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

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation ePA-Dokumentenverwaltung

Version:	1.45.0 CC
Revision:	~~199199~~230700
Stand:	~~02.03~~30.04.2020
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
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		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: 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 Umgekehrt wurden übergreifende Afos nach Kapitel 4 verschoben und Afo-Duplikate storniert 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	gematik
1.2.0	28.06.19		Einarbeitung Änderungsliste P19.1	gematik
			Einarbeitung Änderungsliste P20.1/2	gematik
1.3.0	02.10.19		freigegeben	gematik

1.4.0	02.03.20		freigegeben	gematik
1.5.0 CC	30.04.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik

Inhaltsverzeichnis

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 berechtigte Nutzer. Diese sind der Versicherte selbst oder von ihm benannte Vertreter sowie Leistungserbringerinstitutionen.

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-Modul Frontend des Versicherten werden durch das Zugangsgateway TI an das Kontextmanagement weitergeleitet. Das Kontextmanagement steuert die Instanziierung der Verarbeitungskontexte und leitet Anfragen der Clients an diese weiter.

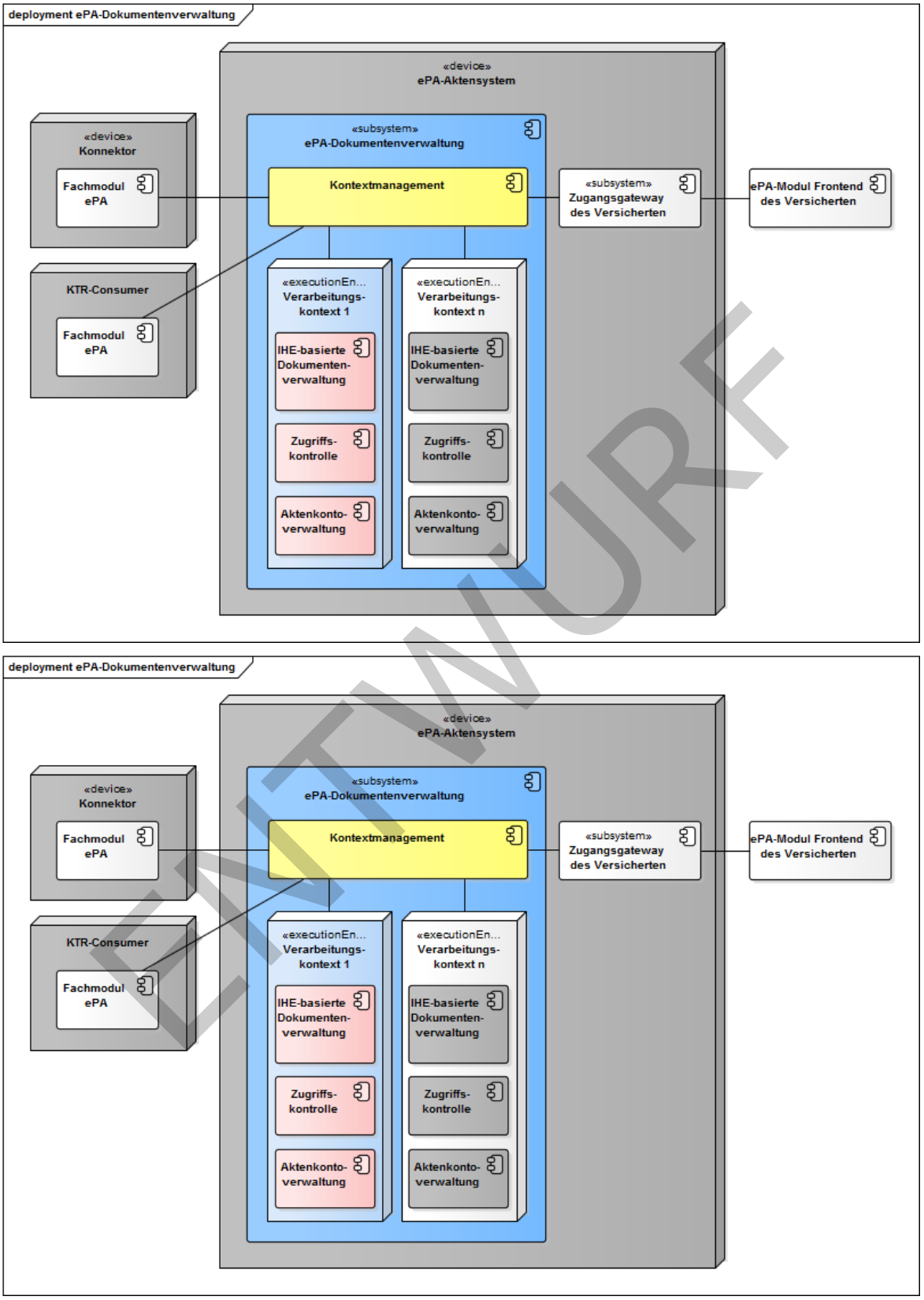

Abbildung 1: Komponentenzerlegung ePA-Dokumentenverwaltung

4 Übergreifende Festlegungen

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

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

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

4.1 Namensräume

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

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

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

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

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

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

A_17826 - Komponente ePA-Dokumentenverwaltung – Außenverhalten der IHE ITI-Implementierung
Die Komponente ePA-Dokumentenverwaltung DARF NICHT vom Verhalten der definierten Außenschnittstellen `I_Document_Management`, `I_Document_Management_Insurance` sowie `I_Document_Management_Insurant` aus Abschnitt 5.1 abweichen. Dies schließt von Abschnitt 4.2.1 hinausgehende Implementierungen von IHE ITI-Akteuren und Optionen innerhalb der Komponente ePA-Dokumentenverwaltung mit ein, sodass zusätzlich implementierte IHE-Funktionalitäten keine Auswirkungen an den definierten Außenschnittstellen aufweisen dürfen. Ferner DARF zusätzliche IHE-Funktionalität Nachrichten an Komponenten außerhalb der ePA-Dokumentenverwaltung NICHT kommunizieren.**[<=]**

4.2.1 Anforderungen an IHE ITI-Akteure

A_13805 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XCDR Responding Gateway
Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XCDR Responding Gateway" gemäß [IHE-ITI-XCDR] implementieren.**[<=]**

A_13806 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XDS Document Registry
Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XDS Document Registry" gemäß [IHE-ITI-TF1] implementieren.**[<=]**

A_14727 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XDS Document Repository
Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XDS Document Repository" gemäß [IHE-ITI-TF1] implementieren.**[<=]**

A_13807 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XCA Responding Gateway
Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XCA Responding Gateway" gemäß [IHE-ITI-TF1] implementieren.**[<=]**

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

A_13809 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs ATNA Audit Record Repository
Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "ATNA Audit Record Repository" gemäß [IHE-ITI-TF1] implementieren. **[<=]**

Die Mechanismen der IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure Application" zur Node Authentication werden über das Konzept "Vertrauenswürdige Ausführungsumgebung" (vgl. Abschnitt4.4) 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 Authenticaton die IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure Application" gemäß [IHE-ITI-TF1] NICHT implementieren.
[<=]

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

A_14654 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs CT Time Client
Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "CT Time Client" gemäß [IHE-ITI-TF1] implementieren.**[<=]**

A_14655 - Komponente ePA-Dokumentenverwaltung – Zeitsynchronisation über Zeitdienst in der TI
Die Komponente ePA-Dokumentenverwaltung MUSS die Systemzeit über den Zeitdienst in der TI gemäß [gemSpec_Net#5.2] synchronisieren.
[<=]

A_14597 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs XUA X-Service Provider
Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "XUA X-Service Provider" gemäß [IHE-ITI-TF1] implementieren.**[<=]**

A_14665 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Document Source
Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDSDocument Source" gemäß [IHE-ITI-TF1] implementieren.**[<=]**

A_14667 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Integrated Document Source/Repository
Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS Integrated Document Source/Repository" gemäß [IHE-ITI-TF1] implementieren.
[<=]

A_14668 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Document Consumer
Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS Document Consumer" gemäß [IHE-ITI-TF1] implementieren.**[<=]**

A_14666 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS Patient Identity Source
Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS Patient Identity Source" gemäß [IHE-ITI-TF1] implementieren.
[<=]

A_14669 - Komponente ePA-Dokumentenverwaltung – Keine Implementierung des IHE ITI-Akteurs XDS On-Demand Document Source
Die Komponente ePA-Dokumentenverwaltung DARF NICHT den IHE ITI-Akteur "XDS On-Demand Document Source" gemäß [IHE-ITI-TF1] implementieren.
[<=]

A_14782 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs APPC Content Consumer
Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "APPC Content Consumer" gemäß [IHE-ITI-APPC] implementieren.**[<=]**

A_14950 - Komponente ePA-Dokumentenverwaltung – Keine Angabe einer Fehlerlokalisierung im RegistryError-Element
Die Komponente ePA-Dokumentenverwaltung DARF NICHT das `location`-Attribut im `rs:RegistryError`-Element in der IHE ITI-Ausgangsnachricht verwenden, sofern ein Fehler bei der Verarbeitung einer IHE ITI-Eingangsnachricht auftritt. Diese Einschränkung gilt nur für Error Stack Traces bzw. der Offenbarung von Programmierdetails.
[<=]

A_15081 - Komponente ePA-Dokumentenverwaltung – Implementierung des IHE ITI-Akteurs RMU Update Responder
Die Komponente ePA-Dokumentenverwaltung MUSS den IHE ITI-Akteur "RMU Update Responder" gemäß [IHE-ITI-RMU] implementieren.**[<=]**

4.2.1.1 APPC Content Consumer

4.2.1.1.1 Gruppierungen mit anderen IHE ITI-Akteuren

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

4.2.1.1.2 Optionen des IHE ITI-Akteurs

A_14787 - Komponente ePA-Dokumentenverwaltung – APPC Content Consumer ohne "View Option"-Option
Die Komponente ePA-Dokumentenverwaltung als APPC-Akteur "Content Consumer" DARF NICHT die Option "View Option" unterstützen.**[<=]**

A_14788 - Komponente ePA-Dokumentenverwaltung – APPC Content Consumer mit "Structured Policy Processing Option"-Option
Die Komponente ePA-Dokumentenverwaltung als APPC-Akteur "Content Consumer" MUSS die Option "Structured Policy Processing Option" unterstützen.**[<=]**

4.2.1.2 RMU Update Responder

4.2.1.2.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_15093 - Komponente ePA-Dokumentenverwaltung – Gruppierung RMU Update Responder mit XCA Responding Gateway und X-Service Provider
Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS mit dem XCA-Akteur "Responding Gateway" gemäß [IHE-ITI-RMU]sowie mit dem XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions verarbeiten.
[<=]

A_17571 - Komponente ePA-Dokumentenverwaltung – Gruppierung RMU Update Responder mit APPC Content Consumer
Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert sein.**[<=]**

4.2.1.2.2 Optionen des IHE ITI-Akteurs

A_15094 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "Forward Update"-Option
Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF NICHT die Option "Forward Update" unterstützen.
[<=]

A_15095 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder mit "XCA Persistence"-Option
Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS die Option "XCA Persistence" unterstützen.
[<=]

A_15096 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "XDS Persistence"-Option
Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF NICHT die Option "XDS Persistence" unterstützen.
[<=]

A_15097 - Komponente ePA-Dokumentenverwaltung – RMU Update Responder ohne "XDS Version Persistence"-Option
Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" DARF NICHT die Option "XDS Version Persistence" unterstützen.
[<=]

4.2.1.3 XCA Responding Gateway

4.2.1.3.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_14598 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit X-Service Provider
Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS mit dem XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions verarbeiten.**[<=]**

A_14725 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit XDS Document Registry
Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS mit dem XDS-Akteur "Document Registry" gemäß [IHE-ITI-TF1 gruppiert sein.**[<=]**

A_14726 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit XDS Document Repository
Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS mit dem XDS-Akteur "Document Repository" gemäß [IHE-ITI-TF1] gruppiert sein.**[<=]**

A_14784 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCA Responding Gateway mit APPC Content Consumer
Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert sein.**[<=]**

4.2.1.3.2 Optionen des IHE ITI-Akteurs

A_13819 - Komponente ePA-Dokumentenverwaltung – XCA Responding Gateway ohne "On-Demand Documents"-Option
Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" DARF NICHT die Option "On-Demand Documents" unterstützen.**[<=]**

A_13820 - Komponente ePA-Dokumentenverwaltung – XCA Responding Gateway ohne "Persistence of Retrieved Documents"-Option
Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" DARF NICHT die Option "Persistence of Retrieved Documents" unterstützen.**[<=]**

4.2.1.4 XCDR Responding Gateway

4.2.1.4.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_13648 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit X-Service Provider
Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS mit dem XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions verarbeiten.**[<=]**

A_14723 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit XDS Document Registry
Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS mit dem XDS-Akteur "Document Registry" gemäß [IHE-ITI-XCDR] gruppiert sein.**[<=]**

A_14724 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit XDS Document Repository
Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS mit dem XDS-Akteur "Document Repository" gemäß [IHE-ITI-XCDR] gruppiert sein.**[<=]**

A_14783 - Komponente ePA-Dokumentenverwaltung – Gruppierung XCDR Responding Gateway mit APPC Content Consumer
Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert sein.**[<=]**

4.2.1.4.2 Optionen des IHE ITI-Akteurs

A_13650 - Komponente ePA-Dokumentenverwaltung – XCDR Responding Gateway ohne "Basic Patient Privacy Enforcement"-Option
Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" DARF NICHT die Option "Basic Patient Privacy Enforcement" unterstützen.**[<=]**

4.2.1.5 XDS Document Registry

4.2.1.5.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_14599 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS Document Registry mit X-Service Provider
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS mit dem XUA-Akteur "X-Service Provider" gemäß [IHE-ITI-TF1] gruppiert sein und X-User Assertions verarbeiten.**[<=]**

A_14785 - Komponente ePA-Dokumentenverwaltung – Gruppierung XDS Document Registry mit APPC Content Consumer
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS mit dem APPC-Akteur "Content Consumer" gemäß [IHE-ITI-APPC] gruppiert sein.**[<=]**

4.2.1.5.2 Optionen des IHE ITI-Akteurs

A_14637 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "Asynchronous Web Services Exchange"-Option
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF NICHT die Option "Asynchronous Web Services Exchange" unterstützen.**[<=]**

A_14638 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry mit "Reference ID"-Option
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS die Option "Reference ID" unterstützen.**[<=]**

A_14639 - Komponente ePA-Dokumentenverwaltung – XDS Document Registry ohne "Patient Identity Feed"-Option
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF NICHT die Option "Patient Identity Feed" unterstützen.
[<=]

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

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

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

4.2.1.6 XDS Document Repository

4.2.1.6.1 Gruppierungen mit anderen IHE ITI-Akteuren

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

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

4.2.1.6.2 Optionen des IHE ITI-Akteurs

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

4.2.1.7 XUA X-Service Provider

4.2.1.7.1 Gruppierungen mit anderen IHE ITI-Akteuren

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

4.2.1.7.2 Optionen des IHE ITI-Akteurs

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

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

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

4.2.2 Überblick über gruppierte IHE ITI-Akteure und Optionen

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

Tabelle 1: Tab_Dokv_10 - Kennzeichnung von Optionalitäten

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

Tabelle 2: Tab_Dokv_11 - Übersicht über gruppierte IHE ITI-Akteure und ~~Optionenan~~Optionen an den Außenschnittstellen der ePA-Dokumentenverwaltung

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

		XDS Document Registry	R		
		XDS Document Repository	R		
ATNA Audit Record Repository	X				
CT Time Client	X				
RMU Update Responder	R			Forward Update	X
				XCA Persistence	R
				XDS Persistence	X
				XDS Version Persistence	X
		APPC Content Consumer	R		
		XCA Responding Gateway	R		
		X-Service Provider	R		
XCDR Responding Gateway	R			Basic Patient Privacy Enforcement	X
		APPC Content Consumer	R		
		ATNA Secure Node oder Secure Application für Node	X		

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

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

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

4.2.3 Einschränkungen auf IHE ITI-Transaktionen bei mehreren Schnittstellen

A_17832 - Komponente ePA-Dokumentenverwaltung – Unterstützung MTOM/XOP
Die Komponente ePA-Dokumentenverwaltung MUSS gemäß den Anforderungen von [IHE-ITI-TF2x#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] verwenden.**[<=]**

4.2.3.1 Provide X-User Assertion [ITI-40]

A_14915 - 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::CrossGatewayRetrieve`
- `I_Document_Management::RestrictedUpdateDocumentSet`
- `I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b`
- `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b`
- `I_Document_Management_Insurant::RegistryStoredQuery`
- `I_Document_Management_Insurant::RemoveDocuments`
- `I_Document_Management_Insurant::RetrieveDocumentSet`

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

A_14594 - Komponente ePA-Dokumentenverwaltung – Validierung der Authentication Assertion
Die Komponente ePA-Dokumentenverwaltung als XUA-Akteur "X-Service Provider" MUSS die X-User Assertion (Authentication Assertion) gemäß der Anforderung A_13690 prüfen und die eingehende Nachricht mit Fehlercodes nach [WSS#12] quittieren, falls diese X-User Assertion nicht gültig ist.**[<=]**

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

A_14549 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Provide and Register Document Set-b
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt registriert und ein Dokument gespeichert wird.

[<=]

A_15162-01~~A_15162~~ - Komponente ePA-Dokumentenverwaltung – Keine Registrierung bei Angabe von Document Entry Relationships in Metadaten
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern die Metadaten die folgenden Association Types nach [IHE-ITI-TF3#4.2.2] enthalten:

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

[<=]

A_14937 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße prüfen
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das SubmissionSet verarbeitet wird. Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung ablehnen und mit einem `MaxDocSizeExceeded`- bzw. `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren, wenn die Gesamtgröße aller übermittelten Dokumente 250 MByte übersteigt oder die Größe mindestens eines einzelnen Dokuments 25 MByte übersteigt.
[<=]

A_14938 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung der Metadaten aus ITI Document Sharing-Profilen durch XDS-Akteur "Document Repository"
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die SubmissionSet- sowie die DocumentEntry-Metadaten der eingehenden Nachrichtvor einer Zugriffskontrolle gemäß Konformität zu den Nutzungsvorgaben in [gemSpec_DM_ePA#A_14760] prüfen. Die Komponente ePA-Dokumentenverwaltung

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

4.2.3.3 Remove Documents [ITI-86]

A_14926 - 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 kein weiteres Dokument mit diesem Submission Set assoziiert ist.**[<=]**

A_14670-01 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Remove Documents
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor ein ~~Dokumentoder~~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.**[<=]**

4.3 Fehlerbehandlung in Schnittstellenoperationen

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

A_15664 - Komponente ePA-Dokumentenverwaltung – Fehlername
Die Komponente ePA-Dokumentenverwaltung MUSS in einer GERROR-Fehlermeldung gemäß [TelematikError.xsd] den in der Operationsdefinition festgelegten Fehlernamen `Name` im Feld `tel:Error/tel:Trace/tel:EventID` verwenden.**[<=]**

A_15665 - Komponente ePA-Dokumentenverwaltung – Fehlertext
Die Komponente ePA-Dokumentenverwaltung MUSS in einer GERROR-Fehlermeldung gemäß [TelematikError.xsd] den in der Operationsdefinition festgelegten Fehlerdetailtext `Fehlertext` im Feld `tel:Error/tel:Trace/tel:ErrorText` verwenden.**[<=]**

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

Tabelle 3: Tab_Dokv_12 - Fehlercodes zu Fehlern gemäß Operationsdefinition

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

[<=]

4.4 Vertrauenswürdige Ausführungsumgebung

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

A_14472 - 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_Managemen`, `I_Document_Management_Insurance` sowie `I_Document_Management_Insurant` im Verarbeitungskontext einer Vertrauenswürdigen Ausführungsumgebung (VAU) umsetzen.**[<=]**

A_18714 - Komponente ePA-Dokumentenverwaltung – Verhalten des Kontextmanagements bei ungeöffnetem Verabeitungskontext
Das Kontextmanagement MUSS mit einer `VAUServerError`-Nachricht und HTTP-Fehler 403 (Fehlermeldung "Access Denied") antworten, wenn für eine Web-Service-Operation der Schnittstellen`I_Document_Management`, `I_Document_Management_Insurant`, `I_Document_Management_Insurance` sowie `I_Account_Management_Insurant` für den angemeldeten Nutzer kein Verarbeitungskontext geöffnet wurde.
[<=]

4.4.1 Verarbeitungskontext

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

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

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

A_14557 - Komponente ePA-Dokumentenverwaltung – Verarbeitungskontext der VAU
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS sämtliche physikalischen Systemkomponenten sowie sämtliche Softwarekomponenten umfassen, deren Sicherheitseigenschaften sich auf den Schutz der personenbezogenen medizinischen Daten vor Zugriff durch Unbefugte bei ihrer Verarbeitung im Klartext auswirken können.**[<=]**

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

A_14581 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung von außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass sämtliche schützenswerten Daten vor einer Speicherung außerhalb der VAU verschlüsselt werden.**[<=]**

A_14582 - Komponente ePA-Dokumentenverwaltung – Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass sämtliche schützenswerten Daten ausschließlich über sichere Verbindungen an autorisierte Nutzer weitergegeben werden.**[<=]**

A_14583 - Komponente ePA-Dokumentenverwaltung – Verschlüsselung der Dokumentmetadaten und technischen Daten der VAU
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS für die Verschlüsselung aller Dokumentmetadaten, Policy Documents und des § 291a-Protokolls des Versicherten sowie eigener technischer Daten den Kontextschlüssel des Aktenkontos verwenden.**[<=]**

A_14566 - Komponente ePA-Dokumentenverwaltung – Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die in ihr ablaufenden Verarbeitungen für die Daten eines Verarbeitungskontextes von den Verarbeitungen für die Daten anderer Verarbeitungskontexte in solcher Weise trennen, dass mit technischen Mitteln ausgeschlossen wird, dass die Verarbeitungen eines Verarbeitungskontextes 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. **[<=]**

A_14559 - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Software der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS eine Manipulation der eingesetzten Software erkennen und eine Ausführung der manipulierten Software verhindern.**[<=]**

A_14560 - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Hardware der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter ePA-Aktensystem ausschließen.**[<=]**

A_14561 - Komponente ePA-Dokumentenverwaltung – Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter ePA-Aktensystem mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann.**[<=]**

A_14562 - Komponente ePA-Dokumentenverwaltung – Kein physischer Zugang des Anbieters zu Systemen der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter ePA-Aktensystem, während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.**[<=]**

A_14563 - Komponente ePA-Dokumentenverwaltung – Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln sicherstellen, dass physischer Zugang zu Hardware-Komponenten der Verarbeitungskontexte nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten extrahiert werden können.**[<=]**

A_14564 - Komponente ePA-Dokumentenverwaltung – Private Schlüssel von Dienstzertifikaten im HSM
Die Komponente ePA-Dokumentenverwaltung MUSS die folgenden privaten Schlüssel in einem Hardware Security Module (HSM) erzeugen und anwenden:

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

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

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

A_14565 - Komponente ePA-Dokumentenverwaltung – HSM-Kryptographieschnittstelle verfügbar nur für Instanzen der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln, die auch Manipulationen durch den Anbieter ePA-Aktensystem ausschließen, gewährleisten, dass nur Instanzen der VAU Zugriff auf die Kryptographieschnittstelle des HSM zur Nutzung des privaten Schlüsselmaterials für ihre Dienstzertifikate erhalten können.**[<=]**

A_14567 - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal vom Client zum Verarbeitungskontext der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS den Aufbau eines vertraulichen und integritätsgeschützten Kommunikationskanals gemäß [gemSpec_Krypt#3.15] zwischen einem Client und einem Verarbeitungskontext erzwingen, bevor der Verarbeitungskontext durch Übergabe des Kontextschlüssels durch den Client aktiviert werden kann.**[<=]**

4.4.3 Kryptographische Aktivierung des Verarbeitungskontextes

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

A_14568 - Komponente ePA-Dokumentenverwaltung – Aktivierung des Verarbeitungskontextes der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln gewährleisten, dass schützenswerte Nutzdaten im Verarbeitungskontext erst nach Aktivierung – mittels Übergabe des korrekten *Kontextschlüssels* an den Verarbeitungskontext durch den Client eines berechtigten Nutzers – entschlüsselt und verarbeitet werden können.**[<=]**

A_15085 - Komponente ePA-Dokumentenverwaltung – Prüfung des Kontextschlüssels durch die VAU
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die Korrektheit des übergebenen Kontextschlüssels prüfen und dabei die folgenden zwei Fälle unterscheiden:

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

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

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

A_14570 - Komponente ePA-Dokumentenverwaltung – Keine Speicherung des Kontextschlüssels in der VAU
Die VAU der Komponente ePA-Dokumentenverwaltung DARF den Kontextschlüssel NICHT über das Ende der Sitzung des letzten verbundenen Nutzers hinaus speichern oder verwenden.**[<=]**

A_15841 - Komponente ePA-Dokumentenverwaltung – Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS sämtliche aktenbezogenen Daten (Nutzdaten, Konfigurationsdaten und 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-Modul Frontend des Versicherten nach [gemSpec_FdV_ePA] zum Verarbeitungskontext des Aktenkontos zu ermöglichen, ist ein Kontextmanagement erforderlich. Das Kontextmanagement ist im Netzwerk der TI für das Fachmodul ePA und für das ePA-Modul Frontend des Versicherten unter mindestens

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

A_14616 - Komponente ePA-Dokumentenverwaltung – Kontextmanagement der Vertrauenswürdigen Ausführungsumgebung
Die VAU der Komponente ePA-Dokumentenverwaltung MUSS ein Kontextmanagement bereitstellen, das Verarbeitungskontexte bedarfsgesteuert initialisiert und terminiert, über initialisierte Verarbeitungskontexte auf der Basis ihrer `RecordIdentifier` Buch führt und Verbindung zwischen Clients und den jeweils benötigten Verarbeitungskontexten vermittelt.**[<=]**

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 - Komponente ePA-Dokumentenverwaltung – Verbindungen vom ePA-Modul Frontend des Versicherten zum Verarbeitungskontextes der VAU über das Zugangsgateway
Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS Verbindungen vom ePA-Modul Frontend des Versicherten ausschließlich über das Zugangsgateway des Versicherten akzeptieren. **[<=]**

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

A_14580 - Komponente ePA-Dokumentenverwaltung – Identität der Dokumentenverwaltung für das Fachmodul ePA und Fachmodul ePA KTR-Consumer
Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS sich innerhalb der TI mittels der Fachdienstidentität `oid_epa_dvw` mit Zertifikatsprofil `C.FD.TLS-S` ausweisen.**[<=]**

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

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

4.5 Anforderungen zur sicherheitstechnischen Validierung

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

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

A_14465 - Komponente ePA-Dokumentenverwaltung – XML Schema-Validierung für SOAP-Eingangsnachrichten
Die Komponente ePA-Dokumentenverwaltung MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-Eingangsnachrichten einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen und gemäß [SOAP] verarbeiten. Sind Nachrichten nicht wohlgeformt oder gültig, 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_13690-01 - Komponente ePA-Dokumentenverwaltung – SAML 2.0 Assertion-Validierung
Die Komponente ePA-Dokumentenverwaltung MUSS die vorliegende Assertion einer grundsätzlichen XML Schema-Prüfung, einer Prüfung gemäß den Prüfvorschriften aus [gemSpec_TBAuth#3.2] sowie einer Prüfung auf Übereinstimmung mit dem erforderlichen SAML 2.0 Assertion-Profil aus [gemSpec_FM_ePA#A_14927, A_15638], [gemSpec_Authentisierung_Vers#A_14109, A_15631], [gemSpec_Autorisierung#A_14491] oder [gemSpec_FM_ePA_KTR_Consumer#A_17253,

A_17254] unterziehen und die Verarbeitung der begleitenden Nachricht abbrechen und gemäß [WSS#12] bzw. im Sonderfall der Authorization Assertion mit einer `VAUServerError`-Nachricht (HTTP-Fehler 403, Fehlermeldung "Access Denied") quittieren, falls eine Übereinstimmung nicht festgestellt werden kann.

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

Tabelle 4: Tab_Dokv_35 - Eingangsparameter für TUC_PKI_018

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

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

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 - 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 nach dem Zertifikatsprofil C.FD.SIG auf die Identität der Komponente Authentisierung Versicherter ausgestellt wurde.
[<=]

A_17387 - Komponente ePA-Dokumentenverwaltung – Authorization Assertion-Validierung
Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass Authorization Assertions nur akzeptiert werden, wenn das zugehörige Signaturzertifikat zeitlich gültig ist, nicht gesperrt wurde und nach dem Zertifikatsprofil C.FD.SIG auf die Identität der Komponente Autorisierung ausgestellt wurde.
[<=]

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

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

A_14735 - Komponente ePA-Dokumentenverwaltung – Verpflichtende Nutzung des "mustUnderstand"-Attributs im SOAP Security Header
Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Nachrichten mit SAML 2.0 Assertions im SOAP Security Header mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren, sofern das SOAP 1.2 `mustUnderstand`-Attribut im SOAP Security Header nicht angegeben ist oder den Wert `false` bzw. `0` hat ([SOAP12#5.2.3] [WSS#5]).**[<=]**

A_14810 - Komponente ePA-Dokumentenverwaltung – Erkennung von Denial-of-Service-Angriffen hinsichtlich dem Parsen von SOAP 1.2-Nachrichten
Die Komponente ePA-Dokumentenverwaltung MUSS die folgenden Angriffstypen in eingehenden SOAP 1.2-Nachrichten erkennen und mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren:

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

[<=]

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

A_14811 - Komponente ePA-Dokumentenverwaltung – Ablehnung von SOAP 1.2-Nachrichten ohne UTF-8 Kodierung
Die Komponente ePA-Dokumentenverwaltung MUSS SOAP 1.2-Nachrichten mit einem HTTP-Statuscode 406 gemäß [RFC7231] quittieren, sofern die Zeichenkodierung im HTTP Header nicht UTF-8 benennt (`Content-Type: charset=utf-8`).**[<=]**

4.6 Protokollierung

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

A_14813 - 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::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::RegistryStoredQuery`
- `I_Document_Management_Insurant::RemoveDocuments`
- `I_Document_Management_Insurant::RetrieveDocumentSet`
- `I_Account_Management_Insurant::GetAuditEvents`
- `I_Account_Management_Insurant::SuspendAccount`
- `I_Account_Management_Insurant::ResumeAccount`

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

A_14816-01 - Komponente ePA-Dokumentenverwaltung – Parameter des § 291a-Protokolls
Die Komponente ePA-Dokumentenverwaltung MUSS einen Protokolleintrag gemäß der Festlegung in [gemSpec_DM_ePA#A_14471] wie folgt erzeugen:

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

Protokoll-parameter	Parameterwerte gemäß aufgerufener Operation
User-ID	Bei Aufrufen einer Operation der Schnittstellen *I_Document_Management*, *I_Document_Management_Insurance* sowie *I_Document_Management_Insurant*: *X*Path-Ausdruck zur " Subject ID" der im Operationsaufruf übergebenen Authentication 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)`
User Name	Bei Aufrufen einer Operation der Schnittstellen *I_Document_Management:* *X*Path-Ausdruck zur "XSPA Organization" der im Operationsaufruf übergebenen Authentication Assertion: `//*[local-name()='Attribute' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion'][@Name= 'urn:oasis:names:tc:xacml:1.0:subject:organization']/*[local-name()='AttributeValue']/text()[normalize-space()]` *I_Document_Management_Insurance* und *I_Document_Management_Insurant:* *XPath-Ausdruck zum SAML Subject der im Operationsaufruf übergebenen Authentication Assertion:*

	//[local-name()='Assertion' and namespace-uri() = 'urn:oasis:names:tc:SAML:2.0:assertion']/*[local-name()='Subject']/*[local-name()='NameID']/text()[normalize-space()]*
Object-ID	Der unveränderbare Anteil der KVNR des `extension`-Attributs aus dem InsurantId-Element des `RecordIdentifier`-Elements oder die documentEntry.patientId des entsprechenden Operationsaufrufs *Hinweis: Bei Aufruf von Operationen ohne diesen Parameter wird der Wert im Protokolleintrag nicht belegt.* Bei Zugriffen auf Dokumente über die Transaktionen CrossGatewayDocumentProvide, ProvideAndRegisterDocumentSet-b, CrossGatewayRetrieve, RetrieveDocumentSet, RemoveDocuments, RestrictedUpdateDocument MUSS die Document Unique ID im Element `ParticipantObjectDetail` hinterlegt werden. Als Attribut `type` MUSS der Wert `DocumentUniqueId` und als Attribut `value` der Wert der Document Unique ID verwendet werden.
Object Name	Bei Zugriffen auf Dokumente über die Transaktionen CrossGatewayDocumentProvide, ProvideAndRegisterDocumentSet-b, CrossGatewayRetrieve, RetrieveDocumentSet, RemoveDocuments, RestrictedUpdateDocument MUSS der Document Title im Element `ParticipantObjectDetail` hinterlegt werden. Als Attribut `type` MUSS der Wert `DocumentTitle` und als Attribut `value` der Wert der Document Title verwendet werden.
Device-ID	Der Parameter `DeviceID` wird im Protokolleintrag nicht belegt.

[<=]

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_15184 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen alter § 291a-Protokolldaten

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

5 Funktionsmerkmale

5.1 Dokumentenverwaltung

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

5.1.1 Schnittstelle I_Document_Management

A_14152 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management

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

Tabelle 6: Tab_Dokv_14 - Schnittstelle I_Document_Management

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

	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
WSDL	DocumentManagementService.wsdl	
XML Schema	• PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd	

[<=]

5.1.1.1 Operation I_Document_Management::CrossGatewayDocumentProvide

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

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

Tabelle 7: Tab_Dokv_15 - Operation Cross-Gateway Document Provide

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

Cross-Gateway Document Provide Message	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	`xdsb:ProvideAndRegisterDocumentSetRequest`	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution, des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638] oder [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n

Ausgangsparameter

Name	Beschreibung	Typ	opt.
Cross-Gateway Document Provide Response Message	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	`rs:RegistryResponse`	n

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

Name	Fehlertext	Details
MaxDocSizeExceeded	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines der übermittelten Dokumente übersteigt 25 MByte.
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.

[<=]

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_14941-02~~A_14941~~ - 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:RPLC` (Replace)~~
- `urn:ihe:iti:2007:AssociationType:XFRM` (Transform)
- ~~`urn:ihe:iti:2007:AssociationType:APND` (Addendum)~~
- `urn:ihe:iti:2007:AssociationType:XFRM_RPLC` (Replace with Transformation)
- `urn:ihe:iti:2007:AssociationType:signs` (Digital Signature)
- `urn:ihe:iti:2010:AssociationType:IsSnapshotOf` (Snapshot of On-Demand document entry)

[<=]

A_13838 - Komponente ePA-Dokumentenverwaltung – Dokumentengröße prüfen
Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das SubmissionSet verarbeitet wird. Die Verarbeitung MUSS abgelehnt werden und mit einem mit einem `MaxDocSizeExceeded`-bzw. `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren, wenn die Gesamtgröße aller übermittelten Dokumente 250 MByte übersteigt oder die Größe mindestens eines einzelnen übermittelten Dokuments 25 MByte übersteigt.
[<=]

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

A_13798 - Komponente ePA-Dokumentenverwaltung – Whitelist-Validierung der Metadaten aus ITI Document Sharing-Profilen durch XCDR-Akteur "Responding Gateway"
Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS die SubmissionSet- sowie die DocumentEntry-Metadaten der eingehenden Nachrichtvor einer Zugriffskontrolle gemäß der Konformität zu den Nutzungsvorgaben in [gemSpec_DM_ePA#A_14760] prüfen. Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht.**[<=]**

A_13715 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Cross-Gateway Document Provide
Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS die Umsetzung der Operation `I_Document_Management::CrossGatewayDocumentProvide` bzw. die Verarbeitung des übermittelten Submission Sets gemäß den definierten Ablauflogiken in [IHE-ITI-XCDR#3.80.4.1.2 und 3.80.4.1.3] und [IHE-ITI-XCDR#3.80.4.2.2 und 3.80.4.2.3] implementieren.**[<=]**

A_13657 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Cross-Gateway Document Provide
Die Komponente ePA-Dokumentenverwaltung als XCDR-Akteur "Responding Gateway" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor ein Registry-Datenobjekt registriert und ein Dokument gespeichert wird.**[<=]**

5.1.1.2 Operation I_Document_Management::CrossGatewayQuery

A_14450 - Komponente ePA-Dokumentenverwaltung – Signatur für Cross-Gateway Query
Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I_Document_Management::CrossGatewayQuery` gemäß der folgenden Signatur implementieren:

Tabelle 7: Tab_Dokv_16 - Operation Cross-Gateway Query

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

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

[<=]

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

5.1.1.2.1 Umsetzung

A_14924 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe von Metadaten zu Policy Documents (Advanced Patient Privacy Consents)
Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" DARF Metadaten zu Policy Documents (Advanced Patient Privacy Consents) gemäß der Anforderung [gemSpec_DM_ePA#A_14961] NICHT zurückgeben bzw. MUSS diese aus der Antwortnachricht entfernen, falls diese den Anfragekriterien entsprechen.
[<=]

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

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

```
    </Resources>
  </Target>
  <Rule RuleId="urn:uuid:bb42d632-c70c-447d-94aa-011f2c9561f4"
Effect="Deny"/>
</Policy>
```

A_14939 - Komponente ePA-Dokumentenverwaltung – Keine Anfragen auf Ordnern

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

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

[<=]

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

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

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

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

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

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

A_18069 - Komponente ePA-Dokumentenverwaltung – Suche über Author Institution bei Cross-Gateway Query
Die Komponente ePA-Dokumentenverwaltung als XCA-Akteur "Responding Gateway" MUSS für den Anfragetyp "FindDocumentsByTitle" den weiteren optionalen Parameter $XDSDocumentEntryAuthorInstitution verarbeiten können, sodass eine Suchergebnismenge über den authorInstitution-Slot der XDSDocumentEntry.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.**[<=]**

5.1.1.3 Operation I_Document_Management::RemoveDocuments

A_14489 - 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**	**opt.**
Remove Documents Message	Eingangsnachricht zum Löschen ein oder mehrerer Dokumente	`rmd:RemoveDocuments_Message`	n
X-User Assertion	Authentication Assertion der authentifizierten Leistungserbringerinstitution	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA#A_14927, A_15638]	n
Ausgangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**

Remove Documents Response Message	Ausgangsnachricht zum Löschen ein oder mehrerer Dokumente	`rmd:RemoveDocumentsResponse_Message`	n
Technische Fehlermeldungen *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_14908 - 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::CrossGatewayRetrieve

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

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

Tabelle 9: Tab_Dokv_18 - Operation Cross-Gateway Retrieve

Operation	**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.

5.1.1.4.1 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 `XDSDocumentUniqueIdError`-Fehlercode enthalten (das Dokument wird nicht herausgegeben) und der Wert `4` des `EventOutcomeIndicator`s im Protokollierungseintrag des § 291a-Protokolls gesetzt werden. Ist ein angefordertes Dokument nicht mehr verfügbar (d.h. es wurde gelöscht), MUSS gemäß IHE ITI der Fehlercode `XDSDocumentUniqueIdError` zurückgegeben werden.**[<=]**

~~**5.1.1.5 Operation I_Document_Management::RestrictedUpdateDocumentSet**~~

~~**A_15057 - 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 10: Tab_Dokv_19 – Operation Restricted Update Document Set**~~

~~Operation~~	~~I_Document_Management::RestrictedUpdateDocumentSet~~

Beschreibung	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. Für die Kenntlichmachung von Dokumenten eines Versicherten oder eines Kostenträgers mit leistungserbringeräquivalenter Relevanz ermöglicht die ePA-Fachanwendung Mitarbeitern einer Leistungserbringerinstitution, Dokumente, die durch einen Versicherten (oder dessen Vertreter) bereitgestellt wurden, anderen berechtigten Leistungserbringerinstitutionen zur Verfügung zu stellen. Dies setzt voraus, dass die entsprechende Leistungserbringerinstitution Zugriff auf die Dokumente eines Versicherten oder die des Kostenträgers hat, um die Sensibilität ändern zu können. Im Detail werden durch einen Versicherten eingestellte Dokumente mit dem Metadatenattribut documentEntry.confidentialityCode "PAT" (Dokument eines Versicherten) gekennzeichnet. Dokumente, welche ein Kostenträger eingestellt hat, werden ferner mit dem Metadatenattribut documentEntry.confidentialityCode "KTR" (Dokument eines Kostenträgers) gekennzeichnet. Durch eine Leistungserbringerinstitution eingestellte Dokumente werden mit dem Metadatenattribut documentEntry.confidentialityCode "LEI" (Dokument einer Leistungserbringerinstitution) gekennzeichnet. Um ein Dokument als leistungserbringeräquivalent zu kennzeichnen, muss der Mitarbeiter einer Leistungserbringerinstitution auch Zugriff auf Dokumente mit dem Metadatenattribut documentEntry.confidentialityCode "PAT" (Dokument eines Versicherten) oder "KTR" (Dokument eines Kostenträgers) haben (vgl. RegistryStoredQuery). Die besagte Kennzeichnung erfolgt durch das Hinzufügen eines weiteren Confidentiality Codes "LEÄ" (Leistungserbringeräquivalentes Dokument eines Versicherten oder Kostenträgers). Dieses Kennzeichen kann nach demselben Mechanismus wieder entfernt werden.
Formatvorgaben	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_14927, A_15638]	n
Ausgangsparameter			
Name	**Beschreibung**	**Typ**	**opt**
Update Responder Restricted Update Document Set Response	Ausgangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	rs:RegistryResponse	n
Technische Fehlermeldungen *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 "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.

5.1.1.5.1 Umsetzung

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

5.1.2 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 - Komponente ePA-Dokumentenverwaltung – Prüfung auf ausschließliche Aktualisierung des Metadatenattributs documentEntry.confidentialityCode~~

~~5.1.3 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 Hinzufügen oder Entfernen des Confidentiality Codes "`LEÄ`" (Leistungserbringeräquivalentes Dokument eines Versicherten oder Kostenträgers) erlaubt. Wenn andere Aktualisierungen für die übermittelten Metadatenattribute in der Eingangsnachricht enthalten sind, MUSS die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" die Weiterverarbeitung abbrechen und die Nachricht mit einem `LocalPolicyRestrictionError` Fehlercode quittieren.~~

~~[<=]~~

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

~~5.1.4 Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS 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.[<=]~~

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

~~5.1.55.1.2 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-Fachmodul 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 `XDSDocumentUniqueIdError` zurückgegeben werden.~~

~~[<=]~~

~~5.1.6~~5.1.3 Schnittstelle I_Document_Management_Insurant

A_14478 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management_Insurant

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

Tabelle 10: Tab_Dokv_20 - Schnittstelle I_Document_Management_Insurant

Schnittstelle	**I_Document_Management_Insurant**	
Version	1.0.1	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente in der Dokumentenverwaltung
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten

	Remove Documents	Löschen ein oder mehrerer Dokumente
WSDL	DocumentManagementService.wsdl	
XML Schema	• PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd	

[<=]

~~5.1.6.1~~5.1.3.1 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 11: Tab_Dokv_21 - Operation Provide And Register Document Set-b

Operation	**I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b**		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation `I_Document_Management_Insurant::putDocuments` technisch um. Sie basiert auf den IHE ITI-Transaktionen "Provide And Register Document Set-b" [ITI-41] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente mitsamt Metadaten im ePA-Aktensystem dauerhaft zu speichern.		
Formatvorgaben	SOAP Action: urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b		
Eingangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**

Provide And Register Document Set-b Message	Eingangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	`xdsb:ProvideAndRegisterDocumentSetRequest`	n
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers# A_14109, A_15631]	n

Ausgangsparameter

Name	**Beschreibung**	**Typ**	**opt.**
Provide And Register Document Set-b Response Message	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	`rs:RegistryResponse`	n

Technische Fehlermeldungen
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.

~~5.1.6.1.1~~5.1.3.1.1 Umsetzung

A_15056 - Komponente ePA-Dokumentenverwaltung – Keine Registrierung von gemischten Dokumentenpaketen mit Policy Documents
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern in der Eingangsnachricht mehr als ein Dokument und Dokumenten-Metadaten gemäß der Anforderung [gemSpec_DM_ePA#A_14961] für Policy Documents (Advanced Patient Privacy Consents) enthalten sind.**[<=]**

A_14912 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide And Register Document Set-b
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Umsetzung der Operation `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b` gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3] und [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3] implementieren.**[<=]**

A_16442 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
[<=]

~~5.1.6.2~~5.1.3.2 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 12: 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.		
Formatvorgaben	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.

~~5.1.6.2.15~~5.1.3.2.1 Umsetzung

A_14835 - Komponente ePA-Dokumentenverwaltung – Keine Anfragen auf Ordnern
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" DARF die folgenden Anfragetypen aufgrund des in ePA nicht verwendeten IHE ITI-Ordnerkonzepts NICHT unterstützen und MUSS die Anfrage mit einem `XDSUnknownStoredQuery`-Fehlercode quittieren:

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

[<=]

A_14913 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Registry Stored Query
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS die Umsetzung der Operation `I_Document_Management_Insurant::RegistryStoredQuery` gemäß der definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3] implementieren.**[<=]**

A_16436 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
[<=]

A_17185 - Komponente ePA-Dokumentenverwaltung – Suchanfragen über das Metadatenattribut DocumentEntry.title
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Registry" MUSS einen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter $XDSDocumentEntryTitle unterstützen, sodass eine Suchergebnismenge über das Attribut XDSDocumentEntry.title eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter $XDSDocumentEntryAuthorPerson. Daswsa: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.**[<=]**

~~5.1.6.3~~5.1.3.3 Operation I_Document_Management_Insurant::RemoveDocuments

A_14488 - Komponente ePA-Dokumentenverwaltung – Signatur für Remove Documents

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

Tabelle 13: 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.

~~5.1.6.3.1~~5.1.3.3.1 *Umsetzung*

A_14909 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Remove Documents
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Umsetzung der Operation `I_Document_Management_Insurant::RemoveDocuments` gemäß der definierten Ablauflogik in [IHE-ITI-RMD#3.86.4.1.2 und 3.86.4.1.3] implementieren.**[<=]**

A_16437 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
[<=]

~~5.1.6.4~~5.1.3.4 Operation I_Document_Management_Insurant::RetrieveDocumentSet

A_14481 - Komponente ePA-Dokumentenverwaltung – Signatur für Retrieve Document Set
Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I_Document_Management_Insurant::RetrieveDocumentSet` gemäß der folgenden Signatur implementieren:

Tabelle 14: Tab_Dokv_24 - Operation Retrieve Document Set

Operation	**I_Document_Management_Insurant::RetrieveDocumentSet**
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation `I_Document_Management_Insurant::getDocuments` technisch um. Sie basiert auf den IHE ITI-Transaktionen "Retrieve Document Set" [ITI-43] sowie "Provide X-User Assertion" [ITI-40] und ist diesbzgl. umzusetzen. Die Operation erlaubt es, ein oder mehrere Dokumente aus dem ePA-Aktensystem abzufragen.

Formatvorgaben	SOAP Action: urn:ihe:iti:2007:RetrieveDocumentSet		
Eingangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**
Retrieve Document Set Message	Eingangsnachricht zum Abruf von Dokumenten	`xdsb:RetrieveDocumentSetRequest`	n
X-User Assertion	Authentication Assertion des authentifizierten Versicherten oder des Vertreters	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631]	n
Ausgangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**
Retrieve Document Set Response Message	Ausgangsnachricht zum Abruf von Dokumenten	`xdsb:RetrieveDocumentSetResponse`	n
Technische Fehlermeldungen *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 "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.

~~5.1.6.4.1~~5.1.3.4.1 Umsetzung

A_14914 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Retrieve Document Set
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Umsetzung der Operation `I_Document_Management_Insurant::RetrieveDocumentSet` gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.43.4.1.2 und 3.43.4.1.3] und [IHE-ITI-TF2b#3.43.4.2.2 und 3.43.4.2.3] implementieren.**[<=]**

A_16443 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_Authentisierung_Vers#A_14109, A_15631] entspricht.
[<=]

A_16200 - Komponente ePA-Dokumentenverwaltung – Prüfung der zurückgegebenen Paketgröße
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS anhand der übergebenen DocumentUniqueIDs die Gesamtgröße ermitteln und bei Überschreitung von 250 MByte die Verarbeitung ablehnen und die Nachricht mit einem `MaxPkgSizeExceeded`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren.
[<=]

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

[<=]

5.1.3.5 Operation I_Document_Management_Insurant::RestrictedUpdateDocumentSet

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

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

Tabelle 15: Tab_Dokv_19 - Operation Restricted Update Document Set

Operation	I_Document_Management::RestrictedUpdateDocumentSet

Beschreibung	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. Für Änderungen an der Vertraulichkeitsstufe von Dokumenten werden im `documentEntry.confidentialityCode` die Werte "`normal`", "`restricted`" oder "`very restricted`" mit der`updateMedata` Operation umgesetzt. Andere Änderungen sind mit dieser Operation nicht möglich.
Formatvorgaben	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_14927, A_15638]	n

Ausgangsparameter

Name	Beschreibung	Typ	opt.
Update Responder Restricted Update Document Set Response	Ausgangsnachricht zum Aktualisieren ein oder mehrerer Dokumentmetadaten	`rs:RegistryResponse`	n

Technische Fehlermeldungen
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.

[<=]

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.

5.1.3.5.1 Umsetzung

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

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

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

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

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

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

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

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

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

Die Komponente ePA-Dokumentenverwaltung als RMU-Akteur "Update Responder" MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor Metadaten einer oder mehrerer Dokumente aktualisiert werden. Beim Aktualisieren der Metadaten durch das ePA-Frontend des Versicherten können einzelne Dokumente bzw. Metadaten durch den zwischenzeitlichen Entzug einer Berechtigung durch den Versicherten oder Ablauf nicht mehr für die Aktualisierung berechtigt sein. Widerspricht ein Dokument bzw. die damit assoziierten Metadaten einer anwendbaren Zugriffsrichtlinie aus zur Verfügung stehenden Policy Documents, so MUSS die Antwortnachricht zum betreffenden Dokument einen`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 `XDSDocumentUniqueIdError` zurückgegeben werden.
[<=]

~~5.1.7~~5.1.4 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 16: Tab_Dokv_36 - Schnittstelle I_Document_Management_Insurance

Schnittstelle	I_Document_Management_Insurance	
Version	1.0.1	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente in der Dokumentenverwaltung
WSDL	DocumentManagementService.wsdl	

XML Schema	• PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd

[<=]

~~5.1.7.1~~5.1.4.1 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 17: Tab_Dokv_37 - Operation Provide And Register Document Set-b

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

	ein oder mehrerer Dokumente		
X-User Assertion	Authentication Assertion des authentifizierten Kostenträgers	SAML 2.0 Assertion gemäß [gemSpec_FM_ePA_KTR_Consumer #A_17253, A_17254]	n
Ausgangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**
Provide And Register Document Set-b Response Message	Ausgangsnachricht zum Registrieren und Speichern ein oder mehrerer Dokumente	`rs:RegistryResponse`	n
Technische Fehlermeldungen *Hinweis: Es werden an dieser Stelle nur zusätzliche Fehlermeldungen definiert, welche über die IHE ITI-Vorgaben (insbesondere [IHE-ITI-TF3#4.2.4] und [IHE-ITI-TF2b#3.40.4.1.3]) hinausgehen.*			
Name	**Fehlertext**	**Details**	
MaxDocSizeExceeded	Die max. Dokumentengröße wurde überschritten.	Die Größe mindestens eines einzelnen übermittelten Dokuments übersteigt 25 MByte.	
MaxPkgSizeExceeded	Die max. Paketgröße wurde überschritten.	Die Gesamtgröße aller übermittelten Dokumente übersteigt 250 MByte.	

[<=]

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.

~~5.1.7.1.1~~5.1.4.1.1 *Umsetzung*

A_17443 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Provide And Register Document Set-b
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Umsetzung der Operation `I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b` gemäß den definierten Ablauflogiken in [IHE-ITI-TF2b#3.41.4.1.2 und 3.41.4.1.3] und [IHE-ITI-TF2b#3.41.4.2.2 und 3.41.4.2.3] implementieren.
[<=]

A_17444 - Komponente ePA-Dokumentenverwaltung – Prüfung nicht passender X-User Assertion
Die Komponente ePA-Dokumentenverwaltung als XDS-Akteur "Document Repository" MUSS die Verarbeitung der Nachricht mit einem Fehlercode gemäß [WSS#12] quittieren, falls die X-User Assertion nicht dem SAML 2.0 Assertion Profil gemäß [gemSpec_FM_ePA_KTR_Consumer#A_17253, A_17254] entspricht.**[<=]**

5.2 Aktenkontoverwaltung

5.2.1 Schnittstelle I_Account_Management_Insurant

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

A_14804 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Account_Management_Insurant
Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle implementieren.

Tabelle 18: Tab_Dokv_25 - Schnittstelle I_Account_Management_Insurant

Schnittstelle	**I_Account_Management_Insurant**	
Version	**1.0.1**	
Namensraum	http://ws.gematik.de/fd/phr/I_Account_Management/v1.0	
Namensraumkürzel	tns	
Operationen	**Name**	**Beschreibung**
	Suspend Account	Die Aktendaten werden in ein Exportpaket exportiert und das Aktenkonto geht in den Zustand "Bereit für Anbieterwechsel" über.

	Resume Account	Das neue Aktenkonto (bei einem anderen Anbieter) wird mit den Daten aus einem Exportpaket befüllt.
	Get Audit Events	Abfrage von Protokollen
WSDL	AccountManagementService.wsdl	
XML Schema	AccountManagementService.xsd	

[<=]

5.2.1.1 Operation I_Account_Management_Insurant::SuspendAccount

A_14805 - Komponente ePA-Dokumentenverwaltung – Signatur für I_Account_Management_Insurant::SuspendAccount

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

Tabelle 19: Tab_Dokv_26 - Operation Suspend Account

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

Package URL	URL, über die das erzeugte Exportpaket vom neuen Anbieter ePA-Aktensystem geladen werden kann	URL mit Prozentkodierung	**n**
Technische Fehlermeldungen			
Name	**Fehlertext**	**Details**	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig.	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
TEMP_UNAVAILABLE	Aktenkonto aufgrund einer andauernden Datenmigration vorübergehend nicht erreichbar	Dies sollte nur auftreten, wenn ein Anbieterwechsel angestoßen, aber noch nicht abgeschlossen wurde.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.	Der Nutzer hat nicht die erforderliche Berechtigung.	

[<=]

5.2.1.1.1 Umsetzung

A_15530 - 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-Modul Frontend des Versicherten verfügbar machen.**[<=]**

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

A_15062 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Suspend Account
Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor die

Operation `I_Account_Management_Insurant::SuspendAccount` ausgeführt wird. Bei einer negativen Autorisierungsentscheidung MUSS die Nachricht mit dem `ACCESS_DENIED`-Fehlercode quittiert werden.**[<=]**

A_14885 - Komponente ePA-Dokumentenverwaltung – Exportpaket des Aktenkontos erstellen
Die Komponente ePA-Dokumentenverwaltung MUSS bei der Ausführung der Operation `I_Account_Management_Insurant::SuspendAccount` für das Aktenkonto

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

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

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

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

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

A_15012 - Komponente ePA-Dokumentenverwaltung – Korrektheit des Exportpakets sicherstellen
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln die Integrität der Daten und Datenstrukturen des Exportpakets während der Erstellung, Bereitstellung und Übermittlung an einen neuen Anbieter ePA-Aktensystem schützen, um damit ein Scheitern des Imports bei einem neuen Anbieter ePA-Aktensystem aufgrund eines fehlerhaften oder beschädigten Exportpakets auszuschließen.**[<=]**

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

A_15005 - Komponente ePA-Dokumentenverwaltung – Kein Aktenzugriff während des Exports der Daten
Die Komponente ePA-Dokumentenverwaltung MUSS während der Ausführung der Operation `I_Account_Management_Insurant::SuspendAccount` für ein Aktenkonto alle Operationen mit der Fehlermeldung "Aktenkonto vorübergehend nicht erreichbar" ablehnen.**[<=]**

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

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

A_15622 - Komponente ePA-Dokumentenverwaltung – Asynchroner Export
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die URL des Exportpakets bestimmen und unmittelbar danach die Antwort auf den Aufruf der Operation `I_Account_Management_Insurant::SuspendAccount` an den Client zurückgeben, unabhängig davon, wie lange die Erstellung und Bereitstellung des Exportpakets dauert.**[<=]**

A_16076 - Komponente ePA-Dokumentenverwaltung – Frist für Bereitstellung des Exportpakets
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS das Exportpaket innerhalb von drei Werktagen für den Download durch den neuen Anbieter bereitstellen.**[<=]**

5.2.1.2 Operation I_Account_Management_Insurant::ResumeAccount

A_14807 - Komponente ePA-Dokumentenverwaltung – Signatur für I_Account_Management_Insurant::ResumeAccount
Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I_Account_Management_Insurant::ResumeAccount` gemäß der folgenden Signatur implementieren:

Tabelle 20: Tab_Dokv_27 - Operation Resume Account

Operation	**I_Account_Management_Insurant::ResumeAccount**		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation `I_Account_Management_Insurant::ResumeAccount` technisch um. Mit dieser Operation wird das Paket mit den Daten aus der Akte eines Versicherten beim vorhergehenden Anbieter ePA-Aktensystem bezogen und importiert.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Account_Management_Insurant/v1.0/ResumeAccount		
Eingangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**
Package URL	URL, über die das vom vorhergehenden Anbieter ePA-Aktensystem erzeugte	URL mit Prozentkodierung	n

	Exportpaket geladen werden kann		
X-User Assertion	Authentication Assertion des authentifizierten des Versicherten als Inhaber der Akte	SAML 2.0 Assertion gemäß [gemSpec_Authentisierung_Vers# A_14109, A_15631]	n
Technische Fehlermeldungen			
Name	**Fehlertext**	**Details**	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
ASSERTION_INVALID	Die übergebene Authentication Assertion ist ungültig.	Die Gültigkeitsdauer ist abgelaufen oder die Signatur ist ungültig	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.		

[<=]

5.2.1.2.1 Umsetzung

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

A_15526 - Komponente ePA-Dokumentenverwaltung – Voraussetzungen für die Ausführung von Resume Account
Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass die Operation `I_Account_Management_Insurant::ResumeAccount` nur ausgeführt wird, wenn der Verarbeitungskontext eines für einen Anbieterwechsel mit Übernahme der Aktendaten registriertes Aktenkonto erstmalig durch den Versicherten geöffnet wurde.**[<=]**

A_15568 - Komponente ePA-Dokumentenverwaltung – Policy Enforcement für Resume Account
Die Komponente ePA-Dokumentenverwaltung MUSS die registrierten und anwendbaren Zugriffsrichtlinien aus zur Verfügung stehenden Policy Documents (Advanced Patient

Privacy Consents) entsprechend der Anforderung A_14822 durchsetzen, bevor die Operation `I_Account_Management_Insurant::ResumeAccount` ausgeführt wird. Bei einer negativen Autorisierungsentscheidung MUSS die Nachricht mit dem `ACCESS_DENIED`-Fehlercode quittiert werden.**[<=]**

A_15013 - ePA-Aktensystem – Download des Exportpakets
Das ePA-Aktensystem MUSS nach Eingang des Requests `I_Account_Management_Insurant::ResumeAccount` das mittels des Aufrufparameters `PackageURL` referenzierte Exportpaket beim vorhergehenden Anbieter ePA-Aktensystem des Versicherten abrufen und für den Import durch den Verarbeitungskontext der ePA-Dokumentenverwaltung verfügbar machen.**[<=]**

A_14905 - Komponente ePA-Dokumentenverwaltung – Import des Exportpakets des vorhergehenden Aktenkontos
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS das vom vorhergehenden Anbieter ePA-Aktensystem des Versicherten bezogene Exportpaket, vom vorhergehenden Anbieter herunterladen sobald es dort verfügbar ist und in das neue Aktenkonto importieren und dazu:

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

[<=]

A_15596 - Komponente ePA-Dokumentenverwaltung – Ersetzen der Home Community ID
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS beim Import eines Exportpakets in sämtlichen Metadatensätzen den anbieterspezifischen Wert in den Feldern DocumentEntry.homeCommunityId und SubmissionSet.homeCommunityId sowie DocumentEntry.repositoryUniqueId mit der neuen Home Community ID aktualisieren.**[<=]**

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-Modul Frontend des Versicherten muss jedoch nicht auf den Abschluss warten, weil der Vorgang auf Ebene der Dienste asynchron abgeschlossen ist, nachdem der Versicherte ihn mittels des Aufrufs der Operation `I_Account_Management_Insurant::SuspendAccount` beim alten Anbieter und dem direkt anschließenden Aufruf der Operation `I_Account_Management_Insurant::ResumeAccount` beim neuen Anbieter ausgelöst hat.

A_15624 - Komponente ePA-Dokumentenverwaltung – Abfrage auf Verfügbarkeit des Exportpakets
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS nach dem Aufruf der Operation `I_Account_Management_Insurant::ResumeAccount` bei unmittelbar vorgesehenem Abruf des Exportpakets bis zum Erfolgsfall periodisch prüfen,

jedoch maximal für einen Zeitraum von drei Werktagen, ob ein Exportpaket unter der vom Client übergebenen URL bereitsteht.**[<=]**

A_15625 - Komponente ePA-Dokumentenverwaltung – Kein Aktenzugriff während des Imports der Daten
Die Komponente ePA-Dokumentenverwaltung MUSS während der Ausführung der Operation `I_Account_Management_Insurant::ResumeAccount` für ein Aktenkonto alle Operationen mit Fehlermeldung "Aktenkonto aufgrund einer andauernden Datenmigration vorübergehend nicht erreichbar" ablehnen.**[<=]**

A_16077 - Komponente ePA-Dokumentenverwaltung – Frist für den Import des Exportpakets
Die Komponente ePA-Dokumentenverwaltung MUSS den Import eines Exportpakets innerhalb von drei Werktagen nach Beginn des Downloads vom vorherigen Anbieter abschließen.
[<=]

A_17845 - Komponente ePA-Dokumentenverwaltung – Offener Verarbeitungskontext während der Verarbeitung des Exportpakets
Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS den für die Operation `I_Account_Management_Insurant::ResumeAccount` geöffneten Verarbeitungskontext so lange geöffnet lassen, bis der Abruf des Exportpakets beim alten Anbieter erfolgt ist und die Verarbeitung der Daten des Exportpakets durch diesen Verarbeitungskontext abgeschlossen ist, jedoch maximal drei Tage, falls kein Exportpaket abgerufen werden kann.
[<=]

5.2.1.3 Operation I_Account_Management_Insurant::GetAuditEvents

A_14490-01 - Komponente ePA-Dokumentenverwaltung – Signatur für Get Audit Events
Die Komponente ePA-Dokumentenverwaltung MUSS die Operation `I_Account_Management_Insurant::GetAuditEvents` gemäß der folgenden Signatur implementieren:

Tabelle 21: Tab_Dokv_28 - Operation Get Audit Events

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

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

[<=]

5.2.1.3.1 Umsetzung

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

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

[<=]

A_15583 - Komponente ePA-Dokumentenverwaltung – Ablauflogik für Get Audit Events
Die Komponente ePA-Dokumentenverwaltung MUSS die Liste der § 291a-Protokolleinträge als Liste `phr:AuditMessage` zurückgeben.**[<=]**

5.3 Zugriffskontrolle

5.3.1 Grob-, mittel- und feingranulare Berechtigungen

Die Zugriffskontrolle ~~basiert auf drei Zugriffsgruppen, welche Dokumente in~~ muss sicherstellen, dass nur solche Zugriffe zugelassen werden, die ~~elektronische Patientenakte eines~~vom Versicherten ~~einstellen. Diese Zugriffsgruppen müssen den einzustellenden Dokumenten jeweils ein vorbestimmtes, nicht änderbares Kennzeichen zuordnen, was ihre Zugriffsgruppe repräsentiert. Diese Gruppen sind:~~

~~Zugriffsgruppe der~~ berechtigt wurden. Zur Berechtigungsvergabe an Leistungserbringerinstitutionen~~, wobei der Leistungserbringer dieses Dokument einstellt~~ (LEI) stehen dem Versicherten dazu grundsätzlich drei Ansätze zur Verfügung:

- ~~Zugriffsgruppe des Versicherten, wobei der Versicherte (oder sein berechtigter Vertreter) dieses Dokument einstellt~~
- ~~Zugriffsgruppe des Kostenträgers, wobei der Kostenträger dieses Dokument einstellt~~

~~Einer Leistungserbringerinstitution werden im Rahmen der Autorisierung durch den Versicherten bzw. seines Vertreters Zugriffsrechte auf Dokumente mit diesen Zugriffsgruppen gewährt. Dies kann in beliebiger Kombination entweder ad-hoc beim Arztbesuch oder über das ePA-Modul Frontend des Versicherten erfolgen. Von einem Versicherten bzw. seinen Vertreter vergebene Zugriffsrechte an eine Leistungserbringerinstitution auf die Dokumente der Zugriffsgruppe des Versicherten oder des Kostenträgers beinhalten das Lesen und Löschen von Dokumenten. Weiterhin haben Mitarbeiter von Leistungserbringerinstitutionen die Möglichkeit, ein Dokument gesondert als leistungserbringeräquivalent zu kennzeichnen, was das Aktualisieren der Dokumentmetadaten erfordert – siehe unten.~~

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

~~Weiterhin können Mitarbeiter aus Leistungserbringerinstitutionen – sofern ein Zugriffsrecht besteht – die Sichtbarkeit bzw. den Zugriff auf Dokumente, die der Zugriffsgruppe der Versicherten oder Kostenträger zugeordnet sind, erweitern. Das bedeutet, ein einzelnes Dokument, welches von einem Versicherten oder einem Kostenträger eingestellt wurde, kann von einem Leistungserbringer als "leistungserbringeräquivalent" gekennzeichnet werden, wenn es für die Behandlung eines Patienten relevant erscheint und auch andere Leistungserbringer darauf Zugriff erhalten sollen. Dies ermöglicht, dass Leistungserbringer ohne Zugriff auf Dokumente des Versicherten oder auf die eingestellten Dokumente eines Kostenträgers dennoch behandlungsrelevante Dokumente einsehen können (nur lesender Zugriff). Der Zugriffsgruppe der Leistungserbringerinstitutionen werden daher implizit auch Zugriffsrechte auf Dokumente mit diesem Kennzeichen eingeräumt. Dieses Kennzeichen kann jederzeit wieder von einem Mitarbeiter einer Leistungserbringerinstitution entfernt werden. All diese Zugriffsszenarien haben keinen Einfluss auf das omnipräsente Lese-~~

~~und Löschrecht auf Dokumente des Versicherten. Das bedeutet, dass der Versicherte bzw. sein Vertreter alle Dokumente aus allen Zugriffsgruppen lesen oder löschen kann.~~

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

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

5.3.2 Berufsgruppenspezifische Einschränkungen

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

Beispielsweise haben Apotheker grundsätzlich keinen Zugriff auf die zahnärztlichen Dokumente des Versicherten. Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen, ändern oder löschen.

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

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

5.3.3 Grundsätzliche Umsetzung der Berechtigungsregeln

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

1. Dynamische Berechtigungsfreigaben (wie z. B. die Entscheidung, welche LEI überhaupt vom Versicherten berechtigt werden, in welcher Stufe, welchen

Kategorien und mit welchen Ausnahmen) werden vom über "Policies" in die Dokumentenverwaltung eingestellt oder auch gelöscht.

2. Unabänderliche Regeln (wie die gesetzlich motivierten Vorgaben für Berufsgruppen) werden über entsprechende AFOs realisiert, insbesondere A_19303. Es ist natürlich umsetzender Software möglich, auch diese Regeln über interne Policies durchzusetzen.

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

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

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

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

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

5.3.4 Vergabe von Zugriffsregeln

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

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

Alle erteilten Zugriffsrechte werden zeitlich begrenzt vergeben. Die Dauer wird für jede einzelne Rechtevergabe vom Versicherten festgelegt und beträgt maximal 540 Tage.

Zusätzlich können für die Upgrade-Phase von ePA 1 zu ePA 2 von Systemen, die nur ePA 1-fähig sind, der OID 1.2.276.0.76.5.491 und dem Code System Name "ePA-Vertraulichkeit" die folgenden Codes dem confidentialityCode zugeordnet sein:

- Code = "LEI", Display Name = "Dokument einer Leistungserbringerinstitution"
- Code = "KTR", Display Name = "Dokument eines Kostenträgers"
- Code = "PAT", Display Name = "Dokument eines Versicherten"

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

- ~~Code = "LEÄ", Display Name="Leistungserbringeräquivalentes Dokument eines Versicherten oder Kostenträgers"~~

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

~~5.3.1~~5.3.5 Funktionsprinzip Policy Administration

Die Berechtigungsvergabe an Leistungserbringerinstitutionen und Vertreter des Versicherten erfolgt durch das Einstellen von Policy Documents (siehe nachstehende Abbildung). Diese Dokumente werden in den Abschnitten 5.3.~~2~~6.2 bis 5.3.~~2~~6.5 für die ePA-Fachanwendung definiert und setzen ferner das Zugriffskontrollmodell Attribute-based Access Control (ABAC) um.

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

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

A_14998 - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen vom Policy Document bei neuem Policy Document mit demselben Berechtigten
Die Komponente ePA-Dokumentenverwaltung MUSS über die Operationen `I_Document_Management::CrossGatewayDocumentProvide` sowie `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b` eine Prüfung auf ein bereits registriertes Policy Document (Advanced Patient Privacy Consent) mit demselben Berechtigten sowie der Aktenidentität (d.h. `xacml:SubjectMatch` und `xacml:ResourceMatch` sind identisch) durchführen und bei Existenz dieses Policy Documents (Advanced Patient Privacy Consent) dieses samt IHE ITI-XDS-Metadaten löschen, bevor ein neues Policy Document gespeichert wird.
[<=]

A_14892-01~~A_14892~~ - Komponente ePA-Dokumentenverwaltung – Automatisiertes Löschen ungültiger Policy Documents
Die Komponente ePA-Dokumentenverwaltung SOLL in Policy ~~Documents (Advanced Patient Privacy Consents) und zugehörige IHE ITI-XDS-Metadaten löschen~~-Dokumenten enthaltene Regeln (<Rule>-Elemente) löschen, wenn ~~diese Policy Documents~~sie ihre ihre

zeitliche Gültigkeit verlieren. Sollte infolgedessen ein Policy-Dokument keine gültigen Regeln mehr enthalten, SOLL die ePA-Dokumentenverwaltung auch das Policy-Dokument selbst und die dazugehörigen IHE XDS-Metadaten löschen.
[<=]

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.
[<=]

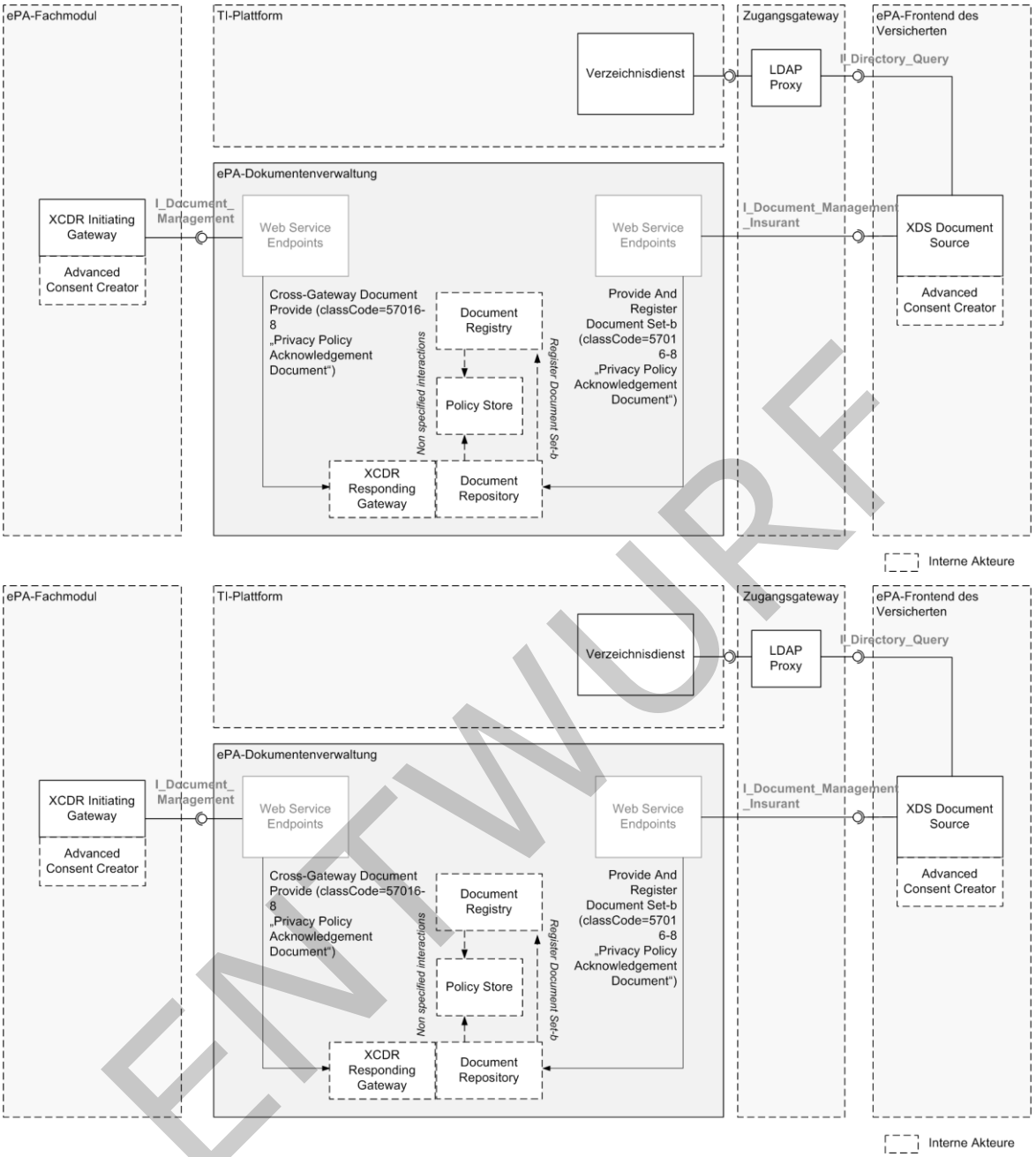

Abbildung 2: Schematische Darstellung zur Vergabe von Berechtigungen

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

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

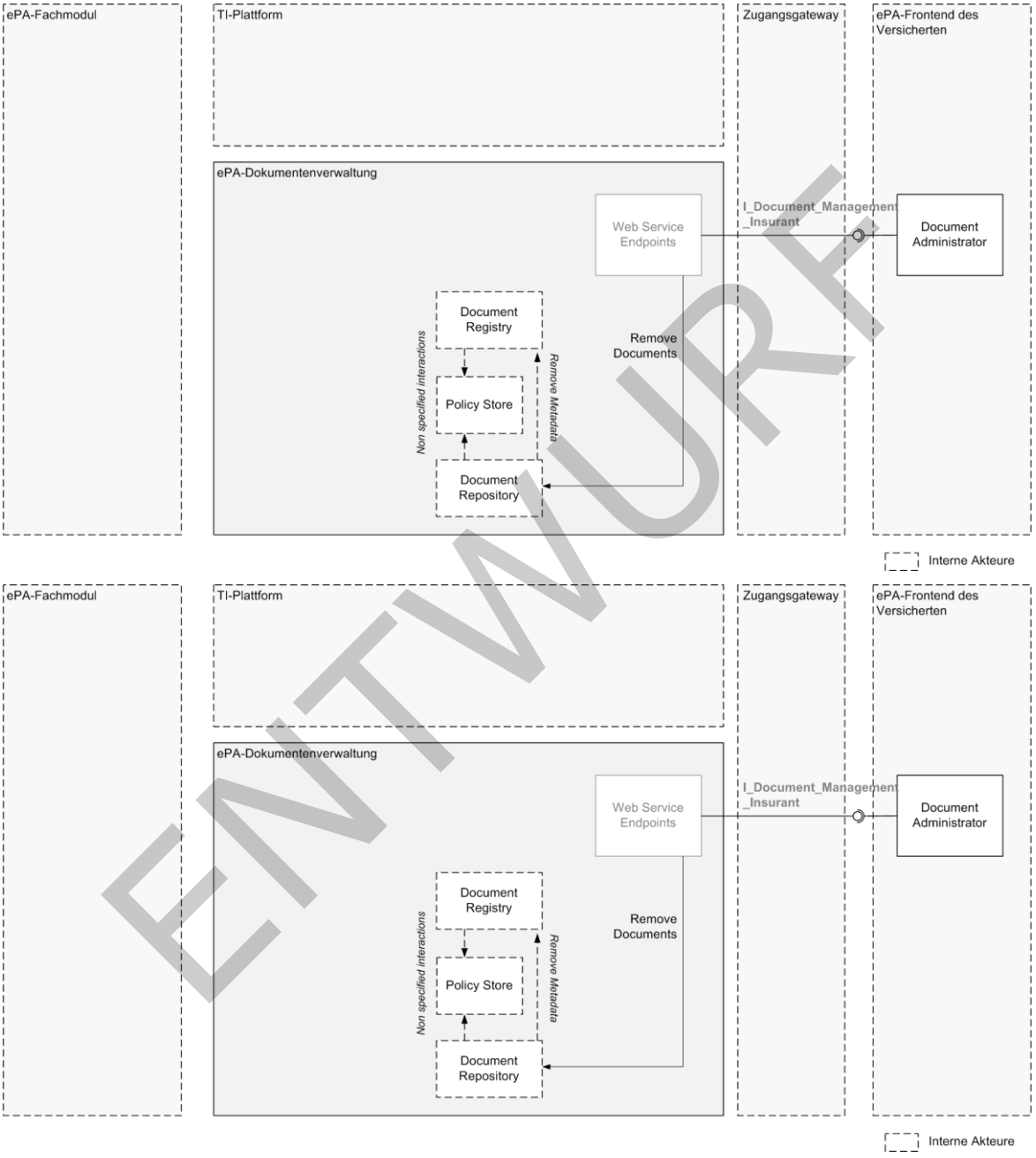

Abbildung 3: Schematische Darstellung zum Entzug von Berechtigungen

~~5.3.2~~5.3.6 Anforderungen an die Zugriffskontrollprüfung

Die Zugriffskontrollprüfung innerhalb des Verarbeitungskontextes der Komponente ePA-Dokumentenverwaltung erfolgt aufbauend auf einer Grundeinstellung, die jeden Zugriff

verweigert, wenn er nicht explizit erlaubt ~~istund~~ist und setzt die Berechtigungsszenarien ~~aus [gemSysL_ePA#Tabelle 4: Übersicht über Berechtigungsszenarien] um~~.

A_19303 - Komponente ePA-Dokumentenverwaltung – Berufgruppenspezifische Zugriffsunterbindungsregeln

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

Tabelle 22 : Tab_Dokv_030 - Zugriffsunterbindungsregeln

Dokumentenkategorie gemäß § 341 PDSG		Zugriffsrecht										
		Arzt	**ZArzt**	**Apo**	Psych	Pflege	Heba	Phys	GD	AM	KTR	Ver
Satz												Identifier aus [gemSpec_DM#Tab_DM_Dokumentenkategorie]
1a1	category_diagnostic_medical	CRUD	CRUD	R	CRUD	R	R	CRUD	-	-	-	RD
1a2	category_diagnostic_dental	CRUD	CRUD	R	CRUD	R	R	CRUD	-	-	-	RD
1a3	category_diagnostic_psych	CRUD	CRUD	R	CRUD	R	R	CRUD	-	-	-	RD
1a4	category_diagnostic_other	CRUD	CRUD	R	CRUD	R	R	CRUD	-	-	-	RD
1b	category_emp	CRUD	CRUD	CRUD	CRUD	R	R	R	-	-	-	RD
1c	category_nfd	CRUD	CRUD	R	CRUD	R	R	R	-	-	-	RD
1d	category_eab	CRUD	CRUD	R	CRUD	R	R	R	-	-	-	RD

2	category_dentalrecord	CR UD	CR UD	-	CR UD	-	-	-	-	-	-	RD
3	category_childsrecord	CR UD	CR UD	R	CR UD	R	CR UD	R	R	-	-	RD
4	category_mothersrecord	CR UD	CR UD	R	CR UD	R	CR UD	R	-	-	-	RD
5	category_vaccination	CR UD	CR UD	CR UD	CR UD	R	R	R	CR UD	CR UD	-	RD
6	category_patientdoc	RD	RD	RD	RD	R	R	R	-	-	-	CRUD
7	category_ega	RD	RD	RD	RD	R	R	R	-	-	C U	RD
8	category_receipt	RD	RD	RD	RD	R	R	R	-	-	C U	RD
11	category_prescription	CR UD	CR UD	CR UD	CR UD	R	R	R	-	-	-	RD

Legende der Zugriffsrecht CRUD, Zuordnung zur Operation:

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

Legende der Institutionen, Zuordnung zur `ProfessionOID`:

- Arzt=oid_praxis_arzt, oid_krankenhaus, oid_vorsorge_reha, oid_sanitaetsdienst_bundeswehr;
- ZArzt=oid_zahnarztpraxis;
- Apo=oid_öffentliche_apotheke;
- Psych=oid_praxis_psychotherapeut;
- Pflege=oid_institution_pflege;
- Heba=oid_geburtshilfe;
- Phys=oid_praxis_physiotherapeut;

- GD=oid_gesundheitsdienst;
- AM=oid_arbeitsmedizin;
- KTR=oid_kostentraeger;

Legende Zugriffsberechtigte, Zuordnung über KVNR:

- Ver=Versicherter/Vertreter;

[<=]

A_15173-02~~A_15173~~ - Komponente ePA-Dokumentenverwaltung – Zugriffsstrategie "Opting-in" mit "Access Deny" als Standardeinstellung
Die Komponente ePA-Dokumentenverwaltung MUSS jeden Zugriff verweigern, der nicht auf der Grundlage definierter Policy Documents (Advanced Patient Privacy Consents) in Kombination mit der entsprechenden Operation gemäß A_19303, A_19997 und A_19998 explizit erlaubt ist.**[<=]**

Policy Documents~~, welche die Berechtigung für klassifizierte Nutzer~~ nach Anhang C steuern ~~(d.h. für~~ den ~~Versicherten, seine~~erlaubten Zugriff für Versicherte, deren Vertreter, für Leistungserbringerinstitutionen sowie Kostenträger~~), referenzieren jeweils eine statische, akteninterne XACML 2.0 Policy (Permission Policy), welche die zulässigen~~. Tatsächlich sind die erlaubten Operationen ~~(in XACML 2.0 sogenannte~~ für alle diese Gruppen jedoch statisch: Sobald ein bestimmter Leistungserbringer (oder ein Angehöriger einer anderen Gruppe) grundsätzlich berechtigt ist, stehen die erlaubten Operationen (Dokumente einstellen, suchen, herunterladen, ...) unveränderlich fest.

Aus diesem Grund ist der Bereich "Actions~~) und~~", der die ~~mit diesen verbundenen ressourcenbezogenen Bedingungen festlegt. Diese statischen Policies müssen für~~erlaubten Operationen üblicherweise in APPC-Policy-Dokumenten beschreibt dort nicht gesetzt, um die ~~Zugriffskontrollprüfung innerhalb des Verarbeitungskontextes verfügbar sein~~APPC-Dokumente übersichtlich zu halten. Stattdessen werden die gemäß Berufsgruppe zur Verfügung stehenden Operationen in Tab_Dokv_030 (via A_15173-02) festgelegt und geprüft.

Beispiel: Ein gemäß APPC-Policy-Dokument berechtigter Kostenträger darf nur Dokumente der Kategorie 7 und ~~verlassen die~~ 8 zugreifen, und zwar nach Tabelle ausschließlich mittels C-Operation (create), d.h. I_Document_Management::CrossGatewayDocumentProvide. Ein Zugriff auf andere Dokumentenkategorien würde durch das APPC-Policy-Dokument verhindert, ein Zugriff durch andere Operationen (bspw. ein Löschen via I_Document_Management::RemoveDocuments) durch Tab_Dokv_030.

A_19997 - Zugriff durch Versicherten auf Schnittstelle I_Account_Management_Insurant
Die Komponente ePA-Dokumentenverwaltung MUSS dem Versicherten über A_15173-02 hinaus den Zugriff auf die Operationen der Schnittstelle I_Document_Management_Insurant erlauben.**[<=]**

~~nicht. XACML 2.0 Policies, welche interne Permission Policies referenzieren, heißen im Folgenden Base Policies.~~

A_19998 - Zugriff durch Vertreter auf Operation I_Account_Management_Insurant::GetAuditEvents
Die Komponente ePA-Dokumentenverwaltung MUSS einem berechtigten Vertreter des Versicherten über A_15173-02 hinaus den Zugriff auf die Operation I_Account_Management_Insurant::GetAuditEvents() erlauben.
[<=]

A_14933 - Komponente ePA-Dokumentenverwaltung – XML Schema-Validierung eines Policy Documents
Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Documents (Advanced Patient Privacy Consents) dieses einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen. Ist ein Policy Document nicht wohlgeformt oder gültig, MUSS die Komponente ePA-Dokumentenverwaltung die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren.**[<=]**

A_15536-01~~A_15536~~ - Komponente ePA-Dokumentenverwaltung – Prüfungen bei Registrierung eines Policy Documents
Die Komponente ePA-Dokumentenverwaltung MUSS bei Registrierung eines Policy Documents (Advanced Patient Privacy Consents) folgende inhaltlichen Prüfungen durchführen und im Fehlerfall die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren:

- *Prüfung der XACML 2.0 Policy-Konformität*
  Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn das Profil der vorliegenden XACML 2.0 Policy nicht mit den Anforderungen aus den Abschnitten 5.3.~~2.2 bis 5.3.2.5 übereinstimmt. Dabei MUSS die Verwendung der PolicySetIdReference(n) zur intendierten Berechtigung passen. Das heißt, eine XACML 2.0 Policy für die Berechtigung eines Kostenträgers darf beispielsweise nur die PolicySetIdReference mit dem Wert "urn:gematik:policy-set-id:permissions-access-group-insurance" verwenden~~6.2 bis 5.3.6.5 übereinstimmt.
- *Prüfung der Aktenidentität*
  Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn das `Resource`-Element mit der Attribut-ID "`urn:ihe:iti:ser:2016:patient-id`" nicht mit der Identität der Akte aus dem internen Policy Document mit der Policy Set ID "`urn:gematik:policy-set-id:insurant`" übereinstimmt.
- *Prüfung des Einstellers*
  Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn die in der Nachricht enthaltene SAML 2.0 Assertion (Authentication Assertion / X-User Assertion) nicht dem Versicherten oder einem seiner Vertreter zugeordnet ist (d.h. das `root`-Attribut des `InstanceIdentifier`-Elements innerhalb des `SubjectMatch`-Elements muss mit der OID "`1.2.276.0.76.4.8`" eine KVNR kennzeichnen).
- *Keine Verwendung des "xsi:schemaLocation"-Attributs*
  Die Komponente ePA-Dokumentenverwaltung MUSS die Verarbeitung der XACML 2.0 Policy abbrechen, wenn ein xsi:schemaLocation-Attribut gemäß [XMLSchema#2.6.3] enthalten ist.

[<=]

A_14822-01~~A_14822~~ - Komponente ePA-Dokumentenverwaltung – Attribute für Anfrage einer Autorisierungsentscheidung
Die Komponente ePA-Dokumentenverwaltung MUSS das "Policy Pull"-Muster gemäß [IHE-ITI-ACWP] umsetzen und die folgenden Daten für eine Berechtigungsprüfung extrahieren sowie eine Autorisierungsanfrage gegen die vorhandenen Policy Documents (Advanced Patient Privacy Consents) stellen, um die autorisierte Verarbeitung eines Dokuments sicherzustellen:

- Subject ID oder XSPA Organization ID der Authentication Assertion / X-User Assertion

- unveränderbarer Teil der KVNR aus der Eingangsnachricht oder serverseitig mit Hilfe von Anfrageparametern beschafft (Aktenidentität)
- `wsa:Action`-Element aus der Eingangsnachricht
- ggf. ~~Confidentiality Code des Dokuments~~Metadaten des DocumentEntry (u.a. confidentialityCode) und des dazugehörigen SubmissionSets

[<=]

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

~~5.3.2.1~~5.3.6.1 Erstmaliges Öffnen eines Verarbeitungskontextes

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

A_15603 - Komponente ePA-Dokumentenverwaltung – Nur Resume Account bei erforderlicher Datenübernahme möglich
Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass ausschließlich die Operation `I_Account_Management_Insurant::ResumeAccount` ausgeführt werden kann, wenn der Verarbeitungskontext erstmalig vom Versicherten geöffnet wurde und eine Übernahme von Daten aus dem Aktenkonto des Versicherten bei einem vorherigen Anbieter erforderlich ist, d.h. das Aktenkonto mit der Option "Registered for Migration" registriert wurde.**[<=]**

~~5.3.2.2~~5.3.6.2 Berechtigung für einen Versicherten

A_15437-01~~A_15437~~ - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Versicherten
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_~~100~~500 in Anhang ~~B~~C durchsetzen~~. (Base Policy).~~
[<=]

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

A_15250 - Komponente ePA-Dokumentenverwaltung – Aktivierung des Policy Documents "urn:gematik:policy-set-id:insurant"
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS eine Personalisierung durchführen. Dazu MUSS die Komponente ePA-Dokumentenverwaltung das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "`urn:gematik:policy-set-id:insurant`" aktivieren und anschließend die darin festgelegten Regeln bei Zugriffsanfragen durchsetzen. Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die Personalisierung im Zuge des ersten

Aufrufs einer fachlichen Operation durchführen und das Policy Document unmittelbar auf die fachliche Operation anwenden, die die Personalisierung ausgelöst hat. Der Aufruf der Operation`I_Document_Management_Connect::OpenContext` zur kryptographischen Aktivierung gilt in diesem Zusammenhang nicht als fachliche Operation.**[<=]**

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

A_15178 - Komponente ePA-Dokumentenverwaltung – Unveränderliches Policy Document "urn:gematik:policy-set-id:insurant"
Die Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "`urn:gematik:policy-set-id:insurant`" nach ihrer Aktivierung kontinuierlich und dauerhaft unverändert für die Zugriffskontrollprüfung wirksam ist.**[<=]**

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

~~**5.3.2.3 Die Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_101 in Anhang B erstellen und durchsetzen (Permission Policy).**~~
~~**[<=]**~~

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

~~**5.3.2.45.3.6.3 Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "`urn:gematik:policy-set-id:permissions-access-group-insurant`" über Suchoperationen NICHT dem ePA-Frontend des Versicherten zur Verfügung stellen. Ferner DARF es NICHT heruntergeladen werden können. [<=]**~~

~~5.3.2.5~~5.3.6.4 Berechtigung für einen Vertreter

~~A_15440-01~~A_15440 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Vertreters
Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten übermittelte XACML 2.0 Policy auf Konformität als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in Tab_Dokv_~~200~~501 in Anhang ~~B (Base Policy)~~C prüfen.~~-~~
[<=]

A_15441-01~~A_15441~~ - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Vertreters mit erlaubten Operationen

Die Komponente ePA-Dokumentenverwaltung MUSS eine XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_~~201~~501 in Anhang ~~B~~ C erstellen und durchsetzen~~. (Permission Policy).~~

[<=]

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

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

~~**[<=]**~~

~~Ein Vertreter darf keine weiteren Vertreter, sondern ausschließlich Leistungserbringerinstitutionen, berechtigen.~~

A_15180 - Komponente ePA-Dokumentenverwaltung – Prüfung auf weitere, unerlaubte Vertreterberechtigungen

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

[<=]

~~5.3.2.6~~5.3.6.5 Berechtigung für eine Leistungserbringerinstitution

A_15442-02~~A_15442-01~~ - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung einer Leistungserbringerinstitution

Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten bzw. vom Fachmodul ePA übermittelte XACML 2.0 Policy auf Konformität als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt ~~in~~von Tab_Dokv_~~300-01~~502 in Anhang C prüfen.

[<=]

~~**Tabelle 22: Tab_Dokv_300-01 – XACML 2.0 Policy für eine Leistungserbringerinstitution (Base Policy)**~~

~~Element-, Attribut- oder Textknoten gemäß [XACML]~~	~~Opt.~~	~~Nutzungsvorgabe~~
~~PolicySet~~	~~R~~	
~~@PolicySetId~~	~~R~~	~~Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.~~

@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
Target	R	Das Element MUSS leer bleiben.
<!-- Leistungserbringerinstitution (repräsentiert durch ihre Telematik-ID) -->		
Subjects	R	
Subject	R	
SubjectMatch	R	
@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
AttributeValue	R	
@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
InstanceIdentifier	R	
@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
@root	R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt werden.
@extension	R	Als Wert MUSS die Telematik-ID gesetzt werden.
SubjectAttributeDesignator	R	
@AttributeId	R	Der Wert "urn:gematik:subject:organization-id" MUSS gesetzt werden.
@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
Subject	R	
SubjectMatch	R	

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

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

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

	text()	R	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: • "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"

[<=]

A_15519 - Komponente ePA-Dokumentenverwaltung - Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung einer Leistungserbringerinstitution mit erlaubten Operationen

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

[<=]

A_15242 - Komponente ePA-Dokumentenverwaltung - Keine Herausgabe des Policy Documents "urn:gematik:policy-set-id:permissions-access-group-hcp"

5.3.2.8 Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-id:permissions-access-group-hcp" über Suchoperationen NICHT dem ePA-Frontend des Versicherten zur

~~Verfügung stellen. Ferner DARF es NICHT heruntergeladen werden können.[<=]~~

~~A_15243 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe des Policy Documents "urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents"~~

~~5.3.2.9 Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents" über Suchoperationen NICHT dem ePA-Frontend des Versicherten zur Verfügung stellen. Ferner DARF es NICHT heruntergeladen werden können.[<=]~~

~~A_17459 - Komponente ePA-Dokumentenverwaltung – Keine Herausgabe des Policy Documents "urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents"~~

~~5.3.2.10~~5.3.6.6 ~~Die Komponente ePA-Dokumentenverwaltung DARF das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents" über Suchoperationen NICHT dem ePA-Frontend des Versicherten zur Verfügung stellen. Ferner DARF es NICHT heruntergeladen werden können.[<=]~~

~~5.3.2.11~~5.3.6.7 Berechtigung für einen Kostenträger

A_17460-01~~A_17460~~ - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Kostenträgers

Die Komponente ePA-Dokumentenverwaltung MUSS eine vom ePA-Frontend des Versicherten übermittelte XACML 2.0 Policy auf Konformität als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an den Inhalt in Tab_Dokv_~~400~~503 in Anhang ~~B (Base Policy)~~ C prüfen.**[**<=**]**

~~5.3.3~~5.3.7 Upgrade von ePA Release 3.1.3 auf ePA Release 4

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

~~A_17461 - Komponente ePA-Dokumentenverwaltung – Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung eines Kostenträgers mit erlaubten Operationen~~Die Komponente ePA-Dokumentenverwaltung MUSS sämtliche XACML 2.0 Policies gemäß Anhang B umwandeln in XACML 2.0 Policies gemäß Anhang C, sobald

- eine XACML 2.0 Policy ~~als~~ gemäß Anhang B eingestellt wird,
- ein Zugriffsversuch auf eine XACML 2.0 Policy ~~Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in Tab_Dokv_401 in Anhang B erstellen und durchsetzen (Permission Policy).[<=]~~ gemäß Anhang B erfolgt.

[<=]

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

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

- Das Ablaufdatum MUSS übernommen werden.
- Bei der Ersetzung der XACML 2.0 Policies ohne Versionsangabe (alt) durch XACML 2.0 Policies mit Versionsangabe (neu) MÜSSEN folgende Zugriffsregeln umgesetzt werden (Zugriffsrecht alt wird zu Zugriffsrecht neu):
- alt: LEI, neu: `category_treatment*`, `category_emp`, `category_nfd`, `category_eab`;
- alt: PAT, neu: `category_patientdoc`;
- alt: KTR, neu: `category_receipt`;
- neu: Die Vertrauensstufe "normal" (grobgranulare Berechtigung) wird vergeben

[<=]

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

~~**A_17462 - Komponente ePA-Dokumentenverwaltung - Keine Herausgabe des Policy Documents "urn:gematik:policy-set-id:permissions-access-group-insurance"**~~Die Komponente ePA-Dokumentenverwaltung ~~DARF das Policy Document (Advanced Patient Privacy Consent) mit der Policy Set ID "`urn:gematik:policy-set-id:permissions-access-group-insurance`" über Suchoperationen NICHT dem ePA-Frontend des~~MUSS bei allen Dokumenten eines Versicherten, bei denen der `confidentialityCode` "PAT", "LEI", "LEÄ" oder "KTR" gesetzt ist, diesen Eintrag löschen und stattdessen den `confidentialityCode` "normal" setzen.

[<=~~ zur Verfügung stellen. Ferner DARF es NICHT heruntergeladen werden können.~~[<=~~]~~

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

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

- alt: LEI, neu: `category_treatment*`, `category_emp`, `category_nfd`, `category_eab`;
- alt: PAT, neu: `category_patientdoc`;
- alt: KTR, neu: `category_receipt`;

[<=]

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

5.4 Vertrauenswürdige Ausführung

5.4.1 Schnittstelle I_Document_Management_Connect

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

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

A_15587 - Komponente ePA-Dokumentenverwaltung – Implementierung des sicheren Verbindungsprotokolls
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS für die Schnittstelle `I_Document_Management_Connect` das Kommunikationsprotokoll gemäß den Vorgaben aus [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6] umsetzen.
[<=]

A_15592-01 - Komponente ePA-Dokumentenverwaltung – Erweiterung des sicheren Verbindungsprotokolls
Ein Client (d.h. ePA-Fachmodul, ePA-Modul Frontend des Versicherten, Fachmodul ePA KTR-Consumer) MUSS bei der Erzeugung der VAUClientHello-Nachricht (vgl. A_16883-01) im „Authorization-Assertion“-Datenfeld die Base64-kodierte Authorization-Assertion eintragen.

Weiterhin MUSS der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung ein optionales Schlüssel-Wert-Paar zur Übermittlung eines Sitzungsbezeichners an das Kontextmanagement im HTTP-Request-Header prüfen und akzeptieren. Das Schlüssel-Wert-Paar hat die Form
`Session: ...Sitzungsbezeichner vom Zugangsgateway...`**[<=]**

A_14631 - Komponente ePA-Dokumentenverwaltung – HTTP-Schnittstelle I_Document_Management_Connect
Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die Schnittstelle `I_Document_Management_Connect` für über das Zugangsgateway vermittelte HTTP-Verbindungen des ePA-Moduls Frontends des Versicherten verfügbar machen.**[<=]**

A_15540 - Komponente ePA-Dokumentenverwaltung – TLS-Schnittstelle I_Document_Management_Connect
Das Kontextmanagement der Komponente ePA-Dokumentenverwaltung MUSS die Schnittstelle `I_Document_Management_Connect` für TLS-Verbindungen des Fachmoduls

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

- die Base64-dekodierte Authorization Assertion der `VAUClientHello`-Nachricht auf Gültigkeit gemäß Anforderung A_13690 sowie auf den gültigen Berechtigungstyp (`AuthorizationType` = "`DOCUMENT_AUTHORIZATION`") prüfen und bei ungültiger Authorization Assertion den Verbindungsaufbau abbrechen und mit dem HTTP-Fehler 403 antworten,
- den Record Identifier des Verarbeitungskontextes über den Wert des Attributs `Resource ID` aus der Authorization Assertion der `VAUClientHello`-Nachricht ermitteln,
- für Clients vom Typ ePA-Modul Frontend des Versicherten die Verbindung auf der Grundlage des vom Zugangsgateway gesetzten HTTP Header-Feldes `Session` registrieren,
- für Clients vom Typ Fachmodul ePA die Verbindung auf Grundlage der TLS-Sitzung 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_14617 - Komponente ePA-Dokumentenverwaltung – Ablauf des Verbindungsaufbaus
Die Komponente ePA-Dokumentenverwaltung MUSS den Verbindungsaufbau von Clients, d.h. von einem ePA-Modul Frontend des Versicherten oder einem Fachmodul so umsetzen, dass der folgende Ablauf in angegebener Reihenfolge ausgeführt wird, nachdem ein HTTP Request mit einer `VAUClientHello`-Nachricht von einem Client empfangen wurde:

Tabelle 23: Tab_Dokv_29 - Ablauf Operation Hello

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

		Authorization Assertion.
2	Kontextmanagement	Extrahieren des Record Identifiers über den Wert des Attributs `XSPA Resource ID` aus der Authorization Assertion
3	Kontextmanagement	Prüfen, ob ein Verarbeitungskontext für den Record Identifier bereits initialisiert ist und Starten eines Verarbeitungskontextes, falls dies nicht der Fall ist
4	Kontextmanagement	Registrieren der Verbindung zwischen dem Client und dem Verarbeitungskontext für den Record Identifier für die Vermittlung des folgenden Nachrichtenaustauschs
5	Kontextmanagement	Weiterleiten der `VAUClientHello`-Nachricht an den Verarbeitungskontext für den Record Identifier
6	Verarbeitungskontext	Registrieren der Authorization Assertion der `VAUClientHello`-Nachricht und Erzeugen der `VAUServerHello`-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
7	Verarbeitungskontext	Senden der `VAUServerHello`-Nachricht
8	Kontextmanagement	Weiterleiten der `VAUServerHello`-Nachricht an den Client
9	Verarbeitungskontext	Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
	(Client)	(Ableiten des Sitzungsschlüssels gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
	(Client)	(Erzeugen und Senden der `VAUClientSigFin`-Nachricht)
10	Kontextmanagement	Prüfen auf Identität des authentifizierten Nutzers (Subject::Subject-id bzw. Subject::Organization-id der Authorization Assertion entspricht der KVNR bzw. Telematik-ID des übergebenen Zertifikats der Client-Authentisierung gemäß [gemSpec_Krypt#A_17070]) Im Fehlerfall MUSS der Verbindungsaufbau abgebrochen und mit einer `VAUServerError`-Nachricht beantwortet werden.
11	Kontextmanagement	Weiterleiten der `VAUClientSigFin`-Nachricht an den Verarbeitungskontext für den `RecordIdentifier` Record Identifier

12	Verarbeitungskontext	Erzeugen der `VAUServerFin`-Nachricht gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]
13	Kontextmanagement	Weiterleiten der `VAUServerFin`-Nachricht an den Client

[<=]

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

A_14545 - Komponente ePA-Dokumentenverwaltung – Operationen des Dokumentenmanagements nur über sicheren Kanal nutzbar
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS die folgenden Operationen ausschließlich über den sicheren Kanal zwischen dem ePA-Modul Frontend des Versicherten bzw. dem Fachmodul ePA und dem Verarbeitungskontext verfügbar machen:

- `I_Document_Management::CrossGatewayDocumentProvide`
- `I_Document_Management::CrossGatewayQuery`
- `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::RegistryStoredQuery`
- `I_Document_Management_Insurant::RemoveDocuments`
- `I_Document_Management_Insurant::RetrieveDocumentSet`
- `I_Account_Management_Insurant::GetAuditEvents`
- `I_Account_Management_Insurant::SuspendAccount`
- `I_Account_Management_Insurant::ResumeAccount`
- `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 - Komponente ePA-Dokumentenverwaltung – Nutzung des sicheren Kanals zwischen ePA-Modul Frontend des Versicherten bzw. Fachmodul ePA, Fachmodul ePA KTR-Consumer und Verarbeitungskontext
Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS den mit dem ePA-Modul Frontend des Versicherten bzw. mit dem Fachmodul ePA sowie dem Fachmodul ePA KTR-Consumer gemäß [gemSpec_Krypt#3.15] und [gemSpec_Krypt#6]

ausgehandelten Sitzungsschlüssel verwenden, um alle Eingangsnachrichten zu entschlüsseln und alle Ausgangsnachrichten zu verschlüsseln.**[<=]**

A_14457 - Komponente ePA-Dokumentenverwaltung – Implementierung der Schnittstelle I_Document_Management_Connect
Die Komponente ePA-Dokumentenverwaltung MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle implementieren.

Tabelle 24: Tab_Dokv_30 - Schnittstelle I_Document_Management_Connect

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

[<=]

5.4.1.1 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 25: Tab_Dokv_31 - Operation OpenContext

Operation	**I_Document_Management_Connect::OpenContext**
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] definierte Operation `I_Document_Management_Connect::OpenContext` technisch um. Mit dieser Operation wird der Kontextschlüssel an den Verarbeitungskontext übergeben.

Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0/OpenContext		
Eingangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**
ContextKey	Der Kontextschlüssel	`ContextKey`	n
Ausgangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**
-	-	-	-
Technische Fehlermeldungen			
Name	**Fehlertext**	**Details**	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	
INVALID_AUT_KEY	Der Kontextschlüssel ist ungültig.	Wenn der Vergleich mit einem bereits im Verarbeitungskontext vorhandenen Kontextsschlüssel keine Übereinstimmung ergibt, oder das Entschlüsseln von Kontextdaten fehlschlägt	
SYNTAX_ERROR	Fehlerhafter Aufrufparameter	Es wurde ein fehlerhafter Aufrufparameter übergeben.	

[<=]

5.4.1.1.1 Umsetzung

A_14687 - 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-Modul Frontend des Versicherten, ein Fachmodul ePA oder ein Fachmodul ePA KTR-Consumer, der folgende Ablauf in angegebener Reihenfolge (1 - 6) ausgeführt wird:

Tabelle 26: Tab_Dokv_32 - Ablauf der Operation Open Context

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

[<=]

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

5.4.1.2 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 27: Tab_Dokv_33 - Operation Close Context

Operation	**I_Document_Management_Connect::CloseContext**		
Beschreibung	Diese Operation setzt die in [gemSysL_ePA] in definierte Operation `I_Document_Management_Connect::CloseContext` technisch um. Mit dieser Operation wird die Verbindung zum Verarbeitungskontext beendet. Der Verarbeitungskontext kann geschlossen werden, falls nicht eine andere Verbindung noch besteht.		
Formatvorgaben	SOAP Action: http://ws.gematik.de/fd/phr/I_Document_Management_Connect/v1.0/CloseContext		
Eingangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**
-	-	-	-
Ausgangsparameter			
Name	**Beschreibung**	**Typ**	**opt.**
-	-	-	-
Technische Fehlermeldungen			
Name	**Fehlertext**	**Details**	
INTERNAL_ERROR	Es ist ein interner Fehler aufgetreten.	Interner Fehler in der Verarbeitungslogik	

[<=]

5.4.1.2.1 Umsetzung

A_14707-01~~A_14707~~ - 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-Modul Frontend des Versicherten, ein Fachmodul ePA oder ein Fachmodul ePA KTR-Consumer, der folgende Ablauf in angegebener Reihenfolge (1 - 6) ausgeführt wird:

Tabelle 28: Tab_Dokv_34 - Ablauf Operation ~~OpenContext~~CloseContext

Nr.	Sub-Komponente	Beschreibung
	(Client)	(Senden der `CloseContextRequest`-Nachricht über den sicheren Kanal zwischen Client und Verarbeitungskontext)
1	Kontextmanagement	Weiterleiten der `CloseContextRequest`-Nachricht an den Verarbeitungskontext gemäß den vorgehaltenen Zuordnungsdaten (siehe Anforderung A_14633)
2	Verarbeitungskontext	Senden der `CloseContextResponse`-Nachricht
3	Kontextmanagement	Weiterleiten der `CloseContextResponse`-Nachricht an den Client
4	Verarbeitungskontext	Prüfen, ob mindestens eine weitere Sitzung existiert, ignorieren der `CloseContextRequest`-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

[<=]

5.4.2 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.

6 Informationsmodelle

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

7 Anhang A – Verzeichnisse

7.1 Abkürzungen

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

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

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

7.4 Tabellenverzeichnis

7.5 Referenzierte Dokumente

7.5.1 Dokumente der gematik

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

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

[gemSpec_TBAuth]	gematik: Spezifikation Tokenbasierte Authentisierung
[gemSysL_ePA]	gematik: Systemspezifisches Konzept ePA

7.5.2 Weitere Dokumente

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

[IHE-ITI-TF2b]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf
[IHE-ITI-TF2x]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2x) – Volume 2 Appendices, Revision 15.1, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf
[IHE-ITI-TF3]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Transaction Specifications and Content Specifications, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf
[IHE-ITI-XCDR]	IHE International (2017): IHE IT Infrastructure (ITI) Technical Framework Supplement, Cross-Community Document Reliable Interchange (XCDR), Revision 1.4 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[OWASP-IP]	Open Web Application Security Project (OWASP) (2017): Input Validation Cheat Sheet, https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet
[OWASP-SAML]	Open Web Application Security Project (OWASP) (2017): SAML Security Cheat Sheet, https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet
[OWASP-WSS]	Open Web Application Security Project (OWASP) (2017): Web Service Security Cheat Sheet, https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, http://tools.ietf.org/html/rfc2119
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231,

	https://tools.ietf.org/html/rfc7231
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), https://www.w3.org/TR/soap12-part1/
[WSA]	OASIS (2004): Web Services Addressing (WS-Addressing), https://www.w3.org/Submission/ws-addressing/
[WSIAP]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, ~~http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile~~ http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[WSIBSP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html
[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
[WSS-SAML]	OASIS (2006): Web Services Security: SAML Token Profile 1.1, https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf
[XACML]	OASIS (2005): eXtensible Access Control Markup Language (XACML) Version 2.0, https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/

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

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

Tabelle 29: Tab_Dokv_99 - Kennzeichnung von Optionalitäten in XACML 2.0 Policies

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

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

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

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

@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
<!-- 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 den unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
ResourceAttributeDesignator	R	

@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
@DataType	R	Der Wert "urn: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 31: 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: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 "`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:CrossGatewayDocumentProvide" MUSS gesetzt werden.
		ActionAttributeDesignator		R	
			@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- 'ProvideAndRegisterDocumentSet-b' -->					

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

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

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

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

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

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

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

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

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

										action:action-id" MUSS gesetzt werden.
						@DataType			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	
							@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.
<!-- 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:xacml:1.0:function:anyURI-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/fd/phr/I_Account_Management_Insurant/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.

3000 8.2 Policy Document für einen Vertreter

3001 8.2.1 Base Policy

3002 **Tabelle 32: Tab_Dokv_200 - XACML 2.0 Policy für einen Vertreter (Base Policy)**

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

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

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

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

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

8.2.2 Permission Policy

Tabelle 33: 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: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 "`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:CrossGatewayDocumentProvide" MUSS gesetzt werden.
		ActionAttributeDesignator		R	
			@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:action:action-id" MUSS gesetzt werden.
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
<!-- 'ProvideAndRegisterDocumentSet-b' -->					

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

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

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

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

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

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

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

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

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

											action:action-id" MUSS gesetzt werden.
							@DataType			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	
							@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.
<!-- 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:xacml:1.0:function:anyURI-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/fd/phr/I_Account_Management_Insurant/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.
			@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 34 Tabelle : Tab_Dokv_300-01 - XACML 2.0 Policy für eine Leistungserbringerinstitution (Base Policy)

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
@PolicyCombiningAlgId	R	Der Wert "`urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides`" MUSS gesetzt werden.
Target	R	Das Element MUSS leer bleiben.
<!-- Leistungserbringerinstitution (repräsentiert durch ihre Telematik-ID) -->		
Subjects	R	
Subject	R	
SubjectMatch	R	

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

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

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

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

	text()	R	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: • "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"

~~8.3.1~~8.3.2 Permission Policy zum Zugriff auf Leistungserbringer-Dokumente

Tabelle 35: 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]	Opt.	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 Leistungserbringerinstitution" MUSS gesetzt werden.
			ResourceAttributeDesignator			R	
				@AttributeId		R	Der Wert "urn:ihe:iti:appc:2016:confidentiality-code" MUSS gesetzt werden.
				@DataType		R	Der Wert "urn: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: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	R	Der Wert "Dokument einer Leistungserbringerinstitution" MUSS gesetzt werden.
								ResourceAttributeDesignator			R	
									@AttributeId		R	Der Wert "urn:ihe:iti:appc:2016:confidentiality-code" MUSS gesetzt werden.
									@DataType		R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
									@MustBePresent		R	Der Wert "true" MUSS gesetzt werden.
						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 "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:appc:2016:confidentiality-code" MUSS gesetzt werden.
			@DataType		R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
			@MustBePresent			Der Wert "true" MUSS gesetzt werden.
<!-- Registry Stored Query 'FindDocuments' -->						
Action					R	

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

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

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

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

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

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

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

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

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

						ActionAttributeDesignator		R	
							@AttributeId	R	Der Wert "`urn:oasis:names:tc:xacml:1.0:action:action-id`" MUSS gesetzt werden.
							@DataType	R	Der Wert "`http://www.w3.org/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/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/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: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' -->										
				Action					R	
					Action Match				R	

							@MatchId				R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
							AttributeValue				R	
								@DataType			R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
								text()			R	Der Wert "urn:ihe:iti:2007: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.
						Action Match					R	
							@MatchId				R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
							AttributeValue				R	
								@DataType			R	Der Wert "http://www.w3.org/2

								001/XMLSchema#anyURI " MUSS gesetzt werden.
				text()			R	Der Wert "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" MUSS gesetzt werden.
			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.	
<!-- 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.

~~8.3.2~~8.3.3 Permission Policy zum Zugriff auf Versicherten- und Kostenträger-Dokumente

Tabelle 36: Tab_Dokv_302 - XACML 2.0 Policy mit erlaubten Operationen für eine Leistungserbringerinstitution zum Zugriff auf Versicherten- und Kostenträger-Dokumente (Permission Policy)

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

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

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

				@codeSystemName	R	Der Wert "ePA-Vertraulichkeit" MUSS gesetzt werden.
				@displayName	O	Der Wert "Dokument eines Kostenträgers" aus MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Kostenträger eingestellt wurden (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents"). Der Wert "Dokument eines Versicherten" MUSS gesetzt werden, sofern diese Policy den Zugriff auf Dokumente erlaubt, welche von einem Versicherten oder seinen berechtigten Vertreter eingestellt wurden (@PolicySetId="urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents").
			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	
<!-- Registry Stored Query 'FindDocuments' -->						
	Action				R	
		ActionMatch			R	
			@MatchId		R	Der Wert "`urn:oasis:names:tc:xacml:1.0:function:anyURI-equal`" MUSS gesetzt werden.
			AttributeValue		R	
				@DataType	R	Der Wert "`http://www.w3.org/2001/XMLSchema#anyURI`" MUSS gesetzt werden.
				text()	R	Der Wert "`urn:ihe:iti:2007:CrossGatewayQuery`" MUSS gesetzt werden.
			ActionAttributeDesignator		R	
				@AttributeId	R	Der Wert "`urn:oasis:names:tc:xacml:1.0:action:action-id`" MUSS gesetzt werden.
				@DataType	R	Der Wert "`http://www.w3.org/2001/XMLSchema#anyURI`" MUSS gesetzt werden.
		ActionMatch			R	
			@MatchId		R	Der Wert "`urn:oasis:names:tc:x`

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

					01/XMLSchema#anyURI" MUSS gesetzt werden.
ActionMatch				R	
	@MatchId			R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
	AttributeValue			R	
		@DataType		R	Der Wert "http://www.w3.org/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/20

					01/XMLSchema#anyURI" MUSS gesetzt werden.
			text()	R	Der Wert "urn:uuid:5c4f972b-d56b-40ac-a5fc-c8ca9b40b9d4" MUSS gesetzt werden.
		ActionAttributeDesignator		R	
			@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: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/20`

					01/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:x

					acml:1.0:function:anyURI-equal" MUSS gesetzt werden.
		AttributeValue		R	
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			text()	R	Der Wert "urn: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/20

					01/XMLSchema#anyURI" MUSS gesetzt werden.
	ActionMatch			R	
		@MatchId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:anyURI-equal" MUSS gesetzt werden.
		AttributeValue		R	
			@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#anyURI" MUSS gesetzt werden.
			text()	R	Der Wert "urn:uuid: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/20

					01/XMLSchema#anyURI" MUSS gesetzt werden.
			text()	R	Der Wert "urn:uuid:d90e5407-b356-4d91-a89f-873917b4b0e6" MUSS gesetzt werden.
		ActionAttributeDesignator		R	
			@AttributeId	R	Der Wert "urn:ihe:iti:2016:RegistryStoredQuery: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/20`

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

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

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

8.4 Policy Document für einen Kostenträger

8.4.1 Base Policy

Tabelle 37: Tab_Dokv_400 - XACML 2.0 Policy für einen Kostenträger (Base Policy)

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

@PolicySetId	R	Es MUSS ein URN-kodierter, global eindeutiger Identifikator gemäß den Vorgaben aus [IHE-ITI-TF2x#Appendix B] vergeben werden.
@PolicyCombiningAlgId	R	Der Wert "`urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides`" MUSS gesetzt werden.
Target	R	Das Element MUSS leer bleiben.
<!-- Kostenträger (repräsentiert durch ihre Betriebsnummer) -->		
Subjects	R	
Subject	R	
SubjectMatch	R	
@MatchId	R	Der Wert "`urn:hl7-org:v3:function:II-equal`" MUSS gesetzt werden.
AttributeValue	R	
@DataType	R	Der Wert "`urn:hl7-org:v3#II`" MUSS gesetzt werden.
InstanceIdentifier	R	
@xmlns	R	Der Wert "`urn:hl7-org:v3`" MUSS gesetzt werden.
@root	R	Der Wert "`1.2.276.0.76.4.188`" MUSS gesetzt werden.
@extension	R	Als Wert MUSS die Betriebsnummer gesetzt werden.
SubjectAttributeDesignator	R	

@AttributeId	R	Der Wert "urn:gematik:subject:organization-id" MUSS gesetzt werden.
@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
Subject	R	
SubjectMatch	R	
@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
AttributeValue	R	
@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
text()	R	Als Wert MUSS der Name des Kostenträgers gesetzt werden.
SubjectAttributeDesignator	R	
@AttributeId	R	Der Wert "urn:oasis:names:tc:xspa:1.0:subject:organization" MUSS gesetzt werden.
@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVNR als Aktenidentifikator -->		
Resources	R	
Resource	R	

ResourceMatch	R	
@MatchId	R	Der Wert "urn: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-insurance" MUSS gesetzt werden.

8.4.2 Permission Policy

Tabelle 38: 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.

3029

9 Anhang C– XACML 2.0-Profile für Policy Documents

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

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

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

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

9.1 Policy Document für einen Versicherten

Tabelle 40: Tab_Dokv_500 - XACML 2.0 Policy für einen Versicherten

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

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

@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
<!-- 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 den unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
ResourceAttributeDesignator	R	

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

9.2 Policy Document für einen Vertreter

Tabelle 41: Tab_Dokv_501 - XACML 2.0 Policy für einen Vertreter

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.
@Version	R	Der Wert "4.0" MUSS gesetzt werden.
Target	R	Das Element MUSS leer bleiben.
<!-- Vertreter (repräsentiert durch seine KVNR) -->		

Subjects	R	
Subject	R	
SubjectMatch	R	
@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
AttributeValue	R	
@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
InstanceIdentifier	R	
@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
@extension	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
SubjectAttributeDesignator	R	
@AttributeId	R	Der Wert "urn:gematik:subject:subject-id" MUSS gesetzt werden.
@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.

Subject	R	
SubjectMatch	R	
@MatchId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
AttributeValue	R	
@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
text()	R	Der Common Name des X.509 Subject Name der eGK MUSS gesetzt werden, um die Lesbarkeit für den Versicherten im ePA-Modul Frontend des Versicherten zu erhöhen, d.h. wem er ein Zugriffsrecht eingeräumt hat.
SubjectAttributeDesignator	R	
@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:subject:subject" MUSS gesetzt werden.
@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- KVNR als Aktenidentifikator -->		
Resources	R	
Resource	R	
ResourceMatch	R	

@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
AttributeValue	R	
@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
InstanceIdentifier	R	
@xmlns	R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
@root	R	Der Wert "1.2.276.0.76.4.8" MUSS gesetzt werden.
@extension	R	Als Wert MUSS der unveränderbare Teil der KVNR (10 Stellen) gesetzt werden.
ResourceAttributeDesignator	R	
@AttributeId	R	Der Wert "urn:ihe:iti:ser:2016:patient-id" MUSS gesetzt werden.
@DataType	R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
PolicySetIdReference	R	
text()	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-representative" MUSS gesetzt werden.

9.3 Policy Document für eine Leistungserbringerinstitution

Tabelle 42: Tab_Dokv_502 - XACML 2.0 Policy für eine Leistungserbringerinstitution

Element-, Attribut- oder Textknoten gemäß [XACML]	Opt.	Nutzungsvorgabe
PolicySet	R	
@PolicySetId	R	Der Wert "urn:gematik:policy-set-id:permissions-access-group-hcp" MUSS gesetzt werden.
@PolicyCombiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides" MUSS gesetzt werden.
@Version	R	Der Wert "4.0" MUSS gesetzt werden.
Target	R	Das Element MUSS leer bleiben.
<!-- Leistungserbringerinstitution (repräsentiert durch ihre Telematik-ID) -->		
Subjects	R	
Subject	R	
SubjectMatch	R	
@MatchId	R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.

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

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

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

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

					AttributeValue			R	
						@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
						text()		R	Der Wert muss dem Enddatum (Format YYYY-MM-DD nach ISO 8601:2004) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen: "heute" + frei eintragbare Anzahl Tage in der Spanne von 1 bis 540
					EnvironmentAttributeDesignator			R	
						@AttributeId		R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.
						@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
	<!-- Prüfung der grobgranularen Berechtigung -->								
	Policy							R	
		@PolicyId						R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp-level" MUSS gesetzt werden.

		@RuleCombiningAlgId									R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides" 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.
			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 "N" MUSS gesetzt werden.
								@codeSystem	R	Der Wert "2.16.840.1.113883.5.25" MUSS gesetzt werden.
								@displayName	O	Der Wert "normal" 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.
					Resource				O	Das <Resource> Element MUSS gesetzt sein, wenn auch erweiterte Berechtigung erteilt werden soll.
					<! -- Bei "erweiterter Berechtigung" <Resource> Element wiederholen mit folgender Abweichung: (@code, @codeSystem, @displayName) = ("R", "2.16.840.1.113883.5.25", "restricted") -->					
		Rule							R	Default Rule, das immer "Deny" liefert.
			@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 "Deny" MUSS gesetzt werden.
	<!-- Prüfung der mittelgranularen Berechtigung (Kategorien Teil 1) -->									
	Policy								R	
		@PolicyId							R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp-categories" MUSS gesetzt werden.
		@RuleComibiningAlgId							R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides" MUSS gesetzt werden.
		<!-- Kategorie "category_emp" -->								
		Rule							O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "Elektronischer Medikationsplan" berechtigt werden soll.
			@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.
			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 "urn:gematik:ig:Medikationsplan:r3.1" MUSS gesetzt werden.
								@codeSystem		R	Der Wert "1.3.6.1.4.1.19376.3.276.1.5.6" MUSS gesetzt werden.
						ResourceAttributeDesignator					
							@AttributeId			R	Der Wert "urn:ihe:iti:appc:2016:document-entry:

									format-code" MUSS gesetzt werden. Der Wert "urn:ihe:iti:appc:2016:document-entry:format-code" ist derzeit nicht durch [IHE-ITI-APPC] abgedeckt. Der angegebene Wert MUSS analog zu "urn:ihe:iti:appc:2016:document-entry:class-code" (fürDocumentEntry.classCode) bezogen auf das Metadatum DocumentEntry.formatCode umgesetzt werden.
							@DataType	R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
							@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
		<!-- Kategorie "category_nfd" -->							
		Rule						O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "category_nfd" berechtigt werden soll.
		<! -- Wie bei "category_emp" mit folgender Abweichung: @code="urn:gematik:ig:Notfalldatensatz:r3.1" -->							
		Rule						O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie

				"category_nfd" berechtigt werden soll.
		<! -- Wie bei "category_emp" mit folgender Abweichung: @code="urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1" -->		
		<!-- Kategorie "category_dentalrecord" -->		
		Rule	O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "category_dentalrecord" berechtigt werden soll.
		<! -- Wie bei "category_emp" mit folgender Abweichung: @code="urn:gematik:ig:Zahnbonusheft:r4.0" -->		
		<!-- Kategorie "category_childsrecord" -->		
		Rule	O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "category_childsrecord" berechtigt werden soll.
		<! -- Wie bei "category_emp" mit folgender Abweichung: @code="urn:gematik:ig:Kinderuntersuchungsheft:r4.0" -->		
		<!-- Kategorie "category_mothersrecord" -->		
		Rule	O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "category_mothersrecord" berechtigt werden soll.
		<! -- Wie bei "category_emp" mit folgender Abweichung: @code="urn:gematik:ig:Mutterpass:r4.0" -->		
		<!-- Kategorie "category_vaccination" -->		
		Rule	O	Das <Rule> Element MUSS

				gesetzt sein, wenn auf die Kategorie "category_vaccination" berechtigt werden soll.
		<! -- Wie bei "Elektronischer Medikationsplan" mit folgender Abweichung: @code="urn:gematik:ig:Impfausweis:r4.0" -->		
		<!-- Kategorie "category_prescription" -->		
		Rule	O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "category_prescription" berechtigt werden soll.
		<! -- Wie bei "category_emp" mit folgender Abweichung: @code="urn:gematik:ig:Verordnungsdatensatz:r4.0" -->		
		<!-- Kategorie "category_patientdoc" -->		
		Rule	O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "category_patientdoc" berechtigt werden soll.
		<! -- Wie bei "category_emp" mit folgenden Abweichungen: • *@code="102"* • *@codeSystem="1.3.6.1.4.1.19376.3.276.1.5.14"* • *@AttributeId="urn:gematik:ig:document-entry:related-submission-set:author-role:id" -->*		Der Wert "urn:gematik:ig:document-entry:related-submission-set:author-role:id" als Attributidentifikator wird derzeit nicht von [IHE-ITI-APPC] unterstützt und MUSS wie folgt umgesetzt werden: Der Wert wählt das zum angefragten DocumenEntry dazu gehörige (d.h. das einzige per

											Assoziation damit verbundene) `SubmissionSet` und darin das Metadatum `authorRole` aus.
		<!-- Kategorie "`category_ega`" -->									
		Rule								O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "`category_ega`" berechtigt werden soll.
			@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.
			Resources								
				Resource						R	
					Resource Match					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 "<OID>" MUSS gesetzt werden.	
							@extension		R	Als Wert MUSS "eGA" gesetzt werden.	
					ResourceAttributeDesignator				R		
						@AttributeId			R	Der Wert "urn:ihe:iti:appc:2016:document-entry:reference-id" MUSS gesetzt werden.	
						@DataType			R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.	
						@MustBePresent			R	Der Wert "true" MUSS gesetzt werden.	

			<!-- Kategorie "category_receipt" -->							
		Rule							O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "category_receipt" berechtigt werden soll.
			@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.
			Resources						R	
				Resource					R	
					Resource Match				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 "VER" MUSS gesetzt werden.	
								@codeSystem	R	Der Wert "1.3.6.1.4.1.19376.3.276.1.5.3" MUSS gesetzt werden.	
						ResourceAttributeDesignator					
							@AttributeId		R	Der Wert "urn:ihe:iti:appc:2016:document-entry:healthcare-facility-type-code" MUSS gesetzt werden.	
							@DataType		R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.	
							@MustBePresent		R	Der Wert "true" MUSS gesetzt werden.	
				Resource					R		
					Resource Match				R		
						@MatchId			R	Der Wert "urn:hl7-org:v3:function:C	

											V-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 "ABRE" MUSS gesetzt werden.
								@codeSystem		R	Der Wert "1.3.6.1.4.1.19376.3.276.1.5.9" MUSS gesetzt werden.
						ResourceAttributeDesignator					
							@AttributeId			R	Der Wert "urn:ihe:iti:appc:2016:document-entry:type-code" MUSS gesetzt werden.
							@DataType			R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
							@MustBePresent			R	Der Wert "true" MUSS gesetzt werden.

<!-- Prüfung der mittelgranularen Berechtigung (Kategorien Teil 2: "category_treatment_medical") -->			
Policy		O	Das <Policy> Element MUSS gesetzt sein, wenn auf die Kategorie "category_treatment_medical" berechtigt werden soll.
	@PolicyId	R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp-category-treatment-medical" MUSS gesetzt werden.
	@RuleComibiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Rule	R	
	<!-- Wie bei Kategorie "category_emp" mit Abweichung @Effect="Deny" -->		
	Rule	R	
	<!-- Wie bei Kategorie "category_nfd" mit Abweichung @Effect="Deny" -->		
	Rule	R	
	<!-- Wie bei Kategorie "category_dentalrecord" mit Abweichung @Effect="Deny" -->		
	Rule	R	
	<!-- Wie bei Kategorie "category_childsrecord" mit Abweichung @Effect="Deny" -->		
	Rule	R	

		<!-- Wie bei Kategorie "category_mothersrecord" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_vaccination" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_prescription" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_patientdoc" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_ega" mit Abweichung @Effect="Deny" -->		
		Rule	R	Prüfung, ob Code "KPSY" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		@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 "Deny" MUSS gesetzt werden.
		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 "KPSY" MUSS gesetzt werden.
								@codeSystem	R	Der Wert "1.3.6.1.4.1.19376.3.276.1.5.4" MUSS gesetzt werden.
						ResourceAttributeDesignator				
							@AttributeId		R	Der Wert "urn:ihe:iti:appc:2016:document-entry:practice-setting-code" MUSS gesetzt werden.
							@DataType		R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
							@MustBePresent		R	Der Wert "true" MUSS gesetzt werden.
		Rule							R	Prüfung, ob Code "PSYC" aus Code System "1.3.6.1.4.1.1937

				6.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="PSYC" -->		
		Rule	R	Prüfung, ob Code "FPSY" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="FPSY" -->		
		Rule	R	Prüfung, ob Code "PSYM" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="PSYM" -->		
		Rule	R	Prüfung, ob Code "MZAH" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="MZAH" -->		
		Rule	R	Prüfung, ob Code "PARO" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="PARO" -->		
		Rule	R	Prüfung, ob Code "ZGES" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="ZGES" -->		

		Rule					R	Prüfung, ob Code "MZKH" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="MZKH" -->						
		Rule					R	Prüfung, ob Code "ORAL" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="ORAL" -->						
		Rule					R	Prüfung, ob Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
			@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.
			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.
							CodedValue		R	
								@codeSystem	R	Der Wert "1.3.6.1.4.1.19376.3.276.1.5.4" MUSS gesetzt werden.
						ResourceAttributeDesignator				
							@AttributeId		R	Der Wert "urn:ihe:iti:appc:2016:document-entry:practice-setting-code" MUSS gesetzt werden.
	<!-- Prüfung der mittelgranularen Berechtigung (Kategorien Teil 2: "category_treatment_dental") -->									
	Policy								O	Das <Policy> Element MUSS gesetzt sein, wenn auf die Kategorie "category_treatment_dental" berechtigt werden soll.
		@PolicyId							R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp-category-treatment-dental" MUSS gesetzt werden.

		@RuleCombiningAlgId							R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
		Rule							R	
		<!-- Wie bei Kategorie "category_emp" mit Abweichung @Effect="Deny" -->								
		Rule							R	
		<!-- Wie bei Kategorie "category_nfd" mit Abweichung @Effect="Deny" -->								
		Rule							R	
		<!-- Wie bei Kategorie "category_dentalrecord" mit Abweichung @Effect="Deny" -->								
		Rule							R	
		<!-- Wie bei Kategorie "category_childsrecord" mit Abweichung @Effect="Deny" -->								
		Rule							R	
		<!-- Wie bei Kategorie "category_mothersrecord" mit Abweichung @Effect="Deny" -->								
		Rule							R	
		<!-- Wie bei Kategorie "category_vaccination" mit Abweichung @Effect="Deny" -->								
		Rule							R	
		<!-- Wie bei Kategorie "category_prescription" mit Abweichung @Effect="Deny" -->								
		Rule							R	
		<!-- Wie bei Kategorie "category_patientdoc" mit Abweichung @Effect="Deny" -->								
		Rule							R	

		<!-- Wie bei Kategorie "category_ega" mit Abweichung @Effect="Deny" -->									
		Rule								R	Prüfung, ob Code "MZAH" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
			@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.
			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 "MZAH" MUSS gesetzt werden.

								@codeSystem	R	Der Wert "1.3.6.1.4.1.19376.3.276.1.5.4" MUSS gesetzt werden.
						ResourceAttributeDesignator			R	
							@AttributeId		R	Der Wert "urn:ihe:iti:appc:2016:document-entry:practice-setting-code" MUSS gesetzt werden.
							@DataType		R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
							@MustBePresent		R	Der Wert "true" MUSS gesetzt werden.
		Rule							R	Prüfung, ob Code "PARO" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "MZAH" mit Abweichung @code="PARO" -->								
		Rule							R	Prüfung, ob Code "ZGES" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "MZAH" mit Abweichung @code="ZGES" -->								
		Rule							R	Prüfung, ob Code "MZKH" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist

		<!-- Wie bei Rule zur Prüfung auf "MZAH" mit Abweichung @code="MZKH" -->									
		Rule								R	Prüfung, ob Code "MZKH" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "MZAH" mit Abweichung @code="MZKH" -->									
		Rule								R	Prüfung, ob Code "ORAL" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "MZAH" mit Abweichung @code="ORAL" -->									
		Rule								R	Prüfung, ob Code "KIEF" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "MZAH" mit Abweichung @code="KIEF" -->									
		Rule								R	Prüfung, ob Code "MZAH" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "PSY" mit Abweichung @code="MZAH" -->									
		<!-- Prüfung der mittelgranularen Berechtigung (Kategorien Teil 2: "category_treatment_psych") -->									
	Policy									O	Das <Policy> Element MUSS gesetzt sein, wenn auf die Kategorie "category_treatment_psych" berechtigt werden soll.

		@PolicyId	R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp-category-treatment-psych" MUSS gesetzt werden.
		@RuleComibiningAlgId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
		Rule	R	
		<!-- Wie bei Kategorie "category_emp" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_nfd" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_dentalrecord" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_childsrecord" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_mothersrecord" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_vaccination" mit Abweichung @Effect="Deny" -->		
		Rule	R	

		<!-- Wie bei Kategorie "category_prescription" mit Abweichung @Effect="Deny" -->								
		Rule							R	
		<!-- Wie bei Kategorie "category_patientdoc" mit Abweichung @Effect="Deny" -->								
		Rule							R	
		<!-- Wie bei Kategorie "category_ega" mit Abweichung @Effect="Deny" -->								
		Rule							R	Prüfung, ob Code "KPSY" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
			@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.
			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 "KPSY" MUSS gesetzt werden.
								@codeSystem	R	Der Wert "1.3.6.1.4.1.19376.3.276.1.5.4" MUSS gesetzt werden.
						ResourceAttributeDesignator				
							@AttributeId		R	Der Wert "urn:ihe:iti:appc:2016:document-entry:practice-setting-code" MUSS gesetzt werden.
							@DataType		R	Der Wert "urn:hl7-org:v3#CV" MUSS gesetzt werden.
							@MustBePresent		R	Der Wert "true" MUSS gesetzt werden.
		Rule							R	Prüfung, ob Code "PSYC" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="PSYC" -->								
		Rule							R	Prüfung, ob Code "FPSY" aus Code System "1.3.6.1.4.1.1937

											6.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="FPSY" -->									
		Rule								R	Prüfung, ob Code "PSYM" aus Code System "1.3.6.1.4.1.19376.3.276.1.5.4" gesetzt ist
		<!-- Wie bei Rule zur Prüfung auf "KPSY" mit Abweichung @code="PSYM" -->									
	<!-- Prüfung der mittelgranularen Berechtigung (Kategorien Teil 2: "category_treatment_other") -->										
	Policy									O	Das <Policy> Element MUSS gesetzt sein, wenn auf die Kategorie "category_treatment_other" berechtigt werden soll.
		@PolicyId								R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp-category-treatment-other" MUSS gesetzt werden.
		@RuleCombiningAlgId								R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
		Rule								R	
		<!-- Wie bei Kategorie "category_emp" mit Abweichung @Effect="Deny" -->									
		Rule								R	

		<!-- Wie bei Kategorie "category_nfd" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_dentalrecord" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_childsrecord" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_mothersrecord" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_vaccination" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_prescription" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_patientdoc" mit Abweichung @Effect="Deny" -->		
		Rule	R	
		<!-- Wie bei Kategorie "category_ega" mit Abweichung @Effect="Deny" -->		
		Rule	R	Prüfung, ob Code System "1.3.6.1.4.1.19376.3.276.1.5.5" gesetzt ist
		@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.
			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.
							CodedValue			R	
								@codeSystem		R	Der Wert "1.3.6.1.4.1.19376.3.276.1.5.5" MUSS gesetzt werden.
						ResourceAttributeDesignator				R	
							@AttributeId			R	Der Wert "urn:ihe:iti:appc:2016:document-entry:practice-setting-code" MUSS gesetzt werden.

<!-- Prüfung der feingranularen Berechtigung: Blacklist -->								
Policy							R	
	@PolicyId						R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp-blacklist" MUSS gesetzt werden.
	@RuleComibiningAlgId						R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides" MUSS gesetzt werden.
	Rule						O	Das <Rule> Element MUSS genau einmal pro gesperrtem Dokument vorhanden sein.
		@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 "Deny" MUSS gesetzt werden.
		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 MUSS dem Wert von "DocumentEntry.uniqueId" des zu sperrenden Dokuments entsprechen.
					ResourceAttributeDesignator			
						@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:resource:resource-id" MUSS gesetzt werden.
						@DataType	R	Der Wert "http//www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
<!-- Prüfung der feingranularen Berechtigung: WhiteList -->								
	Policy						R	
		@PolicyId					R	Der Wert "urn:gematik:policy-id:permissions-access-group-hcp-whitelist" MUSS gesetzt werden.
		@RuleComibiningAlgId					R	Der Wert "urn:oasis:names:tc:xacml:1.0:rule-combining-

										algorithm:permit-overrides" MUSS gesetzt werden.
		Rule							O	Das <Rule> Element MUSS genau einmal pro freigegebenen Dokument vorhanden sein.
			@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.
			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 MUSS dem Wert von "DocumentEntry.uniqueId" des zu sperrenden

									Dokuments entsprechen.
						ResourceAttributeDesignator		R	
							@AttributeId	R	Der Wert "urn:oasis:names:tc:xacml:1.0:resource:resource-id" MUSS gesetzt werden.
							@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.

<OID> für "Importquelle ePA" zu beantragen (siehe <OID>-Platzhalter bei category_ega.

9.4 Policy Document für einen Kostenträger

Tabelle 43: Tab_Dokv_503 - XACML 2.0 Policy für einen Kostenträger

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:permit-overrides" MUSS gesetzt werden.
	@Version				R	Der Wert "4.0" MUSS gesetzt werden.
	Target				R	Das Element MUSS leer bleiben.
	<!-- Kostenträger (repräsentiert durch ihre Betriebsnummer) -->					
	Subjects				R	
	Subject				R	
	SubjectMatch				R	
	@MatchId				R	Der Wert "urn:hl7-org:v3:function:II-equal" MUSS gesetzt werden.
	AttributeValue				R	
	@DataType				R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
	InstanceIdentifier				R	
	@xmlns				R	Der Wert "urn:hl7-org:v3" MUSS gesetzt werden.
	@root				R	Der Wert "1.2.276.0.76.4.188" MUSS gesetzt

												werden.
							@extension				R	Als Wert MUSS die Betriebsnummer gesetzt werden.
					SubjectAttributeDesignator						R	
						@AttributeId					R	Der Wert "urn:gematik:subject:organization-id" MUSS gesetzt werden.
						@DataType					R	Der Wert "urn:hl7-org:v3#II" MUSS gesetzt werden.
						@MustBePresent					R	Der Wert "true" MUSS gesetzt werden.
			Subject								R	
				SubjectMatch							R	
					@MatchId						R	Der Wert "urn:oasis:names:tc:xacml:1.0:function:string-equal" MUSS gesetzt werden.
					AttributeValue						R	
						@DataType					R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.

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

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

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

					AttributeValue					R	
						@DataType				R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
						text()				R	Der Wert muss dem Enddatum (Format YYYY-MM-DD nach ISO 8601:2004) aus der folgenden Festlegungen ab der Ausstellung des Policy Documents entsprechen: "heute" + frei eintragbare Anzahl Tage in der Spanne von 1 bis 540
					EnvironmentAttributeDesignator					R	
						@AttributeId				R	Der Wert "urn:oasis:names:tc:xacml:1.0:environment:current-date" MUSS gesetzt werden.
						@DataType				R	Der Wert "http://www.w3.org/2001/XMLSchema#date" MUSS gesetzt werden.
<!-- Prüfung der mittelgranularen Berechtigung (Kategorien) -->											
			<!-- Kategorie "Elektronische Gesundheitsakte" (category_ega) -->								
			Rule							O	Das <Rule> Element MUSS gesetzt sein, wenn auf die

											Kategorie "Elektronische Gesundheitsakte" berechtigt werden soll.
				@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.
				Resources						R	
					Resource					R	
						ResourceMatch				R	
							@MatchId			R	
								@DataType		R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
								text()		R	Der Wert "EGA" MUSS gesetzt werden,
								ResourceAttributeDesignator			
									@AttributeId	R	Der Wert "submissionset.author.authorInstituti

											on" MUSS gesetzt werden.
									@DataType	R	Der Wert "http://www.w3.org/2001/XMLSchema#string" MUSS gesetzt werden.
									@MustBePresent	R	Der Wert "true" MUSS gesetzt werden.
			<!-- Kategorie "category_receipt" (category_receipt) -->								
			Rule							O	Das <Rule> Element MUSS gesetzt sein, wenn auf die Kategorie "category_receipt" berechtigt werden soll.
			<! -- Wie bei "Elektronischer Medikationsplan" mit folgender Abweichung: text()="KTR" -->								

3046