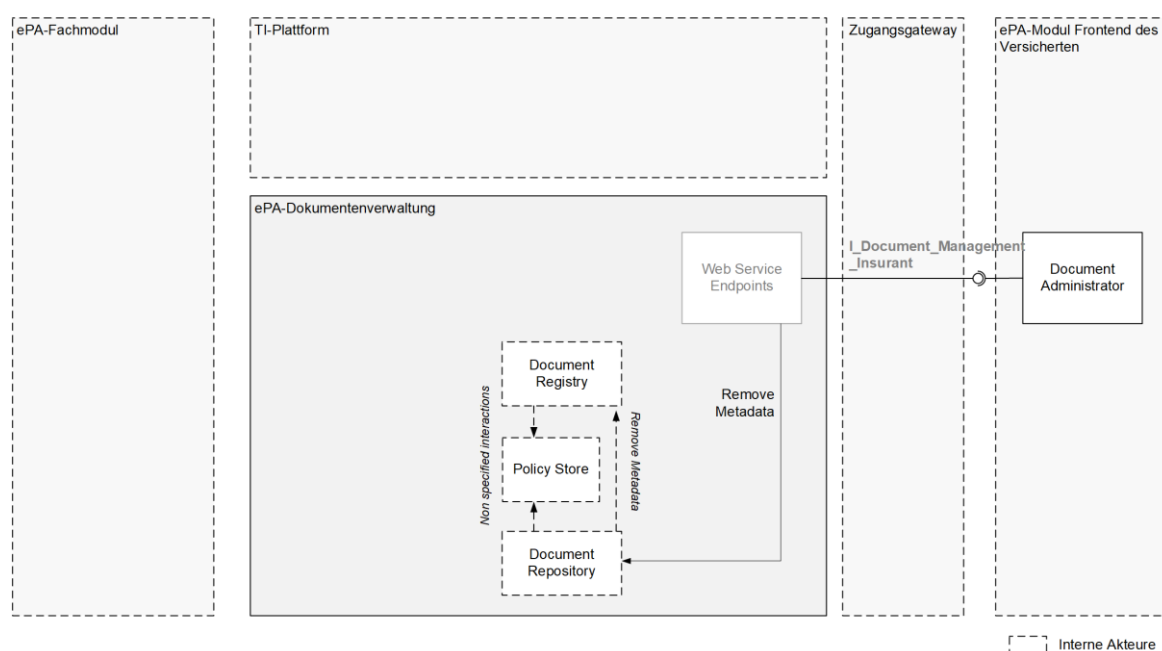


Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen

A_16195-02 - Komponente ePA-Dokumentenverwaltung – UTF-8-Kodierung eines zu registrierenden Policy Documents

Die Komponente ePA-Dokumentenverwaltung MUSS ausschließlich UTF-8-kodierte Policy Documents für eine Registrierung akzeptieren und intern verarbeiten. Im Fehlerfall MUSS die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittiert und der InvalidDocumentContent-Fehlercode mit der UniqueID des Policy Document zurückgeben werden. [\leq]

A_15536-04 - Komponente ePA-Dokumentenverwaltung – Prüfungen bei Registrierung eines Policy Documents

Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Document folgende inhaltlichen Prüfungen durchführen und im Fehlerfall die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und den InvalidDocumentContent-Fehlercode mit der UniqueID des Policy Document zurückgeben:

- *Prüfung der XACML-Konformität*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung des Policy Document abbrechen, wenn das Profil des Policy Document nicht mit den Anforderungen aus den Abschnitten 5.4.2.2 bis 5.4.2.4 übereinstimmt.
- *Prüfung der Aktenidentität*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung des Policy Document abbrechen, wenn das Resource-Element mit der Attribut-ID "urn:ihe:iti:ser:2016:patient-id" nicht mit der Identität der Akte (d.h. die des Akteninhabers) übereinstimmt.
- *Prüfung des Einstellers*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung des Policy Document abbrechen, wenn die in der Nachricht enthaltene SAML 2.0 Assertion (Authentication Assertion / X-User Assertion) nicht dem Versicherten oder einem seiner Vertreter zugeordnet ist (d.h. das root-Attribut des InstanceIdentifier-Elements innerhalb des SubjectMatch-Elements muss mit der OID "1.2.276.0.76.4.8" eine KVN Kennzeichen).

- *Keine Verwendung des "xsi:schemaLocation"-Attributs*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung des Policy Document abbrechen, wenn ein `xsi:schemaLocation`-Attribut gemäß [XMLSchema#2.6.3] enthalten ist.
- *Verstöße gegen Policy-Struktur und -Inhalte*
Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung des Policy Document abbrechen, wenn sie Verstöße gegen die Vorgaben aus [gemSpec_DM_ePA#A_14961-*] erkennt.

[<=]

A_14933-02 - Komponente ePA-Dokumentenverwaltung – XML Schema-Validierung eines Policy Document

Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Document dieses einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen. Ist ein Policy Document nicht wohlgeformt oder gültig, MUSS die Komponente ePA-Dokumentenverwaltung die Registrierung des Policy Document ablehnen, die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und den InvalidDocumentContent-Fehlercode mit der UniqueID des Policy Document zurückgeben. [<=]

A_21647-03 - Komponente ePA-Dokumentenverwaltung – MIOs in Allowlist und Denylist

Die Komponente ePA-Dokumentenverwaltung MUSS dynamische Ordner und statische Ordner der Sammlungstypen uniform und mixed auf der Allowlist oder der Denylist eines Policy Documents akzeptieren. Ein solcher Ordner wird dabei über die Folder.entryUUID referenziert. Dokumente eines MIOs (z.B. Eintrag eines Mutterpasses) DÜRFEN NICHT über die DocumentEntry.entryUUID auf einer der beiden Listen stehen. Liegt eine Verletzung vor, MUSS die Komponente ePA-Dokumentenverwaltung die Registrierung des Policy Document ablehnen, die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und den InvalidDocumentContent-Fehlercode mit der UniqueID des Policy Document zurückgeben.

[<=]

Mit der o.g. Anforderung wird sichergestellt, dass z.B. ein Mutterpass nur in seiner Gesamtheit berechtigt bzw. verborgen werden kann.

Annahme: Es gibt zwei Kinderuntersuchungshefte in der Kategorie "childsrecord". Wenn der Versicherte lediglich ein Kinderuntersuchungsheft freigeben möchte, hat er zwei Möglichkeiten.

1. Über die kategorienbasierte Berechtigung kann er generell den Zugriff auf beide Kinderuntersuchungshefte gewähren und additiv einen über eine Denylist (Folder.entryUUID) sperren.
2. Über die dokumentenspezifische Berechtigung kann nur ein Kinderuntersuchungsheft in einer Allowlist freigeben werden.

A_21650 - Komponente ePA-Dokumentenverwaltung – Ein Dokument darf nicht gleichzeitig auf Deny- und Allowlist stehen.

Die Komponente ePA-Dokumentenverwaltung MUSS unterbinden, dass Dokumente in demselben Policy Document gleichzeitig auf der Denylist und der Allowlist aufgeführt werden. Liegt eine Verletzung vor, MUSS die Komponente ePA-Dokumentenverwaltung die Registrierung des Policy Document ablehnen, die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und den InvalidDocumentContent-Fehlercode mit der UniqueID des Policy Document zurückgeben. [<=]

A_21695-01 - Komponente ePA-Dokumentenverwaltung – Ablehnung einer zu registrierenden Policy bei Verletzung der Zugriffsunterbindungsregeln

Die Komponente ePA-Dokumentenverwaltung MUSS anhand der ProfessionOID sowie die Telematik-ID der zu registrierenden Policy prüfen, ob eine Verletzung der Zugriffsunterbindungsregeln vorliegt. Liegt eine Verletzung vor, MUSS die Komponente ePA-Dokumentenverwaltung die Registrierung des Policy Document ablehnen und den IHE-Fehlercode `PolicyViolation` mit der UniqueID des Policy Document zurückgeben. Eine Ausnahme bei dieser Prüfvorgabe ist eine Vertreter-Berechtigung. [\leq]

A_19303-08 - Komponente ePA-Dokumentenverwaltung – Zugriffsunterbindungsregeln

Die Komponente ePA-Dokumentenverwaltung MUSS alle in der Tabelle Tab_Dokv_030 - Zugriffsunterbindungsregeln aufgeführten Regeln durchsetzen sowie beim Aufruf einer der Operationen der Schnittstelle `I_Document_Management` die übergebene Authentication Assertion dahingehend prüfen, ob die `ProfessionOID` der Zertifikats-Extension `Admission` gemäß [gemSpec_PKI#Anhang A] im Signaturzertifikat C.HCI.OSIG (`/saml2:Assertion/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate`) für die Operation, ausgeführt auf eine bestimmte Dokumentenkategorie, zugriffsberechtigt ist. Das Ausführen von Operationen auf Dokumentenkategorien, die nicht explizit erlaubt sind, muss verhindert werden ("Access Deny"). Ferner MUSS auch das Registrieren von Policy Documents durch die Komponente ePA-Dokumentenverwaltung verhindert werden, wenn inhaltlich die Zugriffsunterbindungsregeln verletzt werden (vgl. A_21695).

Tabelle 31: Tab_Dokv_030 - Zugriffsunterbindungsregeln

Dokumentenkategorie gemäß § 341 PDSG Absatz 2		Zugriffsrecht												
Nr.	Technischer Identifier	Arzt	ZArzt	Apo	Psych	Pflege	Heb a	Phy s	GD	AM	KT R	Ver	Di GA	
1a 1	practitioner	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-	
1a 2	hospital	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-	
1a 3	laboratory	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-	
1a 4	physiotherapy	CR UD	CR UD	R	CR UD	R	R	CR UD	CR UD	R	-	RDM	-	
1a 5	psychotherapy	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-	
1a 6	dermatology	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-	

1a7	gynaecology_urology	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-
1a8	dentistry_oms	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-
1a9	other_medical	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-
1a10	other_non_medical	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-
1b	emp	CR UD	CR UD	CR UD	CR UD	R	R	R	CR UD	R	-	RDM	-
1c	nfd	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-
1d	eab	CR UD	CR UD	R	CR UD	R	R	R	CR UD	R	-	RDM	-
2	dentalrecord	CR UD	CR UD	-	CR UD	R	-	-	CR UD	R	-	RDM	-
3	childsrecord	CR UD	CR UD	R	CR UD	R	CR UD	R	CR UD	R	-	RDM	-
4	mothersrecord	CR UD	CR UD	R	CR UD	R	CR UD	R	CR UD	R	-	RDM	-
5	vaccination	CR UD	CR UD	CR UD	CR UD	R	R	-	CR UD	CR UD	-	RDM	-
6	patientdoc	RD	RD	R	RD	R	R	R	RD	R	-	CRUDM	-
7	ega	RD	RD	R	RD	R	R	R	RD	R	-	CRUDM	-
8	receipt	RD	RD	RD	RD	R	R	R	RD	R	CU	RDM	-
9	diga	R	R	R	R	R	R	R	R	R	-	RDM	CU
10	care	CR UD	CR UD	R	CR UD	CRUD	R	R	CR UD	R	-	RDM	-
11	prescription	CR UD	CR UD	CR UD	CR UD	R	R	R	CR UD	R	-	RDM	-

12	eau	CR UD	CR UD	-	CR UD	-	-	-	CR UD	R	-	RDM	-
13	other	CR UD	CR UD	-	CR UD	-	-	-	CR UD	R	-	RDM	-

Legende der Zugriffsrechte CRUD, Zuordnung zur Operation:

- C (create) = I_Document_Management::CrossGatewayDocumentProvide, 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::RegistryStoredQuery, I_Document_Management_Insurant::RetrieveDocumentSet;
- U (update) = Document Replacement (über urn:ihe:iti:2007:AssociationType: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::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;
- DIGA=oid_diga;

Legende Zugriffsberechtigte, Zuordnung über KVNR:

- Ver = Versicherter/Vertreter;

Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann der Versicherte bzw. sein Vertreter (erkennbar über die Vorlage einer KVNR in der Authentication

Assertion) oder eine Leistungserbringerinstitution gemäß der zuvor genannten Liste definierter professionOIDs sein. Sofern ein Versicherter/Vertreter der EInsteller der Elternnotiz ist, darf er abweichend von den oben aufgeführten Zugriffsunterbindungsregeln in die Dokumentenkategorie mit dem technischen Identifier childsrecord schreiben. [≤]

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_20736-06 - Komponente ePA-Dokumentenverwaltung – Generelles schreibendes Zugriffsrecht für Leistungserbringerinstitutionen oder Kostenträger

Die Komponente ePA-Dokumentenverwaltung MUSS einen schreibenden Zugriff ("Create" und "Update") gemäß der Zugriffsunterbindungsregeln in A_19303 bei einem vorliegenden und gültigen Policy Document gemäß A_15442 für berechnigte LEI bzw. A_17460 für berechnigte Kostenträger zulassen. Für das Schreiben eines MIO-Eintrags der Sammlungstypen "mixed" oder "uniform" durch eine Leistungserbringerinstitution MUSS ein Zugriffsrecht zum zugehörigen MIO über ein Policy Document durch den Versicherten oder seinen berechnigten Vertreter vergeben worden sein, um das generelle Schreibrecht zu legitimieren. Damit ist vor einem Schreibvorgang eine fachliche Bewertung durch ein vorheriges Herunterladen des Passdokuments gewährleistet.

Kann der Zugriff entsprechend dieser Autorisierungsprüfung nicht gewährt werden, MUSS die Komponente ePA-Dokumentenverwaltung das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem IHE-Fehlercode `DocumentAccessNotAuthorized` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die UUID (`DocumentEntry.entryUUID`) des identifizierten Dokuments angegeben werden.

[≤]

A_22998 - Komponente ePA-Dokumentenverwaltung – Entscheidungsbaum zur Sichtbarkeit von Ordnern bei FindFolders

Die Komponente ePA-Dokumentenverwaltung MUSS bei der XDS-Operation FindFolders die Zugriffsregeln entsprechend dem Entscheidungsbaum in der folgenden Abbildung

berücksichtigen.

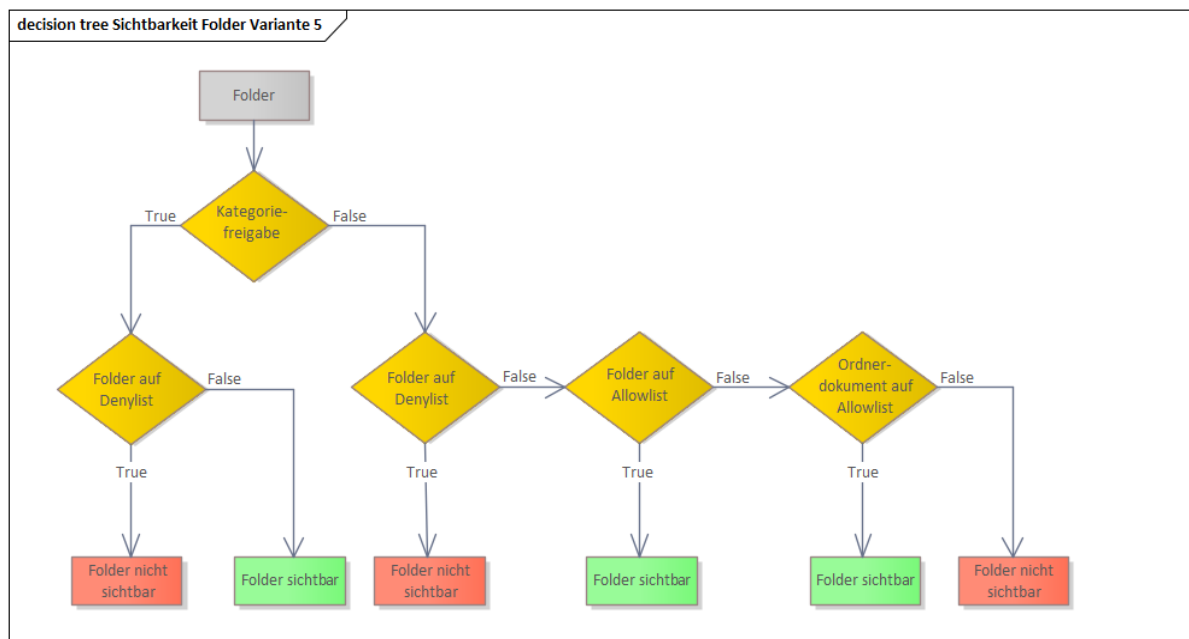


Abbildung 5: Entscheidungsbaum zu Sichtbarkeit von Foldern

Als Ergebnis der Operation dürfen nur Ordner geliefert werden, die entsprechend dem Entscheidungsbaum sichtbar sind. [≤]

5.4.2 Anforderungen an die Zugriffskontrollprüfung

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-* hinaus den Zugriff auf die Operationen der Schnittstellen I_Account_Management_Insurant und I_Key_Management_Insurant erlauben. [≤]

A_19998-01 - Zugriff durch Vertreter auf Operation

I_Account_Management_Insurant::GetAuditEvents und GetSignedAuditEvents

Die Komponente ePA-Dokumentenverwaltung MUSS einem berechtigten Vertreter des Versicherten über A_15173-* hinaus den Zugriff auf die Operation

I_Account_Management_Insurant::GetAuditEvents() und

I_Account_Management_Insurant::GetSignedAuditEvents() erlauben.

[≤]

A_14822-02 - 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 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)
- ggf. Metadaten des DocumentEntry (u.a. confidentialityCode), des dazugehörigen SubmissionSets und etwaiger verbundener Ordner

[<=]

5.4.2.1 Erstmaliges Öffnen eines Verarbeitungskontextes

Beim erstmaligen Öffnen des Verarbeitungskontextes eines neu registrierten Aktenkontos durch den Versicherten muss dieser erkennen, dass er erstmalig geöffnet wird und die Aktenzustände "Registered" und "Registered for Migration" gemäß [\[gemSpec_Aktensystem#6.1.1\]](#) unterscheiden. Darüber hinaus ist der Verarbeitungskontext für den Versicherten 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. [<=]

Die Festlegung des Zeitpunkts der Personalisierung verhindert die Personalisierung eines Verarbeitungskontexts für den Fall, dass für ein mit der Option "Registered for Migration" registriertes Aktenkonto der Verarbeitungskontext geöffnet wird, ohne dass unmittelbar anschließend die Operation `I_Account_Management_Insurant::ResumeAccount` aufgerufen wird. Der Verarbeitungskontext verbleibt damit in seinem initialen (d.h. ungenutzten) Zustand, so dass der Vorgang konsistent neu gestartet werden kann.

5.4.2.2 Berechtigung für einen Vertreter

A_15440-02 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Document zur Berechtigung eines Vertreters

Die Komponente ePA-Dokumentenverwaltung MUSS ein vom ePA-Frontend des Versicherten übermitteltes Policy Document gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt der Policy-Definition [\[gemSpec_ePA_Policy_Vertreter\]](#) prüfen. [<=]

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. [<=]

5.4.2.3 Berechtigung für eine Leistungserbringerinstitution

A_15442-03 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Document zur Berechtigung einer Leistungserbringerinstitution

Die Komponente ePA-Dokumentenverwaltung MUSS ein vom ePA-Frontend des Versicherten bzw. vom Fachmodul ePA übermitteltes Policy Document gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt der Policy-Definition in [gemSpec_ePA_Policy_LEI] prüfen.

[<=]

5.4.2.4 Berechtigung für einen Kostenträger

A_17460-02 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Document zur Berechtigung eines Kostenträgers

Die Komponente ePA-Dokumentenverwaltung MUSS ein vom ePA-Frontend des Versicherten übermitteltes Policy Document gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in der Policy Definition in [gemSpec_ePA_Policy_KTR] prüfen.[<=]

5.4.2.5 Berechtigung für eine DiGA

A_22705 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Document zur Berechtigung einer DiGA

Die Komponente ePA-Dokumentenverwaltung MUSS ein vom ePA-Frontend des Versicherten übermitteltes Policy Document gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in der Policy Definition in [gemSpec_ePA_Policy_DiGA] prüfen.[<=]

Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner gesammelt. Das Anlegen eines DiGA-Ordners erfolgt durch die Dokumentenverwaltung unter der Voraussetzung, dass es eine gültige DiGA-Policy gibt. Der DiGA-Ordner wird von der Dokumentenverwaltung mit der Telematik-ID der DiGA verknüpft. Für jede berechnete DiGA wird je ein Policy Document im Aktenkonto verwaltet. Bei der Erstellung des DiGA-Ordners verwendet die Dokumentenverwaltung den Wert für Folder.title aus der DiGA-Policy (PolicySet/Description). und belegt den Wert für Folder.comment mit urn:gematik:diga:<telematikID>.

Den Namen der DiGA hat das FdV bei der Erstellung der Berechtigung für die DiGA aus dem DiGA-Zertifikat, Wert von subject/commonName <Name der Verordnungseinheit der DiGA>, entnommen.

Die Zuordnung von DiGA-Dokumenten beim Schreiben erfolgt implizit über die TelematikID der Authentication Assertion im Aktensystem. Da ein DiGA-Ordner im Titel immer den Namen der DiGA enthält kann ein Client (z.B. LEI) darüber die relevante DiGA auswählen und auf die Dokumente der DiGA, sofern eine Berechtigung für den Nutzer vorliegt, lesend zugreifen.

Ein Update eines bestehenden Dokuments mit der bekannten DocumentEntry.entryUUID kann durch einen DiGA-Client erfolgen. Hierzu ist es erforderlich, dass ein DiGA-Client die DocumentEntry.entryUUID persistiert und keine symbolischen IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] verwendet.

5.4.3 Upgrade von ePA 1 auf ePA 2

Bei einem Upgrade von ePA 1 auf ePA 2 ändert sich das Berechtigungssystem. Deshalb müssen zum einen Dokumentenmetadaten (d.h. confidentialityCode) und zum anderen die Berechtigungsregeln selbst (Policy Documents) angepasst werden. Davon sind nicht nur neue Dokumente betroffen, sondern es müssen auch bestehende Metadaten und das jeweilige Policy Document angepasst werden.

Im Ergebnis akzeptiert die ePA-Dokumentenverwaltung in ePA 2 alte Policy Documents und Dokumente mit alten confidentialityCodes (beides gemäß ePA 1), liefert nach außen jedoch beides nur nach neuen Vorgaben gemäß ePA 2 zurück. Dieses Verhalten soll es insbesondere Primärsystemen nach alter Spezifikation erlauben, mit einem aktuellen ePA-Aktensystem zu kommunizieren.

A_20039-02 - Komponente ePA-Dokumentenverwaltung – Transformation eines Policy Document

Die Komponente ePA-Dokumentenverwaltung MUSS alle ePA 1 Policy Documents beim Öffnen des Verarbeitungskontextes gemäß A_20049-* transformieren. Die Policy-Definition in Anhang B (ePA1-Policies) MUSS in eine Policy-Definition aus [gemSpec_ePA_Policy_LEI], [gemSpec_ePA_Policy_KTR] sowie [gemSpec_ePA_Policy_Vertreter] (ePA2-Policies) umgewandelt werden, sobald die Zugriffsberechtigung des Anfragenden geprüft wird. [\leq]

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

A_20049-06 - Komponente ePA-Dokumentenverwaltung – Regeln für die Policy-Transformation

Bei der Transformation des Policy Document ohne die Versionsangabe @Version (ePA1-Policies) MUSS das vom Client eingestellte Policy Document durch ein Policy Document mit Versionsangabe @Version (ePA2-Policy) gemäß der Policy-Definitionen in [gemSpec_ePA_Policy_LEI], [gemSpec_ePA_Policy_KTR] sowie [gemSpec_ePA_Policy_Vertreter] ersetzt werden. Bei der Transformation gelten folgende Vorgaben:

Das Ablaufdatum MUSS übernommen werden.

Bei LEI-, KTR- und Vertreter-Base-Policies muss der Name der Institution bzw. des Vertreters aus //PolicySet/Target/Subjects[2]/SubjectMatch/AttributeValue stattdessen nach //PolicySet/Description übernommen werden (Hinweis: das Element Subjects[2]) wird durch die Description abgelöst). Bei einer LEI- und KTR-Base-Policy muss nach dem Namen der Institution gefolgt von einem Doppelpunkt die ProfessionOID angehängt werden. Die ProfessionOID wird gebildet:

Extraktion aus der Authentication Assertion oder

Mapping des Präfix der Telematik-ID wie folgt: 1=oid_praxis_arzt, 2=oid_zahnarztpraxis, 3=oid_öffentliche_apotheke, 4=oid_praxis_psychotherapeut, 5=oid_krankenhaus, 8=oid_epa_ktr;

Bei der Transformation einer LEI-Base-Policy MÜSSEN folgende Zugriffsregeln in einer Policy-Definitionen aus [gemSpec_ePA_Policy_LEI] umgesetzt werden (Zugriffsrecht alt wird zu Zugriffsrecht neu):

alt: LEI, neu: die Kategorien 1a*, 1b (emp), 1c (nfd), 1d (eab), 13 (other) nur dann wenn die zu berechtigende LEI keine Apotheke (oid_oeffentliche_apotheke) ist.

alt: PAT, neu: patientdoc;

alt: KTR, neu: receipt;

neu: Die Vertraulichkeitsstufe "normal" MUSS in der Policy gesetzt werden.

Bei der Transformation einer KTR-Base-Policy MUSS ein Policy Document gemäß [gemSpec_ePA_Policy_KTR] angelegt werden.
Bei der Transformation einer Vertreter-Base-Policy MUSS ein Policy Document gemäß [gemSpec_ePA_Policy_Vertreter] angelegt werden.

Etwaige Dokumente MÜSSEN gemäß A_19388 den Ordnern entsprechend der Dokumentenkategorie zugewiesen werden.

[<=]

A_20046-04 - Komponente ePA-Dokumentenverwaltung – Ergänzung des confidentialityCodes bei eingestellten Dokumenten

Die Komponente ePA-Dokumentenverwaltung MUSS mit dem Update auf ePA 2.0 bei allen Dokumenten eines Versicherten, bei denen der confidentialityCode auf "PAT" gesetzt ist, diese Dokumente dem Folder "patientdoc" (gemäß A_19388, Tab_DM_Dokumentenkategorien, Zeile Nr. 6) zuordnen. Die Komponente ePA-Dokumentenverwaltung MUSS bei allen Dokumenten eines Versicherten, bei denen der confidentialityCode "PAT", "LEI", "LEÄ" oder "KTR" gesetzt ist, den confidentialityCode "normal"="N" setzen. Diese Ergänzung MUSS durch die Komponente ePA-Dokumentenverwaltung nach dem ersten erfolgreichen Öffnen der Akte des Versicherten (Operation I_Document_Management_Connect::OpenContext()) und nachfolgend beim Einstellen jedes DocumentEntry, der noch alte confidentialityCodes enthält, durchgeführt werden, solange es am DocumentEntry noch keine der ConfidentialityCodes "N", "R" oder "V" gibt.

[<=]

Damit soll die Transformation zum frühestmöglichen Zeitpunkt durch die ePA-Dokumentenverwaltung durchgeführt werden.

A_20050-02 - Komponente ePA-Dokumentenverwaltung – Abbildung von Suchanfragen nach confidentialityCodes und deren Ergebnisse

Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS bei Aufrufen der Operationen I_Document_Management::CrossGatewayQuery und I_Document_Management_Insurant::RegistryStoredQuery 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 zurück liefern:

- alt: LEI, neu: practitioner, hospital, laboratory, physiotherapy, psychotherapy, dermatology, gynaecology_urology, dentistry_oms, other_medical, other_non_medical, other, emp, nfd, eab;
- alt: PAT, neu: patientdoc;
- alt: KTR, neu: receipt.

[<=]

Etwaige Berechtigungsregeln, die der Herausgabe einzelner Dokumente an den Client entgegenstehen (z. B. Denylisting einzelner Dokumente oder nicht erteilte Zugriffsberechtigung auf emp) müssen dabei weiterhin berücksichtigt werden.

5.4.4 Simulierte Berechtigung

A_21705 - Komponente ePA-Dokumentenverwaltung – Simulation der lesbaren Dokumente für eine Leistungserbringerinstitution

Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS ein Policy Document anhand der XDS-Metadaten gemäß [gemSpec_DM_ePA#A_14961-*] verarbeiten. Ist anhand der Metadaten SubmissionSet.contentTypeCode = "simulatedAuthorization" erkennbar, dass es eine simulierte Berechtigungsanfrage eines ePA-FdVs ist, MUSS die Komponente ePA-Dokumentenverwaltung mögliche Dokumente identifizieren, welche durch dieses Policy Document durch die Leistungserbringerinstitution lesbar sind oder bei potentieller Registrierung lesbar wären. Das Policy Document DARF NICHT dauerhaft gespeichert werden. Weiterhin MUSS der Submission Request mit einem InvalidDocumentContent-Fehlercode sowie HTTP-Statuscode 200 beantwortet werden. Pro identifiziertes Dokument MUSS ein RegistryError-Element mit der UniqueID des Dokuments (codeContext) und des InvalidDocumentContent-Fehlercode (code) zurückgegeben werden. [\leq]

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. [\leq]

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

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

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

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

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

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

A_15540 - Komponente ePA-Dokumentenverwaltung – TLS-Schnittstelle I_Document_Management_Connect

Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die Schnittstelle `I_Document_Management_Connect` für TLS-Verbindungen des Fachmoduls ePA sowie des Fachmoduls ePA KTR-Consumer verfügbar machen.[<=]

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

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

A_14633-03 - Komponente ePA-Dokumentenverwaltung – Vermittlung der Verbindung zwischen Client und Verarbeitungskontext

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

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

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

[<=]

A_21746-01 - Komponente ePA-Dokumentenverwaltung – Zulässige Operationen bei Betreiberwechselautorisierung

Die ePA-Dokumentenverwaltung MUSS die folgenden Prüfungen durchführen, wenn die Autorisierung mit einer Betreiberwechselautorisierung (AuthorizationType der Authorization Assertion = "ACCOUNT_AUTHORIZATION") erfolgt ist:

- In den Zuständen START_MIGRATION und SUSPENDED des Aktensystems des authentifizierten Nutzers ist als auszuführende Operation nur suspendAccount möglich.
- In den Zuständen REGISTERED_FOR_MIGRATION und DL_IN_PROGRESS des Aktensystems des authentifizierten Nutzers ist als auszuführende Operation nur resumeAccount möglich.
- Im Zustand READY_FOR_IMPORT des Aktensystems des authentifizierten Nutzers darf kein Operationsaufruf erfolgen. Lediglich beim Öffnen des Verarbeitungskontext darf der Import des bereits heruntergeladenen Migrationspakets erfolgen.

Sofern keine dieser Bedingungen erfüllt ist, MUSS die aufgerufene Operation mit dem Fehler ACCESS_DENIED beendet werden.[<=]

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

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

A_14617-02 - Komponente ePA-Dokumentenverwaltung – Ablauf des Verbindungsaufbaus

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

Tabelle 32: Tab_Dokv_29 - Ablauf Operation Hello

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden des HTTP Request mit VAUClientHello-Nachricht)
1	Kontextmanagement	Prüfen der Authorization Assertion der VAUClientHello-Nachricht auf Gültigkeit gemäß Anforderung A_13690-* und Abbruch des Verbindungsaufbaus mit HTTP-Fehler 403

		(Fehlermeldung "Access Denied") bei ungültiger Authorization Assertion.
2	Kontextmanagement	Extrahieren des Record Identifiers über den Wert des Attributs <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 <code>VAUClientSigFin</code> -Nachricht)
10	Kontextmanagement	Weiterleiten der <code>VAUClientSigFin</code> -Nachricht an den Verarbeitungskontext für den <code>RecordIdentifier</code> Record Identifier
11	Verarbeitungskontext	Prüfen auf Identität des authentifizierten Nutzers (Subject::Subject-id bzw. Subject::Organization-id der Authorization Assertion entspricht der KVRN bzw. Telematik-ID des übergebenen Zertifikats der Client-Authentisierung gemäß [gemSpec_Krypt#A_17070-*]) Im Fehlerfall MUSS der Verbindungsaufbau abgebrochen und mit einer <code>VAUServerError</code> -Nachricht beantwortet werden.

12	Verarbeitungskontext	Erzeugen der VAU _{ServerFin} -Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
13	Kontextmanagement	Weiterleiten der VAU _{ServerFin} -Nachricht an den Client

[<=]

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_14545-05 - Komponente ePA-Dokumentenverwaltung – Operationen des Dokumenten-, Konto- und Schlüsselmanagements nur über sicheren Kanal

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

- I_Document_Management::CrossGatewayDocumentProvide
- I_Document_Management::CrossGatewayQuery
- I_Document_Management::RemoveMetadata
- I_Document_Management::RemoveDocuments
- I_Document_Management::CrossGatewayRetrieve
- I_Document_Management::RestrictedUpdateDocumentSet
- I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::RestrictedUpdateDocumentSet
- I_Document_Management_Insurant::RegistryStoredQuery
- I_Document_Management_Insurant::RemoveDocuments
- I_Document_Management_Insurant::RemoveMetadata
- I_Document_Management_Insurant::RetrieveDocumentSet
- I_Account_Management_Insurant::GetAuditEvents
- I_Account_Management_Insurant::GetSignedAuditEvents
- I_Account_Management_Insurant::SuspendAccount
- I_Account_Management_Insurant::ResumeAccount
- I_Key_Management_Insurant::StartKeyChange
- I_Key_Management_Insurant::GetAllDocumentKeys
- I_Key_Management_Insurant::PutAllDocumentKeys
- I_Key_Management_Insurant::FinishKeyChange
- I_Document_Management_Connect::OpenContext
- I_Document_Management_Connect::CloseContext

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

A_14645-01 - Komponente ePA-Dokumentenverwaltung – Nutzung des sicheren Kanals zwischen ePA-Frontend des Versicherten bzw. Fachmodul ePA, Fachmodul ePA KTR-Consumer und Verarbeitungskontext

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

A_14457 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management_Connect

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

Tabelle 33: Tab_Dokv_30 - Schnittstelle I_Document_Management_Connect

Schnittstelle	I_Document_Management_Connect	
Version	1.0.1	
Namensraum	http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Open Context	Übergabe des Kontextschlüssels vom Client an den Verarbeitungskontext der Akte
	Close Context	Beendigung der Client-Verbindung und ggf. Beendigung des Verarbeitungskontextes der Akte
WSDL	DocumentManagementConnectService.wsdl	
XML Schema	DocumentManagementConnectService.xsd	

[≤]

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 34: 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 35: Tab_Dokv_32 - Ablauf der Operation Open Context

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

		Fehlermeldung INVALID_AUT_KEY abgebrochen.
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.

A_22924 - Komponente ePA-Dokumentenverwaltung – Verwerfen ungültiger Policies

Die Komponente ePA-Dokumentenverwaltung MUSS unmittelbar nach dem Öffnen des Verarbeitungskontexts die Policies-Files auf ungültige/veraltete Policies prüfen und diese verwerfen/löschen.[<=]

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 36: 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 37: 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 Nutzung der Akte angelegt, d.h. bevor auf Akteninhalte zugegriffen wird. Sie sind unveränderlich.

A_20191-05 - Komponente ePA-Dokumentenverwaltung – Anlegen von statischen Ordnern

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

I_Document_Managemet_Connect::OpenContext()) folgende Kategorienordner aus A_19388-* und [ValueSet-Speciality] unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in gemSpec_DM_ePA#A_14760-* (Belegung der restlichen Metadatenfelder) für den Versicherten anlegen. Alle statischen Kategorienordner werden mit jeweils einem Ordner pro Kategorie angelegt. Alle statischen Ordner sind nach dem Anlegen initial leer.

Das Anlegen von Submission Sets und zugehöriger Associations zu den statischen Ordnern ist nicht vorgegeben. Das XDS-Informationsmodell MUSS allerdings hinsichtlich der Folder-DocumentEntry- sowie SubmissionSet-HasMember-Associations bei einer Verarbeitung durch die Document Consumer (z.B. Querying) erfüllt werden.

[<=]

Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner pro Kind bzw. Schwangerschaft, mit Folder.title für den Namen des Kindes bzw. ein Kennzeichen der Schwangerschaft.

A_20216-02 - Komponente ePA-Dokumentenverwaltung – Unveränderlichkeit von statischen Akteninhalten

Die Komponente ePA-Dokumentenverwaltung DARF die Metadaten eines statischen Aktenobjekts nach Abschnitt 5.6 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen. Dabei gelten folgende Ausnahmen:

- Folder.lastUpdateTime - Folder.lastUpdateTime wird automatisch von der Dokumentenverwaltung aktualisiert, sobald Dokumente in den Ordner eingestellt oder daraus gelöscht werden, siehe auch [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6].
- Während des Aktenumzugs MUSS bei einem Import eines Exportpakets (mitsamt der Ordner und zugehörigen Assoziationen) der statische Akteninhalt überschrieben werden.

[<=]

6 Informationsmodelle

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

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

Kürzel	Erläuterung
AdV	Anwendungen des Versicherten
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BPPC	Basic Patient Privacy Consents
CRUD	Create Read Update Delete
DiGA	Digitale Gesundheitsanwendung
ePA-FdV	ePA-Frontend des Versicherten
ePA-FdV AdV	ePA-Frontend des Versicherten im KTR-AdV-Terminal
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
KTR	Kostenträger

MIO	Medizinisches Informationsobjekt
MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
PDSG	Patientendaten-Schutz-Gesetz
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	16
Abbildung 2: Zustandsübergänge Schlüsselwechsel	103
Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen	120
Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen	121
Abbildung 5: Entscheidungsbaum zu Sichtbarkeit von Foldern	127
Abbildung 1: Komponentenzerlegung ePA-Dokumentenverwaltung	16
Abbildung 2: Zustandsübergänge Schlüsselwechsel	103
Abbildung 3: Schematische Darstellung zur Vergabe von Berechtigungen	120
Abbildung 4: Schematische Darstellung zum Entzug von Berechtigungen	121
Abbildung 5: Entscheidungsbaum zu Sichtbarkeit von Foldern	127

7.4 Tabellenverzeichnis

Tabelle 1: Tab_Dokv_10 – Kennzeichnung von Optionalitäten	25
Tabelle 2: Tab_Dokv_11 – Übersicht über gruppierte IHE ITI Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung	25
Tabelle 3: Tab_Dokv_12 – Fehlercodes zu Fehlern gemäß Operationsdefinition	33
Tabelle 4: Tab_Dokv_35 – Eingangsparameter für TUC_PKI_018	42
Tabelle 5: Tab_Dokv_13 – Parameter des § 291a-Protokolls	44
Tabelle 6: Tab_Dokv_14 – Schnittstelle I_Document_Management	53
Tabelle 7: Tab_Dokv_16 – Operation Cross-Gateway Query	58
Tabelle 8: Tab_Dokv_17 – Operation Remove Documents	62
Tabelle 9: Tab_Dokv_17 – Operation RemoveMetadata	63
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	69
Tabelle 13: Tab_Dokv_21 – Operation Provide And Register Document Set b	70
Tabelle 14: Tab_Dokv_22 – Operation Registry Stored Query	73
Tabelle 15: Tab_Dokv_23 – Operation RemoveDocuments	76
Tabelle 16: Tab_Dokv_23 – Operation RemoveMetadata	77
Tabelle 17: Tab_Dokv_24 – Operation Retrieve Document Set	79
Tabelle 18: Tab_Dokv_19 – Operation RestrictedUpdateDocumentSet	81
Tabelle 19: Tab_Dokv_36 – Schnittstelle I_Document_Management_Insurance	84
Tabelle 20: Tab_Dokv_37 – Operation Provide And Register Document Set b	85
Tabelle 21: Tab_Dokv_25 – Schnittstelle I_Account_Management_Insurant	88
Tabelle 22: Tab_Dokv_26 – Operation Suspend Account	89
Tabelle 23: Tab_Dokv_27 – Operation Resume Account	93
Tabelle 24: Tab_Dokv_28 – Operation Get Audit Events	97
Tabelle 25: Tab_Dokv_44 – Operation Get Signed Audit Events	99
Tabelle 26: Tab_Dokv_38 – Operation I_Key_Management_Insurant::StartKeyChange()	107
Tabelle 27: Tab_Dokv_39 – Operation I_Key_Management_Insurant::GetAllDocumentKeys()	110
Tabelle 28: Tab_Dokv_40 – Operation I_Key_Management_Insurant::PutAllDocumentKeys()	112
Tabelle 29: Tab_Dokv_41 – Operation I_Key_Management_Insurant::FinishKeyChange()	114
Tabelle 30: Tab_Dokv_42 – Zusätzliche Parameter des § 291a-Protokolls für die Umschlüsselung	116
Tabelle 31: Tab_Dokv_030 – Zugriffsunterbindungsregeln	123

Tabelle 32: Tab_Dokv_29 – Ablauf Operation Hello	134
Tabelle 33: Tab_Dokv_30 – Schnittstelle I_Document_Management_Connect	137
Tabelle 34: Tab_Dokv_31 – Operation OpenContext.....	138
Tabelle 35: Tab_Dokv_32 – Ablauf der Operation Open Context	139
Tabelle 36: Tab_Dokv_33 – Operation Close Context.....	140
Tabelle 37: Tab_Dokv_34 – Ablauf Operation CloseContext.....	141
Tabelle 38: Tab_Dokv_99 – Kennzeichnung von Optionalitäten in XACML 2.0 Policies..	155
Tabelle 39: Tab_Dokv_100 – XACML 2.0 Policy für einen Versicherten (Base Policy)....	155
Tabelle 40: Tab_Dokv_101 – XACML 2.0 Policy mit erlaubten Operationen für einen Versicherten (Permission Policy).....	158
Tabelle 41: Tab_Dokv_200 – XACML 2.0 Policy für einen Vertreter (Base Policy).....	189
Tabelle 42: Tab_Dokv_201 – XACML 2.0 Policy mit erlaubten Operationen für einen Vertreter (Permission Policy).....	193
Tabelle 43: Tabelle : Tab_Dokv_300_01 – XACML 2.0 Policy für eine Leistungserbringerinstitution (Base Policy).....	221
Tabelle 44: Tab_Dokv_301 – XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer Dokumente (Permission Policy)	226
Tabelle 45: Tab_Dokv_302 – XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten und Kostenträger- Dokumente (Permission Policy)	250
Tabelle 46: Tab_Dokv_400 – XACML 2.0 Policy für einen Kostenträger (Base Policy) ...	272
Tabelle 47: Tab_Dokv_401 – XACML 2.0 Policy mit erlaubten Operationen für einen Kostenträger (Permission Policy)	275
Tabelle 1: Tab_Dokv_10 - Kennzeichnung von Optionalitäten	25
Tabelle 2: Tab_Dokv_11 - Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung	25
Tabelle 3: Tab_Dokv_12 - Fehlercodes zu Fehlern gemäß Operationsdefinition	33
Tabelle 4: Tab_Dokv_35 - Eingangsparameter für TUC_PKI_018	42
Tabelle 5: Tab_Dokv_13 - Parameter des § 291a-Protokolls	44
Tabelle 6: Tab_Dokv_14 - Schnittstelle I_Document_Management	53
Tabelle 7: Tab_Dokv_16 - Operation Cross-Gateway Query	58
Tabelle 8: Tab_Dokv_17 - Operation Remove Documents.....	62
Tabelle 9: Tab_Dokv_17 - Operation RemoveMetadata	63
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.....	69
Tabelle 13: Tab_Dokv_21 - Operation Provide And Register Document Set-b	70
Tabelle 14: Tab_Dokv_22 - Operation Registry Stored Query	73

Tabelle 15: Tab_Dokv_23 - Operation RemoveDocuments	76
Tabelle 16: Tab_Dokv_23 - Operation RemoveMetadata	77
Tabelle 17: Tab_Dokv_24 - Operation Retrieve Document Set	79
Tabelle 18: Tab_Dokv_19 - Operation RestrictedUpdateDocumentSet	81
Tabelle 19: Tab_Dokv_36 - Schnittstelle I_Document_Management_Insurance	84
Tabelle 20: Tab_Dokv_37 - Operation Provide And Register Document Set-b	85
Tabelle 21: Tab_Dokv_25 - Schnittstelle I_Account_Management_Insurant	88
Tabelle 22: Tab_Dokv_26 - Operation Suspend Account	89
Tabelle 23: Tab_Dokv_27 - Operation Resume Account	93
Tabelle 24: Tab_Dokv_28 - Operation Get Audit Events	97
Tabelle 25: Tab_Dokv_44 - Operation Get Signed Audit Events	99
Tabelle 26: Tab_Dokv_38 - Operation I_Key_Management_Insurant::StartKeyChange()	107
Tabelle 27: Tab_Dokv_39 - Operation I_Key_Management_Insurant::GetAllDocumentKeys()	110
Tabelle 28: Tab_Dokv_40 - Operation I_Key_Management_Insurant::PutAllDocumentKeys()	112
Tabelle 29: Tab_Dokv_41 - Operation I_Key_Management_Insurant::FinishKeyChange()	114
Tabelle 30: Tab_Dokv_42 - Zusätzliche Parameter des § 291a-Protokolls für die Umschlüsselung	116
Tabelle 31: Tab_Dokv_030 - Zugriffsunterbindungsregeln	123
Tabelle 32: Tab_Dokv_29 - Ablauf Operation Hello	134
Tabelle 33: Tab_Dokv_30 - Schnittstelle I_Document_Management_Connect	137
Tabelle 34: Tab_Dokv_31 - Operation OpenContext	138
Tabelle 35: Tab_Dokv_32 - Ablauf der Operation Open Context	139
Tabelle 36: Tab_Dokv_33 - Operation Close Context	140
Tabelle 37: Tab_Dokv_34 - Ablauf Operation CloseContext	141
Tabelle 38: Tab_Dokv_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies ..	155
Tabelle 39: Tab_Dokv_100 - XACML 2.0 Policy für einen Versicherten (Base Policy)	155
Tabelle 40: Tab_Dokv_101 - XACML 2.0 Policy mit erlaubten Operationen für einen Versicherten (Permission Policy)	158
Tabelle 41: Tab_Dokv_200 - XACML 2.0 Policy für einen Vertreter (Base Policy)	189
Tabelle 42: Tab_Dokv_201 - XACML 2.0 Policy mit erlaubten Operationen für einen Vertreter (Permission Policy)	193
Tabelle 43 Tabelle : Tab_Dokv_300-01 - XACML 2.0 Policy für eine Leistungserbringereinstitution (Base Policy)	221
Tabelle 44: Tab_Dokv_301 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringereinstitution zum Zugriff auf Leistungserbringer-Dokumente (Permission Policy)	226

Tabelle 45: Tab_Dokv_302 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-Dokumente (Permission Policy)	250
Tabelle 46: Tab_Dokv_400 - XACML 2.0 Policy für einen Kostenträger (Base Policy) ...	272
Tabelle 47: Tab_Dokv_401 - XACML 2.0 Policy mit erlaubten Operationen für einen Kostenträger (Permission Policy)	275

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.

[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_IG_ePA]	gematik: Implementation Guides für strukturierte Dokumente (src/implementation_guides), https://github.com/gematik/api-ePA
[gemSpec_ePA_Policy_LEI]	gematik: XACML Policy Definition für Leistungserbringerinstitutionen "hcp-policy-definition.xml", https://github.com/gematik/api-ePA

[gemSpec_ePA_Policy_DiGA]	gematik: XACML Policy Definition für DiGAs "diga-policy-definition.xml", https://github.com/gematik/api-ePA
[gemSpec_ePA_Policy_KTR]	gematik: XACML Policy Definition für Kostenträger "insurance-policy-definition.xml", https://github.com/gematik/api-ePA
[gemSpec_ePA_Policy_Vertreter]	gematik: XACML Policy Definition für Vertreter "representative-policy-definition.xml", https://github.com/gematik/api-ePA
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_TBAuth]	gematik: Spezifikation Tokenbasierte Authentisierung
[gemSysL_ePA]	gematik: Systemspezifisches Konzept ePA
[RefImpl_Exportpaket]	gematik: Referenzimplementierung Exportpaket, https://github.com/gematik/ref-ePA-HealthRecordMigration
[KeyManagementService]	gematik: Schlüsselmanagement Umschlüsselung (src/schema/fd/phr/KeyManagementService.xsd), https://github.com/gematik/api-ePA
[ValueSet-Speciality]	gematik: Value Set für Berechtigungskategorien (src/vocabulary/value_sets/vs-specialty-oth.xml), https://github.com/gematik/api-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
[IHE-ITI-APPC]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Advanced Patient Privacy Consents (APPC), Revision 1.2 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf

[IHE-ITI-RMD]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.2 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-RMU]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.1 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf
[IHE-ITI-TF1]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Integration Profiles, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
[IHE-ITI-TF2a]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2a (ITI TF-2a) – Transactions Part A, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf
[IHE-ITI-TF2b]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf
[IHE-ITI-TF2x]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2x) – Volume 2 Appendices, Revision 15.1, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf
[IHE-ITI-TF3]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Transaction Specifications and Content Specifications, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf
[IHE-ITI-XCDR]	IHE International (2017): IHE IT Infrastructure (ITI) Technical Framework Supplement, Cross-Community Document Reliable Interchange (XCDR), Revision 1.4 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf

[MIO-UH]	Kassenärztliche Bundesvereinigung (2021): Kinderuntersuchungsheft, https://mio.kbv.de/display/UH
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[OWASP-SAML]	Open Web Application Security Project (OWASP) (2017): SAML Security Cheat Sheet, https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://datatracker.ietf.org/doc/html/rfc2119
[RFC5246]	IETF (2008): The Transport Layer Security (TLS) Protocol Version 1.2 https://datatracker.ietf.org/doc/html/rfc5246
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231, https://datatracker.ietf.org/doc/html/rfc7231
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), https://www.w3.org/TR/soap12-part1/
[WSA]	OASIS (2004): Web Services Addressing (WS-Addressing), https://www.w3.org/Submission/ws-addressing/
[WSIAP]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[WSIBSP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html

[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
[WSS-SAML]	OASIS (2006): Web Services Security: SAML Token Profile 1.1, https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLSecurityProfile.pdf
[XACML]	OASIS (2005): eXtensible Access Control Markup Language (XACML) Version 2.0, https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/

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 38: 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 39: Tab_Dokv_100 - XACML 2.0 Policy für einen Versicherten (Base Policy)

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

		Target	R	
		Subjects	R	
		Subject	R	
		SubjectMatch	R	
		@MatchId	R	Der Wert "urn: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:h17-org:v3#II" MUSS gesetzt werden.
				@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
<!-- KVN R als Aktenidentifikator -->						
				Resources	R	
				Resource	R	
				ResourceMatch	R	
				@MatchId	R	Der Wert "urn:h17-org:v3:function:II-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "urn:h17-org:v3#II" MUSS gesetzt werden.
				InstanceIdentifier	R	
				@xmlns	R	Der Wert "urn:h17-org:v3" MUSS gesetzt werden.
				@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
				@extension	R	Als Wert MUSS den unveränderbare Teil der KVN R (10 Stellen) gesetzt werden.
				ResourceAttributeDesignator	R	

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

8.1.2 Permission Policy

Tabelle 40: 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:hl7-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:hl7-org:v3#CV" MUSS gesetzt werden.
						@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
					Actions		R	

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.2 Policy Document für einen Vertreter

8.2.1 Base Policy

Tabelle 41: 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	
<!-- 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 42: 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:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:f26abbcb-ac74-4422-8a30-edb644bbc1a9" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:"

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.3 Policy Document für eine Leistungserbringerinstitution

8.3.1 Base Policy zum Zugriff auf Leistungserbringer-Dokumente

Tabelle 43 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	
<!-- 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#str ing" 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-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.
<!-- Gültigkeitszeitraum des Policy Documents -->							
					Environments	R	

				Environment	R	
				EnvironmentMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:date-greater-than-or-equal" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				text()	R	Der Wert muss dem Tag der Ausstellung (Format YYYY-MM-DD nach ISO 8601:2004) des Policy Documents entsprechen.
				EnvironmentAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				EnvironmentMatch	R	
				@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:date-greater-than" MUSS gesetzt werden.
				AttributeValue	R	
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
				text()	R	Der Wert muss dem Enddatum (Format YYYY-MM-DD nach ISO 8601:2004) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen: "heute"

											+ frei eintragbare Anzahl Tage in der Spanne von 1 bis 540
									EnvironmentAttributeDesignator	R	
									@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: environment:current-date" MUSS gesetzt werden.
									@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
									PolicySetIdReference	R	
									text()	R	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. Es muss mindestens ein und maximal drei der folgenden Werte gesetzt werden: <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 44: Tab_Dokv_301 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Leistungserbringer-Dokumente (Permission Policy)

Element-, Attribut- oder Textknoten gemäß [XACML]		Op t.	Nutzungsvorgabe
PolicySet		R	
	@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp" MUSS gesetzt werden.
	@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
Target		R	Das Element MUSS leer bleiben.
Policy		R	
	@PolicyId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
	@RuleCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Target	R	
	Resources	R	

					Resource	R	
					ResourceMatch	R	
					@MatchId	R	Der Wert "urn: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 "LEI" MUSS gesetzt werden.
					@codeSystem	R	Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.
					@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
					@displayName	O	Der Wert "Dokument einer Leistungserbringereinstitution" MUSS gesetzt werden.
					ResourceAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti: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	
<!-- '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/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:14d4debf- 8f97-4251-9a74-

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

					@DataType	R	Der Wert "http://www.w3.org/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.

							equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3" MUSS gesetzt werden.

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

					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:5c4f972b- d56b-40ac-a5fc- c8ca9b40b9d4" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAssociations' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	

					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
				ActionMatch		R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
				AttributeValue		R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155" MUSS gesetzt werden.
				ActionAttributeDesignator		R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:"

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

							xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/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:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/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/2 001/XMLSchema#anyURI " MUSS gesetzt werden.

						text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
						ActionAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
						ActionMatch	R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
						AttributeValue	R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
						text()	R	Der Wert "urn:uuid:51224314-5390-4169-9b91-b1980040715a" MUSS gesetzt werden.
						ActionAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2

							001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- 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/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:e8e3cb2c-e39c-46b9-99e4-c12f57260b83" " MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" " MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
<!-- Registry Stored Query 'GetRelatedDocuments' -->							
					Action	R	
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" " MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" " MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" " MUSS gesetzt werden.

					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc: xacml:1.0: function:anyURI- equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:d90e5407- b356-4d91-a89f- 873917b4b0e6" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:ihe:iti:2016: RegistryStoredQuery: queryId" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByReferenceId' -->							

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

					ActionAttribut eDesignator				R	
						@Attri buteId			R	Der Wert "urn:oasis:names:tc: xacml:1.0: action:action-id" MUSS gesetzt werden.
						@Data Type			R	Der Wert "http://www.w3.org/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.
					AttributeValu e				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	
						@Attri buteId			R	Der Wert "urn:ihe:iti:2016:Re gistryStoredQuery: queryId" MUSS gesetzt werden.
						@Data Type			R	Der Wert "http://www.w3.org/2

									001/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/2 001/XMLSchema#anyURI " MUSS gesetzt werden.
							text()		R	Der Wert "urn:ihe:iti:2017:Re moveDocuments" 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/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayRetrieve" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					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 45: 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]	O p t.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	<p>Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents" MUSS gesetzt werden, sofern dieses Policy Set den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden.</p> <p>Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents" MUSS gesetzt werden, sofern dieses Policy Set den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden.</p>
@PolicyCombiningAlgId	R	<p>Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.</p>
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</p> <p>(@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</p> <p>(@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents").</p>
							@codeSystem	R	<p>Der Wert "1.2.276.0.76.5.491" MUSS gesetzt werden.</p>
							@codeSystemName	R	<p>Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.</p>

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

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

						text()	R	Der Wert "urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d" MUSS gesetzt werden.
						ActionAttributeDesignator	R	
						@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery:queryId" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindSubmissionSets' -->								
						Action	R	
						ActionMatch	R	
						@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
						AttributeValue	R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007: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:f26abbc-b- ac74-4422-8a30- edb644bbcb1a9" 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/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'GetAll' -->							
				Action		R	
				ActionMatch		R	
				@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.

					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					ActionMatch	R	
					@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3" MUSS gesetzt werden.
					ActionAttributeDesignator	R	

						@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: queryId" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/200 1/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/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:Cros sGatewayQuery" 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/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
						ActionMatch	R	

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

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

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

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

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

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

					AttributeValue	R	
					@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
					text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayQuery" MUSS gesetzt werden.
					ActionAttributeDesignator	R	
					@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
					@DataType	R	Der Wert "http://www.w3.org/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/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocumentsByTitle' -->								
			Ac tio n				R	
				Actio nMat ch			R	
					@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeVal ue		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.
					ActionAttrib uteDesignat or		R	
					@AttributeI d		R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.

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

					@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeValue		R	
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2007:CrossGatewayRetrieve" MUSS gesetzt werden.
					ActionAttributeDesignator		R	
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0: action:action-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RemoveDocuments -->								
			Ac tio n				R	
				Actio nMat ch			R	
					@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0: function:anyURI-equal" MUSS gesetzt werden.
					AttributeVal ue		R	

						@Dat aType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
						text()	R	Der Wert "urn:ihe:iti:2017:Remo veDocuments" MUSS gesetzt werden.
					ActionAttrib uteDesignat or		R	
						@Attr ibuteId	R	Der Wert "urn:oasis:names:tc:xa cml:1.0: action:action-id" MUSS gesetzt werden.
						@Dat aType	R	Der Wert "http://www.w3.org/200 1/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- RestrictedUpdateDocumentSet -->								
				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:2018:Rest rictedUpdateDocuments et" 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 46: 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	

<!-- Kostenträger (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 des Kostenträgers gesetzt werden.
				SubjectAttributeDesignator	R	
				@AttributeId	R	Der Wert "urn:oasis:names:tc:xspa:1.0:subject:organization" MUSS gesetzt werden.
				@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- 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.
				PolicySetIdReference	R	
				text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-insurance" MUSS gesetzt werden.

8.4.2 Permission Policy

Tabelle 47: 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:appc:2016:confidentiality-code" MUSS gesetzt werden.
				@DataType	R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
				@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
				Actions	R	
<!-- 'ProvideAndRegisterDocumentSet-b' -->						
				Action	R	

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