



Grobkonzept der "ePA für alle"

<b>Version:</b>	<b>3.0 RC</b>
Referenzierung:	gemKPT_ePAfuerAlle

## Dokumentenhistorie

Version	Stand	Kap./Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
3.0 RC	22.01.2024		Ersterstellung	gematik

# Inhaltsverzeichnis

1. Einordnung des Dokumentes .....	3
1.1. Zielgruppe .....	3
2. Systemüberblick .....	3
2.1. Aktensystem .....	3
2.2. Clients der ePA .....	4
2.2.1. ePA-Frontend des Versicherten .....	4
2.2.2. Primärsystem/Clientsystem .....	4
2.3. Signaturdienst .....	4
2.4. Beteiligte Systeme .....	4
3. Kernmechanismen .....	5
3.1. Vertrauenswürdige Ausführungsumgebung .....	5
3.2. Sichere Datenablage .....	6
3.3. Zugangssteuerung .....	6
3.3.1. Nutzerauthentisierung .....	6
3.3.2. Zugangssteuerung über Befugnisse .....	6
3.3.3. Zugangssteuerung über Geräte .....	7
3.4. Zugriffssteuerung .....	7
3.4.1. Consent Management .....	7
3.5. Protokollierung für den Versicherten .....	7
3.6. Medical Services .....	7
4. Aktenlokalisierung und Login .....	7
4.1. Lokalisierung der Service-Endpunkte der ePA .....	8
4.2. Lokalisierung der Akte eines Versicherten .....	8
4.3. Login in die Akte des Versicherten .....	8
5. Basisfunktionalitäten .....	9
5.1. Anlage einer Akte .....	9
5.1.1. Migration von "ePA 2.x"-Dokumenten .....	9
5.2. Vertrauenswürdige Ausführungsumgebung .....	10
5.2.1. Isolation der in einer VAU laufenden Verarbeitungen .....	10
5.2.2. Verschlüsselung von außerhalb der VAU gespeicherten Daten .....	10
5.2.3. Schutz der VAU-Schlüssel in einem HSM .....	11
5.2.4. Erkennen von Manipulationen an der VAU (Attestierung) .....	11
5.2.5. Schutz der Daten bei physischen Zugang zur VAU .....	11

5.2.6. Sicherer Kanal vom Client in die VAU (VAU-Kanal) .....	11
5.3. Befugnismanagement .....	11
5.3.1. Informationen des Befugniskontextes .....	12
5.3.2. Befugniskontextmanagement in der LEI-Umgebung .....	12
5.3.3. Befugniskontextmanagement mittels ePA-Frontend des Versicherten .....	13
5.4. Widerspruchsmanagement (Consent Management) .....	14
5.5. Device Management .....	15
5.5.1. Geräteregistrierung und -verifizierung .....	16
5.5.2. Auflisten und Entfernen von Geräten .....	18
5.6. Audit Event Service .....	18
5.7. Anbieterwechsel .....	19
5.7.1. Betreiberübergreifender Anbieterwechsel .....	20
5.7.2. Anbieterwechsel innerhalb eines Betreibers .....	22
6. Medical Services .....	22
6.1. Versorgungsspezifische Services .....	22
7. Abkürzungsverzeichnis und Glossar .....	22
8. Anhang .....	23

# 1. Einordnung des Dokumentes

Die "ePA für alle" realisiert technisch einen souveränen, sicheren und möglichst benutzerfreundlichen Zugang zu den Gesundheitsdaten eines Versicherten. Fachlich ermöglicht die ePA eine Vereinfachung der Anamnese, die Auswertung von longitudinalen Daten und einen verbesserten Übergang in einer sektorenübergreifenden Versorgung.

Dieses Dokument beschreibt wesentliche Kernmechanismen, Basisfunktionalitäten sowie technische Konzepte zu den Diensten des ePA-Aktensystems und den beteiligten Client-Systemen der Fachanwendung ePA.

Eine wesentliche Neuausrichtung der aktuellen ePA-Architektur ist die Unterstützung von digital gestützten Versorgungsprozessen – initial unterstützt die "ePA für alle" den digital gestützten Medikationsprozess. Weiterhin basiert die ePA-Architektur auf einer stringente Serviceorientierung innerhalb des ePA-Aktensystems und einer weiterentwickelten, modernen Sicherheitsarchitektur.

## 1.1. Zielgruppe

Das Dokument richtet sich an die interessierte Öffentlichkeit, an die Fachöffentlichkeit und an die umsetzende Industrie.

## 2. Systemüberblick

Dieses Kapitel gibt einen Systemüberblick über die Fachanwendung ePA und beschreibt sämtliche mit ihr in Verbindung stehende Systeme.

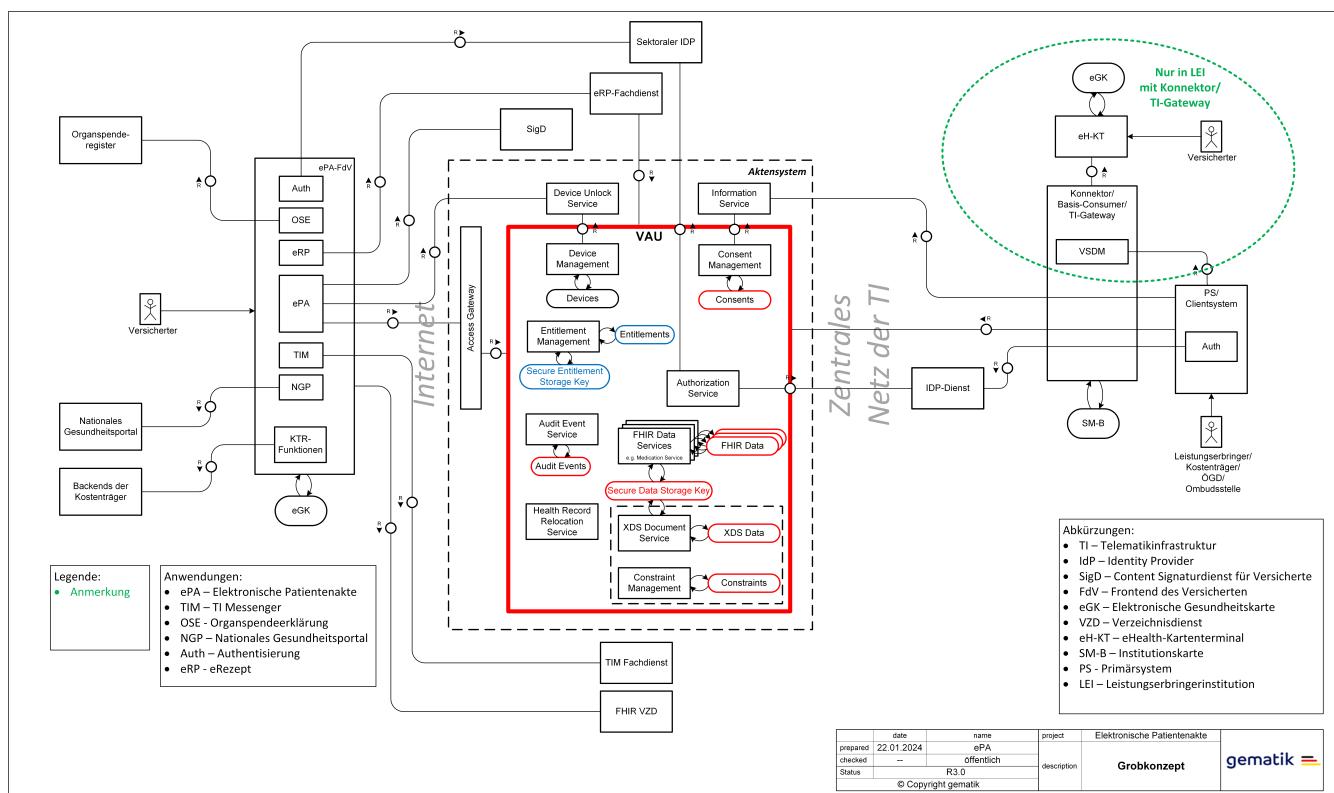


Abbildung 1: Systemüberblick der Fachanwendung ePA (FMC-Blockdiagramm)

## 2.1. Aktenystem

Das **ePA-Aktenystem** verwaltet pro Versicherten-/Aktenkonto alle vom Versicherten oder seinem berechtigten

Vertreter legitimierten Zugriffe auf die Akte. Alle Zugriffe über das **ePA-Frontend des Versicherten** (ePA-FdV) sind ausschließlich über am Aktensystem registrierte Geräte möglich. Die zentralen Funktionen des Aktensystems sind das integre Management von wohl definierten Metadaten und den medizinischen Dokumenten als auch die Unterstützung von digitalen Versorgungsprozessen. Initial bedient das Aktensystem den **digital gestützten Medikationsprozess** durch die Bereitstellung einer Elektronischen Medikationsliste (eML) an Leistungserbringer.

Für das ePA-FdV ist das ePA Aktensystem via Internet über ein **Access Gateway** erreichbar, welches die Weiterleitung von Nachrichten über interne Proxies durchführt. Die ePA wird von mehreren Aktenanbietern/Kostenträgern (KTR) für ihre Versicherten angeboten.

## 2.2. Clients der ePA

### 2.2.1. ePA-Frontend des Versicherten

Das ePA-Frontend des Versicherten (ePA-FdV) unterstützt den Versicherten beim Zugriff auf seine ePA, als auch in seiner Rolle als Vertreter für andere ePAs. Es läuft auf einem Gerät unter der Kontrolle des Versicherten (mobil oder stationär) und kann daher auch sensible Informationen verarbeiten. Alle Anwendungsfälle des Versicherten werden über dieses Frontend bereitgestellt oder integriert. Neben der Funktionalität für die ePA bietet das ePA-FdV das Frontend für verschiedene andere Anwendungen der Telematikinfrastruktur (TI) oder Funktionalitäten des KTR. Die ePA-FdV werden in verschiedenen Realisierungen durch die Kostenträger für die Versicherten bereitgestellt.

### 2.2.2. Primärsystem/Clientsystem

Das **Primär- oder Client-System** (PS/CS) bietet das Frontend für alle Nutzer, ausgenommen den Versicherten. Als Primärsysteme bezeichnen wir die Verwaltungssysteme der Leistungserbringer (Praxisverwaltungssysteme oder Krankenhausinformationssysteme), als Clientsysteme die Systeme anderer Nutzergruppen (z.B. Kostenträger, Digitale Gesundheitsanwendung). Hier liegt die Client-Logik der ePA und werden alle Anwendungsfälle ausgelöst. Die PS/CS gibt es in vielen verschiedenen Realisierungen. Zusammengefasst werden die PS und CS oft als **ePA-Clients** bezeichnet.

## 2.3. Signaturdienst

Der **Signaturdienst** (SigD) stellt den Nutzern eines ePA-FdV, nach erfolgreicher Authentifizierung am **Sektoralen Identity Provider** (Sektoraler IdP), eine kryptographische Identität zur Content-Signatur von Daten bereit. Er wird verwendet, um **Befugnisse**, die über ein **ePA-FdV** eingestellt werden, authentisch und integer zu halten. Die SigD werden von zum **Aktensystem** getrennten Anbietern im Auftrag der KTR bereitgestellt.

## 2.4. Beteiligte Systeme

Unter beteiligten Systemen werden Dienste oder Komponenten der Telematikinfrastruktur verstanden, die in der ePA, aber auch durch andere Anwendungen der Telematikinfrastruktur genutzt werden.

### FHIR Verzeichnisdienst

Bei der Erteilung von Befugnissen für Nutzer der ePA mit einer Telematik-ID, wird der entsprechende Nutzer über das ePA-FdV im **Verzeichnisdienst FHIR-Directory** (VZD-FHIR-Directory) gesucht und dessen Telematik-ID dort entnommen.

## Sektoraler Identity Provider

Der **Sektoraler IdP** der KTR stellt Versicherten eine sichere Digitale Identität (**GesundheitsID**) in der Telematikinfrastruktur bereit. Mit dieser digitalen Identität meldet sich der Versicherte an den Diensten der ePA sowie weiteren Diensten der TI an.

## IDP-Dienst

Der **IDP-Dienst** stellt Nutzern der TI, die sich über eine Institutionskarte (SMC-B) ausweisen können, eine sichere GesundheitsID in der Telematikinfrastruktur bereit. Mit dieser digitalen Identität meldet sich der Nutzer an den Diensten der ePA sowie weiteren Diensten der Telematikinfrastruktur an.

## Konnektor, TI-Gateway und eHealth-Kartenterminal

Der **Konnektor** oder das **TI-Gateway** als sicheres Gerät/Dienst bietet den Primärsystemen/Clientsystemen den netztechnischen Zugang zu den Diensten der ePA an. Über das **eHealth-Kartenterminal** (eH-KT) ermöglicht ein Konnektor den Zugriff auf kartengebundene Identitäten der Institutionen (SMC-B) oder der Versicherten (eGK) in der von ihm verwalteten Umgebung.

## Basis-Consumer

Der **Basis-Consumer** stellt das Gegenstück zum Konnektor in den Rechenzentren der Kostenträger dar. Er ist auf die Nutzungsszenarien und -umgebungen der Kostenträger optimiert. Auch er bietet den Zugriff auf die Identitäten der Kostenträger (SMC-B KTR).

## E-Rezept-Fachdienst

Der **E-Rezept-Fachdienst** (eRP-FD) speichert bei fehlendem Widerspruch alle Verordnungsdaten und die zugehörigen Dispensierinformationen in der Akte des Versicherten ab, damit diese Informationen im **digital gestützten Medikationsprozess** (dgMP) über die **elektronische Medikationsliste** (eML) verwendet werden können. Dem dgMP kann separat widersprochen werden (siehe [Consent Management](#)).

## Externe Services

Die Gruppe der **externen Services** ist vielfältig. Sie umfasst alle Dienste, die außerhalb der Fachanwendung ePA liegen, aber über das ePA-FdV integriert werden. Die Dienste können zu Anwendungen der Telematikinfrastruktur gehören (z.B. der TI-Messenger) oder externe Dienste, die aufgrund der gesetzlichen Vorgaben in das ePA-FdV integriert werden (z.B. Organspendeerkklärung oder das nationale Gesundheitsportal).

# 3. Kernmechanismen

Das folgende Kapitel beschreibt elementare Funktionen des ePA-Aktensystems. Sie stellen die vertrauliche und integre Verarbeitung von medizinischen Daten innerhalb des ePA-Aktensystems sicher.

## 3.1. Vertrauenswürdige Ausführungsumgebung

Die **Vertrauenswürdige Ausführungsumgebung** (VAU) erlaubt es, sensible medizinische Daten im Klartext serverseitig zu verarbeiten sowie Zugang und Zugriff serverseitig durchzusetzen, ohne dass der Anbieter/Betreiber des ePA-Aktensystems und seine Mitarbeiter (u.a. die Administratoren) auf diese Daten zugreifen können. Der Ausschluss des Anbieters/Betreibers erfolgt bei einer VAU durch technische Maßnahmen.

## 3.2. Sichere Datenablage

Die Daten der ePA werden in zwei unterschiedlichen sicheren Speicherbereichen verschlüsselt persistiert:

- Den **Secure Data Storage**, in dem die Fachdaten der ePA, zugehörige Informationen und Konfigurationsdaten gespeichert werden und
- den **Secure Entitlement Storage**, in dem Befugnisse der ePA gespeichert werden.

Die Speicherbereiche werden durch getrennte versicherten individuelle kryptographische Schlüssel gesichert.

Ein Kernelement der Sicherheitsarchitektur der ePA ist, dass der Zugang zum Schlüsselmaterial des **Secure Data Storage** technisch nur möglich ist, wenn für den authentifizierten Nutzer eine Befugnis im ePA-Aktensystem vorliegt. Der Schlüsselspeicher (Hardware Security Module (HSM)) prüft, dass der anfragende ePA-Dienst integer ist, der Nutzer authentifiziert ist sowie zur verifizierten Befugnis passt. Nur bei erfolgreicher Prüfung kann der kryptographische Schlüssel für den **Secure Data Storage** verwendet werden.

## 3.3. Zugangssteuerung

Die Menge der technisch befugten Akteure, welche die Daten einer Akte zur Gesundheitsversorgung implizit in einer **Behandlungssituation** oder explizit auf Wunsch des Versicherten verarbeiten dürfen, werden über **Befugnisse** zusammengefasst. Einer Befugnis liegen in der Regel ein oder mehrere Versorgungs- oder Behandlungskontexte zugrunde, welche in der ePA jedoch nicht abgebildet sind. Diese Kontexte können z.B. eine Episode of Care/Behandlungspfade, ein Workflow, ein stationärer Aufenthalt oder ambulanter Kontakt eines Patienten in einer Gesundheitseinrichtung sein.

Die Zugangssteuerung im ePA-Aktensystem setzt durch, dass ausschließlich über registrierte Befugnisse von authentifizierten Nutzern die sicheren Speicherbereiche für eine Datenverarbeitung zur Verfügung gestellt werden. Über ein ePA-FdV ist zusätzlich noch ein registriertes Gerät am ePA-Aktensystem erforderlich, um eine Befugnis zu legitimieren.

### 3.3.1. Nutzerauthentisierung

Zugreifende Nutzer der ePA werden mittels Identity Provider (IdP) der Telematikinfrastruktur (TI) authentifiziert. Dies bewerkstellt ein **Authorization Service** innerhalb der VAU, der die Kommunikation zu den IdP (**IDP-Dienst** und **Sektoraler IdP**) steuert. Nach einer erfolgreichen Authentisierung wird eine **User Session** etabliert. Im Rahmen dieser Session kann ein Nutzer verschiedene Befugnisse in Akten wahrnehmen.

### 3.3.2. Zugangssteuerung über Befugnisse

Der Zugang zu einer Akte darf nur erfolgen, wenn der authentifizierte Nutzer befugt ist, mit der konkreten Akte zu arbeiten. Diese Befugnis ist integer und authentisch im ePA-Aktensystem gespeichert. Die Integrität und Authentizität der Befugnis wird über eine Signatur umgesetzt. Ist eine Befugnis für den Nutzer gültig, wird ein interner **Health Record Context** aufgebaut. Innerhalb dieses Kontextes kann der Nutzer spezifische Fachoperationen ohne eine erneute Authentisierung ausführen. Auch ist es möglich, den Aktenkontext innerhalb einer User Session zu wechseln.

Über eine vom Kostenträger (KTR) eingerichtete Ombudsstelle oder das ePA-FdV kann ein Verbot für eine Befugnis für eine spezielle Leistungserbringerinstitution (LEI) auf Basis der Telematik-ID registriert werden. Eine für diese LEI eventuell vorhandene Befugnis wird in diesem Fall gelöscht und neu eingestellte Befugnisse über ein Primärsystem dieser LEI werden aktenseitig verworfen und damit nicht gespeichert.

### 3.3.3. Zugangssteuerung über Geräte

Der Zugang des Versicherten zum ePA-Aktensystem über das ePA-FdV setzt voraus, dass das Gerät des Versicherten durch den **Device Management** Service registriert und verifiziert ist. Wird versucht, mit einem nicht registrierten oder unverifizierten Gerät auf das System zuzugreifen, informiert der Device Management Service, dass die User Session aufgrund der fehlenden Registrierung oder Verifizierung des Geräts geschlossen werden muss. Der **Device Unlock Service** regelt die Verifizierung der Geräte, indem er dem Versicherten einen Aktivierungs-Link per E-Mail zusendet.

## 3.4. Zugriffssteuerung

Die Zugriffssteuerung stellt sicher, dass nur solche Zugriffe eines befugten Nutzers zugelassen werden, die den gesetzlichen Zugriffsregeln entsprechen und nicht vom Versicherten oder seinem Vertreter über eine widerspruchsfähige Funktion ausgeschlossen wurden. Eine Autorisierung auf medizinische Daten und Services wird damit durch die Kombination aus einer Befugnis, den gesetzlichen Regeln für Nutzer(-gruppen), als auch möglichen Widersprüchen (z.B. Widerspruch des Medikationsprozesses) repräsentiert. Im Rahmen dieser *Autorisierung* ist ein genereller Schreibzugriff legitim. Im Anhang werden die gesetzlichen Zugriffsregeln in einer "[Legal Policy](#)" im Überblick dargestellt.

### 3.4.1. Consent Management

Das **Consent Management** verwaltet die widerspruchsfähigen Funktionen der Akte durch den Versicherten, Vertreter oder eine vom Versicherten beauftragten Ombudsstelle der Krankenkasse. Es setzt die spezifischen "Opt-out Rechte" des Versicherten um. Es kann gegen die Teilnahme an Versorgungsprozessen widersprochen werden.

Der **Information Service** stellt weiterhin lesend die Konfigurationseinstellungen der Widersprüche zu Versorgungsprozessen außerhalb der VAU für andere Akteure zur Verfügung. Damit kann beispielsweise ein technischer Akteur eines medizinischen Versorgungsdienstes die Daten ohne eine Anmeldung am ePA-Aktensystem verarbeiten und ggf. unnötige Verbindungsversuche zur VAU im Vorfeld vermeiden.

## 3.5. Protokollierung für den Versicherten

Zum Zwecke der Datenschutzkontrolle werden alle versuchten und getätigten Zugriffe auf die Daten des Versicherten im ePA-Aktensystem protokolliert. Die Protokolleinträge können durch den Versicherten oder durch einen befugten Vertreter über das ePA-FdV eingesehen werden. Versicherte ohne ein ePA-FdV können bei ihrer zuständigen Ombudsstelle beantragen, die Protokolldaten zur Verfügung gestellt zu bekommen. Der Zugriff auf die Protokoldaten durch andere Akteure ist technisch ausgeschlossen.

## 3.6. Medical Services

Das ePA-Aktensystem unterstützt sowohl das Verwalten von medizinischen Dokumenten, als auch digital gestützte, versorgungsspezifische Prozesse mittels Medical Services.

## 4. Aktenlokalisierung und Login

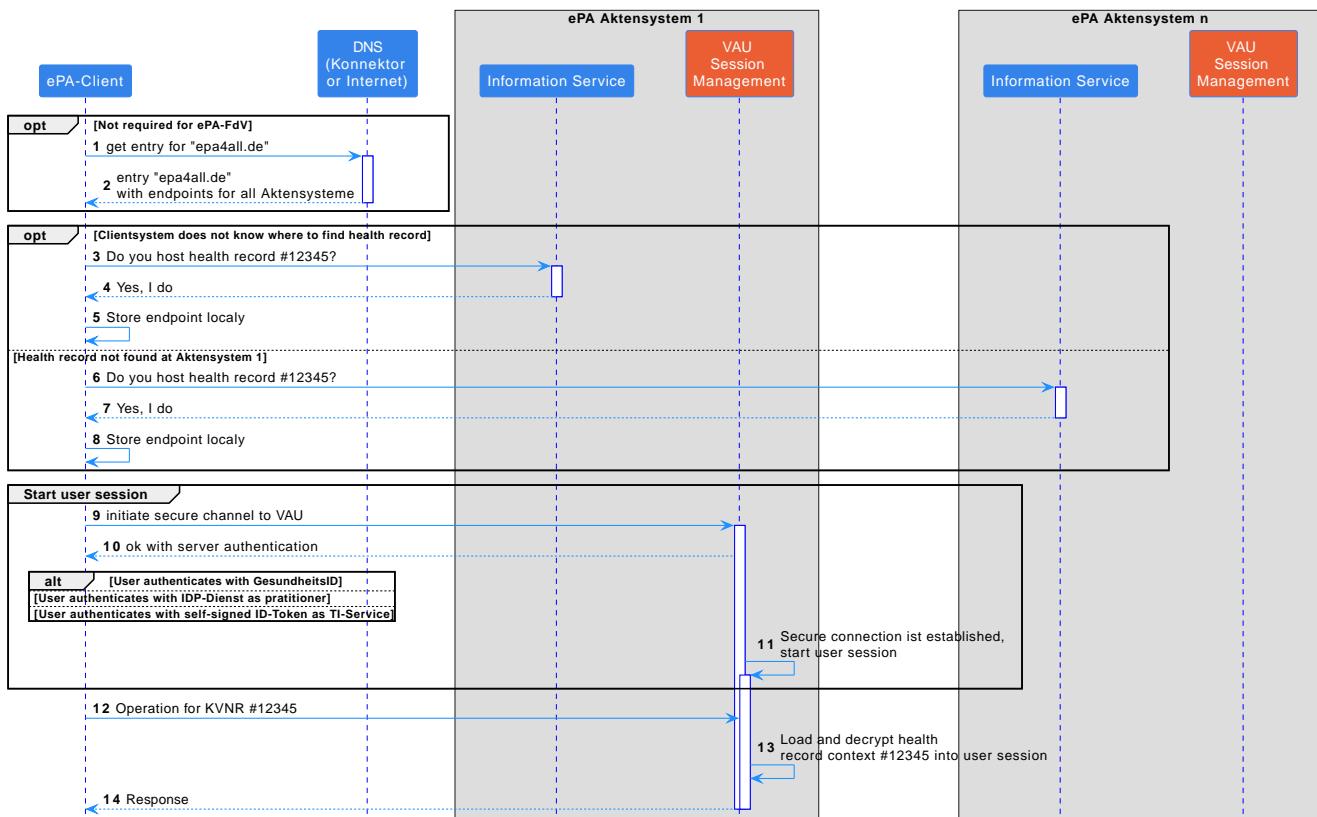


Abbildung 2: Aktenlokalisierung und Login in die Akte

## 4.1. Lokalisierung der Service-Endpunkte der ePA

Die Endpunkte der verschiedenen Aktensysteme erfahren ePA-Clients (nicht das ePA-FdV) über die DNS Service Discovery (DNS-SD) für eine übergreifende Domäne (epa4all.de) entweder über den DNS Resolver des Konnektors oder den konfigurierten DNS Resolver für das Internet. Hinterlegt sind dort alle Service-Endpunkte in der Telematikinfrastruktur (TI) für die verschiedenen Aktensysteme. Die DNS-SD wird durch den entsprechenden ePA-Client einmal täglich abgefragt.

## 4.2. Lokalisierung der Akte eines Versicherten

Die ePA-Clients (Primärsystem, ePA-FdV, E-Rezept-Fachdienst oder auch ein Clientsystem der Kostenträger (KTR) oder der Ombudsstelle) halten den ermittelten zuständigen Service-Endpunkt für eine Akte vor. Sollte diese Information nicht im ePA-Client vorliegen, wendet sich der ePA-Client an den **Information Service**, um dort nach der Akte zu fragen und wenn dort für die gegebene Krankenversicherungsnummer (KVNR) eine Akte existiert den Service-Endpunkt lokal zu speichern. Ist keine Akte auf diesem Aktensystem vorhanden, erfolgt die Abfrage am anderen Aktensystem.

Kennt kein Aktensystem die Akte, hat der Versicherte der Bereitstellung einer ePA widersprochen und es existiert keine Akte.

## 4.3. Login in die Akte des Versicherten

Ein ePA-Client (Primärsystem, ePA-FdV, Clientsystem der Kostenträger oder der Ombudsstelle) oder der E-Rezept-Fachdienst baut einen Kanal in die VAU des Aktensystems auf und authentifiziert dabei die VAU als authentische VAU des Anbieters. Nachfolgend wird eine User Session für den Nutzer angelegt und der Nutzer mit Hilfe des **IDP-Dienstes**, des **Sektoralen IdPs (GesundheitsID)** oder über einen mit dem Zertifikatsprofil C.FD.AUT zugehörigen Schlüssel - selbst signiertes IDToken (nur Dienste der TI) - authentifiziert.

Nach erfolgreicher Aktivierung der User Session können Anfragen vom ePA-Client bzw. E-Rezept-Fachdienst an beliebige Akten gerichtet werden. Mit der ersten Anfrage an eine bestimmte Akte wird diese nach Befugnisprüfung in der User Session als **Health Record Context** geladen und Fachoperationen können beliebig ausgeführt werden.

## 5. Basisfunktionalitäten

In diesem Kapitel werden technische Konzepte zu verschiedenen Basisfunktionalitäten der ePA dargestellt, die der Spezifikation der einzelnen Produkttypen zugrunde liegen.

### 5.1. Anlage einer Akte

Rahmenbedingung für die Aktenanlage ist es, dass Dokumente durch den Kostenträger (z.B. Abrechnungsdaten) durch den E-Rezept-Fachdienst vor der ersten Verwendung der Akte in der Versorgung in die Akte eines Nutzers eingestellt werden können.

Die Initialisierung der Akte erfolgt - wie in der aktuellen ePA - durch den Kostenträger und wird durch organisatorische Prozesse bestimmt. Gleiches gilt für den Widerspruch gegen die Anlage einer Akte durch den Versicherten, der zur Nicht-Anlage oder zur Löschung der Akte mitsamt ihren Inhalten führt. Initialisierte ePA für alle-Akten gehen in den Status "Initialized" über, damit ePA2.x-Konnektoren nicht versuchen diese zu aktivieren. Sollte in der ePA 2.x noch eine Akte im Status "Registered" vorliegen, wird der Status auf "Unknown" zurückgesetzt und für den Versicherten in der ePA für alle eine neue Akte angelegt.

Vor Anlage einer neuen Akte klärt das Aktensystem am **Information Service** der anderen Aktensysteme, ob schon eine Akte für die entsprechende KVNR existiert, da für einen Versicherten nur eine aktive Akte in der Telematikinfrastruktur bestehen darf. Wenn schon eine Akte existiert, wird die Akte vorbereitet und der Anbieterwechsel eingeleitet.

Im **Consent Management** werden die Widerspruchsinformationen mit Standardwerten initialisiert. Damit Widerspruchsinformationen möglichst leichtgewichtig (d.h. ohne die VAU zu öffnen) abgefragt werden können, werden die Widerspruchsinformationen bei Anlage und Änderung in den lokalen Cache des **Information Service** repliziert.

Im **Entitlement Management** sind der Versicherte selbst, der zuständige Kostenträger, die zuständige Ombudsstelle und der E-Rezept-Fachdienst als befugt hinterlegt. Die Befugnisse für den zuständigen Kostenträger und der zuständigen Ombudsstelle müssen durch diese mit deren SMC-B Zertifikatsprofil C.HCI.OSIG signiert werden. Die beiden Befugnisse werden im Aktensystem hinterlegt und beim Start der VAU ins **Entitlement Management** übernommen.

Der Statusübergang zu "Activated" wird durch die Kostenträger nachfolgend separat angestoßen. Danach ist die Akte in der Versorgung nutzbar.

#### 5.1.1. Migration von "ePA 2.x"-Dokumenten

Wenn schon ein aktiviertes Aktenkonto (ePA 2.x) vorliegt, sollen die dort vorliegenden Dokumente in die ePA für alle migriert werden. Dies erfolgt über das **ePA-FdV**, welches dafür weiterhin Zugriff auf das ePA 2.x Schlüsselmaterial benötigt. Das Schlüsselmaterial wird dem **XDS Document Service** übergeben, der damit die Daten der ePA 2.x in die ePA für alle importiert. Die Funktion kann Aktensystemspezifisch im Zusammenspiel mit dem zugehörigen **ePA-FdV** realisiert werden, da kein Interoperabilität zu anderen Produkten nötig ist.

Schon bestehende Berechtigungen für Vertreter müssen durch das **ePA-FdV** als Befugnisse neu eingestellt werden. Die entsprechenden Informationen können im **ePA-FdV** zwischgespeichert werden, um das erneute Einrichten der Vertreter zu unterstützen.

## 5.2. Vertrauenswürdige Ausführungsumgebung

Die **Vertrauenswürdige Ausführungsumgebung** (VAU) gewährleistet mit technischen Maßnahmen, dass sensible Klartextdaten serverseitig im ePA-Aktensystem verarbeitet werden können, ohne dass ein Angreifer (insbesondere auch kein Innenräuber beim Betreiber des Dienstes mit maximalen Zugriffsrechten) auf diese Daten zugreifen kann. Zu den in der VAU verarbeiteten sensiblen Daten gehören die medizinischen Daten des Versicherten, Policies, Befugnisse, Widerspruchsinformationen und Protokolle des Versicherten.

### 5.2.1. Isolation der in einer VAU laufenden Verarbeitungen

Die Verarbeitung der sensiblen Daten innerhalb der VAU erfolgt technisch getrennt von allen außerhalb der VAU laufenden Verarbeitungen des Dienstes (**äußere Isolation der VAU**), so dass technisch verhindert wird, dass ein Zugriff des Aktensystembetreibers auf die im Klartext verarbeiteten Daten in der VAU erfolgen kann.

Innerhalb der VAU erfolgt die Verarbeitung der sensiblen Daten für ein Aktenkonto technisch getrennt von anderen in der VAU laufenden Verarbeitungen für andere Aktenkonten (**innere Isolation der VAU**), so dass innerhalb einer VAU technisch verhindert wird, dass ein Zugriff von einem Aktenkonto eines Versicherten auf ein Aktenkonto eines anderen Versicherten erfolgen kann.

Die Verarbeitungen innerhalb einer VAU werden über User Sessions und Health Record Contexts voneinander getrennt. Innerhalb der VAU werden alle Verarbeitungen und Daten einer User Session technisch getrennt von anderen User Sessions umgesetzt. In einer VAU können mehrere User Sessions vorliegen, die vom **User Session Manager** verwaltet werden.

- **User Session:** Eine User Session ist genau einem Nutzer zugeordnet. Die User Session wird über einen zuvor aufgebauten VAU-Kanal unter Nutzung des für den Nutzer zuständigen Identity Providers aufgebaut. Als Ergebnis hält die User Session das IDToken für den Nutzer. In einer User Session können mehrere Health Record Contexts zu verschiedenen Aktenkonten parallel aufgebaut werden, auf die der Nutzer dann zugreifen kann. Innerhalb einer User Session verwaltet der **Health Record Context Manager** die Health Record Contexts.
- **Health Record Context:** Im Health Record Context erfolgt die Verarbeitung der (medizinischen) Daten eines Aktenkontos. Alle Verarbeitungen in einem Health Record Context beziehen sich auf genau ein Aktenkonto. In einem Health Record Context werden niemals Daten aus unterschiedlichen Aktenkonten verarbeitet.

Für dasselbe Aktenkonto kann in unterschiedlichen User Sessions (zur selben Zeit) mit einem Health Record Context gearbeitet werden. Vom Hersteller des Aktensystems werden daher geeignete Synchronisationsmechanismen umgesetzt, um auch bei parallelen Zugriffen von unterschiedlichen Nutzern auf dasselbe Aktenkonto einen konsistenten Aktenkontozustand zu gewährleisten.

In einer VAU dürfen nur eine maximale Anzahl von User Sessions gleichzeitig aufgebaut sein. Werden über die maximale Anzahl hinaus weitere User Sessions benötigt, werden diese in einer separaten, durch hardwarebasierte Mechanismen getrennten VAU, aufgebaut. Innerhalb einer User Session dürfen ebenfalls nur eine maximale Anzahl von Health Record Contexts gleichzeitig aufgebaut sein.

### 5.2.2. Verschlüsselung von außerhalb der VAU gespeicherten Daten

Sollen die in der VAU verarbeiteten Daten in den Systemen des Aktensystembetreibers gespeichert werden, werden sie zuvor in der VAU verschlüsselt. Hierzu werden ein:

- **Secure Data Storage Key** für die medizinischen Daten und Verwaltungsdaten einer Akte sowie ein
- **Secure Entitlement Storage Key** für die Befugnisse

als Persistierungsschlüssel verwendet.

Die versichertenindividuellen Persistierungsschlüssel werden innerhalb des HSMs aus Masterkeys und der KVNR des Kontoinhabers abgeleitet. Die Persistierungsschlüssel verlassen die VAU niemals und werden beim Schließen der VAU gelöscht. Es wird technisch verhindert, dass der Betreiber des Dienstes auf die Persistierungsschlüssel von Versicherten zugreifen kann.

### 5.2.3. Schutz der VAU-Schlüssel in einem HSM

Die für den Betrieb der VAU notwendigen Schlüssel werden in einem Hardware Security Module (HSM) sicher gespeichert. Dies sind zum einen die Identitäten mit denen sich eine VAU gegenüber ePA-Clients (u.a. ePA-FdV) authentisiert und den Masterkeys, aus denen die versichertenindividuellen Persistierungsschlüssel abgeleitet werden.

Es wird durch das HSM technisch durchgesetzt, dass der Zugriff auf VAU-Schlüssel im HSM nur durch eine attestierte VAU möglich ist. Dadurch wird technisch ausgeschlossen, dass ein Innentäter beim Betreiber auf die VAU-Schlüssel im HSM zugreifen kann.

Für die Ableitung des versichertenindividuellen **Secure Data Storage Key** müssen dem HSM das IDToken des angemeldeten Nutzers und die signierte Befugnis übergeben werden. Das HSM prüft anhand der signierten Befugnis, ob der Nutzer für das Aktenkonto befugt ist. Nur für diesen speziellen Fall wird der versichertenindividuelle **Secure Data Storage Key** für die KVNR im HSM abgeleitet und über einen sicheren Kanal in die VAU übermittelt. Innerhalb der VAU werden die Daten mittels des **Secure Data Storage Key** verschlüsselt und dann außerhalb der VAU gespeichert.

Für die Ableitung des versichertenindividuellen **Secure Entitlement Storage Key** prüft das HSM lediglich, dass es sich um eine attestierte VAU handelt.

### 5.2.4. Erkennen von Manipulationen an der VAU (Attestierung)

Die Integrität der VAU-Software oder der VAU-Hardware wird beim Start einer VAU geprüft, um den Start bei einer manipulierten VAU abzubrechen. Hierzu werden dem HSM in einem gemeinsamen Prozess mit der gematik die zugelassene VAU-Software und die VAU-Hardware bekannt gemacht. Beim Start einer VAU werden sowohl die VAU-Software als auch die VAU-Hardware technisch attestiert. Der Attestierungsnachweis wird im HSM geprüft und ein Zugriff verweigert, wenn die attestierte VAU-Software oder VAU-Hardware dem HSM nicht bekannt sind.

### 5.2.5. Schutz der Daten bei physischen Zugang zur VAU

Auch bei einem physischen Zugang zu den Hardware-Komponenten der VAU gewährleisten technische Maßnahmen, dass keine in der VAU verarbeiteten Daten extrahiert oder manipuliert werden können.

### 5.2.6. Sicherer Kanal vom Client in die VAU (VAU-Kanal)

Die Daten werden ausschließlich über sichere, beiderseitig authentisierte, VAU-Kanäle von Systemen der Nutzer (u.a. Versicherter, Leistungserbringer) in die VAU transportiert bzw. aus der VAU abgerufen. Die VAU-Kanäle stellen sicher, dass sowohl externe Angreifer als auch Innentäter beim Betreiber nicht auf die transportierten Daten zugreifen können.

## 5.3. Befugnismanagement

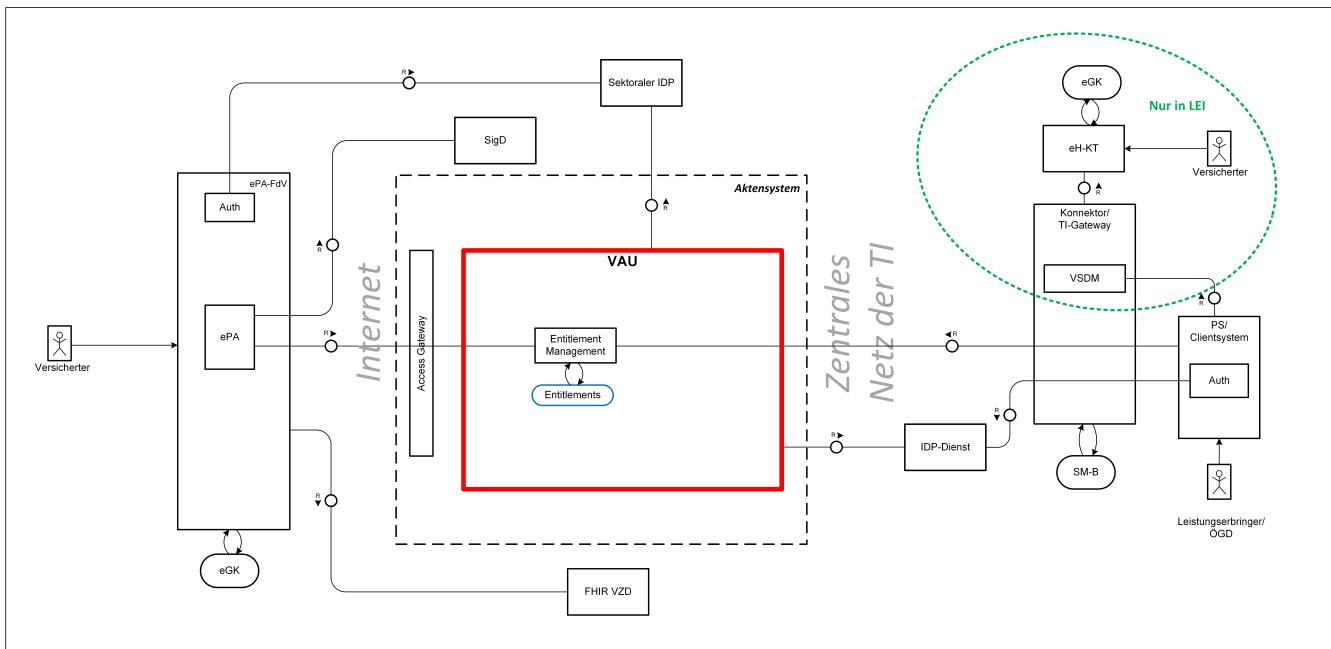


Abbildung 3: Entitlement Management - Beteiligte Komponenten

### 5.3.1. Informationen des Befugniskontextes

Für jeden Nutzer der ePA, der aufgrund einer Behandlungssituation – oder durch den Versicherten bestimmt – für den Zugriff auf die Akte befugt ist, wird eine Befugnis im **Entitlement Management** der ePA hinterlegt. Die Menge aller befugten Nutzer einer Akte stellt deren Befugniskontext dar. Der Versicherte selbst, der zuständige Kostenträger und der E-Rezept-Fachdienst sind statisch befugt – deren Befugnisse können nicht gelöscht werden.

In einer Befugnis werden folgende Attribute verwaltet:

- Nutzer-ID des befugten Nutzers (Telematik-ID/KVNR vom Client übergeben)
- Nutzernname des befugten Nutzers (vom Client übergeben)
- Enddatum (ggf. "unbegrenzt", serverseitig oder durch den Versicherten gesetzt)
- Art der Aufnahme – eingestellt durch einen Vertreter oder ausgelöst durch den Versicherten (serverseitig gesetzt)
- Optional: Name des Vertreters bei Einrichtung von Befugnissen (serverseitig gesetzt)

Das **Entitlement Management** löscht regelmäßig Befugnisse, bei denen das Enddatum in der Vergangenheit liegt.

### 5.3.2. Befugniskontextmanagement in der LEI-Umgebung

#### Hinzufügen einer Befugnis zum Befugniskontext in der Umgebung des Befugten

Wird eine eGK in der Umgebung des zu Befugenden zum Zwecke des Lesens der Versichertenstammdaten gesteckt, wird durch das Primär-/Clientsystem auch eine Befugnis erzeugt und im **Entitlement Management** registriert. Die Dauer der Befugnis für Apotheken, Öffentlichen Gesundheitsdienst (ÖGD) und Institutionen der Arbeits- und Betriebsmedizin beträgt 3 Tage und für sonstige Leistungserbringerinstitutionen 90 Tage.

Zum Erstellen einer Befugnis ist ein Anwesenheitsnachweis der eGK verpflichtend. Dieser wird über den Prüfungsnachweis erzeugt, der aus der Durchführung des VSDM-Anwendungsfalls "ReadVSD" im Konnektor/TI-Gateway resultiert. Damit der Prüfungsnachweis in Verbindung zur Umgebung gesetzt werden kann, wird dieser zudem mit der C.HCI.OSIG-Identität der SMC-B signiert, bevor er im **Entitlement**

**Management** registriert wird.

Eine potentiell bereits bestehende Befugnis wird durch die neue Befugnis ersetzt, falls die Dauer der alten Befugnis geringer ist als die der neu hinzuzufügenden Befugnis.

### 5.3.3. Befugniskontextmanagement mittels ePA-Frontend des Versicherten

#### Anzeige des Befugniskontextes mittels ePA-Frontend des Versicherten

Der Versicherte oder ein berechtigter Vertreter hat sich mit seinem ePA-FdV an der Akte des Versicherten angemeldet. Das ePA-FdV verfügt über eine Funktion zum Anzeigen des Befugniskontexts. Wird diese Funktion ausgeführt, werden die erforderlichen Informationen am **Entitlement Management** abgefragt. Der Befugniskontext liegt dann dem ePA-FdV vor und wird dort zur Anzeige gebracht.

Die Befugnisse für den Kostenträger, für den E-Rezept-Fachdienst und den Versicherten selbst werden nicht zurückgegeben.

#### Hinzufügen eines Nutzers zum Befugniskontext

Unter Verwendung der Suche von Leistungserbringerinstitutionen (LEI) über den Verzeichnisdienst **VZD FHIR-Directory** sucht der Versicherte oder ein berechtigter Vertreter zunächst den neu zu befugenden Nutzer (d.h. eine Leistungserbringerinstitution, Institution des Öffentlicher Gesundheitsdienstes oder eine Institution der Arbeits- und Betriebsmedizin). Das **ePA-FdV** erzeugt dann eine neue Befugnis mit der Telematik-ID aus dem **VZD FHIR-Directory** mit der gewünschten Laufzeit und signiert diese mit Hilfe des Signaturdienstes (SigD). Nach erfolgreicher Anmeldung am Aktensystem wird die Befugnis im **Entitlement Management** registriert.

Der Versicherte bzw. ein berechtigter Vertreter kann die Laufzeit der neuen Befugnis flexibel festlegen oder aber eine dauerhafte Gültigkeit wählen. Die Befugnis für eine DiGA gilt immer bis zu deren Entzug.

Fügt ein Vertreter einen Eintrag zum Befugniskontext des Versicherten hinzu, ist für den Namen des Ausstellers im Eintrag des Befugniskontexts der Name des Vertreters anzugeben.

#### Ändern der Dauer für eine befugte Leistungserbringerinstitution

Die Dauer der Befugnis einer Leistungserbringerinstitution, medizinische Daten in einer Akte zu verarbeiten, kann über das ePA-FdV durch den Versicherten oder einen berechtigten Vertreter geändert werden. Dazu selektiert der Versicherte oder ein berechtigter Vertreter im ePA-FdV die zu bearbeitende Befugnis aus dem bestehenden Befugniskontext und erzeugt eine neue Befugnis mit neuer Gültigkeit. Anschließend wird die neue Befugnis mit Hilfe des SigD signiert.

Das ePA-FdV übermittelt die neue Befugnis der Leistungserbringerinstitution an das **Entitlement Management**. Dort wird die alte Befugnis gelöscht und die neue Befugnis registriert.

Ändert ein Vertreter einen Eintrag zum Befugniskontext des Versicherten, ist für den Namen des Ausstellers im Eintrag des Befugniskontexts der Name des Vertreters zu nutzen.

#### Löschen eines befugten Nutzers

Der Versicherte oder ein berechtigter Vertreter selektiert im ePA-FdV die zu lösche Befugnis des bestehenden Befugniskontexts des Versicherten. Anschließend sendet das ePA-FdV eine Löschanfrage mit dem zu löschen Nutzer an das **Entitlement Management**. Die entsprechende Befugnis wird gelöscht.

#### Befügen eines Vertreters

Voraussetzung für die Befugnis eines Vertreters ist das Wissen um dessen KVNR und dessen E-Mail-Adresse.

Das ePA-FdV erzeugt eine Befugnis für den Vertreter, signiert diese mit Hilfe des SigD und registriert sie am **Entitlement Management**, sofern der Vertreter nicht schon Teil des Befugniskontexts ist. Die Befugnis eines Vertreters gilt immer bis zu deren Entzug. Ein Vertreter kann keinen weiteren Vertreter befugen.

### Entzug der Befugnis für einen Vertreter

Der Versicherte selektiert im ePA-FdV die zu löschen Befugnis des Vertreters. Anschließend sendet das ePA-FdV eine Löschanfrage mit dem zu löschen Vertreter an das **Entitlement Management**. Dort wird die Befugnis aus dem Befugniskontext des Aktenkontos des Versicherten entfernt.

### Der Nutzung durch eine Leistungserbringerinstitution widersprechen

Der Widerspruch gegen die Nutzung der ePA durch eine spezifische Leistungserbringerinstitution erfolgt über die Ombudsstelle des zuständigen Kostenträgers oder das ePA-FdV. Die authentifizierte Ombudsstelle oder der Versicherte (über sein **ePA-FdV**) vermerkt im **Entitlement Management**, dass für die spezifische Leistungserbringerinstitution keine Befugnisse registriert werden dürfen. Eventuell vorhandene Befugnisse werden gelöscht.

## 5.4. Widerspruchsmanagement (Consent Management)

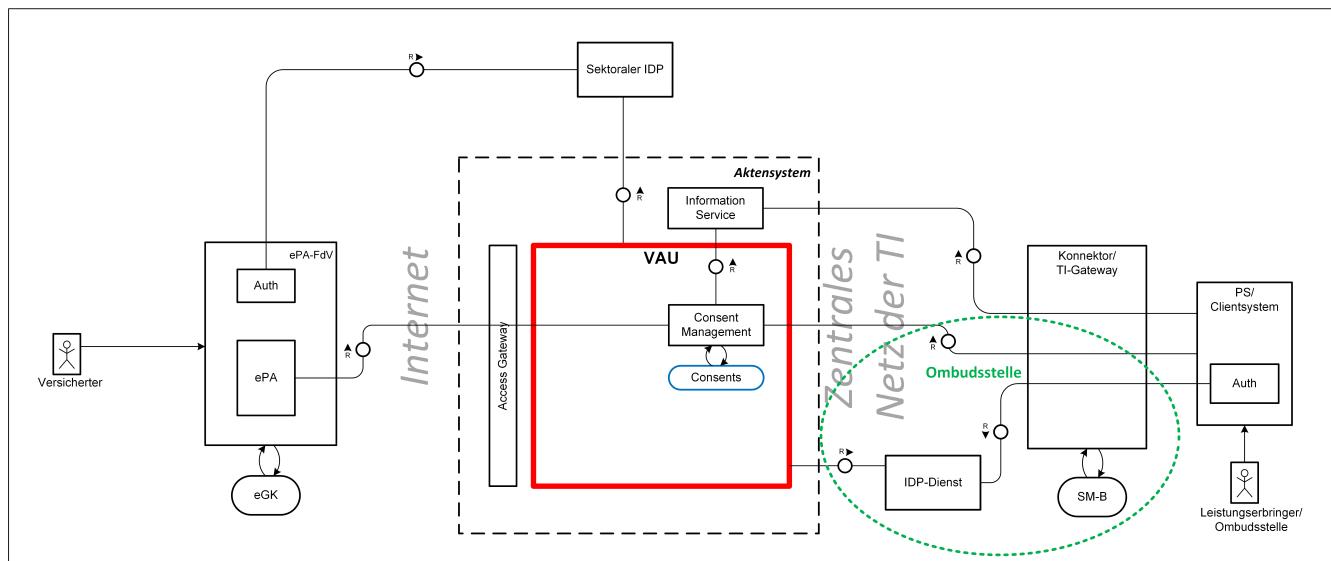


Abbildung 4: Consent Management - Beteiligte Komponenten

Der Versicherte kann der Akte insgesamt widersprechen, diesen Widerspruch aber auch jederzeit wieder zurücknehmen. Der Versicherte oder ein Vertreter kann bei genutzter Akte durch einen Widerspruch folgende Funktionen abwählen oder durch Zurücknehmen des Widerspruchs auch wieder nutzen:

- Teilnahme am digital gestützten Medikationsprozess
- Einstellung von Verordnungs- und Dispensierdaten durch den E-Rezept-Fachdienst
- Einstellung von Abrechnungsdaten durch den Kostenträger

Der Widerspruch gegen das Einstellen von Abrechnungsdaten durch den Kostenträger wird durch die Systeme des Kostenträgers verwaltet und durchgesetzt.

Die Wahrnehmung - auch das Zurücknehmen - von Widersprüchen sind für den Versicherten grundsätzlich möglich. Er kann dies einerseits durch die Nutzung des ePA-FdV selbst durchführen oder andererseits die Ombudsstelle beauftragen, dass dies durchgeführt wird.

Die im Aktensystem hinterlegten Widerspruchsinformationen können mit dem ePA-FdV durch den Versicherten

bzw. den berechtigten Vertreters geändert werden.

Die Widerspruchsinformationen teilen sich auf in Widersprüche gegen Versorgungsprozesse (derzeit ausschließlich Medikationsprozess) und in sonstige Widersprüche. Nur Widersprüche gegen Versorgungsprozesse werden in den **Information Service** gespiegelt.

### Ändern von Widerspruchsinformationen mittels ePA-Frontend des Versicherten

Der Versicherte oder ein Vertreter hat sich mit seinem ePA-FdV an der Akte des Versicherten angemeldet. Das ePA-FdV verfügt über eine Funktion zum Verwalten der Widerspruchsinformationen. Durch Ausführen der Funktion liegen dem ePA-FdV die aktuellen Widerspruchsinformationen vor und werden dort zur Anzeige gebracht.

Der Versicherte bzw. ein Vertreter ändert eine oder mehrere Widerspruchsinformationen. Im **Consent Management** werden daraufhin die Widerspruchsinformationen aktualisiert. Falls sich die Widerspruchsinformationen ändern, werden diese entsprechend der Vorgaben in den Cache des **Information Service** gespiegelt, um eine leichtgewichtige Abfrage für ePA-Clients zu ermöglichen.

Das ePA-Aktensystem reagiert bei Widersprüchen wie folgt:

*Tabelle 1: Auswirkungen von Widersprüchen auf bestehende Daten*

Funktion	Auswirkung
Akte gesamt	Löschen der gesamten Akte inklusive Dokumente und Daten
Medikationsprozess	Sperren des Zugriffs auf den Medication Service und den Medikationsplan
Einstellung Daten E-Rezept-Fachdienst	Löschen aller bisher gesammelten Daten zum Medikationsprozess sowie des Medikationsplans sowie Aktivierung des Widerspruchs zum Medikationsprozess
Abrechnungsdaten	Abrechnungsdaten bleiben in der Akte erhalten

Beim Zurücknehmen des Widerspruchs zur Akte insgesamt wird eine neue Akte durch den Kostenträger angelegt. Beim Zurücknehmen der anderen Widersprüche werden die entsprechenden Funktionen wieder ausgeführt. Wird der Widerspruch zum Medikationsprozess oder zur Einstellung von Daten durch den E-Rezept-Fachdienst zurückgenommen, werden beide Funktionen gesamthaft aktiviert.

### Ändern von Widerspruchsinformationen über die Ombudsstelle

Versicherte, die über kein ePA-FdV verfügen, können Widersprüche gegen einzelne Versorgungsprozesse (derzeit nur der Medikationsprozess) sowie das Einstellen von Verordnungsdaten und Dispensierinformationen durch den E-Rezept-Fachdienst gegenüber der Ombudsstelle ihres Kostenträgers erklären. Diese setzt den entsprechenden Widerspruch nach erfolgreicher Authentifizierung durch das **Consent Management** in der Akte des Versicherten. Die Wirkung ist dabei dieselbe, wie bei der Verwaltung der Widersprüche über das ePA-FdV.

### Abfrage von Widerspruchsinformationen zu Versorgungsprozessen

Damit ein an einem Versorgungsprozess beteiligter Nutzer oder seine Systeme (LE/PS oder E-Rezept-Fachdienst) erkennen kann, ob ein bestimmter Versorgungsprozess von ihm zu bedienen ist, fragt er diese Information am **Information Service** ab. Die Abfrage wird aus den gespiegelten Widerspruchsinformationen bedient und ist ohne Authentisierung möglich.

## 5.5. Device Management

Um Zugang zum ePA-Aktensystem zu erhalten, muss jede ePA-FdV-Installation zuerst registriert und verifiziert

werden. Wird ein Login-Versuch mit einem Gerät unternommen, das nicht verifiziert ist, beendet das ePA-Aktensystem die entsprechende **User Session** und informiert den Nutzer, dass das Gerät nicht autorisiert ist. Das **Device Management** ist für die Registrierung der Geräte und die Zugangskontrolle zum ePA-Aktensystem verantwortlich. Diese Komponente vergibt das **Device Token**, steuert den Verifizierungsprozess der Geräte und überwacht deren Registrierungsstatus.

### 5.5.1. Geräteregistrierung und -verifizierung

Für den Zugriff eines Gerätes (ePA-FdV) auf das ePA-Aktensystem ist eine Registrierung und Verifizierung des Gerätes notwendig. Diese Registrierung erfolgt indirekt, nachdem ein authentifizierter Versicherter versucht hat, sich über das ePA-FdV in das ePA-Aktensystem einzuloggen, jedoch ein nicht registriertes Gerät verwendet. Da das **Device Management** innerhalb der **User Session** angesiedelt ist, kann die Registrierung des Gerätes nur während des Login-Prozesses initiiert werden. Im Rahmen des Geräteverifizierungsprozesses benötigt der Service eine E-Mail-Adresse des Versicherten, welche entweder durch den KTR des Versicherten bereitgestellt oder bei der Einrichtung eines Vertreters im ePA-Aktensystem hinterlegt werden muss. Nach der initialen Registrierung des Geräts erhält der Nutzer einen Verifikations-Link per E-Mail. Durch Anklicken dieses Links, der außerhalb der VAU im ePA-Aktensystem verarbeitet wird, wird das Gerät als verifiziert markiert. Der **Device Unlock Service** ist verantwortlich für das Versenden der Verifikations-E-Mail und die anschließende Verarbeitung der Bestätigung der Verifikation.

Das **Device Management** verwaltet für ein Gerät folgende Attribute:

Tabelle 2: Geräteattribute

Attribut	Beschreibung
Device Identifier	Einzigartiges Kennzeichen, das zur Identifizierung eines spezifischen Gerätes verwendet wird
Device Token	Gerätespezifisches Token
Device Verification Identifier	Gerätespezifischer Verifizierungs-Identifier
Status	Registrierungsstatus+  Zustände: <i>pending</i> oder <i>verified</i>
Created At DateTime	Erstellungsdatum der Registrierung
Display Name	Gerätename
last Login	Zeitstempel des letzten Logins

In der nachstehenden Abbildung [ePA-FdV Registrierung](#) wird konzeptionell das Zusammenspiel zwischen dem ePA-FdV, dem **Device Management** Service und dem **Device Unlock Service** bei der Geräteregistrierung dargestellt.

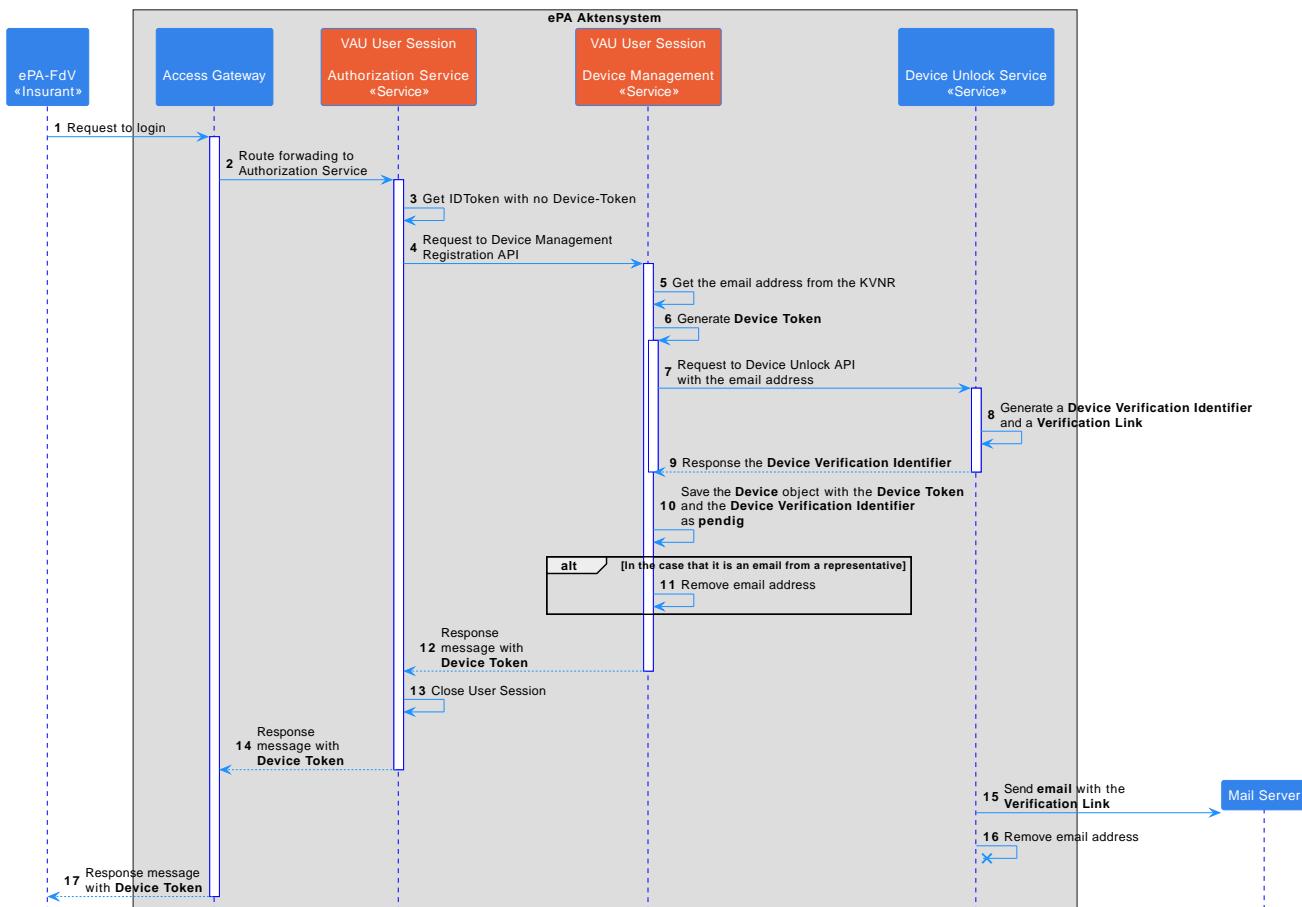


Abbildung 5: ePA-FdV Registrierung

Der **Device Unlock Service** ist dafür zuständig, den Verifikations-Link zu erstellen. Zusätzlich versendet er die Verifikations-E-Mail an den Versicherten und verantwortet die Verarbeitung des Aufrufs dieses Verifikations-Links. Der in der E-Mail enthaltene Verifikations-Link ist zeitlich limitiert und nur einmal gültig.

Eine vereinfachte Darstellung, wie der Versicherte den Verifikations-Link über sein ePA-FdV aufruft, ist in der nachfolgenden Abbildung **Geräteverifizierung** skizziert.

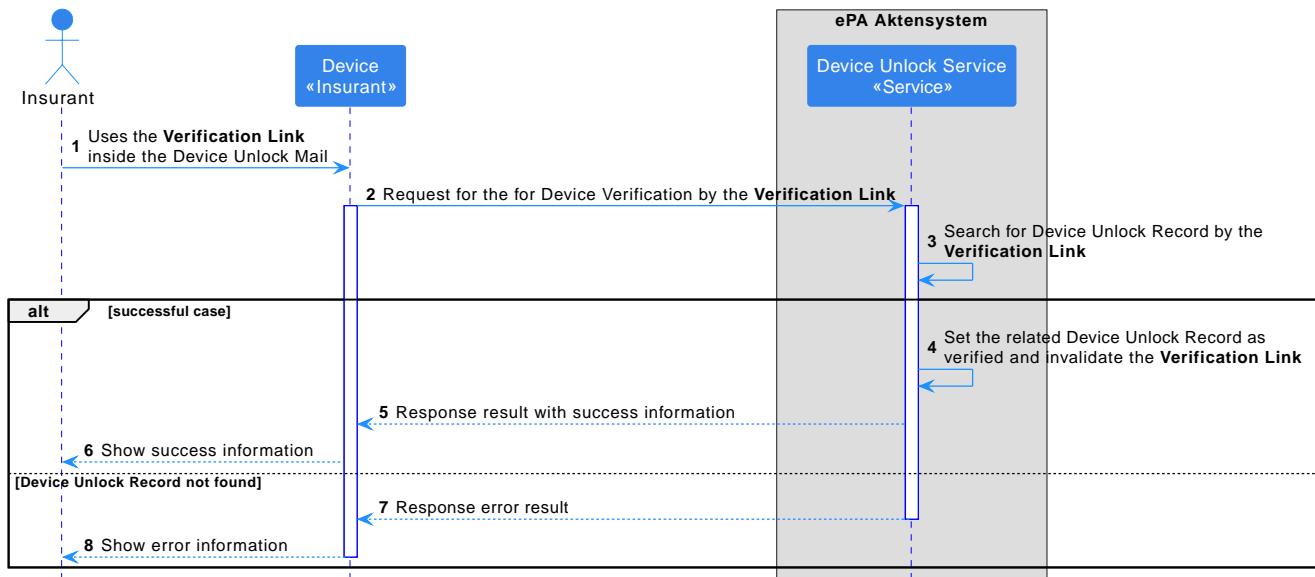


Abbildung 6: Geräteverifizierung

Bei einem ePA-FdV Login wird ein unbekanntes (nicht registriertes) oder nicht verifiziertes Gerät erkannt, woraufhin die aktuelle Anfrage abgebrochen und die **User Session** beendet wird. Der **Device Management**

Service überprüft bei einem Gerät mit dem Status *pending* beim **Device Unlock Service**, ob eine Verifizierung stattgefunden hat. Nach erfolgter Geräteverifizierung ändert der **Device Management** Service den Status des Geräts auf *verified*, wodurch keine weiteren Abfragen beim **Device Unlock Service** erforderlich sind. Die folgende Abbildung **ePA-FdV Login** skizziert konzeptionell eine Anfrage durch ein ePA-FdV.

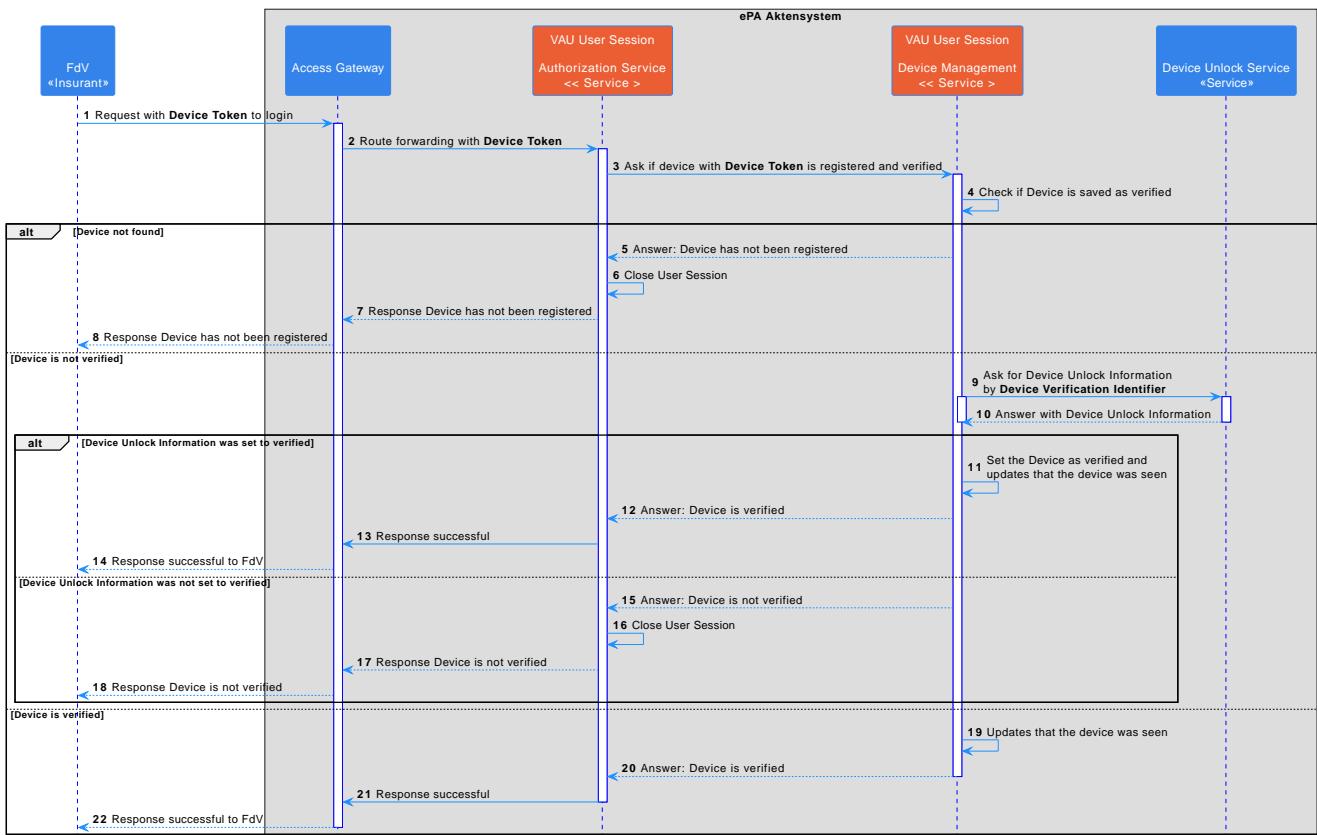


Abbildung 7: ePA-FdV Login

### 5.5.2. Auflisten und Entfernen von Geräten

Das **Device Management** bietet eine RESTful API speziell für das ePA-FdV an. Der Zugriff auf diese RESTful API ist ausschließlich innerhalb einer **User Session** möglich, die von einem authentifizierten Nutzer über das ePA-FdV initiiert wird. Über diese API werden verschiedene Attribute aller Geräte des jeweiligen Versicherten, die im System registriert sind, zur Verfügung gestellt:

- Registrierungs Status (*pending* oder *verified*)
- Erstellungsdatum der Registrierung
- Name des Gerätes (Display Name)
- Zeitstempel des letzten Logins
- Information, dass es sich um das zugreifende ePA-FdV handelt

Die RESTful API ermöglicht es, spezifische Geräte aus dem **Device Management** zu entfernen. Das Verfahren zur Bestätigung des Löschens dieser Geräte wird einzig und allein über das ePA-FdV und somit dem Versicherten zur Verfügung gestellt.

## 5.6. Audit Event Service

Die jeweiligen Services im ePA-Aktensystem protokollieren Ereignisse zum Zwecke der Datenschutzkontrolle für den Versicherten. Es werden alle Ereignisse protokolliert, die für diesen Zweck nötig sind. Dies beinhaltet insbesondere:

- alle Zugriffe und versuchten Zugriffe auf die Daten des Versicherten im XDS Document Service sowie FHIR Data Service (Medication Service),
- das Einstellen neuer Befugnisse sowie das Löschen von Befugnissen im Entitlement Management durch einen Vertreter,
- alle Änderungen im Consent Management,
- alle erfolgreichen Anmeldungen am Authorization Service,
- die Registrierung neuer Geräte im Device Management,
- den Anbieterwechsel beim Health Record Relocation Service,
- den Abruf von Protokollen beim Audit Event Service durch Vertreter oder die Ombudsstelle.

Am Protokolleintrag muss der Versicherte erkennen können, welcher Nutzer was zu welchem Zeitpunkt durchgeführt hat. Die Informationen im Protokolleintrag werden so gewählt, dass sie für den Zweck der Datenschutzkontrolle geeignet sind.

Protokolleinträge werden im Aktensystem mit dem versichertenindividuellen Befugnispersistierungsschlüssel verschlüsselt gespeichert. Protokolleinträge werden im Aktensystem für drei Jahre aufbewahrt, danach werden sie vom Aktensystem automatisch gelöscht, ohne dass dafür eine VAU benötigt würde. Die verschlüsselten Protokolleinträge werden dafür mit entsprechenden unverschlüsselten Metadaten versehen (Löschdatum).

Die Schnittstelle des Audit Event Service ermöglicht dem ePA-FdV den parametrisierten Abruf:

- von Protokolleinträgen mit Rückgabe der Menge, die die Suchparameter erfüllen und
- aller Protokolleinträge in vom Aktensystem signierter Form als PDF/A-Dokument.

Das ePA-FdV ermöglicht dem Nutzer, sich alle im Aktensystem vorhandenen Protokolleinträge in verständlicher Form anzeigen zu lassen. Dem Nutzer werden Filterfunktionen zur Verfügung gestellt. Vertreter dürfen mittels ePA-FdV ebenfalls alle Protokolleinträge des Versicherten einsehen.

Versicherte können bei ihrer zuständigen Ombudsstelle beantragen, die Protokolleinträge zur Verfügung gestellt zu bekommen. Die für den Versicherten zuständige Ombudsstelle wird als befugter Nutzer für das Aktenkonto des Versicherten bei der Anlage der Akte hinterlegt, damit diese die Protolleinträge auslesen und dem Versicherten zur Verfügung stellen kann.

Das Aktensystem stellt sicher, dass ein lesender Zugriff auf die Protokolldaten ausschließlich durch den Versicherten als Aktenkontoinhaber, einen befugten Vertreter oder die befugte Ombudsstelle erfolgen kann. Lesende Zugriffe auf die Protokolldaten durch andere Nutzer werden vom ePA-Aktensystem technisch ausgeschlossen.

Die Ombudsstelle erhält eine SM-B inkl. Authentisierungs-, Verschlüsselungs- und Signaturschlüssel sowie zugehörigen Zertifikaten. Die Zertifikate enthalten eine spezifische Rolle für Ombudsstellen.

Damit eine Ombudsstelle Protokolldaten für einen Versicherten auslesen kann, muss sie sich über den IDP-Dienst mittels des AuthN-Materials ihrer SM-B am Aktenkonto des Versicherten anmelden. In der VAU werden die Protokolleinträge dann mit dem versichertenindividuellen Befugnispersistierungsschlüssel entschlüsselt und die Ombudsstelle kann die Protokolleinträge des Versicherten vom Aktensystem abrufen.

Die Gestaltung der Identifikation des Versicherten und die Mechanismen zur Übermittlung der ausgelesenen Protokolldaten an den Versicherten obliegen der Ombudsstelle. Die gematik macht hier keine Vorgaben.

## 5.7. Anbieterwechsel

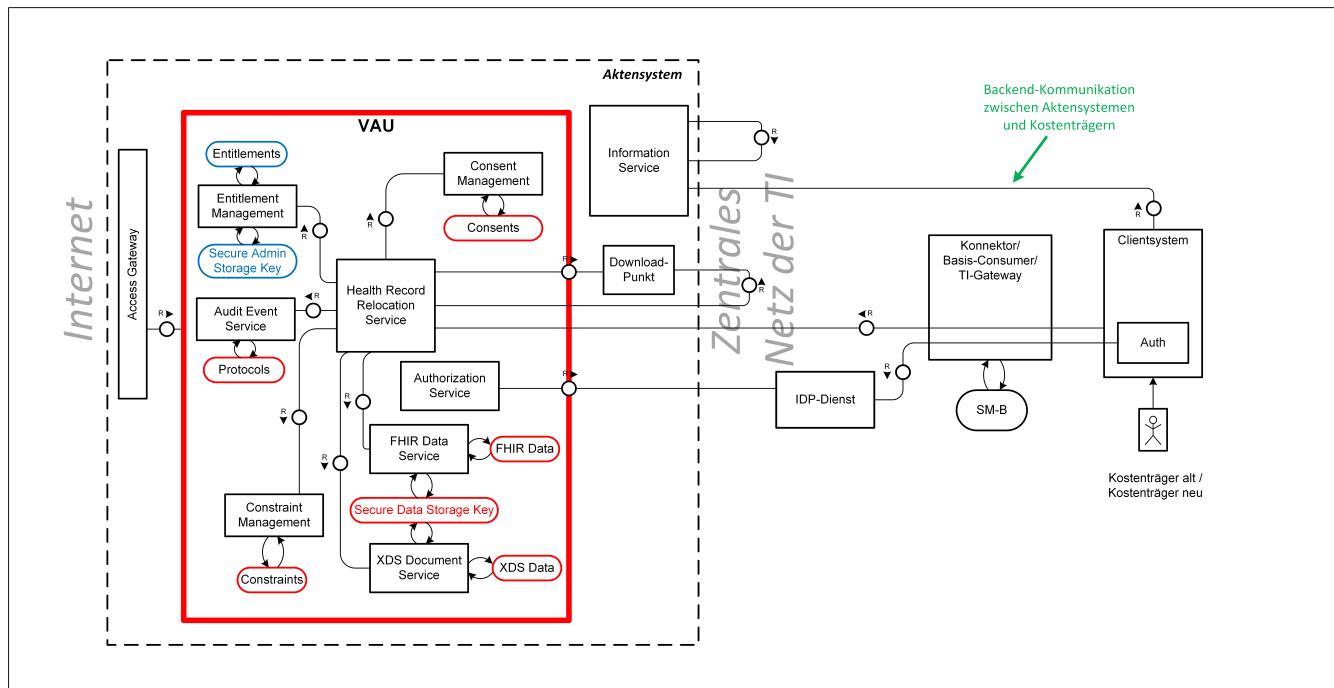


Abbildung 8: Health Record Relocation Service - Beteiligte Komponenten

In der "ePA für alle" erfolgt ein betreiberübergreifender Anbieterwechsel über das Zusammenspiel mit dem Kostenträger, bei dem der Versicherte bisher versichert war ("Kostenträger alt"), und dem Kostenträger, bei dem der Versicherte ab sofort versichert ist ("Kostenträger neu"). Die Kommunikation zwischen den Aktensystemen und den dazugehörigen Kostenträgern ist nicht normiert.

Ein Anbieterwechsel beim selben Betreiber führt lediglich zu einer Anpassung der Verwaltungsdaten und Befugnisse für den Kostenträger und für die Ombudsstelle. Der Wechsel kann daher ohne den Umweg über ein externes Export-Paket durchgeführt werden.

### 5.7.1. Betreiberübergreifender Anbieterwechsel

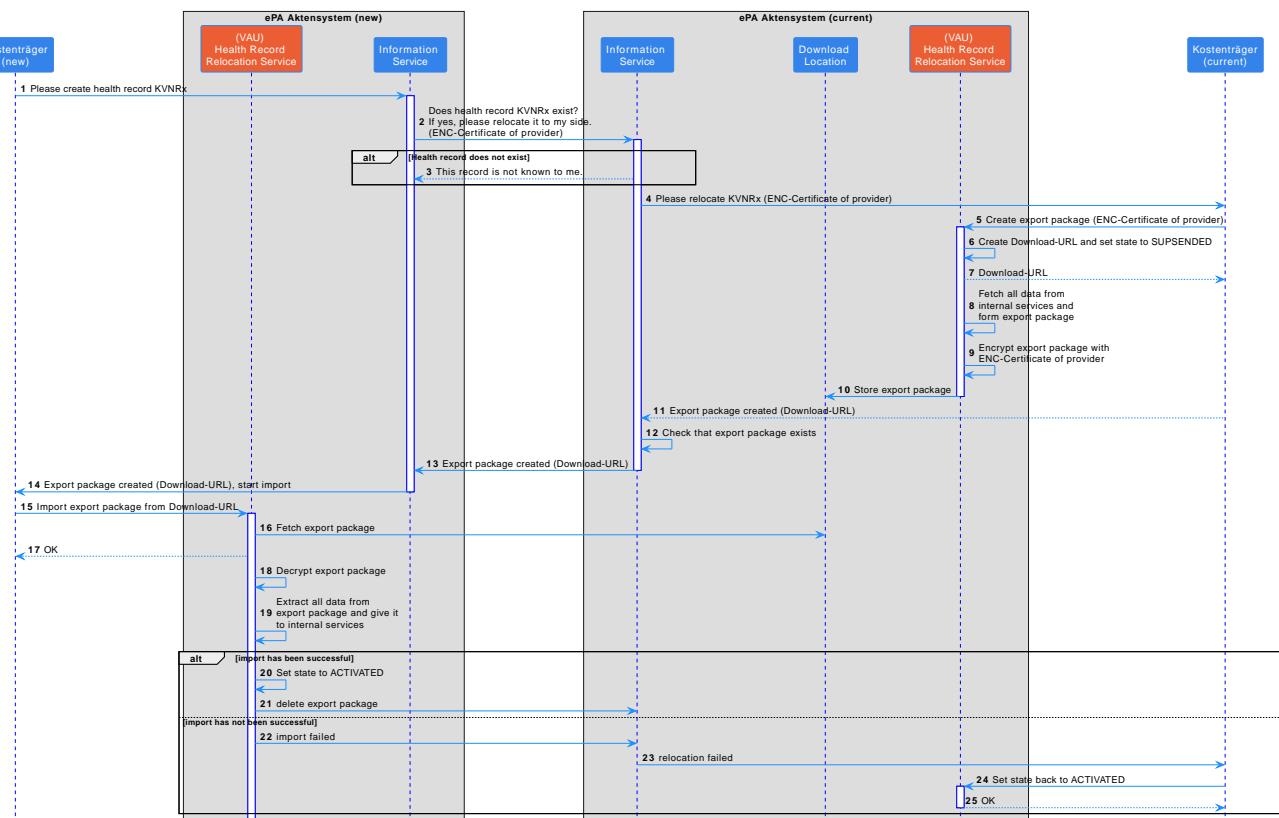


Abbildung 9: Ablauf Anbieterwechsel

### Anstoßen eines Aktentransfers

Der "Kostenträger neu" lässt im Aktensystem eine neue Akte anlegen. Das Aktensystem fragt am **Information Service** der anderen Aktensysteme nach, ob für diese KVNR schon eine Akte existiert. Sollte dies der Fall sein, wird der Anbieterwechsel angestoßen. In dieser Kommunikation wird auch das Verschlüsselungszertifikat des neuen Betreibers ausgetauscht.

Dafür informiert der **Information Service** des alten Aktensystems den "Kostenträger alt" über den Wechsel. Der "Kostenträger alt" meldet sich an der ePA an, startet die Erstellung eines Export-Pakets im **Health Record Relocation Service** und übergibt dabei das Verschlüsselungszertifikat. Der Service ändert den Status der Akte auf "Suspended" und sammelt die zu transferierenden Informationen in allen anderen internen Services ein und erstellt daraus das Export-Paket mit folgendem Inhalt:

- XDS-Dokumente mitsamt Metadaten
- FHIR-Daten aus den Versorgungsprozessen
- Zugriffsprotokolle
- Befugnisse
- Widersprüche
- Informationen zu verborgenen Dokumenten

Nachdem die Informationen im Export-Paket zusammengefasst sind, wird das Export-Paket mit dem Verschlüsselungszertifikat für die VAU des neuen Betreibers verschlüsselt.

Das verschlüsselte Export-Paket wird anschließend auf dem Download-Punkt des Aktensystems, dass bisher die Akte verwaltet hat, abgelegt und die entsprechende Download URL dem "Kostenträger alt" bekannt gemacht. Dieser übermittelt die Download URL an den **Information Service** seines Aktensystems, welches diese an den **Information Service** des neuen Aktensystems übergibt, welches schließlich die Download URL mit der Information, dass ein Anbieterwechsel ansteht, an den "Kostenträger neu" weiterleitet.

Sollte der Import des Export-Pakets nicht erfolgreich durchgeführt werden können, wird die Akte durch den "Kostenträger alt" über den **Health Record Relocation Service** wieder in den Status "Activated" gesetzt und der Export zu einem späteren Zeitpunkt erneut angestoßen.

### Import einer Akte

Der "Kostenträger neu" meldet sich an der ePA an und startet am **Health Record Relocation Service** den Import der Akte. Nachdem der **Health Record Relocation Service** das Export-Paket abgerufen und entschlüsselt hat, werden die Daten in die entsprechenden Services importiert und die Akte ist beim neuen Anbieter nutzbar – der Status wechselt auf "Activated".

### 5.7.2. Anbieterwechsel innerhalb eines Betreibers

Der Anbieterwechsel innerhalb eines Aktensystems erfolgt über die Aktenkontoverwaltung des Betreibers. Der "Kostenträger neu" teilt den Wechsel mit und hinterlegt die mit dem SMC-B Zertifikatsprofil C.HCI.OSIG selbst-signierten Befugnisse des Kostenträgers und der zuständigen Ombudsstelle im Aktensystem. Die Befugnisse werden beim nächsten Öffnen der Akte in das **Entitlement Management** importiert und ersetzen dort die bisherigen Befugnisse des Kostenträgers und der Ombudsstelle.

## 6. Medical Services

In diesem Kapitel werden technische Konzepte zu verschiedenen Medical Services der ePA dargestellt, die der Spezifikation der einzelnen Produkttypen zugrunde liegen.

In den folgenden Links werden technische Konzepte zu verschiedenen Medical Services der ePA vorgestellt, die als Basis für die Spezifikation dienen.

[Dokumentenmanagement \(XDS Document Service\)](#)

### 6.1. Versorgungsspezifische Services

Die ePA unterstützt verschiedene Versorgungsprozesse mittels dedizierter Medical Services. Initial unterstützt die Fachanwendung ePA den **digital gestützten Medikationsprozess** (dgMP) durch die Bereitstellung einer Elektronischen Medikationsliste (eML) über einen FHIR Data Service.

[Medikationsprozess \(Medication Service\)](#)

## 7. Abkürzungsverzeichnis und Glossar

### D

- dgMP – digital gestützter Medikationsprozess – Gesamtheit aller möglichen Teilprozesse des Medikationsprozesses, die ganz oder in Teilen mit strukturierten Daten elektronisch unterstützt werden
- DiGA – Digitale Gesundheitsanwendung

### E

- eML – Elektronische Medikationsliste – Neben dem eMP die Basis für den dgMP
- eMP – Elektronischer Medikationsplan

### F

- FHIR – Fast Healthcare Interoperability Resources – International etablierter IT-Standard für die Beschreibung von u.a. medizinischen Daten
- FMC – Fundamental Modeling Concepts

**G**

- GesundheitsID - Digitale Identität

**H**

- HSM – Hardware Security Module – Sicherer Speicher für kryptographische Schlüssel

**J**

- JSON – JavaScript Object Notation

**K**

- KIM – Kommunikation im Medizinwesen
- KTR – Kostenträger
- KVNR – Krankenversicherungsnummer

**L**

- LE – Leistungserbringer
- LEI – Leistungserbringerinstitution

**O**

- OTC – Over the Counter

**P**

- PZN – Pharmazentralnummer

**S**

- Sektoraler Identity Provider - Sektoraler IdP

**T**

- TI-M – Telematikinfrastruktur-Messenger (kurz: TI-Messenger) – Standard für sicheres, interoperables Instant Messaging im deutschen Gesundheitswesen

**V**

- VAU – Vertrauenswürdige Ausführungsumgebung
- VZD – Verzeichnisdienst

## 8. Anhang

# Legal Policy

Nachstehend werden die gesetzlichen Regeln für Nutzer/Berufsgruppen als Legal Policy zusammengefasst. Einzelne Zugriffsrechte werden über die grundlegenden Operationen zur Verarbeitung von Daten ausgedrückt:

- **C**reate (Erstellen)
- **R**ead (Lesen)
- **U**pdate (Aktualisieren)
- **D**elete (Löschen)

Ein Lesezugriff impliziert generell auch das Ausführen von Suchanfragen.

Tabelle 3: Legal Policy

Datenkategorie gemäß § 341 Abs. 2 SGB V		Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte											
Nr.	Technischer Identifikator	Beschreibung	Arztpraxis, Zahnarzt-praxis, Krankenhaus, Psycho-therapeut, Vorsorge- und Rehabilitation, Öffentlicher Gesundheits-dienst	Öffentlich e Apotheke	Gesundhe its-, Kranken- und Altenpflege	Geburtshil fe	Physiothe rapie	Arbeitsme dizin	Kostenträ ger	Ombudsst elle	Digitale Gesundhe its-anwendung	E-Rezept-Fachdiens t	Versichert er/ Vertreter
Medical Service «XDS Document Service»													

Datenkategorie gemäß § 341 Abs. 2 SGB V			Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte										
1a	reports	Daten zu Befunden, Diagnosen, durchgeföhrten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, Behandlungsbereichten und sonstige untersuchungs- und behandlungsbbezogene medizinische Informationen	CRUD	R	R	R	R	R	CU	-	-	-	RD
1b	emp	Daten des elektronischen Medikationsplans nach § 334 Abs. 1 S. 2 Nr. 4 SGB V	CRUD	CRUD	R	R	R	R	-	-	-	-	RD

Datenkategorie gemäß § 341 Abs. 2 SGB V			Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte											
1c	emergency	Daten der elektronischen Notfalldaten gemäß § 334 Abs. 1 S. 2 Nr. 5 und 7	CRUD	R	R	R	R	R	-	-	-	-	-	RD
1d	eab	Daten in elektronischen Briefen zwischen den an der Versorgung der Versicherten teilnehmenden Ärzten und Einrichtungen (elektronische Arztbriefe)	CRUD	R	R	R	R	R	CU	-	-	-	-	RD

Datenkategorie gemäß § 341 Abs. 2 SGB V			Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte											
2	dental	Daten zum Nachweis der regelmäßigen Inanspruchnahme zahnärztlicher Vorsorgeuntersuchungen gemäß § 55 Abs. 1 in Verbindung mit § 92 Abs. 1 S. 2 Nr. 2 (elektronische Zahnbonusheft)	CRUD	-	R	-	-	R	-	-	-	-	-	RD

Datenkategorie gemäß § 341 Abs. 2 SGB V			Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte											
3	child	Daten gemäß § 92 Absatz 1 Satz 2 Nummer 3 und Absatz 4 in Verbindung mit § 26 beschlossenen Richtlinie des Gemeinsamen Bundesausschusses zur Früherkennung von Krankheiten bei Kindern (elektronische Untersuchungssheft für Kinder)	CRUD	R	R	CRUD	R	R	-	-	-	-	-	RD, CU(*)

Datenkategorie gemäß § 341 Abs. 2 SGB V			Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte											
			CRUD	R	R	CRUD	R	R	-	-	-	-	-	RD
4	pregnancy_childbirth	Daten gemäß § 92 Abs. 1 S. 2 Nr. 4 in Verbindung mit den §§ 24c bis 24f beschlossenen Richtlinie des Gemeinsamen Bundesausschusses über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass) sowie Daten, die sich aus der Versorgung der Versicherten mit Hebammenhilfe ergeben												

Datenkategorie gemäß § 341 Abs. 2 SGB V			Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte											
5	vaccination	Daten der Impfdokumentation nach § 22 des Infektionsschutzgesetzes (elektronische Impfdokumentation)	CRUD	CRUD	R	R	-	CRUD	-	-	-	-	-	RD
6	patient	Gesundheitsdaten, die durch den Versicherten bereit gestellt werden	RD	R	R	R	R	R	-	-	-	-	-	CRUD
8	receipt	Bei Kostenträgern gespeicherte Daten über die in Anspruch genommenen Leistungen des Versicherten	RD	RD	-	R	R	R	CU	-	-	-	-	RD

Datenkategorie gemäß § 341 Abs. 2 SGB V			Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte											
8	diga	Daten des Versicherten aus digitalen Gesundheitsanwendungen des Versicherten nach § 33a SGB V	R	R	R	R	R	R	-	-	CU	-	RD	
10	care	Daten zur pflegerischen Versorgung des Versicherten gemäß §§ 24g, 37, 37b, 37c, 39a und 39c und der Haus- oder Heimpflege gemäß § 44 des Siebten Buches und nach dem Elften Buch	CRUD	R	CRUD	R	R	R	-	-	-	-	RD	

Datenkategorie gemäß § 341 Abs. 2 SGB V			Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte											
12	eau	Daten gemäß § 73 Abs. 2 S. 1 Nr. 9 SGB V ausgestellte Bescheinigung über eine Arbeitsunfähigkeit	CRUD	-	-	-	-	-	R	-	-	-	-	RD
13	other	Sonstige von Leistungserbringern für Versicherten bereitgestellte Daten, insbesondere Daten, die sich aus der Teilnahme des Versicherten an strukturierten Behandlungsprogrammen bei chronischen Krankheiten gemäß § 137f ergeben	CRUD	-	-	-	-	-	R	-	-	-	-	RD

Datenkategorie gemäß § 341 Abs. 2 SGB V			Zugriffsrecht für Berufsgruppen gemäß § 352 SGB V (hier abgeleitete Betriebsstätten), Fachdienste und Versicherte												
14	rehab	Daten der Heilbehandlung und Rehabilitation gemäß § 27 Abs. 1 des Siebten Buches	CRUD	-	-	-	-	-	-	-	-	-	-	-	RD
--	audit	Protokolle von Zugriffen seitens Leistungserbringer auf die Akte des Versicherten gemäß § 309 Abs. 1 SGB V	-	-	-	-	-	-	-	R	-	-	-	-	R

#### Medical Service «Medication Service»

11	medication	Verordnungs-, Dispensier- und Medikationsdaten in einer Elektronischen Medikationsliste (eML)	R	R	R	R	-	R	-	-	-	-	CU	R
----	------------	---	---	---	---	---	---	---	---	---	---	---	----	---

(\*) Der Einsteller einer Elternnotiz eines Kinderuntersuchungshefts kann neben einer Leistungserbringerinstitution der Versicherte bzw. sein Vertreter sein.