1.1 Hintergrund und Ziele zur ePA

Viele der für den Versicherten wichtige Informationen über seine Gesundheit sind derzeit nur in den Datenspeichern der Arztpraxen verfügbar. Geht der Versicherte dann zu einem anderen Arzt, liegen viele dieser Informationen über ihn nicht vor und Untersuchungen müssten ggfs. wiederholt werden.

Ab 2021 können alle gesetzlich Versicherten auf freiwilliger Basis eine elektronische Patientenakte (ePA) ihrer Krankenkassen erhalten. Mit Inkrafttreten des Terminservice- und Versorgungsgesetzes (TSVG) werden die gesetzlichen Krankenkassen verpflichtet, ihren Versicherten spätestens ab dem 1. Januar 2021 eine von der Gesellschaft für Telematik mbH (gematik) zugelassene elektronische Patientenakte (ePA) anzubieten. Die ePA soll jedem Versicherten der GKV lebenslang zur Verfügung gestellt werden.

2 Funktionsumfang

Grundlage der ePA bilden die fachlichen und technischen Vorgaben der gematik, welche zum Zeitpunkt des Vertragsschlusses in Form von Konzepten, Spezifikationen und Produkttypsteckbriefen im Fachportal der gematik (https://fachportal.gematik.de) veröffentlicht worden sind.

2.1 Abgrenzung Funktionsumfang

Bestandteil dieser Leistungsbeschreibungsversion sind die gematik Spezifikationen der Stufe 1 inkl. der Übergangsregelung ePA, sowie die Stufe 2:

- Stufe 1 (Produktivtermin 01.01.2021):
  - ePA-Aktensystem sowie FdV ohne Vertreterregelung und ohne Anbieterwechsel
- Stufe 2 (Produktivtermin 01.01.2022):
  - ePA-Aktensystem sowie FdV mit Vertreterregelung und mit Anbieterwechsel
  - Bereitstellung KTR-Consumer
  - Feingranulares Berechtigungskonzept
  - Unterstützung der Passtechniken (Mutterpass, Impfpass, etc.)

Nicht Bestandteil dieser Leistungsbeschreibungsversion sind die Funktionalitäten der weiteren Folgestufen (ab Stufe 3 ff.) sowie das zukünftig geplante „AdV- / TI-Terminal“ aus der ePA Stufe 2.

2.2 Abgrenzung zur elektronischen Gesundheitsakte (eGA)

Die ePA wird definiert durch die gematik; gesetzliche Grundlage ist § 291a SGB V. Daneben existieren bereits verschiedene sogenannte elektronische Gesundheitsakten, die einzelne Krankenkassen ihren Versicherten als Satzungsleistung bereitstellen können; gesetzliche Grundlage hierfür ist § 68 SGB V. Die elektronische Gesundheitsakte soll nach derzeitiger Kenntnis perspektivisch abgelöst und in die einheitliche ePA integriert werden.

3 Leistungsüberblick ePA

3.1 Komponenten und deren Funktionen

Die ePA von BITMARCK stellt alle durch die gematik vorgegebenen Funktionen zur Verfügung:

3.1.1 ePA-Aktensystem (Datenspeicher)

Das ePA Aktensystem besteht aus den folgenden Komponenten:

1. Dem Zugangsgateway, mit den Aufgaben der:

- sicheren Anbindung der Geräte des Versicherten und
- der Steuerung der Kommunikation mit den Komponenten
    - Authentisierung,
    - Autorisierung,
    - Dokumentenverwaltung und
    - dem Schlüsselgenerierungsdienst und dem Verzeichnisdienst.

2. Der Authentisierung mit folgenden Funktionen:

- Authentisierung von Versicherten
- Authentisierung von Vertretern
- Ansprache durch FdV und Fachmodul ePA im Konnektor
- Ausstellung der Authentisierungs-Token

3. Der Autorisierung und Schlüsselverwaltung:

- Zentrale Verwaltung des empfängerbezogenen, verschlüsselten Schlüsselmaterials (Akten- und Kontextschlüssel) für alle Nutzer.
- Übergabe des verschlüsselten Schlüsselmaterials nach erfolgreicher Authentifizierung an das FdV oder das Fachmodul ePA im Konnektor.

4. Der Dokumentenverwaltung:

- Speichert mit dem Aktenschlüssel verschlüsselte Dokumente
- Verwaltet Metadaten
- Verwaltet Policy-Dokumente (Teil der Berechtigungsvergabe)
- Schnittstellen basieren auf Integrating the Healthcare Enterprise (IHE)
- Beinhaltet die vertrauenswürdige Ausführungsumgebung VAU für eine sichere Laufzeitumgebung

3.1.2 Frontend des Versicherten (FdV)

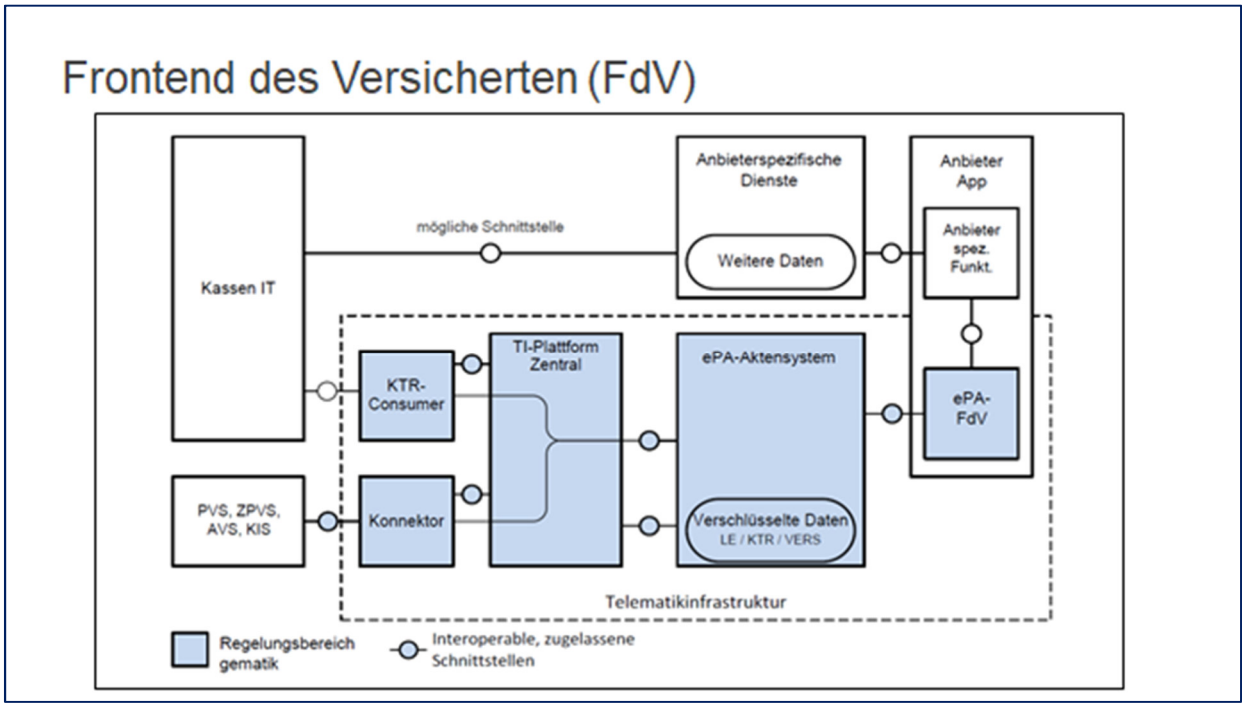

Abbildung 1: Frontend des Versicherten (FdV)

Der Zugang des Versicherten zur ePA wird durch das sog. Frontend des Versicherten (FdV) ermöglicht. BITMARCK stellt das FdV in zwei Ausprägungen zur Verfügung:

- **FdV als eigenständige App**

  Die ePA-Funktionen des FdV sind in einer eigenständigen von der gematik zugelassenen App gebündelt und stehen für den Versicherten im jeweiligen Store des Plattformanbieters (Apple, Google) zum Download zur Verfügung.

  Das Branding der FdV wird durch jede Krankenkasse (Kassenlogo, Farben, etc.) eigenständig individualisiert. Für das Branding stellt BITMARCK ein Branding-Tool über das BITMARCK-Kundenportal zur Verfügung.

- **FdV als Modul**

  Die ePA-Funktionen sind in einem FdV-Modul (Software Development Kit) enthalten und müssen für die Nutzung durch den Versicherten durch die jeweilige Krankenkasse in die App integriert werden. Für diese Integration durch den Lizenznehmer stellt BITMARCK eine technische Dokumentation als Hilfestellung zur Verfügung. Die jeweils aktuellste Version steht im BITMARCK-Kundenportal zur Verfügung.

3.1.2.1 Bereitstellung des FdV in den Stores

Die erstmalige Bereitstellung des FdV in den jeweiligen Stores (Android/Apple) erfolgt durch die Firma RISE als Unterauftragnehmer von BITMARCK.

Die hierfür erforderlichen Zulieferungen sind durch den Lizenznehmer im Rahmen der Mitwirkungspflichten (siehe Kapitel □ „Mitwirkungspflichten des Lizenznehmers“) zu leisten.

Folgebereitstellungen des FdV mit neuen Anpassungen und notwendigen Änderungen erfolgen selbständig durch den Lizenznehmer oder durch einen vom Lizenznehmer beauftragtem Dienstleister.

3.1.2.2 Technische Voraussetzung für die Nutzung des FdV

Die Nutzer des FdV können die Nutzung der ePA-App nur mit den folgenden technischen Voraussetzungen nutzen.

- Alle Smartphones und Tablets mit den folgenden Betriebssystemen:
  - Android Betriebssystem ab Version 8 und (empfehlenswert) mit Near Field Communication Funktion (NFC)
  - Apple iOS Betriebssystem ab Version 13

3.1.3 SigD Authentisierung durch Nutzung von al.vi ohne eGK am mobilen Endgerät

- Das TSP X.509 der eGK, liefert Zertifikate und Schlüssel für die Authentisierung. Alternativ zur eGK wird das alternative Auth-Zertifikat sowie der „private Schlüssel“ im Signaturdienst genutzt.
- Der Signaturdienst (SigD) sorgt für die sichere Zwei Faktor Authentisierung (2FA), für die Freischaltung des privaten Schlüssels im Signaturdienst und für die Signatur des alternativen Auth Zertifikats.
- Als weiterer Bestandteil des Signaturdienstes steht für die Versicherten des Auftraggebers ein Sperrdienst zur Verfügung. Über diesen Sperrdienst werden Sperraufträgen der Sperrberechtigten entsprechend der gematik Spezifikationen entgegengenommen.
- Der Sperrdienst steht den Sperrberechtigten über einen Self-Service bereit. Der Aufruf erfolgt über einen Link bzw. über eine Webseite, über die der Versicherte nach erfolgreicher Authentisierung einen Sperrauftrag erteilen kann.

3.1.4 KVS – Kontoverwaltungssystem (Aktenverwaltung)

Gemäß der gematik Vorgaben wurde eine technische Schnittstelle im ePA-Aktensystem implementiert, die es einem „Kontoverwaltungssystem“ ermöglicht, den Zustandswechsel im Lebenszyklus einer Akte umzusetzen. Hierzu gehören z.B.:

- Die Kontoeröffnung (Aktenkonfiguration hinterlegen)
- Akten-Suspendierung für Anbieterwechsel, bzw. Deaktivierung und Löschung.
- Im ersten Release des KVS werden beispielsweise diese Anwendungsfälle umgesetzt:
- Registrierung zur Initialisierung eines ePA-Aktenkontos.
- Dokumentation der Einwilligungserklärung und Einsicht in die Einwilligungserklärung.
- Schließen einer ePA, z.B. bei Widerruf der Einwilligungserklärungen sowie Löschen der in der ePA vorgehaltenen Daten auf Wunsch des Versicherten.
- Dokumentation und Beauskunften der Aktivitäten inkl. Status auf Basis eines Versicherten.

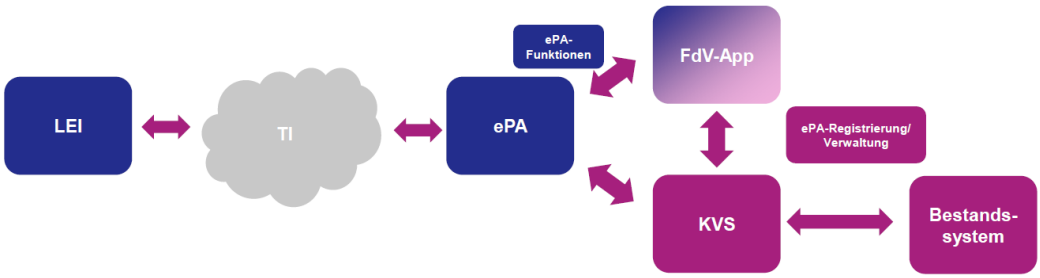

Abbildung 4: Zusammenhang TI mit ePA

3.1.5 IAM (Identity- and Access Management) für die Zugriffs- und Berechtigungsverwaltung

Die Einführung eines Identity and Access Managements (IAM) dient zur sicheren und flexiblen Identifizierung und Authentifizierung des Versicherten.

An einer zentralen Stelle werden die Versicherten als Online-Benutzer gepflegt und können mit Standard-Verfahren wie OAuth2 / OpenID Connect für Single-Sign-On in bestehenden Anwendungen eingebunden werden. Damit werden die Anforderungen des § 217f SGB V aber auch der gematik im Kontext ePA erfüllt.

Der Sperrdienst steht allen Krankenkassen zur Verfügung und die Kosten sind Bestandteil des ePA-Vertrages, die Bereitstellung selbst ist Bestandteil des Signaturdienstes. BITMARCK stellt hierzu einen Link zur Verfügung der vom Lizenznehmer für seine Versicherten angeboten werden kann.

3.1.6 KTR-Consumer

Der KTR-Consumer ermöglicht es, Mitarbeitern der gesetzlichen Krankenkassen als Nutzer an der TI teilzunehmen. Genutzt werden können dabei Fachanwendungen (Unterstützung von sicheren Übermittlungsverfahren (KIM) und ePA (Einstellen von Sozialdaten durch die gesetzliche Krankenkasse in die ePA über ein ePA-Fachmodul)), bei denen die Krankenkassen als berechtigte Nutzer festgelegt sind.

Der Produkttyp KTR-Consumer (gematik Spezifikation: gemZul_Prod_KTR-Consumer_V1.0.0) enthält Fachmodule und das Clientmodul KIM zur Nutzung des sicheren Übermittlungsverfahrens.

In seinen Leistungen deckt der KTR-Consumer alles ab, was laut gematik Spezifikation ein Basis-Consumer leistet.

In Hinblick auf die ePA, ermöglicht der KTR-Consumer zusätzlich auch die Bereitstellung von Abrechnungsdaten gemäß § 305 SGB V in das ePA-Aktensystem.

4 Sicherheit

Neben den Anforderungen der gematik, wurden bei der Entwicklung der ePA gängige Sicherheitsstandards angewandt. Insbesondere gilt hier, dass moderne Verschlüsselungsmethoden gemäß BSI und gematik unterstützt werden.

Die Kommunikation zwischen den betreffenden Systemen erfolgt auf gesicherten Übertragungswegen. Änderungen an den Systemen sind nachvollziehbar:

- Wer hat was wann geändert?
- Revisionssichere Protokollierung der Ereignisse;
- Alarmierung bei Verletzung der Vorgaben.