gematik

Wir sorgen für die Sicherheit der Gesundheitsdaten

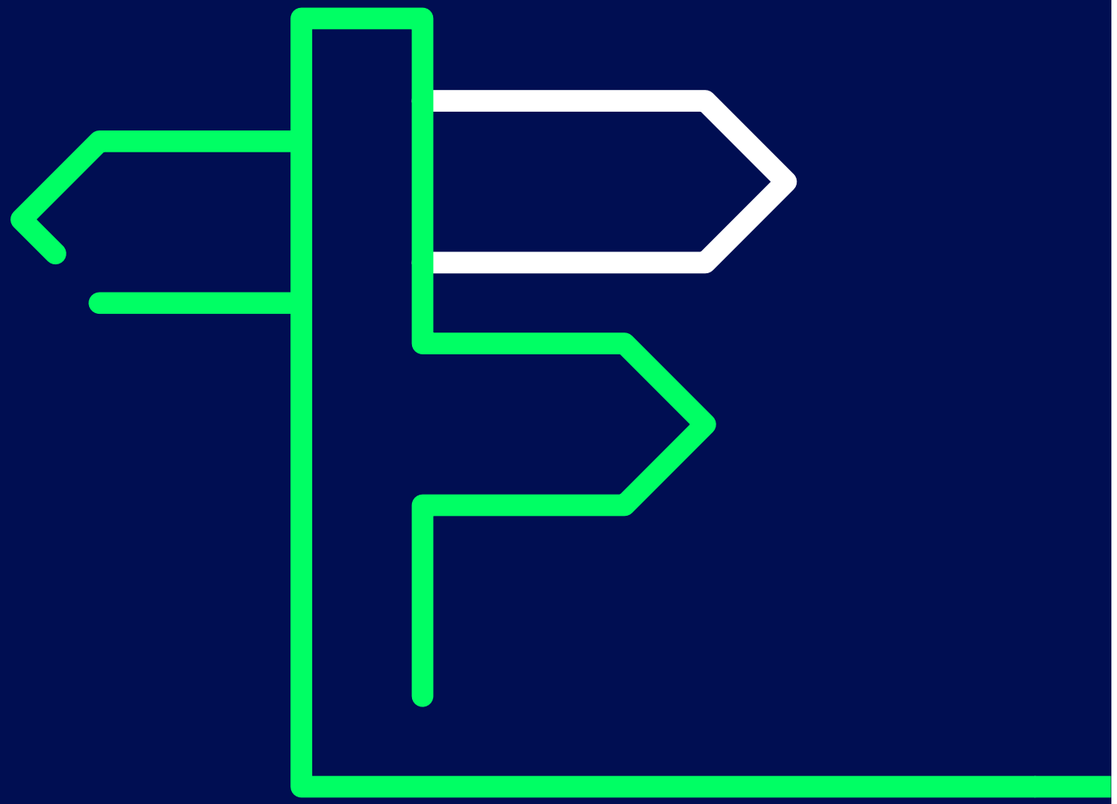
Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur

Inhalt

Gender-Hinweis:
Zugunsten des Leseflusses wird in dieser Publikation meist die männliche Form verwendet.
Wir bitten, dies nicht als Zeichen einer geschlechtsspezifischen Wertung zu deuten.

1 Einleitung

Gesundheitsdaten bedürfen eines besonderen Schutzes. Die Versicherten haben das Recht, selbst zu bestimmen, welche personenbezogenen Daten sie von sich preisgeben möchten und wer sie verwenden darf. Dieses Recht auf informationelle Selbstbestimmung hat auch der Gesetzgeber im Blick. Daher stehen der Datenschutz und die Informationssicherheit beim Aufbau einer digitalen Gesundheitsinfrastruktur in Deutschland im Mittelpunkt.



Datenschutz und Informationssicherheit unterscheiden sich in ihren Zielen: Datenschutz wahrt Persönlichkeits- und Freiheitsrechte, Informationssicherheit schützt Informationen. Bei der Informationssicherheit geht es also nicht zwangsläufig um personenbezogene Daten, sondern etwa um Geschäftsgeheimnisse. Datenschutz und Informationssicherheit überschneiden sich jedoch, wenn die Informationssicherheit zum Schutz von personenbezogenen Angaben eingesetzt wird, etwa beim Verschlüsseln von Patientendaten.

Telematikinfrastruktur – ein sicheres digitales Gesundheitsnetz

Die gematik wird im § 311 des Sozialgesetzbuches (SGB) V damit beauftragt, eine sichere digitale Gesundheitsinfrastruktur – die sogenannte Telematikinfrastruktur – in Deutschland aufzubauen. Darüber können Patientendaten sicher zwischen den berechtigten Teilnehmern ausgetauscht werden. Rund 74 Millionen gesetzlich Versicherte [1], 153.000 niedergelassene Ärzte und Zahnärzte [1], 17.288 Apotheken [1], 1.874 Krankenhäuser [1] und 95 Krankenkassen [2] nutzen die Telematikinfrastruktur. Daher ist es zentral, dass die Telematikinfrastruktur für alle diese Nutzer eine sichere Basis für medizinische Anwendungen bietet.

Datenschutz hat hohe Priorität

Die neuen technischen Möglichkeiten, medizinische Informationen über die Telematikinfrastruktur auszutauschen, werfen Fragen im Bereich des Datenschutzes auf. Versicherte müssen in jedem Fall darauf vertrauen können, dass das Arztgeheimnis gewahrt bleibt. Denn nur so kann das Vertrauensverhältnis zwischen den Heilberuflern und ihren Patienten aufrechterhalten werden. Auch Heilberufler haben ein Interesse am Schutz der Daten, die innerhalb der Telematikinfrastruktur transportiert werden. Denn als Berufsgeheimnisträger unterliegen sie besonders strengen Regelungen.

Der Gesetzgeber hat daher zusammen mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit spezielle Regelungen des Datenschutzes für die Telematikinfrastruktur formuliert. Diese ergänzen die geltenden Datenschutzregelungen, insbesondere der europäischen Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes und des Sozialgesetzbuches X. Datenschutz wird von der Telematikinfrastruktur in ihrer Gesamtheit gewährleistet.

Hohes Informationssicherheitsniveau

Um diesen Datenschutzanforderungen gerecht zu werden und insbesondere die medizinischen Daten von Versicherten zu schützen, verfolgt die Telematikinfrastruktur strenge Grundsätze und hat entsprechende Mechanismen etabliert. Dabei geht es vor allem darum, dass die Kommunikationspartner eindeutig identifizierbar sind und sicher und verschlüsselt kommunizieren können. Außerdem darf kein unbefugter Zugriff auf sensible Informationen möglich sein.

Zielgruppen des Whitepapers

Das Whitepaper richtet sich in erster Linie an die Versicherten und Heilberufler, die sich näher mit dem Datenschutz und der Informationssicherheit in der Telematikinfrastruktur befassen möchten. Es ist aber auch für alle Menschen gedacht, die sich für die Digitalisierung und die damit verbundenen Neuerungen interessieren.
Die Anwendungen der Telematikinfrastruktur werden nach und nach eingeführt. Das Whitepaper beschreibt, wie in der aktuellen Ausbaustufe der Telematikinfrastruktur Datenschutz und Informationssicherheit gewährleistet werden. Auf technische Details wird nur dann eingegangen, wenn sie für das Verständnis notwendig sind.

2 Strategie Datenschutz und Informationssicherheit

Die gematik hat eine Strategie ausgearbeitet, um das erforderliche Datenschutz- und Informationssicherheitsniveau in der Telematikinfrastruktur zu gewährleisten. Dabei folgt sie vier Grundsätzen.

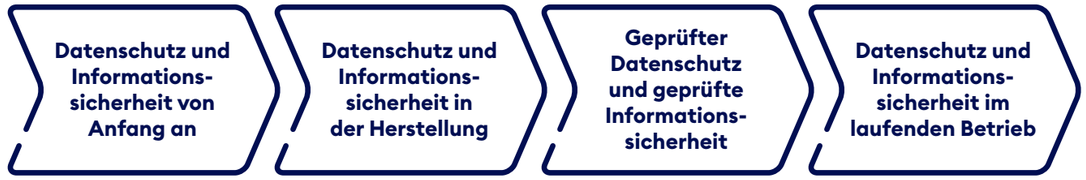


Abbildung 1 – Datenschutz und Informationssicherheit im gesamten Lebenszyklus der Telematikinfrastruktur

Datenschutz und Informationssicherheit von Anfang an

Bereits im Entwurfsstadium werden Datenschutz und Informationssicherheit berücksichtigt, sowohl bei der Erstellung von technischen Spezifikationen als auch bei der Entwicklung von Anwendungen, Komponenten und Diensten der Telematikinfrastruktur. Dies geschieht in enger Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die erarbeiteten Konzepte für eine Anwendung, eine Komponente bzw. einen Dienst der Telematikinfrastruktur werden sodann von datenschutzrechtlichen Aufsichtsbehörden oder Sicherheitsprüfstellen geprüft und bewertet. Die gematik veröffentlicht alle technischen Vorgaben [3]. So können sie auch von den Versicherten und interessierten Dritten eingesehen werden.

Datenschutz und Informationssicherheit in der Herstellung

Die Herstellung von Komponenten und Diensten der Telematikinfrastruktur nach den Anforderungen aus den Spezifikationen erfolgt ebenfalls nach Vorgaben der gematik. Die Hersteller müssen nachweisen, dass ihre Entwicklungs- und Testumgebungen sicher betrieben werden, nachweisbar geschultes Personal für die sichere Herstellung eingesetzt wird, sichere Softwareentwicklungsprozesse etabliert sind und sie über genügend Ressourcen verfügen, um die notwendigen Tests durchführen zu können. Den Nachweis müssen die Hersteller gegenüber der gematik im Rahmen der Zulassung erbringen.

Prüfung bei Zulassung

Alle Komponenten und Dienste in der Telematikinfrastruktur müssen zunächst von der gematik zugelassen werden. Dafür ist der Nachweis erforderlich, dass die Produkte sämtliche Anforderungen an den Datenschutz und die Informationssicherheit erfüllen. Eine Sicherheitsevaluation durch das Bundesamt für Sicherheit in der Informationstechnik (bei technischen Komponenten wie etwa Karten) oder ein Gutachten (bei zentralen Diensten) kann diesen Nachweis erbringen. Das Bundesamt für Sicherheit in der Informationstechnik und die gematik haben die Vorgaben für diese Prüfung gemeinsam erstellt. Nur Sachverständige, die vom Bundesamt für Sicherheit in der Informationstechnik anerkannt wurden, dürfen die technischen Komponenten prüfen. Die Sachverständigen, die die zentralen Dienste begutachten, haben eine entsprechende Zusatzqualifikation erworben. Zusätzlich testen die Hersteller und Anbieter sowie die gematik selbst die Komponenten und Dienste. Erst wenn alle Schritte erfolgreich durchlaufen wurden, kann eine Komponente oder ein Dienst zugelassen und in der Telematikinfrastruktur eingesetzt werden.

Sicherstellung im laufenden Betrieb

Nachdem Komponenten und Dienste zugelassen wurden und an den Start gegangen sind, muss ihr datenschutzkonformer und sicherer Betrieb kontinuierlich überwacht werden. Dafür wurde das Datenschutz- und Informationssicherheitsmanagementsystem der Telematikinfrastruktur entwickelt.

Im laufenden Betrieb sind zwei Dinge besonders wichtig: Zum einen melden die Anbieter Datenschutzverstöße und Informationssicherheitsvorfälle an die gematik. Zum anderen übermitteln die Anbieter regelmäßig Informationen, die der gematik Rückschlüsse auf das aktuelle Datenschutz- und Informationssicherheitsniveau erlauben. Im Einzelfall kann die gematik auch beim Anbieter vor Ort prüfen lassen, ob der Datenschutz und die Informationssicherheit ausreichen.

Kapitel 4 geht ausführlicher auf die Informationssicherheit der Telematikinfrastruktur im laufenden Betrieb ein.

3 Sicherheitsarchitektur

Die Sicherheitsarchitektur der Telematikinfrastruktur (TI) umfasst sowohl organisatorische als auch technische Maßnahmen. Dieses Kapitel stellt die Komponenten und Dienste der Telematikinfrastruktur vor und zeigt auf, wie jeweils der Datenschutz und die Informationssicherheit gewährleistet werden.

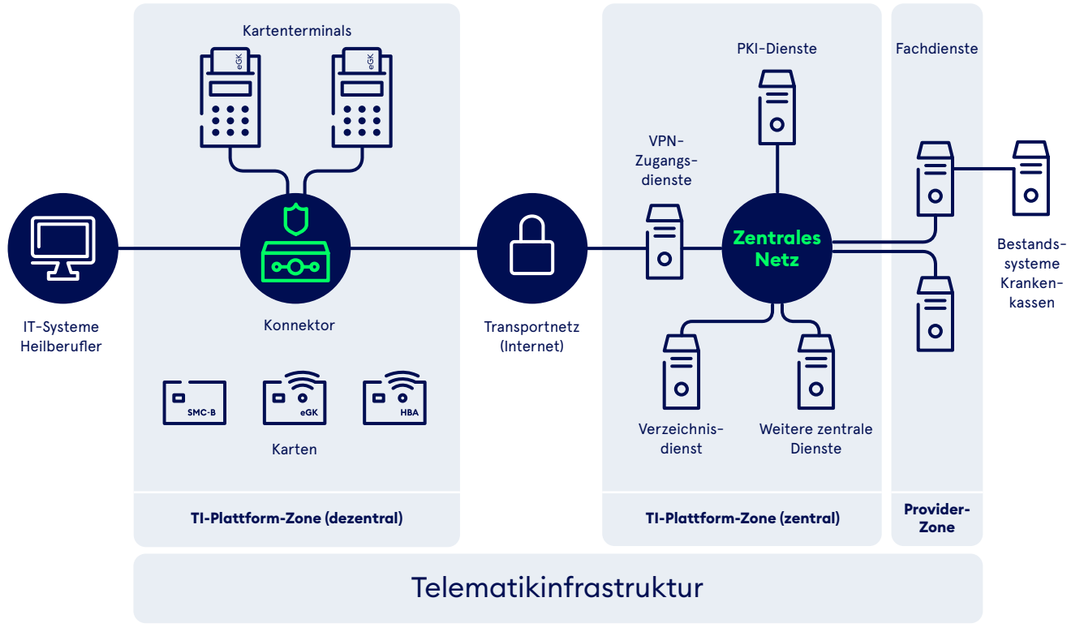
TI-Plattform bietet Sicherheitsfunktionen für die Anwendungen

Es wird zwischen der TI-Plattform (siehe Kapitel 3.1) und den Anwendungen (siehe Kapitel 3.2) unterschieden. Die TI-Plattform bietet übergreifende, grundlegende Funktionalitäten und die Infrastruktur, die die Anwendungen nutzen können. Dies gilt auch für die Sicherheitsfunktionen in der Telematikinfrastruktur. Die TI-Plattform stellt grundlegende Sicherheitsfunktionen wie etwa Authentisierung, Signatur und Verschlüsselung zur Verfügung. Die Anwendungen müssen gewährleisten, dass die durch sie verarbeiteten Informationen sicher sind, und nutzen dafür diese Funktionen der Plattform.

Unterteilung in Zonen regelt, wer Daten austauschen darf

Die Zonen der Telematikinfrastruktur legen fest, welche Komponenten und Dienste miteinander Daten austauschen dürfen. Abbildung 2 gibt einen Überblick über die Zonen der Telematikinfrastruktur und ihre Verbindung zu den existierenden IT-Systemen der Heilberufler und der Krankenkassen. Die in der Abbildung gezeigten Komponenten und Dienste werden im Folgenden näher erläutert.

Abbildung 2 – Die Telematikinfrastruktur im Überblick

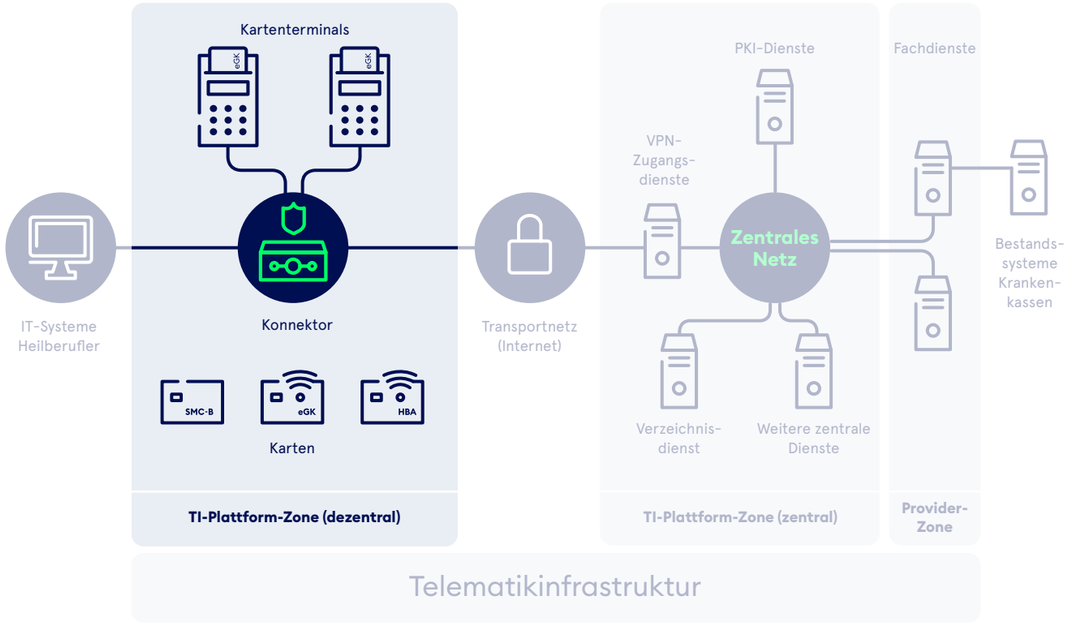


3.1 Dezentrale und zentrale Plattformen der Telematikinfrastruktur

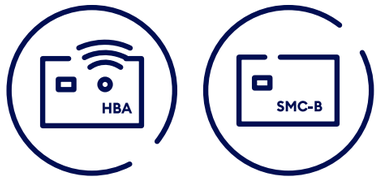
3.1.1 Dezentrale TI-Plattform-Zone

Die dezentrale TI-Plattform-Zone enthält die dezentralen Komponenten. Zu diesen gehören die Karten aller Beteiligten in der Telematikinfrastruktur (elektronische Gesundheitskarte des Versicherten, elektronischer Heilberufsausweis, elektronischer Praxisausweis), Kartenterminals und der Konnektor, über den Leistungserbringer Zugang zur Telematikinfrastruktur erhalten (siehe Abbildung 3). Diese Komponenten werden von den Nutzern der Telematikinfrastruktur eingesetzt: Sie befinden sich also dezentral in den Arztpraxen, Krankenhäusern etc. Alternativ gibt es den Zugang via TI-Gateway, bei dem kein Konnektor mehr dezentral betrieben werden muss (siehe Abbildung 4).

Abbildung 3 – Die dezentrale TI-Plattform-Zone



Die alternative Zugangslösung TI-Gateway gehört formal auch zur dezentralen Zone, wird aber in einem Rechenzentrum durch einen geprüften Anbieter betrieben. Im TI-Gateway werden statt einzelner Konnektoren leistungsstarke Highspeed-Konnektoren auf Server-Hardware verwendet, die die einzelnen Konnektoren virtualisiert zur Verfügung stellen.



Gesundheitskarte des Versicherten

Die elektronische Gesundheitskarte speichert digitale Schlüssel und Daten des Versicherten. Das sind die Versichertenstammdaten (siehe Kapitel 5.1) und zusätzlich die Notfalldaten (siehe Kapitel 5.6), falls der Versicherte dies wünscht. Mithilfe der digitalen Schlüssel kann sich der Versicherte in der Telematikinfrastruktur technisch ausweisen (authentisieren). Diese Mechanismen können verwendet werden, um den Zugriff auf Fachanwendungen zu autorisieren.

Versicherten-PIN und Card-to-Card-Authentisierung

Sensible Daten und die digitalen Schlüssel auf der Gesundheitskarte sind technisch vor unberechtigtem Zugriff geschützt. Hier gibt es zwei Schutzmaßnahmen:

1. Eingabe der PIN des Versicherten und
2. technischer Nachweis der Identität (Authentisierung) des Heilberuflers (in seiner Rolle als Arzt, Apotheker etc.); der Heilberufler authentisiert sich mit seinem elektronischen Heilberufsausweis direkt gegenüber der elektronischen Gesundheitskarte des Versicherten, es findet also eine Authentisierung zwischen zwei Karten statt (Card-to-Card-Authentisierung)

Die PIN wird dem Versicherten von seiner Krankenkasse in einem Brief mitgeteilt. Sie ist sechsstellig und kann vom Versicherten geändert werden.

Um Leistungserbringern den Zugriff auf Fachanwendungsdaten zu ermöglichen, können auch Verfahren ohne PIN-Eingabe Anwendung finden. Durch Schlüssel auf der Gesundheitskarte, die deren Echtheit nachweisen, kann durch Übergabe der Karte an den Leistungserbringer die Befugnis zum Datenzugriff gewährt werden. Leistungserbringer müssen sich gegenüber den Fachanwendungen stets auch selber ausweisen (authentisieren). Ein direkter Zugriff auf Daten ist somit durch Unberechtigte, die beispielsweise die Gesundheitskarte gestohlen haben, nicht möglich. Verliert der Versicherte seine Gesundheitskarte, sollte er dies unabhängig von den bestehenden Schutzmaßnahmen trotzdem unverzüglich seiner Krankenkasse melden. Die Krankenkasse sperrt sie dann – ähnlich wie bei Bank- und Kreditkarten.

Karten der Heilberufler

Auch Ärzte, Zahnärzte, Psychotherapeuten und Apotheker besitzen eine Karte: den elektronischen Heilberufsausweis. Für die Mitarbeiter in den Institutionen des Gesundheitswesens (Arztpraxis, Krankenhaus, Apotheke) gibt es den Praxisausweis. Auch diese Karten besitzen Schlüssel, über die die Heilberufler und Institutionen ihre Identität nachweisen können. Heilberufsausweis und Praxisausweis ermöglichen Heilberuflern, im Zusammenspiel mit der Gesundheitskarte des Versicherten auf medizinische Daten direkt auf der Gesundheitskarte wie auch bei Fachdiensten (beispielsweise in der elektronischen Patientenakte) zuzugreifen.

Durch PIN geschützt

Zur Nutzung seines Heilberufsausweises oder seines Praxisausweises muss der Heilberufler eine PIN eingeben. Erst dann kann er damit auf Daten des Versicherten zugreifen. Daher ist die gefundene oder gestohlene Karte eines Heilberuflers nutzlos, da die für Datenzugriffe notwendigen Schlüssel ohne PIN-Eingabe nicht freigeschaltet sind. Auf dem Heilberufsausweis befindet sich zudem Schlüsselmaterial für eine qualifizierte elektronische Signatur. Mit einer solchen Signatur versichert der Heilberufler rechtsverbindlich, der Urheber der signierten Daten zu sein. Die qualifizierte elektronische Signatur ist das digitale Pendant zur handschriftlichen Unterschrift. Bei der Beantragung eines Heilberufsausweises bzw. eines Praxisausweises müssen die Heilberufler ihre Identität und ihre Berufsgruppenzugehörigkeit nachweisen. Damit wird ausgeschlossen, dass Unbefugte eine solche Karte erhalten.

Kartenterminals sorgen für einen sicheren Kartenzugriff

Die Kartenterminals sind die Bindeglieder zwischen der Gesundheitskarte des Versicherten, den Karten der Heilberufler und dem Konnektor. Sie stellen eine transportgeschützte Verbindung zum Konnektor her, damit die Daten, die von den Karten gelesen bzw. auf sie geschrieben werden, von unbefugten Personen nicht abgefangen oder unbemerkt manipuliert werden können.

Die Kartenterminals für die Telematikinfrastruktur werden als E-Health-Kartenterminals bezeichnet und vor Ort in der Umgebung des Leistungserbringers betrieben. Sie besitzen ein PIN-Pad, ein Display und mindestens zwei Kartenschlitze, sodass zeitgleich eine elektronische Gesundheitskarte und ein Heilberufsausweis bzw. ein Praxisausweis gesteckt werden können.

Konnektor stellt eine sichere Verbindung zur Telematikinfrastruktur her

Die Heilberufler benötigen einen Zugang zur Telematikinfrastruktur. Das findet u. a. über den Konnektor statt. Er ist die steuernde Komponente bei den Heilberuflern vor Ort. Der Konnektor bietet Schnittstellen für die IT-Systeme der Heilberufler an, über die die verschiedenen Funktionen der Telematikinfrastruktur aufgerufen werden können, und kontrolliert die Kommunikation mit den Kartenterminals bei den Kartenzugriffen. Auch die Card-to-Card-Authentisierung wird vom Konnektor gesteuert.

Damit die Heilberufler auf die zentrale TI-Plattform zugreifen können, baut der Konnektor einen sicheren Kanal zu den VPN-Zugangsdiensten der Telematikinfrastruktur auf (siehe Kapitel 3.1.2). Diese auf Netzebene gesicherte Verbindung – ein Virtual-Private-Network-Tunnel (VPN) mittels Internet Protocol Security (IPsec) – zur zentralen TI-Plattform wird über das Internet hergestellt. Sensible Daten, die über diese Verbindung versandt werden, sind zusätzlich auf Transportebene geschützt mittels Transport Layer Security (TLS).

Der Konnektor stellt die Basisfunktionalität und die Sicherheitsfunktionen (wie Verschlüsselung und Authentisierung) zur Verfügung. Diese werden zum einen von Anwendungen der Telematikinfrastruktur genutzt, die entweder Fachlogik im Konnektor als Fachmodul realisieren (z. B. VSDM, NFDM) oder auf dem IT-System des Heilberuflers laufen, aber für Teilaspekte des Anwendungsablaufs die Konnektor-Basisfunktionalität benötigen (beispielsweise zur Authentisierung des Heilberuflers über den Praxisausweis). Zum anderen können die Heilberufler die Funktionen des Konnektors auch direkt nutzen und etwa Dokumente verschlüsseln lassen oder diese mithilfe ihres Heilberufsausweises qualifiziert elektronisch signieren (z. B. E-Rezepte).

Kontrollierter Datenfluss

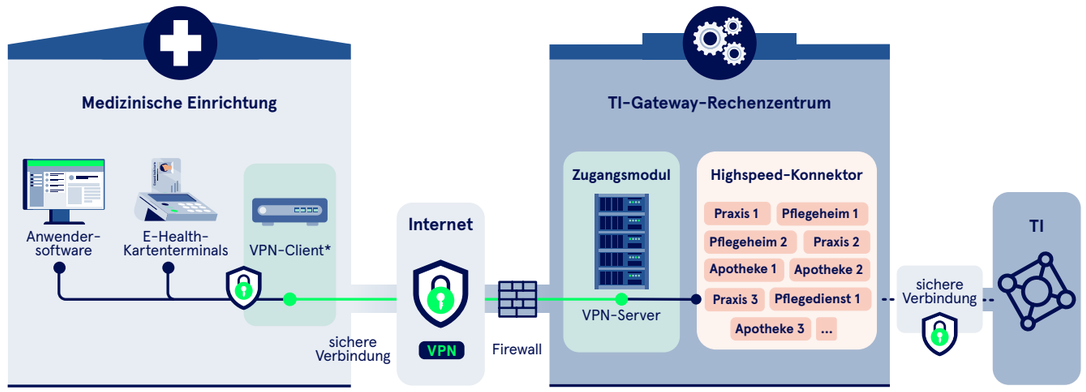
Der Anschluss an die Telematikinfrastruktur bedeutet für den Heilberufler nicht, dass Dienste der Telematikinfrastruktur auf sein IT-System zugreifen können. Nur wenn der Heilberufler dies aktiv auslöst, werden von seinem IT-System Informationen über ihn oder seine Patienten an Dienste der Telematikinfrastruktur übertragen oder auf die elektronische Gesundheitskarte geschrieben.

Die Kommunikation zwischen dem IT-System des Heilberuflers und dem Konnektor sowie die Kommunikation zwischen dem Konnektor und der zentralen TI-Plattform werden stets vom Heilberufler initiiert.

Zugang über TI-Gateway

Der Zugang zur Telematikinfrastruktur über den Konnektor beinhaltet den dezentralen Betrieb des Konnektors direkt in der Institution des Heilberuflers (Praxis, Apotheke). Alternativ dazu gibt es den Zugang zur Telematikinfrastruktur über das TI-Gateway. Hier werden leistungsstarke Highspeed-Konnektoren auf Server-Hardware durch professionelle Anbieter in einem Rechenzentrum betrieben. Ein einzelner Highspeed-Konnektor kann eine Vielzahl von Konnektoren virtualisiert zur Verfügung stellen. Heilberufler, die diesen Zugang wählen, verantworten somit nicht mehr selber den Betrieb der Hardware, da dies vom zugelassenen Anbieter des TI-Gateways übernommen wird. Damit Heilberufler ihren eigenen virtuellen Konnektor im Highspeed-Konnektor erreichen, umfasst das TI-Gateway ein Zugangsmodul, zu dem eine geschützte Verbindung (Virtual Private Network, VPN) aus der Institution des Heilberuflers aufgebaut wird. Über diese VPN-Verbindung wird ein zusätzlicher geschützter Kanal direkt zwischen dem IT-System des Heilberuflers und seinem eigenen virtuellen Konnektor aufgebaut (TLS). Dabei weisen beide Komponenten technisch ihre Identität nach. Dadurch kann das IT-System des Heilberuflers verifizieren, dass es mit dem korrekten virtuellen Konnektor kommuniziert, und ebenso lässt der virtuelle Konnektor nur mit ihm bekannten IT-Systemen beim Heilberufler eine Verbindung zu. Im Gegensatz zum dezentralen Betrieb des Konnektors in der Institution des Heilberuflers werden beim TI-Gateway zentral in einem Rechenzentrum alle TI-Daten des Heilberuflers im Highspeed-Konnektor verarbeitet. Damit der Anbieter, der den Highspeed-Konnektor im TI-Gateway betreibt, keinen Einblick in die dort verarbeiteten Daten erhalten kann, laufen die virtuellen Konnektoren innerhalb einer „vertrauenswürdigen Ausführungsumgebung" (VAU). Für die VAU werden zusätzliche technische und organisatorische Maßnahmen umgesetzt, die bei Diensten mit weniger sensiblen Daten nicht notwendig sind. Wie beim dezentral betriebenen Konnektor findet auch im TI-Gateway keine Speicherung von TI-Daten des Heilberuflers statt. Um die Gesundheitskarte, den Heilberufsausweis oder den Praxisausweis zu verwenden, wird weiterhin ein Kartenterminal dezentral beim Heilberufler betrieben. Auch dieses erreicht über die VPN-Verbindung das TI-Gateway und ist über eine zusätzliche TLS-Verbindung direkt mit dem virtuellen Konnektor des Heilberuflers verbunden.

Abbildung 4 – Anbindung über das TI-Gateway

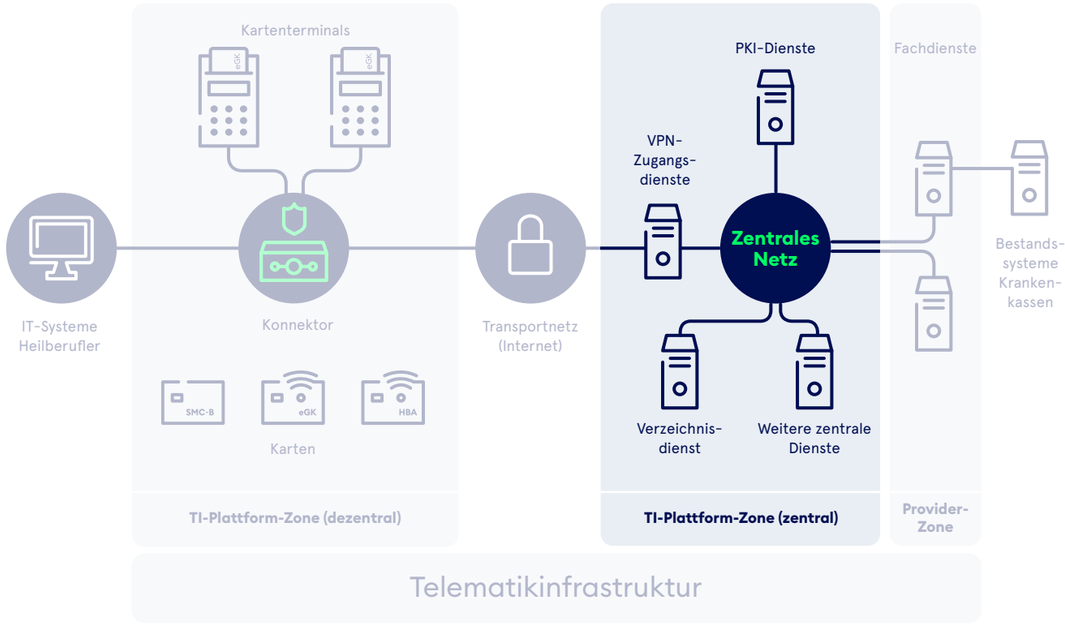


* VPN = virtuelles privates Netzwerk
VPN-Client wird vom Anbieter des TI-Gateways bereitgestellt als Software-Client oder dedizierte Hardware

3.1.2 Zentrale TI-Plattform-Zone

Die zentrale TI-Plattform-Zone enthält die zentralen Dienste der TI-Plattform, die die Anwendungen der Telematikinfrastruktur mit grundlegenden Funktionalitäten unterstützen (siehe Abbildung 5).

Abbildung 5 – Die zentrale TI-Plattform-Zone



VPN-Zugangsdienste verbinden dezentrale und zentrale TI-Plattform

Die VPN-Zugangsdienste stellen die Verbindung zwischen dezentraler und zentraler TI-Plattform dar. VPN steht für Virtual Private Network, ein in sich abgeschlossenes (privates) Netzwerk, mit dem sich Daten über das Internet verschlüsselt versenden lassen. Der Konnektor beim Heilberufler baut einen sogenannten VPN-Tunnel auf, der bei den VPN-Zugangsdiensten der zentralen TI-Plattform endet. Bevor eine solche Verbindung aufgebaut werden kann, muss der Konnektor registriert werden. Dafür ist ein Praxisausweis notwendig. Daher können nur medizinische Institutionen mithilfe des Konnektors das zentrale Netz der Telematikinfrastruktur und darüber die zentralen Dienste und Fachdienste erreichen.

Beim TI-Anschluss via TI-Gateway kommt der VPN-Zugangsdienst nicht zum Einsatz. Der VPN-Tunnel der Institution des Heilberuflers wird hier zum Zugangsmodul des TI-Gateways aufgebaut und der High-speed-Konnektor im TI-Gateway ist direkt an das sichere Netz der Telematikinfrastruktur angeschlossen (siehe nächster Absatz).

Zentrales Netz verfügt über sichere Zugangspunkte

Das zentrale Netz der Telematikinfrastruktur verbindet die zentralen Dienste, Fachdienste und die VPN-Zugangsdienste. Es handelt sich um ein geschlossenes Netz, zu dem der Zugang nur über sichere Punkte möglich ist. Die Dienste bzw. die Rechenzentren, in denen die Dienste betrieben werden, sind dabei direkt an das zentrale Netz der Telematikinfrastruktur angebunden. Aus dem Internet kann man somit nicht auf das zentrale Netz der Telematikinfrastruktur zugreifen.

PKI-Dienste zur Identifikation der Teilnehmer

Grundvoraussetzung für eine datenschutzkonforme und sichere Vernetzung des Gesundheitswesens ist die zweifelsfreie Identifikation der Teilnehmer. Hierzu wird jedem Teilnehmer eine in der Telematikinfrastruktur eindeutige technische Identität zugeordnet – seien es Versicherte, Heilberufler, medizinische Institutionen, dezentrale Komponenten oder auch Dienste der zentralen TI-Plattform.

Die Identitäten der Telematikinfrastruktur werden in einer Public Key Infrastructure (PKI) verwaltet. Technisch wird eine solche Identität durch ein asymmetrisches Schlüsselpaar – bestehend aus einem öffentlichen Schlüssel (Public Key) und einem dazugehörigen privaten Schlüssel – sowie ein Zertifikat realisiert. Das Zertifikat enthält neben dem öffentlichen Schlüssel Informationen zur Identität des Teilnehmers. Eine vertrauenswürdige Stelle beglaubigt das Zertifikat und sichert zu, dass die Informationen zur Identität im Zertifikat richtig sind. Es wird also die Zugehörigkeit eines öffentlichen Schlüssels zur Identität eines Teilnehmers beglaubigt. Entsprechend gelten für die Ausgabe von Zertifikaten in der Telematikinfrastruktur besonders hohe Sicherheitsstandards. Diese Zertifikate zum Identitätsnachweis haben eine begrenzte Gültigkeitsdauer und können gesperrt werden.

Das Zertifikat und der öffentliche Schlüssel dürfen jedem in der Telematikinfrastruktur bekannt sein. Den privaten Schlüssel hingegen besitzt allein der Teilnehmer. Dieser private Schlüssel muss unbedingt geheim bleiben. Nur so kann die Identität des Teilnehmers geschützt werden. Daher werden die privaten Schlüssel von Versicherten und Heilberuflern bzw. medizinischen Institutionen auf einer Karte gespeichert – also Gesundheitskarte oder Heilberufsausweis bzw. Praxisausweis. Hier lassen sie sich nicht auslesen und sind vor einem unberechtigten Zugriff geschützt.

Die Identität eines Teilnehmers wird benötigt, wenn dieser sich in der Telematikinfrastruktur ausweist, diese für ihn verschlüsselt werden soll oder er signiert. Für jeden einzelnen Zweck besitzt der Teilnehmer ein separates Schlüsselpaar und ein dazugehöriges Zertifikat. Somit wird durch die Prüfung des Zertifikats technisch eindeutig festgestellt, mit wem eine Kommunikation stattfindet, für wen etwas verschlüsselt wird oder wer etwas signiert hat.

Zudem ist den Teilnehmern der Telematikinfrastruktur über ein gesondertes Zertifikat eine Rolle (z. B. „Arzt“ oder „Apotheker“) zugeordnet. Darüber wird das in Kapitel 3.1.1 erwähnte Rollen- und Rechtekonzept im Rahmen der Card-to-Card-Authentisierung mit der Gesundheitskarte umgesetzt, das unterschiedlichen Heilberuflerrollen jeweils nur die gesetzlich festgelegten Zugriffsrechte auf Daten der Gesundheitskarte gewährt.

Für Versicherte steht zusätzlich zu den Identitäten über die Public Key Infrastructure auch die GesundheitsID zur Verfügung (siehe Kapitel 3.1.3).

Verzeichnisdienst

Der Verzeichnisdienst ist mit einem Telefonbuch für die Telematikinfrastruktur vergleichbar. Er existiert derzeit in zwei Ausprägungen: der älteren, die auf dem Lightweight Directory Access Protocol basiert, und der neuen, die den FHIR-Standard (Fast Healthcare Interoperability Resources) nutzt. Der Verzeichnisdienst hält Informationen über Heilberufler und medizinische Institutionen bereit, darunter Namen, Adressen, Telefonnummern, KIM-Adressen und Zertifikate, Öffnungszeiten von Apotheken, TI-Messenger-Adressen und Weiteres. Die Informationen sind für jeden Teilnehmer der Telematikinfrastruktur einsehbar.

Weitere zentrale Dienste

Neben den genannten Diensten gibt es auf der zentralen TI-Plattform weitere Dienste mit Funktionen, die in jeder Kommunikations-IT-Infrastruktur benötigt werden. Hierzu gehören beispielsweise ein Zeitdienst für eine einheitliche Zeit in der Telematikinfrastruktur sowie ein Namensdienst, um Dienste zu finden.

3.1.3 GesundheitsID

Seit Januar 2024 steht den Versicherten die GesundheitsID als digitale Identität im Gesundheitswesen zur Verfügung. Sie können sich nun zum ersten Mal mit einer zentralen Identität bei Diensten im Gesundheitswesen anmelden. Diese digitale Identität für das Gesundheitswesen setzt das neu geschaffene Vertrauensniveau „gematik-ehealth-loa-high“ um. Es orientiert sich am Vertrauensniveau „hoch“ der Technischen Richtlinie TR-3107-1 des Bundesamtes für Sicherheit in der Informationstechnik. Um die GesundheitsID einzurichten, ist eine sichere Identifikation mithilfe der Online-Ausweisfunktion, der elektronischen Gesundheitskarte mit PIN oder mithilfe eines anderen geeigneten Vor-Ort-Identifikationsverfahrens erforderlich. Technisch handelt es sich bei der GesundheitsID um eine digitale Identität auf Basis von OpenID Connect. Hierbei stellen die Krankenkassen über beauftragte Dienstleister einen sektoralen Identity Provider (IDP) zur Verfügung. Die sektoralen Identity Provider agieren hierbei innerhalb einer von der gematik betreuten Föderation.

Zur komfortablen Nutzung der GesundheitsID können neben der Authentifizierung mithilfe des Personalausweises oder der elektronischen Gesundheitskarte auch Gerätebindungen auf mobilen Geräten genutzt werden. Hierbei wird das Schlüsselmaterial im sicheren Schlüsselspeicher des Geräts vorgehalten und von den Versicherten mit geeigneten Mitteln freigeschaltet. Die Gültigkeitsdauer der Gerätebindung wird hierbei aus Sicherheitsgründen beschränkt. Je nach Geräteausstattung kann die Gültigkeitsdauer variabel festgelegt werden – von 24 Stunden bis hin zu einer zeitlich unbegrenzten Dauer. Die Freischaltung der Gerätebindung erfordert eine starke Nutzerauthentisierung. Nutzer können hierzu grundsätzlich zwischen einer App und einer System-PIN wählen.

Mit der elektronischen Patientenakte, also der ePA für alle, wurden auch für die GesundheitsID neue Akzeptanzfeatures ermöglicht. Zur Steigerung des Komforts stehen den Versicherten zusätzlich einwilligungspflichtige Optionen zur Verfügung. Hierbei gilt stets, dass Versicherte auch Sicherheitsmaßnahmen nutzen können, die lediglich das Vertrauensniveau „gematik-ehealth-loa-substantial“ erfüllen, solange sie zuvor auf hohem Niveau identifiziert wurden. Zu den möglichen Optionen zählen insbesondere längere Laufzeiten der Gerätebindungen (zwölf Monate) und die Nutzung biometrischer Sensoren.

Auf Wunsch der Versicherten entfällt zusätzlich die Pflicht zur dauerhaften Verwendung einer PIN, an deren Stelle die Nutzung der biometrischen Sensoren tritt. Vor ihrer Einwilligungserklärung werden die Versicherten aufgeklärt, auch über die Risiken der verfügbaren Sensoren. Zudem haben die Versicherten jederzeit die Möglichkeit, ihre Einwilligung zu widerrufen und anschließend Authentisierungsmittel auf hohem Niveau zu nutzen.

Zusätzlich steht ein In-App-Single-Sign-On (SSO) zur Verfügung. Falls die Versicherten es wünschen und sie entsprechend zugestimmt haben, können innerhalb einer Krankenkassen-App die unterschiedlichen angebundenen Gesundheitsanwendungen mit nur einer Authentisierung genutzt werden. Mithilfe App-spezifischer Einstellungen legen die Versicherten individuell pro Anwendung fest, ob SSO genutzt werden soll.

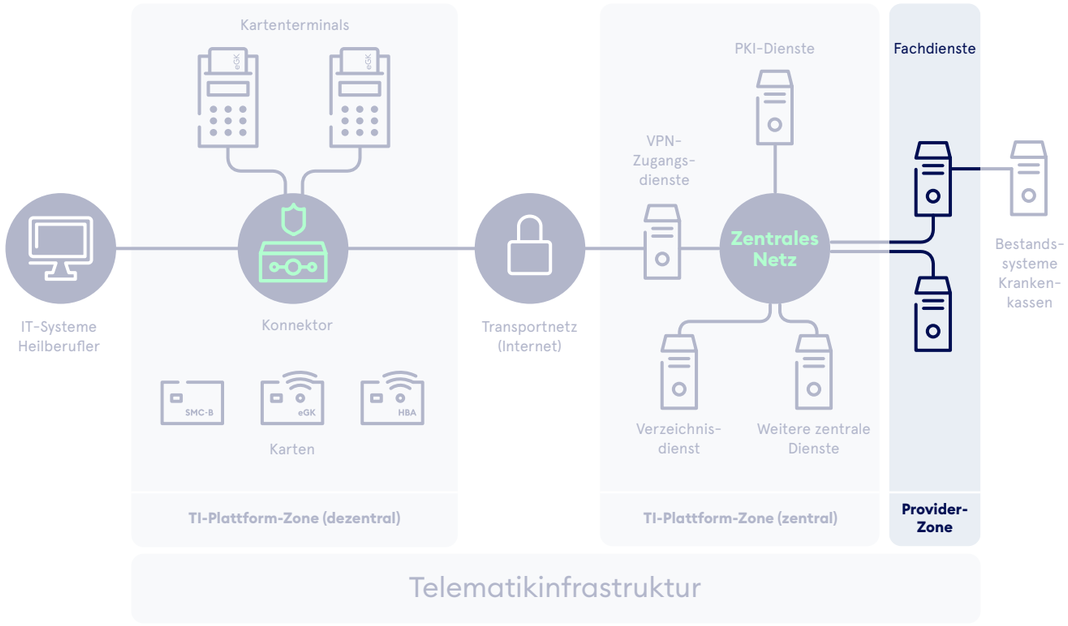
Als eine der ersten TI-Anwendungen unterstützten bereits das E-Rezept, die ePA für alle, das Organspende-Register sowie frühe digitale Gesundheitsanwendungen (DiGA) die Anmeldung mithilfe der GesundheitsID.

Durch die Öffnung der GesundheitsID für weitere Anwendungen des Gesundheitswesens steht den Versicherten zukünftig eine große Anzahl an Gesundheitsdiensten mit nur einer zentralen Identität zur Verfügung.

3.2 Provider-Zone

Anwendungen der Telematikinfrastruktur wie das Versichertenstammdaten-Management, das E-Rezept und die elektronische Patientenakte können aus mehreren Teilkomponenten bestehen. Falls zu einer Anwendung ein oder mehrere zentrale Dienste gehören, sind diese sogenannten fachanwendungsspezifischen Dienste (kurz: Fachdienste) der Provider-Zone zugeordnet (siehe Abbildung 6).

Abbildung 6 – Die Provider-Zone mit den Anwendungen der Telematikinfrastruktur



Die Heilberufler rufen die Fachdienste über den Konnektor und den Zugang zur zentralen Telematikinfrastruktur auf. Der Versicherte kann auf die Fachdienste über das Internet mit einer Client-Software (App) zugreifen, die auf seinem PC, Smartphone oder Tablet ausgeführt wird.

Die Anwendungen der Telematikinfrastruktur sind dafür verantwortlich, den Datenschutz sowie die Informationssicherheit zu gewährleisten. Daher müssen alle Anwendungen im Rahmen der Zulassung nachweisen, dass sie dem Schutzbedarf der durch sie verarbeiteten Informationsobjekte entsprechen und die erforderlichen Maßnahmen ergreifen. Dabei werden auch die entsprechenden Vorgaben des Gesetzgebers berücksichtigt.

Die einzelnen Anwendungen der Telematikinfrastruktur werden in Kapitel 5 vorgestellt.

4 Sicherheit im Betrieb

Die betriebliche Sicherheit umfasst alle Aspekte der Informationssicherheit der Telematikinfrastruktur. Den Kern bildet das Managementsystem für Informationssicherheit (ISMS), das sich auf eine Vielzahl an organisatorischen und technischen Prozessen stützt, die Informationen sammelt, aufbereitet und den jeweiligen Interessengruppen zur Verfügung stellt.

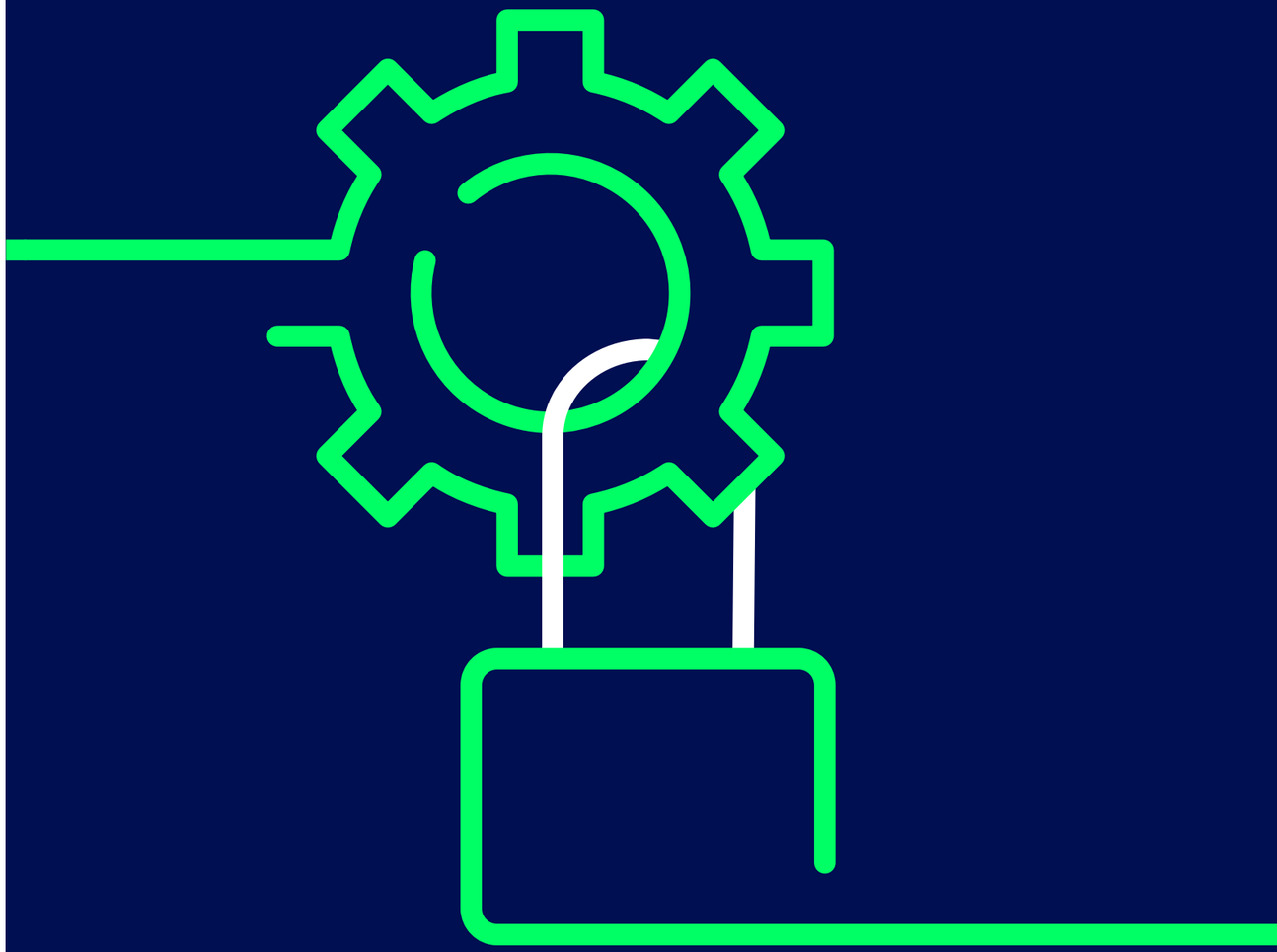


Abbildung 7 – Betriebliche Sicherheit der Telematikinfrastruktur

Managementsystem für Informationssicherheit

Das Managementsystem für Informationssicherheit ist die zentrale Organisationsstruktur für die Sicherheit im Betrieb der Telematikinfrastruktur. Es steuert übergreifende Aspekte wie das Risikomanagement und das Reporting gegenüber den Interessengruppen. Es ist zudem der zentrale Ansprechpartner für alle Funktionsbereiche der betrieblichen Sicherheit.

Audits

Auf Basis eines mehrjährigen Auditprogramms führt die gematik regelmäßig Audits bei den Herstellern und Anbietern der Dienste der Telematikinfrastruktur durch, um zu prüfen, ob die Anforderungen hinsichtlich der Sicherheit der Betriebsleistung erfüllt werden. Im Rahmen der Audits werden Aspekte des IT-Service-Managements der Telematikinfrastruktur sowie des Datenschutzes und der Informationssicherheit untersucht.

Sicherheitsanalysen

Im Rahmen von Sicherheitsanalysen werden insbesondere technische Prüfungen wie Penetrationstests auf Produkte der Telematikinfrastruktur durchgeführt. Auf Basis einer jährlichen Planung werden dabei risikobasiert Komponenten und Dienste identifiziert, die einer solchen Überprüfung unterzogen werden. Die Durchführung wird im Vorfeld mit dem Anbieter bzw. Hersteller eng abgestimmt. Neben technischen Tests wurden in den letzten Jahren zunehmend auch organisatorische Überprüfungen vorgenommen, um beispielsweise Social-Engineering-Angriffe zu simulieren.

Vulnerability Management

Um die Schwachstellenlage anbieterübergreifend in den Blick zu nehmen, führt die gematik kontinuierlich Schwachstellenscans auf allen zum Internet hin exponierten Diensten durch. Neben diesen nicht authentisierten Scans sind Anbieter der Telematikinfrastruktur verpflichtet, der gematik monatlich die Ergebnisse von authentisierten Scans ihrer eingesetzten Systeme zur Verfügung zu stellen. Hierdurch erhält das Cyber Defense Center einen guten Überblick über die Gesamtschwachstellenlage und kann auf dieser Basis steuernd eingreifen, wenn erforderlich, (z. B. durch Anordnung von außerplanmäßigen Sicherheitspatches).

Security Monitoring

Die Notwendigkeit, Anomalien, die auf Angriffsversuche hindeuten können, frühzeitig zu erkennen, hat in den letzten Jahren durch die zunehmend angespannte Bedrohungssituation stark zugenommen. Um eine zuverlässige Angriffserkennung zu gewährleisten, sind Anbieter der Telematikinfrastruktur verpflichtet, ein SIEM-System zu betreiben, hiermit die notwendigen Logquellen auszuwerten und Prozesse zur Analyse und gegebenenfalls Eskalation zu implementieren. Das Cyber Defense Center der gematik betreibt ein zentrales TI-SIEM-System, das Logdaten und Events zentral analysiert und hierdurch eine Qualitätssicherung und Umsetzung des Vier-Augen-Prinzips anbieterübergreifend sicherstellt.

Threat Intelligence

Die kontinuierliche Beobachtung der Bedrohungslage hilft dabei, Entwicklungen im Bereich Cybersecurity frühzeitig zu erkennen und daraus gezielt Maßnahmen abzuleiten. Hierzu werden sowohl öffentliche als auch geschlossene Quellen kontinuierlich analysiert, um Angriffe auf Gesundheitseinrichtungen national wie international umgehend zu erkennen und daraus gegebenenfalls notwendige Handlungen abzuleiten.

Security Incident Management

Ziel des Security Incident Managements ist es, Sicherheitsvorfällen vorzubeugen und gemeinsam mit den betroffenen Anbietern bzw. Herstellern dafür zu sorgen, dass Schäden minimiert werden, falls sie im Vorfeld nicht erkannt wurden. Hierdurch soll das Sicherheitsniveau der Telematikinfrastruktur kontinuierlich gewährleistet sein. Neben Anbietern und Herstellern, die verpflichtet sind, solche Vorfälle unverzüglich an die gematik zu melden, stellt das CERT der gematik auch verschiedene Kommunikationskanäle wie das Coordinated Vulnerability Disclosure Program zur Verfügung, um potenzielle Vorfälle zu melden.

Notfallmanagement

Ziel des Notfallmanagements ist es, durch die präventive Betrachtung von potenziellen Notfallszenarien Risiken frühzeitig zu erkennen, zu bewerten sowie notfallvorbeugende Maßnahmen zu etablieren. Dadurch soll die Eintrittswahrscheinlichkeit von Notfällen gesenkt und das Ausmaß des Schadens verringert werden. Kommt es dennoch zu einem Notfall in der Telematikinfrastruktur, sollen durch koordinierte Handlungen die Auswirkungen und Schäden minimiert werden. Für das Notfallmanagement müssen Alarmierungs- und Eskalationsstrukturen eingerichtet werden. Ebenso gilt es, Vorkehrungen für relevante Notfallszenarien zu treffen und diese regelmäßig hinsichtlich ihrer Aktualität, Wirksamkeit und Vollständigkeit zu überprüfen und gegebenenfalls anzupassen.

Sicherheitsgutachten

Anbieter von Diensten und Hersteller von Komponenten der Telematikinfrastruktur müssen im Rahmen der Zulassung und anschließend im Abstand von drei Jahren ein Sicherheitsgutachten gegenüber der gematik einreichen. Die hierfür eingesetzten unabhängigen Sicherheitsgutachter werden durch die gematik speziell für diese Aufgabe zusätzlich qualifiziert. Im Rahmen der Gutachten prüfen sie die Einhaltung von produktspezifischen und auch produktübergreifenden Sicherheitsanforderungen.

Partnermanagement

Da die Dienste der Telematikinfrastruktur nicht durch die gematik selbst hergestellt bzw. betrieben werden, ist die vertrauensvolle und enge Zusammenarbeit mit Herstellern und Anbietern der Telematikinfrastruktur von essenzieller Bedeutung. Über das Partnermanagement werden alle Aktivitäten zusammengefasst, um Anbieter der Telematikinfrastruktur im laufenden Betrieb kontinuierlich zu steuern.

Im Rahmen von monatlich stattfindenden Security Calls sowie jährlich durchgeführten Partnerworkshops werden die ausgeleiteten Informationen aus allen bereits vorgestellten Prozessen (Findings aus Audits, Sicherheitsanalysen, erkannte Schwachstellen sowie Alarme aus dem Security Monitoring sowie Erkenntnisse aus Notfallübungen und Sicherheitsvorfällen) in einem anbieterbezogenen Sicherheitslagebild zusammengefasst und die Anbieter auf dieser Basis maßnahmenzentriert gesteuert. Daneben findet zweimal jährlich der Arbeitskreis Datenschutz und Informationssicherheit statt, der zum Austausch zwischen Anbietern der Telematikinfrastruktur und der gematik übergreifend dient.

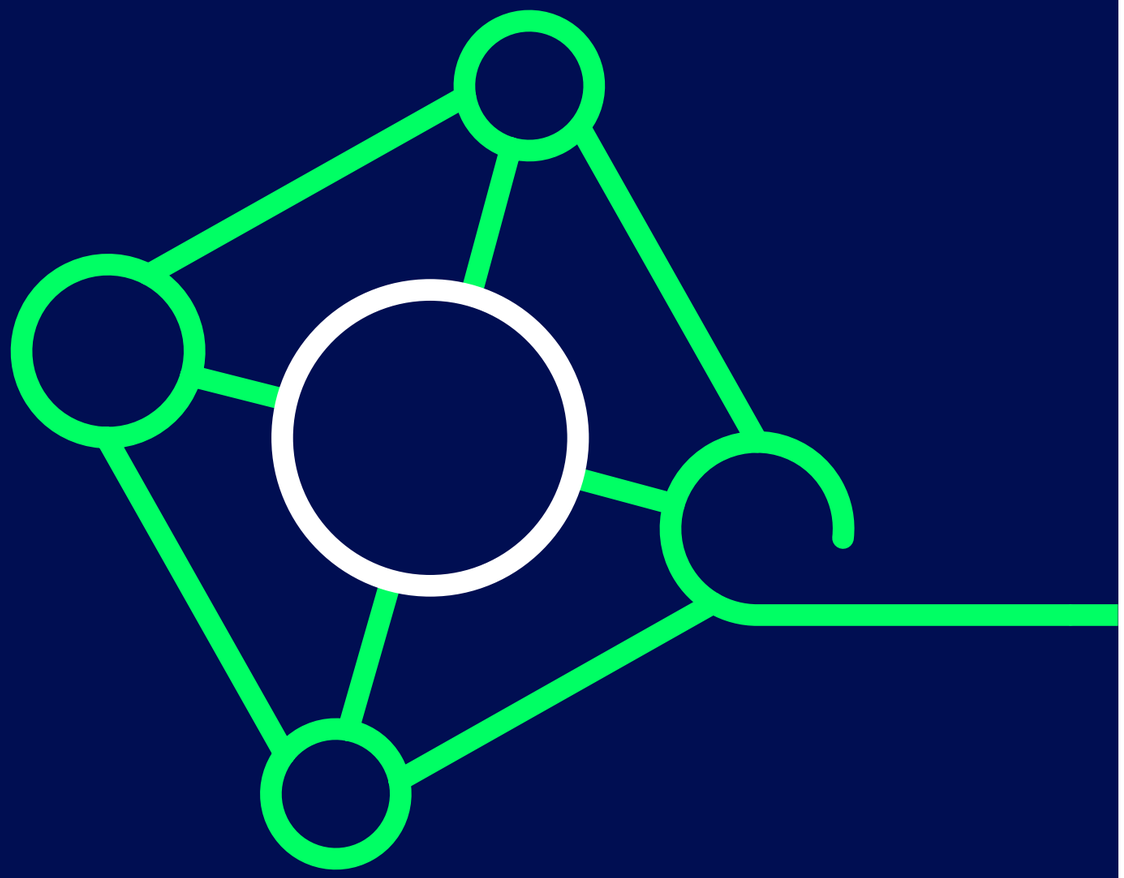
Schnittstellen zu Behörden

Im Kontext der betrieblichen Sicherheit ist die gematik im kontinuierlichen Austausch mit den zuständigen Referaten des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie dem Bundesministerium für Gesundheit (BMG) und stellt diesen gegenüber die übergreifende Sicherheitslage der Telematikinfrastruktur dar. Weiterhin hat die gematik gemäß § 329 (4) SGB V eine Meldepflicht gegenüber dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesgesundheitsministerium, wenn die Funktionalität oder Sicherheit der Telematikinfrastruktur gefährdet ist.

Schnittstellen zu anderen CERTs

Das Computer Emergeny Response Team (CERT) der gematik tauscht regelmäßig Informationen mit anderen CERTs aus. Die gematik ist hierzu sowohl in nationalen als auch europäischen CERT-Verbünden (Deutscher CERT-Verbund und Trusted Introducers) engagiert.

5 Anwendungen der Telematikinfrastruktur



5.1 Versichertenstammdaten-Management

Eine Anwendung der Telematikinfrastruktur ist das sogenannte Versichertenstammdaten-Management. Diese Anwendung ist gesetzlich vorgegeben. Die Krankenkasse kann damit die Versichertenstammdaten auf der elektronischen Gesundheitskarte eines Versicherten sicher über die Telematikinfrastruktur aktualisieren. In den meisten Fällen muss die Gesundheitskarte dann nicht ausgetauscht werden. Die Anwendung besteht aus dem Fachmodul Versichertenstammdaten-Management auf dem Konnektor des Heilberuflers sowie dem entsprechenden Fachdienst in der Provider-Zone der Telematikinfrastruktur.

Gesetzlich verpflichtende Anwendung

Die Krankenkasse ist gesetzlich verpflichtet, die Versichertenstammdaten auf der elektronischen Gesundheitskarte ihrer Versicherten zu speichern (§ 291a Abs. 2 SGB V) und bei Bedarf zu aktualisieren (§ 291b Abs. 1 SGB V), da die Versicherten damit den Nachweis erbringen, dass sie Leistungen der gesetzlichen Krankenversicherung in Anspruch nehmen können. Außerdem benötigt der Heilberufler die Versichertenstammdaten, um seine Leistungen mit der gesetzlichen Krankenkasse abzurechnen.

Die Versichertenstammdaten beinhalten Informationen zur Krankenkasse, zum Versicherungsschutz oder zur Kostenerstattung sowie persönliche Angaben zum Versicherten wie den Namen, das Geburtsdatum, das Geschlecht und die Adresse. Zudem können sensible Informationen wie beispielsweise die Angabe zum Zuzahlungsstatus enthalten sein. Da die Krankenkassen gesetzlich zur Speicherung der Versichertenstammdaten verpflichtet sind, ist hierfür – anders als bei den freiwilligen medizinischen Anwendungen der Telematikinfrastruktur – keine gesonderte Einwilligung des Versicherten erforderlich.

Krankenkassen aktualisieren Versichertenstammdaten

Wenn die Versichertenstammdaten auf der Gesundheitskarte aktualisiert werden müssen, vermerkt die zuständige Krankenkasse dies auf dem Aktualisierungsstatusdienst (Update Flag Service). Eine Aktualisierung ist beispielsweise notwendig, wenn sich die Anschrift des Versicherten oder sein Versichertenstatus, etwa aufgrund eines Renteneintritts, ändert. Die Krankenkasse stellt die zu aktualisierenden Daten über einen weiteren Dienst, den Versichertenstammdatendienst, für den Aktualisierungsvorgang bereit.

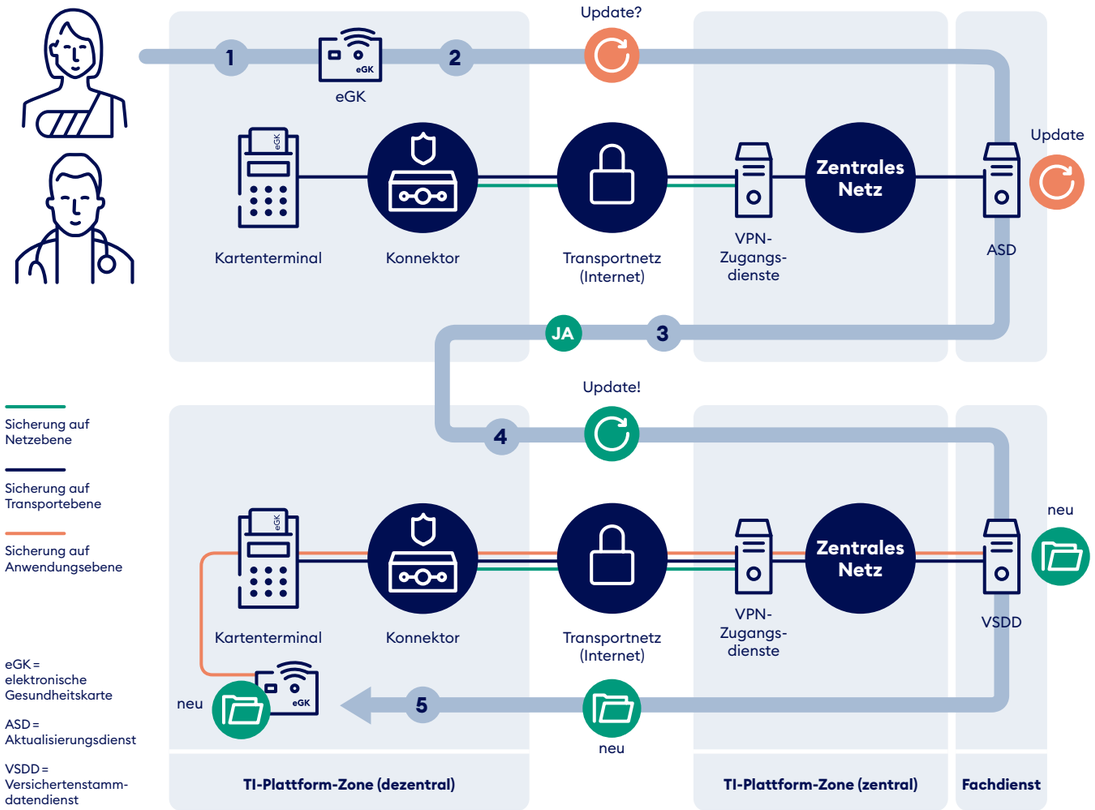
Wird in einem Quartal die Leistung eines Arztes zum ersten Mal in Anspruch genommen, ist der Arzt verpflichtet, die elektronische Gesundheitskarte online zu prüfen. Hierbei wird beim Aktualisierungsstatusdienst abgefragt, ob für die jeweilige Karte eine Aktualisierung vorliegt. Diese Abfrage wird über eine auf Netzebene gesicherte Verbindung (Virtual-Private-Network-Tunnel) zwischen Konnektor und VPN-Zugangsdienst versandt und ist auch auf Transportebene zwischen Konnektor und Aktualisierungsstatusdienst geschützt (Transport Layer Security, TLS).

Müssen die Versichertenstammdaten auf der Gesundheitskarte aktualisiert werden, wird zusätzlich zu den genannten Sicherheitsmaßnahmen eine auf Anwendungsebene gesicherte Verbindung (Secure Messaging) direkt zwischen der Gesundheitskarte und dem Versichertenstammdatendienst aufgebaut, auf dem die neuen Versichertenstammdaten abgelegt sind. Die Verbindung wird mit einem Schlüssel gesichert, der auf der Gesundheitskarte gespeichert ist und sonst nur der Krankenkasse des Versicherten bekannt ist. Der Schlüssel ist dabei für jede elektronische Gesundheitskarte einzigartig. Eine Krankenkasse kann daher die abhör- und manipulationssichere Verbindung ausschließlich zu ihren eigenen Gesundheitskarten aufbauen.

Zudem schützt die Krankenkasse ihre IT-Systeme entsprechend den für sie geltenden Vorschriften des Datenschutzes nach Sozialgesetzbuch V und Sozialgesetzbuch X – und damit auch die in den IT-Systemen gespeicherten Schlüssel der elektronischen Gesundheitskarte.

Die aktuellen Versichertenstammdaten werden dann vom Versichertenstammdatendienst durch den sicheren Kanal direkt zur elektronischen Gesundheitskarte transportiert (Ende-zu-Ende-Schutz) und dort gespeichert. Dank der sicheren Verbindung kann niemand unberechtigt die Versichertenstammdaten einsehen. Beim Transport über das Internet sind die Daten auf drei Ebenen geschützt: Netzebene, Transportebene und Anwendungsebene (siehe Abbildung 8).

Abbildung 8 – Die Versichertenstammdaten werden über einen sicheren Kanal aktualisiert



1 Benachrichtigung über Stecken der eGK

2 Prüfen auf Änderung der Versichertenstammdaten beim Aktualisierungsdienst

3 Signalisierung, dass Änderungen vorliegen

4 Auslösen der Aktualisierung

5 Schreiben neuer Versichertenstammdaten direkt auf die eGK

Auf der elektronischen Gesundheitskarte wird protokolliert, wo die Versichertenstammdaten zu welchem Zeitpunkt aktualisiert wurden. Auch die Krankenkasse erfasst in ihren Systemen, wann welche Versichertenstammdaten auf welche Gesundheitskarte geschrieben wurden.

Arztbezug wird anonymisiert

Die Krankenkasse muss nicht wissen, wo die Gesundheitskarte eines Versicherten geprüft und falls erforderlich aktualisiert wurde. Sie muss lediglich wissen, um welche Gesundheitskarte es sich handelt. Die Telematikinfrastruktur anonymisiert daher den Bezug zum Heilberufler so, dass die Krankenkasse nicht erkennt, von welchem Heilberufler aus die elektronische Gesundheitskarte durch den Fachdienst „Versichertenstammdaten-Management" geprüft und aktualisiert wird.

Krankenkassen erteilen Auskunft

Krankenkassen müssen den Versicherten über die auf der elektronischen Gesundheitskarte gespeicherten Versichertenstammdaten und die durchgeführten Aktualisierungen Auskunft geben. Hierzu können sich die Versicherten an ihre Krankenkasse wenden.

5.2 KIM – Kommunikation im Medizinwesen

Kommunikation im Medizinwesen – kurz KIM – ist eine Anwendung der Telematikinfrastruktur, die es Leistungserbringern, den Institutionen, denen sie angehören, sowie Organisationen des Gesundheitswesens ermöglicht, sicher – das heißt Ende-zu-Ende-verschlüsselt und mit gesicherter Authentizität der Kommunikationspartner – per E-Mail zu kommunizieren.

Bei der Behandlung eines Patienten ist in vielen Fällen eine Kommunikation zwischen verschiedenen Heilberuflern notwendig. So müssen beispielsweise elektronische Arztbriefe, Röntgenbilder und Laborwerte dem behandelnden Arzt übermittelt werden oder die Heilberufler tauschen sich fachlich aus. Andererseits müssen Arbeitsunfähigkeitsbescheinigungen – kurz AU – ihren Weg vom Leistungserbringer zum Kostenträger finden, was bei postalischer Zustellung ein Vorgang mit manuellem und zeitlichem Aufwand ist.

Mit der Anwendung „Sicherer E-Mail- und Datenaustausch im Gesundheitswesen" können die Heilberufler dem Schutzbedarf sensibler Patientendaten gerecht werden, sowohl in der Kommunikation mit anderen Heilberuflern als auch bei der Zustellung elektronischer Arbeitsunfähigkeitsbescheinigungen (eAU) an die Kostenträger. Die Anwendung besteht aus einer Client-Software für das IT-System des Heilberuflers und den entsprechenden Fachdiensten.

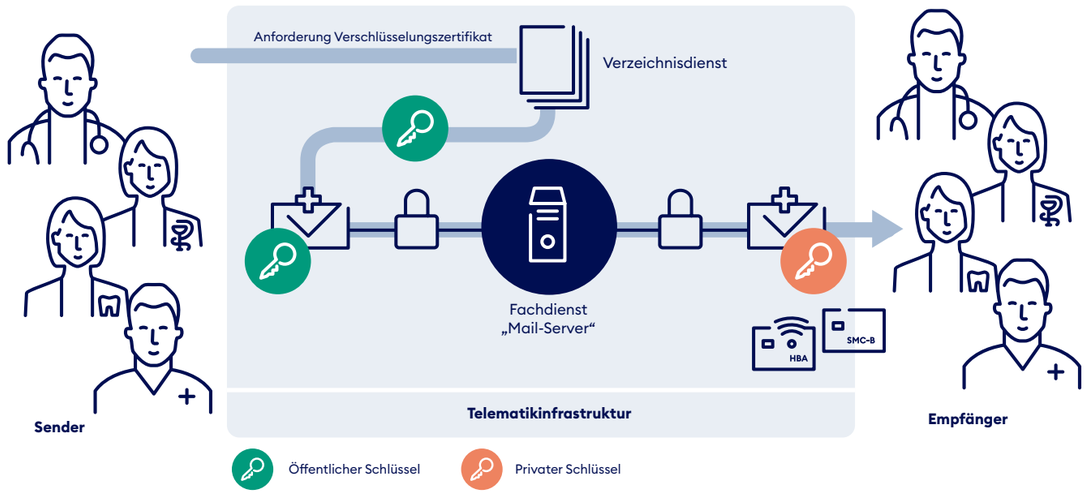
Ausschließlich registrierte Teilnehmer

Diese Anwendung ist Heilberuflern, medizinischen Institutionen und Organisationen des Gesundheitswesens vorbehalten. Sie müssen sich zunächst beim Anbieter dieser Anwendung registrieren lassen. Dabei wird die Identität des Teilnehmers technisch über dessen Zertifikat geprüft. Nach der Registrierung richten die Teilnehmer über den Account-Manager Adressen und Passwörter ein, die sie später bei der Einrichtung ihrer Anwendung im Primärsystem angeben müssen, um über das KIM-Clientmodul die Verbindung zum KIM-Fachdienst herzustellen, sodass Nachrichten gesendet und empfangen werden können.

Ende-zu-Ende-Verschlüsselung

Wird bei kommerziellen E-Mail-Providern mit Verschlüsselung geworben, ist oftmals eine Transportverschlüsselung gemeint. Dabei werden die E-Mails auf dem Versandweg zwischen den Kommunikationspunkten geschützt, damit niemand den Inhalt lesen kann, wenn er die E-Mail abfängt. An den Kommunikationspunkten selbst liegt die E-Mail unverschlüsselt vor, also auch beim E-Mail-Provider, da dort die E-Mails vorgehalten werden, bis der Empfänger diese abruft. Der Provider kann (rein technisch betrachtet) in diesem Fall – auch wenn er besonders strengen Informationssicherheits- und Datenschutzanforderungen unterliegt – alle gesendeten Nachrichten einsehen. Dies ist bei medizinischen Daten allerdings nicht zulässig, da es mit der ärztlichen Schweigepflicht nach § 203

Abbildung 9 – Ende-zu-Ende-Verschlüsselung bei der Kommunikation im Medizinwesen



des Strafgesetzbuches unvereinbar ist. Bei der Anwendung KIM werden die Nachrichten daher vor dem Versand vom Clientmodul und unter Zuhilfenahme des Konnektors automatisch individuell für die Empfänger verschlüsselt. Nur ein rechtmäßiger Empfänger kann somit den Inhalt der Nachricht lesen. Der Fachdienst dieser Anwendung, der als E-Mail-Provider fungiert, ist technisch nicht in der Lage, Nachrichten einzusehen. Dies schützt ebenfalls den Anbieter dieser Anwendung. So kann er auch nicht unbeabsichtigt, etwa bei administrativen Tätigkeiten auf dem Server, medizinische Daten einsehen. Außerdem sinkt damit der technische und wirtschaftliche Aufwand des Anbieters, der für den Schutz der E-Mails aufzubringen ist. Für die Ver- und Entschlüsselung wird das dafür vorgesehene kryptografische Material des Heilberufsausweises bzw. der SMC-B verwendet. Um Nachrichten für einen Empfänger verschlüsseln zu können, ist der öffentliche Teil dieses Materials (das Verschlüsselungszertifikat des Empfängers) notwendig. Diese Daten können die Nutzer der Anwendung KIM aus dem Verzeichnisdienst der TI-Plattform abrufen (siehe Abbildung 9).

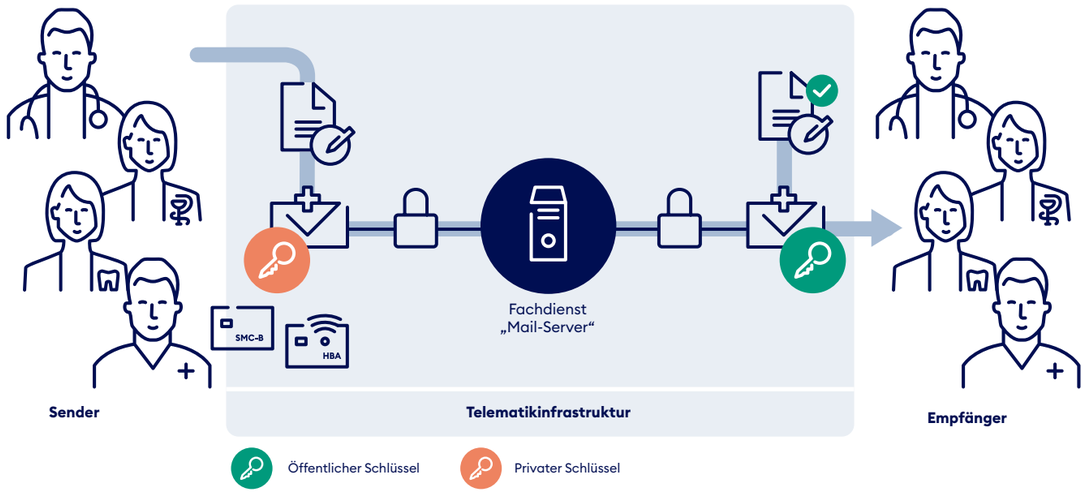
Gesicherte Authentizität von Sender und Empfänger

Die E-Mail-Adressen, die sich Teilnehmer nach der Registrierung anlegen, können nur durch den KIM-Anbieter im Verzeichnisdienst der TI-Plattform eingetragen werden. Somit wird ausgeschlossen, dass ein gefälschter Eintrag erzeugt werden kann, bei dem beispielsweise einem bestimmten Arzt (Name) eine falsche E-Mail-Adresse zugeordnet ist. Vor dem Verschlüsseln von Nachrichten wird zudem überprüft, ob das aus dem Verzeichniseintrag ermittelte Verschlüsselungszertifikat echt und gültig ist. Die Nachrichten werden vor dem Versand automatisch signiert. Dabei kommt das dafür vorgesehene kryptografische Material des Praxisausweises des Senders zum Einsatz. Der Empfänger kann daher sicher nachvollziehen, von welcher medizinischen Institution oder Organisation des Gesundheitswesens die Nachricht gesendet wurde.
Die Signatur schützt zugleich auch die Integrität der Nachricht, da Änderungen an den signierten Daten bei der Signaturprüfung als Fehler angezeigt werden (siehe Abbildung 10).

Automatische Informationssicherheit

Ähnlich wie beim Versichertenstammdaten-Management durchläuft die Kommunikation zwischen Heilberuflern – neben der Sicherung auf Netz- und Transportebene – automatisch sämtliche geschilderten Sicherheitsmaßnahmen. Dafür sorgt das zuvor erwähnte Clientmodul, das in das IT-System des Heilberuflers integriert ist. Ist diese Anwendung beim Heilberufler eingerichtet, kann dieser mit seinem E-Mail-System wie gewohnt Nachrichten schreiben, senden, empfangen und lesen. Hier werden – wie bei gewöhnlichen E-Mail-Providern – Nutzername und Passwort für das Senden und Empfangen abgefragt. Auch kann er etwa Dateien an die E-Mails anhängen. Der Heilberufler muss also keine zusätzlichen Maßnahmen ergreifen, um die Ende-zu-Ende-Sicherheit zu gewährleisten, obgleich er Dokumente, die an Nachrichten angehängt werden, selbstverständlich vorher zusätzlich verschlüsseln oder qualifiziert elektronisch signieren kann.

Abbildung 10 – Die Signatur der Nachricht gewährleistet die Authentizität und Integrität der Daten



5.3 TI-Messenger

Der TI-Messenger ist eine freiwillige Anwendung der Telematikinfrastruktur, die es Leistungserbringern, Kostenträgern und zukünftig auch Versicherten ermöglicht, Ende-zu-Ende-verschlüsselt zu kommunizieren. Basierend auf dem Matrix-Protokoll ermöglicht der TI-Messenger den Teilnehmern den sicheren Austausch von Nachrichten sowie Anhängen – ad hoc und unkompliziert, wie man es von einem Messenger erwartet.

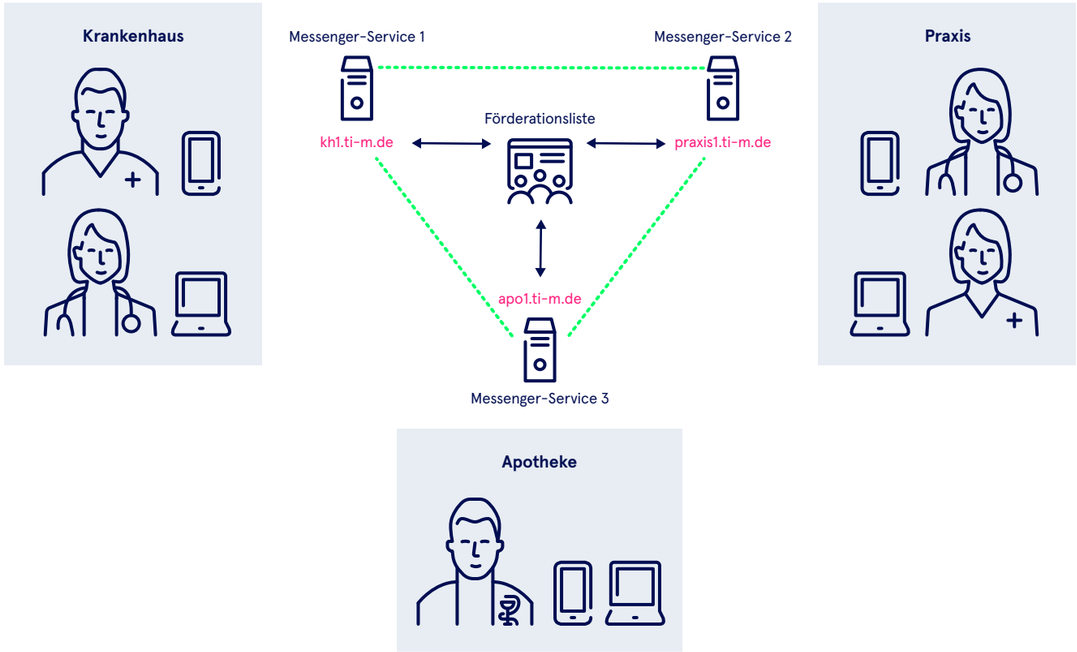
Mit KIM – Kommunikation im Medizinwesen – steht Heilberuflern ein starkes Werkzeug zur sicheren Kommunikation zur Verfügung. Aber so, wie es im privaten Umfeld einen Bedarf für Messenger gibt und die textbasierte digitale Kommunikation nicht ausschließlich via E-Mail stattfindet, existiert dieser Bedarf auch im medizinischen Versorgungsalltag – besonders dann, wenn ad hoc Kurznachrichten ausgetauscht werden sollen, womöglich sogar mobil.
An dieser Stelle schließt der TI-Messenger eine Lücke, indem er den Teilnehmern ebenjene Möglichkeit zum Austausch von Kurznachrichten bietet und dies sogar unabhängig vom Konnektor in der Praxis oder Klinik. Der TI-Messenger ist unkompliziert über das Internet erreichbar, obgleich die teilnehmenden Dienste in einer geschlossenen Föderation arbeiten, um den Anwenderkreis auf berechtige Akteure im Gesundheitswesen zu begrenzen.

Eine Föderation für berechtigte Teilnehmer

Der TI-Messenger kann jetzt schon von Mitarbeitenden von Leistungserbringerinstitutionen und Kostenträgern verwendet werden, ab Mitte des Jahres 2025 dann auch von Versicherten im Rahmen der ePA für alle. Für die Teilnahme an der Kommunikation per TI-Messenger muss sich die Organisation mittels ihrer SM(C)-B bei einem Anbieter des TI-Messenger-Dienstes registrieren – dies dient als Nachweis dafür, dass es sich um eine Organisation des Gesundheitswesens handelt.

Nach erfolgreicher Prüfung der Identität der Organisation wird beim Anbieter ein administratives Konto, der Org-Admin, für den TI-Messenger-Dienst angelegt und die Domain hinterlegt, über die die Organisation in der TI-Messenger-Föderation erreichbar ist.

Abbildung 11 – Einschränkung der Kommunikation auf Domains in der Föderationsliste



Domains, die nicht auf diese Weise für die Teilnahme in der Föderation freigeschaltet wurden, können von anderen TI-Messenger-Diensten nicht erreicht werden – die Teilnahme nicht legitimierter Akteure ist damit ausgeschlossen. Mithilfe des Org-Admin-Kontos kann ein berechtigter Administrator der Organisation dann grundsätzliche Einstellungen für den jeweiligen Dienst vornehmen und Nutzerkonten für diejenigen Mitarbeiter der Organisation anlegen, die in der Lage sein sollen, den TI-Messenger zu nutzen. Darüber hinaus können Heilberufler, die über einen Heilberufsausweis verfügen, ihre Einträge im zentralen Verzeichnisdienst verwalten, um beispielsweise ihre Auffindbarkeit als Leistungserbringer innerhalb der Föderation anzupassen.

Da die SM(C)-B nur für die Registrierung des Dienstes für eine Leistungserbringerinstitution gebraucht wird, nicht jedoch für die einzelnen Nutzerkonten, können diese Konten unabhängig von der physischen Präsenz der SM(C)-B genutzt werden – mobil und ohne VPN-Zugangsdienst. Für die Kennzeichnung von Identitäten verwenden die TI-Messenger Clients deshalb eigenes kryptografisches Material, das unabhängig von dem Schlüsselmaterial auf der SM(C)-B existiert und bei der Inbetriebnahme eines Kontos erzeugt wird. Dabei gibt es einerseits Schlüsselmaterial für die Identität eines Nutzers, aber auch für jedes der von ihm verwendeten Geräte.

Verliert eine Leistungserbringerinstitution ihren Status als Teilnehmer der TI-Messenger-Föderation, beispielsweise weil die zugehörige SM(C)-B ihre Gültigkeit verliert, so wird ihre zuvor registrierte Domain aus der zentral gepflegten Föderationsliste des TI-Messengers entfernt. Da die Föderationsliste regelmäßig von allen Teilnehmern der Föderation abgerufen wird und jedes Nutzerkonto durch seine Adresse einer bestimmten Domain zugeordnet werden kann, können die in der Föderation verbliebenen Messenger-Fachdienste erkennen, ob sie Nachrichten zustellen dürfen, die an bestimmte Nutzer gerichtet sind, oder ob Nachrichten von diesen stammen.

Ende-zu-Ende-Verschlüsselung

Neben dem langfristigen Schlüsselmaterial, das der TI-Messenger für die Klärung der Identität eines Nutzers und seiner Geräte verwendet, kommen beim TI-Messenger kurzlebige und ständig wechselnde Schlüssel für die Ver- und Entschlüsselung einzelner Nachrichten zum Einsatz. Diese können auf Basis der verwendeten Schlüsselaustauschverfahren und zusätzlichen Algorithmen lediglich von den an einer bestimmten Konversation beteiligten Nutzern – oder genauer gesagt von deren verwendeten Endgeräten – abgeleitet werden. Deshalb kann von einer Ende-zu-Ende-Verschlüsselung gesprochen werden, die es anderen Akteuren auf der Strecke, darunter auch den involvierten Fachdiensten, unmöglich macht, Einblick in die Kommunikation zu erhalten.

Auf dem Matrix-Protokoll basierend, kommen im TI-Messenger zu diesem Zweck die Protokolle Olm und Megolm zum Einsatz. Die sogenannten Megolm-Sessions sind Konstrukte, die den Aufwand für die verschlüsselte Kommunikation in großen Gruppen verringern, weil sie eine Alternative zur individuellen Verschlüsselung für jeden einzelnen Teilnehmer in der Gruppe darstellen. Dafür muss eine Megolm-Session aber erst einmal allen Teilnehmern in einer Gruppe (Chat-Raum) bekannt sein. Damit diese wiederum sicher zwischen den Teilnehmern einer Gruppe ausgetauscht werden kann, kommt Olm zum Einsatz, das für die sichere und authentisierte Kommunikation zwischen zwei Punkten – nämlich den Geräten jedes einzelnen Teilnehmers einer Gruppe – verwendet wird. Dies ist ein aufwendiges Verfahren, besonders in großen Gruppen, wird aber nur dann benötigt, wenn eine Megolm-Session erneuert wird, und nicht etwa für jede ausgetauschte Nachricht. Beide Verfahren stellen sicher, dass kein Schlüssel mehrfach verwendet wird, sie tun dies jedoch auf unterschiedliche Weise. Das Prinzip der Megolm-Sessions ist ein Verfahren, das mit dem Matrix-Protokoll erst etabliert wurde, Olm hingegen ist dem Double-Ratchet-Algorithmus entlehnt, der von Whisper Systems erfunden wurde und im Messenger „Signal" zum Einsatz kommt.

Automatische Informationssicherheit

Die beschriebenen Verfahren zum Schutz von Vertraulichkeit mit immer wechselnden Nachrichtenschlüsseln sowie der Authentisierung auf Basis langlebiger Identitätsschlüssel finden automatisch und ohne Zutun der Nutzer statt. In diesem Sinne werden Chat-Räume, in denen die Kommunikation zwischen Teilnehmern stattfindet, standardmäßig als verschlüsselnde Räume angelegt, sodass jede Nachricht, die in den Raum gesendet wird, auch verschlüsselt und authentisiert wird. Angreifer auf der Strecke und selbst die Betreiber der Fachdienste, über die die Kommunikation abgewickelt wird, können keine Einsicht nehmen. Schafft es ein Angreifer, sich im Namen eines legitimen Nutzers in ein existierendes Konto einzuloggen, werden die anderen Teilnehmer vor der Präsenz eines nicht authentisierten Teilnehmers – genauer gesagt Geräts – gewarnt, weil dieser Angreifer mit dem erfolgreichen Login nicht auch die langlebigen Identitäts- und Geräteschlüssel des legitimen Nutzers erhält.

5.4 Elektronische Patientenakte (ePA für alle)

Die elektronische Patientenakte (ePA) ist eine für den Versicherten freiwillige Anwendung der Telematikinfrastruktur. Die zuständige Krankenkasse legt für jeden Versicherten eine ePA an, sofern der Versicherte dem nicht gegenüber seiner Krankenkasse widersprochen hat (Opt-out).

ePA für alle

In die ePA eines Versicherten speichern die ihn behandelnden Leistungserbringer medizinische Informationen, die während der medizinischen Behandlung entstehen. Die Informationen in der ePA können dann auch von anderen Leistungserbringern genutzt werden, die den Versicherten ebenfalls behandeln. Auch der Versicherte selbst kann Informationen in seine ePA stellen, um sie seinen behandelnden Leistungserbringern zur Verfügung zu stellen.

Die ePA wird sukzessive in die Versorgungsprozesse integriert. Zum Beispiel wird durch das Zusammenspiel der ePA mit dem E-Rezept automatisch die **elektronische Medikationsliste** des Versicherten aus den Verordnungs- und Dispensierdaten erzeugt, die vom E-Rezept-Fachdienst in die ePA des Versicherten übermittelt wurden. Leistungserbringer können die elektronische Medikationsliste zur Arzneimitteltherapie nutzen und so beispielsweise unerwünschte Wechselwirkungen von Medikamenten erkennen.

Der Versicherte kann alle Informationen in seiner ePA einsehen. Um die Transparenz des Versicherten über seine Behandlungen weiter zu verbessern, übermittelt die Krankenkasse die ihr vorliegenden Abrechnungsdaten zu den Behandlungen des Versicherten in die ePA.

5.4.1 Nutzer der ePA

Die medizinischen Daten in der ePA stehen nur einem beschränkten Nutzerkreis zur Verfügung.

Hierzu gehört zuallererst der Versicherte als Inhaber der ePA. Der Versicherte kann auf alle Daten seiner ePA zugreifen.

Versicherte können andere Personen (z. B. Partner, Eltern, Enkel) als **Vertreter** einrichten, um auch diesen Personen den Zugriff auf ihre ePA zu erlauben. Vertreter können den Versicherten dann im Rahmen seiner Gesundheitsversorgung unterstützen. Vertreter haben dieselben Zugriffsrechte wie ein Versicherter, können jedoch keine weiteren Vertreter einrichten oder für den Versicherten der ePA widersprechen.

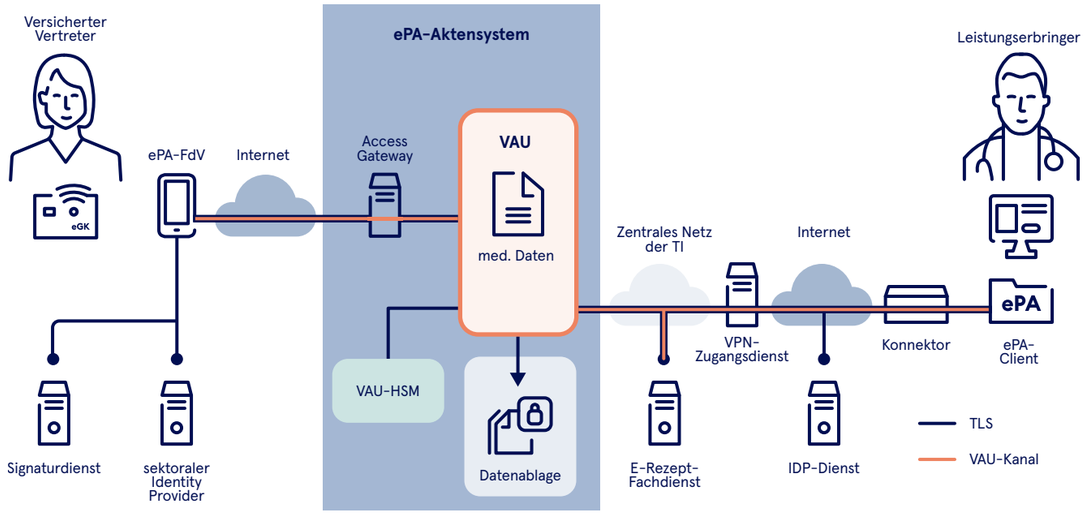
Voraussetzung für den Zugriff eines Arztes, Zahnarztes, Apothekers und sonstigen **Leistungserbringers** ist immer eine zuvor durch den Versicherten oder seinen Vertreter erstellte Befugnis. Befugnisse für Leistungserbringerinstitutionen können entweder mithilfe einer App oder implizit beim Leistungserbringer durch Stecken der elektronischen Gesundheitskarte erstellt werden. Mit einer solchen Befugnis können Leistungserbringer innerhalb des vorgegebenen Rahmens des Sozialgesetzbuches V auf medizinische Daten in ePAs zugreifen.

Die **Krankenkasse** des Versicherten kann im Rahmen der gesetzlichen Vorgaben Informationen für den Versicherten in eine ePA einstellen (z. B. Abrechnungsdaten, Hinweise zum Gesundheitsschutz oder digitalisierte Papierdokumente, die auf Antrag des Versicherten durch die Krankenkasse digitalisiert wurden). Krankenkassen können jedoch keine Daten in einer ePA lesen.

Die **Ombudsstelle** der Krankenkasse kann auf Wunsch des Versicherten die Zugriffsprotokolle aus der ePA auslesen und dem Versicherten zur Verfügung stellen sowie Widersprüche verwalten. Die Ombudsstellen können jedoch nicht auf medizinische Daten einer ePA zugreifen.

Festgelegte Daten einer ePA werden automatisch in pseudonymisierter Form an das **Forschungsdatenzentrum Gesundheit** (https://www.bfarm.de/DE/Das-BfArM/Aufgaben/Forschungsdatenzentrum/_node.html) übermittelt. Es werden ausschließlich Daten der ePA übermittelt, die zuverlässig pseudonymisiert werden können. Dies sind in der ersten Stufe ausschließlich Rezept- und Dispensierinformationen, in Folgestufen können dann weitere Daten hinzukommen. Versicherte können der Übermittlung ihrer Daten an das Forschungsdatenzentrum jederzeit widersprechen oder die Nutzung der übermittelten Daten durch das Forschungsdatenzentrum auf bestimmte Zwecke einschränken.

Abbildung 12 – Sicherheitsarchitektur



5.4.2 Überblick über die Sicherheitsarchitektur

Abbildung 12 gibt einen Überblick über die wesentlichen Komponenten und Dienste der ePA für alle.

ePA-Frontend des Versicherten (ePA-FdV)

Das ePA-FdV ist eine von der Krankenkasse bereitgestellte App, die der Versicherte auf seinem Endgerät (mobil oder stationär) installiert. Mit diesem ePA-FdV nutzen und kontrollieren Versicherte bzw. befugte Vertreter ihre ePA, um z. B. die Daten in der ePA einzusehen, Befugnisse für Leistungserbringerinstitutionen zu erstellen bzw. zu löschen, Widersprüche zu verwalten oder Zugriffe nachzuvollziehen.

ePA-Aktensystem

Die ePA eines Versicherten wird in einem **ePA-Aktensystem** verarbeitet und verschlüsselt gespeichert. Es gibt mehrere Betreiber von ePA-Aktensystemen.

Zentrale technische Sicherheitsmaßnahme im ePA-Aktensystem zum Schutz der im Klartext verarbeiteten medizinischen Daten ist eine **vertrauenswürdige Ausführungsumgebung (VAU)**. Eine VAU stellt mit technischen Maßnahmen sicher, dass niemand, auch nicht Mitarbeiter des Betreibers des Aktensystems mit maximalen Zugriffsrechten, auf Daten, die innerhalb der VAU verarbeitet werden, zugreifen kann. Dadurch können sensible Daten serverseitig im Klartext verarbeitet werden, um z. B. eine elektronische Medikationsliste zu erzeugen oder Zugangs- und Zugriffspolicys serverseitig durchzusetzen.

Ein Hardware Security Module (HSM) speichert die für den Betrieb des ePA-Aktensystems benötigten kryptografischen Schlüssel, z. B. die kryptografische Identität der VAU, mit der sich diese gegenüber einem ePA-FdV bzw. ePA-Clients authentisiert, oder Geheimnisse, die für die Verschlüsselung der medizinischen Daten der ePAs benötigt werden. Diese Schlüssel werden im Vier-Augen-Prinzip zusammen mit der gematik ins HSM eingebracht. Ein HSM ist eine besonders sicherheitsgehärtete und geprüfte Hardwarekomponente. Das HSM für die ePA wird als **VAU-HSM** bezeichnet und besitzt ein spezielles Firmware-Modul zur Umsetzung der ePA-spezifischen Sicherheitslogik. Das Firmware-Modul sorgt z. B. dafür, dass ein Zugriff auf das VAU-HSM nur durch integre VAUs und nicht durch einen Mitarbeiter des Betreibers des ePA-Aktensystems möglich ist.

Versicherte erreichen das ePA-Aktensystem mithilfe eines ePA-FdVs über das Internet. Ein **Access Gateway** im ePA-Aktensystem schützt vor Angriffen aus dem Internet und leitet die Nachrichten über interne Proxys weiter.

ePA-Client

ePA-Clients setzen die Client-Logik der ePA um und laufen in den Systemen der Leistungserbringer (z. B. Ärzte, Zahnärzte, Apotheker), der Krankenkassen oder der Ombudsstellen. Der netztechnische Zugang zum ePA-Aktensystem erfolgt für Leistungserbringer über den Konnektor oder ein TI-Gateway, für Krankenkassen und Ombudsstellen über einen Basis-Consumer.

Sektoraler Identity Provider

Ein sektoraler Identity Provider (IDP) der Krankenkassen stellt Versicherten eine digitale Identität (GesundheitsID) bereit (siehe Kapitel 3.1.3). Versicherte melden sich am ePA-Aktensystem mit ihrer GesundheitsID an.

IDP-Dienst

Leistungserbringer, Krankenkassen und Ombudsstellen nutzen für die Anmeldung am ePA-Aktensystem den IDP-Dienst. Eine Anmeldung am Aktensystem ist ausschließlich nach einer erfolgreichen Authentisierung des Leistungserbringers, der Krankenkasse oder Ombudsstelle am IDP-Dienst mithilfe einer Institutionenkarte SMC-B möglich.

Signaturdienst

Versicherte nutzen den Signaturdienst, um am ePA-FdV erstellte Befugnisse zu signieren.

E-Rezept-Fachdienst

Der E-Rezept-Fachdienst stellt Verordnungs- und Dispensierinformationen in die ePAs der Versicherten ein, sofern der Versicherte dem nicht widersprochen hat.

Schutz der transportierten medizinischen Daten

Die medizinischen Daten der ePA werden ausschließlich über verschlüsselte Kommunikationsstrecken transportiert. Auf jeder Kommunikationsstrecke werden die transportierten medizinischen Daten der ePA dabei immer durch zwei voneinander unabhängige Mechanismen geschützt. Diese Mechanismen stellen sicher, dass weder ein Angreifer im Internet noch ein potenzieller Innentäter beim Betreiber des ePA-Aktensystems auf die transportierten medizinischen Daten zugreifen kann.

Zum Schutz der Kommunikationsstrecken zwischen ePA-Aktensystem und ePA-FdV, ePA-Client bzw. E-Rezept-Fachdienst werden ein serverseitig authentifizierter TLS-Kanal und ein beidseitig authentisierter VAU-Kanal aufgebaut. Der VAU-Kanal endet direkt in der VAU und bietet so auch Schutz gegen einen Innentäter beim Betreiber des ePA-Aktensystems. Das VAU-Protokoll ist so entworfen, dass es Forward-Secrecy und Post-Quantum-Resistenz bietet.

Die Kommunikationsstrecken zwischen ePA-FdV und Signaturdienst bzw. sektoralen Identity Providern sind ebenso mittels TLS gesichert wie die Strecke zwischen ePA-Client und IDP-Dienst. Über die Kommunikationsstrecken zum Signaturdienst und zu den Identity Providern werden keine medizinischen Daten transportiert.

5.4.3 Befugnisse als Zugriffsvoraussetzung

Nutzer können ausschließlich mit einer gültigen Befugnis auf eine ePA zugreifen. Der Versicherte ist immer für seine ePA befugt und kann auf alle Inhalte zugreifen.

Um ihre gesetzliche Pflicht zu erfüllen, sind die Krankenkassen dazu befugt, ihren Versicherten die gesetzlich in die ePA einzustellenden Daten zu übermitteln. Die Krankenkasse kann niemals dazu befugt werden, Daten einer ePA zu lesen.
Die Ombudsstelle der Krankenkasse des Versicherten ist immer dazu befugt, ihren gesetzlichen Pflichten zum Auslesen der Protokolldaten und zur Verwaltung von Widersprüchen nachzukommen. Die Ombudsstelle kann niemals dazu befugt werden, auf medizinische Daten einer ePA zuzugreifen.

Leistungserbringer sind zunächst nicht befugt, auf eine ePA zuzugreifen. Dies wird erst möglich, wenn sie hierzu vom Versicherten oder einem Vertreter technisch befugt wurden. Dies kann entweder explizit am ePA-FdV oder implizit in einer Leistungserbringerinstitution durch Stecken der elektronischen Gesundheitskarte erfolgen. Beim Ausstellen einer Befugnis am ePA-FdV wählt der Versicherte die zu befugende Leistungserbringerinstitution zunächst im Verzeichnisdienst der Telematikinfrastruktur aus. Er setzt die Gültigkeitsdauer der Befugnis (von einem Tag bis zu einer unbegrenzten Gültigkeitsdauer) und signiert die Befugnis mithilfe des Signaturdienstes. Die signierte Befugnis wird vom ePA-FdV an das ePA-Aktensystem übermittelt und das VAU-HSM übernimmt die Befugnis bei positiver Prüfung der Signatur in die ePA des Versicherten. Versicherte können einer Leistungserbringerinstitution die Befugnis am ePA-FdV jederzeit wieder entziehen oder die Gültigkeitsdauer anpassen.

Versicherte können auch Befugnisse für Vertreter am ePA-FdV erstellen. In diesem Fall wird anstelle der Leistungserbringerinstitution die Krankenversicherungsnummer des Vertreters in die Befugnis aufgenommen. Ein befugter Vertreter kann auf alle Inhalte der ePA des Versicherten zugreifen. Er kann zudem Befugnisse für Leistungserbringerinstitutionen für die ePA des Versicherten erstellen. Vertreter können jedoch keine Befugnisse für weitere Vertreter der ePA des Versicherten erstellen.

Leistungserbringerinstitutionen können im Rahmen ihrer gesetzlichen Zugriffsrechte auf die ePA eines Versicherten zugreifen, wenn der Versicherte in der Leistungserbringerumgebung seine elektronische Gesundheitskarte in das dortige Kartenterminal steckt (es ist hierfür keine PIN-Eingabe des Versicherten erforderlich). Durch das Stecken wird ein technischer Nachweis dafür erstellt, dass die elektronische Gesundheitskarte vorhanden ist. Diese Information wird vom Primärsystem an das ePA-Aktensystem übergeben. Das VAU-HSM prüft den technischen Nachweis und übernimmt die Befugnis für die Leistungserbringerinstitution bei positivem Prüfergebnis in die ePA des Versicherten. Je nach fachlicher Rolle der Leistungserbringerinstitution setzt das VAU-HSM die Gültigkeitsdauer der Befugnis auf die gesetzlich vorgegebenen 90 Tage (z. B. Ärzte, Zahnärzte) bzw. drei Tage (z. B. Apotheken).

5.4.4 Einschränken des Zugriffs

Mit einer gültigen Befugnis kann eine Leistungserbringerinstitution auf die ePA zugreifen, in dem Rahmen, den das Sozialgesetzbuch V vorgibt. Die gesetzlichen Vorgaben regeln, welche fachlichen Leistungserbringerrollen (u. a. Ärzte, Zahnärzte, Apotheker, Pflegekräfte) auf welche Kategorien von Daten

(u. a. Arztbriefe, Medikationsdaten, Impfdokumentation) zugreifen dürfen. Die gesetzlichen Vorgaben werden durch das ePA-Aktensystem durchgesetzt. Ein Versicherter kann die gesetzlichen Zugriffsrechte für Leistungserbringerinstitutionen für seine ePA nicht erweitern. Er kann jedoch die Zugriffsmöglichkeiten weiter einschränken:

Blocked User Policy: Versicherte bzw. Vertreter können Leistungserbringerinstitutionen in die Blocked User Policy aufnehmen. Eine solche Leistungserbringerinstitution kann dann nicht mehr befugt werden und nicht mehr auf die ePA des Versicherten zugreifen.

General Deny Policy: Versicherte bzw. Vertreter können einzelne Dokumente, Kategorien oder Ordner von Dokumenten auf die General Deny Policy setzen. Auch befugte Leistungserbringerinstitutionen können diese Dokumente dann nicht mehr sehen. Ein Zugriff auf diese Dokumente ist ausschließlich durch den Versicherten oder einen Vertreter möglich.

User Specific Deny Policy Medication: Versicherte bzw. Vertreter können Leistungserbringerinstitutionen in die User Specific Deny Policy Medication aufnehmen. Diese Leistungserbringerinstitutionen können dann nicht mehr auf den Medication Service zugreifen. Insbesondere können sie nicht mehr die elektronische Medikationsliste einsehen.

5.4.5 Widerspruchsmöglichkeiten des Versicherten

Versicherte haben im Rahmen der ePA unterschiedliche Widerspruchsmöglichkeiten.

Grundsätzlicher Widerspruch gegen die ePA: Versicherte können gegenüber ihrer Krankenkasse jederzeit der Nutzung einer ePA widersprechen. Falls ein Widerspruch gegen die Nutzung der ePA bei der Krankenkasse vorliegt, unterlässt diese die Anlage einer ePA bzw. löscht eine gegebenenfalls bestehende ePA einschließlich aller Daten.

Widerspruch gegen das Einstellen von Abrechnungsdaten: Krankenkassen sind gesetzlich dazu verpflichtet, Abrechnungsdaten in die ePA zu übertragen. Dem können Versicherte gegenüber ihrer Krankenkasse jederzeit widersprechen. Falls ein solcher Widerspruch vorliegt, unterlässt die Krankenkasse das Einstellen von Abrechnungsdaten in die ePA. Die bis zum Zeitpunkt des Widerspruchs übermittelten Abrechnungsdaten bleiben in der ePA erhalten.

Widerspruch gegen die Teilnahme am Medikationsprozess: Bei einem solchen Widerspruch können Leistungserbringer nicht mehr den Medication Service inklusive elektronischer Medikationsliste nutzen. Die vom E-Rezept-Fachdienst eingestellten Daten des Medication Service bleiben jedoch weiterhin in der ePA des Versicherten und können durch den Versicherten bzw. einen befugten Vertreter am ePA-FdV eingesehen werden. Zudem stellt der E-Rezept-Fachdienst weiterhin E-Rezept-Informationen und Dispensierinformationen in die ePA ein.

Widerspruch gegen das automatische Einstellen von Verordnungs- und Dispensierdaten durch den E-Rezept-Fachdienst: Bei einem solchen Widerspruch werden alle vom E-Rezept-Fachdienst in die ePA eingestellten Daten gelöscht und der E-Rezept-Fachdienst stellt zukünftig keine Daten mehr in die ePA ein. Ein Widerspruch gegen das automatische Einstellen von Verordnungs- und Dispensierdaten durch den E-Rezept-Fachdienst in die ePA des Versicherten impliziert einen Widerspruch gegen die Teilnahme am Medikationsprozess.

Widerspruch gegen die Verarbeitung von Daten der ePA zu Forschungszwecken: Das ePA-Aktensystem übermittelt den Widerspruch an das Forschungsdatenzentrum Gesundheit. Ab diesem Zeitpunkt werden entsprechend keine Daten des Versicherten mehr zu Forschungszwecken an das Forschungsdatenzentrum Gesundheit weitergeleitet.

Versicherte haben zudem die Möglichkeit, den Widerspruch auf bestimmte Zwecke nach § 303e Abs. 2 SGB V zu beschränken. In diesem Fall werden die Daten des Versicherten vom Aktensystem weiterhin an das Forschungsdatenzentrum Gesundheit übermittelt, das Forschungsdatenzentrum muss jedoch die vom Versicherten gewünschten Zwecke berücksichtigen.

5.4.6 Protokollierung zur Kontrolle durch den Versicherten

Damit Versicherte die Zugriffe auf ihre ePA kontrollieren können, werden diese im Aktensystem protokolliert. Der Protokolleintrag dokumentiert, welcher Nutzer auf die ePA zugegriffen hat, zu welchem Zeitpunkt und mit welchem Ziel. Protokolliert wird insbesondere

- jeder Zugriff auf die medizinischen Daten des Versicherten,
- jedes Einstellen einer Befugnis,
- jede Änderung eines Widerspruchs.

Der Versicherte oder ein befugter Vertreter kann die Protokolleinträge für die Zeit von drei Jahren mithilfe eines ePA-FdVs einsehen und lokal sichern. Darüber hinaus können Versicherte bei ihrer zuständigen Ombudsstelle beantragen, dass ihnen die in der ePA vorliegenden Protokolldaten zur Verfügung gestellt werden. Dies ist insbesondere eine Alternative für Versicherte, die kein ePA-FdV nutzen.

5.4.7 Verschlüsselte Speicherung der Daten im ePA-Aktensystem

Die medizinischen Daten der ePAs werden im ePA-Aktensystem kryptografisch verschlüsselt gespeichert. Für jeden Versicherten wird hierfür ein eigener symmetrischer Schlüssel verwendet.

Diese versichertenindividuellen Schlüssel werden im VAU-HSM abgeleitet und nur innerhalb des VAU-HSM oder einer VAU verarbeitet. Die versichertenindividuellen Schlüssel werden niemals im ePA-Aktensystem gespeichert und verlassen es auch niemals.
Im Folgenden ist beispielhaft der Ablauf der Verschlüsselung für den Fall dargestellt, dass ein Arzt ein medizinisches Dokument in der ePA eines Versicherten speichert. Bei anderen Nutzern läuft die Verschlüsselung analog ab.

1. Der Arzt meldet sich am ePA-Aktensystem an und übermittelt das zu speichernde Dokument von seinem Primärsystem (ePA-Client) über den verschlüsselten TLS-/VAU-Kanal in eine VAU im ePA-Aktensystem, um es in der ePA des Versicherten zu speichern.
2. Um das übermittelte Dokument in der ePA des Versicherten abspeichern zu können, erfragt die VAU vom VAU-HSM den individuellen Schlüssel des Versicherten.
3. Nur wenn das VAU-HSM erfolgreich technisch prüfen konnte, dass für den angemeldeten Arzt eine gültige Befugnis für die ePA des Versicherten vorliegt, leitet es den versichertenindividuellen Schlüssel aus der Krankenversicherungsnummer des Versicherten und einem im VAU-HSM gespeicherten Geheimnis ab. Der versichertenindividuelle Schlüssel wird über einen beidseitig authentisierten und verschlüsselten Kanal vom VAU-HSM in die VAU übermittelt. Die versichertenindividuellen Schlüssel der Versicherten werden ausschließlich im VAU-HSM oder in einer VAU verarbeitet und niemals gespeichert.
4. In der VAU wird das Dokument mit dem versichertenindividuellen Schlüssel codiert und im ePA-Aktensystem gespeichert. Der versichertenindividuelle Schlüssel wird anschließend in der VAU wieder gelöscht.

Die Entschlüsselung beim Abruf von ePA-Daten läuft ähnlich ab. Auch in diesem Fall wird der benötigte Schlüssel des Versicherten vom VAU-HSM auf Basis einer technisch nachgewiesenen Befugnis abgeleitet und in eine VAU übermittelt, in der dann die verschlüsselten Daten decodiert werden.

5.4.8 Schutz vor Schadcode

In die ePA können sowohl strukturierte FHIR-Daten (Fast Healthcare Interoperability Resources) als auch Dokumente eingestellt werden. Während ein Transport von Schadcode in FHIR-Daten nicht möglich ist, sind einige Dokumentenformate hierfür anfällig, z. B. Zip-Dateien, Office-Dokumente oder PDF-Dokumente. Öffnen Nutzer solche Dokumente mit entsprechend konfigurierten Leseprogrammen kann ein Schadcode, der im Dokument enthalten ist, ausgeführt werden.

Um einen Schaden des ePA-Aktensystems oder der Systeme der Nutzer durch potenziellen Schadcode in Dokumenten einer ePA zu vermeiden, werden die erlaubten Dokumentenformate im ePA-Aktensystem eingeschränkt. Bei den im Aktensystem erlaubten Dokumentenformaten kann kein Schadcode eingebracht werden, der von den zugehörigen Leseprogrammen unmittelbar ausgeführt wird. So können beispielsweise ausschließlich PDF-Dokumente im Format PDF/A-1 und PDF/A-2 in eine ePA eingestellt werden, nicht aber PDF- oder PDF/A-3-Dokumente, die ausführbaren Schadcode enthalten könnten. Beim Einstellen eines Dokuments werden die Formate der Dokumente im Aktensystem geprüft und Dokumente mit unzulässigem Format abgewiesen.

5.5 Elektronisches Rezept

Mit der Einführung des elektronischen Rezepts (E-Rezept) wurde das bisherige Verfahren mit dem gedruckten Formular für apothekenpflichtige Arzneimittel ab Mitte 2021 sukzessive abgelöst. Seit Anfang 2024 ist die Nutzung des E-Rezepts bundesweit für alle Beteiligten Pflicht. Der Funktionsumfang der Anwendung wird laufend erweitert, um die Vorteile der Digitalisierung auch bei anderen Rezepttypen und im Zusammenspiel mit anderen Anwendungen, wie der elektronischen Patientenakte, nutzen zu können. Zudem wurde der Nutzerkreis auf Privatversicherte erweitert, die dafür eine Krankenversicherungsnummer benötigen.

E-Rezept

Die Anwendung „E-Rezept" ermöglicht in der aktuellen Ausbaustufe eine Übermittlung von ärztlichen und zahnärztlichen Verordnungen für apothekenpflichtige Arzneimittel, Mehrfachverordnungen sowie die Verordnung von digitalen Gesundheitsanwendungen (DiGA) in elektronischer Form.

Der verordnende Leistungserbringer erstellt für einen Versicherten ein E-Rezept, das auf dem zentralen E-Rezept-Fachdienst abgelegt wird. DiGA-Verordnungen werden durch die Krankenkasse des Versicherten eingelöst. Für die anderen Verordnungen hat der Versicherte verschiedene Möglichkeiten, sein E-Rezept in einer Apotheke einzulösen.

Der einfachste und am häufigsten genutzte Einlöseweg ist das Stecken der elektronischen Gesundheitskarte in einer Apotheke, wodurch der Apotheker alle E-Rezepte des Karteninhabers abrufen und – wenn vom Versicherten gewünscht – einlösen kann. Aus Gründen der Barrierefreiheit ist hierbei keine Eingabe der PIN durch den Versicherten erforderlich. Übrigens: Auch wenn es den Anschein hat – die E-Rezepte sind auch in diesem Fall nicht auf der Gesundheitskarte gespeichert, sondern immer auf dem zentralen E-Rezept-Fachdienst.

Ein weiterer Einlöseweg ist der Ausdruck der Zugriffsinformationen für ein E-Rezept in Form eines 2D-Codes durch den verordnenden Leistungserbringer. Mit diesem Ausdruck kann der Apotheker auf das E-Rezept zugreifen, indem er den 2D-Code einscannt. Auch hier gilt: Die E-Rezepte sind auf dem zentralen E-Rezept-Fachdienst gespeichert. Auf dem Ausdruck sind lediglich die Informationen aufgedruckt, die für den Zugriff auf ein E-Rezept erforderlich sind – der E-Rezept-Token –, und zusätzliche Informationen, die es dem Versicherten ermöglichen, seine E-Rezepte zu unterscheiden, da auf dem Ausdruck Platz für vier 2D-Codes und vier E-Rezepte vorhanden ist. Durch die Übergabe des Ausdrucks an eine andere Person kann diese als Vertreter die E-Rezepte in einer Apotheke einlösen. Auch wenn bei diesem Einlöseweg wieder Papier zum Einsatz kommt, bleiben wesentliche Vorteile des digitalen E-Rezepts erhalten: Die Informationen werden vollständig digital erfasst, vertraulich und fälschungssicher zwischen den Beteiligten ausgetauscht und können digital in den Systemen der Apotheken und Krankenkassen weiterverarbeitet werden.

Der komfortabelste Einlöseweg ist die Verwendung einer App auf einem mobilen Gerät, die eine Verwaltung und Einlösung von E-Rezepten gestattet. Dies können Apps der Krankenkassen sein, die die E-Rezept-Funktionalität integriert haben, oder die E-Rezept-App der gematik. Mit einer solchen App kann der Versicherte den E-Rezept-Token bereitstellen, der eine Apotheke für den Zugriff auf ein konkretes Rezept auf dem E-Rezept-Fachdienst berechtigt. Der Versicherte übermittelt dabei den E-Rezept-Token entweder elektronisch an eine Apotheke oder legt ihn in Form eines 2D-Codes in einer Apotheke vor. Die elektronische Übertragung des E-Rezept-Tokens an eine Apotheke erfolgt über den E-Rezept-Fachdienst. Die E-Rezept-App bietet die Möglichkeit der Absicherung für den Zugriff auf die lokal gespeicherten Daten

(z. B. durch die elektronische Gesundheitskarte, ein Passwort, ein biometrisches Merkmal) und sie steuert die Authentisierung des Versicherten gegenüber dem E-Rezept-Fachdienst.

Für den Zugang zum E-Rezept-Fachdienst nutzt der Versicherte seine elektronische Gesundheitskarte (eGK) mit NFC-Schnittstelle und eGK-PIN oder seine GesundheitsID, sodass eine Nutzung des E-Rezepts auch ohne zusätzliche Hardware an den Geräten des Versicherten möglich ist.

Der Versicherte hat die Hoheit über seine E-Rezepte, da jeglicher Zugriff auf eines seiner E-Rezepte auf dem E-Rezept-Fachdienst entweder nur für den Versicherten selbst oder – nach Übergabe eines E-Rezept-Tokens – einen Vertreter des Versicherten, eine Apotheke bzw. eine Krankenkasse möglich ist. Der E-Rezept-Token realisiert dabei ein Besitzmodell, d. h. wer im Besitz des E-Rezept-Tokens ist, kann damit die Einlösung des E-Rezepts veranlassen. Ein Versicherter kann sein E-Rezept auch selbst löschen, sich also dafür entscheiden, ein E-Rezept nicht einzulösen. Versicherte können das Löschen auch durch einen Apotheker veranlassen. Dazu müssen sie den entsprechenden E-Rezept-Token an die Apotheke senden oder dort vorweisen. Vertreter von Versicherten können deren E-Rezepte nicht löschen.

Zugriffe auf E-Rezepte werden im E-Rezept-Fachdienst protokolliert und sind durch den jeweils betroffenen Versicherten über die E-Rezept-App einsehbar.

Zum Nachweis der Sicherheit einer App mit E-Rezept-Funktionalität einer Krankenkasse bzw. der E-Rezept-App der gematik musste der jeweilige Hersteller ein externes Sicherheitsgutachten erstellen lassen, das durch das Bundesamt für Sicherheit in der Informationstechnik geprüft wurde.

Übermittlung von Daten in die elektronische Patientenakte

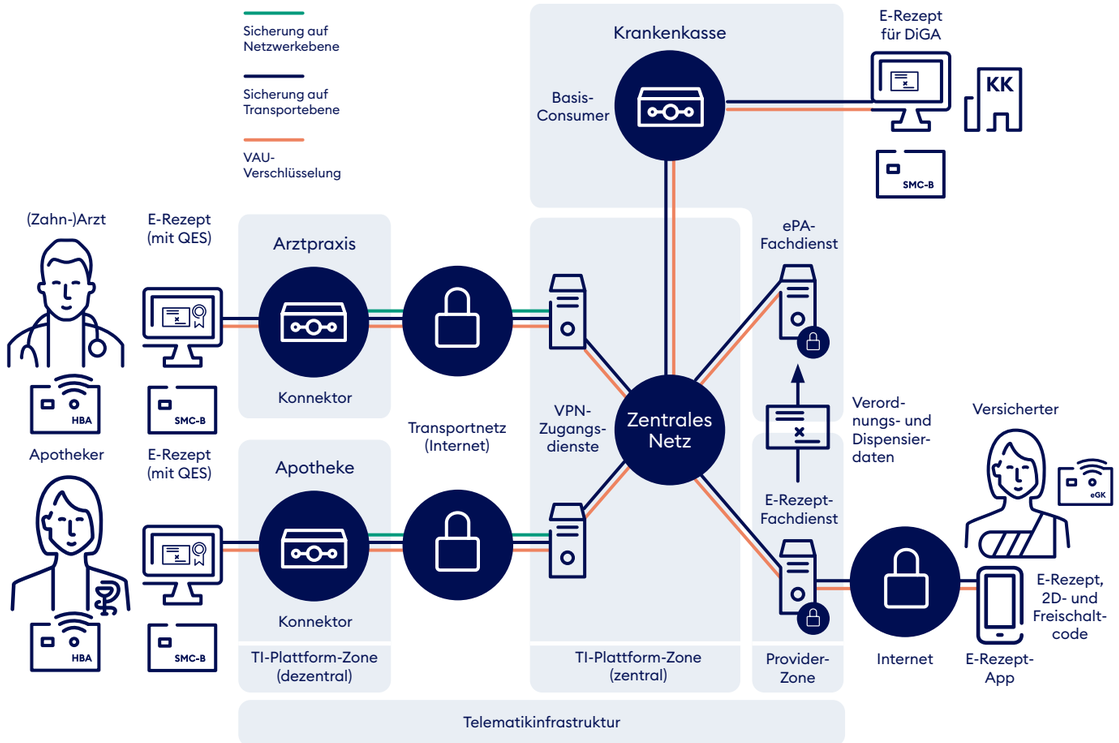
Um den digital gestützten Medikationsprozess (siehe Kapitel 5.4) zu unterstützen, werden die Informationen von ärztlichen und zahnärztlichen Verordnungen für apothekenpflichtige Arzneimittel vom E-Rezept-Fachdienst in die ePA übermittelt – jedoch nur, wenn der Versicherte weder dem Anlegen seiner elektronischen Patientenakte noch dem Einstellen von Daten aus dem E-Rezept-Fachdienst widersprochen hat. Es besteht auch die Möglichkeit, dass der Versicherte nur der Teilnahme am digital gestützten Medikationsprozess (dgMP)widerspricht, nicht aber dem Einstellen der Daten aus dem E-Rezept-Fachdienst. In dieser Konstellation werden die Daten vom E-Rezept-Fachdienst in die ePA übertragen und der Versicherte kann sich diese Daten als elektronische Medikationsliste aufbereitet anschauen. Alle Widerspruchsoptionen werden in der Anwendung elektronische Patientenakte verwaltet.

Die Übertragung der Daten vom E-Rezept-Fachdienst in die ePA erfolgt transportverschlüsselt über das zentrale Netz der Telematikinfrastruktur. Die beiden Dienste (E-Rezept-Fachdienst, ePA-Aktensystem) kommunizieren vor einem Datenaustausch darüber, ob sie jeweils mit dem richtigen Gesprächspartner kommunizieren.

Ende-zu-Ende-Sicherheit

Die verordnenden Leistungserbringer, also insbesondere Ärzte und Zahnärzte, erstellen E-Rezepte in ihren Primärsystemen und signieren diese elektronisch mithilfe ihres Heilberufsausweises und unter Zuhilfenahme des Konnektors. Durch die qualifizierte elektronische Signatur (QES) kann nachvollzogen werden, wer das E-Rezept ausgestellt hat, und die Integrität des E-Rezepts kann vom Apotheker bzw. von der Krankenkasse geprüft werden. Vom IT-System des verordnenden Leistungserbringers wird das E-Rezept über den Konnektor in die Telematikinfrastruktur transportiert. Die Verbindung vom Konnektor zum VPN-Zugangsdienst der Telematikinfrastruktur wird über ein VPN auf Netzwerkebene kryptografisch gesichert. Das IT-System selbst baut eine transportgesicherte Verbindung (TLS) zur Infrastruktur des E-Rezept-Fachdienstes auf.

Abbildung 13 – Ende-zu-Ende-Sicherheit für das E-Rezept



Für Experten:
Vertrauenswürdige Ausführungsumgebung

Wie in allen Anwendungen der Telematikinfrastruktur ist auch beim E-Rezept die Herstellung einer Ende-zu-Ende-Sicherheit für alle Betroffenen das Ziel. E-Rezepte werden nicht Ende-zu-Ende-verschlüsselt, um die Anwendung flexibel und zukunftssicher gestalten zu können. Deshalb musste ein anderer Mechanismus gefunden werden, um das Ziel der Ende-zu-Ende-Sicherheit dennoch zu erreichen. Dieser Mechanismus wird „vertrauenswürdige Ausführungsumgebung" (VAU) genannt.

Die VAU sorgt dafür, dass selbst der Anbieter des E-Rezept-Fachdienstes keinen Einblick in die übertragenen, zu verarbeitenden und gespeicherten E-Rezepte erhält.

Nach dem transportgesicherten Verbindungsaufbau (TLS) zum E-Rezept-Fachdienst wird als zusätzlicher Schutz eine weitere Transportsicherung aufgebaut, die direkt bis in die VAU reicht.

Diese doppelte Transportsicherung greift auch, wenn der Apotheker nach Erhalt eines E-Rezept-Tokens E-Rezepte vom Fachdienst abruft oder ein Versicherter mit der E-Rezept-App auf seine E-Rezepte zugreift.

Über diesen technischen Mechanismus wird sichergestellt, dass der Anbieter des E-Rezept-Fachdienstes zu keinem Zeitpunkt E-Rezepte im Klartext einsehen kann.

In der Telematikinfrastruktur gibt es einen Anbieter für den E-Rezept-Fachdienst, der von der gematik beauftragt ist und den Fachdienst nach den Vorgaben der gematik aufgebaut hat. Der Betrieb findet redundant an mehreren Standorten in Deutschland statt, um die erforderlich hohe Verfügbarkeit des Dienstes zu erreichen.

5.6 Notfalldaten-Management

Das Notfalldaten-Management umfasst zwei freiwillige medizinische Anwendungen der Telematikinfrastruktur, bei denen Daten des Versicherten auf der elektronischen Gesundheitskarte gespeichert und von Heilberuflern bei Bedarf gelesen werden können. Bei den Daten handelt es sich zum einen um den Notfalldatensatz und zum anderen um den Datensatz Persönliche Erklärungen.

Die beiden Anwendungen sind als Fachmodul Notfalldaten-Management auf dem Konnektor des Heilberuflers umgesetzt. Für das Notfalldaten-Management wird also kein Fachdienst in der Telematikinfrastruktur benötigt.

Notfallrelevante Informationen

Der Notfalldatensatz soll Heilberuflern in einer Notfallsituation die Möglichkeit geben, relevante medizinische Informationen zum Versicherten zu erhalten, auch wenn dieser im Moment gar nicht auskunftsfähig ist (z. B. wegen Bewusstlosigkeit oder eines Schocks). In Abstimmung mit den Heilberuflern sind folgende Daten als notfallrelevant definiert worden:

- Befunddaten
  - besondere Hinweise (z. B. Schwangerschaft, Implantate)
  - Allergien und Unverträglichkeiten
  - Diagnosen
- Medikationsdaten, Arzneimittel (Wirkstoffe, Dosierschema)
- freiwillige Zusatzinformationen des Versicherten

Zudem ist im Notfalldatensatz auf der Gesundheitskarte auch jeweils der Name des Heilberuflers hinterlegt, der den Notfalldatensatz erstellt bzw. diesem eine Information hinzugefügt hat.

Hinweise, wo sich die persönlichen Erklärungen befinden

Der Datensatz Persönliche Erklärungen enthält Hinweise auf den Aufbewahrungsort der Gewebe- und Organspendeerklärung, der Vorsorgevollmacht sowie der Patientenverfügung. Er beinhaltet im Gegensatz zum Notfalldatensatz nicht die Daten selbst. In den Informationen zur Vorsorgevollmacht sind, sofern vorhanden, zusätzlich die Kontaktdaten der bevollmächtigten Person vermerkt.

Der Datensatz Persönliche Erklärungen enthält also keine medizinischen Daten. Ebenso wie der Notfalldatensatz soll er dem Heilberufler Informationen zur Verfügung stellen, wenn der Versicherte selbst nicht mehr ansprechbar ist, wie beispielsweise durch ein Koma. In solchen Situationen werden die genannten Willenserklärungen relevant.

Schutz vor unberechtigtem Zugriff

Entscheidet sich ein Versicherter dafür, einen Notfalldatensatz oder einen Datensatz Persönliche Erklärungen anlegen zu lassen, ist es sein Wunsch, dass diese Daten einem Heilberufler auch dann zugänglich sind, wenn er selbst nicht interaktionsfähig ist. Dies schließt einen generellen Zugriffsschutz mittels PIN aus. Trotzdem muss gewährleistet sein, dass nur Berechtigte auf die Daten zugreifen können und nicht jeder, der die Gesundheitskarte gerade in den Händen hält.

Daher ist der Zugriff auf diese beiden Datensätze nur mithilfe einer Card-to-Card-Authentisierung mit Heilberufsausweis oder Praxisausweis möglich. Der Zugriff ist teilweise noch weiter eingeschränkt, und zwar

- je nach Art des zugreifenden Heilberuflers,
- je nach Art des Zugriffs (lesend oder schreibend) und
- je nach der Situation, in der zugegriffen wird.

Zudem muss der Versicherte gegebenenfalls auch seine PIN eingeben. In Notfallsituationen – das sind Versorgungen durch einen Rettungsdienst, in der Notaufnahme eines Krankenhauses sowie ärztliche Behandlungen von Patienten mit Akutbeschwerden im ambulanten Sektor – dürfen (Zahn-)Ärzte und deren Personal sowie Rettungssanitäter mit ihrem Heilberufsausweis oder Praxisausweis, aber stets ohne PIN-Eingabe des Versicherten auf den Notfalldatensatz zugreifen. Über das Protokoll auf ihrer elektronischen Gesundheitskarte können Versicherte im Nachhinein einen solchen Zugriff auf den Notfalldatensatz nachvollziehen.

Eine ausführliche Beschreibung der Regeln, wer für den lesenden und schreibenden Zugriff auf den

Notfalldatensatz und den Datensatz Persönliche Erklärungen berechtigt ist, findet sich in [4].

Notfalldaten sind qualifiziert signiert

Der Notfalldatensatz soll einen Heilberufler bei der Behandlung eines Patienten im Notfall unterstützen. Der Heilberufler muss sich also darauf verlassen können, dass ein (Zahn-)Arzt die Daten nach bestem Wissen und Gewissen erstellt hat. Dies bestätigt der erstellende (Zahn-)Arzt, indem er den Notfalldatensatz mit seinem Heilberufsausweis qualifiziert elektronisch signiert – dem elektronischen Äquivalent zur handschriftlichen Unterschrift. Beim Lesen des Notfalldatensatzes wird immer zunächst die Signatur geprüft. Das Ergebnis der Signaturprüfung wird dem Heilberufler zusammen mit dem Notfalldatensatz angezeigt. Wenn die Signaturprüfung nicht oder nicht vollständig erfolgreich war, wird eine Warnung angezeigt. Ein Heilberufler entscheidet – unabhängig vom Ergebnis der Signaturprüfung – stets selbst, ob er die Informationen aus dem Notfalldatensatz berücksichtigt oder nicht.

5.7 Nutzung weiterer Anwendungen über die Telematikinfrastruktur

Die Telematikinfrastruktur kann auch von weiteren Anwendungen im Gesundheitswesen oder von der Gesundheitsforschung genutzt werden. Der Gesetzgeber verfolgt damit das Ziel, die Telematikinfrastruktur perspektivisch als die maßgebliche Infrastruktur für das deutsche Gesundheitswesen zu etablieren.

Die Architektur der Telematikinfrastruktur sieht verschiedene Anbindungsarten für weitere Anwendungen vor. Die jeweils gewählte Anbindungsart lässt unterschiedliche Integrationsgrade in die Telematikinfrastruktur zu, was Auswirkungen auf mögliche Beeinträchtigungen der Telematikinfrastruktur hat. Je stärker eine Anwendung in die Telematikinfrastruktur integriert ist, desto eher können die Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur beeinträchtigt werden und desto umfassendere Überwachungsmaßnahmen sind zu treffen.

Die Anbieter weiterer Anwendungen müssen zunächst nachweisen, dass sie die Vorschriften zum Datenschutz sowie die Anforderungen an die Sicherheit der Anwendungen im Hinblick auf die Schutzbedürftigkeit der Daten einhalten. Erst dann können sie die Telematikinfrastruktur nutzen. Auch danach sind sie verpflichtet, gegenüber der gematik regelmäßig zu belegen, dass sie diesen Datenschutz- und Sicherheitsanforderungen kontinuierlich entsprechen.

Bei weiteren Anwendungen, die in die Telematikinfrastruktur integriert sind, hat der Anbieter ein Sicherheitsgutachten einzureichen, das von einem dafür qualifizierten unabhängigen Sicherheitsgutachter erstellt wurde. Zudem muss der Anbieter am koordinierenden Datenschutzmanagementsystem/Managementsystem für Informationssicherheit der Telematikinfrastruktur teilnehmen. Dazu gehört insbesondere, schwerwiegende Datenschutzverstöße und Sicherheitsvorfälle zu melden sowie regelmäßig über den Datenschutz und die Informationssicherheit zu informieren. Die gematik kann darüber hinaus Audits beim Anbieter durchführen (lassen).

Die Dienste der Telematikinfrastruktur sind zunehmend über das Internet zu erreichen. Anwendungen, die nicht in die Telematikinfrastruktur integriert werden sollen, können diese Dienste (Plattformanwendungen der Telematikinfrastruktur, PAT) nutzen. So können diese Anwendungen z. B. mit der GesundheitsID arbeiten und den Verzeichnisdienst der Telematikinfrastruktur über das Internet nutzen.

6 Fazit

Die Telematikinfrastruktur ist die Plattform für Gesundheitsanwendungen in Deutschland. Millionen Versicherte profitieren durch die digitalen Anwendungen der Telematikinfrastruktur von einer verbesserten medizinischen Versorgung. Damit dieses Potenzial der Telematikinfrastruktur ausgeschöpft werden kann, muss der Datenschutz nachhaltig gestärkt werden und die Informationssicherheit gewährleistet sein. Das sind für die Telematikinfrastruktur unerlässliche Rahmenbedingungen. Nur damit kann die sichere Vernetzung des Gesundheitswesens gelingen.

Die gematik trägt die Gesamtverantwortung für die Telematikinfrastruktur, die zentrale Plattform für digitale Anwendungen im deutschen Gesundheitswesen. Mit der Definition und Durchsetzung verbindlicher Standards für Dienste, Komponenten und Anwendungen in der Telematikinfrastruktur gewährleistet die gematik, dass diese zentrale Infrastruktur datenschutzkonform, sicher, leistungsfähig und nutzerfreundlich ist und bleibt.

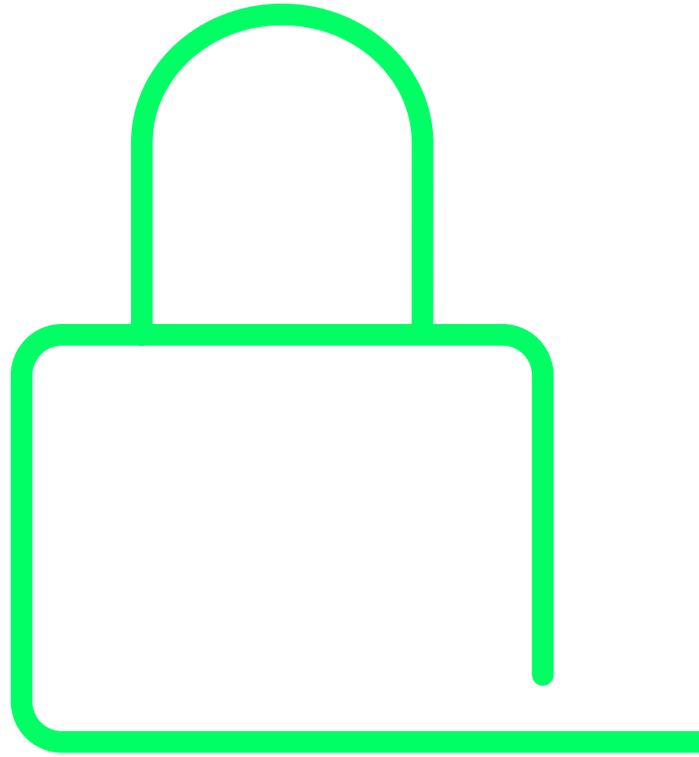
Quellen

[1] https://de.statista.com (abgerufen am 18.03.2025)

[2] GKV-Spitzenverband: Krankenkassenliste.
URL: https://www.gkv-spitzenverband.de/service/krankenkassenliste/krankenkassen.jsp
(abgerufen am 14.11.2024)

[3] gematik: gemSpecPages – Online-Reader.
URL: https://gemspec.gematik.de/ (abgerufen am 14.11.2024)

[4] Zimmer, Lars: Notfalldaten-Management mit der elektronischen Gesundheitskarte.
In: Datenschutz und Datensicherheit – DuD, June 2014, Volume 38, Issue 6, pp. 394–398



Impressum

Herausgeber:
gematik GmbH
Friedrichstraße 136
10117 Berlin

info@gematik.de
www.gematik.de

Gestaltung:
neues handeln AG

Druck:
Königsdruck Printmedien und digitale Dienste GmbH
Alt-Reinickendorf 28
13407 Berlin

Bildnachweis:
© Westend61 via Getty Images, Titel
© Tom Werner via Getty Images, Seite 14, U2
© Thomas Barwick via Getty Images, Seite 29
© gematik/Daniel Chassein, Seite 32
© Oliver Rossi via Getty Images, Seite 37
© Gorodenkoff via shutterstock, Seite 40
© NordWood via Unsplash, Seite 42
© Oliver Rossi via Getty Images, Seite 45

Stand:
Juli 2025