

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Spezifikation Fachmodul ePA im KTR- Consumer**

Version: 1.3.3  
Revision: 720522  
Stand: 11.03.2022  
Status: freigegeben  
Klassifizierung: öffentlich  
Referenzierung: gemSpec\_FM\_ePA\_KTR\_Consumer

---

## Dokumentinformationen

---

### Änderungen zur Vorversion

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

### Dokumentenhistorie

| Version | Stand      | Kap./<br>Seite | Grund der Änderung, besondere<br>Hinweise                | Bearbeitung |
|---------|------------|----------------|----------------------------------------------------------|-------------|
| 1.0.0   | 30.04.2019 |                | initiale Erstellung des Dokuments                        | gematik     |
| 1.1.0   | 28.06.19   |                | Einarbeitung von P19.1                                   | gematik     |
| 1.2.0   | 30.06.20   |                | freigegeben                                              | gematik     |
| 1.3.0   | 12.10.20   |                | Einarbeitung der Scope-Themen von<br>R4.0.1              | gematik     |
| 1.3.1   | 19.02.21   |                | Einarbeitung Änderungsliste P22.5                        | gematik     |
| 1.3.2   | 11.02.22   |                | Einarbeitung Änderungsliste<br>Consumer_Maintenance_21.4 | gematik     |
| 1.3.3   | 11.03.22   | 5.4            | Anpassung nach Absprache mit BfDI                        | gematik     |

---

## Inhaltsverzeichnis

---

|                                                                                |           |
|--------------------------------------------------------------------------------|-----------|
| <b>1 Einordnung des Dokumentes.....</b>                                        | <b>5</b>  |
| 1.1 Zielsetzung.....                                                           | 5         |
| 1.2 Zielgruppe.....                                                            | 5         |
| 1.3 Geltungsbereich.....                                                       | 5         |
| 1.4 Abgrenzungen.....                                                          | 5         |
| 1.5 Methodik.....                                                              | 6         |
| <b>2 Systemüberblick.....</b>                                                  | <b>7</b>  |
| <b>3 Systemkontext.....</b>                                                    | <b>8</b>  |
| 3.1 Akteure und Rollen.....                                                    | 8         |
| 3.2 Nachbarsysteme.....                                                        | 8         |
| <b>4 Zerlegung des Produkttyps.....</b>                                        | <b>9</b>  |
| <b>5 Übergreifende Festlegungen.....</b>                                       | <b>10</b> |
| 5.1 Datenschutz und Sicherheit.....                                            | 10        |
| 5.2 Integrating the Healthcare Enterprise IHE.....                             | 10        |
| 5.3 Vertrauenswürdige Ausführungsumgebung.....                                 | 10        |
| 5.3.1 Verarbeitungskontext.....                                                | 11        |
| 5.3.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld..... | 12        |
| 5.4 Logging.....                                                               | 13        |
| <b>6 Funktionsmerkmale.....</b>                                                | <b>14</b> |
| 6.1 Allgemein.....                                                             | 14        |
| 6.1.1 Aktensession.....                                                        | 14        |
| 6.1.2 Lokalisierung von ePA-Aktensystemen.....                                 | 14        |
| 6.1.3 Kommunikation mit Komponente Autorisierung.....                          | 15        |
| 6.1.4 Kommunikation mit Komponente Dokumentenverwaltung.....                   | 16        |
| 6.2 Implementation ePA-Anwendungsfälle.....                                    | 19        |
| 6.2.1 Login Aktensession.....                                                  | 19        |
| 6.2.2 Logout Aktensession.....                                                 | 25        |
| 6.2.3 Dokumente einstellen.....                                                | 27        |
| 6.3 Realisierung der Leistungen der TI-Plattform.....                          | 30        |
| 6.4 Clientschnittstelle.....                                                   | 31        |
| 6.4.1 Operationsdefinition Logout.....                                         | 31        |
| 6.4.2 Operationsdefinition PutDocuments.....                                   | 32        |
| <b>7 Informationsmodell.....</b>                                               | <b>36</b> |

|                                                                    |           |
|--------------------------------------------------------------------|-----------|
| <b>8 Verteilungssicht.....</b>                                     | <b>37</b> |
| <b>9 Anhang A - Verzeichnisse.....</b>                             | <b>38</b> |
| 9.1 Abkürzungen.....                                               | 38        |
| 9.2 Glossar.....                                                   | 38        |
| 9.3 Abbildungsverzeichnis.....                                     | 38        |
| 9.4 Tabellenverzeichnis.....                                       | 39        |
| 9.5 Referenzierte Dokumente.....                                   | 39        |
| 9.5.1 Dokumente der gematik.....                                   | 39        |
| 9.5.2 Weitere Dokumente.....                                       | 40        |
| <b>10 Anhang B - Übersicht über die verwendeten Versionen.....</b> | <b>42</b> |

---

## **1 Einordnung des Dokumentes**

---

### **1.1 Zielsetzung**

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb der Komponente "Fachmodul ePA im KTR-Consumer" als Teil des Produkttyps KTR-Consumer.

### **1.2 Zielgruppe**

Das Dokument richtet sich an Hersteller des Produktes des Produkttyps KTR-Consumer sowie an Hersteller und Anbieter der weiteren Produkttypen der Fachanwendung ePA.

### **1.3 Geltungsbereich**

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte oder Produkttypsteckbrief) festgelegt 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 der Komponente bereitgestellten (angebotenen) Schnittstellen. Die durch die Komponente benutzten Schnittstellen werden in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch "9.5-Referenzierte Dokumente").

Die vollständige Anforderungslage für die Komponente ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten. Diese sind in dem Produkttypsteckbrief des Produkttyps KTR-Consumer 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

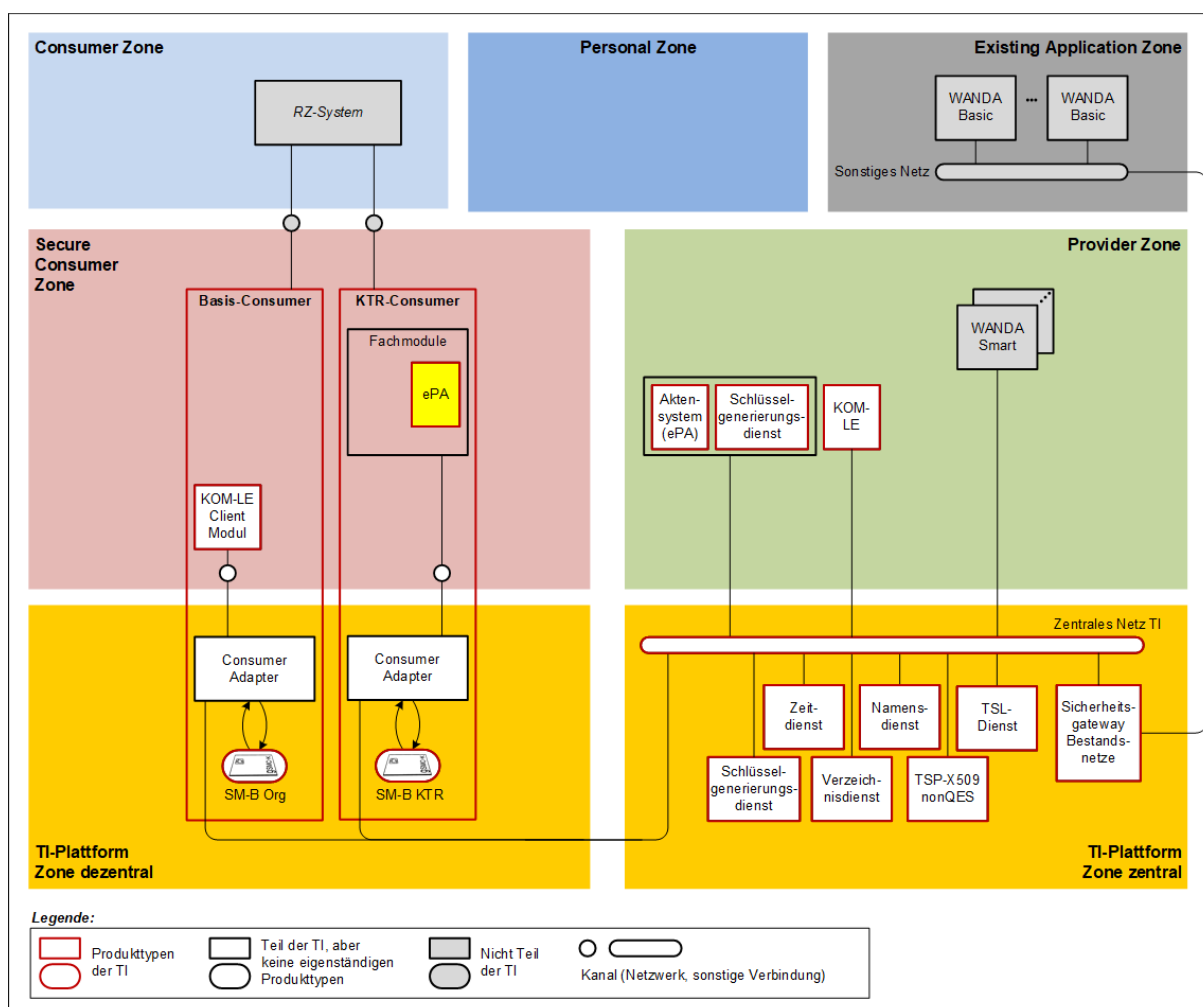
[<=]

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

## 2 Systemüberblick

Der KTR-Consumer ermöglicht es Kostenträgern, ihren Versicherten Dokumente in den ePA-Aktensystemen bereitzustellen.

Das Fachmodul ePA im KTR-Consumer (FM ePA KTR) ist eine Komponente innerhalb des KTR-Consumers, welche die dezentrale Fachlogik der Fachanwendung ePA kapselt. Das FM ePA KTR ist kein eigenständiger Produkttyp.



**Abbildung 1: Systemüberblick Fachmodul ePA im KTR-Consumer**

---

## 3 Systemkontext

---

### 3.1 Akteure und Rollen

Im Systemkontext des FM ePA KTR interagieren verschiedene Akteure (aktive Komponenten) in unterschiedlichen Rollen mit dem FM ePA KTR.

**Tabelle 1: TAB\_FM\_ePA\_KTR\_001 - Akteure und Rollen**

| Akteur | Rolle        | Beschreibung                                                                                     |
|--------|--------------|--------------------------------------------------------------------------------------------------|
| Nutzer | Kostenträger | Primärer Anwender, Ausführen von fachlichen Anwendungsfällen mit Zugriff auf ein ePA-Aktensystem |
| Nutzer | gematik Test | Nutzer im Rahmen des Zulassungstest der gematik                                                  |

Der KTR-Consumer kann mandantenbasiert betrieben werden, d.h. in einem KTR-Consumer Produkt können mehrere Kostenträger als Nutzer auftreten.

### 3.2 Nachbarsysteme

Das FM ePA KTR als Komponente des KTR-Consumers nutzt Schnittstellen der folgenden Produkttypen der TI:

- ePA-Aktensystem mit den Komponenten
  - Autorisierung
  - Dokumentenverwaltung
- Schlüsselgenerierungsdienst

Der KTR-Consumer ist über einen SZZP an das zentrale Netz der TI angebunden. Die Dienste der zentralen TI, wie bspw. Namensdienst und TSP X.509 nonQES, werden über Dienste des KTR-Consumers genutzt, die dem Consumer Adapter gemäß [gemKPT\_Arch\_TIP#4.6 Rechenzentrums-Consumer] entsprechen.

Die von Kostenträgern in die Aktenkonten einzustellenden Dokumente werden über Backend-Systeme der Kostenträger bereitgestellt. Den Kostenträgern ist freigestellt eine individuelle Anbindung der bestehenden Backend-Systeme an das FM ePA KTR zu realisieren.

Um den Test der Schnittstellen im Rahmen der Zulassung durch die gematik zu ermöglichen, wird eine leichtgewichtige Schnittstelle zum Ausführen der Anwendungsfälle spezifiziert. Diese kann aber muss nicht durch die Backend-Systeme der Kostenträger genutzt werden.



---

## **4 Zerlegung des Produkttyps**

---

Um eine datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten Daten innerhalb des FM ePA KTR zu ermöglichen, muss das FM ePA KTR eine Vertrauenswürdige Ausführungsumgebung (VAU) realisieren. Siehe "5.3-  
Vertrauenswürdige Ausführungsumgebung"

Hinweis: Die VAU im FM ePA KTR unterscheidet sich in ihren Anforderungen von der VAU in der Komponente Dokumentenverwaltung des ePA-Aktensystems.

Eine weitere Untergliederung des FM ePA KTR in Komponenten ist nicht erforderlich.

---

## 5 Übergreifende Festlegungen

---

### 5.1 Datenschutz und Sicherheit

Die Anforderungen, die sich aus den Themenfeldern Datenschutz und Sicherheit ergeben, beziehen sich auf die Vertrauenswürdigen Ausführungsumgebung (VAU) und sind in "5.3... Vertrauenswürdige Ausführungsumgebung" beschrieben.

### 5.2 Integrating the Healthcare Enterprise IHE

Die Schnittstellen des ePA-Aktensystems und die Verarbeitungslogik des Fachmoduls basieren auf Transaktionen des IHE ITI Technical Frameworks [IHE ITI TF]. Die IHE ITI-Implementierungsstrategie ist in [gemSpec\_DM\_ePA] beschrieben.

Das Fachmodul nutzt die folgenden Integrationsprofile des IHE ITI TF:

- Cross-Enterprise Document Sharing (XDS.b)
- Cross-Enterprise User Assertion (XUA) Profile

Die folgende Tabelle bietet einen Überblick über die durch das FM ePA KTR umzusetzenden IHE ITI-Akteure und assoziierte Transaktionen. Siehe auch [gemSpec\_DM\_ePA#Abbildung Überblick über IHE ITI-Akteure und assoziierte Transaktionen].

**Tabelle 2: TAB\_FM\_ePA\_KTR\_002 - IHE Akteure und Transaktionen**

| Aktion                    | Profil<br>e | IHE-Akteur      | Transaktion                                | Referenz            |
|---------------------------|-------------|-----------------|--------------------------------------------|---------------------|
| Einstellen von Dokumenten | XDS.b       | Document Source | Provide & Register Document Set-b [ITI-41] | [IHE-ITI-TF2b]#3.41 |
| Authentisierung           | XUA         | X-Service User  |                                            | [IHE-ITI-TF]        |

Die übergreifenden Einschränkungen von IHE ITI-Transaktionen sowie Festlegungen spezieller Umsetzungsvorgaben bzgl. einzelner Transaktionen sind in [gemSpec\_DM\_ePA] und [gemSpec\_Dokumentenverwaltung] beschrieben.

Wenn in der IHE Interface-Beschreibung der Begriff „Patient“ verwendet wird, ist im Rahmen der vorliegenden Spezifikation darunter der Versicherte (Aktenkontoinhaber) zu verstehen.

### 5.3 Vertrauenswürdige Ausführungsumgebung

In diesem Abschnitt werden die Anforderungen an das FM ePA KTR zur Umsetzung einer Vertrauenswürdigen Ausführungsumgebung (VAU) gestellt. Die VAU dient der datenschutzrechtlich zulässigen und sicheren Verarbeitung von schützenswerten

Klartextdaten (Aktenschlüssel und Kontextschlüssel des Aktenkontos eines Versicherten) innerhalb des FM ePA KTR. Die VAU stellt dazu aktenindividuelle Verarbeitungskontexte (d.h. Instanzen der VAU) bereit, in denen die Verarbeitung sensibler Daten im Klartext erfolgen kann. Diese Verarbeitungskontexte sind entsprechend zu schützen.

**A\_17280 - FM ePA KTR-Consumer: Umsetzung der Aktensession in einer Vertrauenswürdigen Ausführungsumgebung (VAU)**

Das Fachmodul ePA im KTR-Consumer MUSS die Verarbeitung der Operationen der Schnittstellen `I_Document_Management_Connect`, `I_Document_Management_Insurance` und `I_Authorization` im Verarbeitungskontext einer Vertrauenswürdigen Ausführungsumgebung (VAU) umsetzen.【<=】

**A\_20652 - FM ePA KTR-Consumer: Festlegung zu nutzender SMC-KTR**

Das Fachmodul ePA im KTR-Consumer MUSS ausschließlich eine SMC-KTR verwenden, deren Zertifikate die Admission `oid_epa_ktr` ausweisen.【<=】

**A\_20653 - FM ePA KTR-Consumer: Exklusive Nutzung der SMC-KTR**

Das Fachmodul ePA im KTR-Consumer MUSS sicherstellen, dass eine SMC-KTR mit Zertifikaten, die die Admission `oid_epa_ktr` ausweisen, ausschließlich durch das Fachmodul ePA im KTR-Consumer verwendet wird.【<=】

### **5.3.1 Verarbeitungskontext**

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

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

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

Die schützenswerten sensiblen Daten sind der Akten- und Kontextschlüssel der Aktenkonten, für die der KTR zugriffsberechtigt ist.

**A\_17346 - FM ePA KTR-Consumer: Verarbeitungskontext der VAU**

Der Verarbeitungskontext des Fachmoduls ePA im KTR-Consumer MUSS sämtliche physikalischen Systemkomponenten sowie sämtliche Softwarekomponenten umfassen, deren Sicherheitseigenschaften sich auf den Schutz des Akten- und Kontextschlüssel eines Versicherten vor Zugriff durch Unbefugte bei ihrer Verarbeitung im Klartext auswirken können.

【<=】

**A\_17347 - FM ePA KTR-Consumer: Verarbeitungskontext der VAU - Keine persistente Speicherung von Akten- und Kontextschlüssel**

Der Verarbeitungskontext des Fachmoduls ePA im KTR-Consumer DARF den Akten- und Kontextschlüssel eines Versicherten NICHT persistent speichern, auch nicht verschlüsselt.【<=】

**A\_17348 - FM ePA KTR-Consumer: Verarbeitungskontext der VAU - Akten- und Kontextschlüssel verlassen VAU nie**

Der Verarbeitungskontext des Fachmoduls ePA im KTR-Consumer MUSS sicherstellen, dass die Akten- und Kontextschlüssel der Versicherten die VAU nur verlassen (unabhängig davon, ob sie verschlüsselt oder unverschlüsselt sind), wenn sie ans ePA-Aktensystem übermittelt werden und die Übermittlung zum ePA-Aktensystem in einem sicheren Kanal erfolgt.

[<=]

Daher müssen die durch das FM ePA KTR genutzten Plattformleistungen, welche sensible Daten verarbeiten (PL\_TUC\_SYMM\_ENCIPHER, PL\_TUC\_SYMM\_DECIPHER), innerhalb der VAU realisiert werden.

**5.3.2 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld**

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

**A\_17350 - FM ePA KTR-Consumer: Isolation der VAU von Datenverarbeitungsprozessen des Anbieters**

Die VAU des Fachmoduls ePA im KTR-Consumer MUSS die im Verarbeitungskontext ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters trennen und damit gewährleisten, dass der Anbieter KTR-Consumer vom Zugriff auf die in der VAU verarbeiteten, schützenswerten Daten ausgeschlossen ist.[<=]

**A\_17351 - FM ePA KTR-Consumer: Ausschluss von Manipulationen an der Software der VAU**

Die VAU des Fachmoduls ePA im KTR-Consumer MUSS die Integrität der eingesetzten Software schützen und damit insbesondere Manipulationen an der Software durch den Anbieter KTR-Consumer ausschließen.[<=]

**A\_17352 - FM ePA KTR-Consumer: Ausschluss von Manipulationen an der Hardware der VAU**

Die VAU des Fachmoduls ePA im KTR-Consumer MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter KTR-Consumer ausschließen.[<=]

**A\_17353 - FM ePA KTR-Consumer: Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU**

Die VAU des Fachmoduls ePA im KTR-Consumer MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter KTR-Consumer mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann.[<=]

**A\_17354 - FM ePA KTR-Consumer: Kein physischer Zugang des Anbieters zu Systemen der VAU**

Die VAU des Fachmoduls ePA im KTR-Consumer MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter KTR-Consumer, während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.[<=]

Die durch den Kostenträger einzustellenden Dokumente gelten im Sinne der ePA als personenbezogene medizinische Daten.

**A\_17355 - FM ePA KTR-Consumer: Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU**

Die VAU des Fachmoduls ePA im KTR-Consumer MUSS mit technischen Mitteln sicherstellen, dass ein physischer Zugang zu Hardware-Komponenten der Verarbeitungskontexte nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten extrahiert werden können.[<=]

**A\_17356 - FM ePA KTR-Consumer: Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes**

Die VAU des Fachmoduls ePA im KTR-Consumer MUSS beim Beenden eines Verarbeitungskontextes sämtliche Daten dieses Verarbeitungskontextes sicher löschen.  
[<=]

## **5.4 Logging**

Das FM ePA KTR soll Logdateien schreiben, die eine Analyse technischer Vorgänge erlauben. Diese Logdateien sind dafür vorgesehen, aufgetretene Fehler zu identifizieren, die Performance zu analysieren und interne Abläufe zu beobachten.

Es gelten die dem Produkttypen KTR-Consumer aus [gemSpec\_OM] zugewiesenen Anforderungen.

**A\_22499 - FM ePA KTR-Consumer: Verbot des Logging von medizinischen und personenbezogenen Daten**

Das Fachmodul ePA KTR DARF medizinische und personenbezogene Daten NICHT loggen.  
[<=]

**A\_22519-01 - FM ePA KTR-Consumer - Löschfrist von Protokolldaten**

Das Fachmodul ePA KTR MUSS Protokolldaten nach spätestens 30 Tagen löschen.[<=]

---

## 6 Funktionsmerkmale

---

### 6.1 Allgemein

#### 6.1.1 Aktensession

Eine Aktensession in einem FM ePA KTR bezeichnet die Sitzung im FM ePA KTR, in der fachliche Anwendungsfälle mit dem Aktenkonto eines Versicherten ausgeführt werden. Sollen bspw. Dokumente in die Aktenkonten verschiedener Versicherter eingestellt werden, dann wird zu jedem Aktenkonto eine separate Aktensession aufgebaut.

Ein Aktenkonto wird eindeutig durch eine Akten-ID (RecordIdentifier, siehe [\[gemSpec\\_DM\\_ePA#RecordIdentifier\]](#)) referenziert. Sie wird aus der Versicherten-ID und der homeCommunityID gebildet.

Eine Aktensession im FM ePA KTR beginnt mit dem Login und endet mit dem Logout. Während einer Aktensession können mehrere fachliche Anwendungsfälle ausgeführt werden (bspw. mehrere Dokumentensets einstellen). Das Logout erfolgt explizit nach Abarbeitung aller fachlichen Anwendungsfälle, mittels eines Time-outs nach Inaktivität oder nach einem Fehler beim Login.

##### **A\_17245 - FM ePA KTR-Consumer: Login nach Notwendigkeit**

Das Fachmodul ePA im KTR-Consumer MUSS den Anwendungsfall "Login Aktensession" vor der Ausführung einer fachlichen Operation starten, wenn im Rahmen der internen Aktensession-Verwaltung kein Verarbeitungskontext mit gültigen Session-Daten vorhanden ist. [ $\leq$ ]

##### **A\_17246 - FM ePA KTR-Consumer: Beenden der Aktensession**

Das Fachmodul ePA im KTR-Consumer MUSS zum Beenden der Aktensession den Anwendungsfall "Logout Aktensession" ausführen. [ $\leq$ ]

##### **A\_17247-01 - FM ePA KTR-Consumer: Beenden nach Inaktivität**

Das Fachmodul ePA im KTR-Consumer MUSS spätestens nach 5 Minuten ohne Zugriff auf das Aktenkonto die Aktensession beenden. [ $\leq$ ]

##### **A\_17999 - FM ePA KTR-Consumer: informationstechnische Trennung von Aktensessions**

Das Fachmodul ePA im KTR-Consumer MUSS die Abarbeitung von Anwendungsfällen, welche verschiedenen Aktensessions zugeordnet werden, informationstechnisch trennen. [ $\leq$ ]

D.h. eine gegenseitige Beeinflussung von Aktensessions durch verborgene Kanäle muss verhindert werden. Direkte Informations- und Kontrollflüsse zwischen verschiedenen Aktensessions dürfen nicht auftreten.

#### 6.1.2 Lokalisierung von ePA-Aktensystemen

Vor dem Zugriff auf eine Akte muss der passende Anbieter inklusive der URL des Aktendienstes und der Endpunkte über den Namensdienst der zentralen TI abgefragt werden.

Das ePA-Aktensystem wird durch die HomeCommunityID identifiziert, welche Bestandteil des RecordIdentifier (siehe [\[gemSpec\\_DM\\_ePA#RecordIdentifier\]](#)) ist.

### **A\_17248 - FM ePA KTR-Consumer: Lokalisierung Komponenten des ePA-Aktensystem**

Das Fachmodul ePA im KTR-Consumer MUSS die zur Kommunikation mit den Komponenten

- Autorisierung,
- Schlüsselgenerierungsdienst Typ1,
- Schlüsselgenerierungsdienst Typ 2 und
- Dokumentenverwaltung

eines ePA-Aktensystems notwendigen Lokalisierungsinformationen per DNS-Abfrage nach den in [gemSpec\_Aktensystem#Tab\_ePA\_Service Discovery] und [gemSpec\_Aktensystem#Tab\_ePA\_FQDN] dargestellten Parametern ermitteln und die URL gemäß [\[gemSpec\\_Aktensystem#A-17969 - Anbieter ePA-Aktensystem - Schnittstellenadressierung\]](#) bilden. [≤]

Das FM ePA KTR kann die Lokalisierungsinformationen unabhängig von der Nutzung seiner Schnittstellen abrufen, zwischenspeichern und wiederverwenden, d.h. die Abfrage muss nicht vor jedem Aufruf einer Schnittstelle erfolgen.

### **6.1.3 Kommunikation mit Komponente Autorisierung**

Im KTR-Consumer baut das FM ePA KTR eine TLS-Verbindung ohne Clientauthentisierung und mit Rollenprüfung zur Komponente Autorisierung auf.

#### **A\_17249 - FM ePA KTR-Consumer: Autorisierung - TLS-Verbindung nutzen**

Das Fachmodul ePA im KTR-Consumer MUSS für die Kommunikation mit der Komponente Autorisierung eine TLS-Verbindung verwenden. [≤]

#### **A\_17281 - FM ePA KTR-Consumer: Autorisierung - Aufbau TLS-Verbindung**

Das Fachmodul ePA im KTR-Consumer MUSS den Aufbau der TLS-Verbindung zur Komponente Autorisierung gemäß der zugewiesenen Anforderungen aus [\[gemSpec\\_Krypt#TLS-Verbindungen\]](#) und [\[gemSpec\\_PKI#TLS-Verbindungsaufbau\]](#) umsetzen.

Das Fachmodul ePA im KTR-Consumer MUSS für den Aufbau der TLS-Verbindung zur Komponente Autorisierung die lokalisierte Adresse verwenden und mittels PL\_TUC\_NET\_NAME\_RESOLUTION auflösen.

Das Fachmodul ePA im KTR-Consumer MUSS für den Aufbau der TLS-Verbindung zur Komponente Autorisierung das vom Zielsystem bereitgestellte Serverzertifikat C.FD.TLS-S auf Gültigkeit gemäß [\[gemSpec\\_PKI#GS-A\\_4663\]](#) mit folgenden Parametern prüfen:

**Tabelle 3 : TAB\_FM\_ePA\_KTR\_003 - TLS-Verbindung - Parameter Zertifikatsprüfung**

|                  |                  |
|------------------|------------------|
| PolicyList       | oid_fd_tls_s     |
| KeyUsage         | digitalSignature |
| ExtendedKeyUsage | id-kp-serverAuth |
| OCSP-Graceperiod | NULL             |
| Offline-Modus    | Nein             |

Das Fachmodul ePA im KTR-Consumer MUSS für den Aufbau der TLS-Verbindung zur Komponente Autorisierung prüfen, ob der Rollenbezeichner oid\_epa\_authz (gemäß

[gemSpec\_OID#GS-A\_4446-\*) in den Rollen-IDs des Zertifikates enthalten ist.  
Das Fachmodul ePA im KTR-Consumer MUSS für den Aufbau der TLS-Verbindung zur Komponente Autorisierung abbrechen, wenn eine der obige Prüfungen mit einem Fehler beendet werden.

[<=]

Hinweis: Der gemäß [\[gemSpec\\_PKI#GS-A\\_4663\]](#) zu nutzende Prüfalgorithmus (TUC\_PKI\_018) liefert als einen der Rückgabewerte die im zu prüfenden Zertifikat enthaltenen Rollen-IDs.

#### **A\_17357 - FM ePA KTR-Consumer: Autorisierung - TLS-Verbindung in VAU terminieren**

Das Fachmodul ePA im KTR-Consumer MUSS den verschlüsselten Benachrichtigungskanal zur Komponente Autorisierung aus der VAU des Fachmoduls ePA im KTR-Consumers initiieren, d.h., die TLS-Verbindung terminiert innerhalb der VAU.

[<=]

### **6.1.4 Kommunikation mit Komponente Dokumentenverwaltung**

Im KTR-Consumer baut das FM ePA KTR eine TLS-Verbindung ohne Clientauthentisierung und mit Rollenprüfung zur Komponente Dokumentenverwaltung auf.

#### **A\_17282-01 - FM ePA KTR-Consumer: Dokumentenverwaltung - TLS-Verbindung nutzen**

Das Fachmodul ePA im KTR-Consumer MUSS für die Kommunikation mit der Komponente Dokumentenverwaltung für jede Aktensession eine zu dieser Aktensession gehörende TLS-Session aufbauen bzw. eine für die Aktensession bestehende TLS-Session nutzen.

[<=]

#### **A\_20626 - FM ePA KTR-Consumer: Dokumentenverwaltung - TLS Session Resumption mittels Session-ID nutzen**

Das Fachmodul ePA im KTR-Consumer MUSS für die Verbindung zwischen Fachmodul und Komponente ePA-Dokumentenverwaltung TLS Session Resumption mittels Session-ID gemäß RFC 5246 nutzen, um für den wiederholten Aufbau von TLS-Verbindungen die bereits ausgehandelten Session-Parameter zu nutzen.[<=]

#### **A\_17283 - FM ePA KTR-Consumer: Dokumentenverwaltung - Aufbau TLS-Verbindung**

Das Fachmodul ePA im KTR-Consumer MUSS den Aufbau der TLS-Verbindung zur Komponente Dokumentenverwaltung gemäß der zugewiesenen Anforderungen aus [\[gemSpec\\_Krypt#TLS-Verbindungen\]](#) und [\[gemSpec\\_PKI#TLS-Verbindungsaufbau\]](#) umsetzen.

Das Fachmodul ePA im KTR-Consumer MUSS für den Aufbau der TLS-Verbindung zur Komponente Dokumentenverwaltung die lokalisierte Adresse verwenden und mittels PL\_TUC\_NET\_NAME\_RESOLUTION auflösen.

Das Fachmodul ePA im KTR-Consumer MUSS für den Aufbau der TLS-Verbindung zur Komponente Dokumentenverwaltung das vom Zielsystem bereitgestellten Serverzertifikat C.FD.TLS-S auf Gültigkeit gemäß [\[gemSpec\\_PKI#GS-A\\_4663\]](#) mit folgenden Parametern prüfen:

**Tabelle 4: TAB\_FM\_ePA\_KTR\_004 - TLS-Verbindung - Parameter Zertifikatsprüfung**

|                  |                  |
|------------------|------------------|
| PolicyList       | oid_fd_tls_s     |
| KeyUsage         | digitalSignature |
| ExtendedKeyUsage | id-kp-serverAuth |



|                  |      |
|------------------|------|
| OCSP-Graceperiod | NULL |
| Offline-Modus    | Nein |

Das Fachmodul ePA im KTR-Consumer MUSS für den Aufbau der TLS-Verbindung zur Komponente Dokumentenverwaltung prüfen, ob der Rollenbezeichner `oid_epa_dvw` (gemäß [\[gemSpec\\_OID#GS-A\\_4446-\\*\)](#)) in den Rollen-IDs des Zertifikates enthalten ist. Das Fachmodul ePA im KTR-Consumer MUSS für den Aufbau der TLS-Verbindung zur Komponente Autorisierung abbrechen, wenn eine der obige Prüfungen mit einem Fehler beendet werden.

[<=]

#### **A\_17358 - FM ePA KTR-Consumer: Dokumentenverwaltung - TLS-Verbindung in VAU terminieren**

Das Fachmodul ePA im KTR-Consumer MUSS den verschlüsselten Benachrichtigungskanal zur Komponente Dokumentenverwaltung aus der VAU des Fachmoduls ePA im KTR-Consumers initiieren, d.h., die TLS-Verbindung terminiert innerhalb der VAU.

[<=]

#### **Aufbau eines sicheren Kanals auf HTTP-Anwendungsschicht zum Verarbeitungskontext der VAU**

Die Kommunikation zum Aktenkonto in der Dokumentenverwaltung wird zusätzlich zu TLS über einen sicheren Kanal zwischen der VAU im FM ePA KTR und der VAU des Aktenkontos in der Dokumentenverwaltung gesichert. Die Dokumentenverwaltung bietet dem FM ePA KTR die folgenden Operationen ausschließlich über einen sicheren Kanal an:

- `I_Document_Management_Insurance::ProvideAndRegisterDocumentSet-b`
- `I_Document_Management_Connect::OpenContext`
- `I_Document_Management_Connect::CloseContext`

Für Informationen zum Kommunikationsprotokoll zwischen FM ePA KTR und einer VAU in der Dokumentenverwaltung siehe [\[gemSpec\\_Krypt#3.15 ePA-spezifische Vorgaben\]](#) und [\[gemSpec\\_Krypt#6 Kommunikationsprotokoll zwischen VAU und ePA-Clients\]](#).

#### **A\_17385 - FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Nutzung sicherer Kanal**

Der Verarbeitungskontext der VAU des Fachmoduls ePA im KTR-Consumer MUSS mit dem Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung des ePA-Aktensystems einen Sitzungsschlüssel gemäß [\[gemSpec\\_Krypt#3.15.1 - Verbindung zur VAU\]](#) und [\[gemSpec\\_Krypt#6 - Kommunikationsprotokoll zwischen VAU und ePA-Clients\]](#) aushandeln und diesen für die Ver- und Entschlüsselung aller ausgetauschten Nachrichten verwenden.

[<=]

#### **A\_17284 - FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Erweiterung des sicheren Verbindungsprotokolls**

Das Fachmodul ePA im KTR-Consumer MUSS beim Aufbau des sicheren Kanals zum Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung des ePA-Aktensystems die `AuthorizationAssertion` aus den Session-Daten als Parameter gemäß [\[gemSpec\\_Dokumentenverwaltung#A\\_15592-\\*\)](#) übergeben.[<=]

#### **A\_17782-01 - FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Serverzertifikat prüfen**

Das Fachmodul ePA im KTR-Consumer MUSS beim Aufbau des sicheren Kanals zum Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung des ePA-Aktensystems eine Zertifikats- und Rollenprüfung für das vom Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung empfangene Zertifikat `C.FD.AUT` prüfen.

**Tabelle 5: TAB\_FM\_ePA\_KTR\_021 - VAU Dokumentenverwaltung -  
PL\_TUC\_PKI\_VERIFY\_CERTIFICATE**

|                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Plattformbaustein<br/>PL_TUC_PKI_VERIFY_CERTIFICATE<br/>nutzen</p> | <p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• Zu prüfendes Zertifikat:<br/>Verschlüsselungszertifikat (C.FD.AUT)</li> <li>• Referenzzeitpunkt: aktueller Zeitpunkt</li> <li>• PolicyList: oid_fd_aut</li> <li>• vorgesehene KeyUsage: digitalSignature</li> <li>• Offline-Modus: Nein</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• Ergebnis Gültigkeit und Statusprüfung</li> <li>• im Zertifikat enthaltene Rollen-OIDs</li> </ul> <p>Die im Zertifikat enthaltenen Rollen<br/>müssen oid_epa_vau beinhalten.</p> <p>Wenn das Zertifikat in der Prüfung abgelehnt<br/>wurde, der Sperrstatus nicht ermittelt werden<br/>konnte oder die Rollenprüfung nicht erfolgreich<br/>war, dann ist das Zertifikat abzulehnen und der<br/>Verbindungsaufbau abubrechen.</p> |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[<=]

#### **A\_17250 - FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Umsetzung sicherer Kanal**

Das Fachmodul ePA im KTR-Consumer MUSS den im Rahmen des sicheren  
Verbindungsaufbaus mit der Verarbeitungskontext der Komponente ePA-  
Dokumentenverwaltung des ePA-Aktensystems ausgehandelten Sitzungsschlüssel  
verwenden, um den HTTP Body aller über den sicheren Kanal zu sendenden Requests an  
die Dokumentenverwaltung zu verschlüsseln und alle über den sicheren Kanal  
gesendeten Responses von der Dokumentenverwaltung zu entschlüsseln.[<=]

#### **A\_17285 - FM ePA KTR-Consumer: VAU Dokumentenverwaltung - Fehler beim Verbindungsaufbau**

Das Fachmodul ePA im KTR-Consumer MUSS, falls beim Aufbau der sicheren Verbindung  
zum Verarbeitungskontext der VAU in der Dokumentenverwaltung ein Fehler auftritt, die  
Operation abbrechen.[<=]

## **6.2 Implementation ePA-Anwendungsfälle**

### **6.2.1 Login Aktensession**

Mit dem Anwendungsfall „Login Aktensession“ wird die Aktensession zu dem Aktenkonto  
eines Versicherten im FM ePA KTR gestartet.

Für das Login werden die Zertifikate der Institutionskarte des Kostenträgers (SMC-KTR)  
verwendet. Nach erfolgreicher Authentisierung und Autorisierung wird das  
empfängerverschlüsselte Schlüsselmaterial heruntergeladen und das Öffnen des

Aktenkontextes in der Komponente Dokumentenverwaltung für das referenzierte Aktenkonto durchgeführt.

### **A\_17251 - FM ePA KTR-Consumer: Login Aktensession**

Das Fachmodul ePA im KTR-Consumer MUSS den Anwendungsfall „UC 1.6 - Login durch einen Kostenträger“ aus [gemSysL\_Fachanwendung\_ePA] gemäß TAB\_FM\_ePA\_KTR\_005 umsetzen.

**Tabelle 6: TAB\_FM\_ePA\_KTR\_005 - Login Aktensession**

|                |                                                                                                                                                                                                                   |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name           | Login Aktensession                                                                                                                                                                                                |
| Auslöser       | <ul style="list-style-type: none"><li>• Es soll ein fachlicher Anwendungsfall mit Zugriff auf das Aktenkonto durchgeführt werden und es besteht noch keine Aktensession.</li></ul>                                |
| Vorbedingung   | Der Versicherte hat seine Einwilligung gegeben.<br>Der RecordIdentifier des Versicherten ist bekannt.<br>Die Zertifikate der SMC-KTR des zugehörigen Kostenträgers sind verfügbar.                                |
| Nachbedingung  | Für die Session liegen gültige Session-Daten im FM ePA KTR vor.                                                                                                                                                   |
| Standardablauf | Aktivitäten im Standardablauf<br><ol style="list-style-type: none"><li>1. Authentisierung KTR mittels des Zertifikates der SMC-KTR</li><li>2. Autorisierung des KTR</li><li>3. Öffnen des Aktenkontexts</li></ol> |
| Varianten      | Im Fehlerfall wird der Anwendungsfall abgebrochen und der Anwendungsfall „Logout Aktensession“ gestartet.                                                                                                         |

[<=]

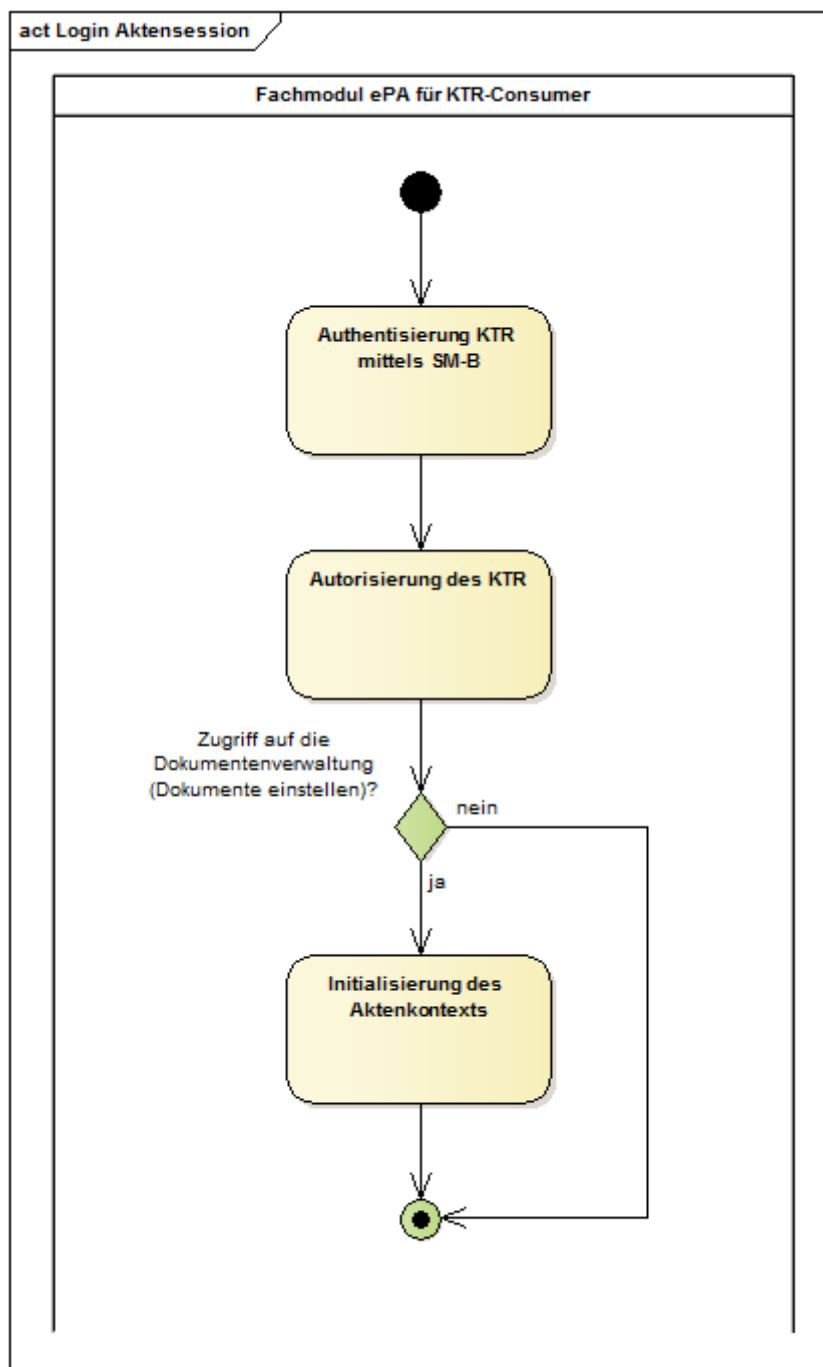


Abbildung 2: Login Aktensession

### Authentisierung KTR mittels Zertifikaten der SMC-KTR

Die Authentisierung KTR mit den Zertifikaten der ausgewählten SMC-KTR erfolgt durch das FM ePA KTR. Hierzu erzeugt das FM ePA KTR ein SAML-Token gemäß, welches dem IHE-Profil "XUA" [IHE-ITI-TF] genügt und als AuthenticationAssertion bezeichnet wird. Das Token wird mit der Identität der für den KTR ausgewählten SMC-KTR signiert.

### A\_17252 - FM ePA KTR-Consumer: Login - Authentisierung KTR mittels SMC-KTR - Auswahl SMC-KTR

Das Fachmodul ePA im KTR-Consumer MUSS für die Authentisierung im ePA-Aktensystem die Identitäten einer SMC-KTR des Kostenträgers benutzen, bei der der Inhaber des Aktenkontos, auf das zugegriffen werden soll, versichert ist. [≤]

#### **A\_17253 - FM ePA KTR-Consumer: Login - Authentisierung KTR mittels SMC-KTR - SAML-Token erstellen**

Das Fachmodul ePA im KTR-Consumer MUSS für die Authentisierung als Authentifizierungsbestätigung eine SAML2-Assertion gemäß dem IHE-Profil "XUA" [IHE-ITI-TF] und [gemSpec\_TBAuth#TAB\_TBAuth\_03] erstellen und dabei folgende Vorgaben beachten:

- das *Issuer* Element muss als Aussteller des Token den Wert "urn:epa:telematik:KTRConsumer" enthalten
- die eingebettete Signatur *ds:Signature* wird mit dem C.HCI.OSIG Zertifikat der ausgewählten SMC-KTR unter Verwendung von PL\_TUC\_SIGN\_HASH\_nonQES erstellt. Die Signatur enthält im *ds:KeyInfo* Element das verwendete Signaturzertifikat.
- das Element *saml2:Subject/saml2:NameID* muss auf Basis des C.HCI.OSIG Zertifikats gebildet werden
- das Attribut *saml2:Subject/saml2:SubjectConfirmation/@Method* muss auf den Wert "urn:oasis:names:tc:SAML:2.0:cm:bearer" gesetzt werden
- das Attribut *saml2:Conditions/@NotBefore* muss auf die Systemzeit gesetzt werden
- das Attribut *saml2:Conditions/@NotOnOrAfter* muss auf (Systemzeit+24 Stunden) gesetzt werden
- das Element *saml2:Conditions/saml2:AudienceRestriction/saml2:Audience* muss auf die FQDN des Anbieters des Aktensystems gesetzt werden
- das Element *saml2:AuthnStatement/saml2:AuthnContext/saml2:AuthnContextClassRef* muss auf den Wert "urn:oasis:names:tc:SAML:2.0:ac:classes:X509" gesetzt werden

[≤]

#### **A\_17254 - FM ePA KTR-Consumer: Login - Authentisierung KTR mittels SMC-KTR - Behauptung im SAML-Token**

Das Fachmodul ePA im KTR-Consumer MUSS die für die Authentisierung als Authentifizierungsbestätigung erstellte SAML2-Assertion im Element *AttributeStatement* mit den Behauptungen gemäß [gemSpec\_TBAuth#TAB\_TBAuth\_02\_1] befüllen und dabei folgende Vorgaben beachten:

- die Behauptungen müssen auf Basis des C.HCI.OSIG Zertifikats gebildet werden
- die in der Tabelle angegebenen Behauptungen müssen enthalten sein, sofern sie aus dem zugrundeliegenden Zertifikat entnommen werden können
- die Behauptung "urn:gematik:subject:organization-id" muss enthalten sein und basierend auf der RegistrationNumber (Telematik-ID) gebildet werden. Das Attribut *Attribute/@NameFormat* muss dabei den Wert "urn:oasis:names:tc:SAML:2.0:attrname-format:uri" haben.

[≤]

Die SAML2-Assertion gemäß A\_17253 wird als *AuthenticationAssertion* in die Session-Daten übernommen.

#### **A\_17255 - FM ePA KTR-Consumer: Löschen der AuthenticationAssertion**

Das Fachmodul ePA im KTR-Consumer MUSS die *AuthenticationAssertion* zur Authentisierung einer KTR spätestens nach Ablauf ihrer Gültigkeitsdauer löschen. [≤]

## **Autorisierung des KTR**

Die Komponente Autorisierung des lokalisierten ePA-Aktensystems prüft, ob im Rahmen der Aktensession der Zugriff auf die mit dem RecordIdentifier referenzierte Akte erlaubt ist. Dazu schickt das FM ePA KTR die im Rahmen der Authentisierung (s.o.) ausgestellte AuthenticationAssertion an die Komponente Autorisierung und erhält nach erfolgreicher Prüfung Akten- und Kontextschlüssel sowie eine Autorisierungsbestätigung (AuthorizationAssertion) zur Kommunikation mit der Dokumentenverwaltung ausgehändigt.

### **A\_17286 - FM ePA KTR-Consumer: Login - Autorisierung - Schlüsselmaterial laden**

Das Fachmodul ePA im KTR-Consumer MUSS im Anwendungsfall "Login Aktensession" das Schlüsselmaterial des Aktenkontos gemäß TAB\_FM\_ePA\_KTR\_006 laden.

**Tabelle 7: TAB\_FM\_ePA\_KTR\_006 - Operation getAuthorizationKey**

|                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I_Authorization::getAuthorizationKey<br>Request erstellen    | Eingangsparameter: <ul style="list-style-type: none"> <li>• AuthenticationAssertion aus Session-Daten</li> <li>• RecordIdentifier aus Session-Daten</li> </ul>                                                                                                                                                                                                                                                                    |
| I_Authorization::getAuthorizationKey<br>Response verarbeiten | Rückgabedaten: <ul style="list-style-type: none"> <li>• AuthorizationKey</li> <li>• AuthorizationAssertion</li> </ul> Der Response beinhaltet im AuthorizationKey ein verschlüsseltes Schlüsselpaar sowie eine AuthorizationAssertion passend zur Telematik-ID.<br>Liefert der Response einen Fehler oder beinhaltet der Response keinen AuthorizationKey oder keine AuthorizationAssertion, wird der Anwendungsfall abgebrochen. |

**[<=]**

Der AuthorizationKey beinhaltet im Element phrs:AuthorizationKey/phrs:EncryptedKeyContainer ein Chifftrat mit dem verschlüsselten Akten- und Kontextschlüssels sowie AssociatedData.

Die Datenstruktur für EncryptedKeyContainer und die Klartextpräsentation für Akten- und Kontextschlüssel ist in [\[gemSpec\\_SGD\\_ePA#8 - Interoperables Austauschformat\]](#) beschrieben.

Die Klartextpräsentation von Akten- und Kontextschlüssel im AuthoritationKey ist doppelt symmetrisch verschlüsselt. Die symmetrischen Schlüssel zur Ver- und Entschlüsselung von Akten- und Kontextschlüssel werden über die Schlüsselableitungsfunktion der Schlüsselgenerierungsdienste Typ 1 und 2 ermittelt. Die Funktionsweise der Schlüsselgenerierung wird in [gemSpec\_SGD\_ePA] beschrieben.

### **A\_17838 - FM ePA KTR-Consumer: Autorisierung - Symmetrische Schlüssel für Akten- und Kontextschlüssel ermitteln**

Das Fachmodul ePA im KTR-Consumer MUSS zur Schlüsselableitung den in [\[gemSpec\\_SGD\\_ePA#2.3 Basisablauf Kommunikation SGD-Client und SGD\]](#) festgelegten Ablauf in der Rolle Client durchführen. [**<=**]

**A\_18185 - FM ePA KTR-Consumer: Prüfung TI-Zertifikate (SGD-Zertifikate)**

Das Fachmodul ePA im KTR-Consumer MUSS X.509-Zertifikate eines Schlüsselgenerierungsdienstes der TI gemäß PL\_TUC\_PKI\_VERIFY\_CERTIFICATE prüfen.

**Tabelle 8: TAB\_FM\_ePA\_KTR\_026 - Schlüsselgenerierungsdienst - PL\_TUC\_PKI\_VERIFY\_CERTIFICATE**

|                                      |                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PL_TUC_PKI_VERIFY_CERTIFICATE nutzen | <p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• zu prüfendes Zertifikat: vom SGD übermitteltes Zertifikat</li> <li>• checkUnspecifiedEECertificate: true</li> <li>• Referenzzeitpunkt: aktuelle Systemzeit</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• Gültigkeit zu Referenzzeitpunkt</li> <li>• Rolle des Zertifikates</li> </ul> |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[**<=**]

Zur Optimierung der Performance muss das FM ePA KTR die Schlüsselableitung für SGD 1 (Basisablauf Schritt 1) und SGD 2 (Basisablauf Schritt 3) und das Erzeugen eines ephemeren ECDH-Schlüsselpaars (Basisablauf Schritt 5) parallel ausführen. Der Request an SGD 1 und SGD 2 in Basisablauf Schritt 7 können ebenfalls parallelisiert werden. Für die bei einer Schlüsselableitung für eine Entschlüsselung im Request für KeyDerivation zu übermittelnden Informationen ist keine Unterscheidung des Anwendungsfalls in SGD notwendig. Es werden sowohl für SGD 1 als auch SGD 2 die Informationen aus dem Element phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:AssociatedData verwendet: KeyDerivation <Teilstring aus AssociatedData für den entsprechenden SGD>

**A\_17996 - FM ePA KTR-Consumer: Autorisierung - Aufrufe zur Schlüsselableitung parallelisieren**

Das Fachmodul ePA im KTR-Consumer MUSS die Schlüsselableitung mit SGD 1 und SGD 2 sowie das Erzeugen des ephemeren ECDH-Schlüsselpaars parallelisieren. [**<=**]

Als Ergebnis bei einer erfolgreichen Schlüsselableitung zum Entschlüsseln erhält das FM ePA KTR von jedem der beiden SGD eine Antwortnachricht für KeyDerivation im Format: "OK-KeyDerivation "+Key+" "+s.

Key ist der für die Entschlüsselung zu verwendende symmetrische Schlüssel für den entsprechenden SGD.

Für das Entschlüsseln gelten die Vorgaben aus [\[gemSpec\\_SGD\\_ePA#8 Interoperables Austauschformat\]](#) sowie [\[gemSpec\\_Krypt#A\\_17872 - Ver- und Entschlüsselung der Akten und Kontextschlüssel \(Schlüsselableitungsfunktionalität ePA\)\]](#).

**A\_17997 - FM ePA KTR-Consumer: Autorisierung - Akten- und Kontextschlüssel entschlüsseln**

Das Fachmodul ePA im KTR-Consumer MUSS beim Entschlüsseln des Akten- und Kontextschlüssel die bei der Schlüsselableitung mit SGD 1 und SGD 2 erhaltenen symmetrischen Schlüssel gemäß [gemSpec\_SGD\_ePA] und [gemSpec\_Krypt] nutzen.

**Tabelle 9: TAB\_FM\_ePA\_KTR\_021 - Akten- und Kontextschlüssel entschlüsseln**

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plattformbaustein PL_TUC_SYMM_DE CIPHER nutzen | <p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• Doc<sub>enc</sub>: EncryptedKeyContainer\Ciphertext aus AuthorizationKey</li> <li>• Cert: aus SGD2 abgeleiteter symmetrischer Schlüssel</li> <li>• AD: SGD2 Anteil aus EncryptedKeyContainer\AssociatedData aus AuthorizationKey</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• Doc: Doc<sub>enc</sub>1 = einfach symmetrisch verschlüsselter Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht)</li> </ul> |
| Plattformbaustein PL_TUC_SYMM_DE CIPHER nutzen | <p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• Doc<sub>enc</sub>: EncryptedKeyContainer\Ciphertext aus Doc<sub>enc</sub>1</li> <li>• Cert: aus SGD1 abgeleiteter symmetrischer Schlüssel</li> <li>• AD: EncryptedKeyContainer\AssociatedData aus Doc<sub>enc</sub>1</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• Doc: Klartextpräsentation von Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel)</li> </ul>                               |

[<=]

Die AuthorizationAssertion, der Aktenschlüssel und Kontextschlüssel werden in die Session-Daten übernommen.

### Öffnen des Aktenkontextes

Für den Verbindungsaufbau zur Dokumentenverwaltung und zur VAU Dokumentenverwaltung siehe "[6.1.4- Kommunikation mit Komponente Dokumentenverwaltung](#)".

### A\_17318 - FM ePA KTR-Consumer: Login - Aktenkontext öffnen - Operation OpenContext

Das Fachmodul ePA im KTR-Consumer MUSS im Anwendungsfall "Login Aktensession" das Übersenden des Kontextschlüssels gemäß TAB\_FM\_ePA\_KTR\_008 umsetzen.

**Tabelle 10: TAB\_FM\_ePA\_KTR\_008 - Operation OpenContext**

|                                            |                                                                                          |
|--------------------------------------------|------------------------------------------------------------------------------------------|
| Vorbedingung                               | AuthorizationAssertion und entschlüsselter Kontextschlüssel liegen in Session-Daten vor. |
| I_Document_Management_Connect::OpenContext | Eingangsdaten:                                                                           |



|                                                                       |                                                                                                   |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Request erstellen                                                     | <ul style="list-style-type: none"> <li>Kontextschlüssel (ContextKey) aus Session-Daten</li> </ul> |
| I_Document_Management_Connect : : OpenContext<br>Response verarbeiten | Rückgabedaten: <ul style="list-style-type: none"> <li>OK oder gematik-Fehler</li> </ul>           |

[<=]

## 6.2.2 Logout Aktensession

Der Anwendungsfall „Logout Aktensession“ beendet eine Session zu einem Aktenkonto.

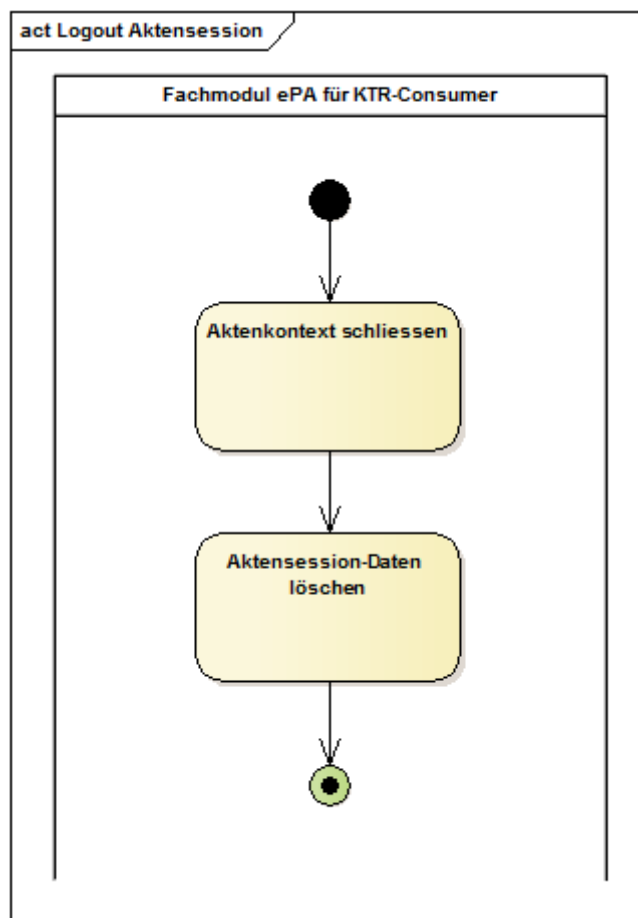
### A\_17256 - FM ePA KTR-Consumer: Logout Aktensession

Das Fachmodul ePA im KTR-Consumer MUSS den Anwendungsfall "UC 1.3 - Logout durch einen Nutzer" aus [gemSysL\_Fachanwendung\_ePA] gemäß TAB\_FM\_ePA\_KTR\_009 umsetzen.

**Tabelle 11 : TAB\_FM\_ePA\_KTR\_009 - Logout Aktensession**

|                |                                                                                                                                                                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name           | Logout Aktensession                                                                                                                                                                                                                                                                           |
| Auslöser       | <ul style="list-style-type: none"> <li>Operation der Schnittstelle zum Backendsystem des KTR</li> <li>Operation der Schnittstelle zu gematik Test</li> <li>auf die Aktensession wurde länger als 5 Minuten nicht zugegriffen (Inaktivität)</li> <li>Fehler im Anwendungsfall Login</li> </ul> |
| Vorbedingung   | Es besteht eine Aktensession.                                                                                                                                                                                                                                                                 |
| Nachbedingung  | Die Session-Daten sind gelöscht.                                                                                                                                                                                                                                                              |
| Standardablauf | Aktivitäten im Standardablauf <ol style="list-style-type: none"> <li>Aktenkontext schliessen</li> <li>Session-Daten löschen</li> </ol>                                                                                                                                                        |

[<=]



**Abbildung 3: Logout Aktensession**

**A\_17257 - FM ePA KTR-Consumer: Logout - Aktenkontext schliessen**

Das Fachmodul ePA im KTR-Consumer MUSS im Anwendungsfall „Logout Aktensession“, wenn ein sicherer Kanal zur Dokumentenverwaltung aufgebaut und der Aktenkontext erfolgreich geöffnet wurde, die Aktivität „Aktenkontext schliessen“ gemäß TAB\_FM\_ePA\_KTR\_010 umsetzen.

**Tabelle 12: TAB\_FM\_ePA\_KTR\_010 - Logout - Aktenkontext schliessen**

| Vorbedingung                                                        | AuthorizationAssertion in Session-Daten |
|---------------------------------------------------------------------|-----------------------------------------|
| I_Document_Management_Connect::CloseContext<br>Request erstellen    |                                         |
| I_Document_Management_Connect::CloseContext<br>Response verarbeiten | HTTP OK oder gematik-Fehlermeldung      |

[<=]

**A\_17258 - FM ePA KTR-Consumer: Logout - Session-Daten löschen**

Das Fachmodul ePA im KTR-Consumer MUSS zum Abschluss des Anwendungsfall „Logout Aktensession“ alle Session-Daten aus dem lokalen Speicher löschen.[<=]

Die Session-Daten sind in "7- Informationsmodell" beschrieben.

### 6.2.3 Dokumente einstellen

Mit diesem Anwendungsfall können Dokumente in das Aktenkonto eines Versicherten geladen werden.

Das ePA-Aktensystem unterstützt nur Dokumente mit bestimmten MIME Types. Die initial zulässigen Typen sind in [gemSpec\_DM\_ePA#A\_14760-\*]

beschrieben. Die Dokumentenverwaltung prüft den Dateitypen anhand der Metadaten beim Hochladen der Dokumente und antwortet mit einem Fehler, wenn der Dateityp nicht unterstützt wird.

Das ePA-Aktensystem lehnt beim Einstellen von Dokumenten Requests mit dem Fehler MaxDocSizeExceeded ab, wenn die Größe eines Einzeldokumentes 25 MB überschreitet. Das ePA-Aktensystem lehnt beim Einstellen von Dokumenten Requests mit dem Fehler MaxPkgSizeExceeded ab, wenn die Summe der Größe der Dokumente in einem Submission Set 250 MB überschreitet. (siehe [\[gemSpec\\_Dokumentenverwaltung#A\\_17441\]](#)) Das FM ePA KTR kann das Einstellen der Dokumente über mehrere Transaktionen verteilen, um die Größenbeschränkung beim Submission Set zu umgehen.

#### **A\_17259 - FM ePA KTR-Consumer: Dokumente einstellen**

Das Fachmodul ePA im KTR-Consumer MUSS den Anwendungsfall "UC 4.11 - Dokumente durch einen Kostenträger einstellen" aus [gemSysL\_Fachanwendung\_ePA] gemäß TAB\_FM\_ePA\_KTR\_011 umsetzen.

**Tabelle 13 : TAB\_FM\_ePA\_KTR\_011 - Dokumente einstellen**

|                |                                                                                                                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name           | Dokumente einstellen                                                                                                                                                                                                                                                                   |
| Auslöser       | <ul style="list-style-type: none"> <li>• Operation der Schnittstelle zum Backendsystem des KTR</li> <li>• Operation der Schnittstelle zu gematik Test</li> </ul>                                                                                                                       |
| Vorbedingung   | Es besteht eine Aktensession mit gültigen Session-Daten. Die hochzuladenden Dokumente sind im lokal eingebundenen Speicher verfügbar.                                                                                                                                                  |
| Nachbedingung  | Die Dokumente sind im ePA Aktenkonto für alle Berechtigten verfügbar.                                                                                                                                                                                                                  |
| Standardablauf | Aktivitäten im Standardablauf <ol style="list-style-type: none"> <li>1. für jedes Dokument <ol style="list-style-type: none"> <li>a. Dokument verschlüsseln</li> <li>b. Dokumentenschlüssel löschen</li> </ol> </li> <li>2. Dokumentenset in Dokumentenverwaltung hochladen</li> </ol> |

[<=]

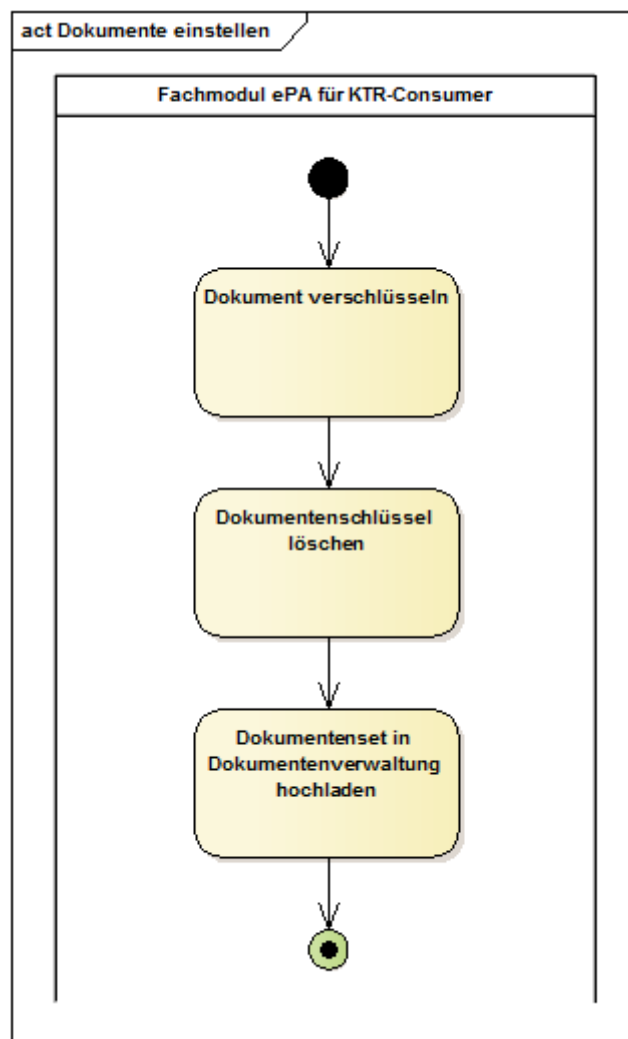


Abbildung 4: Dokumente einstellen

#### **A\_17261-03 - FM ePA KTR-Consumer: Dokumente einstellen - Metadaten**

Das Fachmodul ePA im KTR-Consumer MUSS im Anwendungsfall „Dokumente einstellen“ für jedes einzustellende Dokument Metadaten bereitstellen. Für die XDS-Metadaten von Dokumenten gelten die Nutzungsvorgaben aus [gemSpec\_DM\_ePA#A\_14760-\*] . Für das Element DocumentEntry wird confidentialityCode auf den Wert "N" (für "normal") gesetzt.

Für die Elemente Document Entry und Submission Set wird das Attribut authorRole mit "105" belegt.

Für die Elemente Document Entry und Submission Set wird das Attribut authorInstitution mit Werten aus dem zur Authentisierung genutzten Zertifikat belegt.

[<=]

#### **A\_17323 - FM ePA KTR-Consumer: Dokumente einstellen - Upload verschlüsselter Dokumente**

Das Fachmodul ePA im KTR-Consumer MUSS sicherstellen, dass Dokumente, welche in das ePA-Aktensystem eingestellt werden, verschlüsselt sind.[<=]

Zum Verschlüsseln des Dokuments wird dieses mit einem Dokumentenschlüssel symmetrisch verschlüsselt. Der Dokumentenschlüssel wird dann symmetrisch mit dem Aktenschlüssel verschlüsselt. Für Vorgaben zum Verschlüsseln eines Dokuments für das ePA-Aktensystem siehe [\[gemSpec\\_DM\\_ePA#2.4.1 Verschlüsselung\]](#).

#### **A\_17262 - FM ePA KTR-Consumer: Dokumente einstellen - Dokument verschlüsseln**

Das Fachmodul ePA im KTR-Consumer MUSS im Anwendungsfall „Dokumente einstellen“ für jedes zu übermittelnde Dokument die Aktivität "Dokument verschlüsseln" gemäß TAB\_FM\_ePA\_KTR\_012 umsetzen.

**Tabelle 14: TAB\_FM\_ePA\_KTR\_012 - Dokumente einstellen - Dokument verschlüsseln**

|                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plattformbaustein PL_TUC_SYMM_ENCIPHER für Dokument nutzen            | <p>Dokument mit PL_TUC_SYMM_ENCIPHER verschlüsseln</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• Dokument</li> <li>• Die optionalen Parameter Cert und AD werden nicht verwendet.</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• verschlüsseltes Dokument</li> <li>• Dokumentenschlüssel</li> </ul> <p>Der Dokumentenschlüssel wird in der Aktivität erzeugt und an den Aufrufer zurückgegeben</p> |
| Plattformbaustein PL_TUC_SYMM_ENCIPHER für Dokumentenschlüssel nutzen | <p>Dokumentenschlüssel mit PL_TUC_SYMM_ENCIPHER verschlüsseln</p> <p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• Dokument: Dokumentenschlüssel</li> <li>• Aktenschlüssel aus Session-Daten</li> <li>• Der optionale Parameter AD wird nicht verwendet.</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>• verschlüsselter Dokumentenschlüssel</li> </ul>                                                    |

**[<=]**

Die Dokumentenschlüssel dürfen nicht persistent gespeichert werden und müssen nach ihrer Verwendung gelöscht werden.

#### **A\_17263 - FM ePA KTR-Consumer: Dokumente einstellen - Dokumentenschlüssel löschen**

Das Fachmodul ePA im KTR-Consumer MUSS im Anwendungsfall „Dokumente einstellen“ in der Aktivität "Dokument verschlüsseln" erstellte Dokumentenschlüssel nach dem Ende der Aktivität löschen.**[<=]**

Auf Basis der verschlüsselten Dokumente und der Metadaten wird eine Provide And Register Document Set-b Message für die einzustellende Dokumente erstellt.

#### **A\_17264 - FM ePA KTR-Consumer: Dokumente einstellen - Dokumentenset in Dokumentenverwaltung hochladen**

Das Fachmodul ePA im KTR-Consumer MUSS im Anwendungsfall "Dokumente einstellen" das Hochladen der Dokumente gemäß TAB\_FM\_ePA\_KTR\_013 umsetzen.

**Tabelle 15: TAB\_FM\_ePA\_KTR\_013 - Dokumente einstellen - Dokumentenset in Dokumentenverwaltung hochladen**

|                                                                                                  |                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I_Document_Management_Insurance:<br>:<br>ProvideAndRegisterDocumentSet-b<br>Request erstellen    | Eingangsparameter:<br><ul style="list-style-type: none"><li>• Provide And Register Document Set-b Message gemäß IHE XDS-Transaktion [ITI-41]</li><li>• AuthenticationAssertion aus Session-Daten</li></ul> |
| I_Document_Management_Insurance:<br>:<br>ProvideAndRegisterDocumentSet-b<br>Response verarbeiten | Rückgabedaten:<br><ul style="list-style-type: none"><li>• Provide And Register Document Set-b Response Message gemäß IHE XDS-Transaktion [ITI-41]</li></ul>                                                |

[<=]

#### **A\_17265 - FM ePA KTR-Consumer: IHE XDS-Transaktion [ITI-41]**

Das Fachmodul ePA im KTR-Consumer MUSS für die Nutzung der Operation I\_Document\_Management\_Insurance::ProvideAndRegisterDocumentSet-b gemäß der in [IHE-ITI-TF] definierten IHE XDS-Transaktion [ITI-41] "Provide & Register Document Set-b" als Akteur "Document Source" umsetzen.[<=]

#### **A\_17266 - FM ePA KTR-Consumer: IHE XDS-Transaktion [ITI-41] - Unterstützung MTOM/XOP**

Das Fachmodul ePA im KTR-Consumer MUSS bei der Umsetzung der IHE XDS-Transaktion [ITI-41] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] gemäß [IHE-ITI-TF2x#V.3.6.] verwenden.[<=]

## **6.3 Realisierung der Leistungen der TI-Plattform**

Der Produkttyp KTR-Consumer realisiert die vom FM ePA KTR benötigten Leistungen der TI-Plattform, die in den fachlichen Anwendungsfällen der ePA genutzt werden. Die durch die TI-Plattform bereitgestellten Leistungen umfassen einen für die Fachanwendungen einheitlichen Zugriff auf Smartcards, Leistungen der PKI der Telematikinfrastruktur, Zugriff auf die zentralen Dienste der TI-Plattform etc., die in übergreifenden Spezifikationen der gematik festgelegt sind. Die Definition der Leistungen der TI-Plattform im KTR-Consumer befindet sich in [gemSpec\_Systemprozesse\_dezTI].

Die Plattformleistungen für kryptographische Operationen müssen innerhalb der VAU realisiert werden, da sensible Daten verarbeitet werden.

Das FM ePA KTR verwendet die in der Tabelle TAB\_FM\_ePA\_KTR\_019 dargestellten Plattformleistungen.

**Tabelle 16 : TAB\_FM\_ePA\_KTR\_019 - Verwendete Plattformleistungen**

| <b>Kürzel</b>              | <b>Bezeichnung</b>             |
|----------------------------|--------------------------------|
| PL_TUC_NET_NAME_RESOLUTION | Auflösen von URI in IP-Adresse |

|                               |                                   |
|-------------------------------|-----------------------------------|
| PL_TUC_PKI_VERIFY_CERTIFICATE | Prüfung eines Zertifikates der TI |
| PL_TUC_SIGN_HASH_nonQES       | mit TI-Identität nonQES signieren |
| PL_TUC_SYMM_DECIPHER          | Symmetrisch entschlüsseln         |
| PL_TUC_SYMM_ENCIPHER          | Symmetrisch verschlüsseln         |

## 6.4 Clientschnittstelle

Für die Möglichkeit eines Tests der Funktionalitäten durch die gematik im Rahmen des Zulassungstests wird eine technische Schnittstelle spezifiziert, über welche die Ausführung der Anwendungsfälle getriggert werden kann.

### **A\_17955 - FM ePA KTR-Consumer: ePA-Dienst**

Das Fachmodul ePA im KTR-Consumer MUSS Clientsystemen einen ePA-Dienst anbieten.

**Tabelle 17 : TAB\_FM\_ePA\_KTR\_022 - ePA-Dienst**

| Name              | EPAService                       |                                                |
|-------------------|----------------------------------|------------------------------------------------|
| Version           | Siehe Anhang B                   |                                                |
| Namensraum        | Siehe Anhang B                   |                                                |
| Namensraum-Kürzel | EPA für Schema und EPAW für WSDL |                                                |
| Operation         | Name                             | Kurzbeschreibung                               |
|                   | Logout                           | triggert Anwendungsfall "Logout Aktenkonto"    |
|                   | PutDocuments                     | triggert Anwendungsfall "Dokumente einstellen" |
| WSDL              | EPAService.wsdl                  |                                                |
| Schema            | EPAService.xsd                   |                                                |

[<=]

### 6.4.1 Operationsdefinition Logout

#### **A\_17960 - FM ePA KTR-Consumer: Operation Logout**

Das Fachmodul ePA im KTR-Consumer MUSS die Operation Logout gemäß folgender Signatur implementieren:

**Tabelle 18 : TAB\_FM\_ePA\_KTR\_024 - Definition Logout**

| Operation | Logout |
|-----------|--------|
|-----------|--------|

|                                                                                 |                                                                                |                                            |             |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------|--------------------------------------------|-------------|
| <b>Beschreibung</b>                                                             | Mit dieser Operation wird der Anwendungsfall "Logout Aktensession" getriggert. |                                            |             |
| <b>Formatvorgaben</b>                                                           | Die Definition der Ein- und Ausgabeparameter erfolgt in [EPAService.xsd].      |                                            |             |
| <b>Eingangsparameter</b>                                                        |                                                                                |                                            |             |
| <b>Name</b>                                                                     | <b>Beschreibung</b>                                                            | <b>Typ</b>                                 | <b>opt.</b> |
| insurantId                                                                      | 10-stelliger, unveränderlicher Anteil der KVN = VersichertenID                 | String                                     | -           |
| <b>Fehlermeldungen</b>                                                          |                                                                                |                                            |             |
| <b>Name</b>                                                                     | <b>Fehlertext</b>                                                              | <b>Details</b>                             |             |
| INTERNAL_ERROR                                                                  | Zufallszahl                                                                    | Interner Fehler in der Verarbeitungslogik. |             |
| Fehlermeldungen des ePA-Aktensystems werden an das Clientsystem weitergeleitet. |                                                                                |                                            |             |

[<=]

Die folgenden Anforderungen beschreiben die Umsetzung der Operation Logout.

#### A\_17961 - FM ePA KTR-Consumer: Operation Logout - Anwendungsfall starten

Das Fachmodul ePA im KTR-Consumer MUSS in der Operation Logout den Anwendungsfall "Logout Aktensession" für die der VersichertenID zugeordneten Aktensession durchführen.[<=]

### 6.4.2 Operationsdefinition PutDocuments

#### A\_17962 - FM ePA KTR-Consumer: Operation PutDocuments

Das Fachmodul ePA im KTR-Consumer MUSS die Operation PutDocuments gemäß folgender Signatur implementieren:

**Tabelle 19 : TAB\_FM\_ePA\_KTR\_025 - Definition PutDocuments**

|                   |                                                                                 |        |      |
|-------------------|---------------------------------------------------------------------------------|--------|------|
| Operation         | PutDocuments                                                                    |        |      |
| Beschreibung      | Mit dieser Operation wird der Anwendungsfall "Dokumente einstellen" getriggert. |        |      |
| Formatvorgaben    | Die Definition der Ein- und Ausgabeparameter erfolgt in [EPAService.xsd].       |        |      |
| Eingangsparameter |                                                                                 |        |      |
| Name              | Beschreibung                                                                    | Typ    | opt. |
| insurantId        | 10-stelliger, unveränderlicher Anteil                                           | String | nein |



|                        |                                                                                        |                                            |      |
|------------------------|----------------------------------------------------------------------------------------|--------------------------------------------|------|
|                        | der KVNR = VersichertenID                                                              |                                            |      |
| HomeCommunityId        | HomeCommunityId des Aktensystems                                                       | String                                     | nein |
| Kostentraegerkennung   | Institutionskennzeichen des Kostenträgers                                              | Integer                                    | nein |
| SubmissionSet          |                                                                                        |                                            |      |
| title                  | Titel des Submission Sets                                                              | String                                     | ja   |
| contentTypeCode        | Klinische Aktivität, die zum Einstellen des Submission Set geführt hat.                |                                            | ja   |
| Document               |                                                                                        |                                            |      |
| Data                   | in das Aktenkonto einzustellendes Dokument                                             | base64                                     | nein |
| formatCode             | Global eindeutiger Code für das Dokumentenformat.                                      | String                                     | nein |
| languageCode           | Sprache, in der das Dokument abgefasst ist.                                            | String                                     | nein |
| mimeType               | MIME-Type des Dokuments                                                                | String                                     | nein |
| serviceStartTime       | Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis begonnen wurde. | String                                     | ja   |
| serviceStopTime        | Zeitpunkt, an dem das im Dokument dokumentierte (Behandlungs-)Ereignis beendet wurde.  | String                                     | ja   |
| title                  | Titel des Dokumentes                                                                   | String                                     | ja   |
| typeCode               | Art des Dokuments                                                                      | String                                     | nein |
| <b>Fehlermeldungen</b> |                                                                                        |                                            |      |
| <b>Name</b>            | <b>Fehlertext</b>                                                                      | <b>Details</b>                             |      |
| TECHNICAL_ERROR        |                                                                                        | Interner Fehler in der Verarbeitungslogik. |      |

|                                                                                 |                             |                                                      |
|---------------------------------------------------------------------------------|-----------------------------|------------------------------------------------------|
| SYNTAX_ERROR                                                                    | Fehlerhafte Aufrufparameter | Es wurde ein fehlerhafter Aufrufparameter übergeben. |
| Fehlermeldungen des ePA-Aktensystems werden an das Clientsystem weitergeleitet. |                             |                                                      |

[<=]

#### **A\_17963 - FM ePA KTR-Consumer: Operation PutDocuments - Anwendungsfall starten**

Das Fachmodul ePA im KTR-Consumer MUSS in der Operation PutDocuments den Anwendungsfall "Dokumente einstellen" für die der VersichertenID zugeordneten Aktensession durchführen.[<=]

#### **A\_17958 - FM ePA KTR-Consumer: Operation PutDocuments- RecordIdentifier bilden**

Das Fachmodul ePA im KTR-Consumer MUSS in der Operation PutDocuments den RecordIdentifier mit insurantID und HomeCommunityID bilden.[<=]

#### **A\_17959 - FM ePA KTR-Consumer: Operation PutDocuments - SMC-KTR auswählen**

Das Fachmodul ePA im KTR-Consumer MUSS in der Operation PutDocuments die für die Aktensession zu verwendende SMC-KTR auf Basis der Kostenträgerkennung auswählen.

[<=]

Die VersichertenID dient der Identifikation der Aktensession.

#### **A\_17970 - FM ePA KTR-Consumer: Operation PutDocuments - Metadaten SubmissionSet**

Das Fachmodul ePA im KTR-Consumer MUSS in der Operation PutDocuments die Eingangsparameter zum SubmissionSet (title, contentTypeCode) für die SubmissionSet Metadaten verwenden.[<=]

#### **A\_17971 - FM ePA KTR-Consumer: Operation PutDocuments - Document**

Das Fachmodul ePA im KTR-Consumer MUSS in der Operation PutDocuments zu jedem Document den Eingangsparameter Data als in das Aktenkonto einzustellende Dokument verwenden.[<=]

#### **A\_17972 - FM ePA KTR-Consumer: Operation PutDocuments - Metadaten Document Entry**

Das Fachmodul ePA im KTR-Consumer MUSS in der Operation PutDocuments die Eingangsparameter zu jedem Document (formatCode, languageCode, mimeType, serviceStartTime, serviceStopTime, title, typeCode) für die Document Entry Metadaten verwenden.[<=]

#### **A\_20554 - FM ePA KTR-Consumer: Operation PutDocuments - Konformität der Metadaten**

Das Fachmodul ePA im KTR-Consumer MUSS die Metadaten, die es als Eingangsparameter der Operation PutDocuments zu jedem Document erhalten hat, konform zu den Vorgaben in [gemSpec\_DM\_ePA] und [ITI-41] (in [IHE-ITI-TF2b]) als Eingangsparameter des Anwendungsfalles "Dokument einstellen" setzen.[<=]

Alle nicht durch das Interface übergebenen Metadaten werden durch das FM ePA KTR gesetzt. Optionale Parameter können, wenn sie nicht durch den Operationaufruf mit Werten belegt werden, beliebig gemäß den Richtlinien befüllt werden.

## 7 Informationsmodell

Session-Daten

**Tabelle 20 : TAB\_FM\_ePA\_KTR\_020 - Session-Daten**

| Datenfeld                                          | Herkunft                                                                                | Beschreibung                                                                                                                                                                   |
|----------------------------------------------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telematik-ID                                       | Konfiguration                                                                           | Identität eines Kostenträgers in den Zertifikaten seiner SMC-KTR                                                                                                               |
| Akten-ID<br>(RecordIdentifier)                     | Konfiguration                                                                           | Kennung der Akte des Versicherten beim jeweiligen Anbieter ePA-Aktensystem im Format von RecordIdentifier gemäß [gemSpec_DM_ePA#2.2]<br>Die HomeCommunityID muss bekannt sein. |
| Authentisierungstoken<br>(AuthenticationAssertion) | Authentisierung mittels SMC-KTR                                                         | Authentifizierungsbestätigung als Voraussetzung für die Autorisierung                                                                                                          |
| Autorisierungstoken<br>(AuthorizationAssertion)    | Komponente Autorisierung des ePA-Aktensystems<br>(I_Authorization::getAuthorizationKey) | Autorisierungsbestätigung                                                                                                                                                      |
| Aktenschlüssel<br>(RecordKey)                      | Komponente Autorisierung des ePA-Aktensystems<br>(I_Authorization::getAuthorizationKey) | entschlüsselter Aktenschlüssel                                                                                                                                                 |
| Kontextschlüssel<br>(ContextKey)                   | Komponente Autorisierung des ePA-Aktensystems<br>(I_Authorization::getAuthorizationKey) | entschlüsselter Kontextschlüssel                                                                                                                                               |

---

## **8 Verteilungssicht**

---

Eine Darstellung der hardwareseitigen Verteilung des Produkttyps bzw. seiner Teilsysteme und der Einbettung in die physikalische Umgebung wird nicht benötigt.

---

## 9 Anhang A - Verzeichnisse

---

### 9.1 Abkürzungen

| Kürzel     | Erläuterung                                            |
|------------|--------------------------------------------------------|
| ePA        | Anwendung elektronische Patientenakte                  |
| FM ePA KTR | Fachmodul ePA im KTR-Consumer                          |
| KTR        | Kostenträger                                           |
| MTOM       | Message Transmission Optimization Mechanism            |
| SGD        | Schlüsselgenerierungsdienst                            |
| SMC-KTR    | Sicherheitsmodul für eine Institution der Kostenträger |
| VAU        | Vertrauenswürdige Ausführungsumgebung                  |

### 9.2 Glossar

| Begriff          | Erläuterung                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Funktionsmerkmal | Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems. |
| Versicherten-ID  | Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen Krankenversicherungsnummer (KVNR).                                                |

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

### 9.3 Abbildungsverzeichnis

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Abbildung 1: Systemüberblick Fachmodul ePA im KTR-Consumer..... | 7  |
| Abbildung 2: Login Aktensession.....                            | 20 |
| Abbildung 3: Logout Aktensession.....                           | 26 |
| Abbildung 4: Dokumente einstellen.....                          | 28 |

## 9.4 Tabellenverzeichnis

|                                                                                                                 |    |
|-----------------------------------------------------------------------------------------------------------------|----|
| Tabelle 1: TAB_FM_ePA_KTR_001 - Akteure und Rollen.....                                                         | 8  |
| Tabelle 2: TAB_FM_ePA_KTR_002 - IHE Akteure und Transaktionen.....                                              | 10 |
| Tabelle 3 : TAB_FM_ePA_KTR_003 - TLS-Verbindung - Parameter Zertifikatsprüfung.....                             | 15 |
| Tabelle 4: TAB_FM_ePA_KTR_004 - TLS-Verbindung - Parameter Zertifikatsprüfung.....                              | 17 |
| Tabelle 5: TAB_FM_ePA_KTR_021 - VAU Dokumentenverwaltung -<br>PL_TUC_PKI_VERIFY_CERTIFICATE.....                | 18 |
| Tabelle 6: TAB_FM_ePA_KTR_005 - Login Aktensession.....                                                         | 19 |
| Tabelle 7: TAB_FM_ePA_KTR_006 - Operation getAuthorizationKey.....                                              | 22 |
| Tabelle 8: TAB_FM_ePA_KTR_026 - Schlüsselgenerierungsdienst -<br>PL_TUC_PKI_VERIFY_CERTIFICATE.....             | 23 |
| Tabelle 9: TAB_FM_ePA_KTR_021 - Akten- und Kontextschlüssel entschlüsseln.....                                  | 24 |
| Tabelle 10: TAB_FM_ePA_KTR_008 - Operation OpenContext.....                                                     | 25 |
| Tabelle 11 : TAB_FM_ePA_KTR_009 - Logout Aktensession.....                                                      | 25 |
| Tabelle 12: TAB_FM_ePA_KTR_010 - Logout - Aktenkontext schliessen.....                                          | 26 |
| Tabelle 13 : TAB_FM_ePA_KTR_011 - Dokumente einstellen.....                                                     | 27 |
| Tabelle 14: TAB_FM_ePA_KTR_012 - Dokumente einstellen - Dokument verschlüsseln.....                             | 29 |
| Tabelle 15: TAB_FM_ePA_KTR_013 - Dokumente einstellen - Dokumentenset in<br>Dokumentenverwaltung hochladen..... | 30 |
| Tabelle 16 : TAB_FM_ePA_KTR_019 - Verwendete Plattformleistungen.....                                           | 30 |
| Tabelle 17 : TAB_FM_ePA_KTR_022 - ePA-Dienst.....                                                               | 31 |
| Tabelle 18 : TAB_FM_ePA_KTR_024 - Definition Logout.....                                                        | 32 |
| Tabelle 19 : TAB_FM_ePA_KTR_025 - Definition PutDocuments.....                                                  | 32 |
| Tabelle 20 : TAB_FM_ePA_KTR_020 - Session-Daten.....                                                            | 36 |

## 9.5 Referenzierte Dokumente

### 9.5.1 Dokumente der gematik

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

| [Quelle] | Herausgeber: Titel |
|----------|--------------------|
|----------|--------------------|

|                                |                                                                                                             |
|--------------------------------|-------------------------------------------------------------------------------------------------------------|
| [gemGlossar]                   | gematik: Einführung der Gesundheitskarte - Glossar                                                          |
| [gemKPT_Arch_TIP]              | gematik: Konzept Architektur der TI-Plattform                                                               |
| [gemSpec_Aktensystem]          | gematik: Spezifikation ePA-Aktensystem                                                                      |
| [gemSpec_Autorisierung]        | gematik: Spezifikation Autorisierung ePA                                                                    |
| [gemSpec_DM_ePA]               | gematik: Datenmodell ePA                                                                                    |
| [gemSpec_Dokumentenverwaltung] | gematik: Spezifikation Dokumentenverwaltung ePA                                                             |
| [gemSpec_SGD_ePA]              | gematik: Spezifikation Schlüsselgenerierungsdienst ePA                                                      |
| [gemSpec_Krypt]                | gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur |
| [gemSpec_OID]                  | gematik: Spezifikation Festlegung von OIDs                                                                  |
| [gemSpec_PKI]                  | gematik: Übergreifende Spezifikation Spezifikation PKI                                                      |
| [gemSpec_Systemprozesse_dezTI] | gematik: Spezifikation Systemprozesse der dezentralen TI                                                    |
| [gemSpec_TBAuth]               | gematik: Tokenbasierte Authentisierung                                                                      |
| [gemSysL_Fachanwendung_ePA]    | gematik: Systemspezifisches Konzept ePA                                                                     |

## 9.5.2 Weitere Dokumente

| <b>[Quelle]</b> | <b>Herausgeber (Erscheinungsdatum): Titel</b>                                                                                                                                                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [IHE-ITI-TF]    | IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Revision 15.0                                                                                                                                                                                                        |
| [IHE-ITI-TF2b]  | IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0,<br><a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf</a> |
| [IHE-ITI-TF2x]  | IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2x) – Volume 2 Appendices, Revision 15.1<br><a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf</a>  |
| [MTOM]          | W3C (2005): SOAP Message Transmission Optimization Mechanism,                                                                                                                                                                                                                                   |

|  |                                                                                     |
|--|-------------------------------------------------------------------------------------|
|  | <a href="https://www.w3.org/TR/soap12-mtom/">https://www.w3.org/TR/soap12-mtom/</a> |
|--|-------------------------------------------------------------------------------------|



---

## 10 Anhang B - Übersicht über die verwendeten Versionen

---

**Schemas aus dem Namensraum des KTR-Consumer  
„http://ws.gematik.de/consumer“**

| <b>Name</b>     | <b>Version</b> | <b>TargetNamespace</b>                                                                                              |
|-----------------|----------------|---------------------------------------------------------------------------------------------------------------------|
| EPAService.wsdl | 1.0.0          | <a href="http://ws.gematik.de/consumer/EPAService/WSDL/v1.0">http://ws.gematik.de/consumer/EPAService/WSDL/v1.0</a> |
| EPAService.xsd  | 1.0.1          | <a href="http://ws.gematik.de/consumer/EPAService/v1.0">http://ws.gematik.de/consumer/EPAService/v1.0</a>           |