

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Aktensystem ePA für alle

Version:	1.4.0 CC
Revision:	1132068
Stand:	14.02.2025
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_Aktensystem_ePAfueralle

Dokumenteninformationen

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	30.01.2024		ePA für alle	gematik
1.1.0	28.03.2024		ePA für alle - Release 3.0.1	gematik
1.2.0	12.07.2024		ePA für alle - Release 3.0.2, Zuordnungen für Release E- Rezept 1.6.5	gematik
1.3.0	14.08.2024		ePA für alle - Release 3.1.0	gematik
1.4.0 CC	14.02.2025		ePA für alle - Release 3.0.5 (Themen dgMP und Datenausleitung zur Sekundärdatennutzung für ePA für alle 3.1 herausgenommen)	gematik

Inhaltsverzeichnis

1 Einführung	7
1.1 Zielsetzung	7
1.2 Zielgruppe	7
1.3 Geltungsbereich	7
1.4 Abgrenzungen	7
1.5 Methodik	8
2 Übergreifende Festlegungen	9
2.1 Aktensystem- und Service-Lokalisierung	10
2.2 Redundanz	12
2.3 Datenschutz und Sicherheit	13
2.4 Validierungsaktenkonto	18
2.5 Tracing in Nichtproduktivumgebungen	20
2.6 Benutzerführung	21
2.7 Useragent	22
2.8 Datenmigration	23
2.8.1 Herstellerspezifische Umsetzung der Datenmigration	24
2.8.2 Durchführung der Migration	24
2.8.3 Bereinigung von Registry und Repository im Zuge der Migration	25
2.8.4 Protokollierung der Migration	28
2.8.5 Weitere Datenanpassungen	30
2.9 Performance aus Anwendersicht	31
3 Funktionsmerkmale	32
3.1 Aktenkonto eines Versicherten (Health Record)	32
3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte	32
3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger	32
3.1.2 Lebenszyklus und Zustände eines Aktenkontos	33
3.1.3 Anlage eines neuen Aktenkontos	34
3.1.4 Löschen eines Aktenkontos	36
3.2 Health Record Relocation Service	37
3.2.1 Ablauf eines Aktenkontoumzugs	42
3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter	42
3.2.1.2 Start Transfer eines existierenden Aktenkontos	43
3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen Anbieter	43
3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den neuen Anbieter	43
3.2.1.5 Import des Exportpakets durch den neuen Anbieter	44
3.2.1.6 Abschluss des Transfers durch beide Anbieter	44
3.2.1.7 Fehlersituationen und Handhabung	44

3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich oder derzeit nicht möglich	44
3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter	45
3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter	46
3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter	47
3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM	48
3.4 Befugnisverifikations-Modul	51
3.4.1 VAU-Token-Modul	52
3.4.2 Regeln des Befugnisverifikations-Moduls	59
3.5 Vertrauenswürdige Ausführungsumgebung (VAU)	77
3.5.1 Übergreifende VAU-Anforderungen	78
3.5.1.1 Schutz der Integrität der VAU	78
3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU	79
3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU	80
3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM	80
3.5.1.5 Logging und Monitoring	80
3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU	82
3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU ...	82
3.5.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-VAU	83
3.5.2.3 Konsistenz des Systemzustands	84
3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU	84
3.5.4 Zusätzliche Anforderungen an eine Service-VAU	85
3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU	87
3.6 Umschlüsselung und Überschlüsselung	87
3.7 User Session und Health Record Context	91
3.8 Consent Decision Management	92
3.8.1 Widersprüche für Funktionen der ePA	92
3.8.2 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny Policy Medication)	96
3.9 Entitlement Management	98
3.9.1 Initiale Befugnisse (static Entitlements)	105
3.9.2 Erstellen einer Befugnis durch Clients	106
3.9.2.1 Befugnisvergabe durch ein ePA-FdV	107
3.9.2.2 Befugnisvergabe durch ein Primärsystem	109
3.9.3 Löschen von Befugnissen	110
3.9.4 Befugnisausschluss (Blocked User Policy)	111
3.9.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)	113
3.10 Legal Policy	116
3.11 Constraint Management	123
3.11.1 Aktenkontoweites Verbergen (General Deny Policy)	127
3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes	128
3.12 Device Management	128
3.13 Medical Services	132

3.13.1 XDS Document Service	133
3.13.1.1 <i>Formatprüfung beim Einstellen von Dokumenten</i>	134
3.13.1.2 <i>Anforderungen zur Validierung</i>	136
3.13.1.3 <i>Namensräume</i>	138
3.13.1.4 <i>Nutzung von IHE IT Infrastructure-Profilen für Speicherung und Abruf von Dokumenten</i>	138
3.13.1.4.1 <i>Anforderungen an IHE ITI-Akteure</i>	138
3.13.1.4.2 <i>Überblick über gruppierte IHE ITI-Akteure und Optionen</i>	141
3.13.1.4.3 <i>Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen</i> ...	144
3.13.1.4.4 <i>Sicherheitstechnische Vorgaben bei XDS-Operationen</i>	152
3.13.1.5 <i>Fehlerbehandlung in Schnittstellenoperationen</i>	153
3.13.1.6 <i>Schnittstellen im XDS Document Service</i>	154
3.13.1.6.1 <i>Schnittstelle I_Document_Management</i>	154
3.13.1.6.2 <i>Schnittstelle I_Document_Management_Insurant</i>	157
3.13.1.6.3 <i>Schnittstelle I_Document_Management_Ncpeh</i>	159
3.13.1.7 <i>Statische Metadaten</i>	160
3.13.1.8 <i>Nutzungsvorgaben für IHE ITI XDS-Metadaten</i>	162
3.13.1.8.1 <i>Allgemeine Metadatenvorgaben</i>	162
3.13.1.8.2 <i>Metadaten der Dokumente und SubmissionSets</i>	181
3.13.1.8.3 <i>Metadaten für Datenkategorien</i>	185
3.13.1.9 <i>Strukturierte Dokumente</i>	186
3.13.1.9.1 <i>Sammlungstypen</i>	187
3.13.1.9.2 <i>Konfigurierbarkeit</i>	189
3.13.1.10 <i>Verbergen von Dokumenten durch Verwendung des confidentialityCode</i>	190
3.13.1.11 <i>Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die Dokumente des Aktenkontos</i>	190
3.13.1.12 <i>Auswirkungen bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI auf die Dokumente des Aktenkontos</i>	191
3.13.1.13 <i>Protokollierung von Zugriffen auf den XDS Document Service</i>	192
3.13.1.14 <i>Unterstützungsleistung für das ePA-FdV</i>	195
3.13.2 FHIR Data Services.....	196
3.13.2.1 <i>Patient Information Service</i>	196
3.13.2.2 <i>Medication Service</i>	196
3.14 Audit Event Service	203
3.15 Information Service.....	211
3.15.1 Information Service	211
3.15.1.1 <i>Informationen zu Widersprüchen (Consent Decisions)</i>	212
3.15.1.2 <i>Informationen zur Anwenderperformance (UX Performance)</i>	212
3.15.2 Information Service - Account.....	212
3.16 Email Management	213
3.17 Zusätzliche Anforderungen an den Authorization Service.....	214
3.17.1 <i>Anforderungen an den Authorization Service für die Authentisierung von Versicherten (FdV)</i>	215
3.17.2 <i>Anforderungen an den Authorization Service für Authentisierung mit SMC-B</i>	219

3.17.3 Anforderungen an den Authorization Service für die Authentisierung des E-Rezept-Fachdienstes	221
3.18 Anbindung Verzeichnisdienst FHIR-Directory	222
3.19 Access Gateway	222
3.19.1 Paketfilter	222
3.19.1.1 Funktion	222
3.19.1.2 Redundanz	224
3.19.1.3 Konfiguration	224
3.19.1.4 Adressierung	224
3.19.1.4.1 Access Gateway zum Transportnetz Internet	224
3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz	225
3.19.2 Proxy für das VAU-Protokoll	225
3.19.3 Proxy Schlüsselgenerierungsdienst	225
3.19.4 Tracing in Nichtproduktivumgebungen	225
3.19.5 Übergreifende Festlegungen	227
3.20 Schnittstellen (OpenAPI)	228
3.20.1 Übersicht der Schnittstellen des Aktensystems	229
3.20.2 Übergreifende Festlegungen zu den Schnittstellen	237
4 Informationsmodelle	238
5 Anhang A – Verzeichnisse	239
5.1 Abkürzungen	239
5.2 Glossar	240
5.3 Abbildungsverzeichnis	241
5.4 Tabellenverzeichnis	241
5.5 Referenzierte Dokumente	242
5.5.1 Dokumente der gematik	242
5.5.2 Weitere Dokumente	246

1 Einführung

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zur Herstellung, Test und Betrieb des Produkttyps ePA-Aktensystem.

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 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. gemPTV_ATV_Festlegungen, 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 Übergreifende Festlegungen

Das Grobkonzept der "ePA für alle", siehe [gemKPT_ePAfuerAlle], beschreibt wesentliche Kernmechanismen, Basisfunktionalitäten sowie technische Konzepte zu den Diensten des ePA-Aktensystems und den beteiligten Client-Systemen der Fachanwendung ePA.

A_24986 - ePA-Aktensystem - Rollentrennung ePA-Aktensystem und IDP-Dienst

Falls der Betreiber des ePA-Aktensystems auch den IDP-Dienst betreibt, MUSS der Betreiber sicherstellen, dass die Erstellung oder Änderungen von IDToken beim IDP-Dienst und die Verarbeitung und Prüfung der Client-Attestation im ePA-Aktensystem durch geeignete technische und organisatorische Maßnahmen so wirkungsvoll voneinander getrennt werden, dass ein einzelner Mitarbeiter des Betreibers nicht beide Aktivitäten durchführen kann. [≤]

A_25149-01 - ePA-Aktensystem - Rollentrennung ePA-Aktensystem und sektoraler IDP

Falls der Betreiber des ePA-Aktensystems auch einen sektoralen IDP betreibt, MUSS der Betreiber sicherstellen, dass die Erstellung oder Änderungen von ID-Token beim sektoralen IDP und die Erstellung oder Änderungen der Mailadresse für die Geräteverwaltung im ePA-Aktensystem durch geeignete technische und organisatorische Maßnahmen so wirkungsvoll voneinander getrennt werden, dass ein einzelner Mitarbeiter des Betreibers nicht die Aktivitäten in beiden Diensten durchführen kann. [≤]

A_24673 - Zeitsynchronisation über Zeitdienst in der TI

Das ePA-Aktensystem MUSS die Systemzeit über den Zeitdienst in der TI gemäß [gemSpec_Net#6.2] synchronisieren [≤]

A_25612 - ePA-Aktensystem - Authentisierung gegenüber einem Client innerhalb der TI

Das ePA-Aktensystem MUSS sich beim Aufruf durch einen Client innerhalb der TI mit der TLS-Identität oid_epa_dvw und Zertifikatsprofil C.FD.TLS-S authentisieren. [≤]

A_24676 - Useragent Information in HTTP Header außerhalb des VAU-Kanals

Das ePA-Aktensystem MUSS sicherstellen, dass in der Kommunikation mit den ePA-Clients außerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "x-useragent" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen. [≤]

A_24677 - Useragent Information in HTTP Header innerhalb des VAU-Kanals

Das ePA-Aktensystem MUSS sicherstellen, dass in der Kommunikation mit den ePA-Clients innerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "x-useragent" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen. [≤]

Die Formatvorgaben zum Useragent sind in A_22470* definiert.

A_24816-01 - Aktenkontokennung in HTTP Header innerhalb des VAU-Kanals

Das ePA-Aktensystem MUSS sicherstellen, dass ePA-Clients in der Kommunikation mit den Medical Services der ePA innerhalb des VAU-Kanals ein HTTP Header Element mit dem Namen "x-insurantId" gesendet wird und andernfalls den Request mit HTTP-Fehler 400 ablehnen. [≤]

Hinweis: Das HTTP Header-Element mit dem Namen "x-insurantId", belegt mit einer KVN-R, ist erforderlich, um die Zuordnung zu einer konkreten Akte gewährleisten zu können.

Hinweis: Das betrifft die Kommunikation mit dem XDS Document Service (SOAP) und dem FHIR Data Service (FHIR). Die Operationen aller weiteren Services definieren die Notwendigkeit des Parameters x-insurantId in der jeweiligen Schnittstellenbeschreibung (OpenApi).

A_27443 - Nutzung Terminologiepaket

Das ePA-Aktensystem MUSS die relevanten Terminologien des Terminologiepakets gemäß [gemTerminology] verarbeiten und in der Kommunikation mit dem ePA-Aktensystem berücksichtigen. [≤]

Hinweis zu A_27443:

Das Terminologiepaket wird als FHIR-Package bereitgestellt und enthält z.B. Vocabulary ePA und Value Set für Berechtigungskategorien.

2.1 Aktensystem- und Service-Lokalisierung

Die Lokalisierung der Services der ePA für alle für ePA-Clients, die über das zentrale Netz der TI auf die Anwendung zugreifen, erfolgt mittels der übergreifenden Domäne epa4all.de. Da nicht gesteuert werden kann, welchen DNS ein ePA-Client verwendet, kann diese Domäne sowohl im Internet als auch im DNS der TI aufgelöst werden und verweist immer auf IP-Adressen der TI. Für die verschiedenen Umgebungen der TI werden third-level Domänen eingerichtet: .ref (RU1), .dev (RU2), .test (TU) und .prod (PU).

Ein ePA-Client aus der TI kennt die FQDNs der ePA-Aktensysteme (diese werden hier fest definiert, vgl. A_24592-*). Das Vorgehen der festvorgegebenen FQDNs ist analog zum E-Rezept-Vorgehen.

Ein ePA-FdV kennt den FQDN seines ePA-Aktensystems und erhält die Information über die dort verwendeten Service-Endpunkte über den Abruf einer Konfigurationsdatei unter /.well-known. In dieser Datei sind die verschiedenen Pfade zu den Endpunkten hinterlegt.

Jedes ePA-FdV ruft an seinem ePA-Aktensystem auch eine Liste aus allen Namen der verschiedenen Kostenträger und den zuständigen FQDN ab, damit diese im Falle einer Vertretung genutzt werden können, um das entsprechende Aktensystem zu finden.

A_24592-02 - Anbieter ePA-Aktensystem -Registrierung an übergreifender ePA-Domäne

Der Anbieter des ePA-Aktensystems MUSS seine Hosts und IP-Adressen für Services, die über das zentrale Netz der TI angeboten werden, in der übergreifenden ePA-Domäne epa4all.de für die Sub-Domänen ref (RU1), dev (RU2), test (TU) und prod (PU) unter folgend aufgeführten DNS-Namen (FQDN) registrieren. Diese sind

1. Host und IP-Adressen für den Endpunkt I_Information_Service und der Services in der VAU:
epa-as-`<ePA-Anbieter-Zahl>`.`<Umgebung>`.epa4all.de.
2. Host und IP-Adressen für den Endpunkt I_Information_Service_Accounts:
epa-asisa-`<ePA-Anbieter-Zahl>`.`<Umgebung>`.epa4all.de.

Die "ePA-Anbieter-Zahl" wird durch die gematik festgelegt.

[≤]

Folgende Zuordnungen der "ePA-Anbieter-Zahl" wurden vorgenommen:

ePA-Anbieter-Zahl	Anbieter / Betreiber
1	IBM
2	Bitmarck Technik

Sobald ein neuer Anbieter/Betreiber hinzukommt, wird diesem die kleinste, nicht belegte Ziffer (>0) durch die gematik zugewiesen.

Beispiele der Dienstlokalisierung

PU :

Aktensystem A

```
epa-as-1.prod.epa4all.de A 100.102.x1.x2
ggf. ... weitere IP-Adressen für epa-as-1.prod.epa4all.de (DNS-Round-Robin)
...
epa-asisa-1.prod.epa4all.de A 100.102.x3.x4
```

Aktensystem B

```
epa-as-2.prod.epa4all.de A 100.102.x5.x6
epa-asisa-2.prod.epa4all.de A 100.102.x7.x8
```

TU :

Aktensystem 1

```
epa-as-1.test.epa4all.de A 172.30.x9.x10
...
```

D. h. ein ePA-Client aus der TI (Primärsystem) kennt die für ihn zwei relevanten FQDNs (PU: epa-as-1.prod.epa4all.de und epa-as-2.prod.epa4all.de) und verwendet diese um die beiden Aktensystem zu kontaktieren. Eine dynamisch konfigurierbare Anzahl der Anbieter in einem Primärsystem wird aktuell nicht in der Spezifikation gefordert.

A_14128-04 - Anbieter ePA-Aktensystem - Resource Records FQDN ePA

Der Anbieter des ePA-Aktensystems MUSS in seinen Nameservern im Internet den FQDN des Aktensystems für das ePA-FdV auflösen.

[<=]

A_22688-03 - Anbieter ePA-Aktensystem, Konfiguration Schnittstellen über /.well-known/

Der Anbieter des ePA-Aktensystems MUSS an seinen Access Gateway des Versicherten über den URL-Pfadnamen (bzw. die Datei) /.well-known/epa-configuration.json eine JSON-Repräsentation aller Pfade zu seinen Komponenten verfügbar machen.

D. h. der Aufrufende (ePA-FdV) MUSS wenn er diesen Pfad per HTTP-GET abfragt ein JSON-Objekt (also Content-Type "application/json") vom Access Gateway des Versicherten erhalten der Art

```
{
  "version" : "<Produkttypversion des Aktensystems im Format[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}>",
```

```

"sgd1" : "<pfad_Schlüsselgenerierungsdienst_typ1>",
"sgd2" : "<pfad_Schlüsselgenerierungsdienst_typ2>",
....
}[<=]

```

A_22687 - Aktensystem, Konfiguration Schnittstellen über /.well-known/

Das ePA-Aktensystem MUSS sicherstellen, dass dem Anbieter des ePA-Aktensystems die technische Möglichkeit bereitgestellt wird A_22688-* umzusetzen. [<=]

A_26814 - ePA-Aktensystem - Schnittstellenadressierung

Das ePA-Aktensystem MUSS die Schnittstellenadressierung (relative Pfade) gemäß der Schnittstellenspezifikationen umsetzen. [<=]

Schnittstellenspezifikationen für die fachlichen Requests erfolgen durch WSDL, OpenAPI und FHIR Implementation Guides.

Für Operationen, die innerhalb einer ePA-VAU aufgerufen werden, gelten die Schnittstellenspezifikationen für den inneren HTTP-Request.

Abgrenzend hierzu wird das VAU-Protokoll und die dabei verwendeten Pfade in [gemSpec_Krypt#7] definiert.

A_24801 - Aktensystem, Liste von FQDN im Internet

Das ePA-Aktensystem MUSS dem ePA-FdV eine Liste aller Kostenträger und der FQDN, unter der deren ePA-Aktensystem im Internet erreichbar ist, bereitstellen. Die Liste setzt sich zusammen aus den selbst verwalteten Kostenträgern und den über I_Information_Service_Accounts bezogenen Teillisten der anderen ePA-Aktensysteme. [<=]

2.2 Redundanz

Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf]. Die Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Komponenten des ePA-Aktensystems. In diesem Dokument werden zusätzliche Redundanzanforderungen spezifiziert, wenn die Anforderungen in [gemSpec_Perf] zur Verfügbarkeit nicht ausreichen.

Die Auswahl und der Zugriff auf Services des ePA-Aktensystems wird durch die Primärsysteme anhand definierter FQDNs vorgenommen [siehe Kapitel 2.1]. Auf die Auswahl der Services des ePA-Aktensystems kann der Anbieter des ePA-Aktensystems durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn jedes Primärsystem oder andere Fachdienste (z.B. E-Rezept-Fachdienst, ein anderes ePA-Aktensystem, ...) die Möglichkeit haben, die Services des ePA-Aktensystems zu erreichen. Von der Versichertenseite aus erfolgt der Zugriff auf die Komponenten des ePA-Aktensystems durch das ePA-Frontend des Versicherten.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen Komponenten des ePA-Aktensystems ist über grundlegende Maßnahmen wie redundante Netzteile hinaus nicht erforderlich. Es steht dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern einzusetzen, so dass jede einzelne Komponente des ePA-Aktensystems im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

A_14921 - Anbieter ePA-Aktensystem - lokale Redundanz im Standort des ePA-Aktensystems

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass bei Ausfall einer oder mehrerer Komponenten des ePA-Aktensystems die verbleibenden Komponenten des ePA-Aktensystems in demselben Standort den Datenverkehr aller Clients der ausgefallenen

Komponente zusätzlich übernehmen, die Konsistenz der persistenten Daten erhalten bleibt und die Verfügbarkeit der Komponenten gemäß den geforderten SLAs in [gemSpec_Perf] weiterhin gegeben ist. [≤]

A_15245 - Anbieter ePA-Aktensystem - standortübergreifende Redundanz und Verfügbarkeit

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass bei Ausfall eines Standorts (Rechenzentrum) die Konsistenz der persistenten Daten erhalten bleibt und die Verfügbarkeit der Komponenten gemäß der geforderten SLAs in [gemSpec_Perf] gegeben ist. [≤]

A_24862-03 - Anbieter ePA-Aktensystem – Georedundanz: Verfügbarkeit der Akten innerhalb von fünf Arbeitstagen

Der Betreiber des ePA-Aktensystems MUSS Maßnahmen zur Verfügbarkeit der Akten ergreifen, die sicherstellen, dass bei einem Großereignis, bei dem alle Aktensysteminstanzen ausfallen, die betroffenen Akten innerhalb von fünf Arbeitstagen wieder vollumfänglich für die Versorgung genutzt werden können. Die Maßnahmen zur Erhaltung der Verfügbarkeit des Aktensystems müssen die Sicherheitsanforderungen für das ePA-Aktensystem erfüllen. [≤]

2.3 Datenschutz und Sicherheit

A_15128 - Anbieter ePA-Aktensystem - Schutz der transportierten Daten im ePA-Aktensystem

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die Vertraulichkeit und Integrität der innerhalb des ePA-Aktensystems transportierten Daten gewährleistet ist. [≤]

Die folgenden Anforderungen verhindern Profilbildungen über Versicherte und Leistungserbringer(-institutionen) durch den Anbieter bzw. dessen Mitarbeiter.

A_15103 - Anbieter ePA-Aktensystem - Konzept zur Verhinderung von Profilbildung

Der Anbieter des ePA-Aktensystems MUSS ein Konzept erstellen und umsetzen, dass sicherstellt, dass Mitarbeiter des Anbieters die im ePA-Aktensystem verarbeiteten Daten nicht für Profilbildungen über Versicherte oder Leistungserbringer(-institutionen) nutzen können. [≤]

Hinweis: Das Konzept kann Teil des Sicherheits- oder Datenschutzkonzeptes des Anbieters sein. Es ist nicht notwendigerweise ein eigenes Dokument erforderlich.

A_25722 - ePA-Aktensystem - Löschen von personenbezogenen Daten von Vertretern nach Wegfall der Notwendigkeit

Das ePA-Aktensystem MUSS die personenbezogenen Daten eines Vertreters löschen, sofern der Vertreter kein Aktenkonto im ePA-Aktensystem besitzt und der Vertreter keine Versicherten im ePA-Aktensystem mehr vertritt. [≤]

A_15104 - Anbieter ePA-Aktensystem - Ordnungsgemäße IT-Administration

Der Anbieter des ePA-Aktensystems MUSS die Maßnahmen für erhöhten Schutzbedarf des BSI-Bausteins „OPS.1.1.2 Ordnungsgemäße IT-Administration“ [BSI-Grundsatz] während des gesamten Betriebs des ePA-Aktensystems umsetzen. [≤]

Hinweis: Die Anforderungen des BSI-Bausteins sind entsprechend des dort genannten Schlüsselwortes („MUSS, DARF NICHT/ DARF KEIN, SOLLTE; SOLLTE NICHT/SOLLTE KEIN, KANN/DARF“) umzusetzen.

A_15824 - Anbieter ePA-Aktensystem - Sichere Speicherung von Daten

Unabhängig davon, ob die Daten schon verschlüsselt vorliegen, MUSS der Anbieter des ePA-Aktensystems die Daten des ePA-Aktensystems bei der Speicherung verschlüsseln. [\leq]

Hinweis: Dies kann z. B. durch eine transparente Datenbankverschlüsselung oder eine Festplattenverschlüsselung erfolgen.

A_24774 - Anbieter ePA-Aktensystem - Zwei-Faktor-Authentisierung von Administratoren

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass sich Administratoren mindestens mit einer Zwei-Faktor-Authentisierung anmelden. [\leq]

A_15107-02 - Anbieter ePA-Aktensystem - Keine unzulässige Weitergabe von Daten

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die in seinem Aktensystem verarbeiteten Daten nicht weitergegeben werden, auch nicht in pseudonymisierter oder anonymisierter Form. Davon ausgenommen sind Weitergaben an berechtigte Nutzer der Aktenkonten, an einen durch den Versicherten gewählten Anbieter beim Anbieterwechsel sowie Übermittlungen an das Forschungsdatenzentrum Gesundheit soweit dagegen kein Widerspruch durch den Versicherten oder einen Vertreter vorliegt. [\leq]

A_15119 - Anbieter ePA-Aktensystem - Löschkonzept

Der Anbieter des ePA-Aktensystems MUSS in einem Löschkonzept für die im ePA-Aktensystem verarbeiteten personenbezogenen Daten mindestens folgende Aspekte beschreiben:

- die umgesetzten organisatorischen und technischen Löschmaßnahmen (dies beinhaltet insbesondere auch die Löschung von Backups, Protokollen etc.),
- die Löschregeln und Löschfristen zusammen mit einer nachvollziehbaren Begründung für die getroffenen Fristfestlegungen,
- wie sichergestellt wird, dass alle Auftragnehmer die Löschpflichten ihrerseits umsetzen.

[\leq]

Hinweis: Das Löschkonzept kann Teil des Sicherheits- oder Datenschutzkonzeptes des Anbieters sein. Es ist nicht notwendigerweise ein eigenes Dokument erforderlich.

A_15169 - ePA-Aktensystem - Verbot von Werbe- und Usability-Tracking

Die Komponenten des ePA-Aktensystems DÜRFEN im Produktivbetrieb ein Werbe- und Usability-Tracking NICHT verwenden.

Davon ausgenommen ist das Erfassen des standardmäßigen quantitativen Nutzerverhaltens zur Ermittlung der Standard-Aktenutzung entsprechend der Anforderung A_15154. [\leq]

A_15154 - Anbieter ePA-Aktensystem - Ermittlung von Standard-Aktenutzung

Der Anbieter des ePA-Aktensystems MUSS mindestens einmal im Jahr Werte zu einer Standard-Aktenutzung von LE und Versicherten durch die Profilierung anonymer Zugriffsstatistiken auf das ePA-Aktensystem zum Zweck der Erkennung von Zugriffen gemäß A_15155 ermitteln. [\leq]

A_15155 - Anbieter ePA-Aktensystem - Abweichung von Standard-Aktenutzung

Der Anbieter des ePA-Aktensystems MUSS Zugriffe und Zugriffsmuster, die nicht einer Standard-Aktenutzung entsprechen, erkennen und Maßnahmen zur Schadensreduzierung umsetzen. [\leq]

Hinweis: Diese Erkennung darf keine zusätzliche Persistierung von personenbezogenen Daten auslösen. Ausnahme sind hier nur die notwendigen Daten, falls ein Missbrauch erkannt wird.

A_24778 - Anbieter ePA-Aktensystem - Einsatz zertifizierter HSM

Der Anbieter des ePA-Aktensystems MUSS beim Einsatz eines HSM sicherstellen, dass dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria oder Federal Information Processing Standard (FIPS) in Frage.
Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3 oder
2. FIPS 140-3 Level 3 oder
3. Common Criteria EAL 4+ (mit AVA_VAN.5)

entsprechen. [≤]

A_15157 - Anbieter ePA-Aktensystem - Sicherer Betrieb und Nutzung eines HSMs

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die auf dem HSM verarbeiteten privaten Schlüssel, Konfigurationen und eingesetzte Software nicht unautorisiert ausgelesen, unautorisiert verändert, unautorisiert ersetzt oder in anderer Weise unautorisiert benutzt werden können. [≤]

A_15159 - Anbieter ePA-Aktensystem - Schutzmaßnahmen gegen die OWASP Top 10 Risiken

Der Anbieter des ePA-Aktensystems MUSS in allen Komponenten des ePA-Aktensystems technische Maßnahmen zum Schutz vor den in der aktuellen Version genannten OWASP-Top-10-Risiken umsetzen. [≤]

A_24780-01 - Anbieter ePA-Aktensystem – Versicherte über sensible Änderungen informieren

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass der Versicherte informiert wird, wenn der Anbieter des Aktensystems eine manuelle Änderung bezüglich einer Akte (Aktenverwaltung) im Auftrag eines Versicherten durchführt. [≤]

Hinweis: Dies kann z. B. durch eine Notifikations-E-Mail an den Versicherten erfolgen. Solche E-Mails dürfen keine Details über die Änderungen beschreiben, sondern nur einen Hinweis geben, dass eine Änderung gemacht wurde und dass der Versicherte die Änderungen in seinem Aktenkonto prüfen sollte.

A_15163 - Anbieter ePA-Aktensystem - Angriffen entgegenwirken

Der Anbieter des ePA-Aktensystems MUSS Maßnahmen zur Erkennung von Angriffen und zur Reduzierung bzw. Verhinderung von Schäden aufgrund von Angriffen in allen Komponenten des ePA-Aktensystems umsetzen. [≤]

A_15167 - Anbieter ePA-Aktensystem - Social Engineering Angriffen entgegenwirken

Der Anbieter des ePA-Aktensystems MUSS Maßnahmen zur Erkennung und Verhinderung von Social Engineering Angriffen umsetzen. [≤]

A_24989 - Anbieter ePA-Aktensystem - Schutz vor Angriffen über die TI

Die Anbieter des ePA-Aktensystems MUSS für alle über die TI erreichbaren Schnittstellen des ePA-Aktensystems Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS Lösungen verhindert werden. [≤]

A_15168 - ePA-Aktensystem - Verbot vom dynamischen Inhalt

Die Komponenten des ePA-Aktensystems DÜRFEN dynamischen Inhalt von Drittanbietern NICHT herunterladen und verwenden.

[<=]

A_17080 - Verhindern von Session Hijacking

Die Komponenten des ePA-Aktensystems MÜSSEN geeignete Schutzmaßnahmen gegen Session-Hijacking implementieren.

[<=]

A_16323-01 - ePA-Aktensystem - Verbot von medizinisch irrelevantem Inhalt

Der Anbieter des ePA-Aktensystems MUSS der Ablage von Dokumenten, die für die medizinische Versorgung oder für die Eigenorganisation medizinischer Belange des Versicherten oder zur Erstattung der Behandlungskosten irrelevant sind, mittels AGB auf Anbieterseite entgegenwirken.

[<=]

A_24781 - Sicherer Betrieb des Produkts nach Handbuch

Der Anbieter eines ePA-Aktensystems MUSS die im Handbuch des eingesetzten ePA-Aktensystems beschriebenen Voraussetzungen für den sicheren Betrieb des Produktes gewährleisten.[<=]

A_18953 - Darstellen der Voraussetzungen für sicheren Betrieb des Produkts im Handbuch

Der Hersteller des ePA-Aktensystems MUSS für sein Produkt im dazugehörigen Handbuch leicht ersichtlich darstellen, welche Voraussetzungen vom Betreiber und der Betriebsumgebung erfüllt werden müssen, damit ein sicherer Betrieb des Produktes gewährleistet werden kann.[<=]

A_19122-01 - Anbieter ePA-Aktensystem – Trennung zu anderen Mandanten

Ein Betreiber eines ePA-Aktensystems MUSS sicherstellen, dass die Daten von unterschiedlichen Mandanten organisatorisch und technisch getrennt sind. [<=]

A_21106 - Anbieter ePA-Aktensystem – Signaturschlüssel für Protokolle

Das ePA-Aktensystem MUSS für die Signatur von Listen von Protokollen des Versicherten Schlüsselmaterial der Ausstelleridentität ID.FD.SIG mit einem zugehörigen Zertifikat C.FD.SIG mit der Rolle oid_epa_logging gemäß [gemSpec_OID] besitzen.[<=]

A_21107 - Anbieter ePA-Aktensystem – Speicherung Signaturschlüssel für Protokolle im HSM

Das ePA-Aktensystem MUSS das private Schlüsselmaterial der Ausstelleridentität ID.FD.SIG für die Signatur von Listen von Protokollen des Versicherten in einem HSM speichern.

[<=]

A_22409 - Anbieter ePA-Aktensystem - CA-Anbieterwechsel

Der Anbieter des ePA-Aktensystems MUSS mindestens drei Monate vor dem Wechsel des CA-Anbieters für die Ausstellung der TLS-Zertifikate des Access Gateways die gematik darüber informieren, wer der alte Anbieter war und wer der neue Anbieter wird.[<=]

A_19118-01 - Komponenten des Aktensystems, Schutz vor XSW-Angriffen

Die Komponenten des ePA-Aktensystems, die XML-Signaturen prüfen, MÜSSEN geeignete Maßnahmen gegen XSW-Angriffe umsetzen. Mindestens MÜSSEN sie die FastXPath-Auswertung der XML-Daten und XML-Signaturen gemäß [GJLS-2009] (vgl. auch [BSI-XSpRES]) umsetzen.[<=]

A_24783 - ePA-Aktensystem - Eingabevalidierung von Operationen

Das ePA-Aktensystem MUSS alle Operationsaufrufe seiner Schnittstellen (Requests) sowie die Antwortmeldung auf seine Anfragen (Responses) auf Wohlgeformtheit und

Zulässigkeit prüfen und bei Encoding-, Schema-, Semantik- oder Protokollverletzungen die Operation abbrechen.[<=]

Hinweis: Eine Orientierung für die Validierung ist in [OWASP ASVS] Kapitel 5, Validation, Sanitization and Encoding beschrieben.

A_24992 - ePA-Aktensystem - Zugriffe durch Versicherte übers Access Gateway

Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session für einen Versicherten (NutzerID ist KVNR) ausschließlich über das Access Gateway erreichbar ist.[<=]

A_24993 - ePA-Aktensystem - Zugriffe übers Access Gateway ausschließlich für Versicherte

Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session für einen Nutzer, dessen NutzerID keine KVNR ist (z.B. Leistungserbringerinstitutionen) nicht über das Access Gateway erreichbar ist.[<=]

A_25006 - ePA-Aktensystem - User Session bei Inaktivität Beenden

Das ePA-Aktensystem MUSS sicherstellen, dass eine User Session nach 20 Minuten Inaktivität beendet wird.[<=]

A_25022 - ePA-Aktensystem - Debug-Protokoll für Testbetrieb

Das ePA-Aktensystem KANN im Testbetrieb ein Debug-Protokoll schreiben, welches eine erweiterte Protokollierung für Testzwecke ermöglicht.[<=]

Hinweis: Die Anforderung beschränkt den Debug-Modus auf Testzwecke. Im Produktivbetrieb ist der Debug-Modus nicht zulässig.

A_25023 - ePA-Aktensystem - Keine Echtdaten im Testbetrieb

Das ePA-Aktensystem MUSS sicherstellen, dass im Testbetrieb keine Echtdaten verarbeitet werden.[<=]

A_25042 - ePA-Aktensystem - Prüfung von Signaturen

Das ePA-Aktensystem MUSS bei der Prüfung von Signaturen

- das Signaturzertifikat gemäß A_25040-* prüfen,
- die Signatur prüfen (i. S. v. Verify()-Funktion des kryptographischen Signaturverfahrens ergibt "valid")

[<=]

A_25040-01 - ePA-Aktensystem - Prüfung Signaturzertifikate

Das ePA-Aktensystem MUSS Signaturzertifikate gemäß [gemSpec_PKI#TUC_PKI_018] mit folgenden Parametern auf Gültigkeit prüfen:

Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat

Parameter	C.FD.SIG	C.CH.SIG	C.HCI.OSIG	C.HCI.AUT
PolicyList	oid_fd_sig	oid_egk_sig	oid_smc_b_osig	oid_smc_b_aut
intendedKeyUsage	digitalSignatur	nonRepudiati	nonRepudiatio	digitalSignatu
intendedExtendedKeyUs	(leer)	(leer)	(leer)	id-kp-
age				clientAuth
OCSP-Graceperiod	24 Stunden	24 Stunden	24 Stunden	24 Stunden

Parameter	C.FD.SIG	C.CH.SIG	C.HCI.OSIG	C.HCI.AUT
Offline-Modus	nein	nein	nein	nein
Prüfmodus	OCSP	OCSP	OCSP	OCSP

Das ePA-Aktensystem MUSS sicherstellen, dass die Prüfung des Signaturzertifikats nur erfolgreich ist, falls das Signaturzertifikat anhand der Zertifikatsprüfung für [Zertifikatsignatur "valid" UND zeitlich gültig UND online gültig] befunden wird.
[<=]

2.4 Validierungsaktenkonto

Die Architektur des ePA-Aktensystems verhindert eine Einsichtnahme des Betreibers in Daten von Versicherten. Ebenso ist ein Monitoring der Verfügbarkeit einzelner Schnittstellen und Operationen erschwert. Mit der Anlage eines Validierungsaktenkontos (auf Basis einer Validierungsidentität gem. gemSysL_PK_eGK) im ePA-Aktensystem kann die korrekte Funktionsweise in der Produktivumgebung validiert und überwacht werden. Ein Validierungsaktenkonto verhält sich dabei wie ein Konto eines echten Versicherten. Eine Validierungsidentität ist eine Identität mit Versichertenrolle, deren KVNR sich aufgrund ihrer festgelegten Bildungsvorschrift technisch von der eines echten Versicherten unterscheiden lässt. Die Bildungsvorschrift zur Erzeugung von KVNRn für Validierungskonten weicht dahingehend vom Standard ab, dass hier 4 (oder mehr) aufeinanderfolgende, gleiche Ziffern verwendet werden. Dadurch ist eine Überschneidung mit der Menge der "Echt"-KVNRn ausgeschlossen. Die Zuteilung von KVNR-Nummernkreisen, bzw. die Ausgabe einer KVNR in Form einer Prüfkarte, erfolgt durch die gematik.

Validierungsaktenkonten stehen der gematik, den Aktensystembetreibern selbst und Dritten (z. B. DVOs, Primärsystemhersteller ...) zur Verfügung. Für Dritte übernimmt die gematik die Anforderung der Validierungsaktenkonten bei den Aktensystembetreibern und vertreibt diese zusammen mit den dazugehörigen Prüfkarten. Für Validierungsaktenkonten von Dritten kann der Aktensystembetreiber nur eingeschränkten Support in Form von "Akte anlegen", "Akte zurücksetzen" und "Akte löschen" leisten. Über die Einschränkung sind die Nutzer durch die gematik zu informieren.

Folgende Anwendungsfälle sollen mit den Validierungsaktenkonten adressiert werden:

- Monitoring der Aktensystemfunktionalität
- Troubleshooting bei Störungsmeldungen (über FdV oder Primärsystem)
- Validierung der Konfiguration in der LEU
- Store-Review seitens der App-Store-Betreiber (über FdV)
- Validierung der EU-Anbindung

Die mittels der Validierungskonten in der Produktivumgebung realisierten Anwendungsfälle müssen sich möglichst auf die genannten, unbedingt jedoch auf spezifizierte Anwendungsfälle beschränken.

A_18168-01 - Anbieter des ePA-Aktensystem - Validierungsaktenkonto für gematik

Nach Aufforderung durch die gematik MUSS der Anbieter des ePA-Aktensystems

- für die gematik ein Validierungsaktenkonto im ePA-Aktensystem für die von der gematik übergebene KVNR anlegen, wobei die KVNR die Festlegungen für die Versichertennummer [gem. gemSysL_PK_eGK] erfüllen muss.
- das durch die gematik angegebene Validierungsaktenkonto löschen, sofern die gematik dessen Anlage beantragt hatte.

[<=]

A_18169-02 - Anbieter des ePA-Aktensystem - Validierungsaktenkonto für eigene Zwecke

Falls sich der Anbieter des ePA-Aktensystems ein Validierungsaktenkonto für eigene Zwecke anlegen möchte, MUSS er sicherstellen, dass nur eine Versichertennummer aus dem von der gematik für diesen Anbieter freigegebenen Nummernkreis [gem. gemSysL_PK_eGK] verwendet wird.

[<=]

A_22522-01 - Anbieter des ePA-Aktensystems - Validierungskonto für Dritte

Der Anbieter des ePA-Aktensystems MUSS auf Antrag der gematik

- Validierungsaktenkonten für Dritte (z.B. DVO, PS-Hersteller) für eine vom Antragsteller übermittelte KVNR anlegen, sofern die KVNR die Festlegungen für die Versichertennummer [gem. gemSysL_PK_eGK] erfüllt ist.
- das durch einen Antragsteller angegebene Validierungsaktenkonto löschen, sofern der Antragsteller dessen Anlage beantragt hatte.

[<=]

Hinweis zu A_22522-*: Die Einrichtung der Validierungsaktenkonten für Dritte kann gegen Bezahlung erfolgen. Die Entscheidung *dafür obliegt dem Anbieter des ePA-Aktensystems*.

Im Design der ePA für alle wird die Initialisierung und Aktivierung durch den Kostenträger vorgenommen. Da es diese Rolle bei Validierungsaktenkonten nicht gibt, sind für diese speziellen Aktenkonten die folgenden Besonderheiten zu berücksichtigen:

A_26187 - Anlage von Validierungsaktenkonten

Das ePA-Aktensystem MUSS die Anlage von Validierungsaktenkonten auch ohne KTR- und Ombudsstellen-Befugnisse zulassen.[<=]

A_26188 - Anbieter des ePA-Aktensystems -Aktivierung von Validierungsaktenkonten

Der Anbieter des ePA-Aktensystems MUSS den Status von Validierungsaktenkonten, welche für die gematik (gem. A_18168-*) oder für Dritte (gem. A_22522-*) angelegt wurden, nach der Anlage auf ACTIVATED setzen.[<=]

Falls ein Antragsteller keine Löschung eines Validierungsaktenkontos beim Anbieter des ePA-Aktensystems beantragt, wird das Validierungsaktenkonto nach einer Lebensdauer von maximal 5 Jahren automatisch durch den Anbieter des ePA-Aktensystems gelöscht (ggf. früher aber nicht vor Ablauf der Gültigkeit der Prüf-eGK). Dies verhindert das Auftreten ungenutzter Validierungsaktenkonten im Aktensystem. Die maximale Lebensdauer eines Validierungsaktenkontos ist dabei an die maximale Gültigkeit der Zertifikate der Validierungsidentität gekoppelt, die maximal fünf Jahre betragen kann.

A_22524-01 - Anbieter des ePA-Aktensystems - Löschen von Validierungsaktenkonten nach 5 Jahren

Der Anbieter des ePA-Aktensystems MUSS ein Validierungsaktenkonto spätestens fünf Jahre nach Anlage des Validierungsaktenkontos, frühestens jedoch nach Ablauf der Gültigkeit der dazugehörigen Prüf-eGK, löschen.[<=]

A_22684-01 - Validierungsaktenkonten im Store-Review der FdVs

Der Anbieter/Hersteller des ePA-Aktensystems bzw. Hersteller des ePA-FdVs KANN - ausschließlich für dedizierte KVNRRn von Validierungsaktenkonten zum Zwecke der Verwendung im Store-Review der FdVs – Vorkehrungen treffen, die es ermöglichen auf Gerätebindung, E-Mail-Validierung oder andere Aktivitäten des Registrierungs-/Anmeldeprozesses zu verzichten, um eine Prüfung der FdVs durch die App-Store-Betreiber zu ermöglichen. [\leq]

A_22942 - Besonderheiten bei Validierungsaktenkonten für StoreReviews

Bei Validierungsaktenkonten, für die die Regelung gem. A_22684-* gilt [Validierungsaktenkonten im StoreReview der FdVs], MÜSSEN folgende Besonderheiten berücksichtigt werden:

- die entsprechenden Validierungsaktenkonten dürfen nur für den Zeitpunkt des Reviews aktiviert und erreichbar sein,
- die entsprechenden Validierungsaktenkonten sind unmittelbar nach dem Review zu leeren,
- es sind Zeitraum der Erreichbarkeit und eine eindeutige Referenz auf den Review (z.B. Vorgangsnummer) zu dokumentieren und auf Anforderung an die gematik zu übertragen

[\leq]

A_26209 - Prüfung auf Vertretungsberechtigung für Prüfidentität

Das ePA-Aktensystem MUSS sicherstellen, dass bei der Vertreterbefugnis ausschließlich "echte" Vertreter für "echte" Konten befugt, bzw. auf Validierungsaktenkonten ausschließlich "Validierungs-Vertreter" eingerichtet werden können. [\leq]

A_24539 - Nutzung von Validierungsaktenkonten via FdV

Der Anbieter des ePA-Aktensystems bzw. Hersteller des ePA-FdVs MUSS ein FdV bereitstellen, mit dem der Zugriff auf Validierungsaktenkonten möglich ist. [\leq]

Die Bereitstellung dieser FdVs muss nicht unentgeltlich erfolgen, wenngleich eine Integration dieser Eigenschaft (Kompatibilität mit Validierungsaktenkonten) in das Standard-FdV anzustreben ist.

2.5 Tracing in Nichtproduktivumgebungen

Ein gewonnener Erfahrungswert ist, dass es für die Fehlersuche in Nichtproduktivumgebungen -- insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase -- leistungsfähigere Mechanismen als zuvor geben muss. Gab es zunächst nur die Testschnittstelle ([gemKPT_Test#A_21193-*]) in den ePA-Clients, so wurde mit ePA 2.0 ein Tracing im Aktensystem für Nichtproduktivumgebungen eingeführt und wird mit ePA für alle wie folgt umgesetzt:

1. Innerhalb des AS werden an die für die Fehlersuche in Nichtproduktivumgebungen wichtigen Stellen Sensoren platziert. Diese Sensoren streamen die aktuell transportierten Daten an bestimmte TCP-Ports am Access Gateway. Die Sensorpunkte liegen im AS immer hinter der TLS-Entschlüsselung. Fehlersuchende können sich zu diesen TCP-Ports am Access Gateway verbinden und lesen dann im Read-Only-Modus den aktuellen Datenverkehr, der an den Sensorpunkten vorbeifließt, mit.
2. ePA-Clients müssen in Nichtproduktivumgebungen beim VAU-Protokoll die symmetrischen Verbindungsschlüssel offenlegen [gemSpec_Krypt#A_24477-*].

Damit wird es möglich, für die Fehlersuche in Nichtproduktivumgebungen den Datenverkehr zwischen einem ePA-Client und der VAU-Instanz im Aktensystem mitzulesen. Für ePA für alle konzentriert sich das Tracing auf genau diese Verbindungsstrecke, andere Sensorpunkte vor Services außerhalb der VAU sind optional.

Ein Aktensystem besitzt mehrere HTTPS-Schnittstellen, über die ein ePA-Client auf das Aktensystem zugreift. Die TLS-Sicherung endet vor den VAU-Instanzen. In den VAU-Instanzen möchte man die Trusted Computing Base (TCB) minimieren und setzt dort das VAU-Protokoll als extrem reduziertes TLS-Analogon ein. Der geforderte Sensorpunkt muss hinter der TLS-Terminierung und vor der VAU Instanz liegen.

A_21887-01 - Tracing, Sensorpunkt nahe vor den VAU-Instanzen (Nichtproduktivumgebungen)

Ein ePA-Aktensystem MUSS sicherstellen, dass genau in Nichtproduktivumgebungen der Datenverkehr zur und von den VAU-Instanzen auf TCP-Ebene mitgeschnitten wird (Sensorpunkt). Der aktuell mitgeschnittene Datenverkehr MUSS auf einen TCP-Port im Access Gateway gestreamt werden (siehe A_21890-*). D. h. wenn ein Client sich zu diesem TCP-Port verbindet, MUSS er die aktuell auf dem Interface durchlaufenden Daten gestreamt lesen können.

[<=]

A_21891-01 - Tracing, Tiger-Standalone-Proxy

Ein ePA-Aktensystem MUSS zum Mitschneiden und Streamen der Testdaten in Nichtproduktivumgebungen nach A_21887-* den von der gematik bereitgestellten aggregierenden Tiger-Standalone-Proxy (mindestens der Version 0.20) verwenden.[<=]

A_22581 - Tracing, Abschaltbarkeit

Ein ePA-Aktensystem MUSS den Tiger-Standalone-Proxy (und die damit verbundenen Sensorpunkte) gemäß A_21891-* im Rahmen der Zulassungstests auf Wunsch der gematik aktivieren und insbesondere deaktivieren können.[<=]

Hinweis: Die Aktivier- bzw. Deaktivierbarkeit nach A_22581- kann dabei auch teilweise mit organisatorische Maßnahmen umgesetzt werden, d. h. es ist hier **kein** vollautomatisierter Mechanismus notwendig, der im Millisekunden-Bereich umschalten kann.*

2.6 Benutzerführung

Bietet der Anbieter des ePA-Aktensystems dem Versicherten die Aktenkontoeröffnung, die Änderung von Vertragsdaten und die Aktenkontoschließung auf einem elektronischen Weg an, dann muss die Bedienung für den Nutzer intuitiv gestaltet werden.

A_15842 - Anbieter ePA-Aktensystem - Ergonomie der Benutzerführung

Der Anbieter des ePA-Aktensystems MUSS eine ergonomisch gestaltete Benutzerführung nach den Vorgaben zur Ergonomie in [DIN EN ISO 9241-171] anbieten.[<=]

DIN-Normen und Verordnungen zur Beachtung:

Zusätzlich zu den in diesem Kapitel aufgeführten Anforderungen zur Benutzerführung sollen auch die in der ISO 9241 aufgeführten Qualitätsrichtlinien zur Sicherstellung der Ergonomie interaktiver Systeme und Anforderungen aus der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung – BITV 2.0) beachtet werden.

Insbesondere soll der Fokus auf die nachfolgend aufgeführten Teile der ISO 9241 gerichtet sein:

DIN EN ISO 9241 – Teile mit Bezug zur Software-Ergonomie

- Teil 8: Anforderungen an Farbdarstellungen
- Teil 9: Anforderungen an Eingabegeräte – außer Tastaturen
- Teil 110: Grundsätze der Dialoggestaltung (ersetzt den bisherigen Teil 10)
- Teil 11: Anforderungen an die Gebrauchstauglichkeit – Leitsätze
- Teil 12: Informationsdarstellung
- Teil 13: Benutzerführung
- Teil 14: Dialogführung mittels Menüs
- Teil 15: Dialogführung mittels Kommandosprachen
- Teil 16: Dialogführung mittels direkter Manipulation
- Teil 17: Dialogführung mittels Bildschirmformularen
- Teil 171: Leitlinien für die Zugänglichkeit von Software BITV 2.0

BITV 2.0 - Barrierefreie Informationstechnik-Verordnung

Die Umsetzung der Verordnung dient zur behindertengerechten Umsetzung von Webseiten und anderen grafischen Oberflächen.

Insbesondere sollen deshalb neben der Übernahme der international anerkannten Standards für barrierefreie Webinhalte, die Web Content Accessibility Guidelines (WCAG) 2.1, auch die Belange gehörloser, hör-, lern- und geistig behinderter Menschen berücksichtigt werden.

Die BITV 2.0 regelt unter anderem den sachlichen Geltungsbereich, die einzubeziehenden Gruppen behinderter Menschen und die anzuwendenden Standards.

Weitere Richtlinien und Empfehlungen zur digitalen Barrierefreiheit sind die EU-Richtlinie 2016/2102 für öffentliche Stellen und die europäische Norm EN 301 549 V2.1.2 mit dem Titel "Accessibility requirements for ICT products and services".

A_15846 - Anbieter ePA-Aktensystem - Schnittstellen für die Unterstützung der barrierefreien Bedienungsmöglichkeit

Der Anbieter des ePA-Aktensystems SOLL die Schnittstellen für die Unterstützung der barrierefreien Bedienungsmöglichkeit, welche vom Betriebssystem zur Verfügung gestellt werden, unterstützen.[<=]

2.7 Useragent

A_22470-06 - Definition x-useragent

Das Produkt MUSS für das x-useragent-Element in Eingangs- oder Ausgangsparametern einer Operation folgende Formatvorgaben berücksichtigen:

- der Useragent umfasst 2 Informationen, welche als 1 String - getrennt durch "/" (Slash) - im Header übertragen werden
 - erster Teil: Client-ID = ein bis zu 20 Zeichen langer String (a-z A-Z 0-9, "-"), welcher im Rahmen der Produktregistrierung bei der gematik erzeugt wird,
 - zweiter Teil: Versionsnummer = bis zu 15 Zeichen langer String (a-z A-Z 0-9, "-", ".") welcher die aktuelle Produktversion des Clients repräsentiert.

Beispiel: "CLIENTID1234567890AB/2.1.12-45"

Hinweis: gem. RFC7231 ist im http-Header ein Useragent einzutragen. Dieser RFC-Useragent enthält z.B. Angaben zum Betriebssystem oder zum Browser und ist nicht zu verwechseln mit dem hier definierten x-useragent. Dieser (x-useragent) muss deshalb im x-useragent-Parameter des http-Headers eingetragen werden, NICHT im Useragent-Parameter gem. RFC7231. Ein Beispiel für die Verwendung bieten die OpenAPI-Spezifikationen der fachlichen Aktensystem-Operationen. [≤]

Hinweis zum Erhalt der Client-ID: die Client-ID wird durch die gematik vergeben und übermittelt, sobald sich ein (Client-)Produkthersteller (z.B. FdV oder Primärsystem) unter idp-registrierung@gematik.de registriert hat. Dazu ist im Rahmen dieser Registrierung der Name des Herstellers und der Name des zu registrierenden Produktes zu übermitteln. Sollte im Rahmen einer anderen TI-Anwendung bereits eine Registrierung vorgenommen worden sein, kann die Client-ID auch im ePA-Kontext genutzt werden (sofern es sich um das gleiche Softwareprodukt handelt).

Hinweis für FdV-Hersteller: Bei Entwicklung eines White-Label-Clients ist der Useragent Teil des kundenspezifischen Customizings, sodass über die Client-ID im Useragent das spezifische Kostenträger-ePA-FdV erkennbar sein muss.

2.8 Datenmigration

Jeder Versicherte (vorbehaltlich eines Widerspruchs durch den Versicherten) erhält in ePA 3.0 ein neues, leeres Aktenkonto. Bei der Migration werden Daten und Vertreterberechtigungen aus ePA 2.6 in dieses Aktenkonto übertragen.

Für die Migration eines existierenden Aktenkontos der Version ePA-2.x wird vorausgesetzt, dass ein migriertes Aktenkonto sowohl die Schnittstellen der ePA für alle, als auch die Schnittstellen der bisherigen ePA-Version 2.x bereitstellt und simultan verarbeiten kann.

Die Migration eines existierenden Aktenkontos der ePA-Version 2.x erfordert die Entschlüsselung der existierenden Inhalte durch die Anwendung des aktenkontospezifischen Akten- und Kontextschlüssels und deren Überführung in die Verwaltungs- und Diensteeinheiten der im vorliegenden Dokument beschriebenen ePA-Version 3.x.

Aus einem existierenden Aktenkonto werden die folgenden Artefakte übernommen:

- Kategorien und Ordner, insoweit die Kategorien nicht abgekündigt sind. Ordner erhalten eine feste UUID.
- Dokumente, sowie deren Metadaten
- Protokolle

Die Vertraulichkeitsstufen für die Sichtbarkeit von Dokumenten werden nicht mehr unterstützt. Dokumente mit bisheriger Vertraulichkeitsstufe *confidential* werden bei der Migration der GeneralDenyPolicy des Constraint Managements zugeordnet.

Alle weiteren Nutzergruppen (LEI, Apotheken, usw) erhalten eine Befugnis zur Nutzung dediziert in einer Behandlungssituation oder durch direkte Befugnisvergabe durch den Versicherten oder einen Vertreter mittels ePA-FdV.

Für Versicherte, die keine ePA-FdV nutzen möchten oder können, ist eine Migration der Daten einer existierenden Akte nicht möglich, da die dafür notwendige Übertragung des bisherigen individuellen Akten- und Kontextschlüssels nicht erfolgen kann. Versicherte ohne ePA-FdV erhalten (vorbehaltlich eines Widerspruchs durch den Versicherten) ein

neues, leeres Aktenkonto ohne Inhalten, die womöglich in ePA 2.6 existierten. Eine Befugnisvergabe für Leistungserbringerorganisationen ist in diesem Fall ausschließlich durch die Befugnisvergabe im Behandlungskontext möglich. Dieses erfordert eine LEI mit einem Client gemäß ePA-Version 3.x.

Es resultiert ein Aktenkonto, welches direkt durch den Versicherten, befugte Vertreter, den Kostenträger, die Ombudsstelle und den E-Rezept-Fachdienst genutzt werden kann.

Zusätzlich zur Datenmigration beim Wechseln von ePA 2 nach ePA 3 kann es auch innerhalb von ePA 3 zu notwendigen Datenanpassungen kommen, z. B. wenn das Aktensystem Metadaten zu bestehenden Dokumenten ergänzen soll. Derartige Hinweise finden sich im Unterabschnitt [Weitere Datenanpassungen](#).

2.8.1 Herstellerspezifische Umsetzung der Datenmigration

Die technische Umsetzung der Datenmigration obliegt grundsätzlich dem Hersteller des ePA-Aktensystems. Es muss jedoch sichergestellt werden, dass der Schutz der zu migrierenden Daten durchgehend gewährleistet wird.

A_24995 - Migration: Sicherheitskonzept für Datenmigration

Der Hersteller des ePA-Aktensystems MUSS ein Sicherheitskonzept zur Datenmigration erstellen, in welchem er beschreibt, mit welchen Maßnahmen die zu migrierenden Daten im gesamten Datenmigrationsprozess geschützt werden. [\leq]

A_25000 - Migration: Stärke der Sicherheitsmaßnahmen für Datenmigration

Das ePA-Aktensystem MUSS sicherstellen, dass die zu migrierenden Daten im gesamten Datenmigrationsprozess mit technischen Maßnahmen geschützt werden, die auch gegen einzelne Innentäter beim Betreiber des ePA-Aktensystems wirken. [\leq]

A_25049 - Migration: Migrationskonzept

Der Anbieter des ePA-Aktensystems MUSS ein Migrationskonzept erstellen, welches sowohl die Aktensystemmigration, als auch die Datenmigration, mitsamt der Bereitstellungs- und ggf. Außerbetriebnahme-Zeitpunkte der benötigten Komponenten berücksichtigt. Das Migrationskonzept MUSS dabei auch aufzeigen, welche Abhängigkeiten zu anderen TI-Diensten bestehen, wann und in welchem Umfang die Migration getestet wird und wie eventuelle Roll-Back-Szenarios aussehen. [\leq]

2.8.2 Durchführung der Migration

Das Aktenkonto muss durch den Anbieter für die Migration der Daten vorbereitet werden. Dabei müssen alle Maßnahmen umgesetzt werden, die im Zustand INITIALIZED eines neuen Aktenkontos vor der Aktivierung erforderlich sind (siehe 3.1.3- Anlage eines neuen Aktenkontos). Abweichend von den Maßnahmen für die Erstellung eines neuen Aktenkontos kann auf den Status INITIALIZED verzichtet werden und das Aktenkonto im Status ACTIVATED verbleiben.

Für ein zu migrierendes Aktenkonto sind alle Schritte anzuwenden, die auch für die Erstellung eines neuen Aktenkontos vor der Aktivierung erforderlich sind, insbesondere die Anlage der initialen Befugnisse für den Versicherten, den Kostenträger und die Ombudsstelle, sowie den E-Rezept-Fachdienst.

Im Anschluss an die Initialisierung erfolgt einmalig die Bereitstellung der Akten- und Kontextschlüssel durch ein ePA-FdV. Existierende Daten werden übertragen.

A_25148 - Migration: Information des Versicherten

Der Anbieter des ePA-Aktensystems MUSS den Versicherten über die Notwendigkeit und die Folgen einer Migration vor der eigentlichen Migration informieren, insbesondere darüber, welche Dokumentenformate und welche Berechtigungen übernommen und welche nicht übernommen werden, über die Freiwilligkeit einer Migration. [≤]

Die Entschlüsselung des Datenbestands für die Überführung in das vorbereitete Aktenkonto und die Migration der Berechtigungen der Vertreter wird durch die Nutzung eines ePA-FdV gemäß ePA-Version 3.x abgeschlossen. Bei der ersten Nutzung eines ePA-FdV durch den Versicherten mit dem zur Migration vorbereiteten Aktenkonto erfolgt die Migration über die vom ePA Aktensystem bereitgestellten Schnittstellen.

A_24922 - Migration: Schnittstellen zur Durchführung der Migration

Das ePA-Aktensystem MUSS für jedes Aktenkonto eine Migration von ePA 2.6 auf ePA 3.0 durchführen und geeignete Schnittstellen zum FdV anbieten, mit denen der Versicherte vom FdV das Entschlüsseln der verschlüsselten ePA 2.6-Akteninhalte anstoßen kann. [≤]

In der ePA für alle ist der Zugriff über einen Client der ePA-Version 2.x nicht mehr möglich, da sich die grundsätzliche Architektur und die Schnittstellen und Protokolle geändert haben.

2.8.3 Bereinigung von Registry und Repository im Zuge der Migration

A_24964 - XDS Document Service - Migration: Isolation der Migration

Der XDS Document Service MUSS die Verarbeitung von entschlüsselten Dokumenten, die im Rahmen der Migration durchgeführt werden, so technisch isolieren, dass kein Schaden für Aktenkonten oder das ePA-Aktensystem selbst entsteht. [≤]

A_25730 - XDS Document Service - Konvertierung von PDF in PDF/A bei der Datenmigration

Der XDS Document Service MUSS die Konvertierung von entschlüsselten PDF-Dokumenten in PDF/A-Dokumente, die im Rahmen der Migration durchgeführt wird, in einer Aktenkontoverwaltungs-VAU oder in einer getrennten VAU-Instanz durchführen, wobei

- die Konvertierung innerhalb der Aktenkontoverwaltungs-VAU ausschließlich für die Datenmigration von ePA2.6 auf die ePA3.0 verwendet werden darf und
- es bei einer getrennten VAU-Instanz eine 1:1-Beziehung zur Aktenkontoverwaltungs-VAU geben muss (d.h. die getrennte VAU-Instanz zur Konvertierung ist nur mit einer (1) Aktenkontoverwaltungs-VAU verbunden und eine Aktenkontoverwaltungs-VAU nur mit einer (1) VAU-Instanz für die Konvertierung) und die getrennte VAU-Instanz für die Konvertierung ausschließlich für die Datenmigration von ePA2.6 auf die ePA3.0 verwendet werden darf.

[≤]

A_26682 - XDS Document Service - Konvertierung von Bildformaten in PDF/A bei der Datenmigration

Der XDS Document Service MUSS die Konvertierung von entschlüsselten Bildformaten in PDF/A-Dokumente, die im Rahmen der Migration durchgeführt wird, in einer Aktenkontoverwaltungs-VAU oder in einer getrennten VAU-Instanz durchführen, wobei

- die Konvertierung innerhalb der Aktenkontoverwaltungs-VAU ausschließlich für die Datenmigration von ePA2.6 auf die ePA3.0 verwendet werden darf und

- es bei einer getrennten VAU-Instanz eine 1:1-Beziehung zur Aktenkontoverwaltungs-VAU geben muss (d.h. die getrennte VAU-Instanz zur Konvertierung ist nur mit einer (1) Aktenkontoverwaltungs-VAU verbunden und eine Aktenkontoverwaltungs-VAU nur mit einer (1) VAU-Instanz für die Konvertierung) und die getrennte VAU-Instanz für die Konvertierung ausschließlich für die Datenmigration von ePA2.6 auf die ePA3.0 verwendet werden darf.

Bildformate sind Dokumente im Format "jpeg", "png" oder "tiff".[<=]

A_25002 - XDS Document Service - Migration: Umbenennung von Ordnern

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 in den Werten von `Folder.codeList` die mit ePA 3.0 gegebenenfalls geänderten Kategoriennamen als Werte verwenden. [<=]

A_24562 - XDS Document Service - Migration: Auflösung abgekündigter Ordner

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 die abgekündigten Kategorien auflösen. Dabei MÜSSEN sämtliche Dokumente gemäß der Einordnungsregeln in A_19388-* neu Ordern zugeordnet werden und die Ordner der abgekündigten Kategorien gelöscht werden.[<=]

Die in ePA 2 angelegten dynamischen Ordner der Kategorie `childsrecord` können Kinder identifizieren, deren Daten nicht in ihren eigenen Akten gehalten wurden. Diese dynamischen Ordner sind nach folgender Regel in ePA 2 vom Primärsystem angelegt worden: `Folder.title` wurde mit dem Namen und Geburtsdatum des Kindes belegt. Bildungsregel: Nachname + ", " + 1. Vorname + " Datum im Format TT.MM.YYYY. Beispiel: "Musterkind, Max 03.03.2017".

Die Kinderuntersuchungshefte werden nicht migriert und verbleiben im Ordner `childsrecord`.

A_24963 - XDS Document Service - Migration: Keine Übernahme von Dokumenten mit unzulässigem Format

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 sämtliche Dokumente der ePA2.6 gemäß A_24864-* auf die zulässigen Dokumentenformate prüfen und Dokumente in einem nicht erlaubten Format nicht in die "ePA für alle" migrieren.[<=]

Hinweis zu A_24963-: Für die Migration von Dokumenten der ePA2.6 auf ePA3.0 sind bei der Prüfung auf zulässige Dokumentenformate die Hinweise zu A_24864-* und A_25009-* zu berücksichtigen.*

A_24966 - XDS Document Service - Migration: Konvertieren von PDF- in PDF/A-Dokumente

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 Dokumente im PDF-Format in ein PDF/A-Format konvertieren und ausschließlich das Dokument im PDF/A-Format in das Aktenkonto übernehmen.[<=]

A_25032 - XDS Document Service - Migration: Information des Versicherten zur Nichtübernahme von Dokumenten in bestimmten Formaten

Der Anbieter des ePA-Aktensystems MUSS den Versicherten darüber informieren, das Dokumente in der ePA2.6, die ein bestimmtes Format besitzen, nicht in die "ePA für alle" übernommen werden und informieren, um welche Formate es sich handelt.[<=]

A_24520 - XDS Document Service - Migration: Prüfsumme Dokument erzeugen

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 für jedes Dokument, das im Klartext vorliegt, die kryptographische Prüfsumme des Dokumentes berechnen und in `DocumentEntry.hash` hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die Dokumentengröße für das Feld `DocumentEntry.size` berechnet und gesetzt werden. [`<=`]

A_24847 - XDS Document Service - Migration: Identifizieren und Auflösen von Dokumenten-Dubletten

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 zum Zeitpunkt der Entschlüsselung eine Dublettenerkennung durchführen. Dabei werden entschlüsselte Dokumente innerhalb und außerhalb von Sammlungen verglichen mit Dokumenten, die durch eine zwischenzeitliche Nutzung von ePA für alle in die Akte eingestellt worden sind. Dubletten werden anhand der Gleichheit des Hash-Wertes im Feld `documentEntry.hash` identifiziert. Das Dokument mit dem älteren Einstelldatum wird verworfen. [`<=`]

A_24851 - XDS Document Service - Migration: Dokumente und Ordner mergen

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf die ePA 3.0 zum Zeitpunkt der Entschlüsselung des Datenbestands die Ordnerinhalte einer Kategorie vergleichen, falls es neben den migrierten ePA 2.6-Akteninhalten durch eine ePA3-Aktenutzung ebenfalls Ordnerinhalte gibt. Unter Berücksichtigung der Dublettenprüfung werden alle Dokumente von zwei Ordnern derselben Kategorie (in ePA 2.6 bzw. 3.0 entstanden) in einen Ordner zusammengeführt. Dokumente und RPLC-Ketten, die durch die `documentEntry.uniqueId` erkennbar zusammen gehören, werden unter Wahrung der Abfolge der Einstelldaten zusammengeführt und das jüngste Dokument als aktives Dokument der Kette behandelt. Dokumente erhalten eine `rootDocumentUniqueId` gemäß A_24451-*, falls noch nicht vorhanden. [`<=`]

A_24848 - XDS Document Service - Migration: Auflösung von duplizierten dynamischen Ordnern

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf die ePA 3.0 anhand des Titels dynamischer Ordner erkennen, ob zwei dynamische Ordner zur selben Kategorie vorliegen, z.B. zur selben Schwangerschaft. In diesem Falle werden alle vorhandenen Einträge in einen der Ordner hinein gemergt und der andere Ordner gelöscht.
[`<=`]

A_24522 - XDS Document Service - Migration: Erzeugen von Titeln für Dokumente

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf die ePA 3.0 sicherstellen, dass bei jedem Dokument das Metadatum `DocumentEntry.title` belegt ist. `documentEntry.title=""` oder `""` ist gleichbedeutend mit einem nicht vorhandenen Titel. Wenn title nicht belegt ist, MUSS `title` gemäß folgender Tabelle belegt werden.

Typ	Titel
Dokumente, die einem Implementation Guide zugeordnet sind	IG.displayName
andere Dokumententypen	Die gemäß A_24524-* bereinigte <code>DocumentEntry.URI</code> ohneExtension

[`<=`]

A_24523 - XDS Document Service - Migration: Löschen von ConfidentialityCodes

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 Dokumente und Ordner mit dem `confidentialityCode` "very restricted" auf die GeneralDenyPolicy setzen. Danach werden die `confidentialityCodes` gelöscht. [`<=`]

A_24817 - XDS Document Service - Migration: Normalisieren und Validieren der URI

Der XDS Document Service MUSS im Zuge der Migration von ePA 2.6 die ePA 3.0 für sämtliche Dokumente die `documentEntry.URI` gemäß A_24524-* und A_23447-* normalisieren und validieren. [`<=`]

A_24866-01 - Audit Event Service - Migration: Übernahme von Protokolldaten

Der Audit Event Service MUSS im Zuge der Migration von ePA 2.6 auf ePA 3.0 sämtliche Protokolldaten des Versicherten in die migrierte Akte übernehmen. Für die Migration werden alte Protokolldaten in ein PDF/A überführt und in den Ordner "technical" eingestellt. Für dieses Dokument sind die folgenden Metadaten für `DocumentEntry` zu verwenden:

- `title`: "Zugriffsprotokoll (bis Anfang 2025)"
- `classCode`: "DOK": (Dokumente ohne besondere Form (Notizen))
- `typeCode`: "PATD": (Patienteneigene Dokumente)
- `mimeType`: "application/pdf"
- `formatCode`:
 - `codeSystem` "2.25.154081344090540725127779452347992051720"
 - `code`: "urn:gematik:ig:archivedAuditEventData:v1.0"
 - `displayName`: "Zugriffsprotokoll (bis Anfang 2025)"; (gleicher Text wie 'title')

[`<=`]

2.8.4 Protokollierung der Migration

A_25029-01 - XDS Document Service - Protokollierung der Migration der medizinischen Daten

Der XDS Document Service MUSS den Vorgang der Migration der medizinischen Daten (Dokumente, Folder, Metadaten) gemäß A_24704* protokollieren. Dabei ist die Migration als atomares Ereignis zu betrachten und mit einem Protokolleintrag zu dokumentieren. Für den Protokolleintrag ist folgende Wertebelegung zu berücksichtigen:

Tabelle 2: Protokollierung der Migration der medizinischen Daten

Strukturelement	Wert	Erläuterung
<code>AuditEvent.type</code>	"object"	

Strukturelement	Wert		Erläuterung
AuditEvent.outcome	0		Migration war erfolgreich und ist abgeschlossen. Dieser Wert wird auch gesetzt, wenn einzelne Dokumente (z.B. Dokumente bestimmter Formate) nicht übernommen werden konnten.
	12		Migration wurde abgebrochen und wird ggf wiederholt, keine Datenübernahme ist erfolgt. In der AuditEvent.entity.detail Struktur werden keine Informationen hinterlegt.
AuditEvent.action	E		
AuditEvent.entity.name	"Migration"		
AuditEvent.entity.description	<Hinweistext>		
AuditEvent.source.type.code	"XDSSVC"		
AuditEvent.entity.detail	type	value[x]	dieses Strukturelement ist zu versorgen, wenn einzelne Dokumente nicht übernommen werden konnten
	"DocumentTitle"	<DocumentEntry.title>	Name des Dokumentes, welches nicht übernommen werden konnte

Strukturelement	Wert		Erläuterung
	"DocumentUniqueId"	<Document.uniqueId>	ID des Dokumentes, welches nicht übernommen werden konnte
	"DocumentFormatCode"	<DocumentEntry.formatCode>	kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3].
	"DocumentMimeType"	<DocumentEntry.mimeType>	

[<=]

A_25031-01 - Audit Event Service - Protokollierung der Migration der Protokolldaten des Versicherten

Der Audit Event Service MUSS den Vorgang der Migration der Protokolldaten des Versicherten gemäß A_24704* protokollieren.

Dabei ist die Migration als atomares Ereignis zu betrachten und mit einem Protokolleintrag zu dokumentieren.

Für den Protokolleintrag ist folgende Wertebelegung zu berücksichtigen:

Tabelle 3: Protokollierung der Migration der Protokolldaten des Versicherten

Strukturelement	Wert	Erläuterung
AuditEvent.type	"object"	
AuditEvent.action	E	
AuditEvent.source.type.code	"AUDITSVC"	
AuditEvent.entity.name	"MigrationProtocol"	
AuditEvent.entity.description	<Hinweistext>	dieses Strukturelement ist nur zu versorgen, wenn bei der Migration Fehler aufgetreten sind

[<=]

2.8.5 Weitere Datenanpassungen

A_27482 - XDS Document Service – Metadatenkorrektur bei elektronischen Arztbriefen

Der XDS Document Service MUSS die Metadaten (DocumentEntry) von bestehenden Dokumenten vom Typ "ig-eab.json" (elektronischer Arztbrief)

gemäß [gemSpec_IG_ePA] derartig anpassen, dass DocumentEntry.eventCodeList

zusätzlich um den KDL-Code (code: ED110104, codeSystem: 1.2.276.0.76.5.552, displayName: eArztbrief) erweitert wird, wenn dieser nicht bereits vorhanden ist.

[<=]

Hinweis: Eine Protokollierung der in diesem Abschnitt beschriebenen Datenanpassungen ist nicht notwendig.

2.9 Performance aus Anwendersicht

Im Gegensatz zu den Performancevorgaben, welche in [gemSpec_Perf] gemacht werden und welche lediglich die Aktivitäten im Aktensystem berücksichtigen, stellt sich die Leistungsfähigkeit und Nutzbarkeit in der Wahrnehmung der Clients oftmals anders dar. Aus diesem Grund werden die Endgeräte (Primärsystem und FdV) für definierte Anwendungsfälle (sogenannte UX-Usecases) dazu verpflichtet, eigene Messungen durchzuführen und diese Messwerte an eine definierte Schnittstelle im Aktensystem zu übermitteln. Das Aktensystem verarbeitet diese Informationen und leitet das konsolidierte Ergebnis im Rahmen der Betriebsdatenlieferung weiter an die gematik. Auf diese Weise erhalten sowohl die gematik (im Rahmen der Gesamt-Produktverantwortung) als auch die Anbieter der Aktensysteme Informationen darüber, wie die Anwendung ePA bei den Nutzern (insb. in der LEU und bei Versicherten) hinsichtlich bestimmter Kernfunktionalitäten wahrgenommen wird.

Die Anwendungsfälle umfassen dabei unter anderem das Login und das Hoch- bzw. Herunterladen von Dokumenten / Daten. Eine spezifische Beschreibung ist in der Spezifikation des FdVs bzw. im Implementierungsleitfaden für Primärsysteme zu finden.

Die Übermittlung der Messdaten erfolgt im Anschluss an den erfolgreichen Abschluss des Anwendungsfalles an das gleiche Aktensystem (unter Verwendung der Schnittstelle `InformationService.setUserExperienceResult`), bei dem auch der Anwendungsfall stattgefunden hat. Hierbei ist die Schnittstelle zur Lieferung der Messdaten an der Komponente "Information Service" nur für Primärsysteme normiert. Es steht dem Hersteller des Aktensystems frei, die Lieferschnittstelle für Messdaten von FdVs selbst oder nach dem Vorbild der PS-Schnittstelle zu implementieren.

Die eingegangenen Messergebnisse werden vom Aktensystem verarbeitet und anschließend gemäß der Vorgaben aus [gemSpec_Perf] an die Betriebsdatenerfassung der gematik im Rahmen der Rohdatenlieferung übermittelt.

A_24570-01 - Verarbeitung von UX-Messdaten

Das ePA-Aktensystem MUSS für die im zu betrachtenden Zeitintervall der Betriebsdatenlieferung (gemäß [gemSpec_Perf]) eingegangenen Messdaten je UX-Usecase, je Client-ID und je Client-Version folgende Werte ermitteln und gemäß [gemSpec_Perf] übermitteln:

- Durchschnittswert der Messergebnisse
- Anzahl der berücksichtigten Messergebnisse
- Maximalwert
- Minimalwert[<=]

Die Versionsnummer des Useragents wird bei der Konsolidierung nicht weiter verarbeitet und dient dem Anbieter des ePA-Aktensystems zur Identifikation von möglichen Fehlerquellen im Rahmen des Eigenmonitorings und Troubleshootings.

3 Funktionsmerkmale

3.1 Aktenkonto eines Versicherten (Health Record)

Ein ePA-Aktenkonto wird durch den Kostenträger eines Versicherten als Anbieter der ePA für jeden Versicherten angelegt und für die Nutzung im Rahmen der gesetzlichen Vorgaben zur Verfügung gestellt. Die Anlage eines Aktenkontos erfordert keine Beantragung durch den Versicherten, dieser kann einer Anlage seines Aktenkontos jedoch widersprechen.

3.1.1 Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte

Der Widerspruch des Versicherten gegen die grundsätzliche Nutzung der ePA kann jederzeit erfolgen. Wird dieser im Vorfeld der Anlage eines Aktenkontos erklärt, wird kein Aktenkonto für diesen Versicherten erzeugt. Existiert zum Zeitpunkt des Widerspruchs schon ein Aktenkonto (in einem beliebigen Zustand), so wird dieses gelöscht und alle enthaltenen Daten werden gelöscht.

Die Regelungen zum Widerspruch oder die Rücknahme des Widerspruchs gegen die grundsätzliche Nutzung der ePA sind durch den Anbieter der ePA eigenständig im Rahmen der gesetzlichen Vorgaben umzusetzen und sind nicht Bestandteil dieser Spezifikation.

Für die vereinfachte Prüfung auf einen bereits erteilten Widerspruch des Versicherten bei einem Wechsel des Kostenträgers muss die Information zu einem Widerspruch jedoch vermerkt und über die Schnittstelle `I_Information_Service_Account` [`I_Information_Service_Account`] abrufbar sein.

A_23886 - Anbieter ePA-Aktensystem - Keine Aktenkontoanlage bei Widerspruch des Versicherten

Der Anbieter des ePA-Aktensystems DARF ein Aktenkonto für den Versicherten NICHT anlegen, wenn ein Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte vorliegt. [`<=`]

Der Widerspruch gegen die grundsätzliche Nutzung der ePA kann durch den Versicherten jederzeit zurückgenommen werden. In diesem Fall wird wie bei der Anlage eines neuen Aktenkontos für den Versicherten verfahren.

A_25181 - Anbieter ePA-Aktensystem - Aktenkontoanlage bei Zurücknahme des Widerspruchs des Versicherten

Falls ein Versicherter den Widerspruch gegen die grundsätzliche Nutzung der ePA zurücknimmt MUSS der Anbieter des ePA-Aktensystems ein Aktenkonto für den Versicherten unverzüglich anlegen. [`<=`]

3.1.1.1 Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger

Die Regelungen zum Widerspruch oder die Rücknahme des Widerspruchs gegen das Einstellen von Abrechnungsdaten des Kostenträgers in die ePA sind durch den Anbieter

der ePA eigenständig im Rahmen der gesetzlichen Vorgaben umzusetzen und sind nicht Bestandteil dieser Spezifikation.

3.1.2 Lebenszyklus und Zustände eines Aktenkontos

Ein Aktenkonto durchläuft in seinem Lebenszyklus diverse Zustände. Einige dieser Zustände sind für rein administrative Vorgänge vorgesehen (Initialisierung, Umzug des Aktenkontos zu einem anderen Anbieter), andere für die Nutzung der Akte im Versorgungsprozess. Diese Nutzung für Versorgungsprozesse ist dabei auf den Zustand "Activated" eingeschränkt.

Eine Übersicht der unterschiedlichen Status und der Bedingungen für den Statusübergang sind in der folgenden Tabelle dargestellt.

Tabelle 4: Zustandswechsel im Lebenszyklus eines Aktenkontos

Zustand	Erläuterung	zulässige Transitionen	Folgezustand
UNKNOWN	Für einen Versicherten existiert kein Aktenkonto.	Konto initialisieren	Initialized
INITIALIZED	Ein neues Aktenkonto ist konfiguriert und für eine Aktivierung vorbereitet. Die initialen Befugnisse sind erstellt. Eine Nutzung des Aktenkontos im Versorgungsprozess und die Nutzung medizinischer Dokumente ist jedoch erst nach der Aktivierung möglich. Die Daten eines existierenden Aktenkontos werden importiert.	Widerspruch gegen die Nutzung der ePA	Unknown
		Explizite Aktivierung des Kontos durch den Anbieter. Bei existierendem Aktenkonto bei einem anderen Anbieter erfolgt die Aktivierung erst nach einem Import der Daten des Aktenkontos.	Activated
ACTIVATED	Das Aktenkonto ist aktiv und kann von befugten Nutzern und Nutzergruppen im Versorgungsprozess verwendet werden.	Vorbereitung des Umzugs des Aktenkontos zu einem anderen Anbieter (Erstellung des Exportpakets)	Suspended
		Widerspruch gegen die Nutzung der ePA	Unknown

Zustand	Erläuterung	zulässige Transitionen	Folgezustand
SUSPENDED	Die Daten des Aktenkontos des Versicherten werden zu einem neuen Anbieter übertragen. Die Nutzung des Aktenkontos ist in diesem Zustand nicht möglich.	Erfolgreicher Abschluss des Umzugs Widerspruch gegen die Nutzung der ePA	Unknown
		Der Bereitstellungszeitraum des Exportpakets ist abgelaufen.	Activated

Die Anforderungen in den folgenden Kapiteln legen die zulässigen Zustandswechsel eines Kontos fest.

3.1.3 Anlage eines neuen Aktenkontos

Ein neues Aktenkonto wird für einen Versicherten bei seinem Anbieter automatisch angelegt, wenn der Versicherte der grundsätzlichen Nutzung der ePA nicht widerspricht oder einen zuvor gegebenen Widerspruch zurücknimmt und bei einem anderen Anbieter kein Aktenkonto für den Versicherten existiert.

Die Anlage eines neuen Aktenkontos erfolgt in zwei Stufen: der Initialisierung und der darauffolgenden Aktivierung.

Bei der Initialisierung wird ein neues Aktenkonto bei einem Betreiber eines ePA-Aktensystems für den Versicherten angelegt und die Dienste des Aktenkontos für die Nutzung vorbereitet. Die Identifikation eines Aktenkontos erfolgt dabei über die KVNR des Versicherten (unveränderlicher Anteil der Versichertennummer) im Aktensystem und gegenüber Clients bei Nutzung der ePA.

A_24336 - Anbieter ePA-Aktensystem - Identifizierung eines Aktenkontos

Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos die KVNR des Versicherten zur Identifikation des Aktenkontos im Aktensystem verwenden und sicherstellen, dass diese Identifikation eines Aktenkontos nicht verändert werden kann. [<=]

A_23775 - Anbieter ePA-Aktensystem - Neues Aktenkonto anlegen

Der Anbieter des ePA-Aktensystems MUSS für Versicherte jeweils ein Aktenkonto anlegen, wenn kein Widerspruch des Versicherten gegen die Nutzung der ePA vorliegt, und dabei die KVNR des Versicherten zur Identifikation eines Aktenkontos im Aktenkonto registrieren. Das initialisierte Aktenkonto MUSS den Status INITIALIZED erhalten. [<=]

Wechselt der Versicherte den Anbieter, so kann ein Widerspruch des Versicherten gegen die Nutzung der ePA auch bei diesem bisherigen schon vorliegen. In diesem Fall kann die Anlage eines Aktenkontos bei einem neuen Anbieter entfallen. Andernfalls kann bei dem bisherigen Anbieter ein Aktenkonto existieren, dessen Daten im Rahmen der Anlage eines Aktenkontos beim neuen Anbieter importiert werden müssen.

A_27343 - Anbieter ePA-Aktensystem - verpflichtende Prüfung auf Widerspruch gegen die Nutzung der ePA bei einem anderen Anbieter

Der Anbieter des ePA-Aktensystems MUSS vor der Anlage eines Aktenkontos durch Verwendung der Operationen der Schnittstelle gemäß [I_Information_Service_Accounts]

prüfen, ob bei einem anderen Anbieter ein Widerspruch des Versicherten gegen die Nutzung der ePA vorliegt oder ein Aktenkonto des Versicherten existiert. [\leq]

A_24789 - Anbieter ePA-Aktensystem - verpflichtender Import eines existierenden Aktenkontos

Der Anbieter des ePA-Aktensystems MUSS die Inhalte eines existierenden Aktenkontos in ein neues, initialisiertes Aktenkonto vor dessen Aktivierung übernehmen. [\leq]

A_24302-01 - Anbieter ePA-Aktensystem - verpflichtende Nutzung der Schnittstelle des Information Service Accounts

Der Anbieter des ePA-Aktensystems MUSS bei der Anlage eines neuen Aktenkontos einen Import der Inhalte eines existierenden Aktenkontos von einem anderen Anbieter durch Verwendung der Operationen der Schnittstelle gemäß [I_Information_Service_Accounts] veranlassen. [\leq]

Der weitere Import eines existierenden Aktenkontos vor dessen Aktivierung erfolgt unter Verwendung des Health Record Relocation Service (3.2- Health Record Relocation Service).

A_24790-01 - Anbieter ePA-Aktensystem - keine unbegründeter Import eines Aktenkontos

Der Anbieter des ePA-Aktensystems DARF den Import eines existierenden Aktenkontos von einem anderen Anbieter für Zwecke abweichend der Vorgaben in A_24302-* NICHT nutzen oder veranlassen. [\leq]

A_15870-02 - Anbieter ePA-Aktensystem - Abbruch bei Nichtverfügbarkeit anderer Anbieter

Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen, wenn die Prüfung gemäß A_27343-* mindestens bei einem anderen Anbieters eines ePA-Aktensystems eine technische Fehlermeldung liefert oder dieser nicht erreichbar ist. [\leq]

A_27344 - Anbieter ePA-Aktensystem - Abbruch bei fehlgeschlagenem Import

Der Anbieter des ePA-Aktensystems MUSS die Erstellung eines Aktenkontos abbrechen, wenn ein Import von Daten eines Aktenkontos von einem bisherigen Anbieter erforderlich ist und dieser nicht erfolgreich abgeschlossen werden kann. [\leq]

Hinweis zu A_27344*: Ein Import kann beispielsweise fehlschlagen, wenn schwerwiegende Fehler bei der Exportpaketerstellung oder bei der Übertragung auftreten (siehe 3.2- Health Record Relocation Service).

Für die Geräteregistrierung bei Nutzung eines ePA-FdV durch den Versicherten ist eine E-Mail-Adresse des Versicherten für Bestätigung der Geräteregistrierung erforderlich. Falls vorhanden, kann diese E-Mail-Adresse bei der Anlage eines Aktenkontos im Device Management hinterlegt werden. Ansonsten muss eine E-Mail-Adresse bei der ersten Einrichtung eines ePA-FdV zur Nutzung des Aktenkontos hinterlegt werden. Eine E-Mail-Adresse muss vor der Übernahme in das Aktensystem validiert sein, beispielsweise durch Versand eines Bestätigungslink an diese E-Mail-Adresse.

A_14996-01 - Anbieter ePA-Aktensystem - Manuelle Ergänzung E-Mail-Adresse

Der Anbieter des ePA-Aktensystems MUSS es dem Versicherten auf geeignetem Weg ermöglichen, die Registrierung einer E-Mail-Adresse für die Geräteverwaltung auch nachträglich vorzunehmen. [\leq]

A_14993-02 - Anbieter ePA-Aktensystem - Mailadresse validieren

Der Anbieter des ePA-Aktensystems MUSS eine Mailadresse

- bei der ersten Hinterlegung im Aktensystem,
- bei einer Änderung der Mailadresse

auf Gültigkeit hin validieren. [\leq]

A_24369 - Anbieter ePA-Aktensystem - Initialisierung des Aktenkontos

Der Anbieter des ePA-Aktensystems MUSS die Initialisierung der Bestandteile

- Consent Decision Management (initiale Entscheidungen)
- Constraint Management (Policies)
- Entitlement Management (initiale Befugnisse und Befugnisausschlüsse)
- Information Service (initiale Entscheidungen "Versorgungsprozess")
- XDS Document Service (statische Aktenkontoinhalte)
- Device Management
- Authorization Service
- Audit Event Service
- Medication Service

vor der Aktivierung eines Aktenkontos durchführen. Die genannten Bestandteile MÜSSEN nach der Aktivierung des Aktenkontos sofort nutzbar sein. [≤]

Im Zustand INITIALIZED obliegt es dem Anbieter, ein Aktenkonto mittels administrativer Eingriffe in die verschiedenen Bestandteile des Aktensystems und -kontos auf die Aktivierung vorzubereiten bzw. zu konfigurieren.

A_26005 - ePA-Aktensystem – Optionale Schnittstelle zum Einbringen von initialen Befugnissen

Das ePA-Aktensystem KANN eine Schnittstelle für Kostenträger anbieten, über die Kostenträger die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle ins ePA-Aktensystem einbringen können. [≤]

A_26006 - ePA-Aktensystem – Nutzen der optionalen Schnittstelle zum Einbringen von initialen Befugnissen ausschließlich im Status INITIALIZED

Falls das ePA-Aktensystem eine Schnittstelle für Kostenträger anbietet, über die Kostenträger die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle für ein Aktenkonto einbringen können, MUSS das ePA-Aktensystem sicherstellen, dass diese Schnittstelle ausschließlich genutzt werden kann, wenn sich das Aktenkonto im Status INITIALIZED befindet.

[≤]

Das Aktenkonto wird nach Abschluss der Initialisierung durch den Anbieter aktiviert und kann dann durch befugte Nutzer und Nutzergruppen verwendet werden. Eine Aktivierung erfolgt für den Rollout der ePA Version 3 im Kontext des ePA Go-Live-Termins und zu späteren, individuellen Zeitpunkten, wenn Versicherte als ePA-Nutzer neu dazu gekommen (bspw. Widerspruch wird zurückgenommen und ePA wird später angelegt oder Versicherte Person kommt erstmalig ins Gesundheitssystem im Falle eines Zuzugs oder eines Neugeborenen).

A_24335 - Anbieter ePA-Aktensystem - Neues Aktenkonto aktivieren

Der Anbieter des ePA-Aktensystems MUSS ein neues Aktenkonto nach Abschluss der Initialisierung aktivieren (Status ACTIVATED), wenn die gesetzliche Widerspruchsfrist abgelaufen ist. [≤]

3.1.4 Löschen eines Aktenkontos

Die Löschung eines Aktenkontos bei einem Anbieter und aller darin enthaltenen Daten kann in folgenden Situationen erforderlich sein:

- Widerspruch des Versicherten gegen die Nutzung der ePA,

- nach erfolgreichem Wechsel des Anbieters durch den Versicherten und abgeschlossener Datenübernahme aus dem bisherigen Aktenkonto,
- nach Beendigung des Versicherungsverhältnisses des Versicherten bei seinem Kostenträger.

Ein Versicherter kann nach der Anlage eines Aktenkontos der grundsätzlichen Nutzung der ePA widersprechen. Liegt dieser erklärte Widerspruch vor, werden das Aktenkonto des Versicherten und sämtliche Inhalte durch den Anbieter des Aktenkontos gelöscht.

Bei einem Anbieterwechsel erfolgt die Übernahme der Daten des bisherigen Aktenkontos zu dem neuen Anbieter. Nach erfolgreichem Abschluss der Datenübernahme in das Aktenkonto des neuen Anbieters löscht der bisherige Anbieter das Aktenkonto des Versicherten und alle darin enthaltenen Daten.

Kündigt ein Versicherter das Vertragsverhältnis ohne Übernahme der Daten zu einem neuen Anbieter, löscht der Anbieter des Aktenkontos des Versicherten nach einer angemessenen Wartezeit, bzw. nach Ablauf von vorgeschriebenen Bereitstellungs- und Aufbewahrungszeiträumen, das Aktenkonto und alle darin enthaltenen Daten.

Vor der Ausführung der endgültigen Löschung des Aktenkontos muss es dem Versicherten ermöglicht werden, die Protokolldaten (auch unter Einbindung der Ombudsstelle) für seinen eigenen Gebrauch außerhalb des Aktenkontos zu sichern. Dieses ist nicht erforderlich, wenn das Aktenkonto in Folge eines erfolgreichen Umzugs zu einem anderen Anbieter geschlossen wird.

A_25289 - Anbieter ePA-Aktensystem - Löschen des Aktenkontos durch den Kostenträger

Der Anbieter des ePA-Aktensystems MUSS das Aktenkonto eines Versicherten inklusive aller enthaltenen Daten löschen (sämtliche Dokumente, Schlüsselmaterial, Protokolle, Widerspruchsinformation, Befugnisse und Beschränkungen), wenn dies durch den zuständigen Kostenträger beauftragt wird.[<=]

3.2 Health Record Relocation Service

Transfer eines Aktenkontos zu einem neuen Anbieter (Aktenkontoumzug).

Wechselt der Versicherte den Kostenträger bzw. den Anbieter seines Aktenkontos, so erfolgt der Umzug der Inhalte seines bestehenden Aktenkontos vom bisherigen Anbieter zu einem neuen Anbieter weitestgehend automatisiert.

Seitens der Aktensysteme werden für einen Aktenkontoumzug zwei Schnittstellen angeboten: `I_Health_Record_Relocation_Service` zur Nutzung durch die Anbieter (alt und neu) für den Zugriff auf das Aktenkonto des Versicherten und `I_Information_Service_Accounts` für die Interaktion der Aktensysteme (alt und neu) untereinander. Die notwendige Kommunikation der Kassen-Backends mit ihren Aktensystemen außerhalb der VAU erfolgt dabei in Absprache der Beteiligten und ist nicht Bestandteil der genannten Schnittstellen.

A_24786 - Health Record Relocation Service - Realisierung der Schnittstelle I_Health_Record_Relocation_Service

Der Health Record Relocation Service MUSS die Operationen der Schnittstelle `I_Health_Record_Relocation_Service` gemäß [`I_Health_Record_Relocation_Service`] umsetzen.[<=]

Hinweis: Zur Schnittstelle I_Information_Service_Accounts siehe 3.15.2- Information Service - Account).

A_24821 - Health Record Relocation Service - Suspendierung des Aktenkontos

Der Health Record Relocation Service MUSS sicherstellen, dass das Aktenkontos für die Erstellung eines Exportpakets auf den Status SUSPENDED gesetzt wird.[<=]

A_24827 - Health Record Relocation Service - Reaktivierung des Aktenkontos

Der Health Record Relocation Service MUSS sicherstellen, dass ein Aktenkonto im Status SUSPENDED nach einem Abbruch eines Transfers von einem Anbieter zu einem anderen Anbieter aufgrund eines Fehlers (Datenübertrag ist nicht erfolgt) in den Status ACTIVATED gesetzt wird.[<=]

A_25005-02 - Health Record Relocation Service - Daten des Exportpakets

Der Health Record Relocation Service MUSS sicherstellen, dass alle Daten des Aktenkontos in das Exportpaket übernommen werden aus:

- XDS Document Service
- Medication Service
- Consent Management
- Constraint Management
- Audit Event Service
- Entitlement Management (außer Befugnisse für Versicherte, E-Rezept-Fachdienst, Kostenträger und Ombudsstelle).
- E-Mail Management (die E-Mail-Adresse des Aktenkontoinhabers (falls vorhanden) sowie für alle Vertreter die E-Mail-Adressen, sofern sie die dem exportierenden Aktensystem bekannt sind).

Bei FHIR Data Services MUSS der Health Record Relocation Service sicherstellen, dass die jeweilige Resource.id aller FHIR-Instanzen ebenso in das Exportpaket einfließen, sodass nach einem Import die Identitäten der FHIR-Daten stabil bleiben.

[<=]

Hinweis: Die Geräteregistrierungen des Versicherten oder der Vertreter werden nicht exportiert. Bei einem neuen Anbieter ist für den Versicherten eine erneute Geräteregistrierung erforderlich.

A_25605 - Health_Record_Relocation_Service - Erstellung des Exportpakets

Der Health Record Relocation Service MUSS sicherstellen, dass das Exportpaket gemäß der Vorgaben in [HealthRecordMigration] bezüglich der Struktur, der Formate für die enthaltenen Daten und die Verschlüsselung erfolgt. [<=]

A_25012 - Health Record Relocation Service - Signatur der Befugnisse

Der Health Record Relocation Service MUSS sicherstellen, dass die gemäß A_23734-* signierten Anteile einer Befugnis mit der Signaturidentität ID.FD.SIG (Rolle oid_epa_vau) signiert werden.[<=]

Hinweis: Der CMAC einer Befugnis wird nicht ins Export-Paket übernommen.

A_25719 - Health Record Relocation Service - JWT der Befugnis im Exportpaket

Der Health Record Relocation Service MUSS sicherstellen, dass die Befugnisse im Exportpaket als gültig signierte JWT mit den dargestellten Inhalten abgelegt sind:

Befugnis	Claim Name	Claim	Beispiel
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.SIG	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	
	"exp"	Verfalldatum, = "iat" + 8Tage"	Mindestens für den gesamten Bereitstellungszeitraum des Exportpakets
	"insurantId"	KVNR des Aktenkontos	A123456789
	"actorId"	Identifizier (Telematik-id oder KVNR)	3-883110000092471
	"validTo"	Ende der Gültigkeit,	gemäß [RFC3339], z.B. 2025-06-30T21:59:59Z oder 2025-06-30T23:59:59+02:00

[<=]

Der Wert "ES256" (JWS-Parameters "alg") gilt auch für die Kurve "brainpoolP256r1" (also nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen."

A_24787-01 - Health Record Relocation Service - Verschlüsselung des Exportpaketes

Der Health Record Relocation Service MUSS sicherstellen, dass Exportpakete ausschließlich verschlüsselt für den Download zu einem anderen Betreiber zur Verfügung stehen. Für die Verschlüsselung MUSS das kryptographische Material des ENC-Zertifikats verwendet werden, welches mittels der Regel hsm-r7 vom VAU-HSM abgerufen wurde.[<=]

A_24942 - Health Record Relocation Service – Prüfung Provider ENC Zertifikat

Der Health Record Relocation Service MUSS das übergebene Provider ENC-Zertifikat mittels TUC_PKI_018 (OCSP-Graceperiod=12h, PolicyList= oid_fd_enc, professionOID =

oid_epa_vau) prüfen und ungültige Zertifikate mit der Fehlermeldung " CERTIFICATE_INVALID " ablehnen. [<=]

A_21750 - Health Record Relocation Service – Integritätsschutz Exportpaket

Der Health Record Relocation Service MUSS das erstellte Exportpaket mit einem "Digest" HTTP Response Header (<https://tools.ietf.org/html/rfc5843>) als Integritätsschutz versehen und dabei als Digest Algorithmus SHA-256 verwenden.
Beispiel Digest-Header:

Digest: SHA-
256=MWVkmWQxYTRiMzk5MDQ0MzI3NGU5NDEyZTk5OWY1ZGFmNzgyZTJlODYzYjRjYzFh
OTlmNTQwYzI2M2QwM2U2MQ==
[<=]

A_15051 - Health Record Relocation Service - Authentisierung gegenüber einem neuen Aktenanbieter

Der Health Record Relocation Service, welcher das Exportpaket zur Verfügung stellt, MUSS sich beim Abruf des Exportpakets durch ein anderes ePA-Aktensystem mit der TLS-Identität oid_epa_mgmt und Zertifikatsprofil C.FD.TLS-S authentisieren.
[<=]

A_15048 - Health Record Relocation Service - Authentifizierung des neuen Aktenanbieters

Der Health Record Relocation Service MUSS den Abruf des Exportpakets durch ein anderes ePA-Aktensystem ablehnen, wenn sich der abrufende Client nicht als ePA-Aktensystem in der Rolle oid_epa_mgmt in einem TLS-Zertifikat C.FD.TLS-C authentisiert. [<=]

A_17236 - Health Record Relocation Service - Prüfung der TLS-Zertifikate

Der Health Record Relocation Service MUSS bei der Authentifizierung eines anderen Aktensystems beim Abruf des Exportpakets die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC_PKI_018 durchführen. Zur Prüfung des TLS-Zertifikats C.FD.TLS-S sind dabei die Parameter PolicyList=oid_fd_tls_s, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-serverAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD.TLS-C sind dabei die Parameter PolicyList=oid_fd_tls_c, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-clientAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden.
[<=]

A_15703 - Health Record Relocation Service - Verfügbarkeit Export-Paket

Der Health Record Relocation Service MUSS ein erstelltes Export-Paket für maximal sieben Kalendertage zum Abruf durch einen anderen Anbieter eines ePA-Aktensystems bereithalten. [<=]

A_21239 - Health Record Relocation Service – Verhalten bei Nichtabholen des Exportpakets

Der Health Record Relocation Service MUSS nach Ablauf des Bereithaltungszeitraums entsprechend A_15703* ein erstelltes Export-Paket löschen und den Status des Aktensystems von SUSPENDED auf ACTIVATED zurücksetzen. [<=]

Hinweis: siehe dazu auch 3.2.1.7.3- Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter

A_14905-04 - Health Record Relocation Service – Import des Exportpakets des vorhergehenden Aktenkontos

Der Health Record Relocation Service MUSS das vom vorhergehenden Anbieter ePA-Aktensystem des Versicherten bezogene Exportpaket, in das neue Aktenkonto importieren und dazu:

- das Exportpaket mittels des privaten ENC-VAU-Schlüssels des neuen Betreibers entschlüsseln,
- den Digest gemäß A_21750-* prüfen,
- die Befugnisse mit Regel "rr5" (siehe Tab_AS_Entitlement_Registration_Rules im Aktensystem) registrieren und
- falls DocumentEntry.originalURI im Exportpaket vorhanden ist, wird für jedes Dokument eines SubmissionSet der Inhalt von DocumentEntry.URI durch den Inhalt von DocumentEntry.originalURI ersetzt. (Hinweis: DocumentEntry.originalURI darf nicht als eigenständiges Metadatum in die Registry übernommen werden, da es lediglich dem Transport des Originalwertes von DocumentEntry.URI aus dem alten Aktensystem dient.

[<=]

A_21548-01 - Health Record Relocation Service - Information der Vertreter über neuen FQDN nach Abschluss des Anbieterwechsels

Der Health Record Relocation Service MUSS sicherstellen, dass alle Vertreter nach erfolgreichem Import des Exportpakets und somit Abschluss des Anbieterwechsels über Anbieterwechsel und den FQDN des neuen Aktensystems des Versicherten informiert werden, so dass sie in der Lage sind, die erforderliche initiale Anmeldung und Geräteregistrierung durchzuführen und informiert sind, welche Art von personenbezogenen Daten vom Vertreter im Rahmen der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine Vertreterberechtigung widerrufen kann und gegenüber wem er seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann.[<=]

Hinweis zu A_21548-01: Für die Benachrichtigung derjenigen Vertreter, die dem importierenden Aktensystem nicht bekannt sind, werden die E-Mail-Adressen aus dem Exportpaket genommen. Für die Benachrichtigung der Vertreter, die dem importierenden Aktensystem bekannt sind, wird die im importierenden Aktensystem hinterlegte E-Mail-Adresse des Vertreters verwendet.

A_26257 - Health Record Relocation Service - Löschen der im Exportpaket enthaltenen E-Mail-Adressen der Vertreter

Der Health Record Relocation Service MUSS sicherstellen, dass die im Exportpaket enthaltenen E-Mail-Adressen von Vertretern ausschließlich zur Information der Vertreter gemäß A_21548-* genutzt werden und nach Abschluss des Anbieterwechsels im importierenden Aktensystem gelöscht werden, d.h. nicht im importierenden Aktensystem gespeichert werden.[<=]

A_24788 - Health Record Relocation Service - Löschen des Exportpakets nach Umzug des Aktenkontos

Das Aktensystem MUSS sicherstellen, dass ein vorhandenes Exportpaket nach einem erfolgreichen Transfer eines Aktenkontos eines Versicherten von einem Anbieter zu einem anderen Anbieter gelöscht wird.[<=]

A_24982-02 - Health Record Relocation Service – Protokollierung des Anbieterwechsels eines Aktenkontos

Der Health Record Relocation Service des neuen (importierenden) Aktensystems MUSS nach der erfolgreichen oder einer abgebrochenen Übertragung der Inhalte eines Aktenkontos vom bisherigen Anbieter einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

Tabelle 5 : Health Record Relocation Service Protokollierung

Strukturelement	Wert		Erläuterung
AuditEvent.type	"object"		
AuditEvent.action	E		Übertrag von Daten eines Aktenkontos von einem anderen Anbieter
AuditEvent.agent.type	PAYOR		Umzug wurde ausgelöst vom Kostenträger.
AuditEvent.entity.name	"HealthRecordRelocation"		
AuditEvent.entity.detail	type	value[x]	
	"OriginName"	<Name des Kostenträgers>	Name des Kostenträgers, von welchem ein bestehendes Aktenkonto übernommen wird

[<=]

Hinweis: Das Aktensystem des bisherigen Anbieters muss keinen Protokolleintrag gemäß A_24982 erzeugen.*

3.2.1 Ablauf eines Aktenkontoumzugs

3.2.1.1 Initialisierung des Aktenkontos bei einem neuen Anbieter

Der Anbieter (neu) lässt im Aktensystem (neu) ein neues Aktenkonto anlegen. Dieses erhält den Status INITIALIZED. Hierfür gelten die Anforderungen gemäß 3.1.3- Anlage eines neuen Aktenkontos.

Falls der Versicherte schon einen Widerspruch gegen die Nutzung der ePA bei seinem bisherigen Kostenträger erklärt hat, kann die Initialisierung eines neuen Aktenkontos ggf. entfallen. Ein Transfer, bzw. die Erstellung eines Exportpakets, ist in diesem Fall mangels eines existierenden Aktenkontos beim bisherigen Anbieter nicht erforderlich.

Die Abfrage eines existierenden Widerspruchs des Versicherten bei einem anderen Anbieter ePA-Aktensystem erfolgt über dessen Information Service.

Abfrage eines existierenden Widerspruchs gegen die Nutzung der ePA	
I_Information_Service_Accounts (bisheriges Aktensystem)	
getGeneralConsentDecision	Abfrage des ggf. schon erteilten Widerspruchs gegen die Nutzung der ePA durch den Versicherten

3.2.1.2 Start Transfer eines existierenden Aktenkontos

Hat der Versicherte bei keinem Anbieter einen Widerspruch gegen die Nutzung der ePA erklärt und existiert bei einem bisherigen Anbieter (alt) ein Aktenkonto, wird der Transfer der Daten durch das Aktensystem (neu) initiiert.

Das Aktensystem (alt), bei welchem das Aktenkonto existiert, bestätigt diese Anfrage zum Transfer mit einer Vorgangs-ID.

Starten des Transfers	
I_Information_Service_Accounts (bisheriges Aktensystem)	
startRelocation	initiiieren der Exportpaketerstellung

3.2.1.3 Erzeugung Exportpaket für Transfer durch den bisherigen Anbieter

Das Aktensystem (alt) informiert den Anbieter (alt) über die Anfrage zum Transfer und die Vorgangsnummer. Der Anbieter (alt) öffnet das existierende Aktenkonto des Versicherten und stößt in der VAU die Erzeugung des Exportpakets an. Der Health Record Relocation Service beantwortet diese Anfrage durch Rückgabe einer URL für den späteren Download des Exportpakets durch den neuen Anbieter und startet die Erzeugung des Exportpakets. Das Aktenkonto wird vor der Paketerstellung auf den Status SUSPENDED gesetzt, um weitere Aktivitäten seitens der Nutzer zu verhindern.

Erzeugen des Exportpakets	
I_Health_Record_Relocation_Service_ (bisheriger Anbieter)	
startPackageCreation	Starten der Erzeugung des Exportpakets in der VAU

In dieses Exportpaket werden alle Daten des Aktenkontos gemäß A_25005* übernommen. Das fertige Exportpaket wird mittels ENC-Zertifikat, welches im VAU-HSM eingebracht und gespeichert wurde, verschlüsselt und am vorbereiteten Downloadpunkt bereitgestellt.

3.2.1.4 Übermittlung Download-URL Exportpaket für Transfer an den neuen Anbieter

Der Anbieter (alt) veranlasst nach Erhalt der Download-URL über das Aktensystem (alt) den Versand der Url an das Aktensystem (neu).

Das Aktensystem (alt) prüft vor der Übermittlung der Download-URL an das Aktensystem (neu), ob das Exportpaket für den Download bereitsteht, ggf. wird auf den Abschluss der Paketerstellung gewartet. Ist dieses der Fall, erfolgt die Benachrichtigung des Information_Service des Aktensystem (neu) mit der Übergabe der URL

Übergabe der Download-URL für das Exportpaket	
I_Information_Service_Accounts (neues Aktensystem)	
putDownloadUrlForExportPackage	Übergabe der geprüften Download-URL

3.2.1.5 Import des Exportpakets durch den neuen Anbieter

Der Information Service des Aktensystems (neu) nimmt die Download-URL entgegen und übermittelt diese an den Kostenträger (neu). Dieser öffnet den Zugang zum Aktenkonto (neu) des Versicherten und veranlasst in der VAU den Import des Exportpakets.

Import und Integration des Exportpakets	
I_Health_Record_Relocation_Service (neuer Anbieter)	
startPackageImport	Starten des Imports der vorhandenen Daten

3.2.1.6 Abschluss des Transfers durch beide Anbieter

Das Aktensystem (neu) startet den Download des Exportpakets, entschlüsselt dieses und übernimmt die Daten in das initialisierte Aktenkonto des Versicherten. Nach erfolgreichem Abschluss wird (kann) das Aktenkonto (neu) in den Status ACTIVATED überführt werden.

Unter Verwendung des Information Service wird das Aktensystem (alt) über den erfolgreichen Import und den Abschluss des Transfers informiert. Das Aktenkonto (alt) kann daraufhin, ggf. unter Einhaltung weiterer Bedingungen des Kostenträgers bzw. gesetzlicher Vorgaben, gelöscht werden (Status = UNKNOWN).

Abschluss des Transfers	
I_Information_Service_Accounts (bisheriges Aktensystem)	
deleteExportPackage	Beenden des Vorgangs (Löschen Exportpaket und ggf. bisheriges Aktenkonto)

3.2.1.7 Fehlersituationen und Handhabung

Der gesamte Austausch von Informationen zwischen Aktensystemen und Anbietern kann durch die in Schritt 1 erzeugte Vorgangs-ID genau einem konkreten Relocation Vorgang zugeordnet werden. Diese Vorgangsnummer wird auch verwendet, wenn das jeweils andere Aktensystem über Fehler im Ablauf benachrichtigt werden muss (Incidents).

3.2.1.7.1 Abruf des Exportpakets durch neuen Anbieter nicht mehr erforderlich oder derzeit nicht möglich

Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter (alt) das Exportpaket voraussehbar nicht importieren oder widerspricht der Versicherte nach der Initialisierung des Aktenkontos beim neuen Kostenträger der Nutzung der ePA, so kann durch Übertragung eines Incidents an das Aktensystem (alt) dieser Sachverhalt

mitgeteilt werden, so dass der Transfervorgang abgebrochen und das Exportpaket nicht erzeugt oder wieder gelöscht wird.

Incident Abbruch des Transfers		
I_Information_Service_Accounts (bisheriger Anbieter)		
postExportPackageIncident	Benachrichtigung zum Abbruch des Transfers	
	Incident	
	relocationAborted	Abbruch aus Gründen bei Anbieter (neu). Transfer wird zu gegebener Zeit erneut gestartet

Das Aktenkonto wird bei Anbieter (alt) wieder in den Status ACTIVATED gesetzt, um eine weitere Nutzung zu ermöglichen.

Für einen Transfer zu einem späteren Zeitpunkt muss der Anbieter (neu) den Vorgang durch Anfrage bei den weiteren Anbietern (alt) und Übermittlung eines ENC-Zertifikats erneut starten.

3.2.1.7.2 Fehler beim Download oder Import durch den neuen Anbieter

Kann ein Anbieter (neu) nach dem Start der Exportpaketerzeugung durch den Anbieter (alt) das Exportpaket unter Verwendung der übertragenen Download-URL nicht oder nicht vollständig laden oder die Inhalte des Exportpaketes aufgrund fehlerhafter Verschlüsselung oder fehlerhafter Struktur oder Inhalte nicht erfolgreich integrieren oder

der Anbieter (neu) hat keine Download-URL vom Anbieter (alt) bezogen, so kann durch Übertragung eines Incidents an den Anbieter (alt) dieser Sachverhalt mitgeteilt werden.

Incident Fehler bei Import		
I_Information_Service_Accounts (bisheriges Aktensystem)		
postExportPackageIncident	Benachrichtigung zu Problemen beim Import des Exportpakets	
	Incident	
	importFailed	Exportpaket kann nicht vom Downloadpunkt geladen werden, ist unvollständig oder falsch verschlüsselt
	packageCorrupt	Exportpaket kann nicht verarbeitet werden (strukturelle Fehler oder inhaltliche Fehler)
	urlNotReceived	Download-URL nicht erhalten

Das Aktenkonto verbleibt beim neuen Anbieter in Status INITIALIZED. Die Incidentmeldung an den Anbieter (alt) kann durch Kommunikation der Anbieter und/oder Betreiber untereinander zum Zweck der Problemlösung ergänzt werden.

Der Anbieter (alt) meldet die Korrektur durch erneuten Versand einer Download-URL an den Anbieter (neu) für den unterbrochenen Vorgang.

Es obliegt dem Anbieter (alt), bei zeitlich aufwendigen Korrekturen das Aktenkonto zunächst für eine weitere Nutzung wieder zu aktivieren (Status ACTIVATED) und nach Abschluss der Korrektur wieder in den Status SUSPENDED zu überführen.

Es obliegt dem Anbieter (alt) auch, bei zeitlich aufwendigen Korrekturen den Transfer durch Senden des Incidents "relocationAborted" an den Anbieter (neu) abubrechen und das Aktenkonto zur weiteren Nutzung wieder zu aktivieren (Status ACTIVATED). Der Transfer muss dann durch den Anbieter (neu) erneut gestartet werden.

3.2.1.7.3 Nicht erfolgter Download oder fehlende Rückmeldung durch den neuen Anbieter

Ruft ein neuer Anbieter ein bereitgestelltes Exportpaket nicht ab oder erfolgt durch den neuen Anbieter keine Benachrichtigung über einen erfolgreichen Abschluss des Transfers

oder einen Fehler beim Import des Exportpakets, dann kann eine Benachrichtigung an den neuen Anbieter erfolgen.

Incident Abbruch des Transfers durch bisherigen Anbieter		
I_Information_Service_Accounts (neuer Anbieter)		
postPackageDeliveryIncident	Benachrichtigung zum Abbruch des Transfers	
	Incident	
	noRelocationConfirmation	Nach Ablauf der Bereitstellungszeit gemäß A-15703-* wird der Transfer durch den Anbieter (alt) abgebrochen, da keine Bestätigung eines erfolgreichen Imports erfolgte.

Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei Anbieter (alt) auf den Status ACTIVATED gesetzt, um eine weitere Nutzung zu ermöglichen. Exportpaket und Downloadlink können gelöscht werden. Der Transfer muss durch den Anbieter (neu) erneut gestartet werden.

3.2.1.7.4 Abbruch des Transfers durch den bisherigen Anbieter

Ein Anbieter (alt) kann den Abbruch eines angeforderten Transfers an den Anbieter (neu) signalisieren.

Incident Abbruch des Transfers durch bisherigen Anbieter		
I_Information_Service_Accounts (neuer Anbieter)		
postPackageDeliveryIncident	Benachrichtigung zum Abbruch des Transfers	
	Incident	
	relocationAborted	Das Exportpaket kann aufgrund von Ursachen seitens Anbieter (alt) nicht (länger) bereitgestellt werden. Der Transfer wird vorzeitig abgebrochen und muss erneut gestartet werden.

Der Transfer wird durch den Anbieter (alt) abgebrochen. Das Aktenkonto wird bei Anbieter (alt) auf den Status ACTIVATED zurückgesetzt, wenn dieses schon den Status

SUSPENDED hat, um eine weitere Nutzung zu ermöglichen. Exportpaket und Downloadlink können gelöscht werden. Der Transfer muss durch den Anbieter (neu) erneut gestartet werden.

3.3 Sichere Speicherung sensibler Schlüssel und Informationen im VAU-HSM

Im Folgenden wird beschrieben, welche Informationen in einem HSM (als VAU-HSM bezeichnet) zu speichern sind.

Verständnishinweis: Die HMAC-Schlüssel (symmetrische Schlüssel) für die Prüfung der VSDM+-Prüfnachweise [gemSpec_SST_FD_VSDM], [C_11321] werden von den VSDM-Betreibern erzeugt und für die ePA-VAUs der ePA-Betreiber verschlüsselt exportiert. Die Schlüssel und auch die Export/Import-Vorgänge (Mehr-Augen-Prinzip) sind die gleichen wie sie auch für/bei der E-Rezept-VAU verwendet werden.

A_24611-03 - ePA-Aktensystem - Im VAU-HSM gespeicherte Schlüssel und Informationen für VAU-Betrieb

Das ePA-Aktensystem MUSS sicherstellen, dass folgende, für den Betrieb der VAU notwendigen Schlüssel und Informationen in einem HSM (als VAU-HSM bezeichnet) gespeichert werden:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU (u.a. genutzt für die Authentisierung der VAU beim Aufbau des VAU-Kanals)
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier oid_epa_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel
- Masterkeys für die Ableitung der versichertenindividuellen Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und Überschlüsselung")
- symmetrische Schlüssel für die HMAC-Prüfung der VSDM-Prüfziffern (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

Hinweis:

Es gelten die Anforderungen aus [gemSpec_Krypt#3.18 VSDM-Prüfziffer Version 2] für ein ePA-Aktensystem in der Rolle "Prüfziffer Version 2 prüfendes System". Aus den ins HSM importierten gemeinsamen Geheimnissen erfolgt im HSM eine Schlüsselableitung (A_27299-*) der für die Entschlüsselung der Prüfziffer Version 2 benötigten AES/GCM-Schlüssel.

A_26109 - ePA-Aktensystem - Unterschiedliche private

Authentisierungsschlüssel für AK-, Befugnisverifikations- und Service-VAU

Das ePA-Aktensystem MUSS sicherstellen, dass für die Authentisierungsidentitäten für Aktenkontoverwaltungs-VAUs, Befugnisverifikations-VAUs und Service-VAUs unterschiedliche private Schlüssel verwendet werden. [≤]

A_26110 - ePA-Aktensystem - Unterschiedliche private

Authentisierungsschlüssel für unterschiedliche Service-VAUs

Das ePA-Aktensystem MUSS sicherstellen, dass für unterschiedliche Typen von Service-VAUs unterschiedliche private Schlüssel für die Authentisierung genutzt werden. [≤]

Hinweis zu A_26110: Ein Typ einer Service-VAU könnte beispielsweise eine PDF-Konvertierungs-Service-VAU sein. Alle Instanzen einer PDF-Konvertierungs-Service-VAU nutzen denselben privaten Authentisierungsschlüssel. Die Instanzen der Pseudonymisierungs-Service-VAU dürfen den Authentisierungsschlüssel der PDF-Konvertierungs-Service-VAU jedoch nicht verwenden.

A_24612-04 - ePA-Aktensystem - Erzwingen von 4-Augen-Prinzip für Einbringen und Verwalten von Informationen ins VAU-HSM

Das ePA-Aktensystem MUSS technisch erzwingen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-Prinzip in das VAU-HSM eingebracht und verwaltet werden können:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier oid_epa_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[≤]

A_24614-03 - ePA-Aktensystem - Einbringung von Informationen ins VAU-HSM im 4-Augen-Prinzip mit der gematik

Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die folgenden, für den Betrieb der VAU notwendigen Schlüssel und Informationen ausschließlich im 4-Augen-

Prinzip ins VAU-HSM eingebracht und im VAU-HSM verwaltet werden, bei dem eine von der gematik benannte Person beteiligt ist:

- privater Schlüssel der Authentisierungsidentität der Aktenkontoverwaltungs-VAU
- ggf. private Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU
- ggf. private Schlüssel der Authentisierungsidentitäten für Service-VAUs
- privater Schlüssel der Verschlüsselungsidentität der VAU
- privater Schlüssel der Signaturidentität der VAU
- Zertifikat C.FD.ENC mit policyIdentifier oid_epa_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden.
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse)
- Hashwertrepräsentationen der erlaubten VAU-Software und VAU-Hardware (für die Aktenkontoverwaltungs-VAU, ggf. für die Befugnisverifikations-VAU und ggf. für Service-VAUs)
- Root-CA (nur, falls das Befugnisverifikations-Modul im VAU-HSM läuft).

[<=]

Beim Einbringen der Hashwertrepräsentation der erlaubten VAU-Software ins VAU-HSM prüft die von der gematik benannte Person, dass die Hashwertrepräsentation des VAU-Images zuvor vom Hersteller des ePA-Aktensystems an die gematik übermittelt wurde und zulässig für den Produktivbetrieb ist.

A_24618-03 - ePA-Aktensystem - Zugriff auf Schlüssel und Informationen im VAU-HSM

Das ePA-Aktensystem MUSS sicherstellen, dass auf die folgenden, für den Betrieb der VAU notwendigen und im VAU-HSM gespeicherten Schlüssel und Informationen ausschließlich über attestierte VAU-Instanzen zugegriffen werden kann:

- privater Schlüssel der Authentisierungsidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität der Befugnisverifikations-VAU ausschließlich durch eine Befugnisverifikations-VAU-Instanz
- privater Schlüssel der Authentisierungsidentität eines Service-VAU-Typs ausschließlich durch eine Service-VAU-Instanz dieses Service-VAU-Typs
- privater Schlüssel der Verschlüsselungsidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- privater Schlüssel der Signaturidentität der VAU ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Zertifikat C.FD.ENC mit policyIdentifier oid_epa_vau für die Verschlüsselungsidentität des anderen ePA-Aktensystembetreibers ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Datenpersistierungsschlüssel ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz

- Masterkeys für die Ableitung der versichertenindividuellen Befugnispersistierungsschlüssel ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz
- Masterkeys für die Ableitung der versichertenindividuellen Überschlüsselungsschlüssel (vgl. Abschnitt "Umschlüsselung und Überschlüsselung") ausschließlich durch die Aktenkontoverwaltungs-VAU-Instanz oder durch eine dedizierte Überschlüsselungs-VAU
- symmetrische Schlüssel für HMAC der VSDM-Prüfziffer (jeweils einen pro VSD-Dienst-Betreiber), die im Kontext der Prüfziffer Version 2 auch als gemeinsames Geheimnis bezeichnet werden, ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz
- symmetrischer Schlüssel für CMAC (zur Sicherung der registrierten Befugnisse) ausschließlich durch eine Aktenkontoverwaltungs-VAU-Instanz oder eine Befugnisverifikations-VAU-Instanz.

[<=]

3.4 Befugnisverifikations-Modul

Das Befugnisverifikations-Modul enthält die Regeln zur Befugnisregistrierung (entitlement registration rules) und die Regeln zum Abruf der versichertenindividuellen Persistierungsschlüssel (key rules).

Die folgende Abbildung zeigt die zwei möglichen Architekturvarianten für die Ausführung des Befugnisverifikations-Moduls. In Variante 1 wird es direkt im VAU-HSM ausgeführt. In Variante 2 wird es in einer Befugnisverifikations-VAU ausgeführt, die zwischen einer Aktenkontoverwaltungs-VAU und einem VAU-HSM vermittelt und Prüfungen für das VAU-HSM übernimmt (z. B. prüfen der ID-Token oder registrieren neuer Befugnisse).

In beiden Varianten ist ein Zugriff auf die Schlüssel im VAU-HSM nur durch integrale und attestierte VAUs möglich. Die Prüfung der VAU-Attestierungstoken verbleibt in beiden Varianten im VAU-HSM (VAU-Token-Modul). Das VAU-HSM speichert in Variante 2 neben den Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der Aktenkontoverwaltung zusätzlich auch die Hashwertrepräsentationen der erlaubten VAU-Software und erlaubten VAU-Hardware für die VAU der Befugnisverifikations-VAU. Ein Zugriff auf das HSM ist dann nur mit einem validen Attestierungstoken für die Aktenkontoverwaltung-VAU und die Befugnisverifikations-VAU möglich.

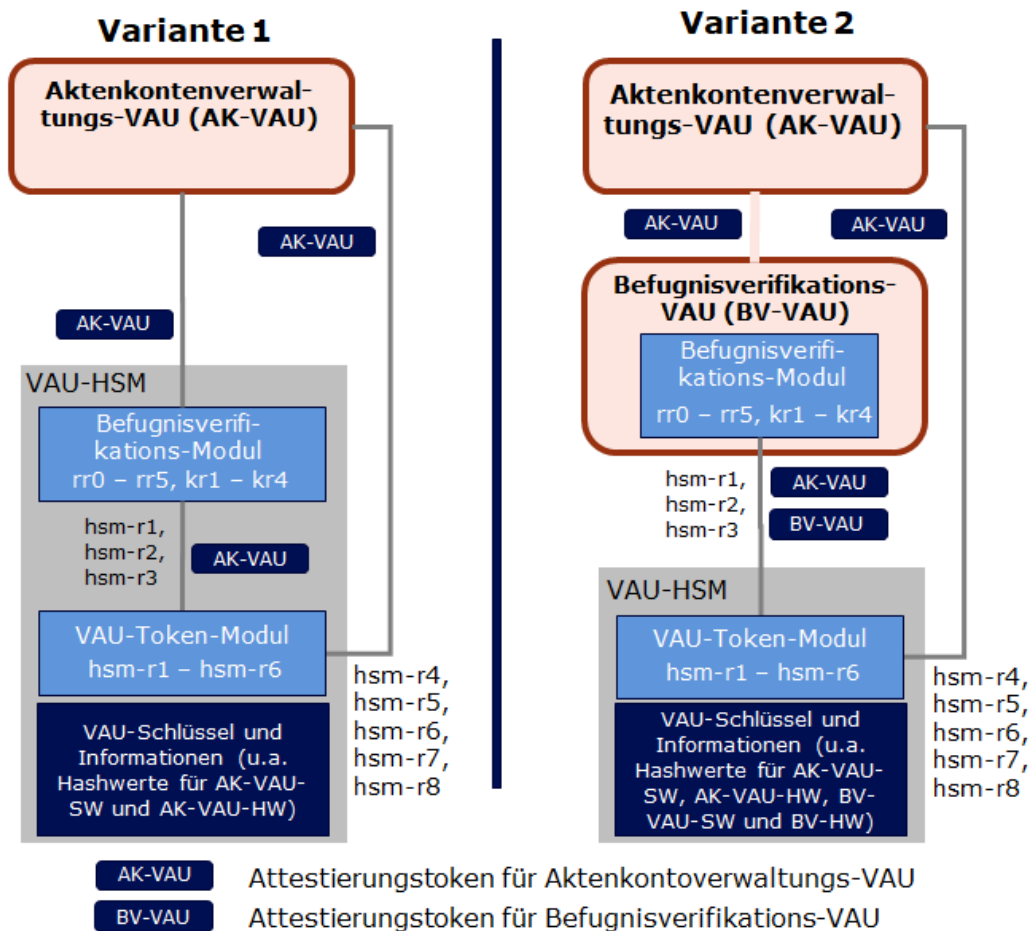


Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls

A_25281 - ePA-Aktensystem - VAU-Token-Modul ausschließlich im HSM

Das ePA-Aktensystem MUSS sicherstellen, dass ein VAU-Token-Modul ausschließlich in einem VAU-HSM ausgeführt wird. [≤]

A_24574 - ePA-Aktensystem - Befugnisverifikations-Modul im HSM oder Befugnisverifikations-VAU

Das ePA-Aktensystem MUSS sicherstellen, dass ein Befugnisverifikations-Modul ausschließlich in einem VAU-HSM oder in einer Befugnisverifikations-VAU ausgeführt wird. [≤]

A_25050 - ePA-Aktensystem - 1:1-Beziehung zwischen Befugnisverifikations-VAU und Aktenkontoverwaltungs-VAU

Das ePA-Aktensystem MUSS sicherstellen, dass eine 1:1-Beziehung zwischen einer Instanz einer Befugnisverifikations-VAU und einer Instanz einer Aktenkontoverwaltungs-VAU gibt. [≤]

3.4.1 VAU-Token-Modul

Dieser Abschnitt enthält die Regeln zum Zugriff auf die Schlüssel im VAU-HSM. Diese werden von einem Befugnisverifikations-Modul genutzt.

A_24712-01 - ePA-Aktensystem - VAU-Token-Modul nur durch Befugnisverifikations-Modul oder Aktenkontoverwaltungs-VAU aufrufbar

Das ePA-Aktensystem MUSS sicherstellen, dass die Regeln hsm-r1 bis hsm-r3 des VAU-Token-Moduls ausschließlich von einem Befugnisverifikations-Modul und die Regeln hsm-r4 bis hsm-r7 ausschließlich von einer Aktenkontoverwaltungs-VAU aufgerufen werden. [≤]

A_25282-02 - ePA-Aktensystem - Regeln des VAU-Token-Moduls

Das VAU-Token-Modul MUSS die in Tabelle *Tab_AS_VAU-Token_Modul_Rules* definierten Regeln umsetzen. [≤]

Tabelle 6: Tab_AS_VAU-Token_Modul_Rules -Prüfregeln VAU Token

Regel	Beschreibung
hsm-r1	<p><i>Diese Regel dient zur Sicherung von Befugnissen und HSM-ID-Token mittels CMAC.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (optional) • Daten <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Daten gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen der Signatur(en)des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Falls die Prüfungen 1) - 3) erfolgreich waren, werden die übergebenen Daten mittels CMAC gesichert.</p>

Regel	Beschreibung
hsm-r2	<p><i>Diese Regel dient zur Ableitung der versichertenindividuellen Persistierungsschlüssel</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • KVNR • gewünschte Persistierungsschlüssel [Label für Datenpersistierungs-Masterkey und/oder Label für Befugnispersistierungs-Masterkey] • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • falls in Eingangsdaten angefordert: versichertenindividueller Befugnispersistierungsschlüssel • falls in Eingangsdaten angefordert: versichertenindividueller Datenpersistierungsschlüssel <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. ggf. prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Falls die Prüfungen 1) - 3) erfolgreich waren, wird der angeforderte versichertenindividuelle Befugnispersistierungsschlüssel und/oder versichertenindividuelle Datenpersistierungsschlüssel für die übergebene KVNR von den durch die Label identifizierten Masterkeys abgeleitet.</p>

Regel	Beschreibung
hsm-r3	<p><i>Diese Regel dient zur Nutzung des HMAC bzgl. VSDM-Prüfziffern der Version 1 oder der Entschlüsselung der VSDM-Prüfziffern der Version 2</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VAU-Attestierungstoken einer Befugnisverifikations-VAU (opt.) • Szenario VSDM-Prüfziffer Version 1 <ul style="list-style-type: none"> • Daten • Bezeichner des HMAC-Schlüssels • Szenario VSDM-Prüfziffer Version 2 <ul style="list-style-type: none"> • VSDM-Prüfziffer in Version 2 <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Szenario VSDM-Prüfziffer Version 1: HMAC der Daten mit dem symmetrischen Schlüssel, der zum übergebenen Bezeichner des HMAC-Schlüssels gehört • Szenario VSDM-Prüfziffer Version 2: innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) bei erfolgreicher Entschlüsselung <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen der Signatur(en) des(r) VAU-Attestierungstoken (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind 3. (opt.) prüfen, ob die im VAU-Attestierungstoken für die Befugnisverifikations-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Szenario VSDM-Prüfziffer Version 1: Falls die Prüfungen 1) - 3) erfolgreich waren, wird der HMAC mit dem gewünschten HMAC-Schlüssel über die Daten gebildet.</p> <p>Szenario VSDM-Prüfziffer Version 2: Falls die Prüfungen 1) - 3) erfolgreich waren, wird die VSDM-Prüfziffer gemäß den Prüfschritten 4. und 5. aus A_27279-* geprüft und entschlüsselt. Bei erfolgreicher Entschlüsselung der VSDM-Prüfziffer wird die innere Struktur der VSDM-Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) zurückgeliefert, ansonsten ein Fehler.</p>

Regel	Beschreibung
hsm-r4	<p><i>Diese Regel dient zur Nutzung der privaten Schlüssel der AUT-Identitäten der VAU</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • Challenge • [VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU] VAU-Attestierungstoken einer Befugnisverifikations-VAU] VAU-Attestierungstoken eines Service-VAU-Typs] <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Challenge signiert mit privatem Schlüssel der AUT-Identität • der Aktenkontoverwaltungs-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU übergeben wurde, • der Befugnisverifikations-VAU, falls in den Eingangsdaten ein VAU-Attestierungstoken einer Befugnisverifikations-VAU übergeben wurde, • des Service-VAU-Typs, falls in den Eingangsdaten ein VAU-Attestierungstoken des Service-VAU-Typs übergeben wurde. <p>Prüfschritte</p> <ol style="list-style-type: none"> 1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und zum VAU-Typ passt. <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, wird die übergebene Challenge mit dem privatem Schlüssel der zum VAU-Attestierungstoken gehörenden AUT-Identität signiert.</p>
hsm-r5	<p><i>Diese Regel dient zur Nutzung des privaten Schlüssels der ENC-Identität der VAU</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • verschlüsselte Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • entschlüsselte Daten <p>Prüfschritte</p> <ol style="list-style-type: none"> 1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind. <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen verschlüsselten Daten mit dem privatem Schlüssel der ENC-Identität der VAU entschlüsselt.</p>

Regel	Beschreibung
hsm-r6	<p><i>Diese Regel dient zur Nutzung des privaten Schlüssels der Signaturidentität der VAU</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • zu signierende Daten • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • signierte Daten <p>Prüfschritte</p> <ol style="list-style-type: none"> 1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Falls die Prüfungen in 1) bis 2) erfolgreich waren, werden die übergebenen Daten mit dem privatem Schlüssel der Signaturidentität der VAU signiert.</p>
hsm-r7	<p><i>Diese Regel dient zum Auslesen des ENC-Zertifikats des anderen Aktensystembetreibers.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Verschlüsselungszertifikat C.FD.ENC des anderen Aktensystembetreibers <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch) 2. prüfen, ob die im VAU-Attestierungstoken für die Aktenkontoverwaltungs-VAU attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind <p>Falls die Prüfungen 1) - 2) erfolgreich waren, wird das ENC-Zertifikat des anderen Aktensystembetreibers zurückgeliefert.</p>

Regel	Beschreibung
hsm-r8	<p>Diese Regel dient zum Ableiten von symmetrischen Schlüsseln für die Ver- bzw. Entschlüsselung von Daten</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • <i>VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder einer Service-VAU</i> • <i>Ableitungsvektor dv</i> • <i>Label für Masterkey (opt.)</i> <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • <i>symmetrischer Schlüssel $symKey$</i> • <i>Label für Befugnis-Masterkey</i> <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. <i>prüfen der Signatur des VAU-Attestierungstokens (herstellerspezifisch)</i> 2. <i>prüfen, ob die im VAU-Attestierungstoken attestierte VAU-Software und VAU-Hardware dem HSM bekannt sind und es sich um die Attestierung einer Aktenkontoverwaltungs-VAU oder Service-VAU handelt</i> 3. <i>falls ein Label für einen Masterkey In den Eingangsdaten enthalten ist, prüfen, ob das Label zu einem Befugnis-Masterkey gehört</i> <p>Falls alle Prüfungen erfolgreich waren, wird $symKey$ wie folgt abgeleitet:</p> <p>Fall: Eingangsdaten enthalten ein Label $mkey_label$ für einen Befugnis-Masterkey: Ableitung eines AES-Schlüssels [FIPS-197] $symKey$ mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#2.4] zulässigen Verfahren auf Basis des Befugnis-Masterkeys mit Label $mkey_label$ und dem Ableitungsvektor "eds: "+ dv. Ausgangsdaten sind der abgeleitete Schlüssel $symKey$ und das Label $mkey_label$.</p> <p>(Verständnishinweis: eds steht für "External Data Storage". Das HSM erzwingt bei dieser Regeln, dass das Präfix "eds: " (also 5 Byte) dem vom Aufrufer übergebenen Ableitungsvektor (dv) vorangestellt wird.)</p> <p>Fall: Eingangsdaten enthalten kein Label für einen Befugnis-Masterkey: Ableitung eines AES-Schlüssels [FIPS-197] $symKey$ mit 256 Bit Schlüssellänge nach einem in [gemSpec_Krypt#Abschnitt 2.4] zulässigen Verfahren auf Basis des aktuellen Befugnis-Masterkeys und dem Ableitungsvektor "eds: " + dv. Ausgangsdaten sind der abgeleitete Schlüssel $symKey$ und das Label des aktuellen Befugnis-Masterkeys.</p>

A_24667 - ePA-Aktensystem -VAU-HSM - Prüfen des VAU-Attestierungstokens

Das VAU-HSM MUSS bei der Prüfung eines VAU-Attestierungstokens sicherstellen, dass dieses zeitlich gültig ist und Replay-Attacken abwehren. [<=]

A_26303 - ePA-Aktensystem - Abgeleitete Verschlüsselungsschlüssel sind ausschließlich einer VAU zugänglich

Das ePA-Aktensystem MUSS sicherstellen, dass ein mit Regel hsm-r8 abgeleiteter Schlüssel ausschließlich einer VAU zugänglich ist und ausschließlich mittels AES/GCM analog [gemSpec_Krypt#GS-A_4389] verwendet wird.[<=]

3.4.2 Regeln des Befugnisverifikations-Moduls

Die folgende Tabelle zeigt die Regeln des Befugnisverifikations-Moduls im Überblick.

Tabelle 7: Überblick über die Regeln des Befugnisverifikations-Moduls

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
rr0	Mit dieser Regel werden ID-Token im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr1	Mit dieser Regel werden vom Aktenkontoinhaber am ePA-FdV erstellte Befugnisse im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signatordienst signiert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr2	Mit dieser Regel werden vom Vertreter am ePA-FdV erstellte Befugnisse für das Aktenkonto des Versicherten im Aktensystem registriert. Die im ePA-FdV erstellen Befugnisse sind vom Vertreter mittels Signatordienst signiert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr3	Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das Stecken der eGK in einer Leistungserbringerumgebung ergeben.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr4	Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der Anlage eines Aktenkontos im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
rr5	Mit dieser Regel werden die Befugnisse bei einem betreiberübergreifenden Anbieterwechsel im Aktensystem registriert.	<i>Tab_AS_Entitlement_Registration_Rules</i>
kr1	Diese Regel wird für die Anmeldung des Aktenkontoinhabers genutzt.	<i>Tab_AS_SDS-Key_Rules</i>

Regel	Kurzbeschreibung	Vollständige Regelspezifikation in
kr2	Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	<i>Tab_AS_SDS-Key_Rules</i>
kr3	Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.	<i>Tab_AS_SDS-Key_Rules</i>
kr4	Diese Regel wird für die Anmeldung des E-Rezept-Fachdienstes verwendet.	<i>Tab_AS_SDS-Key_Rules</i>
kr5	Diese Regel wird für die Überschlüsselung (ggf. mit Umschlüsselung einer Überschlüsselung) verwendet.	<i>Tab_AS_SDS-Key_Rules</i>

A_24573-03 - ePA-Aktensystem - Regeln des Befugnisverifikations-Moduls

Das Befugnisverifikations-Modul MUSS die in den Tabellen *Tab_AS_Entitlement_Registration_Rules* und *Tab_AS_SDS-Key_Rules* definierten Regeln umsetzen. [<=]

Tabelle 8: Tab_AS_Entitlement_Registration_Rules - Regeln zur Registrierung von Befugnissen

Regel	Beschreibung
rr0	<p>Mit dieser Regel werden ID-Token im Aktensystem registriert und zu einem HSM-ID-Token konvertiert.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token mit NutzerID=x signiert durch einen sektoralen Identity Provider, den IDP-Dienst oder den E-Rezept-Fachdienst <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • HSM-ID-Token mit NutzerID=x gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (C.FD.SIG) bei Token eines IDPs bzw. gemäß A_24658-* bei Token des E-Rezept-Fachdiensts (C.FD.AUT). 2. Falls die Prüfung in 1) erfolgreich war, <ol style="list-style-type: none"> a. erstellt das Befugnisverifikations-Modul ein HSM-ID-Token mit der NutzerID=x, einer Gültigkeitsdauer von 24 Stunden und der professionOID aus dem Signaturzertifikat (oid_idpd_sek, oid_idpd oder oid_erp-vau). b. ruft das Befugnisverifikations-Modul die VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und dem HSM-ID-Token auf. <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert das mittels CMAC gesicherte HSM-ID-Token als Ergebnis des Regelaufrufs zurück.

rr1	<p><i>Mit dieser Regel werden vom Aktenkontoinhaber am ePA-FdV erstellte Befugnisse im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Versicherten mittels Signaturdienst signiert.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Befugnis1 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) signiert vom Versicherten <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis2 = (KVNR Aktenkonto, Telematik-ID oder KVNR, Gültigkeitszeitraum) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt <p>oder prüfen des HSM-ID-Tokens</p> <ol style="list-style-type: none"> c. Aufruf der VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. d. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt. 2. prüfen der Befugnis1 <ol style="list-style-type: none"> a. prüfen der Signatur gemäß A_25042-* (Zertifikatsprofil C.CH.SIG) b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_versicherter</code> ist c. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der "KVNR Aktenkonto" in der Befugnis1 übereinstimmt. d. prüfen, dass das JWT gemäß A_24587-* zeitlich gültig ist ($iat - 15s \leq \text{aktuelle Zeit} \leq exp + 15s$) 3. Falls die Prüfungen in 1) bis 2) erfolgreich waren, erstellt das Befugnisverifikations-Modul die Befugnis2. Die Inhalte werden aus Befugnis1 übernommen mit folgender Ausnahme:
-----	---

Regel	Beschreibung
	<p>Für eine Befugnis1 mit oid = oid_ncpeh wird die Gültigkeit validTo in Befugnis2 auf aktuelle Zeit + 1 Stunde gesetzt.</p> <ol style="list-style-type: none">4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis2<ol style="list-style-type: none">a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

rr2	<p><i>Mit dieser Regel werden vom Vertreter am ePA-FdV erstellte Befugnisse für das Aktenkonto des Versicherten im Aktensystem registriert. Die im ePA-FdV erstellten Befugnisse sind vom Vertreter mittels Signaturdienst signiert.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Befugnis1 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) signiert vom Vertreter • Befugnis2 = (KVNR Aktenkonto, KVNR Vertreter) gesichert mittels CMAC <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis3 = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist b. prüfen, ob die KVNR im ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt oder prüfen des HSM-ID-Tokens <ol style="list-style-type: none"> c. Aufruf der VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und HSM-ID-Token und Vergleich des Rückgabewerts mit dem CMAC des übergebenen HSM-ID-Tokens <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. d. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist e. prüfen, ob die KVNR im HSM-ID-Token mit der KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 übereinstimmt. 2. prüfen der Befugnis1 und Befugnis2 <ol style="list-style-type: none"> a. prüfen der Signatur von Befugnis1 gemäß A_25042-* (Zertifikatsprofil C.CH.SIG) b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_versicherter</code> ist c. prüfen des CMAC von Befugnis2 d. prüfen, dass die Telematik-ID in Befugnis 1 keine KVNR ist (Vertreter dürfen keine weiteren Vertreter befugen) e. prüfen, ob die KVNR im Signaturzertifikat C.CH.SIG der Signatur von Befugnis1 mit der „KVNR Vertreter“ in der Befugnis2 übereinstimmt
-----	--

Regel	Beschreibung
	<ul style="list-style-type: none"> f. prüfen, ob die „KVNR Aktenkonto“ in Befugnis 1 mit der „KVNR Aktenkonto“ in Befugnis2 übereinstimmt g. prüfen, dass das JWT gemäß A_24587-* zeitlich gültig ist ($i_{at} - 15s \leq \text{aktuelle Zeit} \leq e_{exp} + 15s$) <ol style="list-style-type: none"> 3. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis3 vom Befugnisverifikations-Modul erstellt. Die Inhalte werden aus Befugnis1 übernommen. 4. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und Befugnis3 <ul style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 5. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis3 als Ergebnis des Regelaufrufs zurück.

rr3	<p>Mit dieser Regel werden Befugnisse im Aktensystem registriert, die sich durch das Stecken der eGK in einer Leistungserbringenumgebung ergeben.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • VSDM-Prüfziffer in Version 1 oder 2 signiert mit AUT-Identität der SMC-B <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis = (KVNR Aktenkonto, Telematik-ID, Gültigkeitszeitraum) gesichert mittels CMA • falls VSDM-Prüfziffer in Version 2, zusätzlich die innere Struktur der Prüfziffer im Klartext gemäß A_27278-* (I_Feld_1, r_iat_8, KVNR) <p>Prüfschritte: <u>Prüfen, ob die übergebene VSDM-Prüfziffer eine Version 1 oder Version 2 ist:</u> Führe für die VSDM-Prüfziffer die Prüfschritte 1. und 2. gemäß A_27279-* durch. Es ergibt sich die dekodierte VSD-Prüfziffer, an der man am Most-significant-Bit erkennt, ob es sich um Version 1 oder Version 2 der Prüfziffer handelt.</p> <p><u>Szenario VSDM-Prüfziffer in Version 1:</u></p> <ol style="list-style-type: none"> 1. prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A_25042-* (C.HCI.AUT) 2. Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert. 3. prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer nicht länger als 20 Minuten zurückliegt mit prüfziffer.timestamp - 30s <= aktuelle Zeit < prüfziffer.timestamp + 20 Minuten +15s) 4. prüfen des HMAC der VSDM-Prüfziffer mittels VAU-HSM Regel hsm-r3 <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 5. Falls die Prüfungen in 1) bis 4) erfolgreich waren, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt: <ul style="list-style-type: none"> • Aktenkonto: die KVNR aus dem VSDM-Prüfziffer • Telematik-ID: die Telematik-ID aus der SMC-B-Signatur • Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur. 6. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.
-----	---

Regel	Beschreibung
	<p>7. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis als Ergebnis des Regelaufrufs zurück.</p> <p><u>Szenario VSDM-Prüfziffer in Version 2:</u></p> <ol style="list-style-type: none"> prüfen der SMC-B-Signatur der signierten VSDM-Prüfziffer gemäß A_25042-* (C.HCI.AUT) Hinweis: ein im JWT evtl. vorhandener iat-Wert bzw. exp-Wert wird ignoriert. Aufruf von VAU-HSM Regel hsm-r3 mit der dekodierten VSDM-Prüfziffer <ol style="list-style-type: none"> Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. prüfen der inneren Struktur nach Prüfschritt 6 gemäß A_27279-* (d.h. eGK ist nicht gesperrt) prüfen, dass der Ausstellungszeitpunkt der VSDM-Prüfziffer (prüfziffer.iat) nicht länger als 20 Minuten zurückliegt (prüfziffer.iat - 30s <= aktuelle Zeit < prüfziffer.iat + 20 Minuten + 15s, Hinweis in der Prüfziffer gibt es kein exp, deshalb wird im Vergleich explizit 20 Minuten + 15 Sekunden angegeben) prüfen des prüfziffer.hcv nach Prüfschritt 8 gemäß A_27279-* bzgl. des hcv im JWT Falls die Prüfungen in 1) bis 6) erfolgreich waren, und die VAU-HSM Regel hsm-r3 den Klartext der inneren Struktur der Prüfziffer zurückgeliefert hat, wird vom Befugnisverifikations-Modul die Befugnis mit folgenden Inhalten erstellt: <ul style="list-style-type: none"> Aktenkonto: KVNR, die als Ergebnis der VAU-HSM Regel hsm-r3 zurückgeliefert wird Telematik-ID: die Telematik-ID aus der SMC-B-Signatur Gültigkeitszeitraum: ergibt sich aus der fachlichen Rollen-OID der SMC-B-Signatur. Aufruf der VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis <ol style="list-style-type: none"> Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis sowie die entschlüsselte innere Struktur der Prüfziffer im Klartext gemäß A_27278-* als Ergebnis des Regelaufrufs zurück.

Regel	Beschreibung
rr4	<p><i>Mit dieser Regel werden die Befugnisse für den Kostenträger und die zuständige Ombudsstelle bei der Anlage eines Aktenkontos im Aktensystem registriert.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • Befugnis1 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) signiert mit SMC-B des Kostenträgers bzw. der Ombudsstelle <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Befugnis2 = (KVNR Aktenkonto, Telematik-ID des Kostenträgers/der Ombudsstelle) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Prüfen der Befugnis1 <ol style="list-style-type: none"> a. prüfen der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle gemäß A_25042-* (C.HCI.OSIG) b. prüfen, ob die professionOID im Signaturzertifikat <code>oid_kostentraeger</code> bzw. <code>oid_ombudsstelle</code> ist c. prüfen, ob die Telematik-ID im Signaturzertifikat C.HCI.OSIG der SMC-B-Signatur des Kostenträgers bzw. der Ombudsstelle mit der Telematik-ID in der Befugnis1 übereinstimmt 2. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 erstellt. Die Inhalte der Befugnis2 sind: <ul style="list-style-type: none"> • Aktenkonto: die KVNR des Aktenkontos aus Befugnis1 • Telematik-ID: die Telematik-ID aus Befugnis1 3. Aufruf der VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 4. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

Regel	Beschreibung
rr5	<p>Mit dieser Regel werden die Befugnisse bei einem betreiberübergreifenden Anbieterwechsel im Aktensystem registriert.</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU Befugnis1 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) signiert vom alten Aktensystembetreiber <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> Befugnis2 = (KVNR Aktenkonto, NutzerID, Gültigkeitszeitraum) gesichert mittels CMAC <p>Prüfschritte:</p> <ol style="list-style-type: none"> Prüfen der Befugnis1 <ol style="list-style-type: none"> prüfen der Signatur gemäß A_25042-* (C.FD.SIG) prüfen, ob im Signaturzertifikat C.FD.SIG der policyIdentifier <code>oid_epa_vau</code> ist prüfen, dass das Signaturzertifikat C.FD.SIG nicht auf das importierende Aktensystem ausgestellt ist. Falls die Prüfungen in 1) erfolgreich waren, wird die Befugnis2 mit den Inhalten aus Befugnis1 erstellt. Aufruf der VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung und der erstellten Befugnis2 <ol style="list-style-type: none"> Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. Das Befugnisverifikations-Modul liefert die mittels CMAC gesicherte Befugnis2 als Ergebnis des Regelaufrufs zurück.

A_24690-01 - ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen des ID-Tokens

Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung eines ID-Tokens durchführen:

- das ID-Token muss gemäß A_25042-* valide signiert sein durch einen sektoralen Identity Provider oder den IDP-Dienst (professionOID ist `oid_idpd_sek` oder `oid_idpd`),
- das ID-Token muss zeitlich gültig sein (Felder: `iat`, `exp`),
- das ID-Token muss im Feld `aud` das ePA-Aktensystem eingetragen haben.

[<=]

A_24691 - ePA-Aktensystem - Befugnisverifikations-Modul: Prüfen von übers ePA-FdV erstellten Befugnissen

Das Befugnisverifikations-Modul MUSS folgende Prüfungen bei der Prüfung einer von einem Versicherten bzw. Vertreter über das ePA-FdV eingestellten signierten Befugnis durchführen:

- die Befugnis muss gemäß A_25042-* valide signiert sein durch einen Versicherten bzw. Vertreter (C.CH.SIG, professionOID ist `oid_versicherter`),
- das JWT für die Befugnis gemäß A_24587-* darf nicht abgelaufen sein (Feld: `exp`),
- das Feld `insurantID` des JWT muss eine KVNR sein,
- das Feld `actorID` des JWT muss eine KVNR oder eine Telematik-ID sein,
- das Feld `validTO` des JWT muss ein zeitliches Datum sein.

[<=]

Die folgenden Regeln dienen zum Abruf der versichertenindividuellen Daten- und Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel und die Ableitungsvorschriften sind in [gemSpec_Krypt] in Abschnitt 3.15.2 festgelegt.

Tabelle 9: Tab_AS_SDS-Key_Rules Key Rules - Regeln zur Ableitung der versichertenindividuellen Persistierungsschlüssel

Regel	Beschreibung
kr1	<p><i>Diese Regel wird für die Anmeldung des Aktenkontoinhabers genutzt.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren). • Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll (ggf. besonderes Symbol "<current>" für jüngsten im VAU-HSM verfügbaren). • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys • versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys <p>Regelverhalten:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) <ol style="list-style-type: none"> a. prüfen, ob die professionOID im Signaturzertifikat <code>oid_idpd_sek</code> ist oder prüfen des HSM-ID-Tokens b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. c. prüfen, ob die professionOID im HSM-ID-Token <code>oid_idpd_sek</code> ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel <code>hsm-r2</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVN-R aus dem ID-Token und den Labeln der zu verwendenden Befugnispersistierungs- und Datenpersistierungs-Masterkeys zur Ableitung von Befugnis- und Datenpersistierungsschlüssel aufgerufen. <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert die abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.

Regel	Beschreibung
kr2	<p><i>Diese Regel wird für den Abruf des versichertenindividuellen Befugnispersistierungsschlüssel genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • KVNR (Aktenkonten-ID) • Label Befugnispersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Befugnispersistierungsschlüssel (SecureAdminStorageKey) + Label des verwendeten Masterkeys • ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Aufruf der VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR und dem Label des Befugnispersistierungs-Masterkeys zur Ableitung des Befugnispersistierungsschlüssels <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 2. Das Befugnisverifikations-Modul liefert den abgeleiteten Befugnispersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.

kr3	<p><i>Diese Regel wird für den Abruf des versichertenindividuellen Datenpersistierungsschlüssels genutzt. Sie wird für die Anmeldung von Nutzern verwendet, für die eine Befugnis im Aktensystem registriert wurde.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • Befugnis = (KVNR Aktenkonto, BefugtenID (TID KVNR), Gültigkeitszeitraum (opt.)) mit CMAC gesichert • Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys • ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. prüfen des ID-Tokens <ol style="list-style-type: none"> a. gemäß A_24690-* (Zertifikatsprofil C.FD.SIG) oder prüfen des HSM-ID-Tokens <ol style="list-style-type: none"> b. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel hsm-r1 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 2. Prüfen der Befugnis <ol style="list-style-type: none"> a. prüfen des CMAC der Befugnis mittels VAU-HSM Regel hsm-r1 <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. b. prüfen, ob dieNutzer-ID im ID-Token bzw. im HSM-ID-Token (KVNR oder Telematik-ID) mit der Befugten-ID in der Befugnis übereinstimmt. c. prüfen, ob die Befugnis noch gültig ist, falls die Befugnis zeitlich begrenzt ist (d. h. ein Gültigkeitszeitraum in der Befugnis enthalten ist). 3. Falls alle Prüfungen in 1) bis 2) erfolgreich waren, wird die VAU-HSM Zugriffsregel hsm-r2 mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR aus dem ID-Tokenbzw. im HSM-ID-
-----	--

Regel	Beschreibung
	<p>Token und dem Label für den Datenpersistierungs-Masterkey zur Ableitung des Datenpersistierungsschlüssels aufgerufen.</p> <p>a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben.</p> <p>4. Das Befugnisverifikations-Modul liefert den abgeleiteten Datenpersistierungsschlüssel als Ergebnis des Regelaufrufs zurück.</p>

Regel	Beschreibung
kr4	<p><i>Diese Regel wird für die Anmeldung des E-Rezept-Fachdienstes verwendet.</i></p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU • ID-Token oder HSM-ID-Token gesichert mit CMAC • KVNR (Aktenkonten-ID) • Label Datenpersistierungs-Masterkey der die Grundlage der Schlüsselableitung sein soll • ggf. Label Überschlüsselungs-Masterkey der die Grundlage der Schlüsselableitung sein soll <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • versichertenindividueller Datenpersistierungsschlüssel (Secure Data Storage Key) + Label des verwendeten Masterkeys • ggf. versichertenindividueller Überschlüsselungsschlüssel + Label des verwendeten Masterkeys <p>Prüfschritte:</p> <ol style="list-style-type: none"> 1. Prüfen des ID-Tokens <ol style="list-style-type: none"> a. prüfen der Signaturgemäß A_25042-* (C.FD.AUT) b. prüfen, ob die professionOID im Zertifikat C.FD.AUT gleich <code>oid_erp-vau</code> ist c. prüfen des ID-Tokens gemäß A_24658-* oder prüfen des HSM-ID-Tokens d. prüfen des CMAC des HSM-ID-Tokens mit VAU-HSM Zugriffsregel <code>hsm-r1</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung <ol style="list-style-type: none"> i. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. e. prüfen, ob die professionOID im HSM-ID-Token <code>oid_erp-vau</code> ist 2. Falls die Prüfungen in 1) erfolgreich waren, wird die VAU-HSM Zugriffsregel <code>hsm-r2</code> mit dem VAU-Attestierungstoken der Aktenkontoverwaltung, der KVNR aus dem ID-Token bzw. dem HSM-ID-Token und dem Label für den Datenpersistierungs-Masterkey zur Ableitung des Datenpersistierungsschlüssels aufgerufen. <ol style="list-style-type: none"> a. Falls das Befugnisverifikations-Modul in einer Befugnisverifikations-VAU ausgeführt wird, wird zusätzlich ein VAU-Attestierungstoken für die Befugnisverifikations-VAU mit übergeben. 3. Das Befugnisverifikations-Modul liefert den abgeleiteten Schlüssel als Ergebnis des Regelaufrufs zurück.

Regel	Beschreibung
kr5	<p>Diese Regel wird für die Überschlüsselung verwendet (ggf. mit Umschlüsselung einer Überschlüsselung).</p> <p>Diese Regel kann von einer VAU (AK-VAU oder dedizierte Überschlüsselungs-VAU) verwendet werden um verschlüsselte Akten zu überschlüsseln (vgl. Abschnitt 3.6- Umschlüsselung und Überschlüsselung). Dabei kann es auch zu einer Umschlüsselung einer älteren Überschlüsselung kommen.</p> <p>Sei <current> ein spezielles Symbol was im VAU-HSM durch das Label des jüngsten Überschlüsselungsschlüssel ersetzt wird. Ein Aufruf braucht so das tatsächliche Label nicht zu kennen. (Der Hersteller ist frei "<current>" durch ein selbstgewählten Symbolnamen zu ersetzen.)</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> • VAU-Attestierungstoken einer Aktenkontoverwaltungs-VAU oder ggf. einer dedizierten Überschlüsselungs-VAU • KVNR (Aktenkonten-ID) • Labelliste: nicht leere Liste von Label-n von Überschlüsselungs-Masterkeys (im Regelfall enthält die Liste mindestens "<current>" als Element) <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> • Liste von Paaren: versichertenindividueller Überschlüsselungsschlüssel (Secure Data Storage Key), Label für verwendeten Überschlüsselungs-Masterkey <p>(Hinweis: Die Liste enthält mindestens ein Element -- im Fall der ersten Überschlüsselung in Intervall 2 (vgl. Abschnitt 3.6))</p> <p>Ablauf:</p> <p>Das VAU-HSM muss des VAU-Attestierungstoken prüfen, ob es sich um eine AK-VAU oder dedizierte Überschlüsselungs-VAU handelt. Falls nein, Abbruch.</p> <p>Das VAU-HSM durchläuft die Label-Liste und führt mit dem entsprechenden Label verbundenen Überschlüsselungs-Masterkey und der KVNR eine Schlüsselableitung durch. Dabei wird im VAU-HSM das spezielle Symbol "<current>" durch das Label des jüngsten Überschlüsselungs-Masterkeys vor Abarbeitung ersetzt.</p> <p>In der Ergebnisse (siehe Ausgangsdaten) ist "<current>" ebenfalls so ersetzt. Die Reihenfolge in der Eingangsliste muss in der Ausgabeliste gleich bleiben.</p>

3.5 Vertrauenswürdige Ausführungsumgebung (VAU)

Eine Vertrauenswürdige Ausführungsumgebung (VAU) gewährleistet mit technischen Maßnahmen, dass Daten serverseitig im ePA-Aktensystem im Klartext verarbeitet werden können, ohne dass einzelne Mitarbeiter des Betreibers auf diese Daten zugreifen können.

Die Datenverarbeitungen der Aktenkontoverwaltung müssen in einer VAU ausgeführt werden. Diese VAU wird im folgenden als Aktenkontoverwaltungs-VAU bezeichnet. Des weiteren kann das Befugnisverifikations-Modul in einer VAU ausgeführt werden. Diese VAU wird im folgenden als Befugnisverifikations-VAU bezeichnet.

A_25716-01 - ePA-Aktensystem - Services ausschließlich in der VAU

Das ePA-Aktensystem MUSS sicherstellen, dass die folgenden Services ausschließlich innerhalb einer VAU ausgeführt werden können und ein Zugriff auf die Schnittstellen ausschließlich über einen VAU-Kanal erfolgen kann:

- Consent Decision Management Service
- Entitlement Management
- Constraint Management
- Device Management
- E-Mail Management
- Audit Event Service
- Authorization Service
- Health Record Relocation Service
- alle Medical Services
- Data Submission Service.

[<=]

In den folgenden Abschnitten werden zunächst die Anforderungen an eine VAU beschrieben, die sowohl von einer Aktenkontoverwaltungs-VAU als auch einer Befugnisverifikations-VAU zu erfüllen sind. Die speziellen Anforderungen an eine Aktenkontoverwaltungs-VAU bzw. an eine Befugnisverifikations-VAU folgen darauf in separaten Abschnitten.

3.5.1 Übergreifende VAU-Anforderungen

3.5.1.1 Schutz der Integrität der VAU

Die folgenden Anforderungen stellen die Integrität der VAU sicher.

A_24613 - ePA-Aktensystem - Bildung Hashwertrepräsentation des VAU-Images

Der Hersteller des VAU-Images MUSS für seine zugelassenen VAU-Images Hashwertrepräsentationen bilden. Diese MÜSSEN signiert und die signierten Hashwertrepräsentationen an die gematik übermitteln. Dabei SOLLEN bezüglich der kryptographischen Vorgaben zur Signatur die Vorgaben aus [gemSpec_Krypt] eingehalten werden.[<=]

Erläuterung zu A_24613-*:

Bei Intel-SGX sind die durch die Intel-Hardware erzeugten Signaturen RSA-3072-Bit-Signaturen, bei denen der öffentliche Exponent 3 ist. Dies entspricht nicht den Vorgaben in [gemSpec_Krypt] für allgemeine RSA-Signaturen (also nicht im SGX-Kontext). Deshalb steht in A_24613-* diesbezüglich nur eine SOLL-Formulierung. Im Kontext SGX ist der öffentliche RSA-Exponent 3 zulässig.

A_24642 - ePA-Aktensystem - Ausschluss von Manipulationen an der Hardware der VAU

Die VAU MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Betreiber des ePA-Aktensystems ausschließen. [≤]

A_24616 - ePA-Aktensystem - Attestierung des VAU-Images und der VAU-Hardware beim Start

Das ePA-Aktensystem MUSS beim Start einer VAU das genutzte VAU-Image sowie die VAU-Hardware, auf der die VAU ausgeführt werden soll, kryptographisch attestieren und ein signiertes VAU-Attestierungstoken erzeugen, welches vom VAU-HSM geprüft werden kann. [≤]

A_24684 - ePA-Aktensystem - Hardwarebasierter Vertrauensanker für Attestierung der VAU

Das ePA-Aktensystem MUSS sicherstellen, dass der kryptographische Vertrauensanker für die Attestierung des VAU-Images und der VAU-Hardware in einem hardwarebasierten sicheren Schlüsselspeicher gesichert ist. [≤]

A_24617 - ePA-Aktensystem - Betreiberunabhängiger Vertrauensanker für Attestierung der VAU

Das ePA-Aktensystem MUSS sicherstellen, dass der kryptographische Vertrauensanker für die Attestierung des VAU-Images und der VAU-Hardware nicht in der Hoheit des Betreibers des Aktensystems liegt. [≤]

Hinweis zu A_24617: Mit der Anforderung soll die Bedrohung abgewehrt werden, dass sich einzelne Innentäter beim Betreiber des ePA-Aktensystems eigene VAU-Software oder VAU-Hardware mit Schwachstellen erstellen und sich für diese einen falschen Hashwert attestieren, der dem VAU-HSM bekannt ist.

A_24620 - ePA-Aktensystem - Attestierung durch Systeme außerhalb der VAU zur Laufzeit

Das ePA-Aktensystem MUSS technisch ermöglichen, dass Änderungen an der VAU-Software und der VAU-Hardware während der Laufzeit durch Systeme außerhalb der VAU automatisiert geprüft werden können. [≤]

Hinweis: Die gematik soll regelmäßig die Integrität der Aktensysteme prüfen können.

3.5.1.2 Schutz der Daten bei Verarbeitung in der VAU

Die folgenden Anforderungen der VAU stellen sicher, dass die innerhalb der VAU verarbeiteten Daten technisch geschützt werden.

A_24621 - ePA-Aktensystem - Äußere Isolation der VAU von Datenverarbeitungsprozessen des Betreibers

Die VAU MUSS die in ihr ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Betreibers technisch trennen und damit gewährleisten, dass der einzelne Mitarbeiter des Betreibers vom Zugriff auf die in der VAU verarbeiteten Daten technisch ausgeschlossen ist. [≤]

A_24638 - ePA-Aktensystem - Schutz der Daten vor physischem Zugang zu Systemen der VAU

Die VAU MUSS mit technischen Mitteln sicherstellen, dass bei einem physischen Zugang zu Hardware-Komponenten der VAU keine Daten aus der VAU extrahiert oder manipuliert werden können. [≤]

A_24651 - ePA-Aktensystem - Betreiber ergreift Maßnahmen gegen physische Angriffe auf die VAU

Der Betreiber des ePA-Aktensystems MUSS mit technischen und/oder organisatorischen Maßnahmen ausschließen, dass ein einzelner Innentäter beim Betreiber des ePA-Aktensystems physische Angriffe auf eine VAU ausführen kann. [≤]

A_24641 - ePA-Aktensystem - Löschen aller Daten beim Beenden einer VAU-Instanz

Das ePA-Aktensystem MUSS sicherstellen, dass beim Beenden einer VAU-Instanz sämtliche Daten dieser VAU-Instanz aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [≤]

A_25244 - ePA-Aktensystem - x-insurantId nicht außerhalb des VAU-Kanals

Das ePA-Aktensystem MUSS sicherstellen, dass das HTTP Header-Element mit dem Namen "x-insurantId" nicht außerhalb des VAU-Kanals gesendet wird. [≤]

3.5.1.3 Schutz der Daten bei Speicherung außerhalb der VAU**A_26314 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Daten**

Das ePA-Aktensystem MUSS sicherstellen, dass eine VAU-Daten, die im System des Aktensystembetreibers gespeichert werden sollen und für die keine spezifischen Anforderungen zum Schutz der gespeicherten Daten existieren, ausschließlich verschlüsselt gespeichert werden und der verwendete Verschlüsselungsschlüssel mittels der Regel hsm-r8 vom VAU-HSM abgeleitet wird. [≤]

Hinweise zu A_26314:

- Spezifische Anforderungen zum Schutz der gespeicherten Daten gibt es z.B. für die Aktenkontoverwaltungs-VAU in Abschnitt 3.5.2.2 und die durch die VAU für den Betrieb erstellten Protokolle in Abschnitt 3.5.1.5.
- Außerhalb der VAU verschlüsselt gespeicherte Daten der ePA3.0, die bisher nicht mit Regel hsm-r8 verschlüsselt sein konnten, sind beim Öffnen der Akte umzuschlüsseln und mit einem Schlüssel zu sichern, der mit Regel hsm-r8 abgeleitet wird. Eine Umschlüsselung ohne Öffnen der Akte ist nicht erforderlich.

A_26322 - ePA-Aktensystem - Unterschiedliche Schlüssel für die Verschlüsselung von außerhalb der VAU gespeicherten Daten bei unterschiedlichen Verarbeitungszwecken

Falls Daten außerhalb der VAU im System des Aktensystembetreibers gespeichert werden, MUSS das ePA-Aktensystem sicherstellen, dass für die Verschlüsselung von Daten, die zu unterschiedlichen Zwecken verarbeitet werden, unterschiedliche Verschlüsselungsschlüssel genutzt werden. [≤]

Hinweis zu A_26322: Verarbeitungszwecke für Daten ist beispielsweise die Verarbeitung von Daten für die Nutzerverwaltung im Aktensystem (insbesondere Geräteinformationen und E-Mail-Adressen).

3.5.1.4 Schutz der Verbindung zwischen VAU und VAU-HSM**A_24653 - ePA-Aktensystem - Sichere Verbindung zwischen VAU und VAU-HSM**

Das ePA-Aktensystem MUSS technisch sicherstellen, dass zwischen einer VAU und einem VAU-HSM eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen. [≤]

3.5.1.5 Logging und Monitoring

Hinweis: Die Anforderungen dieses Abschnitts könnten sich noch ändern, falls sich bei der Umsetzung des ePA-Aktensystems herausstellt, dass weitere Protokollierungen auf Seiten des Betreibers notwendig werden.

A_24910 - ePA-Aktensystem - Erlaubte Zwecke der Betreiberprotokolle

Der Betreiber des Aktensystems MUSS sicherstellen, dass die durch die VAU für den Betrieb erstellten Protokolle des Betreibers ausschließlich zum Zwecke der Fehleranalyse und -behebung anlassbezogen sowie zum Zwecke des Security Monitorings verwendet werden. [≤]

A_24649 - ePA-Aktensystem - Datenschutzkonformes Logging und Monitoring der VAU

Die VAU MUSS die für den Betrieb des ePA-Aktensystems erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dem Betreiber des ePA-Aktensystems vertrauliche oder zur unautorisierten Profilbildung geeignete Daten zur Kenntnis gelangen. [≤]

A_24695 - ePA-Aktensystem - Keine medizinische Informationen in VAU-Protokollen des Betreibers

Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten Protokollen des Betreibers keine personenbezogenen medizinischen Informationen enthalten sind (u. a. medizinische Daten von Versicherten oder Informationen, aus denen sich ableiten lässt, bei welchen Leistungserbringerinstitutionen ein Versicherter in Behandlung ist).

[≤]

A_24909 - ePA-Aktensystem - Nicht KVNR und Telematik-ID gemeinsam protokollieren

Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten Protokollen des Betreibers höchstens die KVNR oder höchstens die Telematik-ID enthalten ist, aber nicht eine Kombination aus KVNR und Telematik-ID und keine solche Verbindung über mehrere Protokolle hergestellt werden kann. [≤]

A_24719 - ePA-Aktensystem - Kein kryptographisches Schlüsselmaterial in VAU-Protokollen des Betreibers

Die VAU MUSS sicherstellen, dass in den durch die VAU für den Betrieb erstellten Protokollen des Betreibers kein kryptographisches Schlüsselmaterial enthalten ist. [≤]

A_24911 - Löschfristen Protokolle

Das ePA-Aktensystem MUSS sicherstellen, dass die

- zum Zwecke der Fehleranalyse erhobenen Protokolle nach Behebung des Fehlers unverzüglich gelöscht werden,
- zum Zwecke des Security Monitorings erhobenen Protokolle nach 3 Monaten gelöscht werden.

[≤]

A_26316 - Anbieter ePA-Aktensystem - Schutz der Protokolle des Betreibers

Der Betreiber des ePA-Aktensystems MUSS sicherstellen, dass die durch die VAU für den Betrieb erstellten Protokolle des Betreibers durch technische und organisatorische Maßnahmen vor einer missbräuchlichen Nutzung geschützt werden. [≤]

gematik-Logdaten zum Zwecke der gesetzlichen Kontrollpflichten der gematik

Hinweis zu A_27336-*: Der geheime Schlüssel für die Pseudonymisierung muss nicht im VAU-HSM gespeichert werden.

A_27333 - ePA-Aktensystem - Geheimer Schlüssel für Pseudonymisierung der gematik-Logdaten nur in VAU

Das ePA-Aktensystem MUSS sicherstellen, dass der für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigte geheime Schlüssel `key_pn_log` im Klartext ausschließlich innerhalb einer VAU-Instanz verarbeitet wird. [≤]

A_27336 - ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung im 4-Augen-Prinzip

Das ePA-Aktensystem MUSS sicherstellen, dass der für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigte geheime Schlüssel `key_pn_log` ausschließlich im 4-Augen-Prinzip ins ePA-Aktensystem eingebracht werden kann. [\leq]

A_27334 - ePA-Aktensystem - Einbringen des Schlüssels für Pseudonymisierung der gematik-Logdaten im 4-Augen-Prinzip

Der Betreiber des ePA-Aktensystems MUSS den für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigten geheimen Schlüssel `key_pn_log` ausschließlich im 4-Augen-Prinzip mit der gematik ins ePA-Aktensystem einbringen. [\leq]

A_27335 - ePA-Aktensystem - Wechsel des Schlüssels für Pseudonymisierung der gematik-Logdaten

Der Betreiber des ePA-Aktensystems MUSS den für die Pseudonymisierung der Logdaten gemäß A_27332-* benötigten geheimen Schlüssel `key_pn_log` spätestens nach 1 Jahr wechseln. [\leq]

3.5.2 Zusätzliche Anforderungen an eine Aktenkontoverwaltungs-VAU**3.5.2.1 Schutz der Daten bei Verarbeitung in der Aktenkontoverwaltungs-VAU****A_24636 - ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen innerhalb einer VAU-Instanz**

Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus ausschließen, dass sich innerhalb einer VAU-Instanz die Verarbeitungen eines Health Record Context oder einer User Session schadhaft auf die Verarbeitungen eines anderen Health Record Context oder einer anderen User Session auswirken können. [\leq]

Hinweis zu A_24636-*: Die Anforderung schließt eine Umsetzung mit Server-Threads, Worker und Ähnlichem nicht grundsätzlich aus, sofern die Sicherheitsleistung der Separation erbracht werden kann.

A_24885 - ePA-Aktensystem - Innere Isolation zwischen Datenverarbeitungsprozessen unterschiedlicher VAU-Instanzen

Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der unabhängig vom Separationsmechanismus in A_24636-* ist, ausschließen, dass sich Verarbeitungen in einer VAU-Instanz schadhaft auf die Verarbeitungen einer anderen VAU-Instanz auswirken können. [\leq]

A_24637 - ePA-Aktensystem - Maximale Health Record Context in einer VAU-Instanz

Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Health Record Context gleichzeitig in einer VAU-Instanz laufen können. [\leq]

A_25028 - ePA-Aktensystem - Keine Kommunikation zwischen Aktenkontoverwaltungs-VAUs

Das ePA-Aktensystem MUSS sicherstellen, dass es keine direkte Kommunikation zwischen VAU-Instanzen von Aktenkontoverwaltungs-VAUs gibt. [\leq]

A_26111 - ePA-Aktensystem - Keine Kommunikation zwischen Health Record Contexts

Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer Aktenkontoverwaltungs-VAU-Instanz keine Kommunikation zwischen Health Record Contexts gibt. [≤]

A_24639 - ePA-Aktensystem - Löschen aller Daten beim Beenden eines Health Record Context

Die VAU MUSS sicherstellen, dass beim Beenden eines Health Record Context sämtliche Daten dieses Health Record Context aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [≤]

A_24640 - ePA-Aktensystem - Löschen aller Daten beim Beenden einer User Session

Die VAU MUSS sicherstellen, dass beim Beenden einer User Session sämtliche Daten dieser User Session aus flüchtigen Speichern sicher gelöscht werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist. [≤]

Hinweis zu A_24639-, A_24640-* und A_24648-*: Eine zeitliche Verzögerung des Löschens ist tolerabel, sofern ein sofortiges Löschen aufgrund der Architektur des Aktensystemherstellers aus Performanzgründen nicht sinnvoll ist. In diesem Fall ist ein geeigneter Kompromiss zwischen dem Löschzeitpunkt und der Performanz zu wählen.*

A_25231 - ePA-Aktensystem - Schließen des Health Record Context beim Beenden einer User Session

Die VAU MUSS sicherstellen, dass beim Beenden einer User Session alle mit dieser User Session verknüpften Health Record Context beendet werden, wenn der jeweilige Health Record Context nicht mit mindestens einer weiteren User Session verknüpft ist. [≤]

A_25051 - ePA-Aktensystem - VAU-Kanal endet immer in einer Aktenkontoverwaltungs-VAU

Die VAU MUSS sicherstellen, dass ein VAU-Kanal von einem Client der ePA (ePA-Client oder ePA-FdV) ausschließlich in einer Aktenkontoverwaltungs-VAU endet. [≤]

Hinweis: Der VAU-Kanal darf z.B. nicht in einer Befugnisverifikations-VAU enden.

3.5.2.2 Schutz der Daten bei Speicherung außerhalb der Aktenkontoverwaltungs-VAU

Die folgenden Anforderungen gewährleisten den Schutz der beim Betreiber des ePA-Aktensystems persistierten Daten von Aktenkonten. Die Verschlüsselung der Daten eines Versicherten erfolgt mit seinem versichertenindividuellen Daten- und Befugnispersistierungsschlüssel. Die kryptographischen Vorgaben für diese Schlüssel sind in [gemSpec_Krypt#3.15.2] festgelegt.

A_24643 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Daten mit dem Datenpersistierungsschlüssel

Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten

1. Daten des FHIR-Data Service
2. Daten des XDS Document Service
3. Daten des Audit Event Service (Protokolle für den Versicherten zum Zwecke der Datenschutzkontrolle)
4. Daten des Constraint Managements (Policies zu verborgenen Daten)
5. Daten des Consent Managements (Widersprüche des Versicherten)

vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health Record Context mit dem zum Health Record gehörenden versichertenindividuellen Datenpersistierungsschlüssel verschlüsselt werden.

[<=]

A_24644 - ePA-Aktensystem - Verschlüsselung von außerhalb der VAU gespeicherten Befugnissen mit dem Befugnispersistierungsschlüssel

Die VAU MUSS sicherstellen, dass die in einem Health Record Context verarbeiteten Daten des Entitlement Managements, d. h. Befugnisse und Befugnisverbote, vor der Speicherung in den Systemen des Betreibers des ePA-Aktensystems innerhalb des Health Record Context mit dem zum Health Record gehörenden versichertenindividuellen Befugnispersistierungsschlüssel verschlüsselt werden.[<=]

3.5.2.3 Konsistenz des Systemzustands

A_24650 - ePA-Aktensystem - Konsistenter Systemzustand eines Health Record Context

Die VAU MUSS sicherstellen, dass ein konsistenter Zustand eines Health Record Context auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw. wiederhergestellt werden kann.[<=]

A_24696 - ePA-Aktensystem - Konsistenz bei parallelen Zugriffen

Die VAU MUSS auch bei parallelen Zugriffen auf dasselbe Aktenkonto durch mehrere Nutzer immer einen konsistenten Zustand des Aktenkontos gewährleisten.[<=]

3.5.3 Zusätzliche Anforderungen an eine Befugnisverifikations-VAU

Eine Befugnisverifikations-VAU ist eine spezielle VAU, in der ausschließlich das Befugnisverifikations-Modul ausgeführt wird.

A_24646 - ePA-Aktensystem - Befugnisverifikations-VAU verarbeitet ausschließlich ein Befugnisverifikations-Modul

Das ePA-Aktensystem MUSS sicherstellen, dass in einer Befugnisverifikations-VAU ausschließlich ein Befugnisverifikations-Modul ausgeführt wird.[<=]

A_24647 - ePA-Aktensystem - Befugnisverifikations-VAU speichert keine Daten

Eine Befugnisverifikations-VAU DARF die Daten, die sie im Rahmen der Regeln des Befugnisverifikations-Moduls verarbeitet, NICHT außerhalb der Befugnisverifikations-VAU speichern.[<=]

Eine Befugnisverifikations-VAU darf insbesondere die vom VAU-HSM abgeleiteten versichertenindividuellen Persistierungsschlüssel nicht speichern.

A_24648 - ePA-Aktensystem - Befugnisverifikations-VAU löscht Daten nach Regelbearbeitung

Eine Befugnisverifikations-VAU MUSS sämtliche Daten, die sie im Rahmen eines Regelaufrufs des Befugnisverifikations-Moduls verarbeitet, sofort nach Abarbeitung der Regel sicher aus der Befugnisverifikations-VAU löschen bzw. einen Zugriff auf diese Daten technisch ausschließen.[<=]

A_24671 - ePA-Aktensystem - Sichere Verbindung zwischen VAU-Instanzen

Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer VAU-Instanz einer Befugnisverifikations-VAU und einer VAU-Instanz einer Aktenkontoverwaltungs-VAU eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen.[<=]

A_24856 - ePA-Aktensystem - Private Authentisierungsschlüssel für sichere Verbindung zwischen VAU-Instanzen

Das ePA-Aktensystem MUSS sicherstellen, dass sich die VAU-Instanzen bei einer Verbindung zwischen einer VAU-Instanz einer Befugnisverifikations-VAU und einer VAU-Instanz einer Aktenkontoverwaltungs-VAU mit privaten Schlüsseln authentisieren, die ausschließlich über die jeweilige VAU-Instanz nutzbar sind. [≤]

3.5.4 Zusätzliche Anforderungen an eine Service-VAU

Spezielle Funktionen der "ePA für alle" können in eigenen, von den Aktenkontoverwaltungs-VAUs (AK-VAU) getrennten, VAUs ausgelagert und ausgeführt werden. Diese VAUs werden als **Service-VAUs** bezeichnet. Es kann Service-VAUs für unterschiedliche Funktionen geben, so dass es dementsprechend unterschiedliche **Typen von Service-VAUs** geben kann.

Service-VAU-Instanzen können durch den Betreiber des Aktensystems gestartet und in einem Pool verwaltet werden. AK-VAU-Instanzen können bei Bedarf auf Service-VAU-Instanzen zugreifen, wenn sie den Service nutzen möchten (in Abbildung 2 mit Service A dargestellt). Ein Kommunikationsaufbau von Service-VAU-Instanzen zu AK-VAU-Instanzen ist nicht möglich.

Eine Service-VAU-Instanz kann von mehreren AK-VAU-Instanzen gleichzeitig genutzt werden (die Service-VAU-Instanz zu AK-VAU-Instanz-Beziehung ist eine n:m-Beziehung).

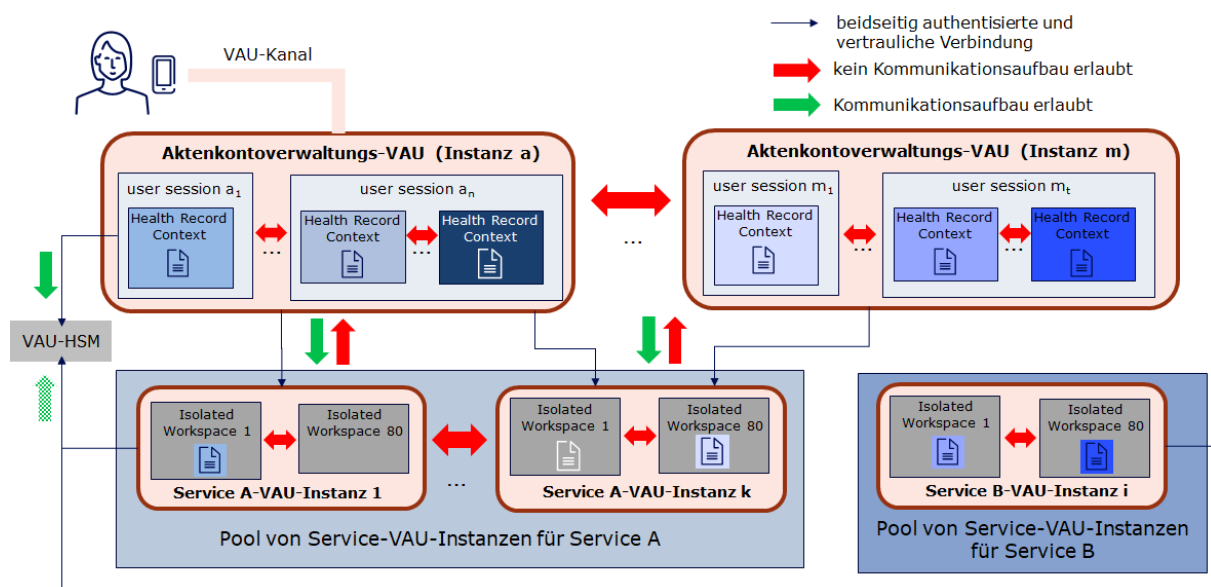


Abbildung 2 - Überblick Service-VAUs

Innerhalb einer Service-VAU-Instanz erfolgt die Verarbeitung unterschiedlicher Service-Requests in voneinander getrennten **Isolated Workspaces**. Isolated Workspaces in Service-VAUs werden analog zu den Health Record Contexts in Aktenkontoverwaltungs-VAUs geschützt.

A_26112 - ePA-Aktensystem - Maximale Isolated Workspaces in einer Service-VAU-Instanz

Das ePA-Aktensystem MUSS sicherstellen, dass maximal 80 Isolated Workspaces gleichzeitig in einer Service-VAU-Instanz laufen können. [≤]

A_26113 - ePA-Aktensystem - Isolation zwischen Isolated Workspaces innerhalb einer Service-VAU-Instanz

Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus ausschließen, dass sich innerhalb einer Service-VAU-Instanz die Verarbeitungen eines Isolated Workspaces schadhaft auf die Verarbeitungen eines anderen Isolated Workspaces auswirken können. [≤]

A_26114 - ePA-Aktensystem - Isolation zwischen unterschiedlichen Service-VAU-Instanzen

Das ePA-Aktensystem MUSS durch einen technischen Separationsmechanismus, der unabhängig vom Separationsmechanismus in A_26113-* ist, ausschließen, dass sich Verarbeitungen in einer Service-VAU-Instanz schadhaft auf die Verarbeitungen einer anderen Service-VAU-Instanz auswirken können. [≤]

A_26115 - ePA-Aktensystem - Isolated Workspace verarbeitet maximal einen Request einer AK-VAU

Nachdem ein Isolated-Workspace einen (1) Service-Request einer Aktenkontoverwaltungs-VAU-Instanz verarbeitet hat, MUSS das ePA-Aktensystem sicherstellen, dass alle Daten des Isolated-Workspaces sicher gelöscht werden, um den Isolated-Workspace für nachfolgende Service-Requests wieder neu zu initialisieren. [≤]

A_26116 - ePA-Aktensystem - In einem Isolated Workspace sind zu einem Zeitpunkt nur Daten eines Versicherten

Das ePA-Aktensystem MUSS sicherstellen, dass in einem Isolated Workspace zu einem Zeitpunkt ausschließlich Daten eines Versicherten verarbeitet werden können, sofern die Auswahl der zu verarbeitenden Daten durch die Logik im ePA-Aktensystem bestimmt wird. [≤]

Hinweis zu A_26116-*: Falls Nutzer die Daten für die Service-VAU auswählen, ohne dass das ePA-Aktensystem auf diese Daten Einfluss hat (z.B. Nutzer wählt zu konvertierende PDF-Dokumente im ePA-FdV aus) kann es dazu kommen, dass zu einem Zeitpunkt auch Daten mehrerer Versicherter in einem Isolated Workspace verarbeitet werden.

A_26117 - ePA-Aktensystem - Keine Kommunikation zwischen Isolated Workspaces

Das ePA-Aktensystem MUSS sicherstellen, dass es innerhalb einer Service-VAU-Instanz keine Kommunikation zwischen Isolated Workspaces gibt. [≤]

A_26118 - ePA-Aktensystem - Keine Kommunikation zwischen Service-VAU

Das ePA-Aktensystem MUSS sicherstellen, dass es keine Kommunikation zwischen Instanzen von Service-VAUs gibt. [≤]

A_26119 - ePA-Aktensystem - Service-VAUs speichern keine Daten in Aktenkonten

Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine Daten in einem Aktenkonto eines Versicherten persistieren. [≤]

A_26120 - ePA-Aktensystem - Service-VAUs verarbeiten keine Identitätstoken

Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen keine Identitätstoken von Nutzern verarbeiten. [≤]

A_26123 - ePA-Aktensystem - Service-VAU-Instanzen haben maximale Lebensdauer

Das ePA-Aktensystem MUSS sicherstellen, dass Service-VAU-Instanzen nach einer definierten Lebensdauer (abhängig von der Funktionalität der Services) keine neuen Service-Requests mehr annehmen können und, nachdem die laufenden Requests abgearbeitet wurden, beendet und neu gestartet werden. [≤]

A_26124 - ePA-Aktensystem - Information über neuen Service-VAU-Typ

Der Hersteller des ePA-Aktensystems MUSS die gematik über die Absicht der Einführung eines neuen Service-VAU-Typs informieren und ggf. für diesen neuen Service-VAU-Typ zu erfüllende Rahmenbedingungen abstimmen.[<=]

Hinweis zu A_26124-*: Hierzu gehört z.B. auch die Festlegung der maximalen Lebensdauer für den neuen Service-VAU-Typ (siehe A_26123-*).

A_26125 - ePA-Aktensystem - Starten ausschließlich attestierter Service-VAUs

Das ePA-Aktensystem MUSS sicherstellen, dass ausschließlich attestierte Service-VAU-Instanzen gestartet werden können.[<=]

3.5.4.1 Kommunikation zwischen AK-VAU und Service-VAU

A_26126 - ePA-Aktensystem - Gesicherte und authentifizierte Verbindung zwischen AK-VAU- und Service-VAU-Instanzen

Das ePA-Aktensystem MUSS sicherstellen, dass zwischen einer Aktenkontoverwaltungs-VAU-Instanz und einer Service-VAU-Instanz eine beidseitig authentifizierte und vertrauliche Verbindung besteht. Die vertrauliche Verbindung muss auch gegen Zugriffe durch einzelne Mitarbeiter des Betreibers des Aktensystems schützen.[<=]

A_26127 - ePA-Aktensystem - Kein Kommunikationsaufbau von Service-VAU-Instanzen zu AK-VAU-Instanzen

Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine Kommunikation zu einer AK-VAU-Instanz aufbauen kann.[<=]

A_26128 - ePA-Aktensystem - Kein Aufruf von Schnittstellen von AK-VAU-Instanzen durch Service-VAU-Instanzen

Das ePA-Aktensystem MUSS sicherstellen, dass eine Service-VAU-Instanz keine Schnittstellen/Services aufrufen kann, die in einer AK-VAU-Instanz ausgeführt werden.[<=]

3.6 Umschlüsselung und Überschlüsselung

Das Kerckhoffs'sche Prinzip von 1883 ist ein Grundpfeiler der Kryptographie. Es besagt u. a. dass die Sicherheit von kryptographischen Verfahren alleinig von der Geheimhaltung der Schlüssel abhängen darf, und dass Schlüssel leicht auswechselbar sein müssen. Damit kryptographische Schlüssel in der Praxis ihre Sicherheitseigenschaft behalten können müssen sie einen Lebenszyklus besitzen (vgl. bspw. [NIST-SP-800-57P1]), der den regelmäßigen Austausch (Wechsel) der Schlüssel vorsieht und umsetzt. Jährlich werden aus diesem Grunde die Masterkey für Akten Daten und die Masterkey für Befugnisse erneuert (vgl. A_15745-* und A_20519-* (beide aus [gemSpec_Krypt])). Bei dieser Erneuerung muss eine Umschlüsselung durchgeführt werden:

- Schlüssel_alt_KVNR = Ableitung (MK_alt, KVNR),
- Schlüssel_neu_KVNR = Ableitung (MK_neu, KVNR),
- Umschlüsselung pro Akte: Schlüssel_alt_KVNR -> Schlüssel_neu_KVNR.

Falls eine AK-VAU Zugriff auf eine Akte besitzt und zu diesem Zeitpunkt feststellt neue Masterkeys (vgl. betreiberspezifische Schlüssel A_15745-*) existieren, muss sie eine Umschlüsselung durchführen (A_20519-*). Falls eine Akte länger nicht verwendet wird, kann eine AK-VAU keinen Zugang zu den Klartexten der Akte erhalten, da sie nur nach erfolgreicher Nutzerauthentisierung vom VAU-HSM die aktenspezifischen Ableitungsschlüssel erhält. Dann kann eine AK-VAU zunächst auch keine Umschlüsselung vornehmen. Aus diesem Grunde muss eine VAU (entweder eine AK-VAU oder eine dedizierte Überschlüsselungs-VAU) eine Überschlüsselung der Chiffre der Akte

vornehmen. Dafür werden Überschlüsselungsschlüssel benötigt. Es gibt analog zu den anderen betreiberspezifischen Schlüssel (A_15745-*) Masterkeys für eine Schlüsselableitung für die Überschlüsselung der Chiffre einer Akte.

A_26197 - ePA-Aktensystem - betreiberspezifische Schlüssel:

Überschlüsselungs-Masterkeys

Ein ePA-Aktensystem MUSS sicherstellen, dass die Menge der betreiberspezifischen Schlüssel aus [gemSpec_Krypt#A_15745-*] um die Kategorie Überschlüsselungs-Masterkeys erweitert wird. Für die Überschlüsselungsschlüssel MÜSSEN die gleichen Vorgaben wie für alle betreiberspezifischen Schlüssel gemäß A_15745-* gelten. Die betreiberspezifischen Schlüssel werden mindestens jährlich aktualisiert (A_20519-*), die alten Schlüssel MÜSSEN solange im VAU-HSM verfügbar sein, solange Chiffre im Aktensystem existieren (bspw. Daten einer Akte), die mit diesen Schlüsseln kryptographisch gesichert sind. [<=]

D. h. wie in Abschnitt 3.3 (bspw. A_24611-*) definiert, gibt es bei den Masterkeys drei Kategorien: (1) Aktenpersistierung, (2) Befugnispersistierung und (3) Überschlüsselung. Initial startet der Betrieb eines Aktensystems mit je einem Schlüssel in den ersten zwei Kategorien. Nach maximal einem Jahr (A_20519-*), oder anders formuliert im nächsten Intervall, werden diese beiden ersten Schlüssel zufällig neu erzeugt. Dabei muss nun ein neuer Überschlüsselungsmasterkey erzeugt werden. Die Anzahl der Schlüssel nach o. g. Kategorie ist anschließend (1) 2, (2) 2, (3) 1.

A_26198 - ePA-Aktensystem - neuer Überschlüsselungsschlüssel bei Erneuerung betreiberspezifischen Schlüssel

Ein ePA-Aktensystem MUSS sicherstellen, dass bei jeder Erneuerung der Masterkeys zur Aktenpersistierung ein weiterer neuer Überschlüsselungsmasterkey zufällig im VAU-HSM erzeugt wird.

[<=]

Bei einer Erneuerung der betreiberspezifischen Schlüssel gibt es verschiedene Zeitabschnitte:

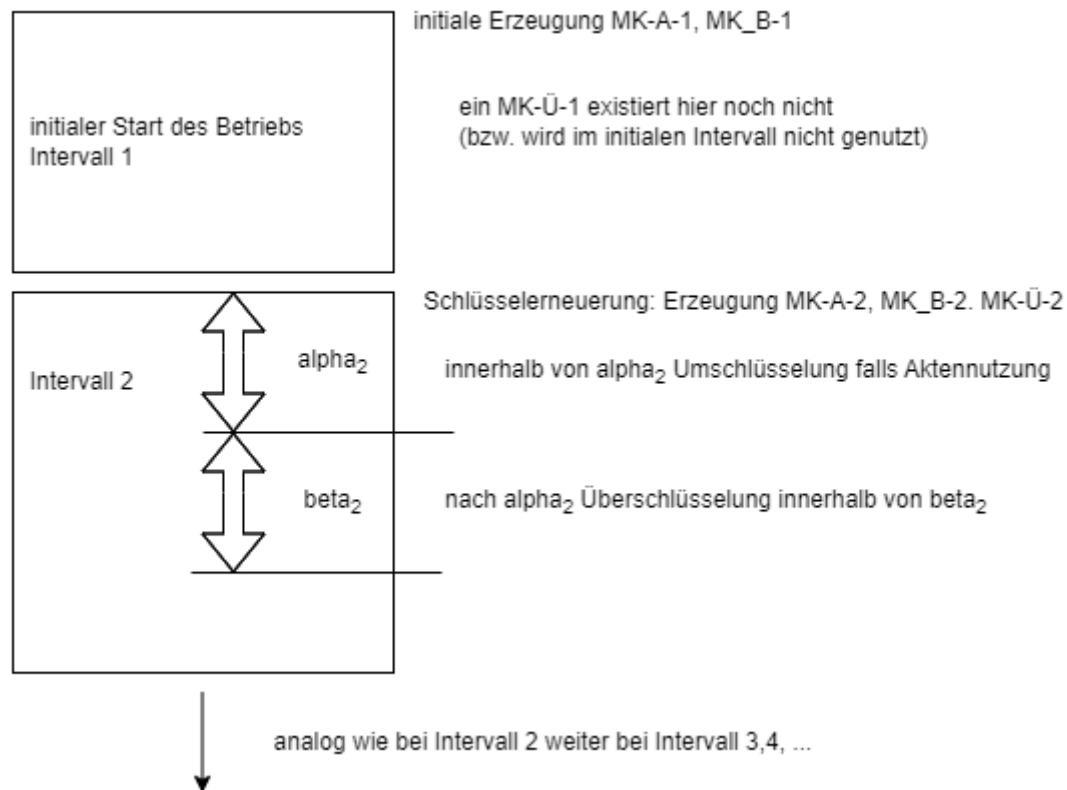


Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung

A_26204 - ePA-Aktensystem - zeitliche Vorgaben zur Durchführung der Umschlüsselung und Überschlüsselung

Ein ePA-Aktensystem MUSS sicherstellen, dass es ein konfigurierbares Zeitintervall alpha gibt, so dass nach einer Schüsselerneuerung der betreiberspezifischen Schlüssel innerhalb von alpha bei einer Aktennutzung eine Umschlüsselung in einer AK-VAU vorgenommen wird, falls die Verschlüsselung der Akte auf einem älteren Masterkey basiert. Das Zeitintervall alpha startet jeweils direkt mit jedem neuen Intervall (Schüsselerneuerung der betreiberspezifischen Schlüssel).

Weiter MUSS es sicherstellen, dass es ein konfigurierbares Zeitintervall beta gibt beginnend direkt nach alpha, so dass nach ablaufen von alpha eine Überschlüsselung von Chiffren von Akten, bei denen keine Umschlüsselung (wegen Nichtaktennutzung innerhalb von alpha) durchgeführt werden konnte, vorgenommen wird.

Der Default-Wert für die Länge von alpha MUSS 100 Tage und für die Länge von beta 60 Tage betragen. ("Default-Wert" bedeutet, Wert wenn der AS-Betreiber dort keinen anderen Wert konfigurieren möchte.)

[<=]

Die folgenden zwei Anforderung geben weitere Details zu A_26204-*.

A_26205 - ePA-Aktensystem - Umschlüsselung

Ein ePA-Aktensystem MUSS sicherstellen, dass wenn die AK-VAU eine Akte verwendet und feststellt, dass diese Akte nicht überschlüsselt ist und die versichertenindividuelle Aktenverschlüsselung auf einem älteren Masterkey (i. S. v. eben nicht aus dem aktuellen Intervall kommend) basiert, die AK-VAU eine Umschlüsselung vornimmt. Die alten Chiffre der Akten (also die Chiffre die auf Basis eines älteren Masterkeys verschlüsselt sind), MÜSSEN im Aktensystem nach erfolgreicher Umschlüsselung gelöscht werden.

Wenn die AK-VAU eine Akte verwendet und feststellt, dass diese überschlüsselt ist, so MUSS die AK-VAU die Überschüsselung entschlüsseln und die nun verfügbare Chiffre der Akten auf Grundlage des aktuellen Masterkeys umschlüsseln. (Hinweis: nach Konstruktion muss die innere Aktenverschlüsselung auf einem älteren Masterkey basieren, ansonsten hätte keine Überschüsselung stattgefunden.) Nach erfolgreicher Umschlüsselung MÜSSEN die alten Chiffre (das Überschüsselungschiffre und das alte "innere" Chiffre der Akte) im Aktensystem gelöscht werden. [\leq]

Hinweis zu A_26205-*: Die notwendigen aktenspezifischen Schlüssel liegen nun in der AK-VAU vor. Die Umschlüsselung muss nicht direkt sofort vor Nutzung der Akte erfolgen, sondern kann auch einige Minuten später erfolgen. Die konkrete Ausgestaltung liegt beim Hersteller.

A_26206 - ePA-Aktensystem - Überschüsselung

Ein ePA-Aktensystem MUSS sicherstellen, dass jeweils im aktuellen Intervall nach Ablauf des Zeitintervalls alpha Akten, die nicht überschlüsselt sind und deren Verschlüsselung auf einem älteren Masterkey (i. S. v. nicht aus dem aktuellen Zeitintervall) basiert, überschlüsselt werden auf Basis des aktuellen Überschüsselungs-Masterkeys. Diese Umschlüsselung MUSS jeweils innerhalb des Zeitintervalls beta für alle solche Akten abgeschlossen werden. Die "alten" Chiffre (Chiffre von solchen Akten vor der Überschüsselung) MÜSSEN im Aktensystem gelöscht werden. [\leq]

Umschlüsselung einer Überschüsselung: Bei einer Akten, die länger nicht verwendet wird, kann es dazu kommen, dass überschlüsselte Akten wieder überschlüsselt werden müssen, weil alpha im nächsten Intervall abgelaufen ist. In diesem Fall wird eine Umschlüsselung mittels der Überschüssel vorgenommen, d. h. die Verschlüsselungstiefe / -kette wird 2 nicht überschreiten -- es gibt maximal eine Überschüsselungsschicht.

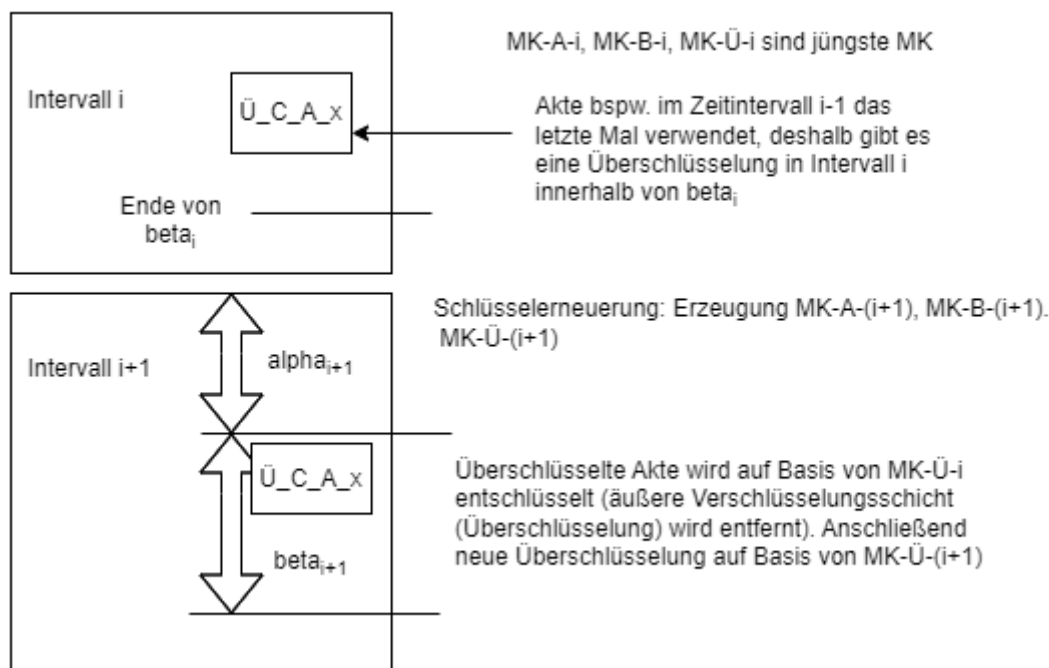


Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer Überschüsselung

A_26208 - ePA Aktensystem - Umschlüsselung einer Überschüsselung

Ein ePA-Aktensystem MUSS sicherstellen, dass jeweils in einem Intervall innerhalb von beta überprüft wird, ob überschlüsselte Akten existieren, deren Überschüsselung auf Basis eines alten Überschüsselungs-Masterkeys (also aus einem früheren Intervall stammend) durchgeführt wurde. Die AK-VAU (oder eine dedizierte Überschüsselungs-VAU) MUSS die überschüsselten Akten umschlüsseln, d. h. die Überschüsselung auf Grundlage eines älteren Überschüsselungs-Masterkeys wird aufgehoben (äußeren Verschlüsselungsschicht innerhalb der VAU entschlüsselt) und das Ergebnis (= Chiffre einer Akte) neu verschlüsselt auf Basis des aktuellen Überschüsselungs-Masterkeys. Die alten Chiffre (also vor der Umschlüsselung der Überschüsselung) MÜSSEN gelöscht werden. Das ePA-Aktensystem MUSS sicherstellen, dass nach Ablauf von beta keine überschüsselten Akten existieren, deren Überschüsselung auf Basis eines Überschüsselungsschlüssel, der nicht aus dem aktuellen Intervall stammt, durchgeführt wurde.

[<=]

Sollte durch irgendeinen Umstand die Sicherheitseigenschaft der Betreiberschlüssel (A_15745-*) in Frage stehen, so muss ein Aktensystembetreiber die Umschlüsselung bzw. die Überschüsselung aktivieren/starten können.

A_26199 - ePA-Aktensystem - Notfall-Aktivierung Umschlüsselung/Überschlüsselung

Ein ePA-Aktensystem MUSS sicherstellen, dass das ePA-Aktensystem es einem ePA-Betreiber ermöglicht eine Erneuerung der betreiberspezifischen Schlüssel zu starten/aktivieren. Es MUSS also dem ePA-Betreiber möglich sein neben der regelmäßigen Erneuerung der betreiberspezifischen Schlüssel (A_205019-*) eine Erneuerung zu initiieren.

[<=]

Nach A_20519-* muss es mindestens jährlich eine Schlüsselerneuerung geben. Mit 26199-* kann ein ePA-Betreiber im Notfall sozusagen den Zyklus "beschleunigen" -- ein neues Intervall sofort einleiten/erzeugen.

Da die Chiffre in einem ePA-Aktensystem mit Verschlüsselungsschlüsseln, die aus unterschiedlichen Masterkeys (aus unterschiedlichen Intervallen) abgeleitet werden, erzeugt werden können, muss an den äußeren Meta-Daten eines Chiffres ersichtlich sein auf welchem Masterkeys sie basieren (vom welchem Masterkey sind sie abgeleitet sind).

A_26223 - ePA-Aktensystem - Metadaten von ePA-spezifischen Chiffren

Ein ePA-Aktensystem MUSS sicherstellen, dass bei ePA-spezifischen Daten (Datenpersistierung von Akten, überschüsselte Aktenchiffre, verschlüsselte Befugnisse etc.) an den äußeren (also unverschüsselten) Meta-Daten des Chiffres erkennbar ist mithilfe welches (oder welcher) Masterkeys die Chiffre entschlüsselbar sind. [<=]

3.7 User Session und Health Record Context

Die Verarbeitungen innerhalb einer VAU werden über User Sessions und Health Record Contexts voneinander getrennt.

Wenn ein ePA-Client einen VAU-Kanal zum Aktensystem aufbaut, wird dieser einer bestimmten VAU-Instanz zugeordnet, in welcher dann eine User Session für den Nutzer des ePA-Clients erzeugt wird. Nach erfolgreicher Authentifizierung des Nutzers unter Verwendung des sektoralen IDPs (Versicherte) oder des IDP-Dienstes (LEI) ist die User Session etabliert und kann durch den ePA-Client genutzt werden. Alle Verbindungen für diesen VAU-Kanal werden immer an dieselbe VAU-Instanz geleitet, die die User Session verwaltet. Eine VAU-Instanz kann mehrere User Sessions verwalten.

Wird durch den ePA-Client eine Operation für eine bestimmte Akte aufgerufen (Parameter x-insurantid) der Operation, wird in der User Session geprüft, ob diese Akte schon verwendet wird (ein anderer Nutzer gerade mit der Akte arbeitet) oder nicht. Sollte die Akte noch nicht verwendet werden, wird die Akte in einem Health Record Context geöffnet und kann durch den ePA-Client in dessen User Session verwendet werden. Existiert für die Akte schon ein geöffneter Health Record Context, darf es durch den parallelen Zugriff zu keinen Inkonsistenzen in der Akte kommen.

Innerhalb einer VAU-Instanz dürfen nur eine maximale Anzahl von Health Record Contexts gleichzeitig aufgebaut sein. Sollte diese Anzahl überschritten werden, wird der am längsten nicht genutzte Health Record Context geschlossen, um einen neuen Health Record Context öffnen zu können.

3.8 Consent Decision Management

Das Consent Decision Management des Aktensystems verwaltet die Entscheidungen eines Versicherten oder eines Vertreters für oder gegen die Nutzung von definiert widerspruchsfähigen Funktionen gemäß gesetzlicher Vorgaben.

Der Widerspruch gegen die grundsätzliche Nutzung der ePA wird nicht im Consent Decision Management berücksichtigt. Die Existenz eines Aktenkontos für einen Versicherten impliziert, dass kein Widerspruch gegen die Nutzung der ePA erteilt wurde. Der Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger wird ebenfalls nicht hier verwaltet (siehe zu beiden Widersprüchen auch 3.1.1- Widerspruch des Versicherten gegen die Nutzung der elektronischen Patientenakte).

3.8.1 Widersprüche für Funktionen der ePA

Die vorgehaltenen Entscheidungen zu einer Funktion umfassen dabei den Zustand "kein Widerspruch erklärt" ("permit") oder "Widerspruch erklärt" ("deny") und den Kontext einer Funktion. Der Kontext ordnet dabei die einzelnen widerspruchsfähigen Funktionen einem für die Umsetzung des Widerspruchs betroffenen Nutzerkreis zu und wird bei den zugreifenden Schnittstellen zur Filterung der Ausgabe verwendet.

Initial, also bei der Erstellung eines neuen Aktenkontos oder bei Übernahme eines existierenden ePA 2.x Aktenkontos, ist für keine widerspruchsfähige Funktion ein Widerspruch gegen die Nutzung erklärt. Ein Versicherter oder ein Vertreter kann im Verlauf der Nutzung des Aktenkontos aktiv der Verwendung von widerspruchsfähigen Funktionen widersprechen oder einen erteilten Widerspruch zurücknehmen.

Die aktuell erteilten Widersprüche können durch einen Versicherten oder einen Vertreter jederzeit über ein ePA-FdV eingesehen und geändert werden. Versicherte und Vertreter, die ein ePA-FdV nicht nutzen möchten, können eine Auskunft über die aktuell erteilten Widersprüche über die Ombudsstelle erhalten und dort auch Änderungen an den Entscheidungen im Aktenkonto veranlassen. Die Ansicht oder Änderung der Widersprüche erfolgt im Aktenkonto stets gesichert innerhalb der VAU, die aktuellen Entscheidungen zu den widerspruchsfähigen Funktionen der ePA sind versichertenindividuell mit dem SecureDataStorageKey verschlüsselt abgelegt.

Die Information über relevante erteilte oder nicht erteilte Widersprüche können Clients auf einfache Weise (ohne Authentisierung oder Etablierung eines VAU-Kanals) im Vorfeld einer Operation über den Information Service abfragen (siehe auch 3.15- Information Service).

Das Consent Decision Management des Aktenkontos spiegelt ("cached") die Entscheidungen zu den Widersprüchen für die schnelle Abfrage über den Information Service in einen Bereich, der ohne den Aufbau eines VAU-Kanals und Verwendung des versichertenindividuellen SecureDataStorageKey nutzbar ist.

Das Aktenkonto unterstützt die Durchsetzung eines erteilten Widerspruchs überall dort, wo Aktivitäten dediziert als Teil einer widerspruchsfähigen Funktion zugeordnet werden können. Beispielsweise wird das Einstellen neuer Verordnungs- und Dispensierdaten in die Ordner der Kategorie "medication" immer verhindert, wenn der Teilnahme am digital gestützten Medikationsprozess widersprochen wurde. Die konkreten Auswirkungen eines Widerspruchs sind in den jeweiligen Kapiteln zur Handhabung von Dokumenten und Daten des Aktenkontos dargestellt (siehe [3.13.1- XDS Document Service](#) und [3.13.2- FHIR Data Services](#)) .

Die jeweils berücksichtigten widerspruchsfähigen Funktionen sind wie folgt definiert. Diese Liste kann in folgenden Versionen der ePA ergänzt oder verändert werden.

A_23874 - Consent Decision Management - Definition der widerspruchsfähigen Funktionen der ePA

Das Consent Decision Management MUSS die Attribute zu widerspruchsfähigen Funktionen der ePA gemäß der folgenden Tabelle verwenden.

Tabelle 10: Widerspruchsfähige Funktionen der elektronischen Patientenakte

Funktion (name)	Funktionsklasse (consent class)	Id der Funktion (id)	Entscheidung (consent decision)
Teilnahme am digital gestützten Medikationsprozess	Versorgungsprozess ("healthcareProcess")	"medication"	"deny"/"permit"
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst	Versorgungsprozess ("healthcareProcess")	"erp- submission"	"deny"/"permit"

[<=]

Hinweis: Die Bezeichnungen in () sind die Bezeichnungen in den Schnittstellen für den Abruf und die Verwaltung der Widersprüche. Eine widerspruchsfähige Funktion wird durch die ID der Funktion eindeutig identifiziert.

Hinweis: Die Verwaltung der Widersprüche gegen die Nutzung des Aktenkontos durch eine spezifische Leistungserbringerinstitution erfolgt über die Befugnisverwaltung (siehe [3.9.4- Befugnisauusschluss \(Blocked User Policy\)](#)).

Die Entscheidungen zu den widerspruchsfähigen Funktionen "medication" und "erp-submission" sind durch das Aktensystem dabei abhängig assoziiert:

A_25300 - Consent Decision Management - Untereinander abhängige Entscheidungen zu Widersprüchen

Das Consent Decision Management MUSS durch interne Maßnahmen sicherstellen, dass bei Erteilung eines Widerspruchs gegen die Nutzung der Funktion der elektronischen Patientenakte 'erp-submission' ('deny') auch der Widerspruch gegen die Nutzung der Funktion 'medication' gesetzt wird ('deny') und dass bei der Rücknahme ('permit') des Widerspruchs gegen die Nutzung der Funktion 'medication' auch der Widerspruch gegen die Nutzung der Funktion 'erp-submission' zurückgenommen wird. **[<=]**

Hinweis zu A_25300: Die Änderung der Entscheidung zur Nutzung der "führenden" Funktion hat automatisch eine Entscheidung zur Nutzung der "abhängigen" Funktion zur Folge. Dieses gilt nur für die aufgeführten Entscheidungsänderungen. Alle weiteren, nicht aufgeführten, Änderungen zu Entscheidungen haben keine "abhängige" Auswirkung auf weitere Entscheidungen zu Funktionen. Beispiel: Wird die Entscheidung für 'medication' von 'permit' auf 'deny' gesetzt, so hat dieses keine weiteren Änderungen an Entscheidungen zur Folge.*

A_23766 - Consent Decision Management - Initialisierung der Widerspruchsinformation zur Nutzung von Funktionen der ePA

Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen Patientenakte bei Erstellung eines neuen Aktenkontos oder bei Übernahme eines existierenden Aktenkontos einer älteren ePA-Version für alle Funktionen, gegen die der Versicherte nicht widersprochen hat mit der Entscheidung "kein Widerspruch erklärt" ("permit") initialisieren sowie alle Funktionen, gegen die der Versicherte widersprochen hat, mit "deny" initialisieren.

[<=]

A_24343 - Consent Decision Management - Speichern der Inhalte

Das Consent Decision Management MUSS die Entscheidungen zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen Patientenakte unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen.[<=]

A_23712 - Consent Decision Management - Übertrag der Widerspruchsinformation zur Nutzung von Funktionen der ePA für den Informationsdienst

Das Consent Decision Management MUSS die aktuellen Entscheidungen zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen Patientenakte der Funktionsklassen

- Versorgungsprozess ("healthCareProcess")

sofort im Anschluss an eine Änderung der Entscheidung im Consent Decision Management für die Abfrage durch den Information Service des Aktensystems ohne Nutzung der VAU und des SecureAdminStorageKeys verfügbar machen.

[<=]

A_24040 - Consent Decision Management - Periodischer Übertrag der Widerspruchsinformation zur Nutzung von Funktionen der ePA für den Informationsdienst

Das Consent Decision Management MUSS die aktuellen Entscheidungen zu Widersprüchen bezüglich der Nutzung von Funktionen der elektronischen Patientenakte der Funktionsklassen

- Versorgungsprozess ("healthCareProcess")

bei jedem Start der VAU (des VAU-Kanals) für die Abfrage durch den Information Service des Aktensystems ohne Nutzung der VAU und des SecureAdminStorageKeys verfügbar machen, unabhängig von einer Änderung der Entscheidungen zu den Widersprüchen.[<=]

Clients der Ombudsstelle und aus der Umgebung des Versicherten nutzen das Consent Decision Management über die Operationen der Schnittstelle

`I_Consent_Decision_Management`. Clients aus der Umgebung der LEI und der E-Rezept-Fachdienst nutzen für die schnelle Abfrage die Operation der Schnittstelle `I_Information_Service`.

A_23824 - Aktensystem - Realisierung der Schnittstelle I_Consent_Decision_Management

Das ePA-Aktensystem MUSS die Operationen der Schnittstelle `I_Consent_Decision_Management` gemäß `[I_Consent_Decision_Management]` umsetzen. [\leq]

A_23919 - Consent Decision Management - unveränderte Übernahme der Widerspruchsentscheidung

Das Consent Decision Management MUSS die über Operationen der Schnittstellen des Consent Managements übermittelten Entscheidungen (consent decisions) zu widerspruchsfähigen Funktionen der ePA in das Aktenkonto übernehmen. Die Entscheidungen zu den in den Operationen nicht adressierten widerspruchsfähigen Funktionen MÜSSEN im Aktenkonto unverändert bleiben. [\leq]

A_24844 - Consent Decision Management - Information über Änderungen der Widerspruchsinformation

Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung einer Widerspruchsinformation, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber informieren, dass Widerspruchsinformationen geändert wurden, wann die Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind. [\leq]

A_24055 - Consent Decision Management – Protokollierung geänderter Entscheidungen zu Widersprüchen

Das Consent Decision Management MUSS Bei Änderungen von Entscheidungen zu den widerspruchsfähigen Funktionen der ePA jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Für die Wertebelegung ist A_23874* zu berücksichtigen und die Protokollstruktur entsprechend zu belegen:

Tabelle 11: Consent Decision Management Protokollierung - Widersprüche für Funktionen der ePA

Strukturelement	Wert		Erläuterung
<code>AuditEvent.action</code>	U		Update
<code>AuditEvent.entity.name</code>	"ConsentDecision"		Eintrag protokolliert eine Widerspruchsentscheidung
<code>AuditEvent.entity.detail</code>	type	value[x]	
	"ConsentClass"	<consent class"	z.b. "healthcareProcess"
	"ConsentClassId"	<consent class Id>	z.b. "medication"
	"ConsentDecision"	<consent decision>	"deny" oder "permit"

[\leq]

Hinweis: Die initiale Entscheidung zu den Widersprüchen bei Anlage eines Aktenkontos wird nicht protokolliert. Die spezifische Protokollierung erfolgt für Folgeänderungen.

3.8.2 Einschränkung des Medication Service für bestimmte LEI (User Specific Deny Policy Medication)

Ein Versicherter bzw. Vertreter kann den Zugriff auf den Medication Service für bestimmte LEI innerhalb seines Aktenkontos einschränken und diese Einschränkung auch wieder zurücknehmen. Durch das Setzen einer LEI auf eine User Specific Deny Policy Medication wird jeder Zugriff dieser LEI auf den Medication Service für das Aktenkonto mit einem Fehler abgebrochen. Durch das Entfernen einer LEI von der User Specific Deny Policy Medication kann diese LEI Operationen des Medication Service (falls kein Widerspruch gegen "medication" vorliegt) wieder nutzen. Die User Specific Deny Policy Medication wird durch das Aktensystem für die in A_26406-* aufgeführten Nutzergruppen angewendet und durchgesetzt.

Der initiale Zustand nach Aktivierung eines Aktenkontos ist eine leere Liste.

A_26400 - Consent Decision Management - Initialisierung der User Specific Deny Policy Medication

Das Consent Decision Management MUSS für ein Aktenkonto eine User Specific Deny Policy Medication ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policy über die Schnittstelle `I_Consent_Decision_Management` gemäß `[I_Consent_Decision_Management]` ermöglichen. [`<=`]

A_26401 - Consent Decision Management - Speichern der Inhalte der User Specific Deny Policy Medication

Das Consent Decision Management MUSS Einträge aus der User Specific Deny Policy Medication unter Verwendung des `SecureDataStorageKeys` gesichert im Aktenkonto ablegen. [`<=`]

A_26403 - Consent Decision Management - Information über Änderungen der User Specific Deny Policy Medication

Das Consent Decision Management MUSS den Aktenkontoinhaber bei einer Änderung der Entscheidungen zu der User Specific Deny Policy Medication, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber informieren, welche Änderungen der User Specific Deny Policy Medication vorgenommen wurden, wann die Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind. [`<=`]

A_26406 - Consent Decision Management - Policy für berechnigte Nutzergruppen und Nutzer

Das Consent Decision Management MUSS die Konfiguration der User Specific Deny Policy Medication auf die folgenden Nutzergruppen einschränken:

Nutzergruppe [professionOID] der User Specific Deny Policy Medication
oid_praxis_arzt
oid_krankenhaus
oid_institution-vorsorge-reha
oid_zahnarztpraxis
oid_öffentliche_apotheke

Nutzergruppe [professionOID] der User Specific Deny Policy Medication
oid_praxis_psychotherapeut
oid_institution-pflege
oid_institution-geburtshilfe
oid_praxis-physiotherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin
oid_diga
oid_praxis-ergotherapeut
oid_praxis-logopaede
oid_praxis-podologe
oid_praxis-ernaehrungstherapeut

[<=]

A_26405 - Consent Decision Management – Protokollierung geänderter Entscheidungen der User Specific Deny Policy Medication

Das Consent Decision Management MUSS für jede Änderung der User Specific Deny Policy Medication einen Protokolleintrag gemäß A_24704* erzeugen:

Tabelle 12: Consent Decision Management Protokollierung - User Specific Deny Policy Medication

Strukturelement	Wert		Erläuterung
AuditEvent.action	C, D		Update
AuditEvent.entity.name	"UdpMedication"		Eintrag protokolliert eine Änderung der User Specific Deny Policy für Medication Service
AuditEvent.entity.detail	type	value[x]	

Strukturelement	Wert		Erläuterung
	"UserId"	<Telematik-ID der LEI>	Telematik-ID der LEI, welche zur User Specific Deny Policy Medication hinzugefügt oder gelöscht wurde
	"UserName"	<displayName>	Name der LEI, welche zur User Specific Deny Policy Medication hinzugefügt oder gelöscht wurde

[<=]

3.9 Entitlement Management

Befugnisse (Entitlements) werden individuell für jeden Nutzer des Aktenkontos erstellt (Versicherter, Vertreter, Leistungserbringerinstitutionen, Kostenträger, Ombudsstelle und Fachdienste). Eine erteilte Befugnis ist notwendige Voraussetzung für die Nutzung des Aktenkontos und zum internen Bezug des Datenpersistierungsschlüssels (SecureDataStorageKey) für den Zugriff auf die Dokumenten- und Datenverwaltung.

Eine Befugnis enthält folgende Informationen:

A_23734-01 - Entitlement Management - Definition einer Befugnis

Das Entitlement Management MUSS für eine individuelle Befugnis die folgenden Daten nutzen und verwalten:

Tabelle 13: Inhalt einer Befugnis

Element	Inhalt	Anmerkung	signiertes Element (*)
Identifizier des Aktenkontos (insurantId)	KVNR des Aktenkontos, für welches die Befugnis ausgestellt ist		ja
Identifizier des befugten Nutzers (actorId)	Telematik-ID oder KVNR		ja
Name des befugten Nutzers (displayName)	Name der Institution, des Nutzers		nein
Rolle des Nutzers (oid)	OID der Nutzerrolle (professionOID)		nein

Element	Inhalt	Anmerkung	signiertes Element (*)
Ende der Gültigkeit (validTo)	Datum und Zeitpunkt (letzter Tag der Gültigkeit, d.h. eine heutige Befugnisvergabe für 3 Tage setzt für validTo das Datum von übermorgen (aktueller Tag + 2 Tage). aktueller Tag ist inklusiv zu bewerten).	Wird gemäß [RFC3339] mit Zeitzone UTC (z.B.: 2024-04-12T22:59:59Z) bzw. Zeitzone-Offset (z.B.: 2024-04-12T23:59:59+01:00) gespeichert. Eine unbegrenzt gültige Befugnis erhält das Datum 9999-12-31T00:00:00Z. . Die Befugnisdauer der Befugnisse (Karte stecken), die durch das Aktensystem erstellt werden, werden auf das Ende des resultierenden Tages der aktuell gültigen Zeitzone in Deutschland gesetzt, z.B.: 2024-04-12T23:59:59+01:00. Wird durch den Versicherten oder einen Vertreter oder das Entitlement Management gesetzt.	ja
Beginn der Gültigkeit, Ausstellungszeitpunkt (issued-at)	Datum und Zeitpunkt	Wird durch das Entitlement Management gesetzt.	nein
Identifizier des Erstellers (issued-actorId)	Telematik-ID oder KVNR	Wird durch das Entitlement Management gesetzt.	nein
Name des Erstellers (issued-displayName)	Name der Institution, des Nutzers	Wird durch das Entitlement Management gesetzt.	nein

【<=】

Hinweis: Ein Nutzer ist der Adressat, für den die Befugnis ausgestellt wird. Der Ersteller ist der Nutzer, welcher die Befugnisausstellung veranlasst hat. Die Bezeichner in () sind die Bezeichner in den Schnittstellenbeschreibungen.

Hinweis (): A_23734 definiert eine "vollständige" Befugnis, welche auch Daten enthält, die für eine Prüfung einer gültigen Befugnis im Kontext einer Schnittstellenoperation nicht notwendig sind. Für diesen Zweck wird nur der (HSM-) signierte Anteil als Ergebnis einer Befugnisverifikation verwendet (signiertes Element = ja). Eine gespeicherte Befugnis enthält jedoch alle Elemente für eine qualifizierte Verwaltung der Befugnisse durch einen Versicherten oder Vertreter.*

Hinweis: Befugnisse können durch das Aktensystem selbst (initiale Befugnisse), durch den Versicherten oder einen befugten Vertreter unter Verwendung eines ePA-FdV oder durch eine Leistungserbringerinstitution in einer Behandlungssituation erstellt werden.

Eine Befugnis kann nur für Nutzer und Nutzergruppen mit bestimmter Rolle erteilt werden. Nutzergruppen mit abweichenden Rollen können nicht befugt werden und erhalten keinen Zugriff auf das Aktenkonto.

Erfolgt die Befugniserteilung durch eine Leistungserbringerinstitution in einer Behandlungssituation, wird eine vorgegebene Gültigkeitsdauer der Rolle des Befugten entsprechend durch das Entitlement Management vergeben. Ein Versicherter oder ein befugter Vertreter kann den Gültigkeitszeitraum frei wählen (ausgenommen Vertreterbefugnisse).

A_23941-01 - Entitlement Management - Erteilung von Befugnissen für berechnigte Nutzergruppen und Nutzer

Das Entitlement Management MUSS die Erteilung von Befugnissen in der jeweiligen Umgebung auf die folgenden Nutzergruppen und Nutzer einschränken:

Tabelle 14: Befugnisse für berechnigte Nutzergruppen und Nutzer

professionOID / Nutzergruppe und Nutzer	Umgebung			Standard- Befugnisdauer [Tage]	Befugnisdauer FdV [Tage]
	LEI	FdV	AS	durch das Entitlement Management bei Erteilung der Befugnis aus der Umgebung LEI	bei Erteilung der Befugnis aus der Umgebung FdV
oid_praxis_arzt	x	x	-	90	var
oid_krankenhaus	x	x	-	90	var
oid_institution-vorsorge-reha	x	x	-	90	var
oid_zahnarztpraxis	x	x	-	90	var
oid_öffentliche_apotheke	x	x	-	3	var
oid_praxis_psychotherapeut	x	x	-	90	var
oid_institution-pflege	x	x	-	90	var
oid_institution-geburtshilfe	x	x	-	90	var
oid_praxis-physiotherapeut	x	x	-	90	var
oid_praxis-ergotherapeut	x	x	-	90	var
oid_praxis-logopaede	x	x	-	90	var

professionOID / Nutzergruppe und Nutzer	Umgebung			Standard- Befugnisdauer [Tage]	Befugnisdauer FdV [Tage]
	LEI	FdV	AS	durch das Entitlement Management bei Erteilung der Befugnis aus der Umgebung LEI	bei Erteilung der Befugnis aus der Umgebung FdV
oid_praxis-podologe	x	x	-	90	var
oid_praxis- ernaehrungstherapeut	x	x	-	90	var
oid_institution-oegd	x	x	-	3	var
oid_institution- arbeitsmedizin	x	x	-	3	var
oid_kostentraeger	-	-	x (statisch)	-	-
oid_ombudsstelle	-	-	x (statisch)	-	-
oid_erp-vau (E-Rezept vertrauenswürdige Ausführungsumgebung)	-	-	x (statisch)	-	-
oid_versicherter (Versicherter)	-	-	x (statisch)	-	-
oid_versicherter (Vertreter)	-	x	-	-	dauerhaft
oid_diga	-	x	-	-	dauerhaft

Hinweis:

'x' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung befugt werden

'-' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung nicht befugt werden

LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-Prüfungsnachweis (Prüfziffer),

FdV = Versicherter oder Vertreter,

KTR = Kostenträger

AS = Aktensystem (systemseitig erteilte Befugnisse)

Tage = Gültigkeit in Tagen: angegebener Wert ist einschließlich aktuellem Datum, z. B. 90 Tage bedeutet aktuelles Datum + 89 Tage.

dauerhaft = Befugnis unbegrenzt gültig (Enddatum = 9999-12-31)

statisch = Gültigkeit analog 'dauerhaft', Befugnis ist implizit vorhanden.

var = Gültigkeitsdauer von 1 Tag bis dauerhaft in jeweils ganzen Tagen[<=]

Befugnisse werden durch das Entitlement Management mit dem SecureAdminStorageKey verschlüsselt und im Aktenkonto gesichert abgelegt.

Einzelne Nutzer können durch den Versicherten, einen befugten Vertreter oder die Ombudsstelle explizit von der Befugnisvergabe ausgeschlossen sein (siehe 3.9.4- Befugnisausschluss (Blocked User Policy)). Eine Befugniserstellung ist dann weder für Leistungserbringerinstitutionen in einer Behandlungssituation, noch durch den Versicherten oder einen Vertreter möglich.

Die Befugnisse für den Versicherten und den E-Rezept-Fachdienst werden dabei nicht persistiert. Diese Befugnisse werden als implizit vorhanden und gültig angenommen.

Eine Besonderheit stellt hierbei eine Befugnis EU-Zugriff dar. Es gibt zu einem Zeitpunkt für ein Aktenkonto maximal eine Befugnis EU-Zugriff. Die Dauer dieser Befugnis wird durch das Aktensystem festgelegt und beträgt 1 Stunde. Das Ende der Gültigkeit (validTo) wird ermittelt vom Ausstellungszeitpunkt + 1 Stunde.

A_26167 - Entitlement Management (EU) - Erteilung der Befugnis EU-Zugriff

Das Entitlement Management MUSS die Erteilung einer Befugnis EU-Zugriff in der jeweiligen Umgebung zusätzlich zu A_23941-* auf die folgenden Nutzergruppen und Nutzer einschränken:

Tabelle 15: Befugnisse EU-Zugriff für berechtigte Nutzergruppen und Nutzer

professionOID / Nutzergruppe und Nutzer	Umgebung			Standard- Befugnisdauer	Befugnisdauer FdV
	LEI	FdV	AS	durch das Entitlement Management bei Erteilung der Befugnis aus der Umgebung LEI	bei Erteilung der Befugnis aus der Umgebung FdV
oid_ncpeh	-	x	-	-	1 Stunde; wird durchgesetzt durch das Aktensystem

Hinweis:

'x' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung befugt werden

'-' bedeutet: diese Nutzer/Nutzergruppe kann aus der angegebenen Umgebung nicht befugt werden

LEI = Leistungserbringerorganisation mit Nachweis der Behandlungssituation über VSDM-Prüfungsnachweis (Prüfziffer),

FdV = Versicherter oder Vertreter,

AS = Aktensystem (systemseitig erteilte Befugnisse)[<=]

A_24371 - Entitlement Management - Verschlüsselung der Befugnisse

Das Entitlement Management MUSS Befugnisse mit dem versichertenindividuellen SecureAdminStorageKey verschlüsseln und im Aktenkonto persistieren.[<=]

A_24372 - Entitlement Management - Keine persistente Ablage unverschlüsselter Befugnisse

Das Entitlement Management MUSS sicherstellen, dass Befugnisse ausschließlich verschlüsselt unter Verwendung des versichertenindividuellen SecureAdminStorageKey im Aktenkonto gespeichert werden.[<=]

A_24687 - Entitlement Management - Keine Speicherung oder Verwendung nicht verifizierter Befugnisse

Das Entitlement Management MUSS sicherstellen, dass ausschließlich Befugnisse persistiert oder für eine Befugnisprüfung verwendet werden, die erfolgreich durch das HSM unter Verwendung der adäquaten Regeln 'rr1 - rr4' gemäß A_24573* befugnisverifiziert sind.[<=]

A_23842 - Entitlement Management - Eindeutigkeit der Befugnisse im Befugniskontext

Das Entitlement Management MUSS sicherstellen, dass im Befugniskontext keine zwei oder mehr Befugnisse existieren, die als Identifier des befugten Nutzers die gleiche Identifikation (`actorId`) aufweisen.[<=]

A_24785 - Entitlement Management - VSDM-Prüfungsnachweis kann höchstens einmal genutzt werden

Das Entitlement Management MUSS sicherstellen, dass ein VSDM-Prüfungsnachweis (Prüfziffer) höchstens einmal zur Registrierung einer Befugnis genutzt werden kann.[<=]

ePA-Clients nutzen zur Befugnisvergabe die Operationen der Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]`. Die initialen Befugnisse des Aktenkontos werden auf organisatorischem Weg direkt im Aktenkonto erstellt.

A_24506 - Entitlement Management- Realisierung der Schnittstelle I_Entitlement_Management

Das Entitlement Management MUSS die Operationen der Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` umsetzen.[<=]

A_26168 - Entitlement Management (EU)- Realisierung der Schnittstelle I_Entitlement_Management_EU

Das Entitlement Management MUSS die Operationen der Schnittstelle `I_Entitlement_Management_EU` gemäß `[I_Entitlement_Management_EU]` umsetzen.[<=]

A_24987-01 - Entitlement Management - Protokolleinträge für Zugriffe auf das Entitlement Management

Das Entitlement Management MUSS für das Erteilen und Entziehen von Befugnissen und das Setzen und Löschen von Befugnisausschlüssen jeweils einen Protokolleintrag gemäß A_24704 erzeugen. Dabei ist folgende Wertebelegung zu berücksichtigen:

Tabelle 16: Entitlement Management Protokollierung

Strukturelement	Wert	Erläuterung
<code>AuditEvent.type</code>	"rest"	

Strukturelement	Wert		Erläuterung
AuditEvent.action	C, D, U		ein Code aus den genannten, je nach Operation
AuditEvent.entity.name	"UserBlocking"		Setzen und Löschen von Befugnisausschlüssen
	"EntitlementManagement"		Erteilen oder Entziehen von Befugnissen
AuditEvent.entity.detail	type	value[x]	
	"blockedUserName"	<Name der LEI>	Name der LEI, für die der Befugnisausschluss gesetzt bzw. der Ausschluss zurückgenommen wurde
	"blockedUserId"	<Telematik-ID der LEI>	Telematik-ID der LEI, für die der Befugnisausschluss gesetzt bzw. der Ausschluss zurückgenommen wurde
	"UserName"	<Name der Institution oder des Vertreters>	Name der Institution oder des Nutzers für die eine Befugnis erteilt oder gelöscht wurden
	"UserId"	<Identifizier der Institution oder des Vertreters>	ID der Institution oder des Nutzers für die eine Befugnis erteilt oder gelöscht wurden
	"entitledValidTo"	<Endzeitpunkt der Gültigkeit der Befugnis>	Angabe des Endes einer erteilten Befugnis, Format gemäß [RFC3339] YYYY-MM-DDThh:mm:ssZ oder YYYY-MM-DDThh:mm:ss+/-time zone

[<=]

Hinweis: Ein Update ("U") eines Entitlements liegt vor, wenn ein existierendes Entitlement aufgrund des längeren Gültigkeitszeitraums eines neuen Entitlements überschrieben wird.

3.9.1 Initiale Befugnisse (static Entitlements)

Einige grundsätzlich notwendige Befugnisse sind zum Zeitpunkt der Aktivierung eines Aktenkontos verfügbar.

Zu diesen initialen Befugnissen gehören die Befugnisse für den Versicherten, den E-Rezept-Fachdienst, den Kostenträger und die Ombudsstelle. Diese Befugnisse müssen in der Phase der Initialisierung eines Aktenkontos durch das Aktensystem erstellt werden.

Diese Befugnisse sind dauerhaft gültig und unveränderbar und können nicht gelöscht werden.

A_24145 - Entitlement Management – Implizite initiale (statische) Befugnisse

Das Entitlement Management MUSS sicherstellen, dass der Versicherte (KVNR des Akteninhabers, oid_versicherter), und der E-Rezept-Fachdienst (registrierte Telematik-ID, oid_erp-vau) dauerhaft den versichertenindividuellen SecureDataStorageKey beziehen können und Zugriff auf die Dokumenten- und Datenverwaltung erhalten. Die Befugnisse MÜSSEN den Vorgaben der folgenden Tabelle entsprechen:

Element	Versicherter	E-Rezept-Fachdienst
Identifizier des befugten Nutzers (actorId)	KVNR des Versicherten (Aktenkontoinhaber)	Telematik-ID der E-Rezept vertrauenswürdigen Ausführungsumgebung
Name des befugten Nutzers (displayName)	Name des Versicherten	Name/ Bezeichnung des E-Rezept-Fachdienstes oder "Fachdienst E-Rezept"
Rolle des Nutzers (oid)	oid_versicherter	oid_erp-vau
Ende der Gültigkeit (validTo)	9999-12-31	9999-12-31

[<=]

A_24374 - Entitlement Management – Signierte initiale (statische) Befugnisse

Das Entitlement Management MUSS sicherstellen, dass für den Kostenträger und die Ombudsstelle gültige Befugnisse mit unbegrenzter Gültigkeitsdauer zum Zeitpunkt der Aktivierung des Aktenkontos gemäß der Vorgaben der folgenden Tabelle vorliegen:

Element	Kostenträger	Ombudsstelle
Identifizier des Aktenkontos (insurantid)	KVNR des Versicherten	KVNR des Versicherten
Identifizier des befugten Nutzers (actorId)	Telematik-ID des Kostenträgers	Telematik-ID der Ombudsstelle

Element	Kostenträger	Ombudsstelle
Name des befugten Nutzers (displayName)	Name des Kostenträgers	Name/ Bezeichnung der Ombudsstelle
Rolle des Nutzers (oid)	oid_kostentraeger	oid_ombudsstelle
Ende der Gültigkeit (validTo)	9999-12-31	9999-12-31

[<=]

A_24688-01 - Entitlement Management – Befugnisverifikation signierter initialer Befugnisse

Das Entitlement Management MUSS sicherstellen, dass die initialen, signierten Befugnisse des Kostenträgers und der Ombudsstelle spätestens beim ersten Zugriff auf das Aktenkonto durch das HSM unter Verwendung der Regel 'rr4' gemäß A_24573* befugnisverifiziert sind.[<=]

A_24533 - Entitlement Management - Keine Änderung statischer Befugnisse

Das Entitlement Management MUSS sicherstellen, dass die dauerhaften Befugnisse des Versicherten, des E-Rezept-Fachdiensts, des Kostenträgers und der Ombudsstelle nicht verändert oder gelöscht werden können.[<=]

A_24784 - Entitlement Management - Höchstens eine Befugnis für KTR und Ombudsstelle pro Aktenkonto

Das Entitlement Management MUSS sicherstellen, dass in einem Aktenkonto höchstens eine Befugnis für einen Kostenträger und höchstens eine Befugnis für eine Ombudsstelle hinterlegt ist.[<=]

A_24955 - Entitlement Management - Befugnis für KTR und Ombudsstelle nur bei Anlage und betreiberinterner Anbieterwechsel

Das Entitlement Management MUSS sicherstellen, dass eine signierte Befugnis des Kostenträgers und eine signierte Befugnis der Ombudsstelle ausschließlich bei einer Anlage eines Aktenkontos (Initialisierung) oder bei einem betreiberinternen Anbieterwechsel in die Befugnisse des Aktenkontos aufgenommen werden.

[<=]

3.9.2 Erstellen einer Befugnis durch Clients

Die Anforderung zur Vergabe einer neuen Befugnis erfolgt durch die Clients der ePA. Bei einer Befugnisvergabe aus der Umgebung der Leistungserbringer ist dieses das Primärsystem (PS), aus der Umgebung des Versicherten ist es das ePA-FdV.

Clients verwenden zur Befugnisvergabe signierte JSON Web Token (JWS). Das Token wird zur Verifikation an das HSM übergeben. Als Ergebnis der HSM Verarbeitung liegt eine bestätigte, CMAC gesicherte Befugnis mit den Elementen `actorId` (Identifizier des zu befugnenden Nutzers), `kvn` (AktenkontoId) und `validTo` (Gültigkeitszeitraum) für die spätere Befugnisprüfung vor. Das HSM Ergebnis wird mit den weiteren Daten gemäß A_23734* (`oid`, `displayName`, `issued`-*) ergänzt und gemäß A_24371* mit dem `SecureAdminStorageKey` gesichert im Aktenkonto abgelegt.

3.9.2.1 Befugnisvergabe durch ein ePA-FdV

Ein ePA-FdV muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

A_24587-01 - Entitlement Management - Befugnis durch ein ePA-FdV

Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ePA-FdV über die Schnittstelle `I_Entitlement_Management` durch Verwendung eines gültig signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:

Befugnis	Claim Name	Claim	Beispiel
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.CH.SIG	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	
	"exp"	Verfalldatum, = "iat" + 20 min	
	"insurantId"	KVNR des Aktenkontos	A123456789
	"actorId"	Identifizier (Telematik-id oder KVNR)	3-883110000092471
	"oid"	professionOid	1.2.276.0.76.4.54
	"displayName"	Name des Befugten	Test-Apotheke
	"validTo"	Ende der Gültigkeit, (Bei unbegrenzter Gültigkeit ist 9999-12-31T00:00:00Z zu verwenden.)	gemäß [RFC3339], z.B. 2025-06-30T21:59:59Z oder 2025-06-30T23:59:59+02:00

[<=]

Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve "brainpoolP256r1 basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

Hinweis zu A_24587: Im Falle der Befugnisvergabe für einen NCPeH (EU-Zugriff, "oid" == "oid_ncpeh") wird durch das Aktensystem sichergestellt, dass die vorgeschriebene*

Gültigkeitsdauer für derartige Befugnisse angewendet wird. Dieses erfolgt durch die Befugnisverifikation gemäß Regel "rr1" im HSM. Die Angabe eines Gültigkeitsendes im "validTo"-Element des JWT wird daher für diesen Fall ignoriert, das Element selbst muss jedoch vorhanden sein.

A_24689 - Entitlement Management - Befugnisverifikation einer Befugnis durch ein ePA-FdV

Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein ePA-FdV unter Verwendung der Regeln 'rr1' (Befugnisvergabe durch den Versicherten) bzw. 'rr2' (Befugnisvergabe durch einen Vertreter) des HSM eine Befugnisverifikation durchführen.[<=]

A_24535 - Entitlement Management - Befugnisse für Vertreter

Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId` = KVNVR) ausschließlich durch den Versicherten erstellt oder gelöscht werden können.[<=]

A_26698 - Entitlement Management - maximale Anzahl Befugnisse für Vertreter

Das Entitlement Management MUSS sicherstellen, dass maximal fünf gültige Befugnisse für Vertreter gleichzeitig in einem Aktenkonto vorhanden sind.[<=]

A_24536 - Entitlement Management - Gültigkeitsdauer der Befugnisse für Vertreter

Das Entitlement Management MUSS sicherstellen, dass Befugnisse für Vertreter (`actorId` = KVNVR) ausschließlich mit einer unbegrenzten Gültigkeit erstellt werden.[<=]

A_24754 - Entitlement Management - E-Mail-Adresse des Vertreters

Das Entitlement Management MUSS sicherstellen, dass bei Befugnissen für Vertreter (`actorId` = KVNVR) eine E-Mail-Adresse des Vertreters für dessen Benachrichtigung angegeben wird.[<=]

Die in A_24754 angegebene E-Mail-Adresse wird ausschließlich zur Benachrichtigung des Vertreters über die eingestellte Befugnis verwendet (vgl. A_24755-*), jedoch nicht für die Geräteregistrierung. Um eine Vertretung wahrnehmen zu können und hierfür Geräte zu registrieren, muss der Vertreter in seinem Home-AS eine E-Mail-Adresse hinterlegt haben.

A_24755-01 - Entitlement Management - Benachrichtigung des Vertreters bei Befugniserstellung

Das Entitlement Management MUSS im Anschluss an die erfolgreiche, neue Befugniserstellung für einen Vertreter eine E-Mail an die E-Mail-Adresse des Vertreters senden, die diesen über die Befugniserstellung für das Aktenkonto des Versicherten geeignet informiert. In der Nachricht MUSS der Name des Versicherten enthalten sein und welche Art von personenbezogenen Daten vom Vertreter im Rahmen der Vertreterberechtigung im ePA-Aktensystem verarbeitet werden, wie der Vertreter eine Vertreterberechtigung widerrufen kann und gegenüber wem er seine datenschutzrechtlichen Betroffenenrechte wahrnehmen kann.[<=]

Hinweis: Unter Art der personenbezogenen Daten ist z.B. „Krankenversichertennummer, Name und E-Mail-Adresse“ gemeint, aber nicht die tatsächliche KVNVR des Vertreters, der tatsächliche Name oder die tatsächliche E-Mail-Adresse.

3.9.2.2 Befugnisvergabe durch ein Primärsystem

A_27288 - Entitlement Management – Abgleich der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer

Das Entitlement Management MUSS sicherstellen, dass für die in `setEntitlementPs` vom Primärsystem in `x-insurantId` übergebene KVNR und die übergebene Befugnis (signiertes JWT) folgendes gilt: die KVNR in `x-insurantId` stimmt mit der KVNR überein, die in der CMAC-gesicherten Befugnis enthalten ist, die als Ergebnis des Aufrufs der Regel `rr3` mit der vom Primärsystem erhaltenen Befugnis (signiertes JWT) vom HSM zurückgegeben wird.

[<=]

Ein Primärsystem muss für die Befugnisvergabe ein JWS gemäß folgender Vorgabe erstellen.

Sollte der öffentliche Schlüssel im Signaturzertifikat zu "x5c" auf der ECC-Kurve "brainpoolP256r1" basieren, so soll der Wert "ES256" (JWS-Parameters "alg") im Kontext der Befugnisvergabe auch für diese Kurve gelten (also nicht nur für P-256). Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

A_27321 - Entitlement Management – Abgleich hcv bei Erstellen einer Befugnis über VSDM-Prüfziffer in Version 2

Falls vom Primärsystem in `setEntitlementPs` eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2 übergeben wird und das Ergebnis des Aufrufs der Regel `rr3` eine interne Datenstruktur der VSDM-Prüfziffer zurückliefert, MUSS das Entitlement Management sicherstellen, dass

- bei einem JWT mit Attribut "hcv" der Wert von "hcv" mit dem Wert von hcv aus der VSDM-Prüfziffer übereinstimmt und ansonsten die Operation `setEntitlementPs` abbricht,
- bei einem JWT ohne Attribut "hcv" die Operation `setEntitlementPs` abbricht, falls der Konfigurationsparameter `enforce_hcv_check` (vgl. A_27342-*) auf `true` gesetzt ist.

[<=]

A_27289 - Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche der KVNR bei Erstellen einer Befugnis über VSDM-Prüfziffer

Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer Stunde maximal fünfmal eine Befugnis (signiertes JWT) über `setEntitlementPs` übermitteln kann, bei der die mitgelieferte KVNR in `x-insurantId` von der KVNR abweicht, die in der Prüfziffer der übermittelten Befugnis (signiertes JWT) enthalten ist, andernfalls für den Nutzer für diesen Zeitraum die Operation `setEntitlementPs` abbrechen.[<=]

A_27322 - Entitlement Management – Maximale Anzahl fehlerhafter Abgleiche der VSD-Update-Zeit bei Erstellen einer Befugnis über VSDM-Prüfziffer in Version 2

Das Entitlement Management MUSS sicherstellen, dass ein Nutzer (LEI) innerhalb einer Stunde maximal fünfmal eine Befugnis (signiertes JWT) mit einer Prüfziffer in Version 2 über `setEntitlementPs` übermitteln kann, bei der die Operation `setEntitlementPs` gemäß A_27321-* abbricht.[<=]

A_24590-02 - Entitlement Management - Befugnis durch ein Primärsystem

Das Entitlement Management MUSS sicherstellen, dass die Befugnisvergabe durch ein Primärsystem über die Schnittstelle `I_Entitlement_Management` durch Verwendung eines

gültig signierten JWT mit den dargestellten Mindest-Inhalten erfolgt:

Befugnis	Claim Name	Claim
Protected Header		
	"typ"	"JWT"
	"alg"	"ES256" oder "PS256"
	"x5c"	Signaturzertifikat C.HCI.AUT
Payload		
	"iat"	Zeitstempel Ausgabezeitpunkt
	"exp"	Verfalldatum, = "iat" + 20 min
	"auditEvidence"	VSDM-Prüfziffer aus dem VSDM-Prüfungsnachweis, base64-kodiert.
	"hcv"	optional solange enforce_hcv_check = FALSE; Hash check value der als Ergebnis der Operation ReadVSD gemäß A_27352-* berechnet wird. Der berechnete hcv-Wert MUSS base64 kodiert werden.

[<=]

A_25249 - Entitlement Management - Befugnisverifikation einer Befugnis durch ein Primärsystem

Das Entitlement Management MUSS für ein signiertes JWT zur Befugnisvergabe durch ein Primärsystem unter Verwendung der Regeln 'rr3' (Stecken der eGK in einer Leistungserbringenumgebung) des HSM eine Befugnisverifikation durchführen. [<=]

A_24537 - Entitlement Management - Standardgültigkeitsdauer für Befugnisse

Das Entitlement Management MUSS sicherstellen, dass neue Befugnisse, die unter Verwendung der Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` erstellt werden, eine vorgegebene, rollenspezifische Befugnisdauer gemäß A_23941-* erhalten. [<=]

3.9.3 Löschen von Befugnissen

Erteilte Befugnisse werden grundsätzlich nach Erreichen des Endzeitpunkts ihrer Gültigkeit durch das Aktensystem gelöscht.

A_24504 - Entitlement Management - Löschen ungültiger Befugnisse

Das Entitlement Management MUSS vorhandene Befugnisse, deren Enddatum der Gültigkeit überschritten ist, unverzüglich aus dem Befugniskontext des Aktenkontos vollständig löschen. [<=]

Das explizite Löschen von Befugnissen innerhalb ihres Gültigkeitszeitraums kann ausschließlich durch den Versicherten oder einen Vertreter mittels eines ePA-FdV erfolgen. Es können alle erteilten Befugnisse gelöscht werden, ausgenommen die initialen Befugnisse gemäß 3.9.1- Initiale Befugnisse (static Entitlements) .

Für das Löschen von Befugnissen durch einen Vertreter gilt darüber hinaus folgende Einschränkung:

A_25246 - Entitlement Management - Löschen von Befugnissen durch einen Vertreter

Das Entitlement Management MUSS sicherstellen, dass eine erteilte Befugnis für einen Vertreter (`actorId` der Befugnis == KVN) durch einen Vertreter nur dann gelöscht werden kann, wenn die KVN des löschenden Vertreters der KVN der `actorId` der zu löschenden Befugnis entspricht. [`<=`]

Hinweis: Ein Vertreter darf nur seine eigene Befugnis löschen, nicht aber die Befugnis weiterer Vertreter.

A_25269 - Entitlement Management - Benachrichtigung des Versicherten bei Löschen einer Vertreterbefugnis durch Vertreter

Falls ein Vertreter seine eigene Vertreterbefugnis löscht MUSS das Entitlement Management für den Fall, dass für den Versicherten mindestens eine E-Mail-Adresse hinterlegt ist, den Versicherten über das Löschen der Vertreterbefugnis an alle seine hinterlegten E-Mail-Adressen informieren. [`<=`]

3.9.4 Befugnisausschluss (Blocked User Policy)

Das Entitlement Management erlaubt die Verwaltung von Widersprüchen des Versicherten oder eines Vertreters gegen die Nutzung des Aktenkontos durch spezifische Leistungserbringerinstitutionen.

Ist ein Widerspruch gegen einen bestimmten Nutzer hinterlegt, so kann für diesen keine Befugnis erstellt werden, bis dieser Widerspruch zurückgenommen wird.

Die Umsetzung dieser Widerspruchsverwaltung bzw. des Befugnisausschlusses erfolgt durch eine Policy (Blocked User Policy). Die Konfiguration dieser Policy obliegt dem Versicherten oder einem befugten Vertreter mittels ePA-FdV oder der Ombudsstelle. Einträge können der Policy hinzugefügt oder entfernt werden. Zum Zeitpunkt der Erstellung des Aktenkontos enthält die Blocked User Policy keine Einträge.

Ein Eintrag in der Policy referenziert einen bestimmten Nutzer über seinen Identifier (Telematik-Id). Die Menge der Einträge ist nicht limitiert.

Jeder Eintrag der Blocked User Policy verhindert grundsätzlich die Erstellung einer Befugnis für den referenzierten Nutzer. Erfolgt der Widerspruch (Anlegen eines neuen Eintrags) bei bestehender Befugnis für den auszuschließenden Nutzer, wird die bestehende Befugnis gelöscht.

Bei Rücknahme eines Widerspruchs gegen die Nutzung des Aktenkontos für eine bestimmte Leistungserbringerinstitution wird der entsprechende Eintrag der Policy gelöscht. Anschließend kann dieser Nutzer befugt werden.

Ein Widerspruch gegen die Nutzung des Aktenkontos kann nur für Nutzer der folgenden Nutzergruppen erfolgen.

A_24463-01 - Entitlement Management - zulässige Rollen für den Widerspruch gegen die Nutzung durch eine Leistungserbringerinstitution

Das Entitlement Management MUSS den Widerspruch gegen die Nutzung durch eine Leistungserbringerinstitution ausschließlich für Nutzer der folgenden Nutzergruppen

zulassen:

professionOID / Nutzergruppe
oid_praxis_arzt
oid_krankenhaus
oid_institution-vorsorge-reha
oid_zahnarztpraxis
oid_öffentliche_apotheke
oid_praxis_psychotherapeut
oid_institution-pflege
oid_institution-geburtshilfe
oid_praxis-physiotherapeut
oid_praxis-ergotherapeut
oid_praxis-logopaede
oid_praxis-podologe
oid_praxis-ernaehrungstherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin

[<=]

Ein Eintrag der Blocked User Policy enthält Angaben gemäß der folgenden Tabelle:
(Beispiel)

Tabelle 17: Inhalt eines Blocked User Policy Eintrags

Element	Inhalt	Beispiel
actorId	Telematik-Id	2-883110000099999
oid	professionOID	1.2.276.0.76.4.5
displayName	Name der Leistungserbringerinstitution	Zahnarztpraxis Dr. Beispiel

Element	Inhalt	Beispiel
at	Zeitpunkt des Widerspruchs (wird durch das Entitlement Management gesetzt)	2025-01-01T12:00:00Z

A_25135 - Entitlement Management - Initialisierung der Blocked User Policy

Das Entitlement Management MUSS für ein Aktenkonto eine Blocked User Policy ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policies über die Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` ermöglichen. [`<=`]

A_24514 - Entitlement Management - Keine Befugnis für von einer Befugnis ausgeschlossene Nutzer

Das Entitlement Management MUSS sicherstellen, dass für keinen durch einen Eintrag der Blocked User Policy referenzierten Nutzer eine Befugnis existiert oder erstellt werden kann. [`<=`]

A_24515 - Entitlement Management- Verschlüsselung der Einträge der Blocked User Policy

Das Entitlement Management MUSS Einträge der Blocked User Policy mit dem Befugnispersistierungsschlüssel (SecureAdminStorageKey) verschlüsseln und im Aktenkonto persistieren. [`<=`]

Die Konfiguration der Blocked User Policy erfolgt über die Schnittstelle `I_Entitlement_Management` gemäß `[I_Entitlement_Management]` durch ein ePA-FdV bzw. durch die Ombudsstelle.

A_24965 - Entitlement Management - Information über Änderungen der Blocked User Policy

Das Entitlement Management MUSS den Aktenkontoinhaber bei einer Änderung der Blocked User Policy, sofern eine E-Mail-Adresse vorliegt, mit einer E-Mail darüber informieren, dass ein Befugnisausschluss geändert wurde, wann die Änderung erfolgte und darauf hinweisen, dass nähere Informationen zur Änderung im Protokoll zu finden sind. [`<=`]

3.9.5 Mengenbegrenzung Befugnisse (Entitlement Rate Limiting)

Die Erstellung von Befugnissen durch Primärsysteme der Leistungserbringerinstitutionen wird durch das Aktensystem mengenmäßig über einen Zeitraum begrenzt. Diese Maßnahme verhindert den massenhaften Zugriff auf Aktenkonten durch Fehlbedienung seitens eines Primärsystems oder durch unzulässige Nutzung der Aktensysteme.

Die maximal zulässige Befugnismenge ist dabei so bemessen, dass die intendierte Nutzung der ePA durch Leistungserbringerinstitutionen im Versorgungsalltag nicht eingeschränkt wird. Diese maximale Befugnismenge ist pro Nutzerrolle separat festgelegt.

Jedes Aktensystem führt dazu aktensystemweit Zähler für erteilte Befugnisse aus der Umgebung der Leistungserbringer pro Telematik-ID. Die Erfassung erfolgt somit pro Leistungserbringerinstitution separat. Die Zuordnung erfolgt zur Telematik-ID der befugniserstellenden Nutzer (nicht des zu befugnenden Nutzers). Die Befugnisvergabe aus der Umgebung des Versicherten mittels ePA-FdV wird nicht erfasst und geht nicht in die Zählerstände ein.

Das Entitlement Management wertet diese Menge der erfassten Befugnisvergaben im Falle einer weiteren Befugnisvergabe durch ein Primärsystem aus der Umgebung der LEI aus

und verhindert die Befugniserstellung bei Erreichen der maximal zulässigen Befugnismenge.

Die zulässige Befugnisrate limitiert dabei einerseits die Menge der innerhalb einer Stunde erstellbaren Befugnisse, als auch die Menge der insgesamt monatlich erstellbaren. Die Zählung erfolgt aktensystemweit pro Aktensystem eines Herstellers und unabhängig vom adressierten Aktenkonto und berücksichtigt nur erfolgreiche Befugnisvergaben. Der Zeitraum pro Stunde, bzw. pro Monat, bezieht sich dabei auf den Zeitraum der aktuellen Stunde, bzw. des aktuellen Monats.

A_27311 - Entitlement Management – RateLimit-oid-List

Das Entitlement Management MUSS eine *RateLimit-oid-List* führen, in der pro oid

- der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden Befugnisse innerhalb einer Stunde,
- der Wert für die maximale Anzahl durch das Primärsystem zu registrierenden Befugnisse innerhalb eines Monats und
- der Zeitpunkt der letzten Änderung der Werte

gespeichert werden.[<=]

Initial ist die RateLimit-oid-List mit folgenden Werten zu belegen:

A_27290 - Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Stunde

Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass eine LEI mit der Rolle

- oid_praxis_arzt maximal 200 Befugnisse
- oid_krankenhaus maximal 1.000 Befugnisse
- oid_institution-vorsorge-reha maximal 1.000 Befugnisse
- oid_zahnarztpraxis maximal 200 Befugnisse
- oid_öffentliche_apotheke maximal 200 Befugnisse
- oid_praxis_psychotherapeut maximal 100 Befugnisse
- oid_institution-pflege maximal 100 Befugnisse
- oid_institution-geburtshilfe maximal 100 Befugnisse
- oid_praxis-physiotherapeut maximal 100 Befugnisse
- oid_institution-oegd maximal 100 Befugnisse
- oid_institution-arbeitsmedizin maximal 100 Befugnisse

innerhalb einer Stunde durch das Primärsystem im Aktensystem registrieren kann.

[<=]

A_27291 - Entitlement Management – RateLimit-oid-List: Maximale Anzahl von Befugnissen für LEI pro Monat

Das Entitlement Management MUSS in der *RateLimit-oid-List* sicherstellen, dass

- oid_praxis_arzt maximal 10.000 Befugnisse
- oid_krankenhaus maximal 200.000 Befugnisse
- oid_institution-vorsorge-reha maximal 200.000 Befugnisse
- oid_zahnarztpraxis maximal 10.000 Befugnisse

- oid_öffentliche_apotheke maximal 25.000 Befugnisse
- oid_praxis_psychotherapeut maximal 10000 Befugnisse
- oid_institution-pflege maximal 10000 Befugnisse
- oid_institution-geburtshilfe maximal 10000 Befugnisse
- oid_praxis-physiotherapeut maximal 10000 Befugnisse
- oid_institution-oegd maximal 10000 Befugnisse
- oid_institution-arbeitsmedizin maximal 10000 Befugnisse

innerhalb eines Monats durch das Primärsystem im Aktensystem registrieren kann.
[<=]

Hinweis zu A_27290-* und A_27291-*: Die Stunde bzw. der Tag müssen sich nicht auf die aktuelle Stunde bzw. Kalendertag beziehen, sondern können auch je Leistungserbringerinstitution auf Requestzeitpunkte bezogen werden. Dann gilt für einen Monat 30 Tage.

A_27318 - ePA-Aktensystem - RateLimit-oid-List: Maßnahmen zum Schutz der Konfiguration

Der Betreiber des ePA-Aktensystem MUSS technisch/organisatorische Maßnahmen umsetzen, die eine unautorisierte Änderung der *RateLimit-oid-List* verhindern.[<=]

A_27312 - ePA-Aktensystem - RateLimit-oid-List: Konfiguration durch Betreiber

Der Betreiber des ePA-Aktensystem MUSS sicherstellen, dass die Werte für die Anzahl der maximalen Befugnisse in der *RateLimit-oid-List* durch den Betreiber des ePA-Aktensystems ausschließlich im Vier-Augen-Prinzip konfigurierbar sind.[<=]

Stellen LEI Befugnisse mittels der Operation `setEntitlementsPs` über das Primärsystem in das ePA-Aktensystem ein, wird für diese LEI geprüft, ob diese bereits das zulässige Limit erreicht hat. Nur falls dies nicht der Fall ist, kann die Befugnis eingestellt werden. Hierzu erfasst das ePA-Aktensystem außerhalb der VAU wann ein Nutzer mit welcher Rolle eine Befugnis registriert hat. Für den Nutzer wird außerhalb der VAU ein Nutzerpseudonym geführt.

A_27313 - Entitlement Management - Prüfen der RateLimit-oid-List beim Einstellen von Befugnissen

Das Entitlement Management MUSS bei Aufruf der Operation `setEntitlementsPs` prüfen, ob für das zur LEI gehörende Nutzerpseudonym und die oid der LEI bereits das in der *RateLimit-oid-List* vorgegebene maximale Limit pro Stunde oder Monat erreicht wurde. Falls ein Limit erreicht wurde, wird die Operation `setEntitlementsPs` mit einem Fehler abgebrochen. Falls kein Limit erreicht wurde, ist die Registrierung für das zur LEI gehörende Nutzerpseudonym zu vermerken.[<=]

A_27310 - ePA-Aktensystem - Erfassung der Nutzer zur Prüfung RateLimit-oid-List

Das ePA-Aktensystem MUSS sicherstellen dass bei der Erfassung der Nutzerdaten außerhalb der VAU zur Prüfung der *RateLimit-oid-List* eine Profilierung über die Nutzer nicht möglich ist und zu diesem Zweck aus der TelematikId eines Nutzers ein Nutzerpseudonym abgeleitet wird, gemäß gemSpec_Krypt#7.5 Routing auf VAU-Instanzen.
[<=]

3.10 Legal Policy

Die Legal Policy enthält die gesetzlich verbindlichen Regelungen der Zugriffsrechte bzgl. der Berufsgruppen und Datenkategorien gemäß § 341 Absatz 2 SGB V.

Für die Datenkategorien sind die grundsätzlichen Zugriffsrechte der Zugriffsoperationen (CRUD - create, read, update, delete) vorgegeben. Diese Zugriffsrechte wirken ausnahmslos für jeden befugten Nutzer.

Beispiele sind:

- Apotheker haben keinen Zugriff auf das zahnärztliche Dokumentation in der Datenkategorie "dental".
- Kostenträger können Dokumente lediglich einstellen, also Dokumente weder lesen noch löschen.

Die Legal Policy wird durch das Aktensystem durchgesetzt und ist jederzeit vorhanden. Die Konfiguration kann durch Clients oder Bestandteile des Aktensystems nicht verändert werden.

A_19303-20 - Legal Policy – gesetzlich vorgegebene Zugriffsrechte

Das ePA-Aktensystem MUSS alle in der folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

Tabelle 18: Legal Policy

Kategorie	Nutzergruppe										
Technischer Identifier	Med	Apo	Pflege	GH	HM E	AM	KT R	O M	DiG A	eR P	Ver
Medical Services (XDS Document Service)	Zugriffsrecht gemäß § 352 SGB V										
reports	CRUD	R	R	R	R	R	-	-	-	-	RD
emp	CRUD	CRUD	R	R	R	R	-	-	-	-	RD
emergency	CRUD	R	R	R	R	R	-	-	-	-	RD
eab	CRUD	R	R	R	R	R	-	-	-	-	RD
dental	CRUD	-	R	-	-	R	-	-	-	-	RD
childsrecord	RD	R	R	RD	R	R	-	-	-	-	RD

Kategorie	Nutzergruppe										
child	CRU D	R	R	CRU D	R	R	-	-	-	-	RD (CU (*))
pregnancy_childbirth	CRU D	R	R	CRU D	R	R	-	-	-	-	RD
vaccination	CRU D	CRU D	R	R	-	CRU D	-	-	-	-	RD
patient	RD	R	R	R	R	R	C	-	-	-	CRU D
receipt	RD	RD	-	R	R	R	CU	-	-	-	RD
health_risk_analysis	-	-	-	-	-	-	C	-	-	-	RD
diga	R	R	R	R	R	R	-	-	CU	-	RD
care	CRU D	R	CRUD	R	R	R	-	-	-	-	RD
eau	CRU D	-	-	-	-	R	-	-	-	-	RD
rehab	CRU D	-	-	-	-	-	-	-	-	-	RD
transcripts	CRU D	-	-	-	-	-	-	-	-	-	RD
other	CRU D	-	-	-	-	R	-	-	-	-	RD
Medical Services (FHIR Data Service)	Zugriffsrecht										
medication	CRU D	CRU D	R	R	R	R	-	-	-	CU	R
Basic Services	Zugriffsrecht										
Consent Decisions	-	-	-	-	-	-	-	x	-	-	x
Constraints	-	-	-	-	-	-	-	-	-	-	x

Kategorie	Nutzergruppe										
Entitlements	x	x	x	x	x	x	-	-	-	-	x
Entitlements.Blocked User	-	-	-	-	-	-	-	x	-	-	x
Audit Events	-	-	-	-	-	-	-	x	-	-	x
Information	x	x	x	x	x	x	x	x	x	x	-
Devices	-	-	-	-	-	-	-	-	-	-	x

Nutzergruppen:

- Med = Arztpraxis, Zahnarztpraxis, Krankenhaus, Psychotherapeut, Vorsorge- und Rehabilitation, Öffentlicher Gesundheitsdienst
 - (oid_praxis_arzt,, oid_krankenhaus, oid_institution-vorsorge-reha, oid_zahnarztpraxis, oid_praxis_psychotherapeut oid_institution-oegd)
- Apo = Öffentliche Apotheke
 - (oid_öffentliche_apotheke)
- Pflege = Gesundheits-, Kranken- und Altenpflege
 - (oid_institution-pflege)
- GH = Geburtshilfe
 - (oid_institution-geburtshilfe)
- HME = Heilmittelerbringer
 - (oid_praxis-physiotherapeut, oid_praxis-ergotherapeut, oid_praxis-logopaede, oid_praxis-podologe, oid_praxis-ernaehrungstherapeut)
- AM = Arbeitsmedizin
 - (oid_institution-arbeitsmedizin)
- KTR = Kostenträger
 - (oid_kostentraeger)
- OM = Ombudsstelle
 - (oid_ombudsstelle)
- DiGA = Digitale Gesundheitsanwendung
 - (oid_diga)
- eRP = E-Rezept vertrauenswürdige Ausführungsumgebung
 - (oid_erp-vau)
- Ver = Versicherter / Vertreter
 - (oid_versicherter)

Legende:

- CRUD = create, read, update, delete; update: Aktualisierung von Metadaten, Aktualisierung eines Dokuments
- "-" = keine Zugriffsrechte;
- "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den Dienst (Service) definiert)
- "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung in einer zukünftigen Version der ePA vorgesehen.

Hinweise:

- (*) Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann der Versicherte bzw. sein Vertreter oder eine Leistungserbringerinstitution gemäß der zuvor genannten Liste definierter professionOIDs sein. Sofern ein Versicherter/Vertreter der Einsteller der Elternnotiz ist, darf er abweichend von den oben aufgeführten Zugriffsunterbindungsregeln in die Datenkategorie mit dem technischen Identifier 'child' schreiben.

[<=]

A_26166-02 - Legal Policy (EU) – EU-Zugriff: gesetzlich vorgegebene Zugriffsrechte

Das ePA-Aktensystem MUSS zusätzlich zu den Regeln aus A_19303-* alle in der folgenden Tabelle aufgeführten Regeln der Legal Policy bei jedem Zugriff auf Daten und Dienste des Aktenkontos durchsetzen.

Tabelle 19: Legal Policy - EU-Zugriff

Kategorie	Nutzergruppe
Technischer Identifier	NCPeH
Medical Services (XDS Document Service)	Zugriffsrecht gemäß § 352 SGB V
reports	-
emp	-
emergency	R
eab	-
dental	-
child	-
childsrecord	-
pregnancy_childbirth	-

Kategorie	Nutzergruppe
vaccination	-
patient	-
receipt	-
health_risk_analysis	-
diga	-
care	-
eau	-
rehab	-
transcripts	-
other	-
Medical Services (FHIR Data Service)	Zugriffsrecht
medication	-
Basic Services	Zugriffsrecht
Consent Decisions	-
Constraints	-
Entitlements	-
Entitlements.Blocked User	-
Audit Events	-
Information	x
Devices	-

Nutzergruppen:

- NCPeH = NCPeH-Fachdienst (oid_ncpeh)

Legende:

- CRUD = create, read, update, delete; update: Aktualisierung von Metadaten, Aktualisierung eines Dokuments
- "-" = keine Zugriffsrechte;
- "x" - grundsätzliches Zugriffsrecht (detaillierte Zugriffsausprägung wird durch den Dienst (Service) definiert)
- "nicht belegt" - diese Kategorie wird nicht verwendet und ist absichtlich unbelegt
- "reserviert für zukünftige Anwendung" - diese Kategorie ist für eine Verwendung in einer zukünftigen Version der ePA vorgesehen.

[<=]

Die folgende Tabelle erläutert die Kategorien aus A_19303-* und A_26166-*:

Tabelle 20: Beschreibung der Kategorien

Technischer Identifier	Beschreibung
Medical Services	XDS Document Service
reports	Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen
emp	Elektronischer Medikationsplan
emergency	Daten der elektronischen Notfalldaten nach § 334 Absatz 1 Satz 2 Nummer 5 und 7
eab	Daten in elektronischen Briefen zwischen den an der Versorgung der Versicherten teilnehmenden Ärzten und Einrichtungen (elektronische Arztbriefe)
dental	Daten aus der zahnärztlichen Dokumentation
child	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)
childsrecord	Archiv aus ePA 2.x: Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder)

Technischer Identifier	Beschreibung
pregnancy_childbirth	Daten gemäß der nach § 92 Absatz 1 Satz 2 Nummer 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass) sowie Daten, die sich aus der Versorgung der Versicherten mit Hebammenhilfe ergeben
vaccination	Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation)
patient	Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden
receipt	Bei Kostenträgern gespeicherte Daten über die in Anspruch genommenen Leistungen des Versicherten
health_risk_analysis	Ergebnisse datengestützter Auswertungen der Krankenkassen zu individuellen Gesundheitsrisiken gemäß SGB V § 25b.
diga	Daten des Versicherten aus digitalen Gesundheitsanwendungen des Versicherten nach § 33a.
care	Daten zur pflegerischen Versorgung des Versicherten nach den §§ 24g, 37, 37b, 37c, 39a und 39c und der Haus- oder Heimpflege nach § 44 des Siebten Buches und nach dem Elften Buch
eau	Daten nach § 73 Absatz 2 Satz 1 Nummer 9 ausgestellte Bescheinigung über eine Arbeitsunfähigkeit
rehab	Daten der Heilbehandlung und Rehabilitation nach § 27 Absatz 1 des Siebten Buches
transcripts	Elektronische Abschriften von der Patientenakte eines Primärsystems gemäß §630g Abs. 2 BGB
other	Sonstige von Leistungserbringern für Versicherten bereitgestellte Daten, insbesondere Daten, die sich aus der Teilnahme des Versicherten an strukturierten Behandlungsprogrammen bei chronischen Krankheiten gemäß § 137f ergeben
Medical Services	Medication Service
medication	Verordnungs-, Dispensier- und Medikationsdaten in einer elektronischen Medikationsliste (eML) und einem elektronischen Medikationsplan (eMP)

Technischer Identifier	Beschreibung
Basic Services	Account Management
Consent Decisions	Management der Entscheidungen zu widerspruchsfähigen Funktionen der ePA
Constraints	Management der Konfiguration der General Deny Policy
Entitlements	Management der Befugnisse für Nutzer und Nutzergruppen
Audit Events	Abruf der Protokolleinträge eines Aktenkontos
Information	Informationen für nicht befugte Nutzer
Devices	Management der registrierten Geräte eines Nutzers

A_21211-01 - Legal Policy - Änderungen der Legal Policy nicht erlauben

Das ePA-Aktensystem MUSS durch technische Maßnahmen sicherstellen, dass Änderungen der Konfiguration der Legal Policy gemäß A_19303-* ausgeschlossen sind. [<=]

A_24548 - Legal Policy - Durchsetzung der Zugriffsrechte der Legal Policy

Das ePA-Aktensystem MUSS sicherstellen, dass Operationen auf Daten und Operationen der Dienste eines Aktenkontos abgebrochen und mit einer Fehlermeldung beendet werden, wenn diese Operation durch die Vorgaben der Legal Policy gemäß A_19303-* für die Nutzergruppe des Aufrufers der Operation nicht zulässig ist. [<=]

3.11 Constraint Management

Das Constraint Management des Aktenkontos stellt sicher, dass nur Zugriffe auf Daten in Ordnern des XDS Document Service über die Vorgaben der Legal Policy hinaus zugelassen werden, welche nicht vom Versicherten oder einem Vertreter unterbunden (verborgen) wurden.

Die Umsetzung dieser Beschränkungen erfolgt anhand der **General Deny Policy** für jeden befugten Nutzer der betroffenen Nutzergruppen des Aktenkontos.

Die General Deny Policy adressiert Nutzergruppen (professionOID) und Metadaten der Daten. Es können einzelne Dokumente, Kategorien oder Ordner verborgen werden. Bei jedem Zugriff auf Daten in Ordnern wird diese Policy bezüglich der Rolle eines Nutzers und der betroffenen Dokumente ausgewertet und durchgesetzt.

Die folgende Anforderung zeigt eine Übersicht der Nutzergruppen, für welche Dokumente durch Einträge in der General Deny Policy vor einem Zugriff verborgen werden können.

A_24306-02 - Constraint Management - Policy für berechnigte Nutzergruppen und Nutzer

Das Constraint Management MUSS die Konfiguration der General Deny Policy auf die folgenden Nutzergruppen einschränken:

Nutzergruppe [professionOID] der General Deny Policy
oid_praxis_arzt
oid_krankenhaus
oid_institution-vorsorge-reha
oid_zahnarztpraxis
oid_öffentliche_apotheke
oid_praxis_psychotherapeut
oid_institution-pflege
oid_institution-geburtshilfe
oid_praxis-physiotherapeut
oid_institution-oegd
oid_institution-arbeitsmedizin
oid_diga
oid_praxis-ergotherapeut
oid_praxis-logopaede
oid_praxis-podologe
oid_praxis-ernaehrungstherapeut

[<=]

A_24390-01 - Constraint Management- Anwendung der General Deny Policy

Das Constraint Management MUSS bei jedem Zugriff auf Daten durch den XDS Document Service durch befugte Nutzer oder Nutzergruppen die General Deny Policy anwenden und den Zugriff verhindern, wenn ein Dokument oder dessen assoziierter Ordner oder dessen assoziierte Datenkategorie in der Policy konfiguriert ist.

[<=]

Dienste des Aktenkontos (Basic Services) können nicht verborgen werden. Hier gelten die Zugriffsregelungen gemäß Legal Policy und die Beschränkungen der Schnittstellen.

Datendienste (Medication Service) können nicht auf Daten- oder Ordner Ebene verborgen werden. Hier gelten die Regelungen bezüglich des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA (siehe 3.8- Consent Decision Management).

Die Kategorie "emp", bzw. einzelne Dokumente dieser Kategorie, des XDS Document Service dürfen nicht verborgen werden. Die Nutzung der Dokumente der Kategorie "emp" wird über das Consent Decision Management, bzw. einen erteilten Widerspruch gegen die widerspruchsfähige Funktion "medication" der ePA verhindert (siehe 3.8- Consent Decision Management).

Die Operationen der Schnittstelle des Constraint Managements erlauben die Konfiguration der General Deny Policy durch den Versicherten oder einen befugten Vertreter.

A_24395 - Constraint Management - Realisierung der Schnittstelle

I_Constraint_Management_Insurant

Das Constraint Management MUSS die Operationen der Schnittstelle

I_Constraint_Management_Insurant gemäß [I_Constraint_Management_Insurant] umsetzen.[<=]

A_24887-01 - Constraint Management - Protokolleinträge für Zugriffe auf das Constraint Management

Das Constraint Management MUSS für das Aufnehmen und Löschen von Einträgen in die General Deny Policy jeweils einen Protokolleintrag gemäß A_24704* erzeugen. Dabei ist folgende Wertbelegung zu berücksichtigen:

Tabelle 21: Constraint Management Protokollierung

Strukturelement	Wert		Erläuterung
AuditEvent.type	"rest"		Bei Änderungen über die API
	"object"		Bei intern ausgelösten Änderungen (XDS Document Service confidentiality code ("CON"), Löschen von Dokumenten oder Ordnern)
AuditEvent.action	C, D		
AuditEvent.entity.name	"GeneralDenyPolicy"		Eintrag für das Aufnehmen(Create) von Einträgen in die oder Löschen (Delete) von Einträgen aus der General Deny Policy
AuditEvent.entity.detail	type	value[x]	

Strukturelement	Wert		Erläuterung
	"DocumentTitle"	<XDSDocumentEntry.title>	wenn sich der Eintrag (Create oder Delete) der Policy auf ein Dokument bezieht
	"RootDocumentId"	<rootDocumentId>	wenn sich der Eintrag (Create oder Delete) der Policy auf ein Dokument bezieht
	"FolderTitle"	<XDSFolder.title>	wenn sich der Eintrag (Create oder Delete) der Policy auf einen Folder bezieht
	"FolderEntryUUID"	<Folder.entryUUID>	wenn sich der Eintrag (Create oder Delete) der Policy auf einen Folder bezieht
	"CategoryId"	<categoryId>	wenn sich der Eintrag (Create oder Delete) der Policy auf eine Kategorie bezieht

[<=]

Für die Policy gelten folgende Vorgaben.

A_24393-01 - Constraint Management - Initialisierung der General Deny Policy

Das Constraint Management MUSS für ein Aktenkonto eine General Deny Policy ohne initiale Einträge, bereitstellen und die Konfiguration der Einträge der Policy über die Schnittstelle `I_Constraint_Management_Insurant` gemäß

[`I_Constraint_Management_Insurant`] ermöglichen. [<=]

A_24462-01 - Constraint Management - Konfiguration der General Deny Policy anpassen nach Löschen von Ordnern

Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn diese einen Ordner referenzieren und dieser Ordner aus dem Aktenkonto gelöscht wird. [<=]

A_24461-01 - Constraint Management - Konfiguration der General Deny Policy anpassen nach Löschen von Dokumenten

Das Constraint Management MUSS Einträge aus der General Deny Policy entfernen, wenn diese ein spezifisches Dokument referenzieren und dieses Dokument aus dem Aktenkonto gelöscht wird. [<=]

A_24516-01 - Constraint Management - Speichern der Inhalte der General Deny Policy

Das Constraint Management MUSS Einträge aus der General Deny Policy unter Verwendung des SecureDataStorageKeys gesichert im Aktenkonto ablegen. [≤]

3.11.1 Aktenkontoweites Verbergen (General Deny Policy)

Die General Deny Policy wird durch das Aktensystem für die in A_24306-* unter "General Deny Policy" aufgeführten Nutzergruppen angewendet und durchgesetzt. Einträge der General Deny Policy gelten dabei immer für alle aufgeführten Nutzergruppen gemeinsam.

Die Konfiguration der General Deny Policy erfolgt durch den Versicherten oder einen befugten Vertreter mittels ePA-FdV. Einträge können hinzugefügt oder entfernt werden. Zum Zeitpunkt der Erstellung des Aktenkontos enthält die General Deny Policy keine Einträge.

Ein Eintrag in der General Deny Policy referenziert entweder ein bestimmtes Dokument, einen dynamischen Ordner oder eine Datenkategorie. Die Menge der Einträge ist nicht limitiert.

Jeder Eintrag der General Deny Policy verbirgt die betroffenen Daten und verhindert deren Nutzung durch Nutzergruppen gemäß A_24306-*. Enthält ein Eintrag der Policy einen dynamischen Ordner oder eine Kategorie, so werden alle in diesem Ordner bzw. Kategorie enthaltenen Daten verborgen und von der Nutzung ausgeschlossen. Ein dynamischer Ordner selbst wird ebenfalls verborgen und von der Nutzung ausgeschlossen, eine Kategorie selbst wird nicht verborgen. Verborgene Daten schränken die Anwendung der Datenoperationen ein, die konkreten Auswirkungen sind bei den jeweiligen Operationen definiert.

Beim kategorienbasierten Verbergen von dynamischen Ordnern kann ein einzelner Ordner oder die Datenkategorie an sich verborgen werden. In letzterem Fall werden alle assoziierten Ordner verborgen.

Bei Kategorien und Ordnern, die zusammengesetzte MIOs oder strukturierte Dokumente enthalten (MIOs oder strukturierte Dokumente, deren Inhalt über mehrere XDS Dokumente mit Zusammenhang verteilt ist - "Passdokumente") ist das Verbergen einzelner XDS Dokumente des MIOs nicht sinnvoll und daher nicht zulässig. In diesen Fällen erfolgt das Verbergen der Daten durch das Verbergen der Kategorie bzw. des dynamischen Ordners. Diese Einschränkung betrifft die Sammlungstypen "mixed" und "uniform".

Für das erfolgreiche Verbergen von Daten durch Einträge der General Deny Policy muss das adressierte XDS Dokument, der Ordner oder die Kategorie im Aktensystem vorhanden sein. Wird im Verlauf von Operationen ein XDS Dokument oder ein Ordner gelöscht, so werden auch die referenzierenden Policy-Einträge automatisch entfernt (siehe A_24461-* und A_24662-*).

Ein Eintrag der General Deny Policy enthält Angaben gemäß der folgenden Tabelle:

Tabelle 22: Inhalt eines General Deny Policy Eintrags

Element		Inhalt	Erläuterung
denyType		"document" oder "folder" oder "category"	Art des zu verbergenden Inhalts,

Element		Inhalt	Erläuterung
parameter:			eine technische Referenz passend zu "denyType"
[choice]	rootDocumentId	documentEntry.referenceIdList, Item "rootDocumentUniqueId"	Identifiziert das zu verbergende XDS Dokument
	folderUUID	folder.entryUUID	Identifiziert das zu verbergende dynamische Ordner
	categoryId	categoryId	technischer Identifizierer der zu verbergenden Kategorie

Beispiel:

Tabelle 23: Verbergen eines Medical Service

General Deny Policy - Verbergen der Datenkategorie "dental" (Daten aus der zahnärztlichen Dokumentation)		
denyType		"category"
parameters:		
	categoryId	"dental"

3.11.1.1 Aktenkontoweites Verbergen durch Verwendung des confidentialityCodes

Das Verbergen über den confidentialityCode ist im Kontext der Operationen des XDS Document Service definiert und in 3.13.1.10- Verbergen von Dokumenten durch Verwendung des confidentialityCode beschrieben.

3.12 Device Management

Die Geräteverwaltung ermöglicht ePA-FdVs die Registrierung und Verwaltung der vom Nutzer verwendeten Geräte. Das Device Management stellt das API zum ePA-FdV für die Geräteverwaltung bereit und ist nur in einer VAU/authentisierten User Session erreichbar.

Im Folgenden wird als **Home-AS** eines Versicherten das ePA-Aktensystem desjenigen Betreibers bezeichnet, der vom Kostenträger des Versicherten beauftragt wurde. Falls der Versicherte der Anlage eines Aktenkontos nicht widersprochen hat, wird sein Aktenkonto im Home-AS verwaltet. Im Falle von Vertretern kann es vorkommen, dass das Home-AS des zu vertretenden Versicherten nicht das Home-AS des Vertreters ist.

Die E-Mail-Adressen und die Geräte eines Versicherten werden ausschließlich im Home-AS des Versicherten verwaltet. Für Vertreter, deren Home-AS nicht das Home-AS des Versicherten ist, können im Home-AS des Versicherten die im Home-AS des Vertreters registrierten Geräte nachgenutzt werden. Das ePA-Aktensystem bietet dem ePA-FdV eine Schnittstelle, über die die durch das Home-AS signierte Geräteinformationen abgerufen werden können.

Bei erstmaliger Nutzung des Gerätes initiiert das ePA-FdV die Geräteregistrierung und erhält dadurch eine DeviceID (bestehend aus deviceIdentifier und deviceToken), welche bei folgenden Verwendungen des ePA-FdV zur Identifizierung des Geräts verwendet wird. Eine neue Geräteregistrierung muss durch den Nutzer bestätigt werden. Der Zugriff auf ein Aktenkonto kann nur mit einem Gerät mit bestätigter Geräteregistrierung erfolgen.

Das Device Management ermittelt dazu die für den Nutzer im ePA-Aktensystem hinterlegte E-Mail-Adresse und versendet bei der Geräteregistrierung eine E-Mail an den Nutzer mit einem generierten Geräteregistrierungscode (confirmationCode). Der Nutzer sendet den Geräteregistrierungscode unter Verwendung des ePA-FdV zurück an das Device Management und bestätigt dadurch die Registrierung des neuen Geräts. Das Gerät kann nach der Bestätigung uneingeschränkt mit einem Aktenkonto genutzt werden.

A_24828 - Device Management - Realisierung der Schnittstelle

I_Device_Management_Insurant

Das Device Management MUSS die Operationen der Schnittstelle

`I_Device_Management_Insurant` gemäß `[I_Device_Management_Insurant]` umsetzen. [`<=`]

A_25164 - Device Management - Beschränkung der Schnittstellenoperationen auf Geräte des Nutzers

Das Device Management MUSS die Operationen der Schnittstelle

`I_Device_Management_Insurant` gemäß `[I_Device_Management_Insurant]` auf die Geräte des aufrufenden Nutzers einschränken. [`<=`]

A_26153 - Device Management - Nutzen von Device Management auch bei Widerspruch gegen Aktenkonto

Das Device Management MUSS sicherstellen, dass das Device Management auch von Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben. [`<=`]

A_26154 - ePA-Aktensystem - Ausschließlich Nutzen von Email Management und Device Management bei Widerspruch

Das ePA-Aktensystem MUSS sicherstellen, dass Versicherte, die einem Aktenkonto widersprochen haben, ausschließlich das Email Management und das Device Management nutzen können. [`<=`]

A_26155 - Device Management - Versicherte nutzen Device Management ausschließlich im Home-AS

Das Device Management des ePA-Aktensystems MUSS sicherstellen, dass das Device Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-Aktensystem das Home-AS ist. [`<=`]

A_24979 - Device Management - Sicheres Löschen von Geräten

Das Device Management MUSS beim Entfernen eines Gerätes sicherstellen, dass das Gerät gelöscht ist und dass das Gerät nicht mehr als verifiziertes Gerät genutzt werden kann. [\leq]

A_17947-03 - Device Management - Gültigkeitszeitraum und Löschung der Devicekennung

Das Device Management MUSS jede generierte und zu einem Nutzer gespeicherte Geräteregistrierung nach 2 Jahren löschen und darf Nutzeranfragen mit dieser Device-Kennung nach diesem Zeitpunkt nicht mehr akzeptieren. [\leq]

Hinweis zu A_17947-*: Der Hersteller des ePA-FdVs kann die Nutzerführung seines ePA-FdVs so gestalten, dass der Versicherte auf ein baldiges Auslaufen der Registrierung hingewiesen wird und automatisch eine neue Registrierung vom ePA-FdV am Aktensystem ausgelöst wird.

A_14595-02 - Device Management - Pflegeprozess Geräteverwaltung

Das Device Management MUSS die interne Liste aller bekannten Geräte derart pflegen, dass ein Gerät nach spätestens 1 Jahr nach der letzten Nutzung des Gerätes automatisch aus der Liste der registrierten Geräte gelöscht wird. [\leq]

Hinweis zu A_14595-*: Der Abruf einer Device Attestation durch ein registriertes Gerät gilt ebenfalls als eine Nutzung dieses Geräts.

A_25270 - Device Management - Erzeugung von Geräteinformationen und Geräteregistrierungscode bei der Geräteregistrierung

Das Device Management MUSS bei der Geräteregistrierung für das zu registrierende Gerät eines Nutzers

- einen deviceIdentifizier als aktensystemweit eindeutigen Gerätebezeichner (uuid),
- ein deviceToken als eine Zufallszahl als String mit 64 Zeichen mit einer Mindestentropie von 120 Bit gemäß [gemSpec_Krypt#GS-A_4367] und
- eine zufällige sechsstellige natürliche Zahl als Geräteregistrierungscode

erzeugen. [\leq]

A_25271-01 - Device Management - Speicherung der Geräteinformationen

Das Device Management MUSS bei einer Geräteregistrierung eines Geräts eines Nutzers folgende Inhalte für den Nutzer verschlüsselt persistieren:

- deviceIdentifizier
- deviceToken
- createdAt (Zeitpunkt der Erzeugung des deviceTokens)
- lastUse
- status
- displayName
- Geräteregistrierungscode,
- Fehlerzähler.

[\leq]

Hinweis zu A_25271-*: Für die verschlüsselte Speicherung der Geräteinformationen sind die Anforderungen aus Abschnitt 3.5.1.3 zu berücksichtigen.

A_25272 - Device Management - Pseudonyme Speicherung der Geräteinformationen

Das Device Management MUSS sicherstellen, dass die Zuordnung der außerhalb der VAU persistierten verschlüsselten Geräteinformationen zum Nutzer eindeutig ist und durch ein Pseudonym erfolgt. [≤]

Hinweis: Aus A_25272 folgt, dass die Zuordnung der Speicherung der verschlüsselten Geräteinformationen nicht über die KVN-R des Nutzers erfolgen darf.

A_25273 - Device Management - Gültigkeitsdauer des Geräteregistrierungscodes

Das Device Management MUSS sicherstellen, dass der bei der Geräteregistrierung erzeugte Geräteregistrierungsscode maximal 6 Stunden nach Erzeugung der DeviceID (createdAt) für die Verifikation eines Gerätes genutzt werden kann. [≤]

A_25274 - Device Management - Löschen nach Gültigkeitsdauer des Geräteregistrierungscodes

Das Device Management MUSS sicherstellen, dass die Geräteinformationen für eine nicht bestätigte Geräteregistrierung nach Ende der Gültigkeitsdauer des Geräteregistrierungscodes gelöscht werden. [≤]

A_25275 - Device Management - Versenden des Geräteregistrierungscodes per E-Mail

Das Device Management MUSS bei der Geräteregistrierung für den Nutzer, für den das Gerät registriert werden soll, alle im Aktensystem hinterlegten E-Mail-Adressen ermitteln und an alle ermittelten E-Mail-Adressen eine E-Mail in einer für den Nutzer verständlichen Form mit folgenden Informationen versenden:

- Zweck der E-Mail,
- Geräteregistrierungsscode,
- Gültigkeitsdauer des Geräteregistrierungscodes.

[≤]

A_25276 - Device Management - Bestätigung mittels Geräteregistrierungscodes

Das Device Management MUSS für einen übergebenen Geräteregistrierungsscode und eine übergebene DeviceID (deviceIdentifier und deviceToken) prüfen, ob der vom Device Management bei der Geräteregistrierung erzeugte Geräteregistrierungsscode für das angegebene Gerät (deviceIdentifier, deviceToken) mit dem übergebenen Geräteregistrierungsscode übereinstimmt sowie der Geräteregistrierungsscode zeitlich gültig ist und

1. bei Gleichheit und
 - a. zeitlicher Gültigkeit
 - den Status für die Geräteregistrierung wechseln, so dass die erfolgreiche Bestätigung des Geräts aus dem Status hervorgeht,
 - den Geräteregistrierungsscode und den Fehlerzähler aus den Geräteinformationen löschen und
 - den Zeitpunkt der erfolgreichen Bestätigung in lastUsed erfassen,
 - b. zeitlicher Ungültigkeit
 - alle Geräteinformationen zu diesem deviceIdentifier löschen,
2. bei Ungleichheit den Fehlerzähler der Geräteinformation um eins erhöhen und

- falls der Fehlerzähler größer oder gleich fünf ist,
 - alle Geräteinformationen zu diesem Gerät löschen.

[<=]

A_25277 - Device Management - Sperrung bei vermehrter Anzahl von abgebrochenen Geräteregistrierungen

Falls für einen Nutzer innerhalb von 8 Stunden drei Geräteregistrierungen abgebrochen werden mussten, MUSS das Device Management sicherstellen, dass dieser Nutzer für 8 Stunden ab dem Zeitpunkt der dritten abgebrochenen Geräteregistrierung keine Geräte mehr registrieren darf.[<=]

A_25291 - ePA-Aktensystem - Health Record Context nur mit verifizierten Gerät

Das ePA-Aktensystem MUSS sicherstellen, dass ein Versicherter (auch wenn er als Vertreter agiert) einen Health Record Context ausschließlich mit einem verifizierten Gerät öffnen kann, außer für den Fall, dass sich der Versicherte am ePA-FdV des Vertreters anmeldet (d.h. `x-authorize-representative=True` bei der Operation `I_Authorization_Service::sendAuthorizationRequestFdV`).[<=]

Eine Geräteregistrierung im Home-AS kann in einem anderen Aktensystem nachgenutzt werden. Hierzu kann ein ePA-FdV mittels `getDeviceAttestation` eine Device Attestation vom Home-AS abrufen, welche beim anderen Aktensystem genutzt werden kann.

A_26157 - Device Management - Device Attestation kann nur mit verifiziertem Gerät abgerufen werden

Das Device Management MUSS sicherstellen, dass die Operation `getDeviceAttestation` ausschließlich nach erfolgreicher Authentifizierung des Nutzers und mit einem auf den Nutzer registrierten und verifizierten Gerät erfolgt.

[<=]

A_26156 - Device Management - Inhalte der Device Attestation

Das Device Management MUSS sicherstellen, dass eine von einem ePA-FdV über die Operation `getDeviceAttestation` abgerufene Device Attestation folgende Inhalte enthält:

Attribut	Inhalt
actorId	KVNR aus dem ID-Token des angemeldeten Nutzers (bzw. der User Session)
iat	Zeitstempel Ausgabezeitpunkt
exp	Verfalldatum, = "iat" + 2 Stunden

[<=]

A_26158 - Device Management - Signatur der Device Attestation

Das Device Management MUSS sicherstellen, dass die über `getDeviceAttestation` abgerufene Device Attestation mit dem privaten Schlüssel der Signaturidentität der VAU des Home-AS signiert wird.[<=]

3.13 Medical Services

A_25830-02 - Medical Services - Reihenfolge der Auswertung Legal Policy, Consent Decisions und Constraints

Die Medical Services MÜSSEN bei der Ausführung von Operationen der Schnittstellen der Medical Services sicherstellen, dass die Prüfung zu Bedingungen

1. der Einschränkung der Rolle des Aufrufenden (oid),
2. der Existenz des Aktenkontos (Status UNKNOWN oder INITIALIZED),
3. des Zustands des Aktenkontos (Status ACTIVATED),
4. der Befugnis des Aufrufenden,
5. der Legal Policy,
6. der Entscheidungen zu widerspruchsfähigen Funktionen der ePA,
7. der Einträge der General Deny Policy
8. des Entscheidungen zum nutzerspezifischen Ausschluss von der Teilnahme am digital gestützten Medikationsprozess

in der dargestellten Reihenfolge erfolgt. Diese Reihenfolge MUSS auch eingehalten werden, wenn einzelne Prüfungen für eine Operation nicht anwendbar, bzw. nicht relevant, sind. [\leq]

Hinweis: Eine Operation kann nicht erfolgreich ausgeführt werden, weil dieses der Legal Policy widerspricht und weil ein Eintrag der General Deny Policy die Ausführung verhindert. Die Fehlermeldung zum Abbruch der Operation resultiert dann aus der Prüfung der Legal Policy, da die Bedingungen dieser gemäß der definierten Reihenfolge vor den Bedingungen der General Deny Policy geprüft werden müssen.

3.13.1 XDS Document Service

Die gesetzlichen Vorgaben schränken den Zugriff Dritter auf Dokumente über berufsgruppenspezifische Vorgaben gemäß § 341 Absatz 2 SGB V ein. Dazu verwendet der XDS Document Service festgelegte Datenkategorien, welche mit spezifischen Zugriffsrechten der grundlegenden Zugriffsoperationen (CRUD - create, read, update, delete) wirken.

Jedes eingestellte Dokument wird vom XDS Document Service mit einer automatischen Zuordnung zu einem statischen Ordner, welcher die Datenkategorie repräsentiert, erweitert. Diese statischen Ordner sind initial bei jedem Aktenkonto eines Versicherten existent. Die serverseitige Zuordnung in diese Ordner erfolgt anhand der XDS-Metadaten in Kombination mit der Nutzergruppe des Einstellers.

Das bedeutet weiterhin, dass das Anlegen von statischen Ordnern durch ePA-Clients nicht erlaubt ist, um eine zweifelsfreie Anwendung der Zugriffsregeln auf Grundlage der Datenkategorien zu gewährleisten.

Eine Ausnahme bilden bestimmte medizinische Informationsobjekte (MIOs), die eine weitere Gruppierung innerhalb der zugeordneten Datenkategorie erfordern. Ein Beispiel dafür ist der Mutterpass. Die Dokumente eines Mutterpasses müssen für die konkrete Schwangerschaft innerhalb der Kategorie separiert werden. Für die betroffenen Kategorien wird daher kein statischer Ordner vorbereitet, sondern der separierende, dynamische Ordner muss zeitgleich mit einer Dokumentenregistrierung durch den ePA-Client angelegt werden,

ePA-Clients, die Dokumente für MIOs einstellen, können die dem MIO zugeordnete Kategorie und die Art des Ordners (statisch, dynamisch) aus den Metadatenvorgaben für MIOs gemäß [Implementation-Guidelines] entnehmen.

Die Durchsetzung der Zugriffskontrolle auf die Kategorien, Ordner und Dokumente gemäß der gesetzlichen Vorgaben und ggf. weiterer Beschränkungen durch den

Versicherten oder einen Vertreter erfolgt durch das Constraint Management (siehe 3.11-Constraint Management).

3.13.1.1 Formatprüfung beim Einstellen von Dokumenten

A_25233 - XDS Document Service - erlaubte Formate für PDF-Dokumente

Der XDS Document Service MUSS sicherstellen, dass ausschließlich die folgenden PDF/A-Formate unterstützt werden:

- PDF/A-1a
- PDF/A-1b
- PDF/A-2a
- PDF/A-2u
- PDF/A-2b

[<=]

A_24864-04 - XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten

Der XDS Document Service MUSS beim Einstellen eines Dokumentes prüfen, dass das Dokument eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und den in Klammern angegebenen Dateiendungen (DocumentEntry.URI) besitzt

- application/pdf nur PDF/A gemäß A_25233 (pdf)
- text/plain (txt)
- application/xml (xml)
- application/hl7-v3 (xml)
- application/pkcs7-mime (p7s oder p7)
- application/fhir+xml (xml)
- application/fhir+json (json)
- application/json (json)

sowie der tatsächliche Inhalt des Dokuments konform mit dem behaupteten MIME-Type ist. Falls die Prüfung nicht erfolgreich ist, muss das Einstellen des Dokumentes abgelehnt werden.[<=]

Hinweise zu A_24864-:*

- *Dokumente im PDF-Format werden vom XDS Document Service abgelehnt, da sie ausführbaren Code enthalten können. Daher müssen die Clients, falls sie Dokumente im PDF-Format einstellen wollen, diese zunächst in ein PDF/A konvertieren.*
- *p7s ist die Default-Dateiendung für Dokumente des mimetypes application/pkcs7-mime in der ePA und für Dokumente dieses mimetypes gemäß [gemSpec_IG_ePA] und für automatisierte Anpassungen von filename extensions bei Dokumentenupload (A_23447-*, A_24451-*) zu berücksichtigen.*

A_25009-03 - XDS Document Service - Prüfen auf zulässiges Format beim Einstellen von Dokumenten durch Versicherte

Der XDS Document Service MUSS sicherstellen, dass Versicherte ausschließlich Dokumente eines der folgenden MIME-Type-Formate (DocumentEntry.mimeType) und den in Klammern angegebenen Dateiendungen (DocumentEntry.URI) einstellen können:

- application/pdf nur PDF/A gemäß A_25233 (pdf)
- text/plain (txt)
- application/fhir+xml (xml)
- application/json (json)

Ferner MUSS der XDS Document Service sicherstellen, dass ausschließlich die Elternnotiz des Kinderuntersuchungshefts als FHIR Document mit dem MIME-Type "application/fhir+xml" registriert werden kann - andere FHIR Documents sind nicht zulässig.

[<=]

Hinweise zu A_24864- und A_25009-*: Die Prüfung des zulässigen Dokumentenformats muss mindestens*

- *bei allen Formaten eine Prüfung auf Magic Bytes (soweit technisch möglich),*
- *bei txt-, XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es bei XML-Dokumenten kein valides UTF8 ist, prüfen auf "restriktives" ISO-8859-15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09, 0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind.",*
- *bei XML-, und JSON-Dokumenten eine Prüfung der XML- bzw. JSON-Validität mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet sind,*
- *auf den signierten Inhalt eines PKCS7-Dokuments sind die Regeln ebenfalls anzuwenden*

umfassen. Eine alleinige Prüfung auf Basis der Magic Bytes ist für kein Format ausreichend. Werden keine zusätzlichen Prüfmaßnahmen durchgeführt, dürfen die Dokumente nicht in die Akte eingestellt werden können.

Für XML-Dokumente muss eine Schema-Validierung ausschließlich auf Basis bekannter, intern vorliegender XML Schema-Definitionen durchführen. Gegen nicht intern vorliegende XML Schema-Definitionen wird nicht validiert. Die Schema-Validierung kann innerhalb des Health Record Contexts ohne zusätzliche Isolation erfolgen.

A_24867 - XDS Document Service - Isolation der Formatprüfung

Der XDS Document Service MUSS die Prüfung des Dateiformats (siehe A_24864-*) beim Einstellen eines Dokuments so technisch isolieren, dass kein Schaden für Aktenkonten oder das ePA-Aktensystem selbst entsteht.

[<=]

Hinweise zu A_24867-:*

Hier kann z.B. eine Art Sandboxing oder eine separate VAU-Instanz verwendet werden, um die Isolation umzusetzen.

Der in A_24636- geforderte technische Separationsmechanismus zur Isolation von Health Record Contexten innerhalb einer VAU-Instanz kann ebenfalls zur Isolation der Formatprüfung in A_24867-* genutzt werden.*

Findet eine Dokumentenformatprüfung innerhalb eines Health Record Context statt, wird durch den Isolationsmechanismus aus A_24636- verhindert, dass sich die*

Dokumentenformatprüfung schadhaft auf andere Health Record Contexte auswirkt. Es verbleibt dann zur Umsetzung der A_24867- noch zu gewährleisten, dass sich die Dokumentenformatprüfung nicht schadhaft auf den Health Record Context auswirkt, in dem die Dokumentenformatprüfung erfolgt.*

Wenn Dokumentenprüfungen innerhalb eines Health Record Contexts ohne Isolation erfolgen, muss sichergestellt werden, dass sich diese Prüfungen nicht schadhaft auf den Health Record Context (oder andere) auswirken können. Dies ist vom Produktgutachter zu prüfen und im Produktgutachten zu dokumentieren.

Ein Ausschluss einer schadhaften Auswirkung auf den Health Record Context ist bei folgenden Prüfungen des Dokumentenformats denkbar, so dass diese innerhalb des Health Record Contexts ohne zusätzliche Isolationsmaßnahmen durchgeführt werden können und kein Verstoß gegen die Anforderung A_24867- vorliegt:*

- *Prüfung der Magic Bytes des Dokuments (wo technisch möglich)*
- *bei txt-, XML-, und JSON-Dokumenten eine Prüfung auf UTF8-Validität. Falls es bei XML-Dokumenten kein valides UTF8 ist, eine Prüfung auf "restriktives" ISO-8859-15. Restriktives ISO-8859-15 heißt, dass die Zeilen 0 (bis auf 0x09, 0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind."*
- *bei XML- und JSON-Dokumenten: Parsen der Dokumente auf valides XML bzw. JSON mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu bestätigen.*
- *bei pkcs7-Dokumenten: Parsen der Dokumente mit Parsern, die entsprechend den Sicherheitsempfehlungen konfiguriert und gehärtet sind. Die Härtung der Parser ist durch den Produktgutachter zu bestätigen.*

Der Produktgutachter muss bei der Umsetzung der oben genannten Prüfungen bestätigen, dass der Ausschluss einer schadhaften Auswirkung auf den Health Record Context (oder andere) durch die Umsetzung im Produkt tatsächlich gegeben ist.

A_25285 - XDS Document Service - Sicheres Löschen von Dokumenten mit unzulässigem Format

Falls der XDS Document Service bei der Prüfung des Dateiformats (siehe A_24864-*) beim Einstellen eines Dokuments ein unzulässiges Format erkennt, MUSS der XDS Document Service das Dokument sicher löschen.

[<=]

A_24943 - XDS Document Service - Formatprüfung exponiert keine Daten aus der VAU heraus

Der XDS Document Service MUSS sicherstellen, dass bei der Formatprüfung (siehe A_24864-*) keine innerhalb der VAU verarbeiteten Daten die VAU verlassen.[<=]

3.13.1.2 Anforderungen zur Validierung

A_15035 - XDS Document Service – Verwendung von SOAP Message Security 1.1

Der XDS Document Service MUSS die Sicherheitsanforderungen aus SOAP Message Security 1.1 [WSS] für die Verarbeitung von SOAP 1.2-Nachrichten umsetzen.[<=]

A_15034 - XDS Document Service – Unterstützung von Profilen der Web Services Interoperability Organization (WS-I)

Der XDS Document Service 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. [≤]

A_15186 - XDS Document Service – Prüfung der Kombination von WS-Addressing Action und SOAP Body

Der XDS Document Service 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 der XDS Document Service die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und die Verarbeitung der Nachricht abbrechen. [≤]

A_15585 - XDS Document Service – Gleichheit von SOAP Action und WS-Addressing Action

Der XDS Document Service MUSS SOAP 1.2-Eingangsnachrichten mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren und die Verarbeitung der Nachricht abbrechen, falls die Werte aus SOAP Action (HTTP Header) und des `Action`-Elements [WSA] des SOAP Headers nicht übereinstimmen. [≤]

A_14465-01 - XDS Document Service – XML Schema-Validierung für SOAP-Eingangsnachrichten

Der XDS Document Service MUSS vor einer Weiterverarbeitung sämtliche SOAP 1.2-Eingangsnachrichten einer XML Schema-Validierung auf Basis ausschließlich intern vorliegender XML Schema-Definitionen unterziehen und gemäß [SOAP] verarbeiten. Sind Nachrichten nicht wohlgeformt oder ungültig, MUSS der XDS Document Service die Nachricht mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren. [≤]

A_14809 - XDS Document Service – Keine Verwendung des "xsi:schemaLocation"-Attributs

Der XDS Document Service 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_14811-01 - XDS Document Service – Ablehnung von SOAP 1.2-Nachrichten ohne UTF-8 Kodierung

Der XDS Document Service MUSS SOAP 1.2-Nachrichten dahingehend prüfen, dass diese der Zeichenkodierung UTF-8 entsprechen, und andernfalls die Operation einem geeigneten HTTP-Statuscode gemäß [RFC7231] ablehnen. [≤]

A_21200 - XDS Document Service und Clients – UTF-8 Kodierung von SOAP 1.2-Nachrichten

Der XDS Document Service und Clients des XDS Document Service MÜSSEN sicherstellen, dass die XML-Inhalte der SOAP 1.2-Nachrichten, die sie senden, der Zeichenkodierung UTF-8 entsprechen. [≤]

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

3.13.1.3 Namensräume

Für die Spezifikation der Schnittstellen des XDS Document Service 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
wsa	http://schemas.xmlsoap.org/ws/2004/08/addressing
wss	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
xdsb	urn:ihe:iti:xds-b:2007
xs	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance

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

3.13.1.4.1 Anforderungen an IHE ITI-Akteure

In diesem Abschnitt werden Anforderungen und Einschränkungen an relevante IHE ITI-Akteure und -Transaktionen des XDS Document Service 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 [3.13.1.4.2-Überblick über gruppierte IHE ITI-Akteure und Optionen](#) zu entnehmen.

Hinweis: Alle spezifizierten Anforderungen der IHE ITI-Akteure definieren das zu implementierende Verhalten an den Außenschnittstellen `I_Document_Management` sowie `I_Document_Management_Insurant`.

A_17826-01 - XDS Document Service – Außenverhalten der IHE ITI-Implementierung

Der XDS Document Service DARF NICHT vom Verhalten der definierten Außenschnittstellen

I_Document_Management, sowie I_Document_Management_Insurant aus Abschnitt 3.13.1.6 abweichen. Dies schließt über die Anforderungslage hinausgehende Implementierungen von IHE ITI-Akteuren und Optionen innerhalb des XDS Document Service mit ein, sodass zusätzlich implementierte IHE-Funktionalitäten keine Auswirkungen an den definierten Außenschnittstellen aufweisen dürfen. [≤]

A_13806 - XDS Document Service – Implementierung des IHE ITI-Akteurs XDS Document Registry

Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Registry" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14727 - XDS Document Service – Implementierung des IHE ITI-Akteurs XDS Document Repository

Der XDS Document Service MUSS den IHE ITI-Akteur "XDS Document Repository" 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 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs ATNA Audit Record Repository

Der XDS Document Service 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" (siehe 3.5- Vertrauenswürdige Ausführungsumgebung (VAU)) umgesetzt, sodass die Nutzung des Integrationsprofils ATNA diesbzgl. eingeschränkt wird.

A_17166 - XDS Document Service – Keine Implementierung der IHE ITI-Akteure ATNA Secure Node sowie ATNA Secure Application für Node Authentication

Der XDS Document Service DARF zur Node Authentication die IHE ITI-Akteure "ATNA Secure Node" sowie "ATNA Secure Application" gemäß [IHE-ITI-TF1] NICHT implementieren. [≤]

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

A_14654 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs CT Time Client

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "CT Time Client" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14665 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs XDS Document Source

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Source" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14667 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs XDS Integrated Document Source/Repository

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Integrated Document Source/Repository" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14668 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs XDS Document Consumer

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Document Consumer" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14666 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs XDS Patient Identity Source

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS Patient Identity Source" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14669 - XDS Document Service – Keine Implementierung des IHE ITI-Akteurs XDS On-Demand Document Source

Der XDS Document Service DARF NICHT den IHE ITI-Akteur "XDS On-Demand Document Source" gemäß [IHE-ITI-TF1] implementieren. [≤]

A_14950 - XDS Document Service – Keine Angabe einer Fehlerlokalisierung im RegistryError-Element

Der XDS Document Service 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 - XDS Document Service – Implementierung des IHE ITI-Akteurs RMU Update Responder

Der XDS Document Service MUSS den IHE ITI-Akteur "RMU Update Responder" gemäß [IHE-ITI-RMU] implementieren. [≤]

3.13.1.4.1.1 Gruppierungen mit anderen IHE ITI-Akteuren

A_15093-02 - XDS Document Service – Gruppierung RMU Update Responder mit Document Registry

Der XDS Document Service als RMU-Akteur "Update Responder" MUSS mit dem XDS-Akteur "Document Registry" gemäß [IHE-ITI-RMU] gruppiert sein. [≤]

3.13.1.4.1.2 Optionen des IHE ITI-Akteurs

A_15094 - XDS Document Service – RMU Update Responder ohne "Forward Update"-Option

Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option "Forward Update" unterstützen. [≤]

A_15095-02 - XDS Document Service – RMU Update Responder ohne "XCA Persistence"-Option

Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option "XCA Persistence" unterstützen. [≤]

A_15096-02 - XDS Document Service – RMU Update Responder mit "XDS Persistence"-Option

Der XDS Document Service als RMU-Akteur "Update Responder" MUSS die Option "XDS Persistence" unterstützen. [≤]

A_15097 - XDS Document Service – RMU Update Responder ohne "XDS Version Persistence"-Option

Der XDS Document Service als RMU-Akteur "Update Responder" DARF NICHT die Option "XDS Version Persistence" unterstützen. [≤]

3.13.1.4.1.3 Gruppierungen mit anderen IHE ITI-Akteuren

3.13.1.4.1.4 Optionen des IHE ITI-Akteurs

A_14637 - XDS Document Service – XDS Document Registry ohne "Asynchronous Web Services Exchange"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "Asynchronous Web Services Exchange" unterstützen.[<=]

A_14638 - XDS Document Service – XDS Document Registry mit "Reference ID"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" MUSS die Option "Reference ID" unterstützen.[<=]

A_14639 - XDS Document Service – XDS Document Registry ohne "Patient Identity Feed"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "Patient Identity Feed" unterstützen.
[<=]

A_14640 - XDS Document Service – XDS Document Registry ohne "Patient Identity Feed HL7v3"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "Patient Identity Feed HL7v3" unterstützen.[<=]

A_14641 - XDS Document Service – XDS Document Registry ohne "On-Demand Documents"-Option

Der XDS Document Service als XDS-Akteur "Document Registry" DARF NICHT die Option "On-Demand Documents" unterstützen.[<=]

3.13.1.4.1.5 Optionen des IHE ITI-Akteurs

A_14636 - XDS Document Service – XDS Document Repository ohne "Asynchronous Web Services Exchange"-Option

Der XDS Document Service als XDS-Akteur "Document Repository" DARF NICHT die Option "Asynchronous Web Services Exchange" unterstützen.[<=]

3.13.1.4.2 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 24: 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 25: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen des XDS Document Service

IHE ITI-Akteur	Opt.			Umzusetzende Option des IHE ITI-Akteurs	Opt.
		Gruppierung mit anderem IHE ITI-Akteur	Opt.		
ATNA Audit Record Repository	X				
CT Time Client	X				
RMU Update Responder	R			Forward Update	X
				XCA Persistence	X
				XDS Persistence	R
				XDS Version Persistence	X
		Document Registry	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

IHE ITI-Akteur	Opt.			Umzusetzende Option des IHE ITI-Akteurs	Opt.
		Gruppierung mit anderem IHE ITI-Akteur	Opt.		
				Patient Identity Feed HL7v3	X
				Reference ID	R
		ATNA Secure Node oder Secure Application für Node Authentication	X		
XDS Document Repository	R			Asynchronous Web Services Exchange	X
		ATNA Secure Node oder Secure Application für Node Authentication	X		
XDS Document Source	X				
XDS Integrated Document Source / Repository	X				
XDS On-Demand Document Source	X				
XDS Patient Identity Source	X				

3.13.1.4.3 Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen

A_17832 - XDS Document Service – Unterstützung MTOM/XOP

Der XDS Document Service MUSS gemäß den Anforderungen von [IHE-ITI-TF2x#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] verwenden. [≤]

A_24524 - XDS Document Service - Migration, Upload: Normalisieren des URI

Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten den `DocumentEntry.URI` normalisieren. Dies gilt für `FileURI`, z. B. "<file:///C:/path/to/file.html#anchor>" oder "`/C/path/to/file.html#anchor`". Die URI MUSS auf den reinen Dateinamen mit Extension (d. h. ohne Pfadangaben) reduziert werden, z. B. "`file.html`". Nach der Normalisierung MUSS eine Validierung der Extension gemäß `A_23447-*` erfolgen. [≤]

A_23447-01 - XDS Document Service - DocumentEntry.URI extension entspricht mimetype

Der XDS Document Service MUSS bei jedem Upload von Dokumenten oder Metadaten das Metadatum `DocumentEntry.URI` daraufhin prüfen, ob `DocumentEntry.URI` eine `filename extension` aufweist, die nicht dem `DocumentEntry.mimetype` entspricht. Zuvor muss die URI mittels `A_24524-*` normalisiert worden sein. Danach MUSS der XDS Document Service sicherstellen, dass in `Document.URI` die `filename extension` dem `DocumentEntry.mimeType` entspricht. Im Falle einer Abweichung MUSS an die ursprüngliche `DocumentEntry.URI` die `filename extension` gemäß `A_24864-*`, bzw. `A_25009-*`, angehängt werden, die dem `mimeType` entspricht. Die Groß-/Kleinschreibung der `filename extension` ist bei der Prüfung nicht relevant. [≤]

A_24451-01 - XDS Document Service - Automatisches initiales Erzeugen einer versionsübergreifenden ID für Dokumente

Der XDS Document Service MUSS beim initialen Einstellen eines Dokumentes die `DocumentEntry.uniqueId` als Eintrag einer `ReferenceID` in die `ReferenceIDList` in folgendem Format einstellen:

```
<DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2023:rootDocumentUniqueId
```

Beim Upload einer neuen Version des Dokumentes DARF dieser Eintrag in der `ReferenceIDList`, d.h. die `rootDocumentUniqueId`, NICHT verändert werden. Er bleibt über alle Versionen des Dokumentes hinweg unverändert erhalten. Der Versuch eines Clients, die `rootDocumentUniqueId` durch ein `Metadata-Update` oder im Zuge des Einstellens einer neuen Dokumentenversion zu verändern, MUSS mit einem IHE-Error `XDSRegistryMetadataError` abgebrochen werden. Es MUSS im `codeContext`-Attribut des zurückgegebenen `XDSRegistryMetadataError`-Elements der Text „`rootDocumentUniqueId must not be changed`“ zurückgegeben werden. [≤]

A_14926-03 - XDS Document Service – Automatisiertes Löschen oder Verbergen von Dokumenten

Der XDS Document Service MUSS bei zu löschenden oder zu verbergenden Dokumenten und `DocumentEntry`-Einträgen im selben Zuge auch alle assoziierten `DocumentEntry`-Einträge und Dokumente löschen bzw. verbergen. [≤]

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

A_13715 - XDS Document Service – Ablauflogik für ProvideAndRegisterDocumentSet-b

Der XDS Document Service MUSS die Umsetzung der Operation `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_15162-05 - XDS Document Service – Keine Registrierung bei Angabe von Document Entry Relationships in Metadaten

Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren, sofern die Metadaten andere Association Types nach [IHE-ITI-TF3#4.2.2.2] als die Folgenden enthalten:

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

[<=]

A_14938-02 - XDS Document Service – Validierung der Metadaten aus ITI Document Sharing-Profilen

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

A_23123 - XDS Document Service – APND-Assoziation mit existierenden Dokument oder Dokument aus SubmissionSet

Der XDS Document Service MUSS bei APND-Assoziationen sowohl Verknüpfungen auf ein existierendes Dokument im Status "Approved" als auch auf ein Dokument aus dem übergebenen `SubmissionSet` ermöglichen.[<=]

A_23124 - XDS Document Service – Addendum nur mit einem Dokument verknüpfen

Der XDS Document Service DARF ein Addendum NICHT mit mehr als einem Dokument verknüpfen.[<=]

Das heißt, ein Addendum-Dokument kann sich gemäß IHE immer nur auf ein einzelnes Vorgängerdokument (IHE: "parent document") beziehen.

A_23125 - XDS Document Service – Kein automatisches "Deprecated" des Addendums

Der XDS Document Service DARF abweichend von [IHE-ITI-TF3#4.2.2.2.3] einem Addendum NICHT den `availabilityStatus` = `Deprecated` zuweisen, wenn das verknüpfte Dokument den `availabilityStatus` `Deprecated` erhält.[<=]

A_24521 - XDS Document Service - Erzeugen von Prüfsummen für Dokumente

Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes Dokument seine kryptographische Prüfsumme berechnen und in `DocumentEntry.hash` hinterlegen. Dabei MUSS SHA-256 verwendet werden. Außerdem MUSS die Dokumentengröße in `DocumentEntry.size` berechnet und gesetzt werden.[<=]

A_24988 - XDS Document Service - Dublettenprüfung für Dokumente

Der XDS Document Service MUSS beim Einstellen von Dokumenten in die Akte für jedes Dokument den hash-Wert vergleichen mit allen bereits in dieser Akte existierenden hash-Werten der Dokumente und bei einer Übereinstimmung das Einstellen mit dem Fehlercode `XSDuplicateDocument` ablehnen. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die Liste der UUIDs (`DocumentEntry.entryUUID`) der identifizierten Dokumente angegeben werden.[<=]

A_24990 - XDS Document Service - Dublettenprüfung für dynamische Ordner

Der XDS Document Service MUSS beim Anlegen dynamischer Folder prüfen, ob ein Ordner bereits existiert, der gemäß vom Titel her identisch ist mit demjenigen, den der Client einzustellen versucht. Im Falle eines identischen Titels MUSS der Einstellversuch mit dem Fehlercode `XDSDuplicateFolder` abgelehnt werden. [`<=`]

A_14937 - XDS Document Service – Dokumentengröße prüfen

Der XDS Document Service MUSS die Dateigröße jedes übergebenen Dokuments ermitteln, bevor das SubmissionSet verarbeitet wird. Der XDS Document Service 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.

[`<=`]

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 Transportcodierung. Größere Dokumente können nicht hochgeladen werden.

A_23098-01 - XDS Document Service – Keine Registrierung bei zeitlicher Ungültigkeit von strukturierten Dokumenten

Der XDS Document Service MUSS beim Einstellen eines strukturierten Dokuments sicherstellen, dass die Vorgaben gemäß [gemSpec_IG_ePA] hinsichtlich der zeitlichen Gültigkeit erfüllt werden und andernfalls das Registrieren und Speichern von Metadaten und Dokument(en) ablehnen und mit einem `XDSRepositoryMetadataError` quittieren. Es MUSS im `codeContext`-Attribut des zurückgegebenen `XDSRepositoryMetadataError`-Elements der Text „Version of submitted structured document is not supported“ zurückgegeben werden. [`<=`]

A_21610-03 - Sonderfälle Anlegen von Foldern durch Clientsysteme

Der XDS Document Service MUSS sicherstellen, dass ausschließlich dynamische Ordner vom Typ "Schwangerschaft und Geburt" (Folder.Code = `pregnancy_childbirth`) durch Clients angelegt werden können. [`<=`]

A_22400-01 - XDS Document Service - Ablehnung Upload bei abweichenden confidentialityCode

Der XDS Document Service MUSS Uploads, die als Resultat einen uneinheitlichen `documentEntry.confidentialityCode` über alle Dokumente in einer mixed- oder uniform-Sammlung haben, mit einem `XDSRegistryMetadataError` ablehnen. [`<=`]

Die Anforderung bezieht sich auf Einträge in `documentEntry.confidentialityCode` die nicht aus dem ValueSet zum Verbergen (`confidentialityCode=CON`), resultieren.

A_24797-04 - XDS Document Service - Ablehnung Upload bei veränderten Metadaten bei einer RPLC Assoziation

Der XDS Document Service MUSS Uploads, die als Resultat ein zum Vorgängerdokument verändertes Metadatum enthalten, mit einem `XDSRegistryMetadataError` ablehnen. Einzige Ausnahmen sind:

- Metadatenattribute `creationTime`, `entryUUID` sowie `uniqueId` und `confidentialityCode` = "CON" (`codeSystem` = `urn:oid:1.2.276.0.76.5.491`).
- Das Metadatenattribut `DocumentEntry.referenceIdList` DARF ohne die `rootDocumentUniqueId` gesendet werden; in dem Fall wird die `rootDocumentUniqueId` automatisch vom XDS Document Service gesetzt (Wert identisch zu dem des ersetzten Dokuments).

[`<=`]

A_24531-04 - Constraint Management - Verbergen von Dokumenten durch confidentialityCode

Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) durch eine Nutzergruppe der Rolle `oid_versicherter` eingestellt wird, nicht Bestandteil einer Sammlung, also eines Ordners der Ausprägung "mixed" oder "uniform" ist, und kein Dokument der Kategorie "emp" ist, dann MUSS der XDS Document Service sicherstellen, dass das Dokument durch einen Eintrag in der General Deny Policy verborgen wird. Es MUSS ein Eintrag mit denyType = "document" für die General Deny Policy erzeugt werden. [\leq]

A_25856-02 - XDS Document Service - Fehlerhaftes Verbergen von Dokumenten durch confidentialityCode

Falls das Dokument, welches mit confidentialityCode = "CON" (codeSystem = urn:oid:1.2.276.0.76.5.491) nicht durch eine Nutzergruppe der Rolle `oid_versicherter` eingestellt wird, oder Bestandteil einer Sammlung, also eines Ordners der Ausprägung "mixed" oder "uniform" ist, dann MUSS der XDS Document Service die Operation abbrechen und mit einem Fehlercode ConstraintViolation beenden. [\leq]

Das Verbergen von Dokumenten ist in Kapitel 3.13.1.10- Verbergen von Dokumenten durch Verwendung des confidentialityCode beschrieben.

3.13.1.4.3.2 Registry Stored Query [ITI-18]

A_14913 - XDS Document Service – Ablauflogik für Registry Stored Query

Der XDS Document Service MUSS die Umsetzung der Operation RegistryStoredQuery gemäß der definierten Ablauflogik in [IHE-ITI-TF2a#3.18.4.1.2 und 3.18.4.1.3] implementieren. [\leq]

A_24761 - XDS Document Service – Ermitteln verknüpfter Approved Documents für Registry Stored Query

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "GetRelatedApprovedDocuments" mit der Query-ID "urn:uuid:1c1f1cea-ad3a-11ed-afa1-0242ac120002" mit denselben Parameternutzungsvorgaben der Registry Stored Query „GetDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.5] mit der Multiplizität 1 unterstützen. Das resultierende DocumentEntry Objekt MUSS

- mit dem Ergebnis von GetDocuments übereinstimmen, falls dieses sich im Zustand approved befindet;
- andernfalls über Associations ermittelt werden. Dabei wird jeweils ausgehend von der übergebenen DocumentEntry.EntryUUID oder DocumentEntry.UniqueId über die Replace- Associations dasjenige DocumentEntry Objekt ermittelt, das sich im Zustand approved befindet.

Das wsa:Action-Element MUSS den Wert "urn:ihe:iti:2007:RegistryStoredQuery" besitzen. [\leq]

A_24762 - XDS Document Service – Suchanfragen über das Metadatenattribut DocumentEntry.title

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.1] sowie den weiteren verpflichtenden Suchparameter \$XDSDocumentEntryTitle unterstützen, sodass eine Suchergebnismenge über das Attribut XDSDocumentEntry.title eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den

Parameter `$XDSDocumentEntryAuthorPerson`. Das `wsa:Action-Element` MUSS den Wert `"urn:ihe:iti:2007:RegistryStoredQuery"` besitzen. [`<=`]

A_25183 - XDS Document Service – Suchanfragen über das Metadatenattribut `DocumentEntry.comment`

Der XDS Document Service MUSS einen zusätzlichen Anfragetyp `"FindDocumentsByComment"` mit der Query-ID `"urn:uuid:2609dda5-2b97-44d5-a795-3e999c24ca99"` 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 `$XDSDocumentEntryComment` unterstützen, sodass eine Suchergebnismenge über das Attribut `XDSDocumentEntry.comment` eingeschränkt werden kann. Weiterhin MUSS dieselbe Suchmusterlogik mittels Platzhalter implementiert sein, wie für Suchanfragen über den Parameter `$XDSDocumentEntryAuthorPerson`. Das `wsa:Action-Element` MUSS den Wert `"urn:ihe:iti:2007:RegistryStoredQuery"` besitzen. [`<=`]

A_24763 - XDS Document Service – Suche über Author Institution bei Registry Stored Query

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

A_24764 - XDS Document Service – Rückgabe unscharfer Suchergebnisse für Registry Stored Query

Der XDS Document Service MUSS bei der Ermittlung der Ergebnisse einer Registry Stored Query bei Auswertung der folgenden Queries und deren Suchparametern beim Durchsuchen des dazugehörigen Suchfelds auch unscharfe, d. h. bezogen auf das jeweilige Suchfeld nicht nur exakt auf die Metadaten passende, sondern auch leicht abweichende Ergebnisse zurück liefern können:

- Query `"FindDocuments"` und Query `"FindDocumentsByTitle"` und Query `"FindDocumentsByComment"`
 - `$XDSDocumentEntryTitle`
 - `$XDSDocumentEntryAuthorInstitution`
 - `$XDSDocumentEntryAuthorPerson`
 - `$XDSDocumentEntry.comment`
- Query `"FindSubmissionSets"`
 - `$XDSSubmissionSetAuthorPerson`

Dabei MUSS der XDS Document Service mindestens unscharfe Ergebnisse bezüglich Groß/Kleinschreibung unterstützen, also Groß/Kleinschreibung für die angegebenen Parameter der ausgewählten Query-Typen ignorieren.

[`<=`]

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

3.13.1.4.3.3 Remove Metadata [ITI-62]

A_14908-02 - XDS Document Service – Ablauflogik für Remove Metadata

Der XDS Document Service MUSS die Umsetzung der Operation RemoveMetadata gemäß der definierten Ablauflogik in [IHE-ITI-RMD#3.62.4.1.2 und 3.62.4.1.3] implementieren. [<=]

A_20701 - XDS Document Service – Unwiderrufliches Löschen bei Remove Metadata

Der XDS Document Service MUSS sicherstellen, dass einmal gelöschte Dokumente und Metadatenobjekte nicht wiederhergestellt werden können. [<=]

A_21715 - XDS Document Service – Kein Löschen von "replaced"-Dokumenten im Status "Deprecated"

Der XDS Document Service MUSS sicherstellen, dass keine Löschanfrage eines ePA-Client auf Dokumenten mit dem availabilityStatus = Deprecated ausgeführt werden darf. [<=]

A_21714-03 - XDS Document Service – Löschen von strukturierten Dokumenten durch ein ePA-FdV

Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein ePA-FdV ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die Nachricht mit dem XDSRegistryError-Fehlercode zurückgeben werden. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt werden. [<=]

A_21817-02 - XDS Document Service – Löschen von strukturierten Dokumenten durch ein Primärsystem

Der XDS Document Service MUSS Löschanfragen eines dynamischen Ordners durch ein Primärsystem ablehnen, wenn zugehörige Submission Sets, Associations oder zugeordnete Dokumente in der Löschanfrage enthalten sind. Das Löschen dieses Ordners impliziert aktensystemseitig immer das Löschen zugehöriger SubmissionSets, Associations sowie zugeordneter Dokumente. Liegt eine Verletzung der Löschvorgaben vor, MUSS die Nachricht mit XDSRegistryError-Fehlercode zurückgeben werden. Es MUSS im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements der Wert "Anfragenachricht darf ausschließlich entryUUID für Folder beinhalten" belegt werden. [<=]

A_24663-01 - XDS Document Service – Bereinigung der General Deny Policy

Der XDS Document Service MUSS als Folge von erfolgreichen Löschanfragen alle Einträge der General Deny Policy entfernen, welche die betroffenen Dokumente oder dynamischen Ordner referenzieren. [<=]

A_24765 - XDS Document Service – Kein Löschen von statischen Ordnern und Associations

Der XDS Document Service MUSS sicherstellen, dass eine Löschanfrage keine statischen Ordner und Assoziationen löschen darf. Dies gilt nicht für dynamische Ordner. Der XDS Document Service MUSS bei Löschung eines Dokumentes die Assoziation zum Folder löschen. [<=]

Dynamische Ordner sind beispielsweise Mutterpass (folderCode = pregnancy_childbirth) oder DiGA (folderCode = diga).

A_20579-01 - XDS Document Service – Löschen von Ordnern

Der XDS Document Service MUSS Requests, die darauf abzielen, einen statischen Folder direkt zu löschen, mit einem XDSRegistryMetadataError ablehnen. [<=]

3.13.1.4.3.4 RetrieveDocumentSet [ITI-43]

A_14914 - XDS Document Service – Ablauflogik für Retrieve Document Set

Der XDS Document Service MUSS die Umsetzung der Operation 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_16201 - XDS Document Service – Prüfung der zurückgegebenen Paketgröße

Der XDS Document Service 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.[<=]

3.13.1.4.3.5 Restricted Update Document Set [ITI-92]

A_15061-07 - XDS Document Service – Ablauflogik für Restricted Update Document Set

Der XDS Document Service MUSS die Umsetzung der Operation 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 inklusive der entryUUID des zu ändernden DocumentEntry-Objekts. Das übermittelte DocumentEntry-Objekt kann sowohl alle vollständigen Metadatenattribute als auch nur zu ändernde Metadatenattribute enthalten. In jedem Fall dürfen Änderungen ausschließlich gemäß A_15083-* angenommen und durchgeführt werden.
- für das Hinzufügen, Ändern oder Löschen eines einzelnen oder mehrerer Werte in DocumentEntry.author, DocumentEntry.confidentialityCode und DocumentEntry.eventCodeList gilt darüber hinaus:
 - es MÜSSEN alle und nicht nur die zu ändernden Werte (z. B. Autoren) über ihre jeweiligen <classification classificationScheme="urn:uuid:...>-XML-Elemente im gewünschten Soll-Zustand gesendet werden.
 - das Löschen aller Werte (z. B. Autoren) MUSS durch Übertragung ein einzelnen, komplett leeren <classification="urn:uuid:...>-XML-Elements signalisiert werden.
- eine SS-DE HasMember-Association, die das SubmissionSet mit dem geschickten DocumentEntry verbindet.
- die „lid“ (logicalID) DARF NICHT gesendet werden.
- der Slot "PreviousVersion" MUSS immer mit dem Wert "1" gesendet werden.
- der Slot „AssociationPropagation“ MUSS auf „no“ gesetzt werden. Zusätzlich MUSS der alternative Slot-Name "associationPropagation" akzeptiert werden.

Der XDS Document Service DARF die gesendete Association und das neue SubmissionSet NICHT dauerhaft speichern.[<=]

Der alternative Slot-Name "associationPropagation" wird unterstützt, da alte Versionen von ePA fälschlicherweise, abweichend von [IHE-ITI-RMU] diesen Wert gefordert haben.

A_15082-02 - XDS Document Service – Validierung der Metadaten aus ITI Document Sharing-Profilen

Der XDS Document Service MUSS die übermittelten DocumentEntry-Metadaten der Operation `RestrictedUpdateDocumentSet` dahingehend prüfen, dass gegenüber den Bestandsdaten die geänderten Metadaten konform zu den Nutzungsvorgaben in [A_14760-*] geändert werden. Der XDS Document Service MUSS das Aktualisieren der Metadatenattribute ablehnen und mit einem `XDSRepositoryMetadataError` quittieren, sofern die Metadaten nicht konform zu den Nutzungsvorgaben sind. Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements angegeben werden, welches Metadatenattribut nicht den Nutzungsvorgaben entspricht. [`<=`]

A_15083-08 - XDS Document Service – Prüfung auf ausschließliche Aktualisierung der erlaubten Metadaten

Der XDS Document Service MUSS die übermittelten DocumentEntry-Metadaten der Operation `RestrictedUpdateDocumentSet` dahingehend prüfen, dass gegenüber den Bestandsdaten ausschließlich die folgenden Metadaten geändert werden:

- `DocumentEntry.author`
- `DocumentEntry.classCode`
- `DocumentEntry.comments`
- `DocumentEntry.confidentialityCode` (`confidentialityCode` = "CON" (`codeSystem` = `urn:oid:1.2.276.0.76.5.491`) ist nicht erlaubt)
- `DocumentEntry.creationTime`
- `DocumentEntry.eventCodeList`
- `DocumentEntry.formatCode`
- `DocumentEntry.healthcareFacilityTypeCode`
- `DocumentEntry.languageCode`
- `DocumentEntry.legalAuthenticator`
- `DocumentEntry.practiceSettingCode`
- `DocumentEntry.referenceIdList`
- `DocumentEntry.serviceStartTime`
- `DocumentEntry.serviceStopTime`
- `DocumentEntry.title`
- `DocumentEntry.typeCode`
- `DocumentEntry.URI`

Wenn das Metadatum `DocumentEntry.referenceIdList` ohne `rootDocumentUniqueId` gesendet wird, MUSS der XDS Document Service den Wert automatisch setzen (identisch zu `rootDocumentId` in `DocumentEntry.referenceIdList` des ersetzten Dokuments). Wenn die `rootDocumentUniqueId` gesendet wird, MUSS der XDS Document Service sicherstellen, dass der Wert dem ansonsten automatisch gesetzten Wert entspricht.

Werden unerlaubte Metadatenänderungen geschickt, muss die Operation mit einem `LocalPolicyRestrictionError`-Fehlercode abgebrochen werden. Werden Metadatenattribute mit leeren Werten übermittelt, signalisiert dies ein Löschen des Metadatoms (z.B. `DocumentEntry.comments`). Es müssen die Kardinalitäten in A_14760-* berücksichtigt bzw. dürfen nicht verletzt werden. Das

Metadatum `DocumentEntry.referenceIdList` MUSS dabei mindestens die `rootDocumentUniqueId` enthalten.

Wenn in der Eingangsnachricht keine Aktualisierung für die erlaubten Metadaten enthalten ist, ist die Weiterverarbeitung abubrechen und die Nachricht mit einem `LocalPolicyRestrictionError`-Fehlercode zu quittieren. [`<=`]

A_21533 - XDS Document Service – Kein Anlegen von Versionen für Restricted Update Document Set

Der XDS Document Service DARF eine echte Versionierung NICHT umsetzen, d. h. er DARF den alten `DocumentEntry` NICHT speichern. Insbesondere DARF der XDS Document Service `DocumentEntry.version` NICHT anlegen und verwalten. [`<=`]

A_21783-03 - XDS Document Service - Vererbung der geänderten Metadaten für Restricted Update Document Set

Der XDS Document Service MUSS die neu gesetzten Metadaten ebenfalls auf alle mit dem geänderten Dokument assoziierten Dokumente setzen. Als assoziierte Dokumente sind im Sinne dieser Anforderung Dokumente einer RPLC-Kette zu betrachten. [`<=`]

Metadaten von Dokumenten einer mixed- oder uniform-Sammlung dürfen nicht geändert werden.

A_25173 - XDS Document Service - Restricted Update Document Set nicht für MIOs

Falls die Operation `RestrictedUpdateDocumentSet` für Dokumente einer mixed- oder uniform-Sammlung aufgerufen wird MUSS der XDS Document Service das Aktualisieren der Metadatenattribute ablehnen, mit einem `XDSRepositoryMetadataError` quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements den Text "Metadata Update for MIOs not allowed" angeben.

[`<=`]

3.13.1.4.4 Sicherheitstechnische Vorgaben bei XDS-Operationen

A_24508-01 - XDS Document Service – Prüfung der Policies bei Suchanfrage

Der XDS Document Service MUSS bei einer Suchanfrage für einen angemeldeten Nutzer die Suchergebnismenge entsprechend der Legal Policy und der General Deny Policy filtern, d. h. die Suchergebnismenge enthält ausschließlich XDS-Metadaten, die für einen angemeldeten Nutzer nicht diesen Policies widersprechen. [`<=`]

A_26222 - XDS Document Service (EU) – Prüfung Zugriffscode bei Suchanfrage EU-Zugriff

Der XDS Document Service MUSS für einen angemeldeten Nutzer mit der Rolle `oid_nceph` bei jeder Suchanfrage und jeder Retrieve-Operation prüfen, dass der im SOAP-Header der Operation übergebene Zugriffscode identisch ist mit dem im Entitlement Management für diesen Nutzer hinterlegten Zugriffscode und andernfalls die Operation mit dem Fehlercode `AccessCodeViolation` beenden. [`<=`]

A_24509 - XDS Document Service - Prüfung der Legal Policy außer Suchanfragen

Der XDS Document Service MUSS die Ausführung einer Operation mit dem Fehlercode `LegalPolicyViolation` beenden, wenn für den angemeldeten Nutzer die Regeln der Legal Policy nicht erfüllt sind und es sich nicht um eine Suchanfrage handelt.

Es MUSS im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError`-Elements die Liste der UUIDs (`DocumentEntry.entryUUID`) der identifizierten Dokumente angegeben werden. [`<=`]

A_24510-02 - XDS Document Service – Prüfung Herunterladen eines verborgenen oder nicht vorhandenen Dokuments

Der XDS Document Service MUSS die Ausführung der Retrieve-Operation mit dem Fehlercode `XDSDocumentUniqueIdError` beenden, wenn das assoziierte Dokument nicht vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind. [\leq]

A_24511-01 - XDS Document Service – Prüfung Löschen eines verborgenen Dokuments oder dynamischen Ordners

Der XDS Document Service MUSS die Ausführung der Remove-Operation mit dem Fehlercode `XDSDocumentUniqueIdError` beenden, wenn für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind. [\leq]

A_24512-02 - XDS Document Service – Prüfung Schreiben eines Dokuments in einen nicht vorhandenen oder verborgenen dynamischen Ordner

Der XDS Document Service MUSS die Ausführung der Provide-Operation mit dem Fehlercode `UnresolvedReferenceException` beenden, wenn der Ordner nicht existiert oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind. [\leq]

A_24513-02 - XDS Document Service – Prüfung Aktualisierung Metadaten eines verborgenen oder nicht vorhandenen Dokuments

Der XDS Document Service MUSS die Ausführung der Update-Operation mit dem Fehlercode `UnresolvedReferenceException` beenden, wenn das assoziierte Dokument nicht vorhanden ist oder für den angemeldeten Nutzer die Regeln der General Deny Policy nicht erfüllt sind. [\leq]

3.13.1.5 Fehlerbehandlung in Schnittstellenoperationen**A_22516-02 - XDS Document Service - Alternative Verwendung von `XDSRegistryMetadataError` anstelle von `XDSRepositoryMetadataError`**

Der XDS Document Service KANN alternativ zum Fehler "`XDSRepositoryMetadataError`" den Fehler "`XDSRegistryMetadataError`" verwenden. [\leq]

A_23148-01 - XDS Document Service – Festlegung zu http-Statuscode bei IHE-Responses

Der XDS Document Service MUSS für den Fall, dass eine IHE-Response in der HTTP-Response enthalten ist, den http-Statuscode 200 zurückgeben. Das gilt auch, wenn die IHE-Response einen IHE-Fehler überträgt. [\leq]

A_26324-01 - XDS Document Service - Aktenkonto im Umzug

Falls sich ein Aktenkonto im Zustand `SUSPENDED` befindet MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem `StatusMismatch`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. [\leq]

A_26325-01 - XDS Document Service - Aktenkonto unbekannt oder im Zustand `INITIALIZED`

Falls sich ein Aktenkonto im Zustand `UNKNOWN` oder `INITIALIZED` befindet MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem `NoHealthRecord`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. [\leq]

A_25683-01 - XDS Document Service - Prüfung auf Befugnis

Falls keine gültige Befugnis für den aufrufenden Nutzer vorliegt MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem `NotEntitled`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. [\leq]

A_26459 - XDS Document Service - keine Authentisierung des Nutzers

Falls keine erfolgreiche Authentifizierung des Nutzers vorliegt MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem `InvalidAuth`-Fehlercode gemäß [IHE-ITI-TF3#4.2.4] quittieren. <=[<=]

3.13.1.6 Schnittstellen im XDS Document Service

In diesem Abschnitt wird die Außenschnittstelle des XDS Document Service 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 des XDS Document Service nicht zwischen Document Registry und Document Repository unterscheidet (ein Zugangspunkt für einen integrierten Dienst mit differenzierten Pfaden, siehe A_26814-*, 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.

3.13.1.6.1 Schnittstelle I_Document_Management

Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen .

A_14152-02 - XDS Document Service – Implementierung der Schnittstelle I_Document_Management

Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle für den Zugriff von ePA-Clients, die über das zentrale Netz zugreifen implementieren.

Tabelle 26: Schnittstelle I_Document_Management

Schnittstelle	I_Document_Management	
Version	2.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	ProvideAndRegisterDocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Metadata	Löschen von Dokumenten oder Ordnern

Schnittstelle	I_Document_Management	
	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
WSDL	[XDSDocumentService]	
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd 	

[<=]

Durch die Legal Policy ist geregelt, welche Clients (professionOID) letztendlich zugreifen dürfen.

3.13.1.6.1.1 Operation I_Document_Management::ProvideAndRegisterDocumentSet-b
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "ProvideAndRegisterDocumentSet-b" [ITI-41] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

Die DiGA-Daten werden pro Anwendung in einem für jede DiGA spezifischen Ordner gesammelt. Das Anlegen eines DiGA-Ordners erfolgt durch den XDS Document Service unter der Voraussetzung, dass es eine gültige Befugnis für die DiGA gibt. Der DiGA-Ordner wird vom XDS Document Service mit der Telematik-ID der DiGA verknüpft. Die Zuordnung von DiGA-Dokumenten beim Schreiben erfolgt implizit über die TelematikID aus dem IDToken des Nutzers. Da ein DiGA-Ordner im Titel immer den Namen der DiGA enthält kann ein Client (z.B. LEI) darüber die relevante DiGA auswählen und auf die Dokumente der DiGA, sofern eine Befugnis für den Nutzer vorliegt, lesend zugreifen.

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

A_21512-04 - XDS Document Service – dynamisches Anlegen von DiGA-Ordern

Falls eine gültige Befugnis für eine konkrete DiGA vorliegt, MUSS der XDS Document Service beim erstmaligen Einstellen eines Dokumentes für diese DiGA in die Akte des Versicherten (Operation I_Document_Management::ProvideAndRegisterDocumentSet-b()) sicherstellen, dass genau ein Ordner für den Versicherten mit den folgenden Eigenschaften angelegt ist:

- DiGA-Ordner der Kategorie diga gemäß A_19388 (Belegung Folder.codeList) unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A_14760 (Belegung der restlichen Metadatenfelder).

- Folder.title wird entsprechend des Attributs "organizationName" aus dem IDToken der zugreifenden DiGA belegt.
- Folder.comment wird belegt mit "urn:gematik:diga:<Telematik-ID>", wobei die Telematik-ID dem Attribut "idNummer" des ID-Token entspricht.
- Folder.EntryUUID wird mit einer aus der TelematikID abgeleiteten UUID belegt.

Die folder.EntryUUID MUSS wie folgend dargestellt aus der TelematikID der DiGA erzeugt werden:

- Algorithmus: Name-Based UUID gemäß [RFC4122#4.3], Version 3 (MD5)
- Namensraum-UUID: "e2310a38-0b62-415e-8b44-994dc8312965"
- Name: "<TelematikId>"

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

[<=]

A_22994-01 - XDS Document Service - automatische Folder-Zuordnung für DiGA

Der XDS Document Service MUSS beim Einstellen eines DiGA-Dokumentes in die Akte des Versicherten (Operation

`I_Document_Management::ProvideAndRegisterDocumentSet-b()` sicherstellen, dass das DiGA-Dokument in den durch die TelematikID referenzierten DiGA-Ordner abgelegt wird. Die TelematikID des zu adressierenden Ordners entspricht dem Attribut "idNummer" des ID-Token .[<=]

A_21713-03 - XDS Document Service – Kein Einstellen von Ordnern

Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) über die

Schnittstelle `I_Document_Management::ProvideAndRegisterDocumentSet-b` ablehnen und mit einem `XDSRegistryMetadataError`-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder enthalten sind. Ausnahme: Folder der Kategorie `pregnancy_childbirth` in `Folder.codeList`. [≤]

A_24497 - XDS Document Service - Verwendung der korrekten Telematik-ID beim Einstellen

Der XDS Document Service MUSS die Telematik-ID aus dem ID-Token der aktuellen User Session abgleichen mit der Telematik-ID aus `SubmissionSet.authorInstitution` und das Abweichen der Telematik-Ids mit einem `XDSRepositoryMetadataError`-Fehlercode quittieren und im `codeContext`-Attribut des zurückgegebenen `rs:RegistryError-Elements` den Text "Telematik-ID does not match" angeben. [≤]

A_24456 - XDS Document Service - Durchsetzung von Uniqueness beim Einstellen von Notfalldaten

Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien "emergency" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein einzelnes NFD- und ein einzelnes DPE-Dokument im Status "approved" gibt. Der Versuch, innerhalb dieses Ordners ein zweites NFD- oder DPE-Dokument einzustellen, MUSS mit dem `IHE-ErrorInvalidDocumentContent` abgebrochen werden. Es MUSS im `codeContext`-Attribut des zurückgegebenen `InvalidDocumentContent`-Elements der Text "Medical information object has to be unique" zurückgegeben werden. [≤]

A_25137 - XDS Document Service - Durchsetzung von Uniqueness beim Einstellen vom Medikationsplan

Der XDS Document Service MUSS beim Einstellen eines Dokumentes der Kategorien "emp" sicherstellen, dass es innerhalb des entsprechenden Ordners nur ein einzelnes eMP-Dokument im Status "approved" gibt. Der Versuch, innerhalb dieses Ordners ein zweites eMP-Dokument einzustellen, MUSS mit dem IHE-Error `InvalidDocumentContent` abgebrochen werden. Es MUSS im `codeContext`-Attribut des zurückgegebenen `InvalidDocumentContent`-Elements der Text "Medical information object has to be unique" zurückgegeben werden. [≤]

3.13.1.6.1.2 Operation `I_Document_Management::RegistryStoredQuery`

Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Registry Stored Query" [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.1.3 Operation `I_Document_Management::RemoveMetadata`

Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.1.4 Operation `I_Document_Management::RetrieveDocumentSet`

Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.1.5 Operation `I_Document_Management::RestrictedUpdateDocumentSet`

Weitere Details zur Ausgestaltung dieser Operation finden sich bezüglich der dazugehörigen IHE ITI-Transaktion "RestrictedUpdateDocumentSet" [ITI-92] in [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x].

Weitere Anforderungen zur Umsetzung der Operation `RestrictedUpdateDocumentSet` befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92].

3.13.1.6.2 Schnittstelle `I_Document_Management_Insurant`

Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen.

A_14478-01 - XDS Document Service – Implementierung der Schnittstelle `I_Document_Management_Insurant`

Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle für den Zugriff des ePA-FdV implementieren.

Tabelle 27: Schnittstelle `I_Document_Management_Insurant`

Schnittstelle	<code>I_Document_Management_Insurant</code>	
Version	2.0.0	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Provide And Register DocumentSet-b	Speichern und Registrieren ein oder mehrerer Dokumente im XDS Document Service

Schnittstelle	I_Document_Management_Insurant	
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
	Remove Metadata	Löschen ein oder mehrerer Dokumente oder Folder
	Restricted Update Document Set	Aktualisierung von Metadaten (Kennzeichen)
WSDL	[XDSDocumentService]	
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd 	

[<=]

A_26460 - XDS Document Service - Zugriff über**I_Document_Management_Insurant mit nicht registriertem Gerät**

Falls Operationen von I_Document_Management_Insurant ohne registriertes Gerät aufgerufen werden MUSS der XDS Document Service die Verarbeitung ablehnen und mit einem UnregisteredDevice-Fehlercode quittieren.[<=]

3.13.1.6.2.1 Operation

I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b

Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Provide And Register Document Set-b" [ITI-41] sind [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

A_21481-04 - XDS Document Service – Kein Einstellen von Ordnern und Associations

Der XDS Document Service MUSS das Registrieren und Speichern von Metadaten und Dokument(en) über die Schnittstelle

I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b() ablehnen und mit einem XDSRegistryMetadataError-Fehlercode quittieren, wenn in der Eingangsnachricht ein oder mehrere neu anzulegende Folder oder andere als die folgenden Assoziationen

- SS-DE

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

enthalten sind. [≤]

Das Referenzieren bestehender Ordner ist davon nicht berührt, wie dies z. B. beim Einstellen von Dokumenten in Sammlungen der Fall ist (z. B. Einstellen eines Dokuments in einen Mutterpass).

A_23144 - XDS Document Service - Automatische Ablage von Dokumenten im Ordner "technical"

Der XDS Document Service MUSS sicherstellen, dass Dokumente mit einem formatCode mit der codeSystem OID "2.25.154081344090540725127779452347992051720", unabhängig von weiteren Metadaten, im statischen Ordner "technical" abgelegt werden. [≤]

3.13.1.6.2.2 Operation I_Document_Management_Insurant::RegistryStoredQuery
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Registry Stored Query" [ITI-18] sind [IHE-ITI-TF2a], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.2.3 Operation I_Document_Management_Insurant::RemoveMetadata
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RemoveMetadata" [ITI-62] sind [IHE-ITI-RMD] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.2.4 Operation I_Document_Management_Insurant::RetrieveDocumentSet
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RetrieveDocumentSet" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.2.5 Operation I_Document_Management_Insurant::RestrictedUpdateDocumentSet
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "RestrictedUpdateDocumentSet" [ITI-92] sind [IHE-ITI-RMU], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

Weitere Anforderungen zur Umsetzung der Operation RestrictedUpdateDocumentSet befinden sich in Kapitel 3.13.1.4.3.5- Restricted Update Document Set [ITI-92].

3.13.1.6.3 Schnittstelle I_Document_Management_Ncpeh

Weitere Vorgaben zu den Operationen befinden sich in 3.13.1.4.3- Vorgaben zu IHE ITI-Transaktionen bei mehreren Schnittstellen .

A_27300 - XDS Document Service (EU) – Implementierung der Schnittstelle I_Document_Management_Ncpeh

Der XDS Document Service MUSS die in der nachstehenden Tabelle definierte Web-Service-Schnittstelle für den Zugriff des ePA-FdV implementieren.

Tabelle 28: Schnittstelle I_Document_Management_Ncpeh

Schnittstelle	I_Document_Management_Ncpeh
Version	2.0.0

Schnittstelle	I_Document_Management_Ncpeh	
Namensraum	urn:ihe:iti:xds-b:2007	
Namensraumkürzel	tns	
Operationen	Name	Beschreibung
	Registry Stored Query	Abfrage von Metadaten zu registrierten Dokumenten
	Retrieve Document Set	Anfrage von registrierten Dokumenten
WSDL	[XDSDocumentService]	
XML Schema	<ul style="list-style-type: none"> • PRPA_IN201301UV02.xsd • PRPA_IN201302UV02.xsd • PRPA_IN201304UV02.xsd • MCCI_IN000002UV01.xsd • query.xsd • rs.xsd • lcm.xsd • rim.xsd • XDS.b_DocumentRepository.xsd 	

[<=]

3.13.1.6.3.1 Operation I_Document_Management_Ncpeh::RegistryStoredQuery
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Registry Stored Query" [ITI-18] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.6.3.2 Operation I_Document_Management_Ncpeh::RetrieveDocumentSet
Weitere Details zur Ausgestaltung dieser Operation in Bezug zur zugehörigen IHE ITI-Transaktion "Retrieve Document Set" [ITI-43] sind [IHE-ITI-TF2b], [IHE-ITI-TF2x] sowie Appendix V aus [IHE-ITI-TF2x] zu entnehmen.

3.13.1.7 Statische Metadaten

Statische Inhalte werden vor der ersten Nutzung des XDS Document Service angelegt, d. h. bevor auf XDS Metadaten zugegriffen wird. Sie sind unveränderlich.

A_24491-02 - XDS Document Service – Anlegen von statischen Ordnern

Der XDS Document Service MUSS nach der erfolgreichen Anlage der Akte des Versicherten die Kategorienordner unter Berücksichtigung allgemeiner Vorgaben für Folder-Metadaten in A_14760* (Belegung der restlichen Metadatenfelder) für den Versicherten gemäß der folgenden Tabelle anlegen. Alle statischen Kategorienordner werden mit jeweils einem Ordner pro Kategorie angelegt. Alle statischen Ordner sind

nach dem Anlegen initial leer.

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

Tabelle 29: Festlegung Folder.entryUUID zu statischen Ordnern

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
reports	b878db05-49e4-4f74-a329-b3bcdd8082c4
emp	7c1054ea-a4df-4a1b-8e10-209f6d8812ee
emergency	a7bb6be7-d756-46dd-90d4-4020ed55b777
eab	2ed345b1-35a3-49e1-a4af-d71ca4f23e57
dental	af547321-b8e8-4e1d-b9af-51bb4a990bda
child	2c898452-4667-40e3-9d3e-c09d7385b527
vaccination	9c3edaf3-a978-46fe-8e6e-021ff4aca60b
patient	d236c9a2-ab01-4902-a00a-1e1dff439fe7
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d
health_risk_analysis	840a59c7-61d4-4caa-80a7-1857af2f166f
care	2d62bf9e-062a-4aa7-9951-9f33bbc665b5
eau	aa7d10d6-204a-47aa-be73-44bdcb77512f
other	605a9f3c-bfe8-4830-a3e3-25a4ec6612cb

Technischer Identifier der Kategorie/Wert von Folder.codeList	Wert von Folder.entryUUID
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31
rehab	173f4204-fb93-4a1a-a1f6-316703b79539
transcripts	6A8E383D-8705-4B0E-A140-39A5F144501D

[<=]

Hinweis: Clientsysteme erstellen für dynamische Ordner jeweils einen Ordner vom Typ "pregnancy_childbirth", mit dem Folder.title für den Namen des Kindes bzw. ein Kennzeichen der Schwangerschaft (A_22515-).*

A_20216-03 - XDS Document Service – Unveränderlichkeit von statischen Akteninhalten

Der XDS Document Service DARF die Metadaten eines statischen Aktenobjekts gemäß A_24491 nach dem Anlegen NICHT ändern oder das statische Aktenobjekt selbst löschen. Dabei gelten folgende Ausnahmen:

- Folder.lastUpdateTime - Folder.lastUpdateTime wird automatisch vom XDS Document Service aktualisiert, sobald Dokumente in den Ordner eingestellt oder daraus gelöscht werden, siehe auch [IHE-ITI-TF2b#3.42.4.1.3.6] und [IHE-ITI-TF3#4.2.3.4.6].

[<=]

3.13.1.8 Nutzungsvorgaben für IHE ITI XDS-Metadaten

Für den XDS Document Service werden Vorgaben bezüglich zu verwendender IHE XDS-Metadatenattribute auf Ebene von Submission Set, Document Entry sowie Folder vorgenommen. Diese Nutzungsvorgaben referenzieren größtenteils Value Sets der IHE Deutschland Arbeitsgruppe "XDS Value Sets" [IHE-ITI-VS] und sind für die ePA-Fachanwendung verbindlich. Diese XDS-Value Sets sind teilweise von IHE-Deutschland als "offen" gekennzeichnet, um Erweiterungen flexibel einbringen zu können. Für die ePA-Fachanwendung gelten jedoch definierte Vorgaben, wie neue Codes und Value Sets sicher über eine Konfigurationsschnittstelle eingebracht werden können. Daher sind die in dieser Spezifikation beschriebenen Nutzungsvorgaben für Value Sets als fest anzusehen bzw. die Offenheit der XDS Value Sets wird nicht unterstützt.

3.13.1.8.1 Allgemeine Metadatenvorgaben

Die Spalten der unten dargestellten, tabellarischen Übersichten für die Metadaten von Dokumenten (IHE XDS.b Document Entry) und Übertragungspaketen (IHE XDS.b Submission Set) haben die folgenden Bedeutungen:

- Die Spalte "Metadatenattribut XDS.b" listet alle aus dem IHE ITI TF vorgesehenen Metadaten für Document Entry- und Submission Set-Elemente auf.
- Die Spalten "Mult. PS" (Multiplizität Primärsystem; alle Primärsysteme außer PS-KTR), "Mult. KTR" (Multiplizität "PS-KTR"), "Mult. DS" (Multiplizität "Document Service"), "Mult. FV" (Multiplizität "ePA-Frontend des Versicherten") kennzeichnen

die Multiplizität des Metadatenattributs beim Erzeugen oder Verarbeiten durch das jeweilige System.

Die Angabe der jeweiligen Spalte entspricht einem Wertebereich. Die Zeichen [...] für Wertebereich wurden zum Zwecke der besseren Darstellbarkeit weggelassen.

- Die Spalte "Kurzbeschreibung" beschreibt kurz die Bedeutung des Metadatenattributs.
- Die Spalte "Nutzungsvorgabe" macht Bedingungen für die Verwendung eines Metadatenattributs (z. B. erlaubte Wertebereiche und Formatangaben), welche über die im IHE ITI TF definierten Vorgaben hinausgehen.
- Die Spalte "FV Edit" beschreibt, ob ein bestimmtes Metadatenattribut beim Einstellen eines Dokuments über das ePA-FdV durch den Versicherten veränderbar gestaltet werden muss. Es sollten dabei immer nur die für den aktuellen Workflow relevanten Metadatenattribute angezeigt werden, um die Komplexität für den Versicherten gering zu halten. Veränderbar gestaltete Metadatenattribute müssen mit sinnvollen Default-Werten vorbelegt werden.

A_14760-25 - Nutzungsvorgaben für die Verwendung von XDS-Metadaten

Der XDS Document Service MUSS sicherstellen, dass Primärsysteme und das ePA-Frontend des Versicherten zur Registrierung von Dokumenten die nachstehenden Nutzungsvorgaben für Metadaten berücksichtigen. Der XDS Document Service MUSS diese Metadaten verarbeiten können und diese Metadaten ggf. während des Registriervorgangs ergänzen. Metadaten können über die Operationen

- `I_Document_Management::ProvideAndRegisterDocumentSet-b` sowie
- `I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b`

registriert oder über die Operationen

- `I_Document_Management::RestrictedUpdateDocumentSet`
- `I_Document_Management_Insurant::RestrictedUpdateDocumentSet`

geändert werden.

Für den Produkttyp DiGA gelten die gleichen Vorgaben wie für die Primärsysteme sofern unter Nutzungsvorgaben keine abweichenden Bedingungen definiert werden.

Tabelle 30: Nutzungsvorgaben für Metadatenattribute XDS

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
Metadaten für DocumentEntry							
author	1. .n	1. .1	0. .0	0. .n	Person oder System, welche(s) das Dokument erstellt hat	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.1] genügen. Das Primärsystem MUSS mindestens das Subattribut authorPerson oder authorInstitution inhaltlich belegen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorPerson	0. .1	0. .1	0. .0	0. .1	Name des Autors	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 3.13.1.8.2- <u>Metadaten der Dokumente und SubmissionSets</u> genügen.	X
authorInstitution	0. .n	0. .n	0. .0	0. .n	Institution, die dem Autor zugeordnet ist	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt 3.13.1.8.2- <u>Metadaten der Dokumente und SubmissionSets</u> (A_21209) genügen.	X
authorRole	0. .n	0. .n	0. .0	0. .n	Rolle des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS aus [gemTerminology] entsprechen.	X
authorSpecialty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung des Autors	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorSpecialtyVS aus [gemTerminology] entsprechen.	X
authorTelecommunication	0. .n	0. .0	0. .0	0. .n	Telekommunikationsdaten des Autors	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.1.4.5] genügen.	X
availabilityStatus	0. .0	0. .0	1. .1	0. .0	Status des Dokuments ("Approved" oder "Deprecated")	Der Wert MUSS initial "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
classCode	1. .1	1. .1	0. .0	1. .1	Grobe Klassifizierung des Dokuments	<p>Der Wert MUSS einem Code des Value Sets EPAXDSClassCodeVS aus [gemTerminology] entsprechen.</p> <p>Sofern das Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9: <u>Strukturierte Dokumente</u> genügen.</p> <p>PS-KTR MUSS für Dokumente</p> <ul style="list-style-type: none"> der Kategorie receipt ausschließlich den Code "ADM" (Administratives Dokument) verwenden und für solche der Kategorie health_risk_analysis den Code "ASM" (Assessment) verwenden. 	X
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.4] genügen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
confidentialityCode	0. .n	0. .n	0. .1	0. .n	Vertraulichkeitskennzeichnung des Dokuments	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3# 4.2.3.2.5] genügen und einem Code des Value Sets EPAXDSConfidentialityCodeVS aus [gemTerminology] entsprechen.</p> <p>Für ProvideAndRegisterDocuments et-b MUSS für das Verbergen des Dokumentes der Code</p> <ul style="list-style-type: none"> Code = "CON", Display Name = "constraint" <p>aus dem Code System 1.2.276.0.76.5.491 (siehe auch Value Set EPAXDSConfidentialityCodeVS aus [gemTerminology]) gesetzt werden.</p>	X
creationTime	1. .1	1. .1	0. .0	1. .1	Erstellungszeitpunkt des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.6] genügen und DARF NICHT in der Zukunft liegen. Bei der Prüfung ist eine Toleranz von 5 Minuten zulässig.	X
entryUUID	1. .1	1. .1	0. .1	1. .1	Intern verwendete, aktenweit eindeutige Kennung des Dokuments	<p>Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.7] genügen.</p> <p>Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.</p>	
eventCodeList	0. .n	0. .0	0. .0	0. .n	Ereignisse, die zur Erstellung des Dokuments geführt haben.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.8] genügen und einem Code des Value Sets EPAXDSEventCodeVS aus [gemTerminology] entsprechen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
formatCode	1. .1	1. .1	0. .0	1. .1	Global eindeutiger Code für das Dokumentenform at. Zusammen mit dem DocumentEntry.t ypeCode eines Dokuments soll es einem potentiellen zugreifenden System erlauben, im Vorfeld festzustellen, ob das Dokument verarbeitet werden kann.	Der Wert MUSS einem Code des Value Sets EPAXDSFormatCode aus [gemTerminology] entsprechen. Der Wert KANN "urn:ihe:iti:xds:2017:mimeT ypeSufficient" (siehe [IHE- ITI-TF-3#4.2.3.2.9]) entsprechen, um anzuzeigen, dass über den MIME-Type hinaus keine genaueren Angaben zum Dokumentenformat gemacht werden können oder der MIME- Type ausreichend ist. Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9- Strukturierte Dokumente genügen.	
hash	0. .0	0. .0	1. .1	0. .0	Kryptographische Prüfsumme des Dokuments	Der Wert wird vom XDS Document Service beim Einstellen des Dokuments in die Akte berechnet.	
healthcareFacilit yTypeCode	1. .1	1. .1	0. .0	1. .1	Art der Einrichtung, in der das dokumentierte Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSHealthcareFacilityTypeC odeVS aus [gemTerminology] entsprechen. Das PS-KTR MUSS healthcareFacilityTypeCode ausschließlich mit dem Wert "VER" (Versicherungsträger) belegen. Die DiGA MUSS healthcareFacilityTypeCo de mit dem Wert "PAT" belegen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
homeCommunityId	0. .1	0. .1	0. .0	0. .1		n/a Eine optional übertragene homeCommunityId wird nicht gespeichert.	
languageCode	1. .1	1. .1	0. .0	1. .1	Sprache, in der das Dokument abgefasst ist.	Der Wert MUSS einem Code des Value Sets EPAXDSLlanguageCodeVS aus [gemTerminology] entsprechen. Es MÜSSEN mindestens die in der Tabelle Tab_LanguageCodes angegebenen Codes unterstützt werden, alle weiteren Codes KÖNNEN unterstützt werden.	X
legalAuthenticator	0. .1	0. .0	0. .0	0. .1	Rechtlich Verantwortlicher für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.14] genügen. Das Attribut DARF NICHT gesetzt werden, falls es sich um ein automatisch erstelltes und nicht durch eine natürliche Person freigegebenes Dokument handelt.	
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierungsattri- but, dass das Metadateneleme- nt DocumentEntry nicht den vollständigen Satz an Metadaten enthält.		

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
contentType	1. .1	1. .1	0. .0	1. .1	MIME-Type des Dokuments	<p>Ein Wert aus der folgenden Liste gemäß A_24864* und A_25009* MUSS als MIME-Type verwendet werden.</p> <p>PS-KTR MUSS für Dokumente der Kategorie health_risk_analysis ausschließlich den Wert "application/pdf" gemäß A_25009-* verwenden. Als formatCode ist dann entsprechend "urn:ihe:iti:xds:2017:mimeTypeSufficient" zu verwenden</p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Vorgaben aus Abschnitt 3.13.1.9-<u>Strukturierte Dokumente</u> genügen. <u>Anmerkung:</u> In Klammern sind die Extentions angegeben, die beim entsprechenden MIME-Type in DocumentEntry.URI für das URI-scheme "file," zu verwenden sind.</p>	
objectType	1. .1	1. .1	0. .0	1. .1	Typ des Dokuments	<p>Der Wert MUSS immer "urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1" betragen. Dieser Wert steht für stabile Dokumente im IHE ITI XDS.b-Profil [IHE-ITI-TF3#4.2.5.2].</p>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
patientId	1. .1	1. .1	0. .0	1. .1	Systemweit eindeutige Kennung des Patienten	Der Wert MUSS den Inhalts- und Formatvorgaben aus A_14974* genügen. Außerdem MUSS der Wert der Identität des Akteninhabers entsprechen und MUSS vom XDS Document Service dahingehend bei Registrierung der Metadaten geprüft werden.	
practiceSettingC ode	1. .1	0. .0	0. .0	1. .1	Art der Fachrichtung der erstellenden Einrichtung, in der das dokumentiere Ereignis stattgefunden hat.	Der Wert MUSS einem Code des Value Sets EPAXDSPracticeSettingCodeVS aus [gemTerminology] entsprechen. Die DiGA MUSS practiceSettingCode mit dem Wert "PAT" belegen.	X
referenceIdList	0. .n	0. .1	1. .1	0. .n	Liste von IDs, mit denen das Dokument assoziiert wird.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.28] genügen. Wenn KTR-Clients einen Wert übertragen, muss es sich um die rootDocumentId im Rahmen einer RMU-Operation (Aktualisierung) oder dem Ersetzen (RPLC) eines Dokuments handeln.	
repositoryUniqu eId	0. .1	0. .1	1. .1	0. .1	Kennung des Document Repository, in welches das Dokument eingestellt wird/wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.2.18] genügen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
serviceStartTime	0. .1	0. .1	0. .0	0. .1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis begonnen wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.19] genügen.	X
serviceStopTime	0. .1	0. .1	0. .0	0. .1	Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis beendet wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.20] genügen.	X
size	0. .0	0. .0	1. .1	0. .0	Größe des Dokuments in Bytes	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.21] genügen. Der XDS Document Service MUSS die Größe des Dokuments berechnen und in den Metadaten während des Registriervorgangs setzen (vgl. [IHE-ITI-TF2b#3.41.4.1.3]).	
sourcePatientId	0. .1	0. .0	0. .0	0. .0	Kennung des Patienten im Quellsystem	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.22] genügen.	
sourcePatientInfo	0. .n	0. .0	0. .0	0. .0	Demographische Daten zum Patienten im Quellsystem	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.23] genügen.	
title	1. .1	1. .1	1. .1	1. .1	Titel des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.24] genügen. Ein leeres Feld <code>DocumentEntry.title=""</code> bzw. ausschließlich mit nicht druckbaren Zeichen befüllt ist nicht erlaubt.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
typeCode	1. .1	1. .1	0. .0	1. .1	Art des Dokuments	<p>Der Wert MUSS einem Code des Value Sets EPAXDSTypeCodeVS aus [gemTerminology] entsprechen.</p> <p>PS-KTR MUSS für Dokumente der Kategorie health_risk_analysis ausschließlich den Code "GRIS" verwenden</p> <p>Sofern das zu beschreibende Dokument ein durch die gematik definiertes, strukturiertes Dokument ist, MUSS der Wert den Inhalts- und Formatvorgaben aus Abschnitt 3.13.1.9-<u>Strukturierte Dokumente</u> genügen.</p>	X
uniqueId	1. .1	1. .1	0. .0	1. .1	Eindeutige, aktenweite Kennung des Dokuments	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.26] genügen.	
URI	1. .1	1. .1	0. .0	1. .1	URI für das Dokument	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.2.27] genügen und mittels A_24524-* normalisiert werden. Die extension der DocumentEntry.URI MUSS wird dem mimetype gemäß A_23447-* angepasst, falls erforderlich.	
Metadaten für SubmissionSet							
author	1. .n	1. .1	0. .0	1. .1	Person oder System, welche(s) das Submission Set erstellt hat.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.1] genügen.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorPerson	0. .1	0. .1	0. .0	0. .1	Name der einstellenden Per son oder des einstellenden Systems	<p>Der Wert MUSS den Formatvorgaben aus Abschnitt <u>3.13.1.8.2- Metadaten der Dokumente und SubmissionSets</u> genügen.</p> <p>ePA-FdV: Das ePA-Aktensystem MUSS die KVNR mit den Inhalten der User Session auf Übereinstimmung prüfen. Eine Gleichheit liegt vor, wenn die KVNR aus der XCN-Struktur des Autors nach den Vorgaben von A_14762-* mit dem entsprechenden Wert aus der User Session übereinstimmt. Ist authorPerson nicht gesetzt, MUSS das ePA Aktensystem das Metadatenattribut authorPerson für Versicherte entsprechend der Vorgaben aus A_14762-* unter Verwendung der entsprechenden Informationen aus der User Session (KVNR, family_name und given_name) setzen.</p> <p>Das ePA Aktensystem KANN in einer übergebenen authorPerson den Nachnamen und Vornamen mit Informationen aus der User Session überschreiben.</p> <p>PS/DiGAs können hier im Bedarfsfall Einträge für Software-Komponente bzw. Gerät als Autor entsprechend A_14762-* vornehmen.</p>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorInstitution	0. .1	0. .1	0. .0	0. .0	Institution, welcher die einstellende Pers on oder das einstellende System zugeordnet ist.	<p>Der Wert MUSS den Formatvorgaben aus Abschnitt <u>3.13.1.8.2- Metadaten der Dokumente und SubmissionSets (A_21209*)</u> genügen.</p> <p>Das ePA-Aktensystem MUSS die Identität von TelematikID-basierten Identitäten mit den Inhalten aus authorInstitution prüfen.</p> <p>Eine Gleichheit liegt vor, wenn Telematik-ID aus der XCN-Struktur des Autors nach den Vorgaben von A_14763-* bzw. A_21511-* mit dem entsprechenden Wert aus der User Session übereinstimmt.</p> <p>Ist authorInstitution nicht gesetzt, MUSS das ePA Aktensystem das Metadatenattribut authorInstitution entsprechend der Vorgaben aus A_14763-* bzw. A_21511-* unter Verwendung der entsprechenden Informationen aus der User Session (organizationName und idNummer) setzen.</p>	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
authorRole	1. .n	1. .n	0. .0	1. .1	Rolle der einstellenden Per son oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorRoleVS aus [gemTerminology] entsprechen. Das PS-KTR MUSS den Code "105" (Kostenträgervertreter) verwenden. Das ePA-Frontend des Versicherten MUSS den Code "102" (der Patient selbst) verwenden. Die DiGA MUSS authorRole mit dem Code "12" (dokumentierendes Gerät) verwenden.	
authorSpecial ty	0. .n	0. .0	0. .0	0. .n	Fachliche Spezialisierung der einstellenden Per son oder des einstellenden Systems	Der Wert MUSS einem Code des Value Sets EPAXDSAauthorSpecialtyVS aus [gemTerminology] entsprechen.	
authorTeleco mmunication	0. .n	0. .0	0. .0	0. .n	Telekommunikati onsdaten der einstellenden Person oder des einstellenden Systems	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.1.4.5] genügen.	
availabilityStatu s	0. .0	0. .0	1. .1	0. .0	Status des Submission Sets ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approved" entsprechen.	
comments	0. .1	0. .1	0. .0	0. .1	Ergänzende Hinweise zum Submission Set in Freitext	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.3.3] genügen.	X

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
contentTypeCode	0. .1	0. .1	0. .0	0. .1	Klinische Aktivität, die zum Einstellen des Submission Set geführt hat.	Der Wert MUSS einem Code des Value Sets EPAXDSContentTypeCodeVS aus [gemTerminology] entsprechen.	
entryUUID	1. .1	1. .1	0. .1	1. .1	Intern verwendete, aktenweit eindeutige Kennung des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.3.5] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI- TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
intendedRecipient	0. .n	0. .0	0. .0	0. .n	Vorgesehener Adressat des Submission Set	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.3.7] genügen.	
limitedMetadata	0. .0	0. .0	0. .0	0. .0	Markierung, welche anzeigt, dass das Submission Set nicht den durch das IHE ITI TF vorgegebenen Satz an Metadaten enthält.		
patientId	1. .1	1. .1	0. .0	1. .1	Patienten-ID, zu der das Submission Set gehört	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
sourceId	0. .0	0. .0	0. .0	0. .0	Weltweit eindeutige, unveränderliche Kennung des einstellenden Systems		

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
submissionTime	1. .1	1. .1	0. .0	1. .1	Zeit, zu der das Submission Set zusammengestellt wurde.	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.10] genügen. Der XDS Document Service MUSS prüfen, ob der Wert der aktuellen Systemzeit entspricht. Sollte diese von der lokalen Zeit über mehr als eine Minute abweichen, MUSS der Wert mit der aktuellen Systemzeit ersetzt werden. Diese Systemzeit MUSS dabei synchron zur Systemzeit des Produkttyps Zeitdienst gemäß A_24673 sein.	
title	0. .1	0. .1	0. .0	0. .1	Titel des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.11] genügen.	X
uniqueId	1. .1	1. .1	0. .0	1. .1	Eindeutige Kennung des Submission Sets	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.3.12] genügen.	
Metadaten für dynamische Folder							
availabilityStatus	1. .1	n/ a	0. .0	n/ a	Status des Ordners ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml-regrep:StatusType:Approved" entsprechen.	
codeList	1. .1	n/ a	0. .0	n/ a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI-TF3#4.2.3.4.2] und einem Code des Value Sets EPADataCategoryOtherVS aus [gemTerminology] entsprechen. Bei Folder.codeList=pregnancy_childbirth MUSS das Primärsystem diese Codes angeben.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
comments	0. .1	n/ a	0. .0	n/ a	Freitextkommentar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.3] entsprechen.	
entryUUID	1. .1	n/ a	1. .1	n/ a	Intern verwendete, aktenweit eindeutige Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI-TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
lastUpdateTime	0. .0	n/ a	1. .1	n/ a	Zeitstempel, an dem der Ordner das letzte mal geändert wurde	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.6] genügen. Der XDS Document Service MUSS den Wert automatisch gemäß [IHE-ITI-TF2b#3.42.4.1.3.6] aktuell halten.	
limitedMetadata	Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden.						
patientId	1. .1	n/ a	0. .0	n/ a	Patienten ID, zu der der Ordner gehört.	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
title	1. .1	n/ a	0. .0	n/ a	Titel des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.8] genügen.	
uniqueId	1. .1	n/ a	0. .0	n/ a	Eindeutige, aktenweite Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.9] genügen.	
Metadaten für statische Folder							

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
availabilityStatus	n/a	n/a	1. .1	n/a	Status des Ordnern ("Approved")	Der Wert MUSS "urn:oasis:names:tc:ebxml- regrep:StatusType:Approved" entsprechen.	
codeList	n/a	n/a	1. .1	n/a	Liste von Codes, die mit dem Ordner assoziiert werden.	Der Wert MUSS den Inhalts- und Formatvorgaben aus Abschnitt [IHE-ITI- TF3#4.2.3.4.2] und einem Code des Value Sets EPADataCategoryOtherVS und EPADataCategoryMedicalVS aus [gemTerminology] entsprechen. Der XDS Document Service MUSS codeList gemäß A_19388* setzen.	
comments	n/a	n/a	0. .1	n/a	Freitextkomment ar für diesen Ordner.	Der Wert MUSS den Inhalts- und Formatvorgaben aus [IHE- ITI-TF3#4.2.3.4.3] entsprechen.	
entryUUID	n/a	n/a	1. .1	n/a	Intern verwendete, aktenweit eindeutige Kennung des Ordnern	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.4] genügen. Der XDS Document Service MUSS symbolische IDs gemäß [IHE-ITI- TF2b#3.42.4.1.3.7] auflösen.	
homeCommunityId	siehe Vorgaben zu DocumentEntry.homeCommunityId						
lastUpdateTime	n/a	n/a	1. .1	n/a	Zeitstempel, an dem der Ordner das letzte mal geändert wurde	Der Wert MUSS den Formatvorgaben aus [IHE-ITI- TF3#4.2.3.4.6] genügen. Der XDS Document Service MUSS den Wert automatisch gemäß [IHE-ITI- TF2b#3.42.4.1.3.6] aktuell halten.	

Metadaten- attribut XDS.b	Multiplizität				Kurz- beschreibung	Nutzungsvorgabe	F V E d i t
	P S	K T R	D S	F d V			
limitedMetadata	Der Wert MUSS analog zu DocumentEntry.limitedMetadata belegt werden.						
patientId	n/ a	n/ a	1. .1	n/ a	Patienten ID, zu der der Ordner gehört.	Der Wert MUSS analog zu DocumentEntry.patientId belegt werden.	
title	n/ a	n/ a	1. .1	n/ a	Titel des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.8] genügen. Der Wert MUSS redundant gefüllt werden mit Folder.Codelist.Code.displayName.	
uniqueId	n/ a	n/ a	1. .1	n/ a	Eindeutige, aktenweite Kennung des Ordners	Der Wert MUSS den Formatvorgaben aus [IHE-ITI-TF3#4.2.3.4.9] genügen.	

Tabelle 31: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language Codes

Language / Country Code Kombination	Language / Country Code Kombination
bg-BG (bulgarisch, Bulgarien)	it-IT (italienisch, Italien) it-CH (italienisch, Schweiz)
cs-CZ (tschechisch, Tschechien)	lt-LT (litauisch, Litauen)
da-DK (dänisch, Dänemark)	lb-LU (luxemburgisch, Luxemburg)
de-AT (deutsch, Österreich) de-DE (deutsch, Deutschland) de-CH (deutsch, Schweiz) de-LI (deutsch, Liechtenstein) de-LU (deutsch, Luxemburg)	lv-LV (lettisch, Lettland)
el-GR (griechisch, Griechenland)	mt-MT (maltesisch, Malta)
en-GB (englisch, Vereinigtes Königreich)	nl-NL (niederländisch, Niederlande) nl-BE (niederländisch, Belgien)
es-ES (spanisch, Spanien)	no-NO (norwegisch, Norwegen)

Language / Country Code Kombination	Language / Country Code Kombination
et-EE (estnisch, Estland)	pl-PL (polnisch, Polen)
fi-FI (finnisch, Finnland)	pt-PT (portugiesisch, Portugal)
fr-FR (französisch, Frankreich) fr-CH (französisch, Schweiz) fr-LU (französisch, Luxemburg) fr-BE (französisch, Belgien)	rm-CH (rätoromanisch, Schweiz)
ga-IE (irisch, Irland)	ro-RO (rumänisch, Rumänien)
hr-HR (kroatisch, Kroatien)	sk-SK (slowakisch, Slowakei)
hu-HU (ungarisch, Ungarn)	sl-SI (slowenisch, Slowenien)
is-IS (isländisch, Island)	sv-SE (schwedisch, Schweden)

[<=]

3.13.1.8.2 Metadaten der Dokumente und SubmissionSets

A_23369-02 - XDS Document Service – Verpflichtender Dokumententitel in DocumentEntry.title

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Metadaten an Dokumenten `DocumentEntry.title` befüllen. Der Titel des Dokumentes soll eine fachliche Beschreibung des Dokumentes enthalten. Bei `DocumentEntry.title` MÜSSEN führende und endende Leerzeichen entfernt werden. In `DocumentEntry.title` DARF NICHT leer sein (`!= ""`) (insbesondere auch nicht nach etwaigen Entfernen von Leerzeichen vorne und hinten). In `Document.title` DÜRFEN keine nicht-druckbaren Zeichen enthalten sein. [≤]

A_25188 - XDS Document Service - Input Sanitization

Der XDS Document Service MUSS sicherstellen, dass bei Anlage und Aktualisierung (Ändern) von Metadaten:

1. führende (leading) und endende (trailing) Whitespace von den Attributen automatisch entfernt werden.
2. die notwendigen Attribute nichtleer sind (insbeondere auch noch Whitespace-Entfernung aus 1.). und
3. Die Attribute nur druckbare Zeichen enthalten.

[<=]

A_14762-05 - XDS Document Service – Nutzungsvorgabe für authorPerson als Teil von DocumentEntry.author und SubmissionSet.author

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an `authorPerson` unterhalb von `DocumentEntry.author` und `SubmissionSet.author` neben [IHE-ITI-TF3#4.2.3.1.4.2] auch die folgenden Vorgaben beachten.

Bei Leistungserbringer als Autor:

1. Lebenslange Identifikationsnummer eines Arztes (Lebenslange Arztnummer - LANR 9 Stellen) oder im Falle eines Zahnarztes die Zentrale Zahnarzt Nummer (ZANR)- sofern die ZANR bekannt ist
2. "^"
3. Nachname
4. "^"
5. Vorname
6. "^"
7. Weiterer Vorname
8. "^"
9. Namenszusatz
10. "^"
11. Titel
12. "^^^&" - sofern LANR oder ZANR angegeben, ansonsten "^^^"
13. "1.2.276.0.76.4.16" - sofern LANR angegeben oder "1.2.276.0.76.4.296", falls ZANR angegeben
14. "&ISO" - sofern LANR oder ZANR angegeben

Beispiele:

165746304^Weber^Thilo^^^Dr.^^^&1.2.276.0.76.4.16&ISO
^Zahnschmerz^Eberhard^^^Dr.^^^

Bei Versichertem als Autor:

1. Der unveränderbare Teil der KVNR (10 Stellen)
2. "^"
3. Nachname
4. "^"
5. Vorname
6. "^"
7. Weiterer Vorname
8. "^"
9. Namenszusatz
10. "^"
11. Titel
12. "^^^&"
13. "1.2.276.0.76.4.8"
14. "&ISO"

Beispiel: G995030566^Gundlach^Monika^^^^^&1.2.276.0.76.4.8&ISO

Sowohl beim LE als auch beim Versicherten müssen Vorname und Nachname belegt werden.

Software-Komponente bzw. Gerät als Autor

Beim (automatisierten) Einstellen von Dokumenten MUSS der max. 256-Zeichen lange Name der Software-Komponente bzw. des Geräts als Nachname und ggf. als Vorname(n) eingetragen werden.

Beispiel: ^PHR-Gerät-XY^PHR-Software-XY

Im Falle einer DiGA MUSS das Feld Autor folgendermaßen aufgebaut sein:

1. Telematik-ID der DiGA
2. "^"
3. Name der DiGA (Name der Verordnungseinheit)
4. "^"
5. Name des DiGA-Herstellers
6. "^"
7. optionale Ergänzung der Bezeichnung der SW
8. "^"
9. optionale Ergänzung der Bezeichnung der SW
10. "^"
11. optionale Ergänzung der Bezeichnung der SW
12. "^^^&"
13. <OID für DiGAs, wie in professionOID>
14. "&ISO"

Für alle drei Arten von Autoren (Versicherter, LE, Gerät) MUSS jeweils Vorname und Nachname angegeben sein. [<=]

A_14763-03 - XDS Document Service - Nutzungsvorgabe für SubmissionSet.authorInstitution

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an

SubmissionSet.authorInstitution neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

Beispiele:

- Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-e518

- gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^8-34923902a

[<=]

A_21511-01 - Nutzungsvorgabe SubmissionSet.authorInstitution für DIGAs

Der XDS Document Service MUSS sicherstellen, dass DiGAs beim Upload von Dokumenten, die folgenden Nutzungsvorgaben für das Metadatenattribut DocumentEntry.authorInstitution sowie SubmissionSet.authorInstitution berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.1.4.1] genügen und ist inhaltlich nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen.

1. Name des Anbieters der DiGA
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der DiGA

[<=]

A_21209-02 - XDS Document Service - Nutzungsvorgabe für DocumentEntry.authorInstitution

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten an DocumentEntry.authorInstitution neben [IHE-ITI-TF3#4.2.3.1.4.1] auch die folgenden Vorgaben beachten.

1. Name der Leistungserbringerinstitution oder Name des Kostenträgers
2. "^^^^^&"
3. "1.2.276.0.76.4.188" (OID zur Kennzeichnung einer Institution über eine Telematik-ID)
4. "&ISO^^^^"
5. Telematik-ID der Leistungserbringerinstitution oder des Kostenträgers

Die Komponenten 2.-5. sind nur anzugeben, wenn die Telematik ID (5.) der Autoreninstitution bekannt ist oder ad-hoc ermittelt werden kann, bspw. über den Verzeichnisdienst der TI-Plattform (VZD). Ansonsten wird ausschließlich der Name gesetzt.

Beispiele:

- Arztpraxis Dr. Thilo Weber^^^^^&1.2.276.0.76.4.188&ISO^^^^1-2c47sd-e518
- gematik Betriebskrankenkasse^^^^^&1.2.276.0.76.4.188&ISO^^^^8-34923902a
- Arztpraxis Dr. Wiebke Werner

[<=]

A_22408-02 - XDS Document Service - DocumentEntry.authorInstitution ohne Telematik-ID

Der XDS Document Service MUSS Nachrichten zum Registrieren von Dokumenten bei fehlender Telematik-ID in `DocumentEntry.authorInstitution` akzeptieren und daraufhin alle Zeichen hinter dem Namen der `authorInstitution` abschneiden und verwerfen. [≤]

A_14974-02 - XDS Document Service - Nutzungsvorgabe für `DocumentEntry.patientId` und `SubmissionSet.patientId`

Der XDS Document Service MUSS sicherstellen, dass ePA-Clients beim Upload von Dokumenten und dem Ändern von Dokumenten-Metadaten die folgenden Nutzungsvorgaben für `DocumentEntry.patientId` und `SubmissionSet.patientId` berücksichtigen. Der Wert MUSS den Vorgaben aus [IHE-ITI-TF3#4.2.3.2.16] bzw. [IHE-ITI-TF3#4.2.3.3.8] genügen und ist inhaltlich nach der folgenden Vorschrift zusammenzufügen bzw. zu belegen:

1. Der unveränderbare Teil der KVN-R des Akteninhabers (10 Stellen)
2. "^^^&"
3. "1.2.276.0.76.4.8" (OID zur Kennzeichnung einer unveränderbaren KVN-R)
4. "&ISO"

Beispiel: G995030566^^^&1.2.276.0.76.4.8&ISO [≤]

3.13.1.8.3 Metadaten für Datenkategorien

A_19388-21 - Nutzungsvorgaben für die Verwendung von Datenkategorien

Der XDS Document Service MUSS beim Einstellen eines Dokuments und beim Ändern von Metadaten die folgende Zuordnung zu einer Datenkategorie (d. h. Assoziierung mit einem bestimmten Folder) vornehmen. Dabei haben Auswertungs- und Zuordnungsregeln, die sich aus A_14761-* und damit verbunden aus [gemSpec_IG_ePA] ableiten, immer den Vorrang gegenüber anderen Auswertungsregeln. Ferner MUSS der XDS Document Service sicherstellen, dass bei einer Aktualisierung eines Dokuments derselbe Ordner des zu ersetzenden Dokuments zugeordnet wird.

Für eine eindeutige Zuordnung zu einer Datenkategorie MUSS die Auswertung der Metadatenvorgaben in der Reihenfolge der folgend dargestellten Einsortierungskriterien erfolgen:

Tabelle 32: Einsortierung_Datenkategorien

Datenkategorie/Technischer Identifier/Foldercode	Einsortierkriterium (anzuwenden auf <code>DocumentEntry</code> , wenn nicht anders angegeben. Oder-Verknüpfungen, wenn nicht "und" angegeben)
receipt	healthcareFacilityTypeCode = VER und typeCode = ABRE und <code>DocumentEntry.authorRole</code> =105 und <code>SubmissionSet.authorRole</code> = 105
health_risk_analysis	healthcareFacilityTypeCode = VER und typeCode = GRIS und <code>DocumentEntry.authorRole</code> =105 und <code>SubmissionSet.authorRole</code> = 105

Datenkategorie/Technischer Identifier/Foldercode	Einsortierkriterium (anzuwenden auf DocumentEntry, wenn nicht anders angegeben. Oder-Verknüpfungen, wenn nicht "und" angegeben)
patient	Dokumente bei denen der Einsteller der Versicherte oder sein Vertreter ist: Submissionset.authorRole = 102 Dokumente bei denen der Einsteller der Kostenträger ist: Submissionset.authorRole = 105
pregnancy_childbirth	healthcareFacilityTypeCode = HEB eventCodeList=SD070104 (KDL-Code Neugeborenenenscreening)
eab	classCode = BRI
care	PracticeSettingCode = PFL*
rehab	practiceSettingCode = REHA
dental	practiceSettingCode = MZKH*
emergency	eventCodeList = <ul style="list-style-type: none"> • ED110102 (KDL-Code Notfalldatenmanagement (NFDm)) • AU190104 (KDL-Code Notfalldatensatz) • AD020105 (KDL-Code Notfall-/Vertretungsschein)
transcripts	eventCodeList = <ul style="list-style-type: none"> • UB999997 (KDL-Code Gesamtdokumentation stationäre Versorgung) oder • UB999998 (KDL-Code Gesamtdokumentation ambulante Versorgung)
reports	classCode = ANF, ASM, BEF, BIL, DOK, DUR, LAB oder PLA
other	Alle Dokumente, die in keine andere Kategorien eingeordnet werden können

*Falls Basiskonzepte angegeben werden, dann gelten automatisch alle Subkonzepte, z.B. gilt für die Kategorie "care" die Einsortierregel bei PracticeSettingCode = PFL wie auch für die Sub-Konzepte ALT (Altenpflege) und KIN (Kinderpflege).【<=】

3.13.1.9 Strukturierte Dokumente

Die elektronische Patientenakte unterstützt unterschiedliche sogenannte "strukturierte Dokumente", deren Aufbau über Implementation Guides genau vorgegeben ist. Der

Umfang der unterstützten strukturierten Dokumente wird durch den Umfang der veröffentlichten Implementation Guides festgelegt (3.13.1.9.2- Konfigurierbarkeit). Für alle strukturierten Dokumente gelten spezifische Metadatenvorgaben, um sie eindeutig zu identifizieren und gezielt verarbeiten zu können.

A_14761-08 - Nutzungsvorgaben für die Verwendung von IHE ITI XDS-Metadaten bei strukturierten Dokumenten

Der XDS Document Service MUSS die Nutzungsvorgaben für strukturierte Dokumente unter [gemSpec_IG_ePA] berücksichtigen. Dabei ist das Format des Dokuments, welches über einen Code des Metadatenattributs `formatCode` ausgedrückt wird, führend. Das bedeutet, bei Registrierung eines strukturierten Dokuments mit einem `formatCode` MÜSSEN die weiteren Metadatenattribute `classCode`, `typeCode`, `mimeType` sowie `eventCodeList` entsprechend belegt werden. Der XDS Document Service MUSS eine solche Registrierung diesbzgl. prüfen und im Fehlerfall analog zu A_14938-* antworten. [`<=`]

3.13.1.9.1 Sammlungstypen

Je nach Art ihrer Zusammensetzung und ihrer Handhabung existieren unterschiedliche Typen strukturierter Dokumente, sogenannte medizinische Informationsobjekte. Ein medizinisches Informationsobjekt (MIO) ist eine **Sammlung** von Informationen zu medizinischen, strukturellen oder administrativen Sachverhalten, die in sich geschlossen oder entsprechend verschachtelt vorliegt. Zudem ist ein MIO eine klar definierte Vorgabe, wie diese Informationssammlung in der elektronischen Patientenakte gespeichert wird, damit semantische und syntaktische Interoperabilität gewährleistet werden. Die Festlegung dieser Vorgaben ist gemäß SGB V Aufgabe der KBV. Beispiele für medizinische Informationsobjekte sind der Impfpass, das Kinderuntersuchungsheft, der Mutterpass, das zahnärztliche Bonusheft, oder DiGA. MIOs werden über Sammlungen und Sammlungstypen umgesetzt.

Einige strukturierte Dokumente sind für sich genommen vollständig und schlüssig wie z. B. ein Elektronischer Arztbrief. Sie sind ohne Zuhilfenahme weiterer Dokumente in der ePA für einen Benutzer sinnvoll zu verwenden. Andere Typen strukturierter Dokumente müssen hingegen fast immer in Kombination betrachtet werden, z. B. Impfpassdokumente. Bei letzteren spiegelt jedes Impfpassdokument ein oder mehrere Impfungen wieder. Ein Impfpass, wie er in der analogen Welt geläufig und als logisches Konstrukt sinnvoll ist, besteht immer aus der gemeinsamen Betrachtung aller Impfpassdokumente und somit aller vorhandenen Impfeinträge. Die Kombination ein oder mehrerer strukturierter Dokumente ergeben eine Sammlung.

Eine Sammlungsinstanz (z. B. der Mutterpass der ersten Schwangerschaft der Patientin Martha Mustermann) ist eine konkrete Ausprägung der Information, die zwischen den beteiligten Akteuren ausgetauscht wird. Nicht jede Sammlung besteht zwangsläufig aus Dokumenten desselben Formats: Ein Kinderuntersuchungsheft beispielsweise besteht aus Dokumenten mit drei verschiedenen strukturierten Dokumenttypen. Zentral für alle Sammlungstypen ist immer mindestens ein strukturiertes Dokument mit einem festgelegten Dokumentenformat. Für eine technische Umsetzung sind die Sammlungstypen "mixed" und "uniform" zu unterscheiden, die technisch unterschiedlich umgesetzt werden und zum Teil unterschiedliche Operationen erlauben.

Der Sammlungstyp "mixed" fasst semantisch zusammengehörige, strukturierte Dokumente unterschiedlicher Struktur mittels Ordner zu einer Sammlung zusammen. Der Sammlungstyp "uniform" wird ebenfalls intern über Ordner abgebildet. Dies stellt sicher, dass zukünftige Versionen dieser strukturierten Dokumente/Pässe oder DiGA verlässlich verarbeitet werden können. Ordner gelten als "statische Ordner", bis auf Sammlungen der Kategorie Mutterpass und DiGA ("dynamische Ordner"). Der dynamische Ordner für

einen konkreten Mutterpass wird durch den Client angelegt, weil es aus Gründen, die nur der Client kennt (Anzahl der Schwangerschaften), mehrere Ordner dieses Typs geben kann ("nicht-statische Ordner", vgl. A_21610-*). Die Version der Struktur eines Dokuments ist am Format Code erkennbar.

Passdokumente

A_20577-06 - Definition und Zuweisung von Sammlungstypen

Der XDS Document Service MUSS jeder Sammlung einen von zwei Sammlungstypen zuweisen:

Tabelle 33: TAB_EPA_Sammlungstypen

Sammlungstyp	Definition
mixed	Ordner, die einer Sammlung des Typs "mixed" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) mit einem für die Sammlung festgelegten Code in der Folder.codeList abgelegt werden.
uniform	Ordner, die einer Sammlung des Typs "uniform" angehören, können stets ein oder mehrere strukturierte Dokumente entsprechend der Art der Sammlung enthalten. Alle Dokumente einer Sammlung MÜSSEN in einen Ordner (XDS Folder) abgelegt werden.

Es gelten die Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA]. In den unter [gemSpec_IG_ePA] gemachten Vorgaben werden auch Ordner-Kardinalitäten für spezifische Sammlungen festgelegt. Diese Angaben sagen aus, wie viele Instanzen einer Sammlung (d. h. minimal und maximal) registriert werden können. [\leq]

A_20707-04 - XDS Document Service – Keine unpassenden Dokumente in nicht-statische Ordner

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

A_20581-06 - XDS Document Service – Löschen von Dokumenten aus Sammlungen der Typen "mixed" und "uniform" durch ein ePA-FdV

Der XDS Document Service MUSS beim Löschen eines Dokuments der Sammlungstypen "mixed" und "uniform" durch das ePA-FdV sicherstellen, dass die Operation mit dem Fehler `ReferencesExistException` abgebrochen wird, wenn die Löschanfrage nicht alle Dokumente der Sammlung enthält. Es besteht folgende Ausnahme: Das Löschen einer Elternnotiz im Kinderuntersuchungsheft ist erlaubt. [\leq]

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

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

3.13.1.9.2 Konfigurierbarkeit

A_17546-02 - Konfigurierbarkeit von strukturierten Dokumenten

Der XDS Document Service MUSS die Liste strukturierter Dokumente konfigurierbar machen, indem dieser die Unterstützung strukturierter Dokumente unter Angabe folgender Eigenschaften ermöglicht:

- Vorgaben der Metadaten für strukturierte Dokumente gemäß [gemSpec_IG_ePA] konfigurativ hinzufügen bzw. entfernen,
- Sammlungen zu TAB_EPA_Sammlungstypen gemäß [gemSpec_IG_ePA] konfigurativ hinzufügen bzw. entfernen.

[<=]

Das Entfernen der Unterstützung von strukturierten Dokumenten oder Sammlungen bedeutet, dass diese zu einem früheren Zeitpunkt in das Aktensystem geschrieben werden konnten, aber durch Erreichen von "clientReadOnlyFromDate" nicht mehr geschrieben werden dürfen. Das Schreiben umfasst das Aktualisieren oder neu Anlegen. Das Lesen ist weiterhin erlaubt.

A_17551-01 - Prüfanforderungen zur Konfigurierbarkeit von Value Sets

Der Anbieter des ePA-Aktensystems MUSS sicherstellen, dass die zu konfigurierenden Value Sets des XDS Document Service gemäß der Anforderung A_17546-* den folgenden Prüfkriterien unterliegen, bevor bestehende, im XDS Document Service verarbeitete Value Sets verändert werden:

- Es DÜRFEN KEINE Codes der Value Sets gelöscht werden, lediglich das Hinzufügen von Codes zu existierenden Value Sets ist aus Kompatibilitätsgründen erlaubt.
- Neue Codes MÜSSEN den Formatvorgaben gemäß Tabelle 4.2.3.1.7-2 in [IHE-ITI-TF3#4.2.3.1.7] entsprechen und gegenüber einer internen Referenzliste validiert werden. Dies schließt auch Prüfungen zur Zeichenkodierung, der Datentypen als auch zu den Längenbeschränkungen ein.

[<=]

A_21212-01 - Restriktionen zur Konfigurierbarkeit von Metadaten für strukturierte Dokumente und Sammlungen

Der XDS Document Service MUSS durch technische Maßnahmen sicherstellen, dass Änderungen an den in den Implementierungsvorgaben in [gemSpec_IG_ePA] spezifizierten Codes ausgeschlossen sind.[<=]

A_21214-03 - Konfiguration strukturierter Dokumente im Rahmen der Veröffentlichung durch die gematik

Der Anbieter des ePA-Aktensystems MUSS durch organisatorische Maßnahmen sicherstellen, dass die Konfiguration im Aktensystem zur Unterstützung strukturierter Dokumente aus [gemSpec_IG_ePA] ausschließlich im Rahmen der Veröffentlichung der Implementation Guides durch die gematik erfolgt.[<=]

Bei Einführung neuer strukturierter Dokumente werden die beschriebenen Konfigurationsmöglichkeiten so verwendet, dass eine Erweiterung der Spezifikation und daraus resultierend eine Änderung des ePA-Aktensystems mit erneuter Zulassung nicht erforderlich sind.

3.13.1.10 Verbergen von Dokumenten durch Verwendung des confidentialityCode

Der Versicherte oder ein Vertreter kann vorhandene Dokumente des Aktenkontos durch die Verwendung der General Deny Policy des Constraint Managements verbergen oder sichtbar machen.

Der Versicherte oder ein Vertreter kann ein neues Dokument auch direkt beim Einstellen in das Aktenkonto verbergen. Dazu wird durch den XDS Document Service beim Einstellen bzw. Aktualisieren (Replace) eines Dokuments der `DocumentEntry.confidentialityCode` der Dokumentmetadaten ausgewertet. Enthält der `confidentialityCode` beim Einstellen bzw. Aktualisieren den Wert "CON" (constraint), wird durch das Aktensystem ein Eintrag in der General Deny Policy erzeugt und das Dokument verborgen.

Diese zusätzliche Art des direkten Verbergens ist dabei grundsätzlich nur auf Dokumententypen anwendbar, welche durch einen Versicherten oder einen Vertreter über ein ePA-FdV eingestellt werden können (keine MIOs oder strukturierten Dokumente).

Das Metadatum `DocumentEntry.confidentialityCode` = "CON" (`codeSystem` = `urn:oid:1.2.276.0.76.5.491`):

1. Führt beim Einstellen und Replace eines Dokuments zum Verbergen des Dokuments, d.h. das Dokument wird auf die General Deny Policy des Aktenkontos gesetzt.
2. Wird im Aktensystem nicht persistiert sondern über dort intern über eine General Deny Policy umgesetzt.
3. Wird im ePA-FdV nicht zur Anzeige gebracht und kann dort auch nicht geändert werden.
4. Ein PS darf `DocumentEntry.confidentialityCode` = "CON" nicht verwenden.

3.13.1.11 Auswirkungen bei Widerspruch gegen Funktionen der ePA auf die Dokumente des Aktenkontos

Wird ein Widerspruch gegen die Nutzung einer Funktion der ePA erklärt, verhindert der XDS Document Service, abhängig von der jeweils widersprochenen Funktion, deren weitere Nutzung.

Im Falle eines Widerspruchs gilt:

Tabelle 34: Auswirkungen bei Widerspruch gegen eine Funktion der ePA

widerspruchsfähige Funktion	Auswirkung bei erteiltem Widerspruch
Teilnahme am digital gestützten Medikationsprozess ("medication")	Das Einstellen, Verändern, Lesen oder Suchen von Dokumenten des Ordners "emp" (elektronischer Medikationsplan) wird durch den XDS Document Service abgelehnt. Ausgenommen hiervon sind der Versicherte und befugte Vertreter.

widerspruchsfähige Funktion	Auswirkung bei erteiltem Widerspruch
Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst ("erp-submission")	Alle vorhandenen Dokumente des Ordners "emp" (elektronischer Medikationsplan) werden gelöscht.

Hinweis zum Medikationsprozess: Dadurch wird verhindert, dass Leistungserbringer im Versorgungsprozess veraltete oder unvollständige Daten verwenden.

A_23860 - XDS Document Service - Löschen der Dokumente des Medikationsprozesses

Der XDS Document Service des Aktensystems MUSS alle Dokumente aus dem Ordner elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") löschen, wenn der Status der widerspruchsfähigen Funktion "Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst" (Id = "erp-submission") auf "Widerspruch erklärt" ("deny") geändert wird. [\leq]

A_23895-02 - XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch

Falls ein Widerspruch zur widerspruchsfähigen Funktion "Teilnahme am Medikationsprozess" (Id = "medication" und status = "deny") vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für alle Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid_versicherter), ablehnen und die Operation mit dem Fehlercode ConsentDecisionViolation abrechnen.
[\leq]

A_25151-01 - XDS Document Service – Prüfung der Widersprüche bei Suchanfrage

Der XDS Document Service MUSS bei einer Suchanfrage die Suchergebnismenge für alle Nutzer, ausgenommen der Versicherte oder befugte Vertreter (oid_versicherter), filtern und sicherstellen, dass diese keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält, wenn ein Widerspruch gegen die widerspruchsfähige Funktion "Teilnahme am digital gestützten Medikationsprozess" (Id = "medication" und status = "deny") vorliegt.
[\leq]

3.13.1.12 Auswirkungen bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI auf die Dokumente des Aktenkontos

Wird ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI erklärt, verhindert der XDS Document Service, dass auf die Dokumente der Kategorie "emp" zugegriffen werden kann.

A_26429 - XDS Document Service - Keine Operationen mit Dokumenten des Medikationsprozesses bei Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service das Auslesen, Verändern, Einstellen und Löschen (CRUD) von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") für diese LEI, ablehnen und

die Operation mit dem Fehlercode ConsentDecisionViolation abbrechen.

[<=]

A_26430 - XDS Document Service – Prüfung des Widerspruchs gegen die Nutzung des Medication Service durch eine spezifische LEI bei Suchanfrage

Falls ein Widerspruch gegen die Nutzung des Medication Service durch eine spezifische LEI vorliegt, MUSS der XDS Document Service bei einer Suchanfrage die Suchergebnismenge für diese LEI filtern und sicherstellen, dass die Suchergebnismenge keinerlei XDS-Metadaten von Dokumenten des Ordners elektronischer Medikationsplan (codeSystem = "urn:oid:1.2.276.0.76.5.512"; code = "eMP") enthält.

[<=]

3.13.1.13 Protokollierung von Zugriffen auf den XDS Document Service

A_24715-01 - XDS Document Service - Protokolleinträge für Zugriffe auf den XDS Document Service

Der XDS Document Service MUSS für die Operationen

- ProvideAndRegisterDocumentSet-b,
- RetrieveDocumentSet,
- RemoveMetadata,
- RestrictedUpdateDocumentSet,
- RegistryStoredQuery (entfällt, wenn Nutzung durch den Versicherten erfolgt)

Protokolleinträge gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 35: XDS Document Service Protokollierung

Strukturelement	Wert	Erläuterung
AuditEvent.type	"document"	
AuditEvent.action	C	Für ProvideAndRegisterDocumentSet-b ohne Replace Option
	U	Für ProvideAndRegisterDocumentSet-b mit Replace Option
	U	Für RestrictedUpdateDocumentSet
	R	Für RegistryStoredQuery
	R	Für RetrieveDocumentSet
	D	Für Zugriffe mit RemoveMetadata

Strukturelement	Wert		Erläuterung
AuditEvent.entity.description	<Operation>		ein Wert aus {ProvideAndRegisterDocumentSetb, RetrieveDocumentSet, RemoveMetadata, RestrictedUpdateDocumentSet, RegistryStoredQuery}
Parameterwerte für die Operationen ProvideAndRegisterDocumentSetb, RetrieveDocumentSet und RemoveMetadata			
AuditEvent.entity.name	<DocumentEntry.title>		wenn in der entity Struktur ein XSDDocument beschrieben wird
	<Folder.title>		wenn in der entity Struktur ein XDSFolder beschrieben wird
AuditEvent.entity.detail	type	value[x]	
	"DocumentFormatCode"	<DocumentEntry.formatCode>	wenn in der entity Struktur ein XSDDocument beschrieben wird. kodiert als Datentyp „Coded String“ gemäß [IHE-ITI- TF3]. Wenn es sich beim Wert von DocumentEntry.formatCode um den Code urn:ihe:iti:xds:2017:mimeTypeSufficient (Code System 1.3.6.1.4.1.19376.1.2.3) handelt, MUSS stattdessen der Wert von DocumentEntry.mimeType hier eingetragen werden.
	"DocumentUniqueId"	<Document.uniqueId>	wenn in der entity Struktur ein XSDDocument beschrieben wird
	"FolderTitle"	<Folder.title>	wenn in der entity Struktur ein XDSFolder beschrieben wird
	"FolderCodeList"	<Folder.codeList>	wenn in der entity Struktur ein XDSFolder beschrieben wird kodiert als Datentyp „Coded String“ gemäß [IHE-ITI-TF3] z.B. "pregnancy_childbirth^^^&1.2.276.0.76.5.512&ISO"
	"FolderEntryUUID"	<Folder.entryUUID>	wenn in der entity Struktur ein XDSFolder beschrieben wird
Parameterwerte für die Operation RegistryStoredQuery der Schnittstellen I_Document_Management und I_Document_Management_Insurant (nur Vertreter)			

Strukturelement	Wert		Erläuterung
AuditEvent.entity.name	"AdhocQuery"		fester Wert
AuditEvent.entity.detail	type	value[x]	
	"QueryId"	<Parameter Query ID>	Der Wert MUSS der Parameter Query ID gemäß [IHE-ITI-TF2]#3.18.4.1.2.4 und für das Aktensystem definierten Anfragetypen entsprechen.
Parameterwerte für die Operation RestrictedUpdateDocumentSet			
<p>Alle Metadaten, die geändert wurden, sind mit altem und neuem Wert mit den Parameternamen AuditEvent.entity.detail.type und .value[x] zu protokollieren. In A_15083* sind die Metadaten genannt, die geändert werden können. Der Parameter type ist ein Kompositum aus Objekt (Document) + Attribut in Groß/Kleinschreibung. Wird das geänderte Metadatum adressiert, wird noch der Präfix "prev" ergänzt. z.B. Metadatum: DocumentEntry.formatCode -> Parameter valuetype: DocumentFormatCode und prevDocumentFormatCode. Attributunterstrukturen werden ebenfalls in gemischter Groß/Kleinschreibung zusammengesetzt (z.B. author.Person -> AuthorPerson).</p>			

[<=]

Hinweis: In der AuditEvent.entity Struktur sind Dokumente und/oder Folder zu berücksichtigen, die in der zu protokollierenden Operation referenziert werden.

A_24925 - XDS Document Service - Protokolleinträge für Zugriffe gleicher Art

Werden mehrere XDS Dokumente bzw Folder in der zu protokollierenden Operation referenziert und die Zugriffe sind gleicher Art (AuditEvent.action) KANN der XDS Document Service einen Protokolleintrag erzeugen, der mehreren AuditEvent.entity Strukturen enthält. [<=]

Das bedeutet, wenn in einer ProvideAndRegisterDocumentSet-b Operation zehn Dokumente eingestellt werden, kann für diesen Zugriff ein AuditEvent mit zehn Entity Strukturen erzeugt werden. Werden zehn Dokumente eingestellt und das zehnte Dokument ersetzt ein bereits vorhandenes, kann in einem Protokolleintrag das Einstellen (Create) mit neun Entity Strukturen dokumentiert und muss in einem weiteren Protokolleintrag ein Ersetzen (Update) (zehnte Dokument) protokolliert werden.

A_25007 - XDS Document Service - Nicht zu protokollierende Zugriffe

Werden mit der Operation RestrictedUpdateDocumentSet keine geänderten Metadaten eines referenzierten DocumentEntry gesendet, d.h. die gesendeten Metadateninhalte unterscheiden sich nicht von bereits persistierten Werten, DARF der XDS Document Service diesen Zugriff NICHT protokollieren. [<=]

A_27253 - XDS Document Service - Nicht zu protokollierende Zugriffe auf Ordner "technical"

Der XDS Document Service DARF Zugriffe auf den statischen Ordner "technical" oder dessen Inhalte NICHT protokollieren. Ausgenommen hiervon sind Zugriffe auf Dokumente mit Daten der Protokollierung gemäß A_24866-* (Protokolle aus der Migration eines ePA-2.6 Aktenkontos) [<=]

A_27254 - XDS Document Service - Protokollierung von Nutzerzugriffen auf den Ordner "technical"

Der XDS Document Service MUSS Nutzerzugriffe auf den Ordner "technical" dann protokollieren, wenn durch den Zugriff Dokumente gemäß A_24466-* (Protokolldokumente einer ePA-2.6 Aktenkontomigration) betroffen sind. Diese Protokollierung MUSS gemäß der Vorgaben in A_24715-* erfolgen. [\leq]

3.13.1.14 Unterstützungsleistung für das ePA-FdV

Der XDS Document Service akzeptiert aus Sicherheitsgründen nur bestimmte Dokumentenformate. Das schränkt auch das Format PDF auf bestimmte PDF/A-Varianten ein (siehe auch A_25233*). Daher müssen PDF-Dokumente des Versicherten unter Umständen vor dem Einstellen in die ePA konvertiert werden.

Um das ePA-FdV dabei zu entlasten und Komplexität aus dem ePA-FdV zu nehmen, wird eine Funktion angeboten, durch die ein PDF in ein PDF/A konvertiert werden kann. Das ePA-FdV muss aber berücksichtigen, dass die Konvertierung ggf. technisch nicht durchgeführt werden kann oder das Ergebnis der Konvertierung durch ein geändertes Layout ggf. nicht verwendbar ist.

A_25456 - XDS Document Service - Keine negativen Auswirkungen auf Folgekonvertierungen von PDF zu PDF/A

Der XDS Document Service MUSS sicherstellen, dass eine Konvertierung eines PDF-Dokuments sich nicht schädlich auf folgende Konvertierungen auswirken kann. [\leq]

Hinweis zu A_25456*: Die Anforderung soll erreichen, dass ein potentiell über ein PDF-Dokument eingebrachter Schadcode nach der Konvertierung gelöscht wird, z.B. durch Zurücksetzen der Sandbox oder der VAU-Instanz

A_25455 - XDS Document Service - Isolation der Konvertierung von PDF zu PDF/A

Der XDS Document Service MUSS die Verarbeitung von PDF-Dokumenten, die im Rahmen der Konvertierung in ein PDF/A durchgeführt wird, in einer separaten VAU-Instanz durchführen, die ausschließlich eine Verbindung zu einem ePA-FdV besitzen darf. [\leq]

A_25454 - XDS Document Service - Realisierung der Schnittstelle I_Tool_Convert_PDF_Insurant

Der XDS Document Service MUSS die Operationen der Schnittstelle I_Tool_Convert_PDF_Insurant gemäß [I_Tool_Convert_PDF_Insurant] umsetzen [\leq]

A_26129 - ePA-Aktensystem - Rahmenbedingungen bei Nutzung einer Service-VAU für PDF-Konvertierung

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die vom ePA-FdV übermittelten PDF-Dokumente in der Aktenkontoverwaltungs-VAU ausschließlich weitergeleitet aber ansonsten nicht verarbeitet werden. Gleiches gilt für die von der Service-VAU an das ePA-FdV übermittelten konvertierten PDF/A-Dokumente. [\leq]

A_26130 - ePA-Aktensystem - maximale Lebensdauer einer Service-VAU für PDF-Konvertierung

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass die Lebensdauer einer solchen Service-VAU-Instanz maximal 12 Stunden beträgt. [\leq]

A_26131 - ePA-Aktensystem - Keine Speicherung von in der Service-VAU für PDF-Konvertierung verarbeiteten Daten

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass weder die vom ePA-FdV übermittelten und zu konvertierenden PDF-Dokumente noch die daraus konvertierten PDF/A-Dokumente von der "PDF-VAU" im ePA-Aktensystem gespeichert werden. [≤]

A_26121 - ePA-Aktensystem - Keine Verarbeitung von Geräteinformationen

Falls das ePA-Aktensystem zur Umsetzung der Unterstützungsleistung für das ePA-FdV für die Konvertierung von PDF-Dokumenten in PDF/A-Dokumente eine Service-VAU verwendet ("PDF-VAU"), MUSS das ePA-Aktensystem sicherstellen, dass keine Geräteinformationen (Device Management) von Nutzern verarbeitet werden. [≤]

3.13.2 FHIR Data Services

3.13.2.1 Patient Information Service

A_26252-01 - Patient Information Service - Realisierung der Schnittstelle des FHIR IG Patient Information Service

Der Patient Information Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide für den Patient Information Service [IG_Patient_Information_Service] umsetzen. [≤]

A_26254 - Patient Information Service - Protokolleinträge für Zugriffe auf den Patient Information Service

Der Patient Information Service MUSS einen Protokolleintrag gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 36: Patient Information Service Protokollierung

Strukturelement	Wert	Erläuterung
AuditEvent.type	"rest"	
AuditEvent.action	U	Update
AuditEvent.entity.name	Patient	
AuditEvent.entity.description	operation:upsertPatient	

[≤]

3.13.2.2 Medication Service

A_26253-01 - Medication Service - Realisierung der Schnittstellen des FHIR IG Medication Service

Der Medication Service MUSS die Implementierungsvorgaben des FHIR Implementation Guide für den Medication Service [IG_Medication_Service] umsetzen. [≤]

A_26317 - Medication Service - Erzeugung eines xHTML-Exports

Der Medication Service MUSS gemäß den Vorgaben von [IG_Medication_Service] für die Generierung der Medikationsliste im xHTML-Format nach [XHTML] sicherstellen, dass kein ausführbarer Code im Export enthalten ist. [≤]

A_24820 - Medication Service - Ablehnung von Request bei vorliegendem Widerspruch

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID != oid_erp-vau, oid_versicherter mit dem HTTP Status Code 423 (LOCKED) abrechnen, sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("medication") die Entscheidung ("deny") gesetzt ist. [≤]

A_25152 - Medication Service - Ablehnung neuer Daten bei vorliegendem Widerspruch

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID == oid_erp-vau mit dem HTTP Status Code 423 (LOCKED) abrechnen, sofern im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny") gesetzt ist. [≤]

A_25153 - Medication Service - Löschen der Daten des Medication Service

Der Medication Service MUSS alle vorhandenen fachlichen Daten des Medication Service löschen, wenn im Consent Decision Management in der Funktionsklasse ("healthcareProcess") mit der Funktion ("erp-submission") die Entscheidung ("deny") gesetzt wird. [≤]

A_26399 - Medication Service - Ablehnung von Request bei vorliegendem Widerspruch

Der Medication Service MUSS jeden HTTP Request von Clients mit professionOID gemäß A_26406-* mit dem HTTP Status Code 423 (LOCKED) abrechnen, sofern im Consent Decision Management die LEI der User Session in der User Specific Deny Policy des Medication Service enthalten ist. [≤]

A_24841-02 - Medication Service - Schemavalidierung

Der Medication Service MUSS die im Body der HTTP-POST-Operation übertragenen Parameter gegen das jeweilige Schema der Operationsdefinition aus

- <https://gematik.de/fhir/epa-medication/OperationDefinition/add-amts-allergies-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/add-amts-observation-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/add-medication-information-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/amts-observation-entered-in-error-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-dispensation-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-dispensation-erp-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/cancel-prescription-erp-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-list-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-plan-OP>

- <https://gematik.de/fhir/epa-medication/OperationDefinition/get-medication-plan-history-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/link-prescription-process-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/manage-amts-allergies-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/manage-medicationstatement-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/manage-note-amts-observation-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/manage-medication-plan-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/medication-entered-in-error-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-dispensation-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-dispensation-erp-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-medication-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-medication-plan-note-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/provide-prescription-erp-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/remove-medication-plan-note-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/replace-medication-information-OP>
- <https://gematik.de/fhir/epa-medication/OperationDefinition/verify-medication-plan-OP>

prüfen und bei Nicht-Konformität das Ausführen der Operation mit dem HTTP Status Code 400 abbrechen, damit kein Schadcode und keine fachfremden Daten in den Medication Service hochgeladen werden. [<=]

A_24849-02 - Medication Service - Protokolleinträge für Zugriffe auf den Medication Service

Der Medication Service MUSS einen Protokolleintrag gemäß A_24704* erzeugen und dabei folgende Wertebelegung berücksichtigen:

Tabelle 37: Medication Service Protokollierung

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
type		"rest"	
action	OperationId: providePrescription_MedicationSvc	"C"	Einstellen von Verschreibungsdaten
	OperationId: provideDispensation_MedicationSvc	"C"	Einstellen einer Medikamentenabgabe
	OperationId: cancelPrescription_MedicationSvc	"U"	Stornieren von Verschreibungsdaten
	OperationId: cancelDispensation_MedicationSvc	"U"	Stornieren einer Medikamentenabgabe
	OperationId: addAMTSAllergyIntolerance_MedicationSvc	"C"	Einstellen von Allergie- oder Intoleranzinformationen im Rahmen von arzneimittelsicherheitsrelevanten Zusatzinformationen
	OperationId: addAMTSObservation_MedicationSvc	"C"	Einstellen von arzneimittelsicherheitsrelevanten Zusatzinformationen
	OperationId: createMedicationStatement_MedicationSvc	"C"	Einstellen von Medikamentenzusatzinformationen
	OperationId: enteredInErrorMedication_MedicationSvc	"U"	Markieren von Medikamentenzusatzinformationen als fehlerhaft

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
	OperationId: cancelDispensationPS_MedicationSvc	"U"	Stornieren einer Medikamentenabgabe
	OperationId: getMedicationList_MedicationSvc	"R"	Abruf der Medikationsliste
	OperationId: getMedicationPlan_MedicationSvc	"R"	Abruf des Medikationsplans
	OperationId: getMedicationPlanHistory_MedicationSvc	"R"	Medikationsplanshistorie
	OperationId: linkPrescriptionProcess_MedicationSvc	"U"	Verknüpfen von Verschreibungs- und Medikamentenabgabedaten
	OperationId: manageAllergyIntolerance_MedicationSvc	"U"	Aktualisieren von Allergie- und Intoleranzinformationen
	OperationId: updateMedicationStatement_MedicationSvc	"U"	Aktualisieren von Medikamentenzusatzinformationen
	OperationId: manageNoteAMTSObservation_MedicationSvc	"U"	Aktualisierung von Beobachtungsdaten im Rahmen von arzneimittelsicherheitsrelevanten Zusatzinformationen
	OperationId: manageMedicationPlan_MedicationSvc	"U"	Aktualisierung des Medikationsplans

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
	OperationId: enteredInErrorMedication_MedicationSvc	"U"	Kennzeichnen eines hinterlegten Medikaments als fehlerhaft eingestellt
	OperationId: provideDispensationPS_MedicationSvc	"C"	Einstellen von Medikamentenabgabe ohne Verschreibung
	OperationId: provideMedication_MedicationSvc	"C"	Einstellen eines Medikaments
	OperationId: provideMedicationPlanNote_MedicationSvc	"C"	Einstellen eines Medikationsplan-übergreifenden Hinweises
	OperationId: removeMedicationPlanNote_MedicationSvc	"D"	Löschen eines Medikationsplan-übergreifenden Hinweises
	OperationId: replaceMedicationInformation_MedicationSvc	"U"	Medikaments und ggf. dazugehöriger Medikamentenzusatzinformationen
	OperationId: verifyMedicationPlan_MedicationSvc	"U"	Verifizieren des aktuellen Medikationsplans
	OperationId: renderMedicationListToHTML_MedicationSvc	"R"	Abruf der Medikationsliste im HTML-Format
	OperationId: renderMedicationListToPDF_MedicationSvc	"R"	Abruf der Medikationsliste im PDF-Format
	OperationId: renderMedicationPlanToPDF_MedicationSvc	"R"	Abruf des Medikationsplans im PDF-Format

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
	OperationId: listAllergyIntolerances_MedicationSvc	"R"	Abruf von Allergie- und Intoleranzinformationen
	OperationId: listMedications_MedicationSvc	"R"	Abruf von Medikamenteninformationen
	OperationId: listMedicationDispenses_MedicationSvc	"R"	Abruf von Medikamentenabgabeformationen
	OperationId: listMedicationRequests_MedicationSvc	"R"	Abruf von Verschreibungsinformationen
	OperationId: listMedicationStatements_MedicationSvc	"R"	Abruf von Medikamentenzusatzinformationen
	OperationId: listObservations_MedicationSvc	"R"	Abruf von Beobachtungsdaten im Rahmen von arzneimittelsicherheitsrelevanten Zusatzinformationen
	OperationId: listOrganizations_MedicationSvc	"R"	Abruf von Organisationsinformationen
	OperationId: listPractitioners_MedicationSvc	"R"	Abruf von Leistungserbringerinformationen
	OperationId: getMedicationList_MedicationSvc	"R"	Abruf der Medikationsliste
	OperationId: listPractitionerRoles_MedicationSvc	"R"	Abruf von Leistungserbringerinformationen
	FHIR Query API:	"R"	Suche über die FHIR Query API

Strukturelement [AuditEvent.]	Operationen der Schnittstellen I_Medication_Service_FHIR und I_Medication_Service_eML_Render und FHIR Query API	Wert	Erläuterung
entity.name		<ul style="list-style-type: none"> "Medical Service" bei Operationen <FHIR Resource Name> bei FHIR Query API 	
Nur, wenn nicht FHIR Query API:			
entity.description		OperationId der ausgeführten Operation, z. B. "provideMedication_MedicationSvc"	
entity.detail.type		"display-text"	
entity.detail.value[x]		Text der oben für die jeweilige OperationId angegebenen Erklärungsspalte, z. B. "Einstellen eines Medikaments"	
Nur bei FHIR Query API:			
entity.detail.type		"search-parameters"	
entity.detail.value[x]		<ResourceName>?parameter1=<value>¶meter2=<value>&...mehr	Suchkriterien in URL-Query-Notation

Sofern ein lesender Zugriff ("Read-Operation") durch den Versicherten erfolgt, DARF der Medication Service keinen Protokolleintrag erzeugen.

[<=]

3.14 Audit Event Service

Ereignisse und Zugriffe auf die ePA eines Versicherten werden im ePA Aktensystem protokolliert. Die Protokollierung dient der Datenschutzkontrolle für den Versicherten.

Der Audit Event Service ist ein FHIR Data Service und ermöglicht dem Versicherten, befugten Vertretern bzw. der Ombudsstelle den Zugriff auf diese Protokollinformationen.

A_24704 - Audit Event Service - FHIR-Ressource AuditEvent

Der Audit Event Service MUSS die FHIR-Ressource AuditEvent gemäß der FHIR-Profilierung [IG_Audit_Event_Service] unterstützen. [≤]

In der Struktur eines Protokolleintrages (AuditEvents) sind folgende Zugriffsinformationen hinterlegt:

Tabelle 38 : Inhaltliche Definitionen eines AuditEvent

Information	Strukturelement
Wann ist der Zugriff erfolgt bzw. hat das Ereignis stattgefunden?	AuditEvent.recorded
Wer war der Akteur/Auslöser?	AuditEvent.agent
Welcher Art Service wurde angefragt?	AuditEvent.type
Worauf wurde zugegriffen?	AuditEvent.source
Welcher Art war der Zugriff?	AuditEvent.action
War der Zugriff erfolgreich?	AuditEvent.outcome
Informationen zu Daten/Dokumente/Objekte	AuditEvent.entity

Die spezifische Befüllung eines Audit Events gemäß A_24704* wird durch die jeweiligen Services vorgegeben. Allgemeine Elemente sind wie folgt zu befüllen:

A_25154-03 - ePA-Aktensystem - Befüllung der Elemente recorded, agent und source eines Audit Events

Das ePA-Aktensystem MUSS die Audit Event Elemente AuditEvent.recorded, AuditEvent.agent und AuditEvent.source wie folgt befüllen.

Tabelle 39 Befüllung AuditEvent

Element [AuditEvent.]		Beschreibung	Beispiel
recorded		Systemzeit bei Erstellung des AuditEvents im Format YYYY-MM-DDThh:mm:ssZ	"2025-01-15T14:52:04.928Z"
agent[client].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem; Fest vorgegebener Wert: "http://dicom.nema.org/resources/ontology/DCM"	"http://dicom.nema.org/resources/ontology/DCM"
	code	Der verwendete Code aus dem Codesystem; Fest vorgegebener Wert: "110150"	"110150"
	display	Der Bezeichner zur Anzeige aus dem Codesystem; Fest vorgegebener Wert: "Application"	"Application"
agent[client].who.identifizier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/sid/telematik-id"
	value	<Telematik-Id>	"1-883110000092404"
agent[client].	altId	<value> aus agent.who.identifizier	"1-883110000092404"

Element [AuditEvent.]		Beschreibung	Beispiel
agent[client].	name	<ul style="list-style-type: none"> <display_name> des auslösenden Akteurs aus dem ID-Token der UserSession "Elektronische Patientenakte Fachdienst" für intern ausgelöste AuditEvents 	1) "E-Rezept-Fachdienst" 2) "Elektronische Patientenakte Fachdienst" 3) "Portugal" (Beispiel EU-Zugriff)
agent[client].	requestor	Fest vorgegebener Wert "false"	"false"
agent[user].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	" http://terminology.hl7.org/CodeSystem/v3-RoleClass "
	code	Der verwendete Code aus dem Codesystem	"PROV"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"healthcare provider"
agent[user].who.identifier.		Identifikation des Auslösers des Audit Events gemäß der zulässigen Value Sets	
	system	Das verwendete Codesystem	"https://gematik.de/fhir/sid/telematik-id"
	value	<Telematik-Id> oder <KVNR>	1) "2-121212121212121" 2) "Z123456789"

Element [AuditEvent.]		Beschreibung	Beispiel
agent[user].	altId	<value> aus agent.who.identifizier	1) "2-121212121212121" 2) "Z123456789"
agent[user].role.coding		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthProfessionalRole.	
	system	Das verwendete Codesystem	"urn:oid:1.3.6.1.4.1.12559.11.10.1.3.2.2.2"
	code	Der verwendete Code aus dem Codesystem	"Resident Physician"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Resident Physician"
agent[user].extension		Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: healthcareFacilityType; extension mit url="https://gematik.de/fhir/dev-epa/StructureDefinition/epa-healthcare-facility-type-extension">	
	system	Das verwendete Codesystem	"urn:oid:2.16.840.1.113883.2.9.6.2.7"
	code	Der verwendete Code aus dem Codesystem	"221"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Medical Doctors"

Element [AuditEvent.]		Beschreibung	Beispiel
agent[user].	name	Gilt nur für oid = oid_ncpeh: Wert aus SOAP-header des Requests: <leiName> / <healthProfessionalName> Andernfalls: <display_name> des auslösenden Akteurs aus dem ID-Token der UserSession	EU-Zugriff: "Dr. Manuel Dos Santos / Clínica de Dos Santos" Andernfalls: "John Doe"
agent[user].	requestor	Fest vorgegebener Wert "false"	false
agent[internal].type.coding.		Information zum Auslöser des Audit Events gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	"http://dicom.nema.org/resources/ontology/DCM"
	code	Der verwendete Code aus dem Codesystem	"110150"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Application"
agent[internal].	altId	Fest vorgegebener Wert "ePA"	"ePA"
agent[internal]	name	Fest vorgegebener Wert "ePA"	"ePA"
agent[internal].	requestor	Fest vorgegebener Wert "false"	"false"
source		Informationen zum auslösenden Service des Aktensystems	

Element [AuditEvent.]		Beschreibung	Beispiel
source.observer.	display	Fester Wert "Elektronische Patientenakte Fachdienst"	"Elektronische Patientenakte Fachdienst"
source.type.		Der auslösende Service gemäß des zulässigen Value-Sets.	
	system	Das verwendete Codesystem	" https://gematik.de/fhir/epa/ValueSet/epa-auditevent-sourcetype-vs "
	code	Der verwendete Code aus dem Codesystem	"CDMGMT"
	display	Der Bezeichner zur Anzeige aus dem Codesystem	"Consent Decision Management"

Hinweis:

agent[client]: Angaben zur Applikation, z. B. eRezept-Fachdienst, NCPeH

agent[user]: Angaben zu LEI oder Vertreter oder Versicherter

agent[internal]: Angaben zu systemeigenen Prozessen, z. B. Datenexport für das FDZ

[<=]

A_24503 - ePA-Aktensystem - Aufbewahrungsdauer der Protokolleinträge

Das ePa-Aktensystem MUSS die zum Zwecke der Datenschutzkontrolle für den Versicherten erstellten

Protokolleinträge für drei Jahre aufbewahren. Danach sind sie vom Aktensystem automatisch zu löschen. [≤]

Die Protokolleinträge können durch den Versicherten oder durch einen befugten Vertreter mittels ePA-FdV eingesehen werden. Versicherte ohne ePA-FdV können bei ihrer zuständigen Ombudsstelle beantragen, die Protokolldaten zur Verfügung gestellt zu bekommen.

Für eine Abfrage der Protokolleinträge als strukturierte Einträge nutzen ein ePA-FdV und die Ombudsstelle den Audit Event Service [IG_Audit_Event_Service].

A_24714-01 - Audit Event Service - Realisierung der Query API: AuditEvent

Der Audit Event Service MUSS die "Query API: AuditEvent" des FHIR Implementation Guide für den Audit Event Service [IG_Audit_Event_Service] umsetzen. [≤]

A_24750-02 - Audit Event Service - Realisierung der Render API: PDF Audit

Der Audit Event Service MUSS die "Render API: PDF Audit" des FHIR Implementation Guide für den Audit Event Service [IG_Audit_Event_Service] umsetzen. [≤]

A_25172 - Audit Event Service - Speicherung der Protokolldaten

Der Audit Event Service MUSS die Daten der Protokolleinträge verschlüsselt im SecureDataStorage persistieren. [≤]

Hinweis: Die Notwendigkeit eines Protokolleintrag gemäß A_25172* entfällt, wenn ein Protokolleintrag mangels eines befugten Nutzers (kein Bezug des SecureDataStorageKeys möglich) nicht im SecureDataStorage abgelegt werden kann.

A_25018 - Audit Event Service - PAdES-Signatur in renderAuditEventsToPDF

Der Audit Event Service MUSS bei der Operation `renderAuditEventsToPDF` beim Signieren eines Protokolls im PDF/A-Format eine PAdES-Signatur gemäß [PAdES-3] und [PAdES Baseline Profile] erstellen. Bei der Signaturerstellung ist das Attribut `signing certificate reference` gemäß den Vorgaben aus [PAdES-3] Kapitel 4.4.3 „Signing Certificate Reference Attribute“ anzulegen. [≤]

Durch die Baseline-Profilierung [PAdES Baseline Profile] wird festgelegt, wie der Signaturzeitpunkt, gemessen als Systemzeit des ePA-Aktensystems, in die Signatur eingebracht wird.

A_24991 - Audit Event Service – Protokollierung von Zugriffen auf die Protokolldaten

Der Audit Event Service MUSS für die Zugriffe der Ombudsstelle oder eines Vertreters auf die protokollierten Daten jeweils einen Protokolleintrag gemäß A_24704* erzeugen.

Tabelle 40: Audit Event Service Protokollierung

Strukturelement	Wert	Erläuterung
AuditEvent.type	"rest"	
AuditEvent.action	R	Read

Strukturelement	Wert		Erläuterung
AuditEvent.entity.name	"AuditEvent"		
AuditEvent.entity.description	Passend zur ausgeführten Operation ein Wert aus folgender Liste: <ul style="list-style-type: none"> • listAuditEvents • getAuditEventById • renderAuditEventsToPDF 		
AuditEvent.entity.detail	type	value[x]	
	parameters	parameter1=<value>¶parameter2=<value>& ...mehr	Nur bei getAuditEventList
	identifizier	<id> des AuditEvents	Nur bei getAuditEvent

[<=]

Hinweis: Zugriffe des Versicherten auf die Protokolle des Aktenkontos werden nicht protokolliert.

3.15 Information Service

3.15.1 Information Service

Der Information Service ist ohne die Nutzung eines VAU-Kanals nutzbar. Die über den Information Service genutzten Daten sind ausschließlich persistierte Daten des Aktenkontos, die weder mit dem SecureAdminStorageKey noch mit dem SecureDataStorageKey gesichert sind.

Der Zugang erfolgt durch Nutzung der Schnittstelle `I_Information_Service`.

A_24344 - Information Service - Realisierung der Schnittstelle `I_Information_Service`

Der Information Service MUSS die Operationen der Schnittstelle `I_Information_Service` gemäß [`I_Information_Service`] umsetzen. [<=]

A_24345 - Information Service - Kein Zugriff auf verschlüsselte Daten des Aktenkontos

Der Information Service DARF NICHT auf Daten zugreifen, die nicht explizit für die Verwendung durch den Informationsdienst bereitgestellt wurden. Dazu gehören insbesondere alle Daten des Aktenkontos, die mit den versichertenindividuellen

Schlüsseln zur Daten- oder Befugnispersistierung (SecureDataStorageKey oder SecureAdminStorageKey) gesichert sind.[<=]

3.15.1.1 Informationen zu Widersprüchen (Consent Decisions)

Die Widersprüche eines Versicherten gegen die Nutzung von Funktionen der elektronischen Patientenakte werden durch das Consent Decision Management gesichert administriert. Änderungen an den Widersprüchen erfolgen dort.

Der Information Service bietet für die Nutzergruppen der ePA eine einfache Abfragemöglichkeit der aktuell erteilten oder nicht erteilten Widersprüche auch ohne die Nutzung des Consent Decision Managements an. Liegt ein Widerspruch gegen die Nutzung einer Funktion vor, kann auf die Ausführung der zur Nutzung dieser Funktion notwendigen Aktionen mit der ePA eines Versicherten durch den Client verzichtet werden.

Für diese vereinfachte Abfragemöglichkeit der aktuellen Widersprüche verwendet der Information Service den durch das Consent Decision Management persistent übertragenen Zustand der Widersprüche ("Cache" des Zustands der Widersprüche). Berücksichtigt wird dabei die Widerspruchsinformation, für die eine vereinfachte Abfrage vorgesehen ist (Widersprüche der Klasse "Versorgungsprozess").

3.15.1.2 Informationen zur Anwenderperformance (UX Performance)

Der Information Service stellt für die Umgebung der Leistungserbringer die Operation zur Sammlung der Messwerte zu den Anwendungsfällen der Nutzererfahrung zur Verfügung. Die Weiterverarbeitung der gesammelten Daten ist in 2.9- Performance aus Anwendersicht definiert und vorgegeben.

3.15.2 Information Service - Account

Die Operationen der Information Service - Account werden für den Umzug eines existierenden Aktenkontos zu einem neuen Anbieter verwendet. Die Nutzung der Operationen erfolgt exklusiv durch die Aktensystembetreiber.

Die Verwendung der einzelnen Operationen erfolgt im Verbund mit den Operationen der Schnittstelle I_Health_Record_Relocation_Service für die Umsetzung der Anwendungsfälle eines automatischen Aktenkontoumzugs und sind in 3.2- Health_Record_Relocation_Service erläutert.

A_24424 - Information Service Account - Realisierung der Schnittstelle I_Information_Service_Accounts

Der Information Service MUSS die Operationen der Schnittstelle I_Information_Service_Accounts gemäß [I_Information_Service_Accounts] umsetzen.[<=]

A_24665 - Information Service Account - Nutzung beidseitig authentisiertes TLS

Der Information Service MUSS sicherstellen, dass die Operationen der Schnittstelle I_Information_Service_Accounts ausschließlich unter Verwendung einer beidseitig authentisierten TLS-Verbindung zwischen den beteiligten Aktensystemen genutzt werden und die Operationen ansonsten abgebrochen und mit einer Fehlermeldung gemäß Vorgaben in [I_Information_Service_Accounts] beantwortet werden.[<=]

A_25054 - Information Service Account - Gegenseitige Authentisierung Aktensysteme

Die Information Service Account Dienste der Aktensysteme MÜSSEN sich mit der TLS-Identität mit professionOID `oid_epa_mgmt` mittels des Zertifikats C.FD-TLS-S gegenseitig

authentisieren.

[<=]

A_25053 - Information Service Account - Prüfung der TLS-Zertifikate

Der Information Service Account MUSS bei der Authentifizierung eines jeweils anderen Aktensystems die Prüfung der verwendeten TLS-Zertifikate entsprechend TUC_PKI_018 durchführen. Zur Prüfung des TLS-Zertifikats C.FD-TLS-S sind dabei die Parameter PolicyList=oid_fd_tls_s, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-serverAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden. Zur Prüfung des TLS-Zertifikats C.FD-TLS-C sind dabei die Parameter PolicyList=oid_fd_tls_c, IntendedKeyUsage=digitalSignature, intendedExtendedKeyUsage=id-kp-clientAuth, OCSP-Graceperiod=60 Minuten, Offline-Modus=nein zu verwenden.

[<=]

3.16 Email Management

Das Email Management ermöglicht einem FdV-Nutzer die Verwaltung seiner E-Mail-Adresse und einem Kostenträger die Verwaltung von E-Mail-Adressen von Versicherten, die bei diesem Kostenträger versichert sind.

Die Schnittstelle zum Verwalten der E-Mail-Adressen durch den Kostenträger dient dem ausschließlichen Zweck des Einstellens, Lesens und der Änderung von E-Mail-Adressen auf Verlangen des Versicherten. Dies ermöglicht dem Kostenträger, seinen Versicherten die Wahrnehmung der datenschutzrechtlichen Betroffenenrechte auf Berichtigung und Auskunft bzgl. der im Aktensystem verarbeiteten E-Mail-Adresse zu gewährleisten.

Für einen Versicherten kann nur genau eine E-Mail Adresse hinterlegt werden.

A_25435 - Email Management - Realisierung der Schnittstelle

I_Email_Management

Das Email Management MUSS die Operationen der Schnittstelle

I_Email_Management gemäß [I_Email_Management] umsetzen.[<=]

A_25438 - Email Management - Beschränkung der Schnittstellenoperationen auf E-Mail-Adressen des FdV-Nutzers

Das Email Management MUSS die Operationen der Schnittstelle

I_Email_Management gemäß [I_Email_Management] auf die E-Mail-Adresse des aufrufenden Nutzers einschränken, sofern der Nutzer ein FdV-Nutzer ist.[<=]

A_26161 - Email Management - Nutzen von Email Management auch bei Widerspruch

Das Email Management MUSS sicherstellen, dass das Email Management auch von Versicherten genutzt werden kann, die einem Aktenkonto widersprochen haben.[<=]

A_26162 - Email Management - Versicherte nutzen Email Management ausschließlich im Home-AS

Das Email Management des ePA-Aktensystems MUSS sicherstellen, dass das Email Management ausschließlich von Versicherten genutzt werden kann, für die das ePA-Aktensystem das Home-AS ist.[<=]

Hinweis: Für das Email Management ist auch Anforderung A_26154 umzusetzen.

A_25439 - Email Management - Kostenträger kann ausschließlich E-Mail-Adressen der eigenen Versicherten verwalten

Das Email Management MUSS sicherstellen, dass ein Kostenträger mittels der Operationen der Schnittstelle I_Email_Management gemäß [I_Email_Management]

ausschließlich E-Mail-Adressen von Versicherten verwalten kann, die beim Kostenträger versichert sind. [<=]

A_25440-01 - Email Management - Benachrichtigung bei Änderung der E-Mail-Adresse

Falls eine E-Mail-Adresse a) ersetzt oder b) ergänzt wird, MUSS das Device Management bei a) eine E-Mail an die alte und die neue E-Mail-Adresse senden und bei b) eine E-Mail an die neue E-Mail-Adresse senden, in der bei a) über die Ersetzung bzw. bei b) die Ergänzung einer E-Mail-Adresse informiert wird. In der E-Mail MUSS darüber informiert werden, wann und ob der FdV-Nutzer selbst oder der Kostenträger die E-Mail ersetzt bzw. ergänzt hat. [<=]

A_25441 - Email Management - Information bzgl. der Ergänzung bei E-Mail-Adressen

Das Email Management MUSS sicherstellen, dass der FdV-Nutzer für eine im Email Management hinterlegte E-Mail-Adresse erkennen kann, wann und von wem diese E-Mail-Adresse ergänzt wurde. [<=]

A_25968-01 - Email Management - Maximale Anzahl E-Mail-Adressen

Das Email Management MUSS sicherstellen, dass für einen Nutzer maximal eine E-Mail-Adresse hinterlegt werden kann. [<=]

A_26163 - Email Management - Keine Persistierung einer im Rahmen der Vertretereinrichtung übergebenen E-Mail-Adresse

Das Email Management MUSS sicherstellen, dass eine im Rahmen des Anwendungsfalls der Vertretereinrichtung vom Nutzer übermittelte E-Mail-Adresse nicht persistiert und spätestens bei Beendigung der User Session gelöscht wird. [<=]

A_26164 - Email Management - Keine Geräteregistrierung mit der im Rahmen der Vertretereinrichtung übergebenen E-Mail-Adresse

Das Email Management MUSS sicherstellen, dass keine E-Mail-Adressen zur Übermittlung eines Geräteregistrierungscodes genutzt werden, die dem ePA-Aktensystem im Rahmen des Anwendungsfalls der Vertretereinrichtung übermittelt wurden. [<=]

Hinweis zu A_26163 und A_26164: Die im Rahmen des Anwendungsfalls der Vertretereinrichtung übermittelte E-Mail-Adresse wird ausschließlich zur Information des Vertreters über die Einrichtung der Vertretung genutzt (vgl. A_24755-*).

3.17 Zusätzliche Anforderungen an den Authorization Service

Der ePA Authorization Service wird sowohl für die Authentisierung der Versicherten über das FdV als auch für die Authentisierung von Leistungserbringern und Kostenträgern über deren Primärsystem benötigt. Ebenso muss die Zugriffsautorisierung für andere Fachdienste wie z.B. E-Rezept geprüft werden. Die Festlegungen für den Authorization Server finden sich in [gemSpec_IDP_FD]. Dieser Abschnitt des vorliegenden Dokuments enthält spezifische Anforderungen, die vom Authorization Service des Aktensystems zusätzlich umzusetzen sind.

A_24923 - Authorization Service - I_Authorization_Service

Der Authorization Service MUSS die Operationen der Schnittstelle `I_Authorization_Service` implementieren gemäß [I_Authorization_Service]. [<=]

A_25283 - Authorization Service - Konvertieren von ID-Token

Der Authorization Service MUSS sicherstellen, dass für ein nach erfolgreicher Authentifizierung des Nutzers vorliegendes ID-Token mittels Regel `rr0` gemäß

Tab_AS_Entitlement_Registration_Rules ein HSM-ID-Token erstellt wird, bevor das ID-Token zeitlich ungültig ist. [≤]

3.17.1 Anforderungen an den Authorization Service für die Authentisierung von Versicherten (FdV)

Im Rahmen der Authentisierung des Versicherten erfolgt die Prüfung der Geräteregistrierung (Verifikation) direkt. Das Gerät muss dafür die Geräteparameter eines zuvor ausgeführten und bestätigten Registrierungsprozesses verwenden

Bisher nicht registrierte Geräte, bzw. Geräteparameter einer bisher nicht bestätigten Geräteregistrierung, können unter Verwendung des Device Management registriert, bzw. bestätigt werden (siehe Kapitel 3.12- Device Management).

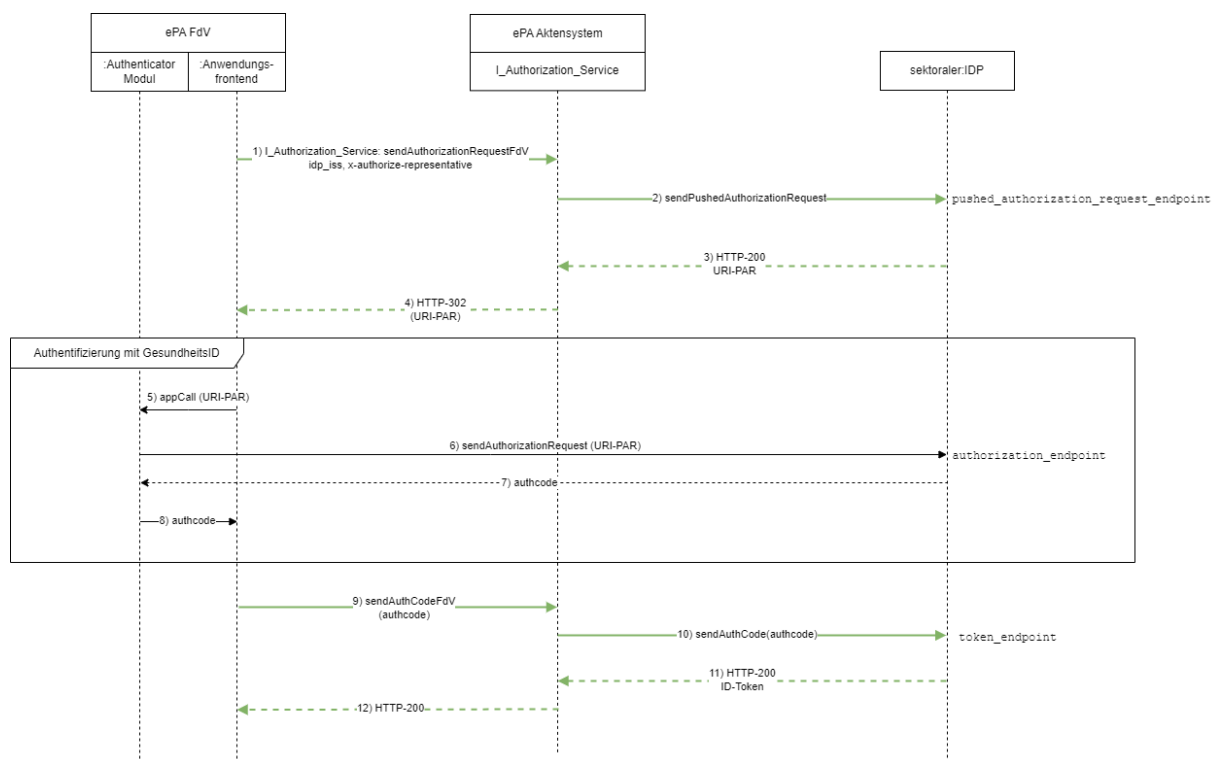


Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP

A_25717-03 - Authorization Service - Pushed Authorization-Request des Authorization Service an sektorale Identity Provider

Der ePA Authorization Service MUSS den Pushed Authorization Request (PAR) an durch den vom ePA-FdV übergebenen Parameter `idp-iss` adressierten sektoralen IDP gemäß [gemSpec_IDP_FD#AF_10117] mit folgenden Parametern aufrufen:

Parameter	Wert	Anmerkung
scope	"openid urn:telematik:display_name urn:telematik:versicherter urn:telematik:family_name urn:telematik:given_name"	Notwendige Scopes für den Zugriff für die Autorisierung von Nutzern am ePA-Aktensystem

Parameter	Wert	Anmerkung
acr_values	"gematik-ehealth-loa-high"	Angefordertes Niveau der Nutzerauthentisierung
redirect_uri	Inhalt des Parameters x-redirecturi [sendAuthorizationRequestFdV in I_Authorization_Service], andernfalls eine herstellerspezifische Standard-redirect_uri.	Diese URI muss unter dem claim redirect_uris im Entity Statement des Authorization Service enthalten sein. Mandanten, welche eine eigene redirect_uri verwenden [sendAuthorizationRequestFdV in I_Authorization_Service] , müssen diese im Rahmen des Registrierungsprozesses beim Authorization Service bekannt geben.

[<=]

Hinweis 1: An die redirect_uri im Pushed Authorization Request sendet der sektorale IDP den ausgestellten Authorization Code (siehe [gemSpec_IDP_Sek])

Hinweis 2: Der Redirectaufruf, der vom Authenticator Modul an die redirect_uri ausgeführt wird, wird vom ePA-FdV über Plattformmechanismen (deeplink/universallink) gefangen und stellt selbst einen POST-Request an den Endpunkt des Authorization Service.

A_26584 - Authorization Service - Liste der redirect_uris im Entity Statement

Der Authorization Service MUSS in seinem Entity Statement im claim redirect_uris die redirect_uris aller Mandanten auflisten, welche bei der Registrierung an einem beliebigen ePA Authorization Service eine eigene redirect_uri angegeben haben. Über Änderungen des claim redirect_uris MUSS der Anbieter des Federation Master vor produktiver Verwendung informiert werden[<=]

Hinweis: Im Registrierungsprozess eines Mandanten mit eigener redirect_uri muss sichergestellt sein,

- dass alle Anbieter von ePA Authorization Servern (ePA Aktensystem Anbieter) entsprechend informiert sind und das Entity Statement anpassen
- dem Hersteller des Federation Master über ein ITSM Change bekannt gemacht wird, dass sich die Entity Statements aller ePA Authorization Server ändern

A_27145 - Synchronisation "redirect_URI" mit Marktteilnehmer - E-Mail-Adresse

Der Anbieter ePA-Aktensystem MUSS der gematik eine E-Mail-Adresse mitteilen, über welche er die eigenverantwortliche Registrierung (von redirect-URIs im Entity-Statement) durchführt und über die der Anbieter bei Änderungen erreichbar ist.

Hinweis: Diese E-Mail-Adressen werden durch das Provider Management der gematik anschließend unter den relevanten Anbietern verteilt bzw. können dort erfragt werden. Die Änderung der E-Mail-Adressen ist ebenfalls zu kommunizieren.

Hintergrund: Für Stellvertretung via ePA-FdV ist eine Synchronisierung der redirect_URIs notwendig. [≤]

A_27186 - Synchronisation "redirect_URI" mit Marktteilnehmer - Information

Der Anbieter ePA-Aktensystem MUSS bei Änderungen der redirect_URIs im eigenen Entity Statement allen anderen Marktteilnehmern des gleichen Fachdiensttyps diese Änderung innerhalb 24 Stunden mitteilen. [≤]

A_27187 - Synchronisation "redirect_URI" mit Marktteilnehmer - Aktualisierung

Der Anbieter ePA-Aktensystem MUSS nach dem Empfang der Mitteilungen über Änderungen der Redirect URIs in einem externen Entity Statement diese Änderung binnen 24 Stunden in den Redirect URIs des eigenen Entity Statement synchronisieren.

Hinweis: Diese Änderung erfordert anschließend keine Information nach A_27186. [≤]

A_24878-01 - Authorization Service - Authentifizierung eines Versicherten am ePA-FdV des Vertreters

Falls der Eingangsparameter `x-authorize-representative=True` der Operation `I_Authorization_Service::sendAuthorizationRequestFdV` gesetzt ist, MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:guest:eGK` belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [≤]

A_26189-01 - Authorization Service - Authentifizierung eines Versicherten im Gastmodus mit eGK und PIN

Falls der Eingangsparameter `x-authorize-egk=True` der Operation `I_Authorization_Service::sendAuthorizationRequestFdV` gesetzt ist, MUSS der Authorization Service im PAR als Parameter `amr` mit den Werten `urn:telematik:auth:guest:eGK` belegt sein, um sicherzustellen, dass sich der Nutzer nur über eGK+PIN authentisieren darf. [≤]

A_24937-01 - Authorization Service - Einschränkung bei Authentifizierung eines Versicherten am ePA-FdV des Vertreters

Der Authorization Service MUSS sicherstellen, dass ein mit `x-authorize-representative=True` authentisierter Nutzer ausschließlich Zugriff auf das Entitlement Management erhält. [≤]

A_26159 - Authorization Service - Prüfen der Device Attestation

Der Authorization Service MUSS sicherstellen, dass von einem anderen ePA-Aktensystem signierte Device Attestations ausschließlich akzeptiert werden, wenn

- die Device Attestation gemäß A_25042-* valide von einer Signaturidentität der VAU eines anderen ePA-Aktensystems signiert wurde,
- die KVNR in der Device Attestation mit der KVNR im ID-Token des angemeldeten Nutzers übereinstimmt,
- die Device Attestation zeitlich gültig ist.

[≤]

A_26160 - Authorization Service - Keine Persistierung der Device Attestation

Der Authorization Service MUSS sicherstellen, dass die von einem anderen ePA-Aktensystem signierte Device Attestation und deren Inhalte spätestens bei Beendigung der User Session gelöscht und nicht persistiert werden. [≤]

A_25310-01 - Authorization Service - Einschränkung bei Authentifizierung mit einem unregistrierten Gerät

Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wird und der Nutzer nicht mit `x-authorize-representative=True` authentisiert wurde, MUSS der Authorization Service sicherstellen, dass der Nutzer ausschließlich Zugriff auf das Device Management erhält. [≤]

Hinweis:

Ein vollständiger Zugriff eines authentisierten Nutzers auf alle Dienste des Aktensystems kann nur mit einem Gerät erfolgen, dessen Geräteregistrierung bei der Authentifizierung des Nutzers erfolgreich verifiziert wurde.

Ein Nachweis einer Geräteregistrierung ist entweder DeviceID (deviceIdentifier und deviceToken), die für den Nutzer im Aktensystem bekannt sind oder die vom Client übergebene Device Attestation (deviceAttestation), die zuvor am Device Management des Home Aktensystems durch den Client abgerufen wurde.

A_24804-01 - Authorization Service - Prüfung auf registriertes Gerät

Falls es sich nicht um eine Authentifizierung eines Versicherten am ePA-FdV des Vertreters handelt und im Operationsaufruf

`I_Authorization_Service::sendAuthCodeFdV` eine DeviceID (deviceIdentifier und deviceToken) übermittelt wird, MUSS der Authorization Service bei der Authentifizierung eines Versicherten prüfen, ob die übergebene DeviceID auf den authentifizierten Nutzer registriert und bestätigt ist und übereinstimmt. [≤]

A_24914-03 - Authorization Service - Prüfung auf registriertes Gerät - kein registriertes Gerät

Falls kein gültiger Nachweis einer Geräteregistrierung übergeben wurde, MUSS der Authorization Service die Operation `sendAuthCodeFdV` mit einer Fehlermeldung abbrechen und die User Session beenden. [≤]

A_24915-01 - Authorization Service - Prüfung auf registriertes Gerät - registriertes Gerät nicht bestätigt

Falls als Nachweis einer Geräteregistrierung eine DeviceID (deviceIdentifier und deviceToken) einer unbestätigten Geräteregistrierung übergeben wurde (status == 'pending'), MUSS der Authorization Service die Operation `sendAuthCodeFdV` mit einer Fehlermeldung abbrechen und die User Session beenden. [≤]

3.17.2 Anforderungen an den Authorization Service für Authentisierung mit SMC-B

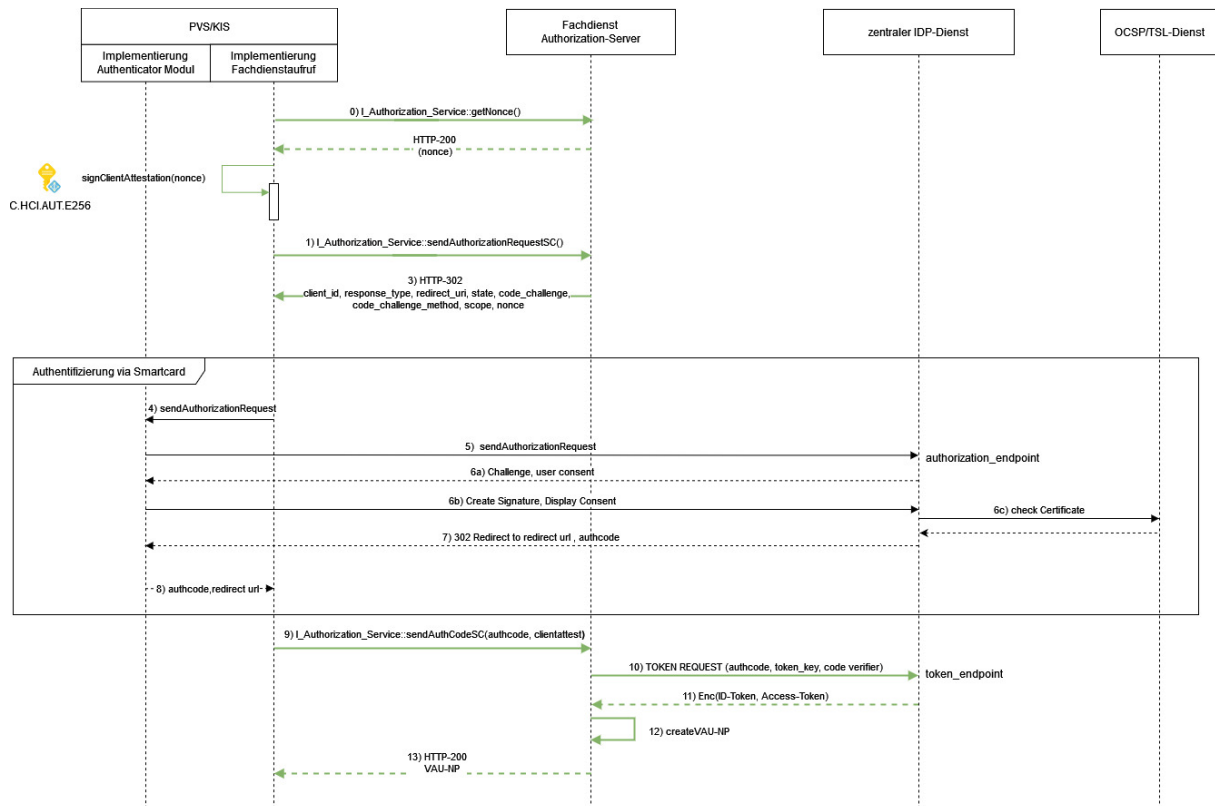


Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP

A_24717 - Authorization Service: IDToken vom IDP-Dienst nur mit Client-Attestation nutzbar

Der Authorization Service MUSS sicherstellen, dass ein vom IDP-Dienst abgerufenen ID-Token für Nutzer "TelematikID_X" nur dann akzeptiert wird, falls im Authorization Service auch eine Client-Attestation vom Nutzer "TelematikID_X" vorliegt. [<=]

A_24718 - Authorization Service: Client-Attestation nur einmal nutzbar (Replay Angriffe)

Der Authorization Service MUSS sicherstellen, dass eine Client-Attestation eines Nutzers im Authorization Service mit dem ID-Token nur einmalig für die Aktivierung einer User Session verwendet wird. [<=]

A_25444-01 - Authorization Service - JWT Client Attestation

Der Authorization Service MUSS bei der Authentifizierung einer Leistungserbringerinstitution prüfen, dass das übermittelte JWT der Client Attestierung

mindestens die folgenden Inhalte aufweist.

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256" oder "PS256"	
	"x5c"	Signaturzertifikat C.HCI.AUT	
Payload			
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"
	"exp"	Verfalldatum, = "iat" + 20 min	Beispiel: "1705675744"
	"nonce"	Nonce aus einer <code>getNonce</code> Operation	siehe [I_Authorization_Service]

[<=]

Für das Signaturzertifikat zu "x5c" (AUT-Zertifikat der SMC-B) gilt: Basiert der öffentlichen Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

3.17.3 Anforderungen an den Authorization Service für die Authentisierung des E-Rezept-Fachdienstes

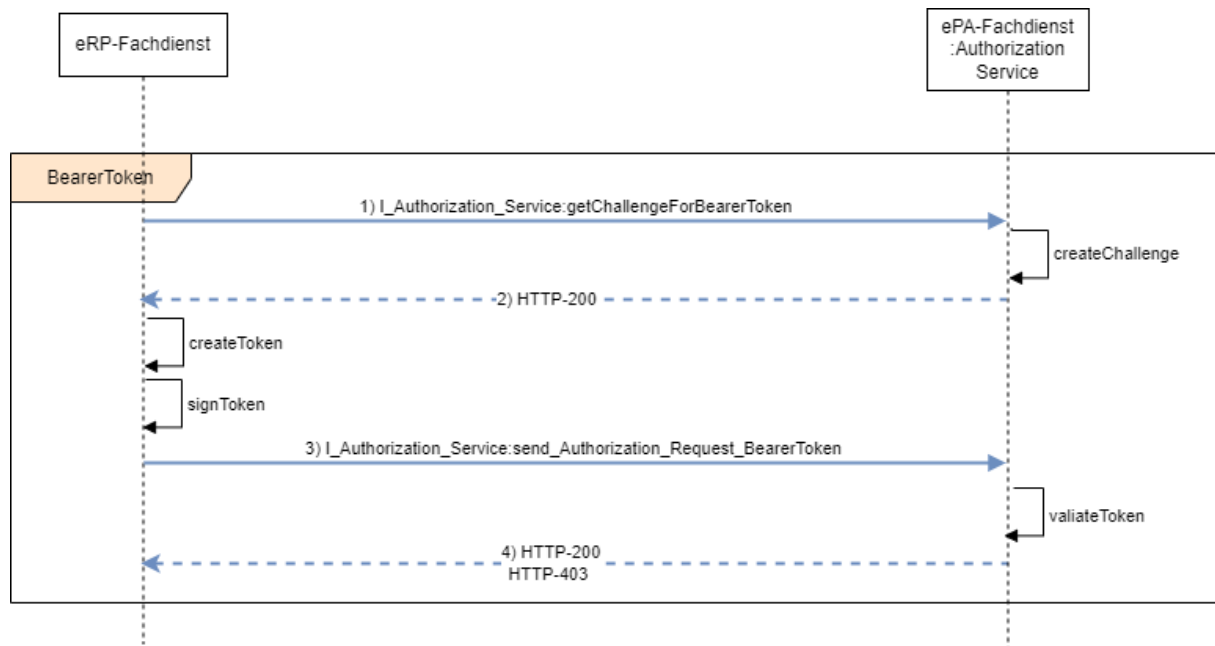


Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes

A_25165-03 - Authorization Service: JWT Bearer-Token des E-Rezept-Fachdienstes

Das Authorization Service MUSS sicherstellen, dass die Authentifizierung des E-Rezept-Fachdienstes über die Schnittstelle `I_Authorization_Service` durch Verwendung eines gültig signierten JWT Bearer Token mit den dargestellten Mindest-Inhalten und Prüfung durch Regel 'rr0' des Befugnisverifikations-Moduls erfolgt. Die Claims in 'Payload' MÜSSEN dazu die Vorgaben aus [gemSpec_Krypt], A_24658* befolgen.

Part	Claim Name	Claim	Anmerkung
Protected Header			
	"typ"	"JWT"	
	"alg"	"ES256"	
	"x5c"	Signaturzertifikat C.FD.AUT	
Payload			
	"type"	"ePA-Authentisierung über PKI"	fester Wert
	"iat"	Zeitstempel Ausgabezeitpunkt	Beispiel: "1705674544"

Part	Claim Name	Claim	Anmerkung
	"challenge"	Frischeparameter (freshness parameter)	siehe [gemSpec_Krypt]
	"sub"	Telematik-ID des E-Rezept-Fachdienstes	

[<=]

Das Signaturzertifikat zu "x5c" (AUT-Zertifikat der E-Rezept-VAU) kommt aus der Komponenten-PKI der TI. Basiert der öffentliche Schlüssel auf der ECC-Kurve brainpoolP256r, so gilt der Wert "ES256" (Parameters "alg") ebenfalls für diese Kurve und nicht nur für die ECC-Kurve P-256. Die Signatur und Kodierung des JWT ist gemäß [RFC7515] zu erstellen.

3.18 Anbindung Verzeichnisdienst FHIR-Directory

A_25176 - ePA-Aktensystem - Anbindung Verzeichnisdienst FHIR-Directory

Das ePA-Aktensystem MUSS bei der Suche des Versicherten nach Einträgen im Verzeichnisdienst FHIR-Directory und bei der initialen Anlage einer Akte den Anwendungsfall "AF_10219* - Versicherter sucht Einträge im FHIR-Directory" gemäß [gemSpec_VZD_FHIR_Directory] als Fachdienst unterstützen und dabei für die Client-Anfrage von search-access_token die Operation getFHIRVZDtoken gemäß [I_Authorization_Service.yaml] bereitstellen. [<=]

3.19 Access Gateway

Das Access Gateway ermöglicht den Versicherten bzw. deren berechtigten Vertretern den Zugang zum zugehörigen Aktensystem über das Internet. Auf der einen Seite dient es der Abschottung des ePA-Aktensystems in Richtung Internet, auf der anderen Seite regelt es den kontrollierten Zugriff der Versicherten auf das Aktensystem mit seinen funktionalen Komponenten.

3.19.1 Paketfilter

3.19.1.1 Funktion

Der Paketfilter stellt die Anbindung des ePA-Aktensystems an das Internet her und gewährleistet die Abschottung des ePA-Aktensystems in Richtung Internet.

A_14017 - Access Gateway, Sicherung zum Transportnetz Internet durch Paketfilter

Das ePA-Aktensystem MUSS zum Transportnetz Internet durch einen Paketfilter (ACL) gesichert werden, welcher ausschließlich die erforderlichen Protokolle weiterleitet. Der Paketfilter der Komponente Access Gateway MUSS frei konfigurierbar sein auf der Grundlage von Informationen aus OSI-Layer 3 und 4, das heißt Quell- und Zieladresse, IP-Protokoll sowie Quell- und Zielport. [<=]

A_14018 - Access Gateway, Platzierung des Paketfilters Internet

Der Paketfilter der Komponente Access Gateway, zum Schutz in Richtung Transportnetz Internet, DARF NICHT auf den anderen, zum Access Gateway gehörenden, physischen Komponenten implementiert werden. [\leq]

A_14019-02 - Access Gateway, Richtlinien für den Paketfilter zum Internet

Der Paketfilter der Komponente Access Gateway MUSS die Weiterleitung von IP-Paketen an der Schnittstelle zum Internet auf die nachfolgenden Protokolle beschränken:

1. HTTPS, und
2. OSCP-Zugriffe für das OSCP-Stapling (vgl. Hinweis nach A_14019-02), ggf. notwendige DNS Anfragen (und Antworten).

Ein Verbindungsaufbau aus dem ePA-Aktensystem über das Access Gateway in Richtung Internet MUSS unterbunden werden, mit Ausnahme der Verbindungen aus Punkt 2 . [\leq]

Hinweis zu A_14019-02: Der Aktensystem-Anbieter muss für seine HTTPS-Schnittstelle ein TLS-Zertifikat von einem durch das CAB-Forum zulässigen TSP erwerben (dessen CA-Zertifikate also über einen aktuellen Webbrowser prüfbar ist, vgl. A_14776). Für dieses TLS-Zertifikat fragt das Access Gateway (die HTTPS-Schnittstelle ist Teil davon) regelmäßig für das OSCP-Stapling (vgl. [gemSpec_Krypt#A_24913-]) den OSCP-Responder des TSP nach dem Sperrstatus des TLS-Zertifikats. Als Antwort erhält das Access Gateway eine OSCP-Response. Diese wird nach A_19126 geprüft und anschließend von der HTTPS-Schnittstelle verwendet (vgl. <https://tools.ietf.org/html/rfc6066#section-8> und bspw. http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_stapling).*

Um dies zu ermöglichen, muss der Paketfilter entsprechende stateful-Firewall-Regeln gemäß A_14019-* und A_19126 definieren.

A_19126-02 - Access Gateway, OSCP-Status für das OSCP-Stapling

Der Paketfilter der Komponente Access Gateway MUSS bezüglich des OSCP-Stapling (vgl. A_24913-*) folgende Vorgaben umsetzen:

1. Für das vom Aktensystem-Anbieter erworbene TLS-Zertifikat (vgl. Hinweis zu A_14019-01) MUSS die Komponente initial die IP-Adresse (ggf. die IP-Adressen) des entsprechenden OSCP-Responser ermittelt.
2. Diese IP-Adresse(n) MÜSSEN gemäß A_14019-01 per stateful-Firewalling Verbindungen von der HTTPS-Schnittstelle an den OSCP-Responder erlaubt werden.
3. Gemäß OSCP-Stapling (<https://tools.ietf.org/html/rfc6066#section-8>) MUSS die Komponente regelmäßig eine OSCP-Response vom entsprechenden OSCP-Responder beziehen (Die Regelmäßigkeit wird vom zertifikatsausgebenden TSP und der Gültigkeitsdauer dessen OSCP-Responses bestimmt).
4. Die OSCP-Responses MÜSSEN von der Komponente geprüft werden (Signaturprüfung, CertID in der OSCP-Response passt zum angefragten Zertifikat). Falls eine der Prüfung ein nicht-positives Ergebnis liefert, so MUSS die erhaltene OSCP-Response verworfen werden.
5. Sollte die letzte in der Komponente vorhandene OSCP-Response zeitlich nicht mehr gültig sein (bspw. der OSCP-Responder im Internet war länger nicht erreichbar), so MUSS diese OSCP-Response verworfen werden und ein von einem Klienten (ePA FdV) initiiertes TLS-Verbindungsaufbau der HTTPS-Schnittstelle ohne OSCP-Stapling durchgeführt werden.

[\leq]

A_14776 - Access Gateway, Richtlinien zum TLS-Verbindungsaufbau

Die Komponente Access Gateway MUSS sich beim TLS-Verbindungsaufbau gegenüber dem Client mit einem Extended Validation TLS-Zertifikat eines Herausgebers gemäß [CAB Forum] authentisieren. Das Zertifikat MUSS an die Schnittstelle der Proxy-Komponente gebunden werden.[<=]

3.19.1.2 Redundanz

Die Anforderungen zur Verfügbarkeit ergeben sich aus [gemSpec_Perf#3.18.1.3]. Die Verfügbarkeit wird hergestellt durch Anzahl, Verteilung und Konfiguration der Access Gateways.

Die Auswahl der Access Gateways wird durch das ePA-Frontend des Versicherten aus einer durch DNS übermittelten Liste vorgenommen. Auf die Auswahl des Access Gateways kann der Anbieter des ePA-Aktensystems durch die Konfiguration und Anpassung der DNS-Einträge Einfluss nehmen. Die Verfügbarkeit ist hergestellt, wenn jeder Versicherte mit existierendem Konto beim Anbieter des ePA-Aktensystems oder dessen berechtigter Vertreter die Möglichkeit zum Verbindungsaufbau hat.

Eine hardwaretechnische Hochverfügbarkeit der einzelnen Access Gateways ist über grundlegende Maßnahmen, wie redundante Netzteile hinaus nicht erforderlich. Es steht dem Anbieter jedoch frei, zur Sicherstellung der Verfügbarkeitsanforderungen technische Lösungen, wie z. B. Load-Balancer und Stateful Failover innerhalb von Clustern einzusetzen, so dass jedes einzelne Access Gateway im Ergebnis eine höhere Verfügbarkeit oder Leistungsfähigkeit besitzt.

A_14026 - Access Gateway, Redundanz der Paketfilter im Access Gateway

Die Komponente Access Gateway MUSS sicherstellen, dass bei Ausfall eines von mehreren Paketfiltern die verbleibenden Paketfilter in dem-selben Standort den Datenverkehr aller Mandanten des ausgefallenen Paketfilters zusätzlich übernehmen können.[<=]

3.19.1.3 Konfiguration

A_14030 - Access Gateway, Verhalten des Access Gateways bei Vollauslastung

Die Komponente Access Gateway MUSS den Paketfilter Internet so konfigurieren, dass bei Vollauslastung der Systemressourcen im ePA-Aktensystem keine weiteren Verbindungen angenommen werden.[<=]

Durch die Zurückweisung von Verbindungen wird sichergestellt, dass das ePA-Frontend des Versicherten einen Verbindungsaufbau mit einem anderen Access Gateway des jeweiligen ePA-Aktensystems versucht, bei dem die erforderlichen Ressourcen zur Verfügung stehen.

3.19.1.4 Adressierung

3.19.1.4.1 Access Gateway zum Transportnetz Internet

A_14031 - Access Gateway, IPv4-Adressierung der Internetschnittstellen des Access Gateways

Der Anbieter des ePA-Aktensystems MUSS jedem Access Gateway genau eine öffentliche IPv4-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentlichen IP-Adressen des Access Gateways MÜSSEN vom Anbieter des ePA-Aktensystems zur Verfügung gestellt werden.[<=]

A_14032 - Access Gateway, IPv6-Adressierung der Internetschnittstellen des Access Gateways

Der Anbieter des ePA-Aktensystems SOLL jedem Access Gateway eine IPv6-Adresse zuweisen. Diese Adresse MUSS auf der physischen Schnittstelle zum Internet konfiguriert werden. Die öffentliche IPv6-Adresse MUSS vom Anbieter des Access Gateways zur Verfügung gestellt werden. [≤]

3.19.1.4.2 ePA-Aktensystem zum Zentralen Netz

Die Adressen des ePA-Aktensystems am Übergang zur TI werden vom Anbieter des Zentralen Netzes aus dem Adressblock TI_Zentral zugewiesen.

3.19.2 Proxy für das VAU-Protokoll

Das Access Gateway leitet Anfragen vom ePA-FdV über den VAU-Kanal an die zuständige VAU-Instanz weiter, damit diese dort in der User Session des Versicherten verarbeitet werden können.

A_24331 - Access Gateway - Data Proxy

Das Access Gateway MUSS die VAU-Protokoll-Kommunikation des ePA-Frontend des Versicherten an die zuständige VAU-Instanz weiterleiten. [≤]

3.19.3 Proxy Schlüsselgenerierungsdienst

Zur Nutzung der in [gemSpec_SGD_ePA] beschriebenen Schlüsselableitungsfunktionalität für den Schutz von Akten- und Kontextschlüssel einer ePA werden Aufrufe zu den Schlüsselgenerierungsdiensten SGD 1 und SGD 2 über den "Proxy Schlüsselgenerierungsdienst" ermöglicht.

Der Proxy SGD stellt sicher, dass ein ePA-FdV Aufrufe an den SGD 1 und SGD 2 durchführen kann.

Die Information, auf welche Anfragen (Pfade) des ePA-FdV der Proxy SGD aktiv wird ("/SGD1" für den SGD 1 und "/SGD2" für den SGD 2), sind in [gemSpec_SGD_ePA#2.2 Tabelle 2] angegeben.

A_17495 - Access Gateway, Zugriff auf den Schlüsselgenerierungsdienst

Der Proxy Schlüsselgenerierungsdienst der Komponente Access Gateway MUSS sicherstellen, dass das ePA-FdV auch ohne Authentisierung und Autorisierung Zugriff auf den SGD 1 und den SGD 2 erhält.

[≤]

3.19.4 Tracing in Nichtproduktivumgebungen

Für die Fehlersuche - insbesondere bei IOP-Problemen zwischen Produkten verschiedener Hersteller in einer fortgeschrittenen Entwicklungsphase - hat es sich als notwendig erwiesen, dass ein Fehlersuchender den Klartext der Kommunikation zwischen ePA-Client und VAU-Instanz mitlesen kann. (vgl. auch 2.5- Tracing in Nichtproduktivumgebungen)

Das Access Gateway stellt Informationen über die aktuell verfügbaren Sensorpunkte im AS bereit. Weiterhin exponiert das Access Gateway die Daten der Sensorpunkte über TCP (i. S. v. nicht TLS-gesichert) bspw. über Port 8001,...,8009. Die dort von den Sensorpunkten ge-streamten Daten sind nur Testdaten, also keine Echtdaten, d. h. sie haben keinen Schutzbedarf bezüglich Vertraulichkeit. Um die exponierten Sensordaten-Punkte vor DoS-Angriffen zu schützen, erlaubt das Access Gateway im Fall der Fälle die TCP-Ports auf IP-Layer über Firewall-Regeln abzusichern.

A_21890-01 - Access Gateway, Sensorpunkt für Nichtproduktivumgebungen

Die Komponente Access Gateway MUSS genau in Nichtproduktivumgebungen:

- die Daten der Sensorpunkte des Aktensystems auf TCP-Ports (bspw. ab Port 8000) öffentlich (ggf. auch ohne TLS-Sicherung) im Internet zur Verfügung stellen, indem die aktuell an den Sensorpunkten auflaufenden Daten auf dem TCP-Port am Access Gateway öffentlich gestreamt werden.
- die Möglichkeit bieten, den Zugriff auf diese TCP-Ports durch Firewall-Einstellungen auf IP-Layer zu beschränken.

Weiterhin MUSS das Access Gateway über die URL /tracingpoints Informationen über die aktuell im AS verfügbaren und damit auch im Access Gateway öffentlich exponierten Sensorpunkt-Daten als JSON-Array (=> Response-Type 'application/json') der folgenden Form bereitstellen:

```
[
  { "name" : "zentraler Tigerproxy",
    "port" : 8001,
    "DoS-protection-type" : „secret_url“
    "DoS-protection-port" : „udp/46789“
  },
  { "name" : "Extra Sensor VAU RZ2/B1/R1",
    "port" : 8002,
    "DoS-protection-type" : „ssh_tunnel“
    "DoS-protection-port" : „tcp/46790“
  }, ...
]
```

Sollten keine Sensorpunkte aktuell im AS aktiviert sein (bspw. bei Lasttests) so ist das Array leer: [].

Sollte es keinen optionalen DoS-Schutzmechanismus gemäß A_22582-* geben, so fallen die DoS-* Attribute in der o. g. Datenstruktur weg (sind nicht existent).

Die einzelnen Felder des Arrays sind associative array (oder auch maps oder dictionaries genannt). Diese KÖNNEN neben "name" und "port" beliebige vom AS definierbare, weitere key-value-Paare enthalten. Der Eintrag "port" gibt an, an welchem öffentlich erreichbaren TCP-Port des Access Gateway die Sensordaten des entsprechenden Sensors abrufbar sind (gestreamt werden).

[<=]

Hinweis zu A_21890-: Die semistatische JSON-Datei, welche ein Client unter dem Pfad „/tracingpoints“ erhalten kann, ist eine einfache Form von Service-Discovery. Damit kann ein Client (Fehlersuchende(r)) erfahren, welche Tracing-Quellen es aktuell im AS gibt i. S. v. welche Tracing-Quellen ein Client zur Fehlersuche aktuell verwenden kann.*

A_22582 - Tracing in Nichtproduktivumgebungen, DoS-Schutz

Die Komponente Access Gateway KANN Sicherheitsmechanismen bereitstellen und aktivieren, die es genau in Nichtproduktivumgebungen ermöglichen, temporär, automatisiert und nur nach erfolgreicher Authentifizierung die TCP-Ports für das Streaming der Sensorpunkte für Clients nach A_21890-* freizuschalten. [<=]

Hinweis zu A_22582-: In den Nichtproduktivumgebungen darf es keine Echtdaten geben. Es dürfen sich dort nur Daten befinden, deren Schutzbedarf bezüglich Vertraulichkeit niedrig ist. Der optionale Schutzmechanismus nach A_22582-* braucht nur einen einfachen DoS-Schutz leisten gegen einen Angreifer mit niedrigen Angriffspotential. Der Anbieter ist, sofern er einen solchen Mechanismus einsetzen möchte, frei, dafür den Mechanismus selbst zu wählen. Er wählt dann bei "DoS-protection-type" (vgl. A_21890-*) einen selbstdefinierten (möglichst sprechenden) Namen.*

Beispiele für Umsetzungsmöglichkeiten:

1. Es gibt im Access Gateway eine geheime URL (bspw. /tracing/964b059de83d20581f43dd1b867d740c). Ein Client kennt das Geheimnis und ruft diese URL auf. Daraufhin wird im Access Gateway für die IP-Adresse des Clients die Tracing-Quelle im Access Gateway frei geschaltet (TCP-Port 8000, ...).
2. Die gematik stellt eine Beispielimplementierung zur Verfügung. Dort gibt es einen UDP-Server (Access Gateway) und einen UDP-Client (Fehlersuchende), die beide ein gemeinsames HMAC-Geheimnis teilen. Wenn der Client die aktuelle Zeit und dessen IP-Adresse per HMAC authentisiert dem UDP-Server sendet, so schaltet der UDP-Server nach erfolgreicher Prüfung des HMACs den entsprechenden TCP-Port für die authentifizierte IP-Adresse des Clients frei.
3. Auf dem Access Gateway läuft ein SSH-Daemon. Der öffentliche Authentisierungsschlüssel eines Clients ist dort als gültiger Nutzer konfiguriert (Login-Shell: /bin/false). Die Tracing-Quellen im Access Gateway sind so konfiguriert, dass sie nur mittels authentisierten SSH-Port-Forwarding (<https://www.ssh.com/academy/ssh/tunneling/example>) erreichbar sind.

3.19.5 Übergreifende Festlegungen

A_14249 - Komponente Access Gateway - Separierung der Schnittstellen für verschiedene Umgebungen

Die Komponente Access Gateway MUSS die Bereitstellung von Schnittstellen für die Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen Umgebungen der TI (RU/TU, PU) sicherstellen und voneinander separieren. [<=]

A_14034 - Access Gateway, Übergang des ePA-Aktensystems zur TI

Die Komponente Access Gateway MUSS sicherstellen, dass der Zugriff auf Dienste der TI ausschließlich über einen Sicheren Zentralen Zugangspunkt (SZZP) erfolgt. [<=]

A_14036 - Access Gateway, Synchronisierung der Komponenten mit den Stratum-1-NTP-Servern der TI

Die Komponente Access Gateway MUSS alle Komponenten seines Access Gateways mit den Stratum-1-NTP-Servern der TI synchronisieren. [<=]

A_13879 - Access Gateway, Serverseitige Authentisierung

Die Komponente Access Gateway MUSS sich gegenüber dem ePA-Frontend des Versicherten beim Aufbau der TLS-Session durch sein ExtendedValidation-Zertifikat authentisieren. Die Beschaffung des Zertifikats erfolgt durch den Anbieter über eine öffentliche CA. [<=]

A_14033 - Access Gateway, TLS Verschlüsselung

Die Komponente Access Gateway MUSS sicherstellen, dass jede Kommunikation mit dem ePA-Frontend des Versicherten TLS verschlüsselt erfolgt. [<=]

Die Verwendung der SoapAction ermöglicht einer Reverse-Proxy-Komponente innerhalb des Access Gateways, die Nachrichten zu verarbeiten, ohne die http-Payload zu untersuchen.

A_13876 - Access Gateway, Kein direkter Zugriff auf Dienste der zentralen TI-Plattform

Die Komponente Access Gateway MUSS einen direkten Zugriff aus dem Internet auf Dienste der zentralen TI-Plattform verhindern. [<=]

A_14016 - Access Gateway, Schutz vor Angriffen aus dem Internet

Die Komponente Access Gateway MUSS für alle vom Internet erreichbaren Schnittstellen Maßnahmen zum Schutz vor DoS-Angriffen auf Anwendungsebene treffen. Weitere

Angriffe auf Anwendungsebene MÜSSEN mindestens durch Einsatz geeigneter IDS/IPS Lösungen verhindert werden. [<=]

A_15196 - Access Gateway, Schutz vor volumetrischen DoS-Angriffen

Die Komponente Access Gateway MUSS bei Beauftragung eines qualifizierten Dienstleisters zum Schutz vor volumetrischen DoS-Angriffen Kriterien des BSI zur Auswahl qualifizierter Dienstleister umsetzen. [<=]

Als Maßnahme gegen volumetrische Denial-of-Service-Angriffe wird die Verwendung von DNS- oder BGP-Routing-Diensten empfohlen. Hinweise des BSI:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahrenungen/DDoS/ddos_node.html.

3.20 Schnittstellen (OpenAPI)

Hinweis: Die Vorgaben in den beschreibenden Dateien der REST-Schnittstellen (yaml) sind normativ für den Anbieter der Schnittstellen. Die Anforderungen im vorliegenden Dokument ergänzen diese Vorgaben, insbesondere, wenn diese für sicherheitstechnische Gutachten erforderlich sind.

3.20.1 Übersicht der Schnittstellen des Aktensystems

Tabelle 41: Übersicht der Schnittstellen des Aktensystems

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Consent_Decision_Management	
Schnittstelle des Consent Decision Managements gemäß [I_Consent_Decision_Management]	
updateConsentDecision	Diese Operation erlaubt dem FdV und der Ombudsstelle die Änderung des Zustand des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen der ePA für eine Funktion.
getConsentDecisions	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen aller Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der ePA.
getConsentDecision	Diese Operation erlaubt dem FdV und der Ombudsstelle das Lesen eines Widerspruchs einer Funktion gegen die Nutzung von widerspruchsfähigen Funktionen.
getUserSpecificMedicationDenyList	Diese Operation erlaubt dem FdV und der Ombudsstelle die Ansicht, welche LEI keinen Zugriff auf den Medication Service haben.
setUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI in die Liste der LEIs aufzunehmen, die keinen Zugriff auf den Medication Service haben.
getUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine bestimmte LEI aus der Liste der LEIs anzuzeigen, die keinen Zugriff auf den Medication Service haben.
deleteUserSpecificMedicationDeny	Diese Operation erlaubt dem FdV und der Ombudsstelle eine LEI aus der Liste der LEIs zu entfernen, damit diese LEI wieder Zugriff auf den Medication Service haben kann.
I_Constraint_Management_Insurant	

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
Schnittstelle des Constraint Managements gemäß [I_Constraint_Management_Insurant]	
getDenyPolicyAssignments	Diese Operation gibt eine Liste aller konfigurierten Einträge der General Deny Policy aus.
setPolicyAssignment	Diese Operation fügt der General Deny Policy einen neuen Eintrag hinzu.
deletePolicyAssignment	Diese Operation löscht einen bestimmten Eintrag der General Deny Policy.
I_Entitlement_Management	
Schnittstelle des Entitlement Management gemäß [I_Entitlement_Management] zur Vergabe von Befugnissen und Befugnisausschlüssen	
setEntitlementPs	Diese Operation fügt eine Befugnis für eine Leistungserbringerinstitution in einer Behandlungssituation hinzu.
getEntitlements	Diese Operation erlaubt dem FdV den Abruf aller aktuellen Befugnisse.
getEntitlement	Diese Operation erlaubt dem FdV den Abruf einer bestimmten Befugnis.
setEntitlement	Diese Operation erlaubt dem FdV das Setzen einer Befugnis für einen Nutzer.
deleteEntitlement	Diese Operation erlaubt dem FdV den Abruf das Löschen einer existierenden Befugnis.
getBlockedUserPolicyAssignments	Diese Operation erlaubt dem FdV den Abruf der aktuell vorhandenen Befugnisausschlüsse.
setBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Befugnisausschluss für einen Nutzer.
getBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV den Abruf eines bestimmten Befugnisausschlusses.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
deleteBlockedUserPolicyAssignment	Diese Operation erlaubt dem FdV die Aufhebung eines Befugnisausschlusses.
I_Entitlement_Management_EU	
Schnittstelle des Entitlement Management EU-Zugriff gemäß [I_Entitlement_Management_EU] zur Verwaltung Befugnis EU-Zugriff	
setEntitlementEu	Diese Operation erlaubt dem FdV das Setzen einer Befugnis EU-Zugriff für einen Versicherten.
getAccessCode	Diese Operation erlaubt dem FdV den Abruf des Zugriffscodes für die Befugnis EU-Zugriff.
Render API: PDF Audit	
Schnittstelle des Audit Event Service gemäß [IG_Audit_Event_Service] zum Abruf der Protokolldaten in lesbarer Form	
renderAuditEventsToPDF	Diese Operation erlaubt FdV und Ombudsstelle den Abruf der Protokolldaten als PDF.
Query API: AuditEvent	
Schnittstelle des Audit Event Service gemäß [IG_Audit_Event_Service] zum Abruf der Protokolldaten im FHIR-Format	
listAuditEvents_AuditEventSvc	Diese Operation ermöglicht die Suche nach AuditEvent Instanzen.
getAuditEventById_AuditEventSvc	Diese Operation ermöglicht das Lesen einer AuditEvent Instanz.
I_Health_Record_Relocation_Service	
Schnittstelle zur Steuerung des Aktenumzugs aus der Umgebung des Kostenträgers	
startPackageCreation	Diese Operation initiiert die Erstellung eines Export Pakets für den Umzug eines Aktenkontos zu einem neuen Anbieter.

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
startPackageImport	Diese Operation initiiert den Import eines Export Pakets in ein neu erstelltes Aktenkonto.
I_Device_Management_Insurant	
Schnittstelle zur Geräteverwaltung aus der Umgebung des Versicherten	
getDevice	Diese Operation ruft eine bestimmte Geräteregistrierung ab.
getDevices	Diese Operation ruft alle Geräteregistrierungen ab.
updateDevice	Diese Operation ändert den Displayname einer Geräteregistrierung.
deleteDevice	Diese Operation löscht eine bestimmte Geräteregistrierung.
registerDevice	Diese Operation erzeugt eine neue Geräteregistrierung und neue Geräteparameter
confirmPendingDevice	Diese Operation bestätigt eine neue Geräteregistrierung mit einem Geräteregistrierungscode
getDeviceAttestation	Diese Operation ruft die Bestätigung einer Geräteregistrierung am Home-AS ab.
I_Authorization_Service	
Schnittstelle der Autorisierung für den Login	
getFHIRVZDtoken	Diese Operation bezieht das search-access-token für den Zugriff auf den FHIR VZD vom Aktensystem
getNonce	Diese Operation bezieht einen eindeutigen einmalig generierten Zufallswert für die Client Attestierung
sendAuthorizationRequestSC	Diese Operation initiiert die Authentifizierung eines Leistungserbringers

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
sendAuthorizationRequestFdV	Diese Operation initiiert die Authentifizierung eines ePA-FdV
getFreshnessParameter	Diese Operation erzeugt einen Frischeparameter für die Authentisierung mittels Bearer Token
sendAuthorizationRequestBearerToken	Diese Operation initiiert die Authentifizierung über Bearer Token
sendAuthCodeSC	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
sendAuthCodeFdV	Diese Operationen übergibt den Authorization Code für den Bezug des ID-Token
logoutFdV	Diese Operation beendet aktiv die Sitzung
I_Medication_Service_eML_Render	
renderEMLAsHTML	Diese Operation gibt die Medikationsliste im html-Format zurück.
renderEMLAsPDF	Diese Operation gibt die Medikationsliste im PDF/A-Format zurück.
I_Medication_Service_FHIR	
REST-Schnittstelle zum Abruf der Medikationsdaten im FHIR-Format	
I_Email_Management	
getEmailAddress	Diese Operation ruft die hinterlegte E-Mail-Adresse des Versicherten ab.
replaceEmailAddress	Diese Operation setzt oder ändert die E-Mail Adresse für einen Versicherten ab.
I_Tool_Convert_PDF_Insurant	
Schnittstelle des XDS Document Managements gemäß [I_Tool_Convert_PDF_Insurant]	
convertPDF	Diese Operation konvertiert ein PDF in ein PDF/A Format

Schnittstellen des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Data_Submission_Service	
Schnittstelle des Data Submission Service gemäß [I_Data_Submission_Service]	
getSubmissionPackage	Diese Operation stellt dem FDZ ein Datenpaket für eine bestimmte SubmissionID bereit.

Schnittstellen des Aktensystems (Nutzung ohne VAU-Kanal)	
I_Information_Service	
Schnittstelle des Informationsdienstes gemäß [I_Information_Service]	
getConsentDecisionInformation	Diese Operation liest den aktuellen Zustand der Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der Funktionsklasse "Versorgungsprozess" aus.
setUserExperienceResult	Die Operation dient der Sammlung von Client Performedaten aus der Umgebung der Leistungserbringer.
getRecordStatus	Diese Operation fragt Existenz und Status eines bestimmten Aktenkontos bei einem Betreiber an.
I_Information_Service_Accounts	
Schnittstelle des Information Service gemäß [I_Information_Service_Accounts] für Anbieter Aktensystem im Kontext eines Aktenkontoumzugs	
getGeneralConsentDecision	Diese Operation dient der Abfrage eines Widerspruchs gegen die Nutzung der ePA bei einem anderen Aktensystemanbieter.
startRelocation	Diese Operation initiiert die Erstellung eines Export Pakets für die Relocation.
deleteExportPackage	Diese Operation schließt den Vorgang der Relocation erfolgreich ab.
postExportPackageIncident	Diese Operation erhält Benachrichtigungen zum Relocation-Prozess.
putDownloadUrlForExportPackage	Diese Operation initiiert den Import eines Export Packages.
postPackageDeliveryIncident	Diese Operation erhält Benachrichtigungen zum Relocation-Prozess.
getProviderList	Diese Operation gibt eine Liste von FQDNs der Versicherungen / ePA-Anbieter aus

Die Schnittstellen (REST) und Operationen sind funktional in den Beschreibungen der jeweiligen Schnittstelle beschrieben. Darüber hinaus gelten die folgenden übergreifenden Anforderungen.

3.20.2 Übergreifende Festlegungen zu den Schnittstellen

A_23918 - Schnittstellen (OpenApi) - Prüfung der Befugnis

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) eine vorhandene und gültige Befugnis (entitlement) für den Nutzer der Operation fordern und diese nicht vorliegt. [\leq]

Hinweis: A_23918 deckt auch die Fehlersituationen "kein VAU-Kanal" und "keine User Session" ab, da diese eine Vorbedingung für den Nachweis einer gültigen Befugnis sind.

A_24365 - Schnittstellen (OpenApi) - Prüfung des Aktenkontos

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) die Existenz des adressierten Aktenkontos fordern und diese nicht für den Operationsaufruf verwendet wird. [\leq]

Hinweis A_24365 deckt auch die Fehlersituation "kein Health Record Context" ab, da dieses nur infolge eines nicht vorhandenen Aktenkontos auftritt.

A_24538 - Schnittstellen (OpenApi) - Prüfung des Aktenkontostatus

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) einen vorgegebenen Status des Aktenkontos fordern und dieser nicht vorhanden ist. [\leq]

A_24366 - Schnittstellen (OpenApi) - Prüfung der Rolle

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) die Zulässigkeit der Operation auf bestimmte Rollen (professionOID) einschränken und der Nutzer der Operation diese nicht nachweist. [\leq]

A_24367 - Schnittstellen (OpenApi) - Prüfung des Identifiers

Das ePA-Aktensystem MUSS die Ausführung der Operationen der REST-Schnittstellen ablehnen und mit einem Fehler beenden, wenn diese in ihren Bedingungen (Conditions) die Zulässigkeit der Operation auf bestimmte Identifier (KVNR oder Telematik-ID) einschränken und der Nutzer der Operation diese nicht nachweist. [\leq]

A_24580 - Schnittstellen (OpenApi) - Protokollierung der Operationen

Das ePA-Aktensystem MUSS nach der Ausführung der Operationen der REST-Schnittstellen einen Protokolleintrag erstellen, wenn die Protokollierung in den Nachbedingungen (Postconditions) der Operationen gefordert ist (log-entry). [\leq]

4 Informationsmodelle

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

5 Anhang A – Verzeichnisse

5.1 Abkürzungen

Kürzel	Erläuterung
AdV	Anwendungen des Versicherten
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BGP	Border Gateway Protokoll
BPPC	Basic Patient Privacy Consents
CRUD	Create Read Update Delete
DiGA	Digitale Gesundheitsanwendung
ePA-FdV	ePA-Frontend des Versicherten
ePA-FdV AdV	ePA-Frontend des Versicherten im KTR-AdV-Terminal
HL7	Health Level Seven
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IHE ITI TF	IHE IT Infrastructure Technical Framework
JWT	JSON-Web-Token
JWS	signiertes JSON-Web-Token
KTR	Kostenträger
MIO	Medizinisches Informationsobjekt

Kürzel	Erläuterung
MTOM	Message Transmission Optimization Mechanism
OASIS	Advancing Open Standards for the Information Society
OID	Object Identifier
PDSG	Patientendaten-Schutz-Gesetz
PHR	Personal Health Record
RMU	Restricted Metadata Update Profile
SAML	Security Assertion Markup Language
TLS	Transport Layer Security
UUID	Universally Unique Identifier
VAU	Vertrauenswürdige Ausführungsumgebung
W3C	World Wide Web Consortium
WS-I	Web-Services Interoperability Consortium
XCA	Cross-Community Access Profile
XDS	Cross-Enterprise Document Sharing Profile
XDW	Cross-Enterprise Document Workflow Profile
XOP	XML-binary Optimized Packaging
XSPA	Cross-Enterprise Security and Privacy Authorization Profile

5.2 Glossar

Begriff	Erläuterung
Authenticator-Modul	Das Authenticator-Modul ist die Client-Komponente zum sektoralen Identity Provider. Über die das Authenticator-Modul authentifiziert sich der Versicherte gegenüber des sektoralen IDP. Das Authenticator-Modul kann in ein App (z.B. Service-App einer Krankenkasse oder ePA-FdV) integriert oder als eigenständige App implementiert werden (siehe auch [gemSpec_IDP_Sek]).

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

5.3 Abbildungsverzeichnis

Abbildung 1: Alternativen zur Ausführung des Befugnisverifikations-Moduls	52
Abbildung 2 - Überblick Service-VAUs	85
Abbildung 3: Zeitabschnitte Umschlüsselung und Überschlüsselung	89
Abbildung 4: Zeitabschnitte Umschlüsselung lange nicht verwendeter Akten bei einer Überschlüsselung	90
Abbildung 5: Ablauf der Authentifizierung von Versicherten über den sektoralen IDP ..	215
Abbildung 6: Ablauf der Authentifizierung einer LEI über den Smartcard IDP	219
Abbildung 7: Ablauf der Authentisierung des E-Rezept-Fachdienstes	221

5.4 Tabellenverzeichnis

Tabelle 1: Tab_Prüfung_Signaturzertifikate Parameter Prüfung Signaturzertifikat	17
Tabelle 2: Protokollierung der Migration der medizinischen Daten	28
Tabelle 3: Protokollierung der Migration der Protokolldaten des Versicherten	30
Tabelle 4: Zustandswechsel im Lebenszyklus eines Aktenkontos.....	33
Tabelle 5 : Health Record Relocation Service Protokollierung	42
Tabelle 6: Tab_AS_VAU_Token_Modul_Rules -Prüfregeln VAU Token	53
Tabelle 7: Überblick über die Regeln des Befugnisverifikations-Moduls	59
Tabelle 8: Tab_AS_Entitlement_Registration_Rules - Regeln zur Registrierung von Befugnissen	61
Tabelle 9: Tab_AS_SDS-Key_Rules Key Rules - Regeln zur Ableitung der versichertenindividuellen Persistierungsschlüssel	71
Tabelle 10: Widerspruchsfähige Funktionen der elektronischen Patientenakte	93
Tabelle 11: Consent Decision Management Protokollierung - Widersprüche für Funktionen der ePA	95
Tabelle 12: Consent Decision Management Protokollierung - User Specific Deny Policy Medication	97
Tabelle 13: Inhalt einer Befugnis	98
Tabelle 14: Befugnisse für berechtigte Nutzergruppen und Nutzer	100
Tabelle 15: Befugnisse EU-Zugriff für berechtigte Nutzergruppen und Nutzer	102
Tabelle 16: Entitlement Management Protokollierung	103
Tabelle 17: Inhalt eines Blocked User Policy Eintrags	112
Tabelle 18: Legal Policy	116

Tabelle 19: Legal Policy - EU-Zugriff	119
Tabelle 20: Beschreibung der Kategorien.....	121
Tabelle 21: Constraint Management Protokollierung.....	125
Tabelle 22: Inhalt eines General Deny Policy Eintrags	127
Tabelle 23: Verbergen eines Medical Service.....	128
Tabelle 24: Kennzeichnung von Optionalitäten	141
Tabelle 25: Übersicht über gruppierte IHE ITI-Akteure und Optionen an den Außenschnittstellen des XDS Document Service	142
Tabelle 26: Schnittstelle I_Document_Management	154
Tabelle 27: Schnittstelle I_Document_Management_Insurant	157
Tabelle 28: Schnittstelle I_Document_Management_Ncpeh.....	159
Tabelle 29: Festlegung Folder.entryUUID zu statischen Ordnern.....	161
Tabelle 30: Nutzungsvorgaben für Metadatenattribute XDS	163
Tabelle 31: Tab_LanguageCodes - Mindestanforderung an zu unterstützende Language Codes	180
Tabelle 32: Einsortierung_Datenkategorien.....	185
Tabelle 33: TAB_EPA_Sammlungstypen	188
Tabelle 34: Auswirkungen bei Widerspruch gegen eine Funktion der ePA	190
Tabelle 35: XDS Document Service Protokollierung.....	192
Tabelle 36: Patient Information Service Protokollierung.....	196
Tabelle 37: Medication Service Protokollierung	199
Tabelle 38 : Inhaltliche Definitionen eines AuditEvent	204
Tabelle 39 Befüllung AuditEvent	205
Tabelle 40: Audit Event Service Protokollierung.....	210
Tabelle 41: Übersicht der Schnittstellen des Aktensystems	229

5.5 Referenzierte Dokumente

5.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemKPT_ePAfuerAlle]	gematik: Grobkonzept der "ePA für alle"

[Quelle]	Herausgeber: Titel
[gemSpec_FdV_ePA]	gematik: Spezifikation ePA-Frontend des Versicherten
[gemSpec_IDP_Sek]	gematik: Spezifikation des sektoralen IDP (GesundheitsID)
[gemSpec_IDP_FD]	gematik: Spezifikation der Fachdienste der TI-Föderation
[gemSpec_IDP_Frontend]	gematik: Spezifikation der Frontendkomponenten für Fachdienste der TI-Föderation
[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform
[gemSpec_IG_ePA]	gematik: Implementation Guides für strukturierte Dokumente GitHub: GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/implementation_guides
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory
[gemTerminology]	gematik: Terminologies for Telematics Infrastructure (TI) Simplifier: https://simplifier.net/packages/de.gematik.terminology/1.0.5
[I_Consent_Decision_Management]	gematik: I_Consent_Decision_Management REST-Schnittstell zum Management der Widersprüche zu Versorgungsprozessen GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Consent_Decision_Management.yaml

[Quelle]	Herausgeber: Titel
[I_Constraint_Management_Insurant]	gematik: I_Constraint_Management_Insurant.yaml REST-Schnittstelle zum Verbergen und Sichtbarmachen von Dokumenten GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Constraint_Management_Insurant.yaml
[I_Entitlement_Management]	gematik: I_Entitlement_Management REST-Schnittstelle zur Verwaltung von Befugnissen und Befugnisausschlüssen GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Entitlement_Management.yaml
[I_Entitlement_Management_EU]	gematik: I_Entitlement_Management_EU REST-Schnittstelle zur Verwaltung von Befugnissen EU-Zugriff GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Entitlement_Management_EU.yaml
[I_Device_Management_Insurant]	gematik: I_Device_Management_Insurant.yaml REST-Schnittstelle zur Geräteverwaltung GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Device_Management_Insurant.yaml
[I_Health_Record_Relocation_Service]	gematik: I_Health_Record_Relocation_Service REST-Schnittstelle zum Aktenumzug GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Health_Record_Relocation_Service.yaml
[I_Information_Service_Accounts]	Schnittstellenspezifikation Information Service für Betreiber GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Information_Service_Accounts.yaml
[I_Information_Service]	Schnittstellenspezifikation Information Service GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Information_Service.yaml
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung und impliziten Geräteregistrierung GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Authorization_Service.yaml

[Quelle]	Herausgeber: Titel
[IG_Audit_Event_Service]	gematik: FHIR Implementation Guide "Audit Event Service" Simplifier: https://simplifier.net/guide/audit-event-service?version=1.0.0
[I_Email_Management]	gematik: I_Email_Management REST-Schnittstelle zum Management von E-Mail-Adressen eines Versicherten GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Email_Management.yaml
[I_Tool_Convert_PDF_Insurant]	gematik: I_Tool_Convert_PDF_Insurant Schnittstelle für die PDF Formatkonvertierung GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/openapi/ I_Tool_Convert_PDF_Insurant.yaml
[XDSDocumentService]	gematik: XDSDocumentService.wsdl IHE-Schnittstelle des XDSDocumentService GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/schema
[HealthRecordMigration]	gematik: ref-ePA-HealthRecordMigration Referenzimplementierung und Vorgaben für das Exportpaket bei einem Anbieterwechsel GitHub: https://github.com/gematik/ref-ePA-HealthRecordMigration Branch: ePA-3.1
[IG_Patient_Information_Service]	gematik: FHIR Implementation Guide "Patient Information Service" Simplifier: https://simplifier.net/guide/patient-information-service?version=1.0.0
[IG_Medication_Service]	gematik: FHIR Implementation Guide "Medication Service" Simplifier: https://simplifier.net/guide/medication-service?version=1.1.0

5.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-RMD]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.6 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-RMU]	IHE International (2021): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.3 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf
[IHE-ITI-TF1]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Profile definition, use-case analysis, actor definition, and use of transactions and content, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume1/
[IHE-ITI-TF2]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume2/
[IHE-ITI-TF3]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Document Sharing Metadata and Content Profiles, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume3/
[I_VST]	Vertrauensstelle ePA – Pseudonymisierungskonzept Datenausleitung ePA zu Forschungszwecken Version 2.0 (12.07.2024), Herausgeber: Robert Koch-Institut, Nordufer 20, 13353 Berlin
[MIO-UH]	Kassenärztliche Bundesvereinigung (2022): Kinderuntersuchungsheft, https://mio.kbv.de/display/UH1X0X1
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://datatracker.ietf.org/doc/html/rfc2119

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC3339]	IETF (2002): Date and Time on the Internet: Timestamps, RFC 3339, https://datatracker.ietf.org/doc/html/rfc3339
[RFC4122]	IETF (2005) A Universally Unique IDentifier (UUID) URN Namespace, RFC 4122 https://datatracker.ietf.org/doc/html/rfc4122
[RFC5246]	IETF (2008): The Transport Layer Security (TLS) Protocol Version 1.2 https://datatracker.ietf.org/doc/html/rfc5246
[RFC7231]	IETF (2014): Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, RFC 7231, https://datatracker.ietf.org/doc/html/rfc7231
[RFC7515]	IETF (2015): JSON Web Signature (JWS), RFC-7515 https://datatracker.ietf.org/doc/html/rfc7515
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), https://www.w3.org/TR/soap12-part1/
[WSA]	OASIS (2004): Web Services Addressing (WS-Addressing), https://www.w3.org/Submission/ws-addressing/
[WSIAP]	Web-Services Interoperability Consortium (2007): WS-I Attachment Profile V1.0, http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[WSIBSP]	Web-Services Interoperability Consortium (2006): WS-I Basic Security Profile Version V1.1, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html
[WSS]	OASIS (2006): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[XMLSchema]	W3C (2004): XML Schema Part 1: Structures Second Edition, http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/
[XHTML]	W3C (2010): XHTML 1.1 - Module-based XHTML - Second Edition, https://www.w3.org/TR/xhtml1/