Die elektronische Patientenakte (ePA) der KKH

Die KKH ePA dient der Verwaltung von medizinischen Dokumenten in einer elektronisch geführten Akte in einem hochsicheren System in Deutschland.

Die Nutzung der ePA ist freiwillig.

Der Nutzer meldet sich über die KKH-ePA-App gesichert in seiner Akte an. Dort kann er oder ein Leistungserbringer, den er berechtigt hat, Dokumente verwalten. Zum Verwalten gehören hochladen, ansehen und löschen. Dokumente des Nutzers kann nur der Nutzer löschen.

Der Nutzer berechtigt einen Leistungserbringer über ein Leistungserbringerverzeichnis, das in der KKH ePA-App angezeigt wird und in dem der Leistungserbringer eingetragen sein muss. Das Leistungserbringerverzeichnis wird durch die Leistungserbringer gepflegt.

Die Berechtigungsvergabe erstreckt sich im Jahr 2021 auf den gesamten Akteninhalt. Die Berechtigung kann vom Nutzer zeitlich begrenzt und jederzeit entzogen werden.

Der Zugang zur ePA erfolgt über die KKH ePA-App grundsätzlich mittels NFC-eGK und PIN.

Es wird auch ein sogenannten Komfortzugriff, die alternativen Versichertenidentität (al.vi) angeboten. Hier wird nur neben der Gerätebindung ein Passwort verlangt, was entsprechende Unsicherheiten birgt.

Betreiber der KKH ePA ist die Bitmarck Unternehmensgruppe mit der Firma Research Industrial Systems Engineering („RISE“).

Im folgenden Dokument finden Sie eine weitergehende Produktbeschreibung

Produktbeschreibung der KKH ePA (elektronische Patientenakte)

Inhaltsverzeichnis

1 Einführung

Die BITMARCK-Unternehmensgruppe kümmert sich als sozialrechtliche Arbeitsgemeinschaft um die wesentlichen Belange ihrer Gesellschafter in allen wesentlichen IT-Angelegenheiten.

In Abstimmung mit dem Aufsichtsrat (Entscheidung vom 12. März 2019) hat BITMARCK die Aufgabe übernommen, eine zentrale Beschaffung der elektronischen Patientenakte (ePA) vorzunehmen. Damit wurde ermöglicht, dass BITMARCK den Versicherten der angeschlossenen Gesellschafterkassen eine ePA zur Verfügung stellt.

Die zentrale Beschaffung über die Arbeitsgemeinschaft BITMARCK ist aus Sicht der betreffenden Krankenkassen insbesondere unter Wirtschaftlichkeitsgesichtspunkten sinnvoll.

1.1 Hintergrund und Ziele zur ePA

Viele der für den Versicherten wichtigen 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 die das wollen 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 zeitlich unbegrenzt zur Verfügung gestellt werden.

2 Funktionsumfang

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

2.1 Abgrenzung Funktionsumfang

Bestandteil dieser Produktbeschreibung sind die gematik Spezifikationen der Stufe 1:

- Stufe 1 (Produktivtermin 01.01.2021):
    - ePA-Aktensystem sowie Frontend des Versicherten (FdV) ohne Vertreterregelung und ohne Anbieterwechsel

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

3 Leistungsüberblick ePA

3.1 Funktionale Zerlegung der ePA

In der nachfolgenden Grafik wird die funktionale Zerlegung entsprechend der gematik Systemlösung ePA dargestellt:

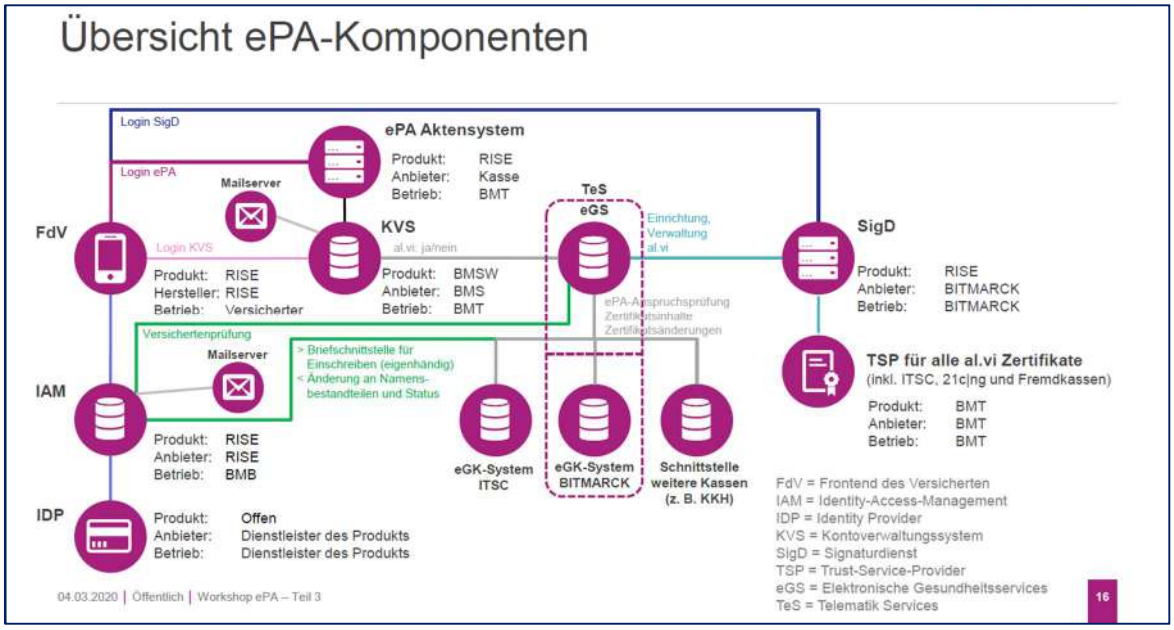

Abbildung 1: Übersicht der ePA Komponenten

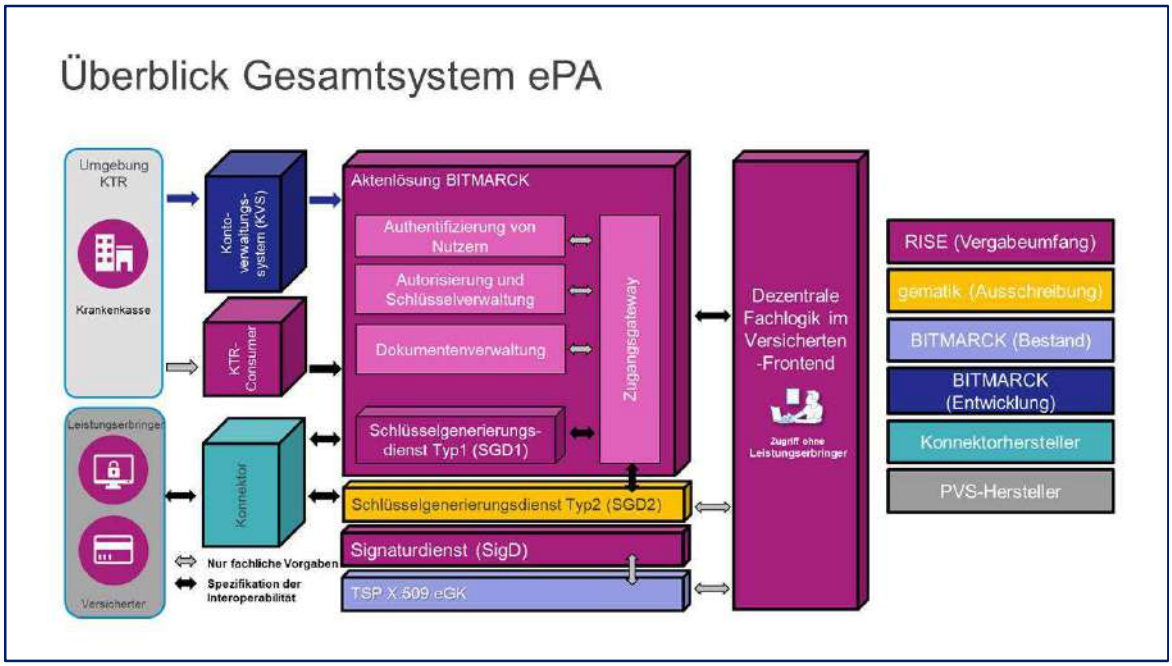

Abbildung 2: Überblick des Gesamtsystems ePA

3.2 Komponenten und deren Funktionen

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

3.2.1 ePA-Aktensystem (Datenspeicher)

Das ePA Aktensystem besteht aus den folgenden Komponenten:

1. Dem Zugangsgateway, mit den Aufgaben der:
    - sicheren Anbindung der Geräte des Versicherten
    - steuert die Kommunikation mit den Komponenten:
        - Authentisierung (wer bist du?)
        - Autorisierung (darf der das?)
        - Dokumentenverwaltung
        - dem Schlüsselgenerierungsdienst und dem Verzeichnisdienst der Leistungserbringer

2. Der Authentisierung mit folgenden Funktionen:
    - Authentisierung von Versicherten
    - Authentisierung von Vertretern
    - Wird von der KKH ePA - App und vom Praxisverwaltungssystem des Arztes aufgerufen,
    - und stellt Authentisierungs-Token aus.

3. Der Autorisierung und Schlüsselverwaltung:
    - Zentrale Verwaltung des empfängerbezogenen, verschlüsselten Schlüsselmaterials (Akten- und Kontextschlüssel) für alle Nutzer.
    - Übergibt nach erfolgreicher Authentifizierung das verschlüsselte Schlüsselmaterial an die KKH ePA-App oder in das Praxisverwaltungssystem beim Arzt.

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

3.2.2 Frontend des Versicherten (FdV) – KKH ePA-App

Der Zugang des Versicherten zur ePA wird durch die KKH ePA-App ermöglicht.

- **KKH ePA-App**

  Die ePA-Funktionen der KKH ePA-App 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.

3.2.2.1 Bereitstellung der KKH ePA-App in den Stores

Die erstmalige Bereitstellung der KKH ePA-App in den jeweiligen Stores (Android/Apple) erfolgt durch die BITMARCK.

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

- Die elektronische Gesundheitskarte (eGK), liefert Zertifikate und Schlüssel für die Authentisierung. Alternativ zur eGK wird ein alternatives 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.

3.2.4 KVS - Kontoverwaltungssystem (Aktenverwaltung)

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

- Die Kontoeröffnung (Aktenkonfiguration hinterlegen)
- Akten-Schließung 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.

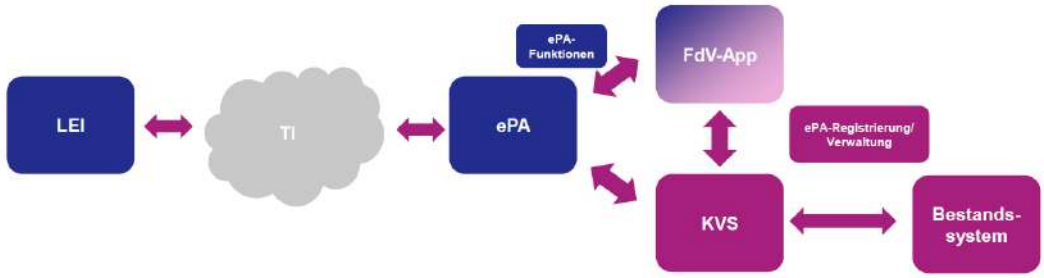

Abbildung 3: Zusammenhang TI mit ePA

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

Die Einführung eines Identity- and Accessmanagements (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-Authentisierungsverfahren in bestehenden Anwendungen eingebunden werden. Damit werden die Anforderungen des § 217f SGB V, aber auch der gematik im Kontext ePA erfüllt.

4 Sicherheit ePA

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.

5 Abbildungsverzeichnis