Elektronische Gesundheitskarte und Telematikinfrastruktur

Anschluss von Krankenhäusern an die TI – Eine Übersicht über die Telematikinfrastruktur im stationären Sektor

Version:	1.4.2
Stand:	22.06.2023
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemInfo_Anschluss_KH_TI

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Das Dokument sowie weitere Informationen zur TI-Anbindung von Krankenhäusern finden Sie unter: https://fachportal.gematik.de/informationen-fuer/krankenhaeuser

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	23.04.21		freigegeben	gematik
1.1.0	04.05.2021	2.4.1, 2.4.6	redaktionelle Änderungen Ergänzung der SMC-B (Kapitel 2.4.1, Lesen von VSDM) Hinweis KIM für elektronische Arbeitsunfähigkeitsbescheinigung (Kapitel 2.4.6)	gematik
1.2.0	05.05.2021	2.4.2	Notfalldatensatz aktualisieren	gematik
1.3.0	18.05.2021	2.4.2 2.4.4	Richtigstellung der QES eines Notfalldatensatzes Ergänzungen des Beispielszenarios zur Durchführung einer Komfortsignatur	gematik
1.3.1	06.05.2022	3.2.2.1	Anpassung des Geltungsbereichs für SMC-B-Karten vom Typ ‚Krankenhaus'	gematik
1.4	12.04.2023	4.2.6, 4.2.7	Prüf- und Schulungskonzept basierend auf der Prüf-eGK 2.1	gematik
1.4.1	26.04.2023	3.4.3	Entscheidungshilfe zur Anschaffung eines Konnektors.	gematik
1.4.2	22.06.2023	3.2.2.1	Austausch SMC-B wegen abgelaufenem Zertifikat	gematik

Inhaltsverzeichnis

1 Einleitung

Mit der flächendeckenden Einführung der elektronischen Gesundheitskarte (**eGK**) für gesetzlich Krankenversicherte und dem Aufbau der Telematikinfrastruktur (**TI**) als das sichere zentrale Netz des deutschen Gesundheitswesens ergibt sich für Krankenhäuser die Notwendigkeit, sich nicht nur technisch an die TI anzubinden, sondern auch die internen medizinischen Versorgungsprozesse mit den Anwendungen der TI zu verknüpfen.

Seit dem 01.01. 2021 sind Kliniken zudem gesetzlich verpflichtet, mit den für den Zugriff auf die TI-Anwendung „elektronische Patientenakte" (**ePA**) erforderlichen Komponenten und Diensten ausgestattet zu sein (siehe § 341 Absatz 7 SGB V). Daneben müssen Krankenhäuser die bereits in der TI betriebenen Anwendungen „Versichertenstammdaten-Management" (**VSDM**), „Notfalldaten-Management" (**NFDM**) und „elektronischer Medikationsplan" (**eMP**) bedienen können. Des Weiteren ist der stationäre Sektor angehalten, die Anwendung „Kommunikation im Medizinwesen" (**KIM** - vormals bekannt als KOM-LE) zu nutzen (siehe § 295 SGB V, Stichwort „Arbeitsunfähigkeitsdaten").

Am **01. 07. 2021** wird die neue TI-Anwendung „elektronisches Rezept (**E-Rezept**)" als Teil der elektronischen Verordnungen eingeführt (vgl. §§ 312 und 334 Absatz 1 Satz 2 Nummer 6 SGB V). **Ab** dem **01.01.2022** werden Ärzte[1] und Zahnärzte, die in zugelassenen Krankenhäusern tätig sind, verpflichtet, Verordnungen von verschreibungspflichtigen Arzneimitteln elektronisch auszustellen und für die Übermittlung der Verordnungen die Dienste und Komponenten der TI zu nutzen (vgl. § 360 Absatz 2 SGB V und Änderungen des § 360 Absatz 2 SGB V gemäß Gesetzentwurf zum DVPMG – Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz). Für Krankenhäuser ist diese Anwendung insofern relevant, als dass Entlassrezepte und Rezepte für die ambulante Behandlung eines Patienten mit Zytostatika oder parenteralen Zubereitungen als E-Rezept ausgestellt werden.[2]

Neben den Anwendungen stellt das vorliegende Dokument auch die qualifizierte elektronische Signatur (**QES**) sowie die Komfortsignatur kurz vor. Diese Funktionen sind insbesondere bei der Arbeit mit dem E-Rezept oder dem Notfalldatensatz relevant.

Bereits anhand dieser kurzen Darstellung zeigt sich also: Bereits die Anbindung der TI-Anwendungen in Krankenhäusern geht mit zahlreichen Änderungen einher, die die medizinischen Versorgungsprozesse auf technischer und prozessualer Ebene beeinflussen.

1.1 Zielsetzung

Mit der Anbindung an die TI und der Nutzung der gesetzlichen und freiwilligen TI-Anwendungen ergeben sich für Krankenhäuser als Leistungserbringer Veränderungen in ihren informationstechnischen Systemen bzw. informationstechnischen Umgebungen.

Dieses Dokument gibt deshalb einen Überblick über alle relevanten Aspekte der TI-Anbindung von Krankenhäusern. Dabei richtet sich das Dokument an IT-Entscheider und insbesondere an das IT-Fachpersonal eines Krankenhauses (z. B. Administratoren),

[1] Zugunsten des Leseflusses wird in dieser Publikation meist die männliche Form verwendet. Wir bitten, dies nicht als Zeichen einer geschlechtsspezifischen Wertung zu deuten.

[2] Diese Regelung gilt vorbehaltlich der Einschränkung, dass die Ausstellung von Verordnungen von verschreibungspflichtigen Arzneimitteln in elektronischer Form technisch möglich ist und dazu die erforderlichen Dienste und Komponenten zur Verfügung stehen.

die mit dem Anschluss an die Telematikinfrastruktur bzw. dem damit zusammenhängenden IT-Support befasst sind.

Dabei wird möglichst praxisnah vermittelt:

- vor welchen besonderen Anforderungen Krankenhäuser verschiedener Größe und Struktur beim Anschluss stehen

und

- wie diese Anforderungen erfolgreich umgesetzt werden können.

Nach einer kurzen **Einführung zur Telematikinfrastruktur** und der **gematik** in **Kapitel 2** geht das Dokument auf folgende **Fachanwendungen bzw. Dienste der TI** (ab **Kapitel 2.4**) ein:

- Versichertenstammdaten-Management (**VSDM**),
- Notfalldaten-Management (**NFDM**) inklusive persönlicher Erklärungen bzw. Hinweise auf Erklärungen des Versicherten (**DPE** – Datensatz Persönliche Erklärungen),
- elektronischer Medikationsplan/Arztmitteltherapiesicherheit (**eMP/AMTS**),
- qualifizierte elektronische Signatur (**QES**) und Komfortsignatur,
- elektronische Patientenakte (**ePA**),
- Kommunikation im Medizinwesen (**KIM** – vormals KOM-LE) und
- elektronisches Rezept (**E-Rezept**).

All diese Fachanwendungen richten sich zunächst – neben den Leistungserbringern – an die Versicherten der gesetzlichen Krankenversicherungen, welche im Fokus der derzeitigen gesetzlichen Regelungen zur TI stehen. Im Dokument werden daher die Anwendungen der TI ausschließlich mit Bezug zu den gesetzlich Versicherten beschrieben.

Wenn im Folgenden von Leistungserbringern die Rede ist, ist damit nicht nur die Gruppe der Ärzte, ihrer berufsmäßigen Gehilfen und der medizinischen Angestellten eines Krankenhauses, sondern die Zielgruppe Krankenhaus als Erbringer medizinischer Leistungen im Allgemeinen adressiert.

Für das Verständnis des vorliegenden Dokumentes ist es allerdings wichtig, zwischen Leistungserbringern auf der einen Seite und dem IT-Fachpersonal eines Krankenhauses bzw. einem von dem Leistungserbringer Krankenhaus beauftragten IT-Dienstleiter zu unterscheiden.

Im engeren Sinne wird ein interner oder externer IT-Dienstleister von einem Leistungserbringer (bspw. Arzt) oder dem Krankenhaus als Leistungserbringerinstitution beauftragt, die informationstechnischen Voraussetzungen für die Anbindung eines Krankenhauses und seiner Abteilungen und Bereiche an die TI zu planen, die Anbindung an die TI vorzunehmen und zu unterhalten. Leistungserbringer sind dabei immer diejenigen, die letztlich die TI-Anwendungen nutzen.

Zur Vereinfachung werden im Folgenden die Begriffe „**Leistungserbringer**“ und „**Krankenhaus**“ gleichbedeutend verwendet, während das **IT-Fachpersonal** dagegen immer davon getrennt angesprochen wird.

Im Dokument werden zudem die Begriffe „Primärsystem“ (**PS**), „Praxisverwaltungssystem“ (**PVS**) sowie „Krankenhausinformationssystem“ (**KIS**)

gleichbedeutend verwendet, selbst wenn hier unterschiedliche Leistungserbringer bzw. Leistungserbringerinstitutionen adressiert sind. Im fachlichen Zusammenhang spielt diese Unterscheidung allerdings keine Rolle.

Was wird (noch) nicht behandelt?

Änderungen, die sich durch den Gesetzentwurf zur digitalen Modernisierung von Versorgung und Pflege (Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz DVPMG, siehe Drucksache des Bundesrates 52/21 vom 22. 01. 2021) ergeben, werden im Rahmen dieses Dokumentes nur insofern berücksichtigt, als dass belastbare Informationen vorliegen und bei der gematik bereits diesbezügliche Planungen zur Umsetzung erfolgen. Auf Änderungen des DVPMG wird jeweils explizit im Text hingewiesen.

Nicht behandelt werden kann z. B. die mit diesem Gesetzesentwurf eingebrachte **elektronische Patientenkurzakte**, welche ab dem 01. 01. 2023 von den gesetzlichen Krankenversicherungen[3] zur Verfügung gestellt werden soll und schrittweise die eGK-basierten Anwendungen NFDM und eMP/AMTS ablösen wird.

Zusätzlich sollen ab Januar 2023 die bislang ebenfalls auf der elektronischen Gesundheitskarte gespeicherten Hinweise des Versicherten auf ggf. vorhandene Vorsorgevollmachten, Patientenverfügungen oder eine papierbasierte Erklärung zur Organspende sowie deren jeweilige Aufbewahrungsorte in die elektronische Patientenkurzakte überführt werden. Zur Patientenkurzakte liegen derzeit noch keine für die Krankenhäuser relevanten TI-umsetzungsrelevanten Informationen vor.

Weiterhin können aufgrund der derzeit noch nicht gefestigten Datenlage weder das in Umsetzung befindliche **zentrale Organ- und Gewebespendenregister** (gemäß Gesetz zur Stärkung der Entscheidungsbereitschaft bei der Organspende, siehe Bundesgesetzblatt 2020, Nr. 13 vom 19.03.2020) noch das ebenfalls neu zu schaffende **zentrale Implantateregister** (siehe Implantateregister-Errichtungsgesetz – EIRD) behandelt werden.

Exkurs FHIR® und ISiK

Der Gesetzgeber hat die gematik gemäß § 373 SGB V damit beauftragt, im Benehmen mit der Deutschen Krankenhausgesellschaft (DKG) und den maßgeblichen Bundesverbänden der Industrie im Gesundheitswesen verbindliche Standards für den Austausch von Gesundheitsdaten über **I**nformationstechnische **S**ysteme **i**n **K**rankenhäusern zu erarbeiten (kurz: **ISiK**). Die verbindlichen Vorgaben der gematik zu ISiK basieren auf dem Standard „Fast Healthcare Interoperability Resources" (**FHIR**®), welcher von „Health Level Seven International" (HL7) ins Leben gerufen wurde.[4]

FHIR® hat sich seit 2014 als Standard zum Datenaustausch zwischen unterschiedlichen Softwaresystemen im Gesundheitswesen etabliert. Bei FHIR® steht nicht ein bestimmtes Dokument im Vordergrund, sondern dessen Inhalte, welche als **Ressourcen** bezeichnet und über eine Schnittstelle zum Austausch mit anderen Systemen angeboten werden. Mit FHIR® werden unter Federführung unterschiedlicher Organisationen des Gesundheitswesens sogenannte Profile entwickelt, die von HL7 Deutschland, dem deutschen HL7-Ableger, veröffentlicht werden. Deutschsprachige Informationen werden dabei vom „Technischen Komitee (TC – Technical Committee) zur Verfügung gestellt.

Die gematik hat einen FHIR®-Implementierungsleitfaden veröffentlicht, der die für den vorgenannten gesetzlichen Auftrag entwickelten FHIR®-Profile sowie das Application

[3] Im Gegensatz zu den Krankenkassen steht es den privaten Krankenversicherungen frei, eine elektronische Patientenakte anzubieten. Details regelt § 362 SGB V.

[4] Weiterführende Informationen zu HL7 finden Sie unter hl7.de.

Programming Interface (API) beschreibt.[5] Diese API basiert auf dem Paradigma „Representational State Transfer" (**REST**) für Softwarearchitekturen verteilter Systeme. Die REST-API wird in diesem Zusammenhang im Wesentlichen vom FHIR®-Standard vorgegeben. Der Leitfaden konkretisiert die ISiK-relevanten Funktionen der Standard-REST-API und trifft inhaltliche Festlegungen zu den ISiK-relevanten Ressourcen in Form von Ressourcen-Profilen. Hersteller bestätigungsrelevanter Systeme sollen durch diesen Leitfaden in die Lage versetzt werden, eine konforme Implementierung zu erstellen und das gleichnamige **Bestätigungsverfahren ISiK** der gematik erfolgreich zu absolvieren.

Der Leitfaden ist zum Zeitpunkt des Redaktionsschlusses des vorliegenden Dokumentes noch nicht abgeschlossen. Dessen ungeachtet finden Sie alle tagesaktuellen Informationen zu diesem Thema im Fachportal der gematik.

Erläuterungen zum Aufbau des Dokuments

Voraussetzung, um vorgenannten TI-Fachanwendungen im Krankenhaus nutzen zu können, sind die zu installierenden **dezentralen TI-Komponenten**. Sie werden in **Kapitel 3** kurz vorgestellt. Für diese Komponenten gelten hohe Sicherheitsanforderungen hinsichtlich ihrer Installation und ihres Betriebes.

Eine dieser dezentralen Komponenten, der **Konnektor**, enthält zudem ein konfigurierbares **Informationsmodell**, mit dem sich die Organisationsstruktur eines Krankenhauses abbilden lässt.

Zur Authentisierung und Nutzung der TI-Anwendungen sind krankenhausseitig die Smartcards Institutionskarte (Security Module Card Typ B – **SMC-B**) und der Heilberufsausweis (**HBA**) erforderlich. Diese werden zusammen mit der elektronischen Gesundheitskarte (**eGK**) ebenfalls in Kapitel 3 besprochen. Hier erfahren Sie auch, wie die SMC-B in verschiedenen Krankenhausszenarien eingesetzt werden kann.

In **Kapitel 4** werden die wesentlichen **Administrationsaufgaben** für die Installation, Implementierung, Inbetriebnahme, Betrieb und Wartung der dezentralen TI-Komponenten aufgeführt und erläutert.

Anschließend geht **Kapitel 5** darauf ein, in welchen Szenarien die TI-Anwendungen in einem Krankenhaus zum Einsatz kommen können.

Für das Verständnis dieses Dokumentes ist es nicht unbedingt erforderlich, das Dokument strikt bei Kapitel 1 beginnend zu lesen.

Gleichwohl bieten insbesondere die ersten beiden Kapitel einen Überblick über die wesentlichen Bestandteile der TI und ihre Einordnung in die Gesamtgemengelage. Ergänzend finden sich am Ende eines jeden Kapitels Hinweise auf weiterführende Informationen. Ein bereits TI-erfahrener Leser kann jedoch problemlos gezielt gewünschte Textstellen ansteuern

Zusätzlich zu den Informationen im vorliegenden Dokument finden Sie https://fachportal.gematik.de/informationen-fuer/krankenhaeuser eine Zusammenstellung ausgewählter, typischer Fragestellungen, die von Vertretern der Krankenhäuser, Krankenhausträgern oder Krankenhausgesellschaften an die gematik gestellt bzw. in gemeinsamen Workshops diskutiert wurden.

Beachten Sie, dass dieses Dokument **nicht** die Lektüre von (Administrator-) **Handbüchern ersetzt**, die z. B. im Lieferumfang von Konnektoren enthalten sind. So erfordert bspw. jede Version eines Konnektors eine eigene Konfiguration mit jeweils

[5] Der Leitfaden „ISiK-Basismodul" steht Ihnen im Fachportal zur Verfügung. Bitte beachten Sie auch die weiteren Hinweise hierzu im Fachportal.

spezifischen Einstellungen. In diesem Dokument werden lediglich die übergreifenden und architektonischen Planungs- und Konfigurationsmaßnahmen beschrieben, unabhängig von Herstellern oder Produktausprägungen.

Weitere Informationsangebote

Nutzen Sie zur weiteren Informationsbeschaffung auch das umfangreiche Informationsangebot auf den Internetseiten der gematik (gematik.de), hier insbesondere das Fachportal (fachportal.gematik.de). Auf dem Fachportal finden Sie neben Informationen zur TI, den TI-Anwendungen und Komponenten auch alle normativen Dokumente wie Spezifikationen und Konzepte. Darüber hinaus bietet Ihnen das Fachportal u. a. themenspezifische Verlinkungen zu GitHub und Simplifier.

Im Fachportal steht Ihnen außerdem das vollständige Glossar der gematik (fachportal.gematik.de/glossar) zur Verfügung.

Interessant kann für Sie auch das Informationsnagebot auf den gematik-Internetseiten für Dienstleister vor Ort (DVO) sein, die Arztpraxen und Apotheken anschließen (fachportal.gematik.de/dvo).

Auf der Seite für Primärsystemhersteller finden Sie zahlreiche Implementierungsleitfäden zu einzelnen TI-Anwendungen (fachportal.gematik.de/hersteller-anbieter), auf die in diesem Dokument immer wieder referenziert wird.

Ebenfalls im Fachportal finden Sie die Übersichten über die von der gematik zugelassenen Produkte, Komponenten, Dienste und Anbieter (fachportal.gematik.de/zulassungs-bestaetigungsuebersichten).

1.2 Zielgruppe

Das Dokument richtet sich, wie zuvor erwähnt, an IT-Entscheider und insbesondere an das IT-Fachpersonal (z. B. IT-Architekten und Administratoren) in Krankenhäusern. Also an alle, die mit der Anbindung an die Telematikinfrastruktur sowie die TI-Anwendungen beauftragt sind.

Zur adäquaten Unterstützung wird mit möglichst praxisnahen Aufgabenstellungen und Beispielen aufgezeigt:

- **welche dezentralen TI-Komponenten** notwendig sind, um die TI-Fachanwendungen im Krankenhaus nutzen zu können,
- wie diese Komponenten in einem Krankenhaus **installiert, implementiert, konfiguriert, betrieben** und **gewartet** werden können und
- wie die TI-Fachanwendungen **in einen krankenhaustypischen Prozess integriert** werden können.

1.3 Geltungsbereich

Das Dokument dient der praxisnahen Vorbereitung und Durchführung der Anbindung von Krankenhäusern an die TI. Es ist als Informationssammlung erstellt und dient daher als fachlich-informatorisches, nicht normatives Begleitdokument.

1.4 Informationsbasis

Informationsbasis dieses Dokuments sind im Wesentlichen Fragestellungen, die die gematik mit IT-Entscheidern, dem IT-Fachpersonal und weiteren Vertretern von Krankenhäusern, deren Trägern und Gesellschaften bspw. im Rahmen von Workshops erörtert hat.

Des Weiteren wurden Fragen aufgegriffen, die direkt an die gematik gerichtet wurden.

1.5 Methodik

Referenzierte Dokumente der gematik sind in eckigen Klammern dargestellt und im Fachportal der gematik einsehbar.

2 gematik und Telematikinfrastruktur – das müssen Sie wissen

2.1 Die gematik – mit gesetzlichem Auftrag zur Digitalisierung des Gesundheitswesens

Für die Telematikinfrastruktur spielt die gematik eine herausragende Bedeutung. Die heutige gematik GmbH (ehemals: Gesellschaft für Telematik Anwendungen der Gesundheitskarte, im Folgenden, kurz: gematik) wurde im Jahr 2005 mit Sitz in Berlin gegründet. Ihr Wirkungs- und Aufgabenfeld ist durch das Sozialgesetzbuch Fünftes Buch (SGB V) definiert. Demnach ist die gematik mit der Schaffung, dem Aufbau und dem Betrieb der Telematikinfrastruktur sowie mit der Zulassung von Komponenten und Diensten sowie dem sicheren Zugang zur TI betraut (vgl. §§ 306, 310 ff. SGB V).

Hauptgesellschafter und Mehrheitseigner der gematik ist die Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit (BMG). Zu den weiteren Gesellschaftern zählen die Spitzenorganisationen des deutschen Gesundheitswesens (siehe § 306 SGB V, Absatz 1 Satz 1), wobei das BMG die Rechtsaufsicht über die gematik führt.

Eine wesentliche Aufgabe der gematik besteht darin, Spezifikationen für die Dienste und Komponenten der TI zu erstellen, die neben der Funktionalität insbesondere die Anforderungen zu Interoperabilität, Kompatibilität und Sicherheit umfassen. Des Weiteren ist die gematik damit beauftragt, diese Dienste, Komponenten sowie Anbieter per Verfahren zuzulassen oder zu bestätigen. Die bereits zugelassenen oder bestätigten Dienste, Komponenten und Anbieter sind auf den Internetseiten der gematik veröffentlicht. Die gematik ist zudem für den sicheren Betrieb der TI verantwortlich.

Weiterführende Informationen zum gesetzlichen Auftrag der gematik, ihren Aufgabenbereichen und Leistungen finden Sie auf www.gematik.de. Sämtliche gesetzlichen Grundlagen sind vornehmlich im SGB V, dort insbesondere ab § 306 ff., verankert.

2.2 Die Telematikinfrastruktur – Das sichere Netz des deutschen Gesundheitswesens

Die Anforderungen an die Telematikinfrastruktur (TI) sind im Sozialgesetzbuch Fünftes Buch (SGB V) verankert. Gemäß § 306 Absatz 1 SGB V ist sie „die interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur, die der Vernetzung von Leistungserbringern, Kostenträgern, Versicherten und weiteren Akteuren des Gesundheitswesens dient." Sie ist erforderlich, um die elektronische Gesundheitskarte (eGK) und die Anwendungen der TI zu nutzen.

Die TI umfasst eine dezentrale und eine zentrale Infrastruktur sowie eine Anwendungsinfrastruktur. Die **dezentrale Infrastruktur** besteht aus Komponenten zur Authentifizierung und zur sicheren Übermittlung von Daten in die zentrale Infrastruktur. Dezentrale TI-Komponenten kommen auch im Krankenhausumfeld zum Einsatz kommen (z. B. eHealth-Kartenterminal oder Konnektor). Die **zentrale Infrastruktur** besteht aus sicheren Zugangsdiensten als Schnittstelle zur dezentralen Infrastruktur und einem gesicherten Netz einschließlich der für ihren Betrieb notwendigen Dienste.

Die **Anwendungsinfrastruktur** wiederum besteht aus Diensten und nutzerbezogenen Funktionalitäten zur Verarbeitung von Gesundheitsdaten in der TI. Dabei wird unterschieden nach Anwendungen, die nur durch Einsatz der eGK genutzt werden können und solchen, die ohne eGK auskommen.

TI-Anwendungen, die ausschließlich per eGK genutzt werden können, sind gemäß § 334 Abs. 2 SGB V:

- die elektronische Patientenakte (ePA),
- der Medikationsplan nach § 31a SGB V einschließlich Daten zur Prüfung der Arzneimitteltherapiesicherheit (elektronischer Medikationsplan – eMP),
- medizinische Daten, soweit sie für die Notfallversorgung erforderlich sind (elektronische Notfalldaten – NFD) und
- Hinweise der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen zur Organ- und Gewebespende sowie Hinweise der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Vorsorgevollmachten oder Patientenverfügungen nach § 1901a des Bürgerlichen Gesetzbuchs (DPE – Datensatz Persönliche Erklärungen).

Der Zugriff von Versicherten auf die TI-Anwendung E-Rezept hingegen ist auch ohne eGK möglich. Zur Authentifizierung und Autorisierung von Versicherten per eGK hat die gematik einen Identity-Provider (IdP) in der TI eingerichtet.

Im Gegensatz zu den zuvor genannten Anwendungen ist der Übermittlungsdienst KIM – Kommunikation im Medizinwesen keine gesetzlich explizit definierte TI-Anwendung. KIM resultiert vornehmlich aus § 311 Absatz 6 SGB V, wobei die in § 67 SGB V definierten Ziele aufgegriffen werden. Diese Anwendung soll u. a. den „Daten- und Kommunikationsfluss unter den Leistungserbringern [sowie] zwischen den Krankenkassen und Leistungserbringern" und die „Qualität und Wirtschaftlichkeit der Versorgung" verbessern.

Wie Sie der nachfolgenden Abbildung[6] entnehmen können, bietet die TI neben den bisher aufgeführten Anwendungen weitere Dienste, darunter:

- einen sichereren Zugang zur TI für Leistungserbringer (mittels zugelassenem VPN-Zugangsdienst),
- die Signierung von Arztbriefen mittels qualifizierter elektronischer Signatur

  und
- die Möglichkeit, weitere Anwendungen aus bereits bestehenden Netzen des Gesundheitswesens sicher an die TI und damit an Krankenhäuser anzubinden.

All diese Dienste dienen dazu, mithilfe der TI zukünftig alle für eine medizinische Behandlung relevanten Informationen sicher, schnell und zuverlässig innerhalb eines Sektors ebenso wie zwischen Sektoren des Gesundheitswesens austauschen zu können – und zwar genau dann, wenn sie gebraucht werden. Auf diese Weise trägt die TI zu einer nachhaltigen Verbesserung der medizinischen Versorgung bei. Gleichzeitig leistet die TI damit im Rahmen von Versorgungsituationen einen wesentlichen Beitrag zur Förderung der Transparenz, der Qualität und der Wirtschaftlichkeit.

[6] Diese Übersicht über die TI finden Sie auch unter gematik.de/telematikinfrastruktur.

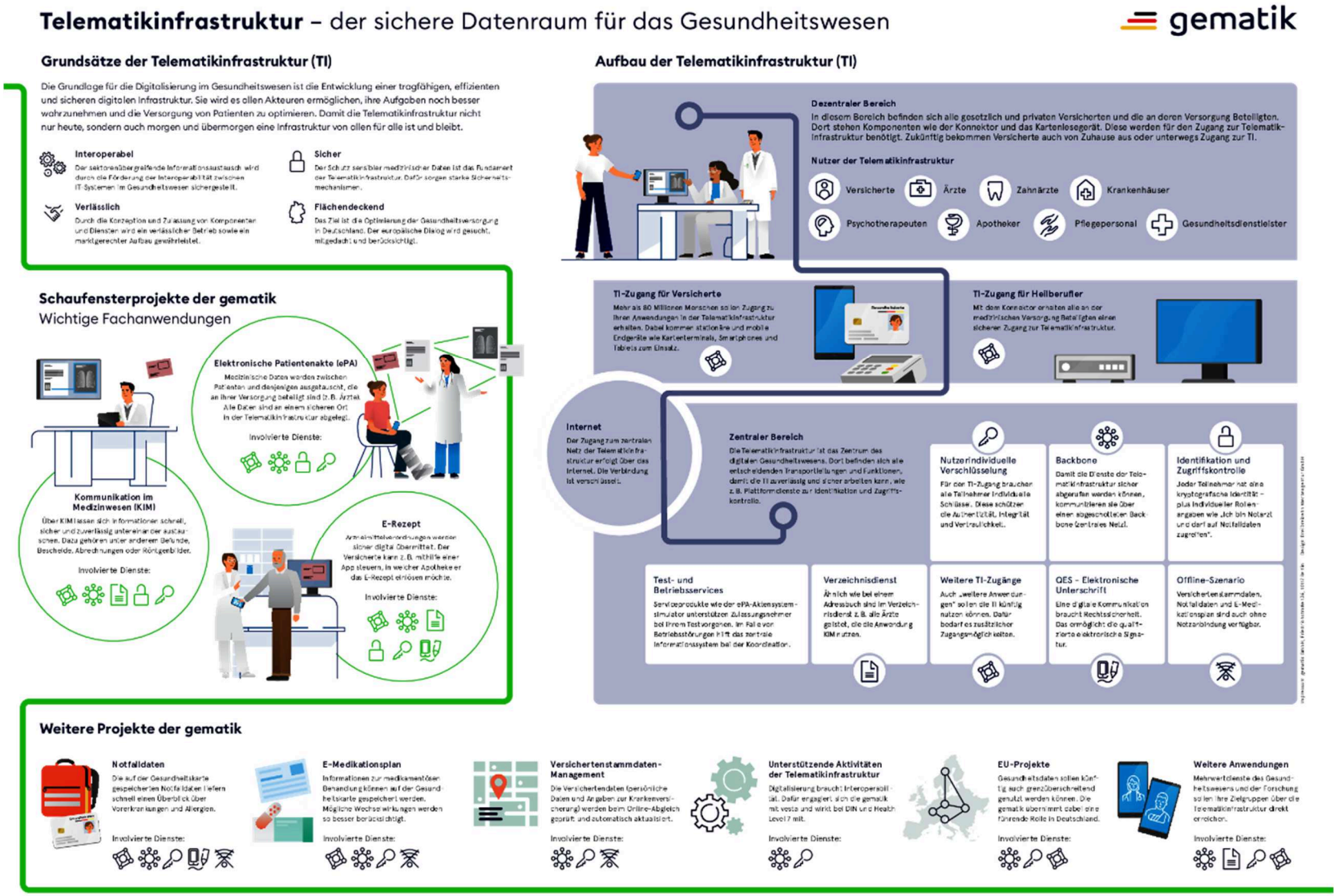

Abbildung 1: Übersicht Telematikinfrastruktur

2.3 Architektur der Telematikinfrastruktur

Die Telematikinfrastruktur ist derzeit als geschlossenes Netz konzipiert, wobei der Zugang zu diesem Netz strikt geregelt ist und ausschließlich über von der gematik spezifizierte und zugelassene Komponenten erfolgt. Um den Aufbau der Telematikinfrastruktur besser verstehen zu können, sind zur Veranschaulichung mehrere logische Sichtweisen dargestellt.

Schichtenmodell

Die TI besteht logisch aus mehreren Schichten (siehe folgende Abbildung), wobei die Systeme der TI-Plattform (TIP) von der Anwendungsschicht technologisch, semantisch und syntaktisch entkoppelt sind.

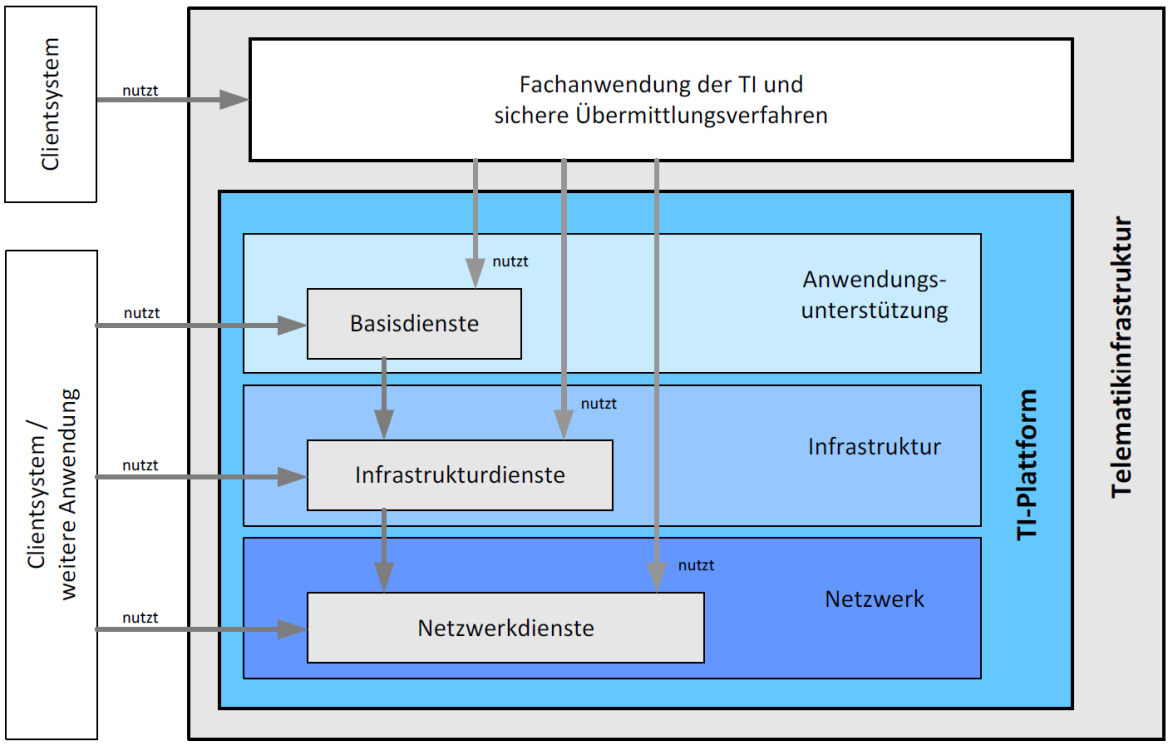

Abbildung 2: Logische Architekturschichten der TI (Quelle: gematik)

Die **Fachanwendungen der TI**[7] (siehe auch Kapitel 2.4) stellen die eigentlichen Anwendungen für die Leistungserbringer in einem Krankenhaus; wahlweise einer Arztpraxis oder einer Apotheke dar (zukünftig gilt dies auch für bspw. Hebammen, Pflegeeinrichtungen, Lieferanten von Hilfs- und Heilmitteln).

Die Fachanwendungen nutzen ihrerseits **Basisdienste**, welche umfassende Leistungen auf der anwendungsunterstützenden Ebene anbieten, darunter die komplette Abwicklung einer Signaturvalidierung inklusive mathematischer Prüfungen und Zertifikatsprüfung.

Die **Infrastrukturdienste** bieten generische Funktionen auf Infrastrukturebene an (bspw. Namensauflösung – DNS, Dienste der Public Key Infrastructure, Zeitdienst – NTP) und sind systemnäher als Basisdienste. Sie werden häufig direkt von Basisdiensten zur Erbringung ihrer Leistungen benötigt.

[7] Die Anwendung KIM wird in den normativen Dokumenten der gematik, u.a. zur Architektur der TI, auch als sicheres Übermittlungsverfahren bezeichnet.

Die **Netzwerkdienste** schließlich bilden die Transportschnittstelle der dezentralen Komponenten zu dem geschlossenen zentralen Netz der TI-Plattform und ermöglichen den Transport von Daten zwischen den zentralen Diensten der TI-Plattform, den fachanwendungsspezifischen Diensten und den dezentralen Komponenten der TI-Plattform. Die Netzwerkdienste können von Infrastrukturdiensten, Basisdiensten und Fachdiensten direkt genutzt werden.

Zonenmodell

Die nachfolgende Abbildung aus dem Architekturkonzept der TI gibt einen Überblick über den logischen Aufbau der TI (siehe auch [gemKPT_Arch_TIP#2.1.3]). Das Architekturkonzept benennt die Produkttypen der TI und legt die Schnittstellen dieser auf konzeptueller Ebene fest.

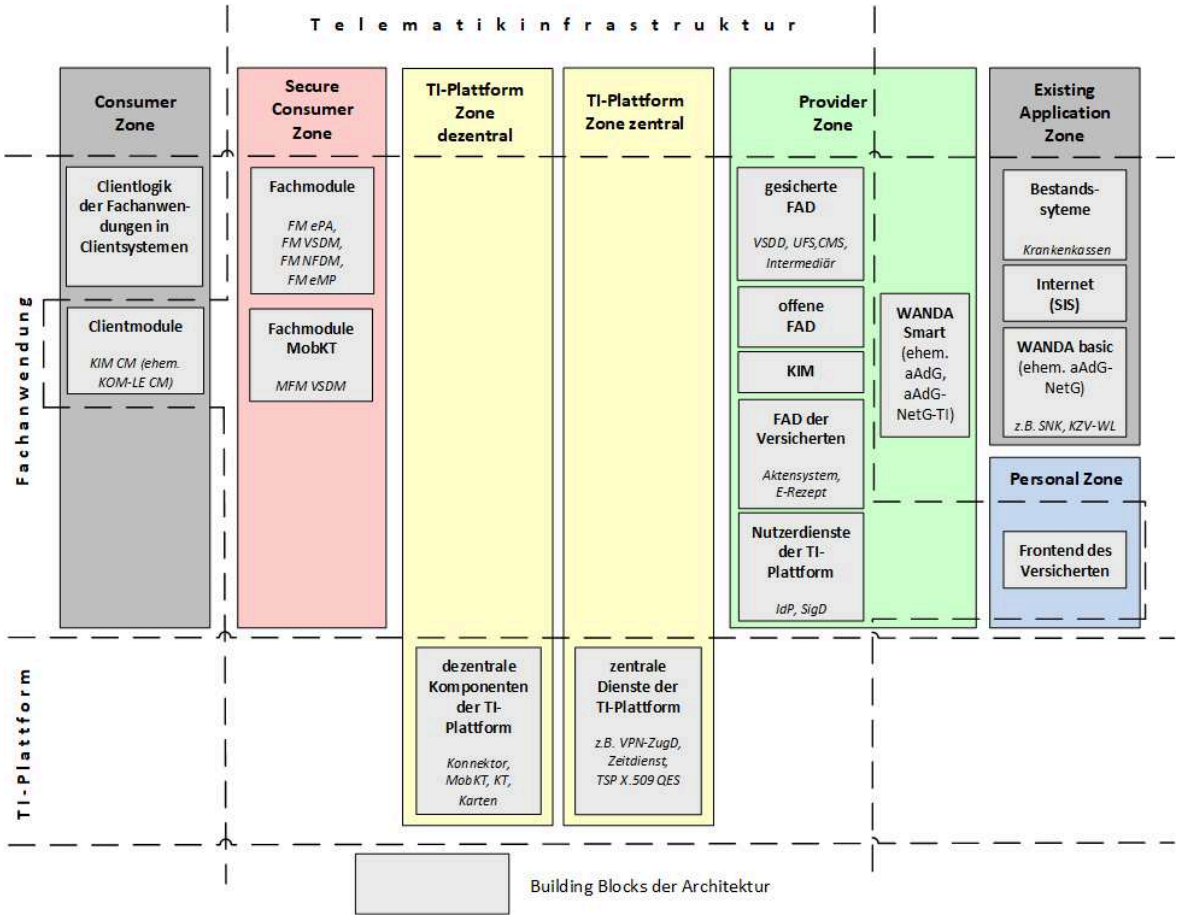

Abbildung 3: Logische Architekturschichten (Zonen) und Building Blocks der TI (Quelle: gematik)[8]

Die TI teilt sich derzeit logisch in mehrere Architekturschichten (Zonen) auf. Entlang der Architekturschichten vom Consumer zum Provider erfolgt eine Zuordnung von architektonischen Building Blocks. Die Architekturschichten sind ebenso wie die Building Blocks als logische Strukturen zu verstehen. Sie implizieren zunächst keine Trennung auf Hardwareebene.

[8] CM = Clientmodul, FM = Fachmodul, MobKT = Mobiles Kartenterminal, MFM VSDM = Fachmodul VSDM auf dem mobilem Kartenterminal, FAD = Fachanwendungsspezifischer Dienst, CMS = Card Management System, SigD = Signaturdienst, SNK = Sicheres Netz der KVen; KZV-WL = Abrechnungsportal der Kassenzahnärztlichen Vereinigung Westfalen-Lippe, SIS = Sicherer Internet Service, UFS = Update Flag Service

Die **Consumer Zone** (z. B. Krankenhaus) steht unter Kontrolle eines Nutzers der TI und enthält Komponenten des Benutzerinterfaces für fachliche Funktionalität oder separat verteil- und installierbare Komponenten der Fachanwendung (Clientmodule). Komponenten dieser Zone haben eingeschränkten Zugriff auf die Basisdienste der TI-Plattform. Die Consumer Zone steht nicht unter der Kontrolle des Versicherten. Wird dort die eGK eingesetzt, so wird die Verwendung der eGK über die TI abgesichert.

Ein **Clientsystem** ist z. B. ein Krankenhausinformationssystem (KIS), das auf dem Arbeitsplatzrechner eines berechtigten Akteurs (Arzt, medizinisches Fachpersonal) ausgeführt wird. Das Clientsystem stellt die Verbindung zu den Fachanwendungen der TI her und bietet das Interface zum Nutzer einer Anwendung oder eines Dienstes der TI. **Clientmodule** sind Komponenten der Fachanwendung (z. B. elektronische Verordnungen) und einem konkreten fachanwendungsspezifischen Dienst zugeordnet (z. B. Fachdienst E-Rezept). Clientmodule werden den Nutzern oder Betreibern der Consumer-Zone von einem Anbieter der betreffenden Fachanwendung zur Verfügung gestellt.

Im Gegensatz zu Komponenten der Consumer Zone werden Komponenten der **Secure Consumer Zone** (z. B. ein Fachmodul auf dem Konnektor) grundsätzlich Zugriff auf alle Basisdienste gewährt. Ein **Fachmodul** ist dabei ein dezentraler Anwendungsanteil der Fachanwendung innerhalb der TI mit sicherer Anbindung an die TI-Plattform unter Nutzung der Schnittstellen- und Ablaufdefinitionen der TI-Plattform. Fachmodule stellen geprüfte Client-Logik einer Fachanwendung dar, die durch ihre Umgebung (Krankenhaus) vor Manipulation geschützt ist.

Die **TI-Plattform** (TIP) ist unterteilt in eine **dezentrale** und eine **zentrale** Zone. Diese beiden Zonen erbringen die Basisdienste sowie die Infrastruktur- und Netzwerkdienste der TI-Plattform und sind frei von Komponenten mit fachspezifischer Logik. Darüber hinaus dienen die Zonen der Vermittlung zwischen Consumer/Secure Consumer Zone und Provider Zone. Die TI-Plattform Zone dezentral umfasst die Komponenten der TI-Plattform, die in den Umgebungen der Nutzer der TI betrieben werden – z. B. Konnektoren, Kartenterminals und Smartcards. Sie dient als Schutz der Infrastruktur vor Bedrohungen aus dem Client-Netz und umgekehrt. Zur zentralen TI-Plattform Zone gehören die zentralen Dienste der TI, wie z. B. OCSP-Responder, Konfigurationsdienst etc. Hier wird die zentrale Kommunikationsleistung der TI erbracht.

Die **Provider Zone** ist direkt an die zentrale TI-Plattform angebunden und ermöglicht die direkte Nutzung der zentralen Dienste. Die Provider Zone liegt fachlich in der Hoheit von Anwendungen, in der von der gematik zugelassene bzw. bestätigte Anbieter entsprechende Dienste betreiben. Dabei unterscheiden sich solche Anwendungen, die Teil der TI sind (Fachanwendungen und sichere Übermittlungsverfahren) und deren Sicherheit, Kompatibilität und Interoperabilität durch die gematik zugesichert sind von denen, die nicht Teil der TI sind, ihre Leistungen aber über die TI bereitstellen.

In der Provider Zone werden die fachliche Logik und die fachlichen Schnittstellen der Fachanwendungen (z. B. VSDM, ePA, E-Rezept), die Dienste des sicheren Übermittlungsverfahrens (KIM) sowie die Nutzerdienste der TI-Plattform bereitgestellt. Eine Reihe der fachanwendungsspezifischen Dienste der Versicherten sind nur von Fachmodulen aus erreichbar, die im Konnektor integriert sind.

Eine Besonderheit stellen die sog. weiteren Anwendungen (WANDA, unterteilt in WANDA smart und WANDA basic)[9] dar. Diese werden von unterschiedlichen Anbietern zur Verfügung gestellt und stellen für verschiedene Zielgruppen oder Kunden spezifische

[9] Vormalige Bezeichnung: aAdG = andere Anwendungen des Gesundheitswesens; aAdG-NetG = andere Anwendungen des Gesundheitswesens **ohne** Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens und aAdG-NetG-TI = andere Anwendungen des Gesundheitswesens **mit** Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens

Funktionalitäten bereit, die über die TI erreichbar sind. Weitere Anwendungen und deren Dienste werden von der gematik nicht spezifiziert; lediglich die Anbindung an die TI wird durch die gematik im Rahmen von Bestätigungsverfahren geprüft und zugelassen. Je nach Anbindungsart werden die Dienste der weiteren Anwendungen in der Provider Zone oder in der Existing Application Zone betrieben.

Die **Existing Application Zone** umfasst die Bestandssysteme der Fachanwendungen. Auch Netze des Gesundheitswesens mit weiteren Anwendungen des Gesundheitswesens ohne Zugriff auf zentrale Dienste der TI (WANDA basic) sind hier eingeordnet.

Die **Personal Zone** steht unter der Kontrolle der Versicherten. Dort betreibt er seine Geräte bzw. die Frontends auf seinen Geräten, mit denen er die Fachanwendungen für Versicherte bedienen kann.

2.4 Anwendungen und Dienste der Telematikinfrastruktur

2.4.1 Versichertenstammdaten-Management (VSDM)

Das Versichertenstammdaten-Management (VSDM) war die erste verfügbare Fachanwendung der TI und ermöglicht die Onlineprüfung und Onlineaktualisierung von Versichertenstammdaten (**VSD**) auf der eGK. Es handelt sich hierbei um eine **gesetzliche Pflichtanwendung**, die **bestätigt**, dass ein **Versicherter** im Rahmen der vertragsärztlichen Versorgung **Leistungen beanspruchen darf**.

Zu den Versichertenstammdaten gehören:

- persönliche Daten des Versicherten (u. a. Name, Geburtsdatum, Adresse),
- Informationen zur Krankenversicherung sowie
- Angaben zum Versicherungsschutz und zur Kostenerstattung.

Medizinische Daten, z. B. Notfalldaten (siehe Kapitel 2.4.2) oder elektronischer Medikationsplan (siehe Kapitel 2.4.3), die ebenfalls auf der eGK gespeichert sind, gehören nicht zu den Versichertendaten.

Die VSD sind auf der elektronischen Gesundheitskarte gespeichert. Bei Bedarf kann über die TI der jeweils aktuellste Stand der Daten vom Versichertenstammdatendienst abgerufen werden.

Durch Nutzung der Fachanwendung **VSDM** in einem Krankenhaus ist es möglich, **online zu prüfen**, ob ein **aktuell gültiges Versicherungsverhältnis** des Patienten vorliegt. Initiiert wird die Online-Prüfung durch einen berechtigten Akteur im Clientsystem (KIS). Weiterhin können die auf der eGK des Versicherten aktuellen VSD mit denen im **KIS gespeicherten Daten abgeglichen** bzw. in **das KIS übertragen** werden. So wird ein möglicher Missbrauch bei der Inanspruchnahme der medizinischen Leistungen weitgehend verhindert. Die Zugriffe auf die VSD werden auf der eGK protokolliert.

Das Lesen der VSD auf der eGK eines Versicherten in einem Krankenhaus setzt den Einsatz dezentraler, von der gematik zugelassener TI-Komponenten voraus (eHealth-Kartenterminal, Konnektor). Darüber hinaus ist der Einsatz einer Institutionskarte (SMC-B) erforderlich. Diese muss in einem Kartenterminal gesteckt und freigeschaltet sein. Da auf der eGK auch besonders schützenswerte Versichertendaten gespeichert sind, ist zum Lesen dieser Daten die **PIN-Eingabe einer SMC-B oder eines Heilberufsausweises** erforderlich. Diese müssen für den Lesevorgang der geschützten Daten in einem Kartenterminal gesteckt sein (Card-to-Card-Authentisierung).

Zur Onlineprüfung in einem Krankenhaus ist der Betrieb eines Konnektors erforderlich. Das darin enthaltene VSDM-Fachmodul steuert dabei die Zugriffe auf die TI. Die Administration der Fachmodule auf einem Konnektor gehören zu den Aufgaben des IT-Fachpersonals eines Krankenhauses.

Weiterführende Informationen zum VSDM

- Dokument „Implementierungsfaden Primärsysteme – Telematikinfrastruktur (TI)" [gemILF_PS]
- fachportal.gematik.de/hersteller-anbieter/primaersysteme
- https://fachportal.gematik.de/anwendungen

2.4.2 Notfalldaten-Management (NFDM)

Mithilfe des Notfalldaten-Managements (NFDM) können notfallrelevante medizinische Informationen, wie Befunde und Daten zur Medikation, über den Versicherten als Notfalldatensatz sowie Hinweise zum Ablageort von Willenserklärungen des Versicherten als Datensatz für die persönlichen Erklärungen (DPE) direkt auf der eGK gespeichert werden (siehe auch § 358 SGB V). Dabei muss die Verarbeitung von elektronischen Notfalldaten auf der eGK auch ohne Netzzugang möglich sein.

Das **NFDM** ist eine für Versicherte **freiwillige Fachanwendung** und enthält als Notfalldatensatz eine Übersicht über Vorerkrankungen und mögliche medizinische Zusammenhänge, bspw. chronische Erkrankungen, regelmäßig eingenommene Medikamente oder Allergien. Ergänzend finden sich im Notfalldatensatz Kontaktdaten von Angehörigen, die im Notfall benachrichtigt werden sollen, und von behandelnden Ärzten. Sofern ein Versicherter über einen Organspendeausweis, eine Patientenverfügung oder eine Vorsorgevollmacht verfügt, können Informationen über den Aufbewahrungsort im „Datensatz Persönliche Erklärungen" (DPE) gespeichert werden.

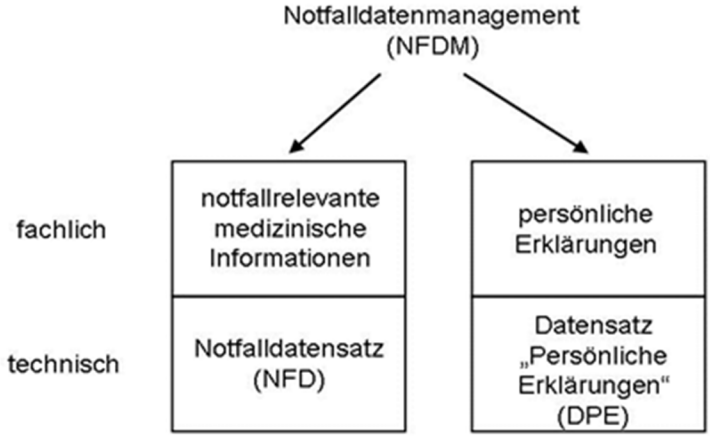

Abbildung 4: Informationsmodell NFDM (Quelle: [gemSysL_NFDM])

Nur Ärzte, Zahnärzte und deren Mitarbeiter sowie Angehörige anderer Heilberufe, darunter Notfallsanitäter, können in Notfallsituationen diese notfallrelevanten medizinischen Informationen einsehen (sog. lesender Zugriff). Das **NFDM unterstützt** somit eine **gezielte Diagnostik und Therapie** – insbesondere in Situationen, in denen für die Behandlung entscheidende anamnestische Angaben fehlen.

Die **Übermittlung und Aktualisierung** der Notfalldaten auf die eGK des Versicherten erfolgt **mittels Primärsystem bzw. KIS**.

Nach Einlesen des auf der eGK des Versicherten befindlichen Notfalldatensatzes (NFD) liegt dieser im KIS vor. Der Arzt nimmt nun die erforderliche Aktualisierung des NFD im KIS vor und signiert diesen mittels qualifizierter elektronischer Signatur (QES). Die qualifizierte Signierung setzt den Einsatz eines elektronischen Heilberufsausweises (HBA) voraus. Der HBA muss dabei in einem Kartenterminal gesteckt sein, das wiederum mit einem Konnektor verbunden sein muss. Die eigentliche Signierung wird dabei über das im Konnektor befindliche NFDM-Fachmodul vorgenommen (siehe auch Kapitel 2.4.4). Der im KIS vorliegende, qualifiziert signierte NFD kann „nun" (auch zu einem späteren Zeitpunkt) auf die eGK des Patienten übermittelt werden. Für das Schreiben des aktualisierten und qualifiziert signierten NFD auf die eGK des Patienten muss diese in einem Kartenterminal gesteckt sein. **Aktualisierung und Signierung des NFD** und das **Schreiben des NFD** auf die eGK des Patienten **können zeitlich und räumlich unabhängig voneinander erfolgen**. Das Schreiben des NFD auf die eGK des Patienten (z. B. bei Entlassung des Patienten) kann dabei durch befugtes Krankenhauspersonal ohne den Einsatz eines HBA erfolgen. Zum Schreibvorgang ist aber (mindestens) der Einsatz einer SMC-B erforderlich. Der Patient kann den NFD auf seiner eGK auf Wunsch per PIN vor dem unbefugten Zugriff schützen. Zugriffe auf den Notfalldatensatz werden zur Einsicht durch den Versicherten auf der eGK protokolliert.

Hinweis: Notfalldatensätze können auch in der elektronischen Patientenakte (ePA) des Versicherten abgelegt und von dort eingelesen werden (siehe § 341 Abs. 2 Nummer 1c SGB V). Gemäß derzeitigem Stand des Gesetzentwurfes DVPMG soll die Anwendung NFDM ab dem 01. 01. 2023 technisch auf die mit DVPMG-Gesetzentwurf neu eingeführte Patientenkurzakte überführt werden (siehe § 334 DVPMG).

Weiterführende Informationen zum NFDM

- Dokument „Implementierungsfaden Primärsysteme Notfalldaten-Management (NFDM)" [gemILF_PS_NFDM] sowie die Checklisten zum NFDM, einsehbar unter https://fachportal.gematik.de/anwendungen/notfalldatenmanagement
- gematik.de/anwendungen/notfalldaten/

2.4.3 Elektronischer Medikationsplan (eMP)/Arzneimitteltherapiesicherheit (AMTS)

Mit dem elektronischen Medikationsplan (kurz: E-Medikationsplan oder eMP) haben Ärzte, Zahnärzte, Apotheker und Psychotherapeuten, die an der Behandlung eines Versicherten beteiligt sind, mehr Transparenz zu den eingenommenen Medikamenten des Patienten.

Der eMP wird auf der eGK gespeichert (vgl. § 358 SGB V) und enthält einen strukturierten Überblick darüber, welche Medikamente ein Versicherter aktuell einnimmt. Darüber hinaus enthält der eMP medikationsrelevante Informationen, die wichtig sind, um unerwünschte Wechselwirkungen zu vermeiden, bspw. zu Allergien.

Der E-Medikationsplan wird auf Wunsch des Versicherten erstellt[10]. In der Regel übernimmt der Hausarzt die **Erstanlage** des **E-Medikationsplans**. Dies **kann aber auch im Krankenhaus erfolgen**, sofern der Patient dies ausdrücklich wünscht und in die Speicherung einwilligt. Zu diesem Zweck wird ein eHealth-Kartenterminal, eine Institutionskarte (SMC-B), ein AMTS-fähiges Clientsystem (KIS) und ein Zugang zur TI via Konnektor benötigt. Auf dem Konnektor befindet sich das entsprechende AMTS-

[10] Sobald ein Versicherter mindestens drei systemisch wirkende, zu Lasten der gesetzlichen Krankenversicherung verschriebene Arzneimittel dauerhaft, also über einen Zeitraum von mindestens 28 Tagen, anwendet, hat er Anspruch auf die Erstellung und Aktualisierung eines eMPs.

Fachmodul. Für den Zugriff auf die medizinischen Daten der eGK ist gesetzlich zudem das Vorhandensein eines elektronischen Heilberufsausweises (HBA) festgelegt.

Sobald die SMC-B bzw. der HBA und die vom Versicherten freigeschaltete eGK im Kartenterminal stecken, kann der berechtigte Akteur in seinem KIS den standardisierten Datensatz für den eMP auf der eGK anlegen. Der eMP-Datensatz ist standardmäßig durch eine PIN geschützt. Der Versicherte kann diese PIN jedoch bei Bedarf deaktivieren.

Durch die Übergabe seiner eGK und, falls aktiviert, durch Eingabe seiner PIN, erlaubt der Versicherte behandelnden Ärzten, Zahnärzten, Psychotherapeuten bzw. Kliniken oder auch Apotheken den Zugriff auf seinen E-Medikationsplan. Zugriffe auf den eMP/AMTS-Datensatz werden zur Einsichtnahme für den Versicherten auf der eGK protokolliert.

Das Datenmodell des eMP wurde in enger Abstimmung mit dem Bundeseinheitlichen Medikationsplan (BMP) erstellt, so dass auf Basis dieser Daten gleichermaßen ein eMP auf der Karte gespeichert und ein ausgedruckter BMP übergeben werden kann.

Daten des elektronischen Medikationsplans können auch in der elektronischen Patientenakte (ePA) des Versicherten abgelegt und von dort eingelesen werden (siehe § 341Absatz 2 Nummer 1b SGB V).

Gemäß Gesetzentwurf DVPMG soll der elektronische Medikationsplan ab dem 01. 01. 2023 nicht mehr auf der elektronischen Gesundheitskarte gespeichert werden, sondern als eigenständige Online-Anwendung im Rahmen der TI zur Verfügung stehen.

Weiterführende Informationen zum eMP/AMTS

- Dokument „Implementierungsfaden Primärsysteme – elektronischer Medikationsplan/AMTS-Datenmanagement" [gemILF_PS_AMTS] sowie die Checklisten zum eMP, einsehbar unter https://fachportal.gematik.de/anwendungen/elektronischer-medikationsplan
- gematik.de/anwendungen/e-medikationsplan/

2.4.4 Qualifizierte Elektronische Signatur (QES) und Komfortsignatur

Mithilfe der qualifizierten elektronischen Signatur (QES) können Leistungserbringer, bspw. Ärzte, medizinische Dokumente und Datensätze elektronisch rechtssicher signieren. Dabei ist die QES der Unterschrift per Hand gleichgestellt. Die qualifizierte elektronische Signatur ist eine Basisfunktion für (gesetzliche) TI-Anwendungen und an die digitale TI-Identität eines Leistungserbringers gekoppelt.

Die Erstellung einer QES erfordert neben einem Zugang zur TI ein entsprechend angepasstes KIS, einen Konnektor, ein eHealth-Kartenterminal, einen elektronischen Heilberufsausweis sowie die Eingabe einer PIN (PIN.QES des HBA).

Zur QES-Funktionalität stellt der Konnektor generische Schnittstellen für verschiedene QES-Basisdienste (SignatureService, EncryptionService, CertificateService, AuthSignatureService) zur Verfügung. Diese Schnittstellen können vom Clientsystem (KIS) in einer Vielzahl von Szenarien genutzt werden:

- Signatur und Signaturprüfung mit Identitäten von SMC-B (nonQES) und HBA (QES),
- Verschlüsselung und Entschlüsselung von Dokumenten und Daten mit SMC-B und HBA,
- Authentisierung mit SMC-B und HBA und

- Smartcard-Zertifikatsabfragen sowie Prüfung von Zertifikaten.

Die Operationen dieser Dienste können einzeln genutzt werden. Sie ermöglichen es, Dokumente mithilfe von Zertifikats- und Verschlüsselungsmaterial der TI-Smartcards (HBA, SMC-B) zu verschlüsseln und zu signieren. Wenn es sich bei der Smartcard um eine sichere Signaturerstellungseinheit für qualifizierte Signaturen (also den HBA) handelt, so wird das Niveau einer qualifizierten elektronischen Signatur erreicht.

Das Clientsystem kann den Leistungsumfang der Komfortsignatur des Konnektors nur nutzen, wenn am Konnektor der Parameter SAK_COMFORT_SIGNATURE konfiguriert ist.

Nach der Einführung von elliptischen Kurven auf TI-Smartcards der Generation G2.1 ist es optional möglich, bei Operationen des Signatur-, Verschlüsselungs- und Zertifikatsdienstes und der Authentisierung auszuwählen, ob ECC- oder RSA-Zertifikate verwendet werden. Das Default-Verhalten an der Konnektorschnittstelle ist so beschaffen, dass ohne explizite Steuerung der Optionen RSA oder ECC durch das Primärsystem (KIS) der Konnektor ab Version PTV4 unter Auswertung der verfügbaren Karten die geeigneten Zertifikate auswählt. PTV3-Konnektoren verwenden auch bei Karten der Generation G2.1 deren RSA-Zertifikate.

Des Weiteren ermöglicht der Konnektor im Zusammenspiel mit dem HBA als Signaturkarte eine Stapelsignatur. Das Clientsystem stellt hierfür Dokumente zu einem Stapel zusammen, um sie mit einem Signatur-Request vom Konnektor signieren zu lassen.

Eine weitere Vereinfachung der Signaturnutzung ermöglicht der Konnektor durch die **Komfortsignatur**. Die Nutzung der Komfortsignatur ist von der Konfiguration der Leistungserbringerumgebung abhängig. Sie erlaubt die Erstellung von bis zu 250 qualifizierten elektronischen Signaturen im Laufe eines Tages mit nur einer Freischaltung der PIN.QES des HBA. Die PIN-Freischaltung erfolgt bei der täglichen Aktivierung der Komfortsignaturfunktion. Anschließend können die Signaturen mit der Authentisierung durch das Primärsystem ohne erneute PIN-Eingabe erstellt werden.

Nachfolgend wird ein Beispielszenario zur Anwendung der Komfortsignatur im Krankenhaus mit zwei Konnektoren und jeweils einem Freischalt-KT dargestellt.

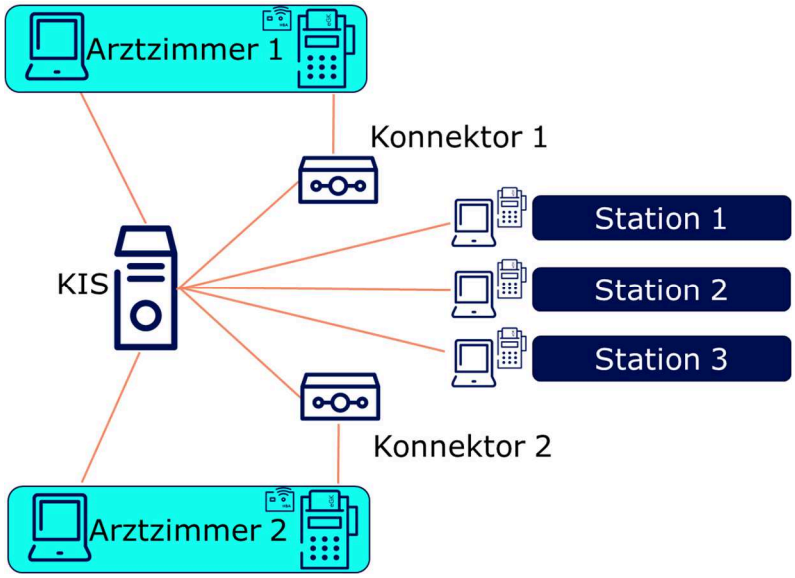

Abbildung 5: Beispielhafte Anwendung Komfortsignatur im Krankenhaus

In diesem Beispielszenario steckt der HBA in einem zugriffsgeschützten Kartenterminal. Ein zugriffsgeschütztes Kartenterminal kann dort eingerichtet werden, wo es die

Arbeitsorganisation erlaubt (hier: Arztzimmer). Der Arzt aktiviert die Komfortsignatur direkt am zugriffsgeschützten Kartenterminal oder über eine Remote-PIN-Eingabe an einem dedizierten Kartenterminal (Freischalt-KT). Beide Kartenterminals müssen am selben Konnektor terminieren. Das KIS identifiziert den Konnektor zum HBA des Arztes. Die Signatur kann dann ohne Interaktion des Kartenterminals von beliebigen Arbeitsplätzen ausgeführt werden (hier im Beispiel: in unterschiedlichen Stationen). Die Ansteuerung des zutreffenden Konnektors, an dem der HBA angebunden ist, übernimmt dabei das KIS.

Zur Nutzung einer personengebundenen Primärsystemsitzung gelten folgende Voraussetzungen:

- Jeder Nutzer (Arzt, KH-Personal …) hat eine eigene Sitzung am Primärsystem (verwaltet durch z. B. Betriebssystem oder Anwendung).
- Der Zugang zu diesen Sitzungen erfordert eine Authentifizierung (PIN, Passwort, Biometrie, Token).
- Der Zugang zu diesen Sitzungen ist organisatorisch gegen Missbrauch geschützt (z. B. Bildschirmsperre).

Bei der Authentifizierung bei der Signaturerstellung authentifiziert das Primärsystem den Nutzer durch:

- Eingabe einer dedizierten Signaturfreigabe-PIN oder
- Eingabe eines Passwortes oder
- Einlesen eines biometrischen Merkmales oder
- Einlesen eines Tokens (z.B. NFC-Token).

Das Primärsystem muss das Authentifizierungsmerkmal bei der Eingabe der PIN.QES mit dem Nutzer verknüpfen (Komfortsignatur aktivieren, Token auflegen, PIN.QES freischalten).

Das Primärsystem ermittelt die zu diesem Nutzer erzeugte starke UserID und verwendet sie im Kontext des Signaturauftrages.

Beispiel zur Authentifizierung mittels PIN

Bei der Aktivierung der Komfortsignatur wird der Anwender zur Eingabe einer Signaturfreigabe-PIN aufgefordert. Das Primärsystem speichert den Hash der Signaturfreigabe-PIN zusammen mit dem Common Name (CN, Vor- und Nachname des Inhabers) des HBA und der starken UserID in der zentralen Datenbank. Die UserID ist eine eindeutige vom Primärsystem vergebene interne ID, die nur bei Zugriffen auf einen HBA erforderlich ist. Sie wird temporär im Konnektor gespeichert und einem HBA zugeordnet, wenn eine HBA-Kartensitzung in einen erhöhten Sicherheitszustand versetzt wird (PIN-Eingabe). Sie bleibt gespeichert und zugeordnet, solange die Kartensitzung gültig ist (i. d. R. solange der HBA steckt). Bei Zugriffen auf den HBA im weiteren Verlauf muss die bei der Eröffnung verwendete UserID im Kontext korrekt angegeben sein (z. B. Signatur oder Entschlüsselung). Bei der Signaturerstellung wählt der Nutzer den HBA aus und gibt die Signaturfreigabe-PIN ein. Das KIS sucht aus der zentralen Datenbank die zu PIN und HBA passende UserID und sendet den Signaturauftrag an den Konnektor.

Beispiel zur Authentifizierung mittels NFC-Token

Bei der Aktivierung der Komfortsignatur wird der Anwender zum Auflegen des NFC-Token aufgefordert. Das Primärsystem koppelt die UserID mit dem Token auf sichere

Art und Weise (UserID darf für unberechtigte nicht einsehbar sein). Bei der Signaturerstellung legt der Nutzer den NFC-Token auf. Das PS prüft die Berechtigungen des Nutzers anhand des Tokens und sendet den Signaturauftrag ggf. an den Konnektor.

Wie letztlich das KIS, das in Ihrem Krankenhaus eingesetzt wird, die QES-Funktionen des Konnektors ansteuert und nutzt, können Sie den Unterlagen des jeweiligen KIS-Herstellers entnehmen.

Weiterführende Informationen zu QES und Komfortsignatur

- Dokument „Implementierungsfaden Primärsysteme – Telematikinfrastruktur (TI)" [gemILF_PS]
- fachportal.gematik.de/anwendungen/qualifizierte-elektronische-signatur

2.4.5 Elektronische Patientenakte (ePA)

Ab dem 01.01.2021 haben alle gesetzlich Versicherten Anspruch auf eine elektronische Patientenakte. Die Fachanwendung ePA wird in der TI stufenweise eingeführt. In der ersten Phase beginnt ab dem 01. 01. 2021 eine Test- und Einführungsphase mit ausgewählten Arztpraxen. In der zweiten Phase werden ab dem 01. 04. 2021 alle Vertragsärzte mit der ePA verbunden, zum 01. 07. 2021 müssen dann alle vertragsärztlich tätigen Leistungserbringer in der Lage sein, die ePA zu nutzen. In den **Krankenhäusern müssen spätestens bis zum 01. 01. 2022** alle Voraussetzungen für die Nutzung der ePA geschaffen sei.

Ziel der ePA ist eine umfassende Vernetzung des deutschen Gesundheitswesens – sowohl zwischen verschiedenen Fachärzten oder Apotheken als auch zwischen Ärzten, Apotheken und Patienten. Viele bisher analog oder in Papierform ablaufende Arbeitsschritte können durch die ePA digitalisiert und damit vereinfacht werden. Fachärzte unterschiedlicher Disziplinen sind dank der ePA in der Lage, ihre Patienten in Zukunft ganzheitlich zu betrachten, sofern ein Patient eine ePA führt und Leistungserbringer zum Zugriff auf seine ePA berechtigt. Die Dokumente in der ePA sind bundesweit verfügbar und können einrichtungs- und sektorenübergreifend ausgetauscht werden.

Die ePA ist eine vom Patienten geführte Akte; die Nutzung der ePA ist für den Versicherten freiwillig und kostenfrei. In der ePA eines Versicherten werden Medikationspläne, Therapieansätze und Befunde hinterlegt, sofern der Versicherte eine ePA bei seiner Krankenversicherung beantragt und eingerichtet hat.

Nach § 348 Abs. 1 SGB V haben Versicherte „Anspruch auf Übermittlung von Daten nach § 341 Absatz 2 Nummer 1 bis 5, 10, 11 und 13 in die elektronische Patientenakte und dortige Speicherung, soweit diese Daten im Rahmen der Krankenhausbehandlung des Versicherten elektronisch erhoben wurden und soweit andere Rechtsvorschriften nicht entgegenstehen." In einem **Krankenhaus müssen** daher **folgende Daten in die ePA** eines Versicherten **übertragen werden können**:

- Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen,
- Daten des elektronischen Medikationsplans,
- Daten der elektronischen Notfalldaten,
- Daten in elektronischen Briefen zwischen den an der Versorgung der Versicherten teilnehmenden Ärzten und Einrichtungen (elektronische Arztbriefe),

- Daten zum Nachweis der regelmäßigen Inanspruchnahme zahnärztlicher Vorsorgeuntersuchungen (elektronisches Zahn-Bonusheft),
- Daten zur Früherkennung von Krankheiten bei Kindern (elektronisches Untersuchungsheft für Kinder),
- Daten über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung (elektronischer Mutterpass),
- Daten der Impfdokumentation (elektronische Impfdokumentation),
- Daten zur pflegerischen Versorgung des Versicherten,
- Daten elektronischer Verordnungen sowie
- sonstige von den Leistungserbringern für den Versicherten bereitgestellte Daten.

Anbieter der ePA ist i.d.R. die Krankenversicherung des Versicherten. Das Aktensystem ePA ist die Serverseite der Fachanwendung ePA und wird ebenfalls von der jeweiligen Krankenversicherung verantwortet. Weitere, in den Betrieb des ePA-Aktensystems eingebundene Unternehmen, handeln stets im Auftrag des Anbieters. Letzterer trägt dabei die gesamte betriebliche Verantwortung. Weder Anbieter noch Betreiber können Inhalte der Akte lesen.

Das Aktensystem ePA besteht aus den folgenden Komponenten (siehe Abbildung 6 auf der nachfolgenden Seite):

- **Authentifizierung von Nutzern**

  Die Komponente „Authentisierung Versicherter" ist eine Teilkomponente der Komponente Zugangsgateway des ePA-Aktensystems. Sie wird von der dezentralen Fachlogik im ePA-Frontend des Versicherten und dem ePA-Fachmodul des Konnektors verwendet, um die Authentifizierung von Versicherten und deren berechtigten Vertretern zu erstellen.

- **Zugangsgateway des ePA-Aktensystems**

  Das Zugangsgateway für Versicherte (in Abbildung 6: Zugangsgateway TI) ermöglicht den Versicherten bzw. ihren berechtigten Vertretern den Zugang zum Aktensystem über das Internet. Auf der einen Seite dient das Zugangsgateway der Abschottung des ePA-Aktensystems in Richtung Internet. Auf der anderen Seite regelt es den kontrollierten Zugriff der Versicherten auf das Aktensystem mit seinen funktionalen Komponenten.

- **Autorisierung und Schlüsselverwaltung**

  Die Komponente „Autorisierung" stellt authentifizierten Nutzern eines Aktenkontos bei gegebener Autorisierung das für sie jeweils empfängerverschlüsselte Schlüsselmaterial bereit.

- **Dokumentenverwaltung**

  Die Komponente „Dokumentenverwaltung" des ePA-Aktensystems dient dem sicheren Speichern und Auffinden von Dokumenten des Versicherten in seiner persönlichen Akte. Diese Funktion können der Versicherte selbst oder von ihm benannte Vertreter, Leistungserbringer und Kostenträger nutzen.

- **Schlüsselgenerierungsdienst (SGD)**

  Die Dokumente der Patienten werden in der elektronischen Patientenakte mehrfach vor unberechtigtem Zugriff geschützt. Da die Dokumente Ende-zu-Ende-verschlüsselt werden, finden Ver- und Entschlüsselung in den Produkttypen der dezentralen Umgebungen statt (ePA-Fachmodul, ePA-Modul Frontend des Versicherten, KTR-Consumer). Dazu wird für jedes Dokument in der dezentralen Umgebung ein zufälliger, symmetrischer Dokumentenschlüssel generiert, mit

dem das Dokument verschlüsselt wird. Dieser Dokumentenschlüssel wiederum wird mit dem Aktenschlüssel eines Aktenkontos verschlüsselt und dem verschlüsselten Dokument beigefügt. Dieses Verschlüsselungspaket stellt dasjenige Daten-objekt dar, das als „Dokument" in der Komponente „Dokumentenverwaltung" gespeichert wird.

Aktenschlüssel und Kontextschlüssel werden darüber hinaus für jeden Zugriffsberechtigten nacheinander mit zwei symmetrischen Schlüsseln verschlüsselt. Das Verfahren zur Generierung der berechtigten individuellen symmetrischen Schlüssel wird durch ein zweistufiges Verfahren von zwei unabhängigen Schlüsselgenerierungsdiensten (SGD) umgesetzt. Dabei wird das Chiffrat des durch den Anbieter des Aktensystems betriebenen SGD 1 durch einen weiteren, von einem unabhängigen Anbieter betriebenen SGD 2 noch einmal gesichert (in der Abbildung nicht aufgeführt).

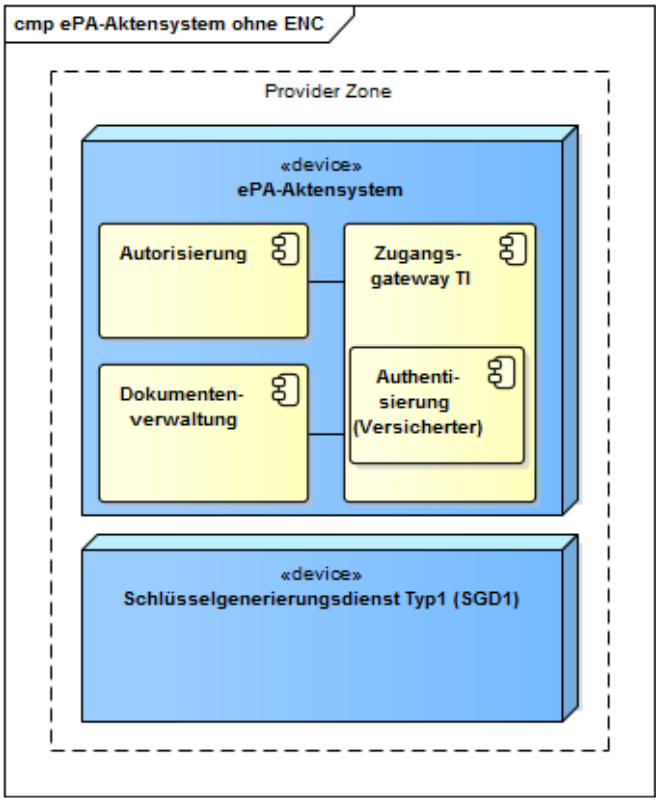

Abbildung 6: Komponenten des ePA-Aktensystems (Quelle: [gemSpec_Aktensystem])

Das ePA-Aktensystem eines Anbieters kommuniziert in Richtung des Versicherten jeweils mit einem (oder mehreren) ePA-Frontends des Versicherten (FdV). In Richtung der Leistungserbringerinstitution kommuniziert das ePA-Aktensystem ausschließlich mit dem Fachmodul ePA im Konnektor. Das Fachmodul ePA im Konnektor übernimmt die Kommunikation mit dem KIS. Das ePA-Aktensystem nutzt außerdem zentrale Dienste der TI-Plattform. Eine Übersicht über die benachbarten Systeme des ePA-Aktensystems bietet Ihnen Abbildung 7[11].

[11] LE = Leistungserbringer (bspw. Arzt); LEI = Leistungserbringerinstitution (bspw. Klinik), HSM = Hardware Security Module, SMC-B-KTR = spezielle Variante der Institutionskarte SMC-B für Kostenträger (bspw. Krankenversicherung)

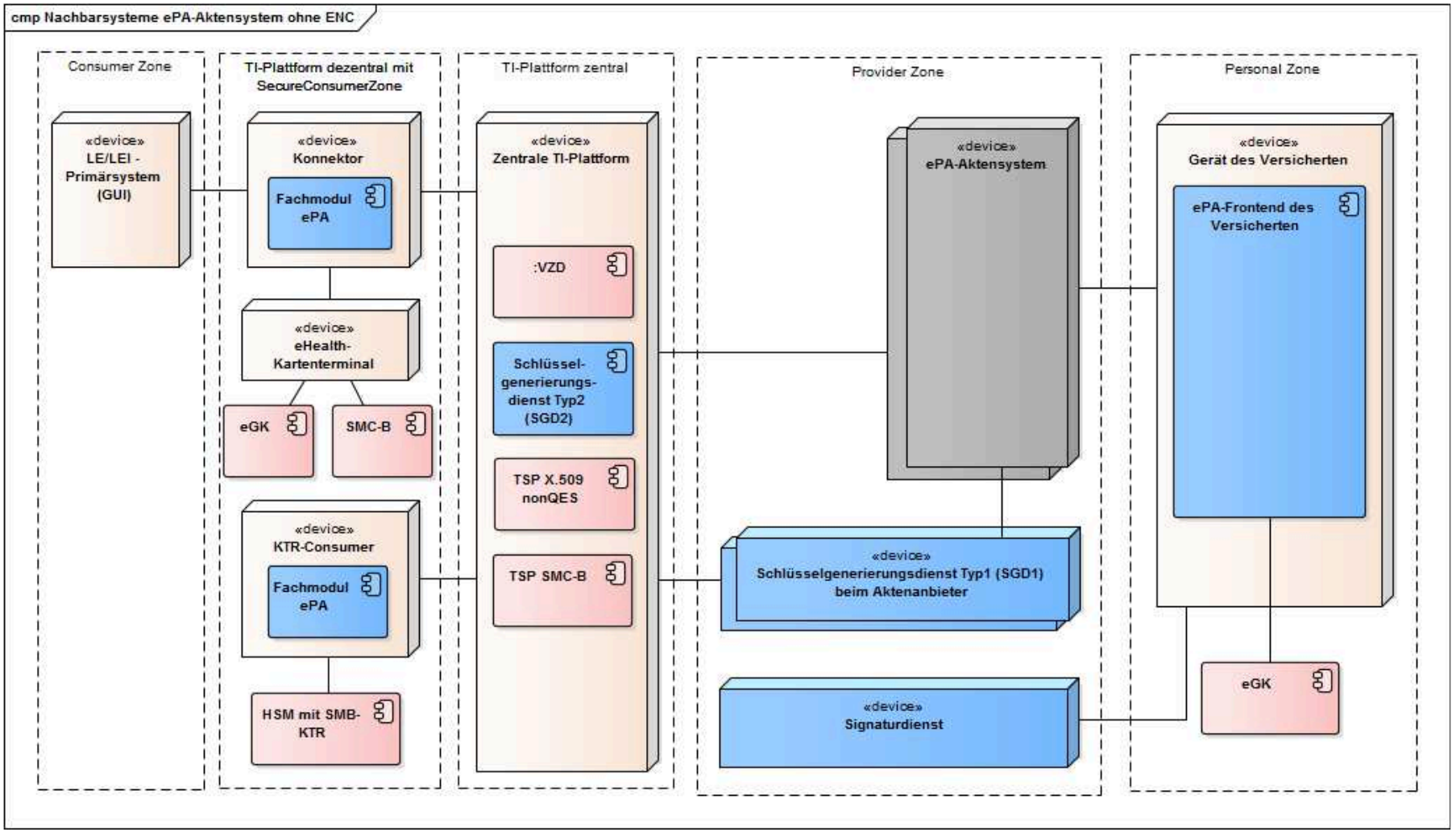

Abbildung 7: ePA-Aktensystem und Nachbarsysteme (Quelle: [gemSpec_Aktensystem])

Damit Ärzte oder andere Leistungserbringer auf Dokumente innerhalb der ePA zugreifen können und sie einen schnelleren Überblick über den Gesundheitszustand ihres Patienten erhalten, muss der Versicherte ihnen Zugriff erteilen. Die Versicherten entscheiden selbstständig darüber, welche Leistungserbringer in seiner ePA auf welche Dokumente und über welchen Zeitraum hinweg zugreifen dürfen. Einmal vergebene Zugriffsrechte können vom Versicherten jederzeit widerrufen werden.

Bei Aufnahme des Patienten in ein Krankenhaus kann der Zugriff auf die ePA vom Patienten freigegeben oder am Kartenterminal vor Ort angefordert werden. Dann können ausgewählte Daten in das KIS eingespielt werden. So erhält das Krankenhaus bspw. schnell Einblick in den Notfalldatensatz und den elektronischen Medikationsplan des Patienten.

Während der Behandlung werden wie üblich alle Informationen im KIS dokumentiert. Erst bei der Entlassung des Patienten werden auf seinen Wunsch hin alle relevanten Dokumente in die ePA hochgeladen, die für die nachbehandelnden Ärzte wichtig sind. Diese administrative Bearbeitung der ePA kann auch an das Fachpersonal delegiert werden, denn nicht nur ein Krankenhausarzt allein ist hierzu berechtigt. Einige Anwendungen oder bestimmte Dokumente, wie der Arztbrief, die elektronische Arbeitsunfähigkeitsbescheinigung oder die Aktualisierung eines Notfalldatensatzes, erfordern allerdings eine qualifizierte elektronische Signatur (QES). Hierfür wird ein elektronischer Heilberufsausweis (HBA) benötigt.

Um in einem Krankenhaus auf die ePA eines Versicherten zugreifen zu können, werden – neben einem ePA-fähigen KIS – PTV4-Konnektoren und eHealth-Kartenterminals benötigt. Der Konnektor macht zusätzlich die zentralen und dezentralen Komponenten der TI für das KIS zugänglich. Daneben ist zur Authentisierung in der TI die Institutionskarte SMC-B erforderlich.

Die Berechtigung zum Zugriff auf die ePA des Versicherten erteilt der Versicherte entweder mit Hilfe seines Frontends (App auf dem Smartphone) oder im Krankenhaus mittels einer Ad-hoc-Berechtigung. Dabei fordert die medizinische Fachangestellte des Krankenhauses nach Stecken der eGK in das Kartenterminal vor Ort eine Ad-hoc-Berechtigung am KIS an. Der Patient muss nun die Berechtigung am Kartenterminal durch Eingabe der PIN bestätigen. Auf dem Display des Kartenterminals wird dabei die Anforderung zur Ad-hoc-Berechtigung sowie die Dauer der Gültigkeit der Zugriffsberechtigung für das Krankenhaus angezeigt. Das KIS fügt der lokalen Primärdokumentation ein ePA-Kennzeichen als Markierung einer bestehenden Zugriffsberechtigung hinzu.

Weiterführende Informationen zur ePA

- Dokumente „Implementierungsfaden Primärsysteme – Elektronische Patientenakte (ePA)“ [gemILF_PS_ePA] und „Spezifikation ePA-Aktensystem“ [gemSpec_Aktensystem]
- fachportal.gematik.de/anwendungen/elektronische-patientenakte
- gematik.de/anwendungen/e-patientenakte/
- https://www.dkgev.de/themen/digitalisierung-daten/telematik-infrastruktur/elektronische-patientenakte-epa/ [Umsetzungshinweise und Anwendungsfälle für die elektronische Patientenakte]

2.4.6 Kommunikation im Medizinwesen (KIM)

Als sicheres Übermittlungsverfahren (SÜV) ermöglicht die Anwendung „Kommunikation im Medizinwesen“ (KIM – ehemals KOM-LE) Leistungserbringern, ihren Organisationen

und den gesetzlichen Krankenversicherungen den sicheren Versand digitaler Nachrichten und Dokumente. Beispielsweise dient KIM für die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) als Übermittlungsverfahren. Spezielle Funktionen von KIM unterstützen die gesicherte Zustellung und ermöglichen eine automatisierte Auswertung auf der Empfängerseite.

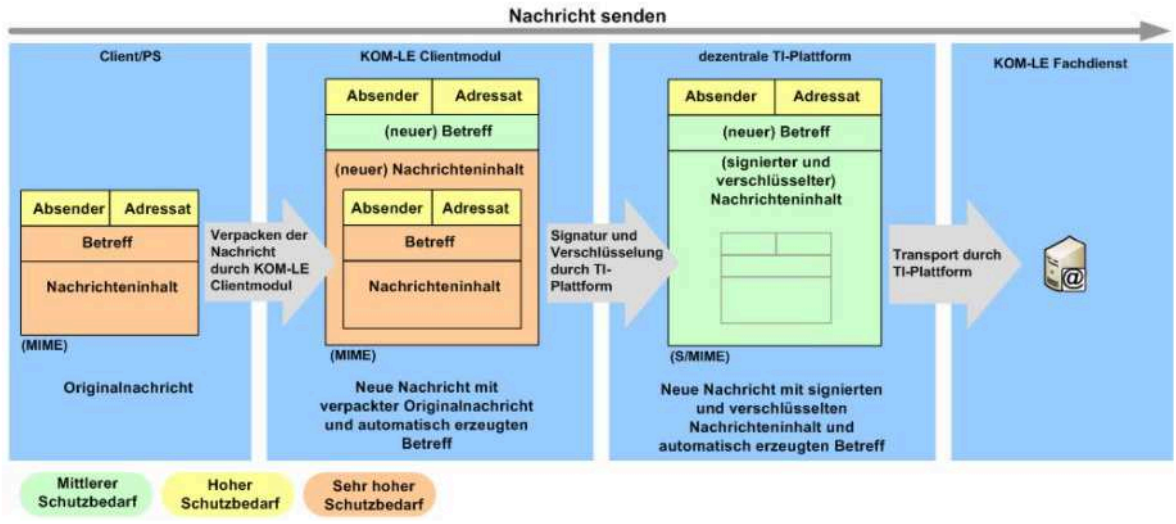

Abbildung 8: Integritäts- und Vertraulichkeitsschutz beim Senden einer KOM-LE-Nachricht der Fachanwendung KIM (Quelle: [gemSysL_KOMLE])

KIM basiert auf E-Mail-Kommunikation und wird von mehreren, von der gematik zugelassenen Anbietern angeboten. Alle Anbieter haben die von der gematik vorgegebenen Produkteigenschaften gleichermaßen umgesetzt. Die Dienste der KIM-Anbieter sind untereinander interoperabel, so dass ein zuverlässiger Versand und eine sichere Zustellung der Nachrichten erfolgt, und zwar unabhängig davon, welcher KIM-Anbieter in Ihrem Krankenhaus beauftragt wurde.

KIM ist Signatur- und Verschlüsselungsfunktionen ausgestattet und erlaubt ab Version 1.5 das Versenden großer Dokumenten-Anhänge (mindestens bis zu 500 MB). Ein speziell für diesen Zweck entwickeltes **KIM-Clientmodul**, welches zwischen dem Clientsystem des Nutzers (z. B. KIS, Microsoft Outlook) und dem **KIM-Fachdienst** (Mailserver) positioniert wird, setzt diese Sicherheitsfunktionen um. Dieses KIM-Clientmodul kann ein separat zu installierendes Modul sein – ab der KIM-Version 1.5 ist es allerdings auch möglich, dieses in ein Primärsystem oder KIS zu integrieren (siehe auch Kapitel 4.3).
Das KIM-Clientmodul kann – eine separate Installation vorausgesetzt – in einem Krankenhaus auch mehrfach betrieben werden; je nach Ausgestaltung des Kommunikations-Architekturkonzepts.

Beachten Sie, dass ein **KIM-Clientmodul in der Ausbaustufe 1.0** immer nur **einen einzigen Konnektor** bedienen kann. Erst mit Umsetzung der nächsten Ausbaustufe (**KIM-Version 1.5**) kann das **KIM-Clientmodul mehrere Konnektoren ansprechen**. Wann ein solcher Multikonnektorbetrieb auch in Ihrem Krankenhaus erfolgen kann, erfahren Sie von Ihrem KIM-Anbieter.

Versand und Empfang von KIM-Nachrichten

Eine Übersicht über die Funktionsweise und Schnittstellen der beteiligten Systeme bietet Abbildung 9.

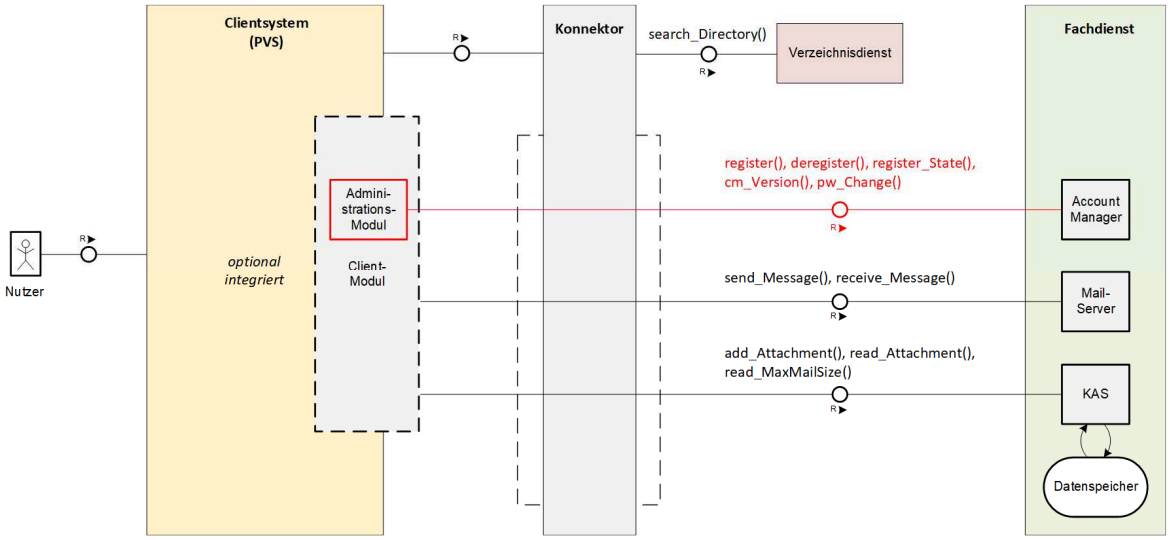

Abbildung 9: Systemkomponenten KIM (Quelle: [gemSpec_CM_KOMLE])

Leistungserbringer werden auf die Anwendung KIM in der Regel über ihr Primärsystem (KIS) oder über einen etablierten E-Mail-Client zugreifen. Dabei erfolgt eine Authentisierung per SMC-B/HBA über Konnektor und eHealth-Kartenterminal. Der Sender einer Nachricht wählt für den Versand aus dem **(KIM-) Verzeichnisdienst** (**VZD**) ein oder mehrere Empfänger (bzw. deren E-Mail-Adressen) aus. Eine im Clientsystem des Nutzers für den Versand erstellte und freigegebene Nachricht (inkl. ggf. zugehöriger Anhänge) wird dann auf dem KIM-Clientmodul mit der SMC-B des Senders signiert und für jeden Empfänger mit dem/den jeweiligen öffentlichen Schlüssel/n verschlüsselt. Die für diese Verschlüsselung erforderlichen Zertifikate der Empfänger werden vom KIM-Clientmodul aus dem VZD der TI mit Hilfe der (KIM-) E-Mail-Adressen ermittelt. Nach erfolgreicher Signierung und Verschlüsselung erfolgt die Übertragung zu den Ziel-KIM-Fachdiensten, von wo aus Empfänger ihre Nachrichten abrufen können.

Beim Senden (und beim Empfangen) von KIM-Nachrichten baut das Clientsystem zum KIM-Clientmodul eine Verbindung auf. Das KIM-Clientmodul wiederum baut Verbindungen zu den KIM-Fachdiensten und zum Konnektor auf. Sämtliche Verbindungen werden über TLS-Verschlüsselungen abgesichert.

Beim **Nachrichtenversand** findet die Kommunikation zwischen dem Clientsystem, dem KIM-Clientmodul und dem KIM-Fachdienst über SMTP statt. Das **KIM-Clientmodul fungiert als SMTP-Proxy**, der das Clientsystem mit dem KIM-Fachdienst verbindet, die Integrität und Vertraulichkeit der vom Clientsystem gesendeten Nachricht schützt und die Nachricht an den KIM-Fachdienst übermittelt. Das KIM-Clientmodul stellt dabei sicher, dass die Nachricht erfolgreich zu dem KIM-Fachdienst übertragen wird. Die korrekte Zustellung der Nachricht zum Ziel-Fachdienst des Empfängers erfolgt ebenfalls innerhalb der Fachanwendung KIM. Falls die Übermittlung einer Nachricht fehlschlägt, benachrichtigt das KIM-Clientmodul das Clientsystem unter Verwendung entsprechender Antwortcodes über den Fehler.

Die Zustellung von KIM-Nachrichten wird vom Clientsystem des Nutzers initiiert, d.h., das Clientsystem ruft über das KIM-Clientmodul die Nachrichten am KIM-Fachdienst ab. Beim **Abruf von Nachrichten** findet die Kommunikation zwischen dem Clientsystem, dem KIM-Clientmodul und dem KIM-Fachdienst über POP3 statt. Das **KIM-Clientmodul fungiert dabei als POP3-Proxy**, der das Clientsystem mit dem KIM-Fachdienst (POP3-Server) verbindet, die Entschlüsselung und Signaturprüfung für die abgeholten Nachrichten durchführt und die entschlüsselten Nachrichten an das Clientsystem liefert. Die Ergebnisse der Signaturprüfung werden dem Nutzer als Vermerk, der in den Inhalt

der Nachricht integriert wird, sowie als ein detaillierter Bericht in Form einer angehängten PDF-Datei mitgeteilt.

Zusätzlicher Bestandteil des KIM-Clientmoduls ist ein Administrationsmodul, mit dem die Verwaltung des Accounts des KIM-Teilnehmers ermöglicht wird. Dazu kommuniziert das Administrationsmodul über eine TLS-Verbindung mit dem Account Manager des KIM-Fachdienstes. Mit Hilfe des Administrationsmoduls kann ein neuer KIM-Teilnehmer registriert, ein bestehender Teilnehmer de-registriert, entsprechende Abfragen zum Registrierungsstatus des KIM-Teilnehmers durchgeführt sowie das benötigte Client-Zertifikat (PKCS#12-Datei) heruntergeladen werden (manuell oder automatisiert). Des Weiteren können mittels Administrationsmodul Abwesenheitsnotizen verwaltet und die KIM-Mail-Adresse auf eine andere Telematik-ID portiert werden.

KIM nutzt neben anderen anwendungsübergreifenden Diensten der TI insbesondere den zuvor kurz erwähnten **Verzeichnisdienst** (VZD) der TI. Dabei ermitteln KIM-Teilnehmer über den VZD die Kontaktdaten der KIM-Empfänger („Adressbuch-Funktion"). Die Abfrage des VZD vom Clientsystem des Nutzers kann über LDAP erfolgen. Um LDAP-Anfragen gegenüber dem VZD durchzuführen, fungiert der Konnektor als LDAP-Proxy[12], wobei die Kommunikation über das LDAPv3 Protokoll erfolgt.

Exkurs Verzeichnisdienst (VZD)

Im VZD werden gemäß § 313 SGB V Daten zu Leistungserbringern, organisatorischen Einheiten von Leistungserbringern (z. B. Krankenhäuser, Fachabteilungen der Krankenhäuser) und anderen juristischen Personen oder deren Mitarbeitern, welche die TI nutzen, geführt. Die Daten umfassen den Namen, die Adressdaten, technische Adressierungsdaten, eine eindeutige Identifikationsnummer (Telematik-ID), das Fachgebiet und den öffentlichen Teil der technischen Identität des Nutzers. Daten von Versicherten werden nach derzeitiger Gesetzeslage nicht im VZD geführt.

Sowohl der Ersteintrag als auch die weitere Pflege der VZD-Daten obliegen unterschiedlichen Akteuren. Nach Herausgabe einer oder mehrerer SMC-Bs zu einer Telematik-ID legt der jeweilige Kartenherausgeber zu dieser **Telematik-ID** (siehe auch Kapitel 3.2.2) einen initialen Datensatz im VZD an und befüllt ihn mit Basisdaten. Die Identifikation des Datensatzes im VZD und damit auch die Identifikation der im VZD eingetragenen natürlichen oder juristischen Person bzw. der Institutionseinheit erfolgt daher ebenfalls über die Telematik-ID. Die Basisdaten enthalten zunächst keine über KIM adressierbare E-Mail-Adressen.

Basis für einen SMC-B-basierten VZD-Eintrag einer Arztpraxis sind beispielsweise:

- Name der Betriebsstätte
- Straße und Hausnummer
- Postleitzahl und Ort
- Bundesland (bspw. Bereich der Kassenärztlichen Vereinigung der Betriebsstätte)
- Betriebsstättennummer (BSNR)
- Spezielle Fachgebietscodierung

Das vollständige Datenmodell des VZD können Sie der gematik-Spezifikation „Verzeichnisdienst" [gemSpec_VZD] entnehmen, die Sie im Internet-Fachportal der gematik abrufen können (bspw. unter fachportal.gematik.de/dokumentensuche. Die **sektorspezifische Ausprägung** für **Krankenhäuser teilt** Ihnen Ihr **Kartenherausgeber mit**.

[12] Weiterführende Informationen dazu bietet Ihnen die Konnektorspezifikation [gemSpec_Kon].

Erst wenn eine im VZD geführte Person bzw. Institution KIM-Teilnehmer wird (hier: Krankenhaus beauftragt einen KIM-Anbieter), werden die der Person bzw. Institutionseinheit zuzuordnenden KIM-Adressen vom zugelassenen KIM-Anbieter eingetragen und gepflegt (Kundenauftrag). Die KIM-Adressen entsprechen den bekannten Namens- und Aufbaukonventionen von E-Mail-Adressen. Beachten Sie, dass die im VZD angelegten E-Mail-Adressen eine **KIM-spezifische Namensgebung** aufweisen und sich die KIM-Adressen daher von denen der bisher in Ihrem Krankenhaus genutzten E-Mail-Adressen unterscheiden. **Sie können also keine bereits vorher im Krankenhaus verwendeten E-Mail-Adressen im VZD eintragen lassen**.

Bestellt ein Krankenhaus mehrere SMC-Bs zu einer Telematik-ID (in Abhängigkeit vom gewählten Architekturmodell), werden sämtliche SMC-Bs **unter einem einzigen VZD-Eintrag** geführt. Im **VZD** können **pro Telematik-ID** (bzw. pro SMC-B) **bis zu 100 E-Mail-Adressen** hinterlegt werden. Für **Sie als IT-Dienstleister** eines Krankenhauses ist es **wichtig**, darauf zu achten, **dass zu allen HBAs und SMC-Bs**, die über KIM adressierbar sein sollen bzw. die für die KIM-Adressierung im Krankenhaus verwendet werden sollen, im VZD die für die KIM-Verschlüsselung notwendigen **Zertifikate abgerufen werden können**. Die Hinterlegung dieser Zertifikate erfolgt dabei vom jeweiligen Kartenherausgeber. Die im VZD hinterlegten Zertifikate werden zur Verschlüsselung der Nachrichten durch das KIM-Clientmodul benötigt.

Um eine Unterbrechung des KIM-Verkehrs aufgrund eines Ausfalls einer (singulären) SMC-B zu vermeiden, ist es ratsam, eine **Ersatz-SMC-B** zu bestellen. Bei Auftreten eines Defektes oder bei Verlust der SMC-B wird die Karte gesperrt. Spätestens am nächsten Tag sind somit die mit der SMC-B verbundenen KIM-Adressen aus Sicherheitsgründen nicht mehr erreichbar bzw. adressierbar (der Eintrag selbst bleibt allerdings noch eine Zeitlang erhalten). Sie haben zwar die Möglichkeit, eine weitere SMC-B zur vorhandenen Telematik-ID bei Ihrem Kartenherausgeber nachzubestellen, aber bis Sie diese in Betrieb nehmen können, können unter Umständen mehrere Wochen vergehen. In der Zwischenzeit wären Sie gezwungen, über Ihren KIM-Anbieter die Zieladressen auf eine andere Telematik-ID registrieren zu lassen. Parallel dazu müssten Sie ggf. auch Änderungen in Ihrem Architekturkonzept bzw. an Ihrem Informationsmodell vornehmen.

Mehrere SMC-Bs pro Telematik-ID

Zur Erstellung eines geeigneten Kommunikations-Architekturkonzepts für Ihr Krankenhaus müssen Sie wissen, dass Sie im VZD zu jeder Telematik-ID mehrere KIM-Adressen führen können (bis zu 100 Stück). Weiterhin können Sie zu einer Telematik-ID mehrere SMC-Bs bestellen. Wählt nun der Sender einer KIM-Nachricht eine dieser Telematik-ID zugeordneten KIM-Empfangs-Adresse aus, so erfolgt die Verschlüsselung der Nachricht durch das KIM-Clientmodul anhand **aller** im VZD dieser Telematik-ID zugeordneten (Empfänger-) Zertifikate. Auf der Empfängerseite benötigt das dortige KIM-Clientmodul lediglich einen einzigen passenden Schlüssel, um die Nachricht zu entschlüsseln. Sobald das KIM-Clientmodul über den angebundenen Konnektor eine zu den Empfänger-Zertifikaten passende SMC-B findet, kann es die Nachricht entschlüsseln und dem Zielpostfach zustellen. Es ist also nicht erforderlich, dass das KIM-Clientmodul sämtliche dieser Telematik-ID zugeordneten SMC-Bs erreichen muss.

Werden zu einem HBA im VZD eine oder mehrere KIM-Adressen angelegt, so wird zur sicheren Übermittlung einer Nachricht an diese E-Mail-Adresse das dem HBA zugeordnete Zertifikat zur Verschlüsselung dieser Nachricht verwendet.

Persönliche Postfächer und Funktionspostfächer

KIM bietet die Möglichkeit, sowohl persönliche als auch Funktionspostfächer zu adressieren. In einem Krankenhaus werden **HBA-basierende KIM-Adressen** vermutlich durchgehend als **persönliche Postfächer** geführt, um die Vertraulichkeit

der Daten und die Persönlichkeitsrechte des HBA-Inhabers zu wahren. Ggf. sind dabei Vertretungsregelungen einzurichten, die sich von denen des in Ihrem Krankenhaus bereits etablierten E-Mail-Konzepts nicht grundsätzlich unterscheiden, insbesondere, wenn für die persönliche Kommunikation ein bereits bestehendes Postfach des im Krankenhaus etablierten E-Mail-Systems angesprochen werden soll.

Bei personengebundenen KIM-Adressen (im VZD werden zu einem HBA eine oder mehrere E-Mail-Adressen geführt) ist zu beachten, dass bei Abruf der KIM-Nachrichten durch das Clientsystem des Empfängers der betreffende HBA über den Konnektor erreicht werden muss, der an dem betreffenden KIM-Clientmodul angeschlossen ist, über das der Abruf der Nachrichten vom Clientsystem aus erfolgt. Das ist insbesondere dann der Fall, wenn der Abruf abteilungsunabhängig erfolgen soll.

Wie bereits vorstehend angegeben, kann in der derzeitigen KIM-Version 1.0 ein KIM-Clientmodul nur einen einzigen Konnektor bedienen. Erst **ab** der **KIM-Ausbaustufe 1.5** ist der **Betrieb einer Multikonnektorumgebung** möglich. Des Weiteren wird mit der KIM-Version 1.5 die Parameterübergabe der Konnektor-ID beim Abruf von Nachrichten vom Clientsystem an das KIM-Clientmodul verpflichtend (derzeit fest konfiguriert). Dabei wird beim Abruf des Clientsystems jeweils auch der Konnektor angegeben, über den das Schlüsselmaterial des Benutzers (und sein HBA bzw. die SMC-B) für das KIM-Clientmodul erreichbar ist.

SMC-B-basierende KIM-Adressen werden in einem Krankenhaus voraussichtlich durchweg als **Gruppen- bzw. Funktionspostfächer** oder als Verteilerpostfächer geführt. Technisch kann im VZD eine SMC-B-basierende KIM-Adresse auch als persönliche Adresse angelegt werden. Die Verteilung bzw. Zustellung (z. B. auf ein Gruppenpostfach) liegt dabei im Ermessen des Krankenhauses und richtet sich nach den diesbezüglichen Regelungen und Vorgaben. Es ist daher für Sie wichtig zu wissen, welche Regelungen und Bedingungen in Ihrem Krankenhaus dazu erfüllt werden müssen.

Da in einem Krankenhaus die über KIM adressierbaren Funktionspostfächer bereits oft über das etablierte E-Mail-System eingerichtet sind, können Sie diese Postfächer auch weiterhin als Zieladressen für den KIM-Nachrichtenverkehr verwenden. Wie bereits vorstehend ausgeführt, unterscheiden sich aber die KIM-Adressen von den Adressen des bereits etablierten E-Mail-Systems. Daher müssen Sie, sofern ein bestehendes Postfach vom Benutzer unverändert weiter genutzt werden soll, die eingehenden KIM-Nachrichten auf dieses Postfach mappen. Gleiches gilt für die Zustellung auf ein bereits bestehendes persönliches Postfach.

Achten Sie **beim Mappen der KIM-Adressen** auf Ihre hausinternen (bspw. Outlook-) Adressen darauf, dass bei der Zustellung der KIM-Bezug im Zielpostfach erhalten bleibt. So können Antworten vom Benutzer direkt korrekt adressiert werden. Zudem ist jederzeit Übertragungsmittel (KIM) und Quelle bzw. Ziel der Korrespondenz nachvollziehbar.

Welche Unterstützung KIM-seitig zum Mapping bzw. zur Verwaltung der unterschiedlichen Adressbereiche bestehen, teilt Ihnen Ihr KIM-Anbieter mit.

Dienstkennung und Datenformate

KIM bietet die Möglichkeit, eine E-Mail vor dem Versenden gemäß dem Nachrichteninhalt zu kategorisieren. Dafür wurden für den im Medizinumfeld zu erwartenden Nachrichtenverkehr spezielle Dienstkennungen festgelegt. Über die Auswertung dieser Dienstkennung ist es beim Empfang einer E-Mail möglich, eine automatisierte Weiterverarbeitung der E-Mail bzw. des E-Mail-Anhangs (z. B. elektronischer Arztbrief) durch das Primärsystem oder ein dediziertes Zielsystem durchführen zu lassen. Eine Übersicht aller bisher durch die jeweiligen Akteure festgelegten Dienstkennungen und

deren bereitgestellten Spezifikationen finden Sie im Fachportal (siehe auch blaue Infobox am Ende des Kapitels). Dort finden Sie auch Hinweise auf die verwendeten Datenformate sowie eine Verlinkung auf die jeweilige Webseite der für die Spezifikation verantwortlichen Organisationen.

Zusammenfassung der Funktionen von KIM-Version 1.5

Die gematik veröffentlicht im Laufe des ersten Halbjahres 2021 die Spezifikationen für die KIM-Version 1.5. Wann diese Neuerungen dann auch für Sie im Krankenhaus nutzbar sind, hängt von der Umsetzung des von Ihnen beauftragten KIM-Anbieter ab.

Mit der KIM-Version 1.5 ergeben sich folgende wesentliche Änderungen:

- Ein KIM-Clientmodul kann mehrere Konnektoren bedienen,
- Bei Wechsel eines KIM-Anbieters kann technisch das bisherige KIM-Clientmodul beibehalten werden bzw. KIM-Clientmodul und KIM-Fachdienst können in einem Krankenhaus von unterschiedlichen Herstellern/Anbietern eingesetzt werden. Falls ein Krankenhaus Verträge mit mehreren KIM-Anbietern abgeschlossen hat, können nun mit jedem KIM-Clientmodul alle KIM-Anbieter bedient werden.
- Änderung im Aufrufkontext des Clientsystems, d.h. die Angabe beim Nachrichtenabruf und die korrekte Verarbeitung der Konnektor-ID durch das KIM-Clientmodul wird verpflichtend.
- Die Beschränkung auf 25 MByte große Anhänge wird aufgehoben. Mit der KIM-Version 1.5 können mindestens bis zu 500 MB große Nachrichten versendet werden.

Weiterführende Informationen zu KIM

- Dokument „Spezifikation KOM-LE-Clientmodul“ [gemSpec_CM_KOMLE]
- fachportal.gematik.de/anwendungen/kommunikation-im-medizinwesen
- fachportal.gematik.de/toolkit/dienstkennung-kim-kom-le
- https://www.gematik.de/anwendungen/kim/

2.4.7 E-Rezept

Die Fachanwendung E-Rezept (elektronisches Rezept; Teil der elektronischen Verordnungen, kurz: E-Rezept) ermöglicht die Übermittlung von ärztlichen und zahnärztlichen Verordnungen in elektronischer Form. Perspektivisch soll das E-Rezept alle derzeit auf Papier ausgestellten Verordnungen ablösen. Die Umsetzung erfolgt in einem Stufenkonzept, wobei die erste Stufe ärztliche und zahnärztliche Verordnungen für apothekenpflichtige Arzneimittel umfasst.

Im Krankenhaus betrifft die Einführung des E-Rezepts v. a. das Entlassmanagement (Entlassrezept). Darüber hinaus werden E-Rezepte, die im Krankenhaus erstellt, krankenhausintern verwendet und gemäß § 129a SGB V abgerechnet werden und für die kein Fremdzuweisungsverbot gilt, als E-Rezept verordnet. Dies umfasst auch die ambulante Behandlung von Patienten mit Zytostatika oder parenteralen Zubereitungen.

Die **Erstellung des E-Rezepts erfolgt im Krankenhausinformationssystem** und wird zur späteren Einlösung auf dem E-Rezept-Fachdienst gespeichert. Zur Übermittlung des E-Rezepts in die Apotheke ist auch ein Ausdruck als 2D-Barcode (Datamatrix-Code) inklusive Zusatzinformationen vorzusehen.

Ein Entlassrezept kann vom Patienten in seiner E-Rezept-App verwaltet oder via Papierausdruck in die Apotheke zur Einlösung überbracht werden. Für

patientenindividuelle Rezepte ist vorgesehen, dass diese – wie bisher auch – direkt in der ambulanten Behandlung eingelöst werden. Entsprechende vertragliche Regelungen sind weiterhin mit den Patienten zu vereinbaren.

In noch folgenden Stufen zur Umsetzung des E-Rezeptes werden gemäß DVPMG weitere Rezeptarten umgesetzt:

- Betäubungsmittel-Rezepte und T-Rezepte (T-Rezepte sind Verschreibungen von Arzneimitteln mit besonderen teratogen wirkenden Wirkstoffen)
- Digitale Gesundheitsanwendungen
- Häusliche Krankenpflege und Außerklinische Intensivpflege
- Verordnung von Soziotherapie
- Verordnung Heil- & Hilfsmittel

Eine Übersicht über die Fachwendung E-Rezept gibt die Abbildung 10 auf der nachfolgenden Seite.

Zentraler Baustein der Fachanwendung E-Rezept ist der E-Rezept-Fachdienst. Dieser ist ein zentraler Dienst in der Provider-Zone der TI zur Ausführung der Fachanwendung E-Rezept. Der **E-Rezept-Fachdienst** verwaltet E-Rezepte in der Telematikinfrastruktur als ein zentraler Ressourcenserver auf **Basis des FHIR-Standards** mit einer **RESTful API**. Die Rezepte werden dabei über eine eindeutige Ressourcen-ID (Rezept-ID) adressiert.

Der Fachdienst prüft, ob es sich um ein valides E-Rezept inkl. QES-Signatur handelt. Eine QES-signierte Schadsoftware würde in diesem Fall abgelehnt werden. Zusätzlich protokolliert der E-Rezept-Fachdienst alle Zugriffe auf ein E-Rezept für den Versicherten und verwaltet die Statusübergänge eines E-Rezepts.

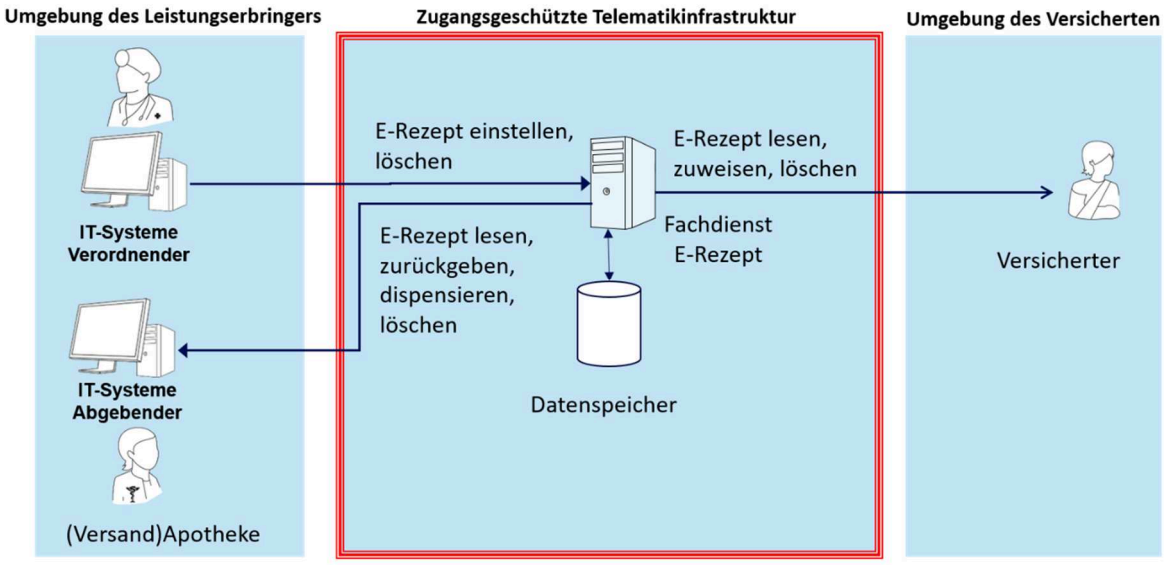

Abbildung 10: Systemkontext E-Rezept-Fachdienst (Quelle: [gemSpec_FD_eRp])

Die Autorisierung für den Zugriff auf die auf dem Fachdienst befindlichen Daten erfolgt auf Basis eines Tokens, das der Identity Provider bereitstellt. Dies geschieht unter Verwendung des OpenID-Standards.

Der E-Rezept-Fachdienst stellt mehrere Schnittstellen bereit:

- im Verordnungsprozess zum Krankenhausinformationssystem,
- für die Dispensierung zum Apothekenverwaltungssystem und

- für die Zuweisung und Verwaltung der E-Rezepte zum E-Rezept-Frontend des Versicherten (E-Rezept-FdV – die E-Rezept-App).

Für den außerklinischen Bereich ist zudem ein Nachrichtenaustausch zwischen Apotheken und Versicherten über die Verfügbarkeit von Medikamenten, die Belieferung von E-Rezepten und die Vertretung beim Einlösen eines E-Rezepts vorgesehen. Die Kommunikation erfolgt ebenfalls über den E-Rezept-Fachdienst.

Damit in der ambulanten Versorgung (z. B. mit Zytostatika) eine Apotheke auf ein E-Rezept zugreifen kann, ist eine Autorisierung mittels des vorgenannten 2D-Barcodes notwendig. Für die Übergabe des 2D-Barcodes können Dienste der TI verwendet werden (KIM, Fachdienst E-Rezept). Ebenso ist es möglich, den 2D-Barcode über KIS-eigene Kommunikationswege zu übergeben.

Weiterführende Informationen zum E-Rezept

- Dokument „Implementierungsfaden Primärsysteme – Elektronisches Rezept" [gemILF_PS_eRp], Systemspezifisches Konzept E-Rezept [gemSysL_eRp] unter
- fachportal.gematik.de/anwendungen/elektronisches-rezept
- https://www.gematik.de/anwendungen/e-rezept/

3 Karten, Konnektoren und Kartenterminals – die dezentralen Komponenten der TI

3.1 Dezentrale Komponenten – Allgemeine Informationen

Unter dem Begriff **dezentrale Komponenten** fallen diejenigen TI-Komponenten, die in den dezentralen Zonen (siehe Kapitel 2.3), also beispielsweise in den Krankenhäusern, aufgestellt und installiert werden. Zu den dezentralen TI-Komponenten zählen Smartcards, stationäre Kartenterminals (eHealth-Kartenterminal, kurz: eH-KT) und mobile Kartenterminals (MobKT) sowie Konnektoren. Diese Komponenten werden von der gematik als Produkte zugelassen. Die Herausgeber personengebundener Smartcards durchlaufen noch zusätzliche Zulassungs- bzw. Bestätigungsverfahren. Der Herausgeber eines HBA muss beispielsweise nachweisen, dass die Personalisierung der Karten, d.h. das Aufbringen der persönlichen Daten des (zukünftigen) Karteninhabers, anforderungsgemäß und sicher erfolgt.

Dezentrale TI-Komponenten werden von verschiedenen Herstellern produziert und vertrieben. In den Krankenhäusern dürfen Sie bei der Einrichtung eines Zuganges zur TI **ausschließlich von der gematik zugelassene Komponenten** verwenden. Eine Übersicht zugelassener Komponenten finden Sie im Fachportal der gematik.

3.2 Smartcards – Allgemeine Informationen

Als **Smartcards** bzw. Chipkarten werden im TI-Kontext Mikroprozessorkarten bezeichnet, die mit einem Betriebssystem – dem sog. Card Operating System (COS) für Dateiverwaltung, Prozesssteuerung, Befehlssatz etc. – laufen.

In der TI werden die folgenden Kartentypen eingesetzt:

- Security Module Card – Typ B (Institutionsausweis) (SMC-B),
- gerätespezifische Security Module Card – Typ Kartenterminal (gSMC-KT), welche durch den KT-Hersteller angeboten bzw. mitgeliefert wird,
- gerätespezifische Security Module Card – Typ Konnektor (gSMC-K), welche in den Geräten fest verbaut ist,
- elektronischer Heilberufsausweis (HBA) und
- elektronische Gesundheitskarte (eGK).

Gebunden sind diese Smartcards entweder an Personen – wie eGK und HBA –, an Leistungserbringerinstitutionen – wie die SMC-B (Institutionskarte) – oder an Geräte – wie gSMC-K und gSMC-KT. Allen ist gemein, dass sie den sicheren Datenaustausch durch Authentifizierung und Verschlüsselung gewährleisten. Hierbei authentisieren sich die Chipkarten der TI gegenseitig, wobei eine Chipkarte ihre Echtheit gegenüber einer anderen Chipkarte offline mittels einer Card-to-Card-Authentisierung nachweist.

Die personengebundenen Karten werden von unterschiedlichen Kartenherausgebern ausgegeben:

- Die eGK wird durch die Krankenkassen an ihre Versicherten herausgegeben.
- Der HBA (personengebunden) wird durch die Ärztekammern an Ärzte ausgegeben.
- Die SMC-B für Krankenhäuser wird durch die DKTIG (Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH) ausgegeben.

Smartcards werden nicht nur offline, sondern auch online auf ihre Gültigkeit geprüft. Dabei kann sich herausstellen, dass sie ungültig sind. Gründe für eine Ungültigkeit können sein:

- ein Ablauf der Gültigkeit der Zertifikate,
- eine Sperrung der Zertifikate sowie
- eine veraltete Kartengeneration.

Grundsätzlich haben alle **Smartcards** eine **maximale Laufzeit von fünf Jahren** (bzw. die auf der Karte aufgebrachten Zertifikate). Aufgrund ihrer begrenzten Lebensdauer und der zeitlich begrenzten Gültigkeit kryptographischer Schlüssel und Verfahren müssen Smartcards (bzw. deren Schlüssel und Zertifikate) nach spätestens fünf Jahren erneuert bzw. „getauscht" werden.

Zusätzlich zu den vorstehenden Smartcards gibt es noch die Prüfkarte eGK (s. Kapitel 3.2.6.1), die von der gematik herausgegeben wird. Sie ermöglicht es, die erfolgreiche Installation dezentraler TI-Komponenten im Krankenhausumfeld mittels Durchführung spezifischer Anwendungsfälle zu prüfen.

Weiterführende Informationen zum Thema Smartcards der TI

- fachportal.gematik.de/karten-und-identitaeten

3.2.1 Betrieb der Smartcards

Im Außenverhältnis legitimiert das Organisationszertifikat des Krankenhauses in der SMC-B die Zugriffe aus dem Krankenhaus in die TI. Im Innenverhältnis regelt das Krankenhaus über sein internes Identitäts- und Berechtigungsmanagement den Kreis der Zugriffsberechtigten und die gesetzeskonforme Umsetzung des Zugriffsrechts. Ein HBA ist dann erforderlich, wenn er für signaturgesetz-konforme Prozesse benötigt wird, also für Erklärungen nach außen, z. B. das Signieren eines Arztbriefes.

In der Regel sind Smartcards wartungsfrei. Eine Passwortverwaltung für die PINs der in einem Krankenhaus eingesetzten Karten unterstützt ihre reibungslose Verwendung, auch durch wechselnde Administratoren. Durch Ausfall eines Konnektors kann eine SMC-B betroffen sein (Stichwort: Verbindungsverlust des Konnektors zur SMC-B). In diesem Falle muss die vom Verbindungsverlust betroffene SMC-B neu verifiziert werden. In der Regel wird der Verifizierungsprozess über das KIS von Benutzern einer entsprechenden Berechtigungsebene angestoßen.

Für die Remote-Verifizierung einer SMC-B ist eine Einrichtung von Remote-PIN-Arbeitsplätzen im Konnektor erforderlich. Damit es nicht zu Störungen im Regelbetrieb kommt, sollten Sie nach einer PIN-Freischaltung (Remote PIN) ein geeignetes Monitoring aufsetzen, so dass der Freischaltungsstatus der gesteckten SMC-B überwacht und Störungen erkannt und an die Administratoren eskaliert werden können. Sie können auch ein Supportteam (Help Desk) definieren, das über die Remote-PIN und die entsprechenden Berechtigungen verfügt, um 24/7 auf Ausfälle reagieren zu können.

Informationen über ein bevorstehendes Gültigkeitsende von Smartcards erhalten Sie über den Karteninhaber bzw. vom Kartenantragsteller, der eine entsprechende Abfrage auf dem Antragsportal des Kartenherausgebers durchführen kann. Sie können aber auch mit dem KIS die Gültigkeitsdauer über den Konnektor erfragen (nur für SMC-B und HBA, die Abfragemöglichkeit der Gültigkeit der SMC-KT ist derzeit nur optional). Auf dem mobilen Kartenterminal (MobKT) können Sie Informationen zu einem unmittelbar bevorstehenden Ablaufdatum nur von lokal gesteckten SMC-Bs und HBAs auf der Nutzeroberfläche abfragen. Eine Übertragung der Ablaufinformationen vom MobKT an das KIS ist nicht vorgesehen.

Tabelle 1: Übersicht Smartcards in Krankenhäusern

Aktivitäten	SMC-B[13]	gSMC-KT	HBA[14]
Beschaffung	Antrag beim Karten-herausgeber für Krankenhäuser (DKTIG)	Beschaffung beim Hersteller des Kartenterminals	Antrag des Arztes/ Zahnarztes beim Kartenherausgeber (sektorspezifisch)
Inbetrieb-nahme-verfahren	Alternativen: a) einmaliges Umwandeln der zugesandten Transport-PIN in eine selbst gewählte PIN b) Nutzung der zugesandten Echt-PIN	Pairing: einmaliges Herstellen eines gemeinsamen Sicherheitskontextes zwischen dem Konnektor und dem stationären Kartenterminal (siehe Kapitel 3.3.1)	Alternativen: a) einmaliges Umwandeln der zugesandten TransportPIN in eine selbst gewählte PIN b) Nutzung der zugesandten Echt-PIN
Szenarien stationäre PIN-Eingabe	Jedes Mal, wenn die SMC-B benötigt wird und zuvor noch keine PIN-Eingabe erfolgte: a) nach dem Hochfahren des Konnektors, b) nach dem Stecken einer SMC-B und c) nach dem Verbindungsverlust zum eH-KT, in dem die SMC-B steckt.	keine PIN spezifiziert	QES: vor jeder Signatur nonQES, Entschlüsselung, C2C, Authentisierung: Jedes Mal, wenn der HBA benötigt wird und zuvor noch keine PIN-Eingabe erfolgte: a) nach dem Hochfahren des Konnektors, b) nach dem Stecken eines HBA und c) nach Verbindungs-verlust zu dem eH-KT, in dem der HBA steckt
Mobile PIN-Eingabe	C2C: PIN-Eingabe zur Freischaltung	Keine gerätegebundene Karte vorhanden	C2C: PIN-Eingabe zur Freischaltung
Sperrung	Nach Vorgabe Herausgeber	Keine Sperrung möglich	Nach Vorgabe Herausgeber
Lebenszyklus	Zertifikate begrenzt gültig (max.5 Jahre), danach Neubeschaffung erforderlich	Zertifikate begrenzt gültig (max.5 Jahre), danach Neubeschaffung erforderlich	Zertifikate begrenzt gültig (max.5 Jahre), danach Neubeschaffung erforderlich

3.2.2 Security Module Card – Typ B (SMC-B) (Institutionskarte)

Eine Security Module Card – Typ B (**SMC-B**) für Krankenhäuser wird durch die DKTIG (Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH) herausgegeben. Sie dient als Institutionsausweis und ermöglicht den Zugriff einer berechtigten Institution, Einrichtung oder Organisation des Gesundheitswesens (hier: Krankenhaus, Fachabteilung oder Bereich eines Krankenhauses) auf die TI. Ohne eine in einem stationären Kartenterminal gesteckten und freigeschalteten SMC-B baut der Konnektor keine Verbindung zur TI auf. Gleiches gilt für die Ersteinrichtung eines

[13] Ein HSM-B verhält sich analog zur SMC-B. SMC-Bs, die nicht dem Krankenhaus zugeordnet sind, aber ggf. in einem Krankenhaus eingesetzt oder von der Krankenhaus-IT verwaltet werden (Herausgabe der SMC-Bs erfolgt in diesem Fall nicht durch die DKTIG), werden hier nicht betrachtet.

[14] HBA-Vorläuferkarten werden an dieser Stelle nicht beachtet, weil sie außerhalb der TI beschafft werden.

Konnektors und bei der erstmaligen Registrierung beim VPN-Zugangsdienst (s. auch Kapitel 4.2.3.1).

Eine SMC-B wird zwar – wie der HBA und die eGK (siehe Kapitel 3.2.5 und 3.2.6) – im Scheckkartenformat (Format ID-1) ausgegeben, jedoch weist sie um ihren Chip herum einen vorgestanzten Bereich auf. Dieser entspricht der Größe einer SIM-Karte für Mobiltelefone (Format ID-000). Je nach Größe des Kartenslots des eHealth-Kartenterminals (eH-KT, siehe Kapitel 3.3.1) kann die SMC-B in „voller Größe" (Format ID-1) eingesetzt oder muss aus dem vorgestanzten Bereich herausgebrochen werden. Im Gegensatz zur gSMC-KT wird die SMC-B nicht mit einem Slotsiegel (gSMC-KT und Slotsiegel siehe Kapitel 3.2.3) geschützt.

Auf der SMC-B eines Krankenhauses sind u. a. folgende Daten gespeichert:

- Integrated Circuit Card Serial Number (kurz: ICCSN, eindeutige/weltweit einmalige Kennnummer),
- Art der Institution (hier: Krankenhaus),
- Name der Institution,
- Telematik-ID.

Die Telematik-ID auf der SMC-B identifiziert die einzelne Institution oder Einrichtung des Gesundheitswesens und wird sektorspezifisch (hier über die DKTIG) vergeben. Ein Krankenhaus kann, je nach organisatorischer oder technischer Struktur bzw. Zielsetzung, mehrere SMC-Bs mit identischer Telematik-ID und/oder auch SMC-Bs mit unterschiedlichen Telematik-IDs beantragen.

Bitte informieren Sie sich rechtzeitig vor Inbetriebnahme bzw. Anbindung Ihres Krankenhauses an die TI bei Ihren zuständigen internen Stellen, ob eine (oder mehrere) SMC-Bs bei der DKTIG beantragt wurde/n bzw. wer die Beantragung vornehmen wird. **Beachten Sie, dass Sie zum Anschlusstermin an die TI mindestens eine von Ihrem VPN-Zugangsdienst-Anbieter freigeschaltete SMC-B benötigen.**

3.2.2.1 Austausch SMC-B wegen abgelaufenem Zertifikat

Die SMC-B-Zertifikate haben eine Gültigkeit von 5 Jahren. Wenn Sie sie austauschen müssen, bekommen sie eine neue SMC-B mit gleicher Telematik-ID und neuen Zertifikaten.

Achten Sie darauf, dass Sie die neue Karte bereits nutzen bevor die alte abgelaufen ist um eine unterbrechungsfreien Betrieb zu gewährleisten.

3.2.2.2 Sollten KIM-Nachrichten existieren, die mit einer mittlerweile abgelaufenen SMC-B verschlüsselt wurden, können diese weiterhin mit der alten Karte entschlüsselt werden (Der Konnektor prüft beim Entschlüsseln nicht das Zertifikat).Geltungsbereich für SMC-Bs vom Typ ‚Krankenhaus'

Die SMC-B eines Krankenhauses repräsentiert gegenüber der TI die elektronische Identität einer Organisation, Einrichtung oder Institution vom Typ ‚Krankenhaus'. Genaueres entnehmen Sie bitte den Internetseiten der DKTIG unter https://dktig.de/smc-b/ueberblick/. Wenden Sie sich bei Bedarf an die dort angegebenen Anlaufstellen bzw. Ansprechpartner.

Nicht der Institution „Krankenhaus" zuzuordnende Bereiche eines Krankenhauses, beispielsweise persönlich ermächtigte Ärzte (vgl. § 116 SGB V) bzw. allgemein „Vertragsärzte", benötigen keine eigene institutionelle Identität (SMC-B), sofern eine datenschutzwirksame Trennung (durch das gemeinsam genutzte KIS) von

Zugriffsberechtigten und Nicht-Zugriffsberechtigten auf die persönlichen Daten eines Versicherten realisiert wird (siehe dazu auch die TI-Hinweise der DKG, Kapitel 3.4: https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.5._Telematik-Infrastruktur/2.1.5.3_TI-Hinweise/TI-Hinweise_3_2_.pdf).

Ein KIS, das von Vertragsärzten und der Organisation ‚Krankenhaus' gemeinsam genutzt wird, ist in vielen Krankenhäusern der Regelfall. Es obliegt dem Krankenhaus – natürlich im Konsens mit seinen Vertragsärzten –, wie viele SMC-B-Karten eingesetzt werden, damit Anforderungen an Datenschutz und Wirtschaftlichkeit gleichsam erfüllt werden können.

Im Folgenden werden verschiedene Modelle aufgezeigt, die dabei helfen können, eine geeignete SMC-B-Struktur in einem Krankenhaus aufzubauen. Die Einbindung von SMC-Bs, welche nicht dem Typ Krankenhaus entsprechen, werden in diesem Dokument nicht weiter erörtert.

3.2.2.3 Anwendungsgetriebenes Modell

Beim anwendungsgetriebenen Modell wird eine SMC-B einer bestimmten Anwendung wie ePA und KIM zugewiesen (siehe Abbildung 11, linke Seite). Dieses Modell kann in spezialisierten Organisationseinheiten eines Krankenhauses angewandt werden, beispielsweise in einer zentralen Aufnahme, bei der die Einwilligung auf die ePA vom Versicherten abgefragt wird. In diesem Falle kann eine Autorisierung der behandelnden Ärzte des Krankenhauses auf die ePA-Daten des Versicherten stattfinden, ohne dass diese Autorisierung in den jeweiligen Fachabteilungen (erneut) durchgeführt werden muss. Ein weiterer Anwendungsfall kann durch eine zentrale Poststelle für die Anwendung KIM bestehen. Voraussetzung ist dabei; dass die SMC-Bs eine identische Telematik-ID aufweisen, d.h. die gleiche Institution abbilden.

3.2.2.4 Fachabteilungs-(Institutions-)getriebenes Modell

Die Aufteilung von SMC-Bs nach Abteilungen bietet sich an, wenn jede Fachabteilung anwendungsübergreifend mit eigenen SMC-Bs ausgestattet werden soll (siehe Abbildung 11, rechte Seite). Hierbei ist zu erwähnen, dass beispielsweise bei einem ePA-Zugriff die Autorisierung in jeder Fachabteilung separat stattfinden muss, selbst dann, wenn es sich um den gleichen Patienten handelt. Allerdings können hier dann die Autorisierungen anwendungsübergreifend verwendet werden.

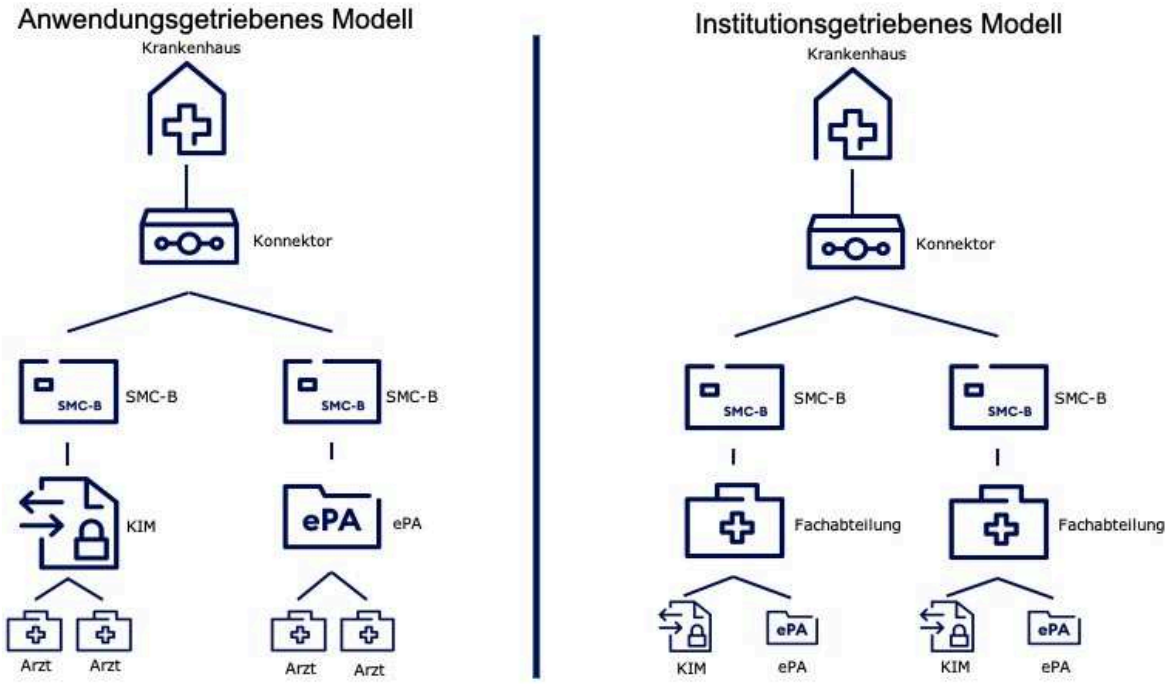

Abbildung 11: Das anwendungsgetriebene- und fachabteilungsgetriebene SMC-B Modell im Krankenhaus.

3.2.2.5 Institutionsmodell „1:n"

Wie vorstehend bereits beschrieben kann in einem Krankenhaus mit mehreren SMC-Bs mit einheitlicher Telematik-ID der Freigabe-Prozess für den Zugriff auf die ePA eines Patienten initial bei der Aufnahme erfolgen. Jeder weitere Zugriff aus den Fachabteilungen des Krankenhauses erfolgt dann mittels dieser Telematik-ID.

3.2.2.6 Institutionsmodell „n:n"

Eine weitere Möglichkeit stellt das Institutionsmodell „n:n" dar. Hierbei werden SMC-Bs unterschiedlicher Telematik-IDs benutzt, wobei SMC-B mit einer identischen Telematik-ID nur von einer oder speziellen Fachabteilungen eingesetzt werden.

Diese Modellform eignet sich für Einrichtungen mit mehreren Fachabteilungen, die separate Berechtigungen erhalten sollen. Jede Fachabteilung kann mit bestimmten Daten arbeiten. Für diese Art von Institutionsarchitektur sind verschiedene Freigabe-Iterationen notwendig (z. B. bei der Übergabe eines Patienten an andere Fachabteilungen).

3.2.3 Gerätespezifische Security Module Card – Typ Kartenterminal (gSMC-KT)

Eine **gerätespezifische Security Module Card – Typ Kartenterminal** (**gSMC-KT**) ist eine Chipkarte, über die die Authentisierung eines stationären Kartenterminals gegenüber einem Konnektor erfolgt. Diese Karte wird mit dem Kartenterminal geliefert. Eine gSMC-KT hat das Format einer SIM-Karte für Mobiltelefone (Format ID-000). Ggf. müssen Sie sie aus einer größeren Karte (Scheckkartenformat) aus einem vorgestanzten Bereich um den Chip herum herausbrechen.

Die gSMC-KT muss nach Einstecken in den Slot des Kartenterminals durch ein Slotsiegel geschützt werden. Dieses Slotsiegel ist im Lieferumfang enthalten. Der Administrator

bringt es im Beisein des Leistungserbringers an. Ggf. muss ein Leistungserbringer dieses Slotsiegel vom Leistungserbringer unterschreiben.

3.2.4 Gerätespezifische Security Module Card – Typ Konnektor (gSMC-K)

Eine **gerätespezifische Security Module Card – Typ Konnektor** (**gSMC-K**) dient als Sicherheitsmodul und authentisiert den Konnektor gegenüber dem VPN-Zugangsdienst (siehe Kapitel 4.2.3.1) sowie den anderen TI-Komponenten, z. B. einem HBA. Im Gegensatz zu den anderen Chipkarten ist die gSMC-K fest durch den Hersteller verbaut und somit für den Nutzer nicht am Gerät sichtbar und auch nicht austauschbar.

3.2.5 Heilberufsausweis (HBA)

Der elektronische **Heilberufsausweis** (**eHBA** oder kurz: **HBA**) wird von der zuständigen Berufskammer eines Leistungserbringers herausgegeben. Wie die Bezeichnung bereits andeutet, wird der HBA einerseits als Sichtausweis für Leistungserbringer benutzt, andererseits können sich Leistungserbringer mit dem HBA auch digital ausweisen. Ferner können Leistungserbringer mit dem HBA Daten verschlüsseln und per QES signieren. Der HBA ermöglicht zudem den Zugriff auf Daten, die auf der eGK gespeichert sind.

Abbildung 12: Muster eines HBA (Quelle: Bundesärztekammer)

3.2.6 Elektronische Gesundheitskarte (eGK)

Seit dem 1. Januar 2015 gilt ausschließlich die **elektronische Gesundheitskarte** (**eGK**) als Berechtigungsnachweis eines Patienten, medizinische Leistungen einer gesetzlichen Krankenversicherung in Anspruch nehmen zu können. Eine eGK ist zwar im Besitz eines Versicherten, verbleibt jedoch im Eigentum der ausstellenden Krankenkasse.

Auf der eGK sind persönliche Daten des Versicherten bzw. Angaben zu seiner Mitgliedschaft in der Krankenversicherung gemäß § 291a Absatz 2 und 3 SGB V digital gespeichert oder aufgedruckt (siehe Abbildung 12, wobei die Abbildung der Europäischen Krankenversicherungskarte auf der Rückseite der eGK optional ist).

Die eGK:

- ermöglicht u.a. die Authentisierung des Versicherten bzw. Authentifizierungsprozesse in der TI,
- enthält in seinem Speicherbereich Fachdaten, etwa die VSD, an denen auch der Versicherungsstatus ermittelt werden kann und
- bietet einen sehr hohen Schutz für kryptographische Identitäten und Fachdaten, indem sie selbstständig prüft, ob der Zugriff auf diese Informationen gestattet werden darf.

Abbildung 13: Muster für die eGK (Quelle: gematik)

Als Administrator werden Sie unter Umständen bei einem fehlerhaften eGK-Lesevorgang von einem Arzt oder anderen Mitarbeitern konsultiert. In diesem Fall prüfen Sie zunächst die TI-Funktionalität in Ihrem Krankenhaus. Wenn Sie ausschließen können, dass es sich um ein generelles TI-Problem, ein technisches Problem der dezentralen Komponenten oder des Primärsystems handelt, muss sich der Karteninhaber an seine Krankenkasse wenden (siehe dazu auch Kapitel 4.5.5 und 4.5.6).

3.2.6.1 Prüfkarte eGK

Die Prüfkarte eGK dient IT-Dienstleistern als Hilfsmittel zum Nachweis einer erfolgreichen Anbindung einer Einrichtung an die TI. Mit dieser Karte können Sie zum einen überprüfen, ob die Online-Anbindung an die TI korrekt konfiguriert ist und zum anderen, ob alle dezentralen Komponenten sowie das KIS korrekt auf die eGK zugreifen können. Darüber hinaus können Sie mit der Prüfkarte eGK kontrollieren, ob die Installation von KIS, eHealth-Kartenterminals und Konnektor in Bezug auf die Fachanwendung VSDM und die Konfiguration der dezentralen Komponenten erfolgreich war (siehe auch Kapitel 4.2.4 und 4.2.6).

Im Gegensatz zu den zuvor genannten Smartcards wird die Prüfkarte eGK nicht im regulären Versorgungsalltag von Leistungserbringern oder Versicherten genutzt bzw. kann dazu nicht genutzt werden. Wie Abbildung 14 zeigt, lässt sich die Prüfkarte eGK leicht von einer „echten" eGK unterscheiden. Eine Verwechselung mit der eGK eines Versicherten ist somit ebenso ausgeschlossen wie ein missbräuchlicher Einsatz im regulären Versorgungsalltag.

Abbildung 14: Muster für die eGK-Prüfkarte[15]

[15] Die Rückseite der Prüfkarte eGK ist weiß.

Die eGK-Prüfkarte kann auf der Internetpräsenz der gematik kostenpflichtig erworben werden (siehe fachportal.gematik.de/toolkit/pruefkarte-egk-fuer-dvo). Sie ist keine Voraussetzung zur erfolgreichen Anbindung an die TI.

3.3 Kartenterminals – Allgemeine Informationen

Im Rahmen der TI werden zwei Arten von Kartenterminals (auch Kartenlesegeräte) unterschieden: **stationäre** (**eHealth-**) und **mobile Kartenterminals**. Mithilfe der Kartenterminals können u. a. Daten auf einer eGK gelesen werden.

3.3.1 Stationäre Kartenterminals

Aktuell gibt es zwei Arten stationärer Kartenterminals – die älteren BCS-Kartenterminals und die neueren eHealth-Kartenterminals. Beide Arten kommen nur in den Räumlichkeiten von Leistungserbringern zum Einsatz.

eHealth-Kartenterminals (eH-KT)

Im Gegensatz zu den BCS-Kartenterminals werden die eHealth-Kartenterminals (**eH-KT**) nicht lokal über einen direkten PC-Anschluss betrieben. eH-KTs werden vom Konnektor erkannt und können somit via LAN-Verbindung gesteuert werden. Zu diesem Zweck muss ein eH-KT mit einem Konnektor bekannt gemacht („**gepairt**") werden. Grundsätzlich können mehrere eH-KTs innerhalb einer Leistungserbringerinstitution mit einem Konnektor gepairt werden. Hierzu müssen diese Kartenlesegeräte im sog. „Infomodell" des Konnektors administriert werden.[16]

eH-KTs funktionieren nur bei gesteckter und mit dem Konnektor gepairter gSMC-KT. Um die hohen Sicherheitsbestimmungen einzuhalten, müssen sich diese Kartenterminals bei jedem Verbindungsaufbau des Konnektors mit Hilfe der gSMC-KT gegenüber dem Konnektor selbst authentisieren. Zeitgleich müssen diese Kartenlesegeräte das zuvor erfolgte Pairing nachweisen.

Vor einer Installation müssen Sie mindestens die folgenden Sicherheitsmerkmale eines eH-KTs überprüfen:

- Unversehrtheit des Gerätes
- Unversehrtheit der Gehäusesiegel
- Unversehrtheit des Slotsiegels, falls die gSMC-KT bereits gesteckt ist
- Korrektheit der Geräteversion (Hardware- und Softwareversion, angezeigt in der Selbstauskunft des Gerätes)
- Sicherheitshinweise des Herstellers im (Administrator-)Handbuch des Geräts

Der Zugriff auf die medizinischen Gesundheitsdaten wird im Rahmen der TI über das „Zwei-Schlüssel-Prinzip" geregelt: Ein Zugriff auf diese geschützten Daten kann nur dann erfolgen, wenn sich sowohl der Leistungserbringer (mittels HBA oder SMC-B als Schlüssel 1) als auch der Versicherte (mittels eGK als Schlüssel 2) authentisieren. Für den Zugriff auf geschützte Daten der eGK kann zusätzlich die Eingabe der PIN in einem Kartenlesegerät durch den Versicherten erforderlich sein.

Bitte beachten Sie grundsätzlich auch die herstellerspezifischen Angaben in den jeweiligen (Administrator-)Handbüchern.

[16] In diesem Fall ist es egal, in welchem eHealth-Kartenterminal die SMC-B steckt, d. h, dass eine eGK in einem Kartenterminal und die SMC-B in einem anderen Kartenterminal stecken kann.

BCS-Kartenterminals

Während Ihrer Anschlussarbeiten können Sie in einem Krankenhaus noch auf ein älteres BCS-Kartenterminal stoßen. Diese Terminals wurden im Rahmen des sog. Basis-Rollouts der TI verwendet. Sie verfügen über einen USB-Anschluss und werden via KIS gesteuert. BCS-Kartenterminals können nicht mit dem Konnektor verbunden werden. Somit können Sie in der TI nicht (mehr) genutzt werden.

Unter Umständen werden Sie gebeten, das Modell zu entsorgen.[17] Wenn dies der Fall ist, setzen Sie bitte das Kartenlesegerät auf die Werkseinstellungen zurück.

3.3.2 Mobiles Kartenterminal (mobKT)

Ein **mobiles Kartenterminal** (**mobKT**) ist für ein mobiles Einsatzszenario geschaffen und kommt – wie die Bezeichnung bereits andeutet – mobil bzw. außerhalb der stationären Einrichtung zum Einsatz. Ein mobKT erlaubt es, Versichertendaten von der eGK auszulesen. Abrechnungsdaten werden verschlüsselt im mobKT zwischengespeichert.

mobKT sind nicht online in die TI eingebunden. Sie können – im Gegensatz zu stationären eHealth-Kartenterminals – nicht mit einem Konnektor kommunizieren und haben keine gSMC-KT.

Die Übertragung der zwischengespeicherten Daten an das KIS erfolgt über die Host-Schnittstelle, die das CT-API-Protokoll zur Übertragung nutzt. Vor der Übertragung muss erneut entweder der Heilberufsweis oder die Institutionskartemittels PIN-Eingabe freigeschaltete werden. Erst dann ist Entschlüsselung der zwischengespeicherten Daten möglich.

3.4 Konnektor – Allgemeine Informationen

Ein **Konnektor** verbindet die IT-Systeme der Krankenhäuser über ein Transportnetz (typischerweise das Internet via sicherer VPN-Verbindung) mit der TI. Ein Konnektor wird von der gematik zugelassen, so dass in einem Krankenhaus nur zugelassene Konnektoren zum Einsatz kommen dürfen. Der Zugang zur TI (über das Internet) muss weiterhin über einen ebenfalls von der gematik zugelassenen VPN-Zugangsdienst-Anbieter[18] erfolgen (zugelassene Komponenten und Dienste sowie Anbieter finden). Die in einem Krankenhaus eingesetzten Konnektoren müssen zuvor bei diesem registriert und freigeschaltet werden (siehe Kapitel 4.2.3.1).

Manche VPN-Zugangsdienst-Anbieter bieten im Bundle die Nutzung (und Administration) einer unterschiedlichen Anzahl von Konnektoren an, so dass Sie diese nicht selbst beschaffen oder (vollständig) administrieren müssen, da dies bereits im Leistungsumfang des Anbieters enthalten ist.

Darüber hinaus ermöglicht der Konnektor dem KIS über die netzwerkfähigen stationären eHealth-Kartenterminals (eH-KT) den sicheren Zugriff auf die Smartcards der TI (HBA, SMC-B, eGK) im lokalen Netzwerk (LAN) des Krankenhauses.

Als Schnittstelle stellt der Konnektor technologisch einen eigenen Gerätetyp dar, in dem die eigens entworfene Firmware/Software alle sicherheitsrelevanten Funktionen vereinigt. So verfügt der Konnektor bspw. über die Sicherheitsfunktionalität einer

[17] Bitte beachten Sie, dass eine Entsorgung nicht immer notwendig ist. Denkbar wäre bspw. die weitere Verwendung außerhalb der TI (z. B. als Signaturterminal).

[18] Über die aktuell zugelassenen Komponenten informiert Sie das Fachportal der gematik unter https://fachportal.gematik.de/zulassungs-bestaetigungsuebersichten

Firewall und eines VPN-Clients. So kann der Konnektor das LAN des Krankenhauses und die dort installierten Clientsysteme vor Angriffen aus der TI schützen (bei serieller Anbindung, siehe Kapitel 4.2.2.1) – und umgekehrt, die TI vor Angriffen aus dem LAN.

Der Konnektor ist – nicht zuletzt aufgrund seiner komplexen Funktionalität – die dezentrale Komponente mit dem höchsten Konfigurationsaufwand und dem höchsten Rechenaufwand. Beachten Sie, dass ein Konnektor nur eine begrenzte Kapazität zur performanten Bearbeitung für Ver- und Entschlüsselung aufweist (vor allem bei Einsatz KIM) und daher nur bis zu einer gewissen Größenordnung belastet werden sollte. In der Regel gibt der Hersteller dazu eine produktspezifische Faustformel an. Folgen Sie bitte diesen diesbezüglichen Hinweisen und Vorgaben des Herstellers. Beachten Sie weiterhin die spezifischen Installations- und Konfigurationsvorgaben des (Betriebs-, Administrations-) Handbuches des jeweiligen Herstellers.

3.4.1 Hinweise zu Installationsvorkehrungen

Ein Konnektor darf in einem Krankenhaus nur innerhalb eines zugriffsgeschützten bzw. zugriffsbeschränkten Bereichs aufgestellt werden (abschließbarer Schrank, Technik- oder Serverraum, Rechenzentrum). Dieser Bereich muss den Schutz des Geräts gegen physische Angriffe sicherstellen und einen unbefugten Zugriff verhindern. Es dürfen weiterhin nur autorisierte Personen Zutritt zu dem Konnektor erhalten. Befolgen Sie bei der Wahl eines geeigneten zutrittsgeschützten Bereiches auch die herstellerspezifischen Hinweise.

Je nach Hersteller weist ein Konnektor eigene Mechanismen auf, um Manipulationen und Angriffe zu erschweren oder sofort zu erkennen, darunter bspw. diverse Versiegelungen. Ferner führt er Selbsttests zur Überprüfung seiner Integrität durch. Daneben kann ein Konnektor bestimmte Arten von Manipulationsversuchen selbstständig erkennen und diese per Meldung auf der Managementoberfläche, über das Clientsystem und (falls vorhanden) auf dem lokalen Display anzeigen.

Vor einer Installation müssen Sie mindestens folgende Sicherheitsmerkmale prüfen:

- Ist das Verpackungssiegel auf der Transportverpackung intakt?
- Sind alle weiteren Bestandteile des Lieferumfangs intakt?
- Sind die Einwegschrauben am Gehäuse des Konnektors intakt?
- Sind die Sicherheitssiegel an den Gehäuseseiten intakt?
- Ist das Typenschild intakt?[19]

Sobald eines dieser Sicherheitsmerkmale nicht zutrifft bzw. Sie eine Manipulation des Gerätes erkennen, brechen Sie die Installation/Inbetriebnahme ab bzw. deinstallieren einen bereits angeschlossenen Konnektor (siehe auch Kapitel 4.5.3).

[19] Beachten Sie, dass Art und Umfang der Gehäuseversiegelung herstellerspezifisch sind.

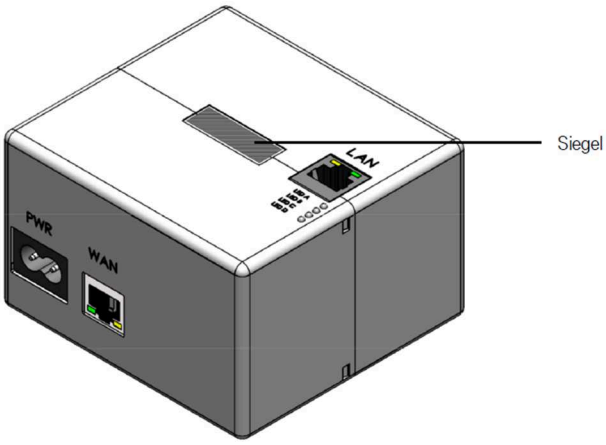

Abbildung 15: Beispielhafte Siegelplatzierung auf einem Konnektor

3.4.2 Betriebshinweise

Bei einer **planmäßigen Außerbetriebnahme** eines Konnektors (z. B. bei einer Fehlfunktion oder einem Modellwechsel) de-registrieren Sie das Gerät gemäß Herstellervorgaben. Anschließend führen Sie einen RESET am Gerät durch und informieren den VPN-Zugangsdienst-Anbieter.

Einen de-registrierten und zurückgesetzten Konnektor müssen Sie gemäß Sicherheitsvorgaben entsorgen. Informieren Sie sich zu diesem Zweck beim jeweiligen Supportanbieter und beachten Sie die Vorgaben des Herstellers.

Bei der Behebung von Störungen gelten die vertraglich zwischen Ihnen und dem Konnektorhersteller, einem IT-Dienstleistungsunternehmen oder dem VPN-Zugangsdienst-Anbieter vereinbarten vertraglichen Konditionen. Falls kein Betreuungsvertrag mit einem Dienstleister besteht, der im Falle eines Ausfalles zeitnah einen Ersatzkonnektor zur Verfügung stellt, ist es ratsam, dass Sie einen Ersatzkonnektor vorhalten, um längere Ausfallzeiten zu vermeiden.

3.4.3 Highspeed-Konnektor (HSK)

Die Dokumentation zum HSK finden Sie auf dem Webportal der gematik.

Für Krankenhäuser stellt sich die Frage ob der Einsatz eines eigenen HSK lohnenswert ist.

Im Folgenden sehen Sie ein Ablaufdiagramm sowie erklärenden Text zum Thema.

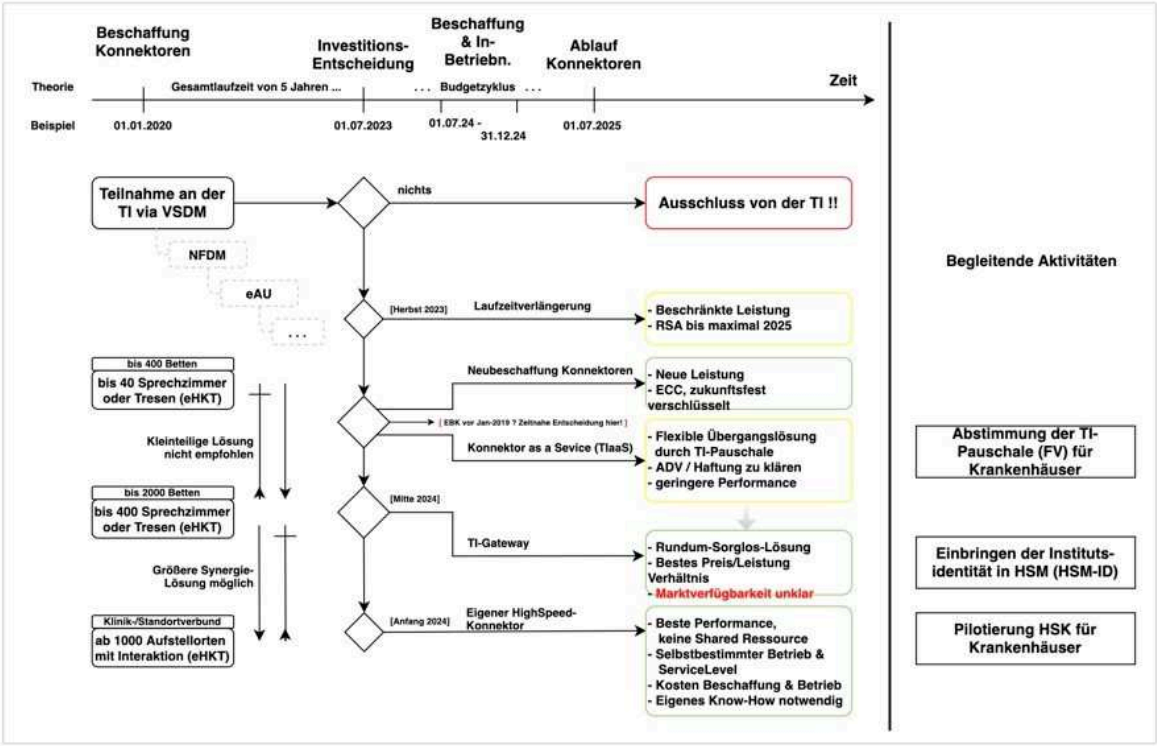

Abbildung 16: Ablaufdiagramm

Begleittext zum Ablaufdiagramm:

Mitte dieses Jahrs erreichen die ersten festverbauten Konnektorzertifakte (gSMC-K) ihr Laufzeitende. Diese gSCM-K haben eine Laufzeit von 5 Jahren und daher werden entsprechend ihres Produktionszeitpunktes potenzielle ab Mitte 2023 Ersatzlösungen benötigt. Nach Ablauf der gSMC-K funktionieren die Konnektoren augenblicklich nicht mehr! Leistungserbringer bzw. deren Administratoren müssen also rechtzeitig Maßnahmen zum Weiterbetrieb der TI-Dienste ergreifen. Dazu haben sie folgende Möglichkeiten:

1. Laufzeitverlängerung der gSMC-K im vorhandenen Konnektor: Diese Laufzeitverlängerung ist, Stand Januar 2023, technisch noch nicht möglich, wird aber ab Herbst 2023 verfügbar sein. Die genaue Verfügbarkeit muss direkt bei dem entsprechenden Konnektorhersteller erfragt werden.

   Einschränkung: *Konnektoren, die noch auf RSA-Basis verschlüsseln (Baujahr vor 2020), können nur bis maximal 2025 verlängert werden, da die Nutzung von RSA nur bis zu diesem Zeitpunkt zulässig ist. Konnektoren die bereits mit ECC-Verschlüsselung arbeiten (Baujahr 2020 und später) können voraussichtlich ab Heribst 2023 um weitere 5 Jahre verlängert werden. Ein Software-Upgrade von RSA nach ECC ist technisch nicht möglich. Durch eine Laufzeitverlängerung ändert sich die Leistungsfähigkeit der TI-Anbindung nicht. Mit fortschreitender Digitalisierung, besonders der Einführung der ePA für alle 2024, kann sich eine nach den Bedürfnissen von VSDM ausgelegte Infrastruktur aus Einboxkonnektoren als unzureichend erweisen.*
2. Stückgleicher Ersatz der vorhandene Konnektoren: Ein neuer Konnektor kann für weitere 5 Jahre betrieben werden und möglicherweise danach Laufzeitverlängert werden. Je nach Modell kann ein neuer Konnektor leistungsfähiger sein als der ersetzte Konnektor. Zu bedenken ist, dass sich die bestehende Infrastruktur aus Einboxkonnektoren bei fortschreidender Digitalisierung als unzureichend erweisen kann, da benötigte

Leistung des TI Zugangs wesentlich von der Intensität seiner Nutzung abhängt. Um den Nutzungsumfang einzuschätzen, können die Auswertung von Konnektorlogs sowie eine nach Wahrnehmung und Erfahrung (Schätzwerte von Durchsatz und Dauer) ermittelte Verarbeitungszeiten hilfreich sein.

3. Übergangsweise Nutzung eines Konnektor-as-a-Service-Angebots: Es gibt Anbieter bei denen sie den TI Zugang mit Hilfe eines Konnektors mieten können, auch TI-as-a-Service (TIaaS) genannt. Dabei ist die LEI via VPN an das RZ des TIaaS-Anbieters angebunden, welcher einen (oder mehrere) dedizierten klassischen Konnektor für den Kunden betreibt. Bei großer Planungsunsicherheit oder im Notfall kann dies als Interimslösung in Frage kommen. Dieses Konnektor-Hosting lagert zwar die Betriebsaufwände zu einem professionellen Anbieter aus, bringt aber keine technischen Performancevorteile und sogar potenziell spürbar verzögerte Antwortzeiten in der Kommunikation (Latenzen).
4. Nutzung des TI-Gateways als Serviceleistung mit HighUmstieg auf den Highspeed-Konnektor, HSK, in Form des TI-Gateways als Serviceleistung: In dieser Variante setzt der entsprechende Anbieter im Hintergrund des Service-Bundles einen Highspeed-Konnektor ein. Dadurch reduzieren sich die Konfigurations- und Betriebsaufwände vor allem für größere LEI wie z.B. Krankenhäuser deutlich. Diesem standardisierten Service-Angebot steht das Konzept einer shared Ressource mit eventuellen Leistungsdellen bei Abfragespitzen gegenüber. Das TI-Gateway ist stand heute noch nicht am Markt verfügbar.
5. Beschaffung und Betriebs eines Highspeed-Konnektors: Im Vergleich zum TI-Gateway-Modell eine Investitionsentscheidung unter dem Gesichtspunkt der Leistungsmaximierung. Diese Investition geht einher mit den folgenden Punkten.
    - Höhere Anschaffungskosten, die individuell mit dem Hersteller zu klären sind.
    - Veränderte Struktur der Betriebskosten, vor allem durch die aktive Teilnahme am ITSM der TI.
    - **Gesteigerte Performance**, technische Flexibilität und Abdeckung eines hohen individuellen Sicherheits- und Kontrollbedarfs.

3.4.3.1 Fragen und Hilfestellungen zur Bewertung der vorhandenen TI-Zugangslösung:

Wann fand die Beschaffung der Konnektoren statt, wie alt sind die aktuell vorhandenen Konnektoren?

Wenn sie bereits vor 2020 Konnektor beschafft haben, sollten sie schnellstmöglich aktiv werden. Es besteht die Chance, dass ein Modell haben was generell nicht ECC fähig ist. Zusätzlich entwickelt IT-Hardware schnell weiter und vermutlich haben sie bereits heute ein eingeschränktes Nutzererlebnis. Im konkreten Einzelfall kommt es auf das Produktionsdatum der bei Ihnen eingesetzten Konnektoren an.
Es ist empfohlen, dass sie zeitnah einen konkreten Zeitplan zum Austausch der veraltenen TI-Komponenten erarbeiten. Zu Sicherheit, betrachten bitte sie auch das Alter und die ECC-Fähigkeiten der eingesetzten eHealth Kartenterminal.

Wie viele eHealth Kartenterminals werden aktuell in ihrem Haus an wie vielen Aufstellorten betrieben?

Je nachdem wie fragmentiert sich der Campus, die Aufnahme und der Entlass in ihrer Institution darstellt, haben sie bereits heute nicht zu vernachlässigenden Aufwand für ihre IT-Mitarbeiter. Dieser aktuelle Aufwand spiegelt sich in der Anzahl notwendiger Kartenterminals für die Interaktion durch Ärzte und Versicherte wider. Bei bis zu 40 eHealth Kartenterminal (2 Konnektoren) lässt sich das bekannte Modell - der Kauf von klassischen Konnektoren - weiterhin effektiv und überschaubar betreiben. Ab ungefähr

1000 eHealth Kartenterminals (50 Konnektoren) an den verschiedensten Aufstellorten (Sprechzimmer, Stationsthresen, Krankenhaus-Apotheke usw.) sollten sie die Beschaffung eines eigenen Highspeed-Konnektors bewerten.

Wie groß ist ihre IT Abteilung, das genutzte Rechenzentrum und wie viele Personentage pro Monat werden für die Betreuung der TI-Komponenten benötigt?

Für den Betrieb eines Highspeed-Konnektors benötigen Sie IT-Admins, deren Wissen über das eines Applikationsbetreuers hinausgeht. Eine Aufwandsersparnis ist zu erwarten, wenn sie bereits heute mehr als 0.5 VZÄ nur für den Support und Betrieb der TI-Komponenten in ihrem Haus benötigen. Idealerweise ist ihre sonstige IT-Hardware bereits heute in einem professionell betriebenen Rechenzentrum (z. B. durch Angliederung an eine Universität) untergebracht, in dem der Highspeed-Konnektor aufgestellt werden kann.

Was ist der notwendige Planungshorizont, wie weit reicht ihr nächster Budgetzyklus?

Abhängigkeit vom Umfang der zu planenden Mittel (Anzahl Konnektoren), lässt sich das notwendige Budget mit mehr oder weniger Vorlaufzeit beschaffen. Zukünftige TI-Produkte hänge von den Zulassungsverfahren und damit verbundenen Sicherheitszertifizierungen ab, potenziell sind Nacharbeiten notwendig bevor eine Zulassung erteilt werden kann. Auch der Abschluss einer weiterführenden bzw. die Anpassung der bestehenden Finanzierungsvereinbarung steht noch aus. Wenn Sie aufgrund ihrer Planungszyklen in kurzfristiger Zukunft eine belastbare Kostenschätzung benötigen, dann rechnen Sie nur mit den am Markt verfügbaren Produkten wie z. B. dem Konnektor oder unter Umständen einer Übergangslösung in Form von Konnektor-Hosting Angeboten.

4 Administrationsaufgaben im dezentralen Bereich der TI

4.1 Einleitung

Bevor Sie als IT-Mitarbeiter Ihres Krankenhauses oder als IT-Dienstleister im Auftrag eines Krankenhauses die Anbindung zur TI schaffen, sollten Sie sich darüber im Klaren sein, dass Sie gemäß § 332 Absatz 1 SGB V „besondere Sorgfalt bei der Herstellung und Wartung des Anschlusses an die TI walten lassen und über die notwendige Fachkunde verfügen (müssen), um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme und Komponenten zu gewährleisten". In Absatz 2 heißt es weiter „Die Erfüllung der Anforderungen muss den Leistungserbringern auf Verlangen auf geeignete Weise nachgewiesen werden."

4.1.1 Fachliche Vorabkenntnisse

Im dezentralen TI-Bereich sollten folgende Vorab-Kenntnisse zu Ihrem Fachrepertoire gehören:

- Kenntnisse der IT-Infrastruktur Ihres Krankenhauses,
- Erfahrung in der Netzwerktechnik und mit Netzwerkprotokollen,
- Kenntnisse in der Absicherung von Netzwerkumgebungen,
- Kenntnisse der Datenschutzbestimmungen,
- Kenntnisse der Installation und Funktionsweise der KIS sowie
- Erfahrung in der strukturierten Analyse und Behebung von Fehlern.

4.1.2 Hauptaufgaben

Bei der Planung, Schaffung und dem Betrieb des TI-Zuganges eines Krankenhauses kommen auf Sie folgende Hauptaufgaben (oder Teile davon) zu:

- Beschaffung der notwendigen dezentralen TI-Komponenten (siehe Kapitel 3.1),
- Installation und Inbetriebnahme der dezentralen TI-Komponenten (insbesondere von Kartenterminals und Konnektoren, siehe Kapitel 3.3 und 3.4),
- Dokumentation der Installation bzw. Inbetriebnahme,
- Wartung der dezentralen TI-Komponenten sowie
- Störungssuche, -meldung und -beseitigung.

Weiterhin müssen Sie **Störungen** im **dezentralen Bereich der TI** selbstständig oder unter Mitwirkung des Herstellers beheben. Bei Störungen im **zentralen Bereich der TI** wenden Sie sich an den Help Desk Ihres **VPN-Zugangsdienstes** (siehe Kapitel 4.2.3.1). Treten Störungen bei KIM auf, wenden Sie sich an den beauftragten **KIM-Anbieter** (siehe Kapitel 2.4.6).

4.1.3 Überblick über die Supportstruktur der TI

Die TI besteht aus einer Vielzahl von Komponenten, Diensten, Anwendungen, die von unterschiedlichen Herstellern und Anbietern zur Verfügung gestellt werden. Um ein erfolgreiches Zusammenspiel der Komponenten, Dienste und Anwendungen in der betrieblichen Praxis zu gewährleisten, wurde eine dienstleisterübergreifende Supportstruktur etabliert, die Sie als IT-Fachpersonal eines Krankenhauses kennen sollten.

Die Supportstruktur sieht mehrere Rollen vor:

- **Anbieter von Komponenten und Diensten (auch: Hersteller)**

  Anbieter von Komponenten und Diensten sind Unternehmen, die ein TI-Produkt für den dezentralen oder den zentralen Bereich der TI gemäß Spezifikationslage der gematik herstellen. TI-Produkte können Komponenten (Geräte, Software), Dienste und Anwendungen sein. Die TI-Produkte werden von der gematik zugelassen. Hersteller übernehmen die Produkthaftung gemäß den gesetzlichen Vorgaben sowie den Produkt-Support. Sie unterscheiden sich von Anbietern von Betriebsleistungen insbesondere dadurch, dass das verantwortete Produkt keinen IT-Service darstellt bzw. keine Betriebsleistungen in der TI umfasst. Ein typischer Hersteller im dezentralen TI-Bereich ist der Hersteller (bzw. Anbieter) von Konnektoren oder Kartenterminals.

- **Anbieter von Betriebsleistungen**

  Anbieter von Betriebsleistungen sind von der gematik zugelassene Unternehmen, die einen TI-Service (Dienste und Anwendungen) für End-Nutzer oder andere Servicenehmer offerieren und den Betrieb der dafür erforderlichen technischen Betriebsmittel verantworten. Diese Anbieter betreiben von der gematik zugelassene TI-Produkte oder lassen diese von Dritten betreiben. Ein typischer Anbieter von Betriebsleistungen ist der VPN-Zugangsdienst.

Alle Anbieter müssen für ihre Kunden einen Support unterhalten. Bei Störungen, die durch Komponenten und informationstechnische Systeme in Ihrem Krankenhaus verursacht werden (Kartenterminal, Konnektor, Netzwerk, Firewalls, KIS), liegt die Verantwortung der Störungsbehebung zunächst bei Ihnen selbst. Dabei können Sie auf den vorstehenden Hersteller- bzw. Produkt-Support zurückgreifen.

Stellen Sie in Ihrem Krankenhaus jedoch Störungen fest, dessen Ursache Sie in der TI, entweder beim VPN-Zugangsdienst oder einem dahinterliegenden Dienst der TI vermuten, so melden Sie diese an den 1st-Level-Support Ihres VPN-Zugangsdienst-Anbieters. Der VPN-Zugangsdienst-Anbieter trägt Ihnen gegenüber der Verantwortung für die Behebung der Störung, ganz gleich, ob seine eigenen Systeme die Störung verursachen oder ein anderer Dienst der TI.

Liegt die Ursache der Störung beim VPN-Zugangsdienst selber, muss er die Behebung der Störung in Eigenregie vornehmen. Stellt der VPN-Zugangsdienst-Anbieter jedoch fest, dass die von Ihnen gemeldeten Störung von einem anderen Dienst der TI (mit)verursacht wird, so ist der VPN-Zugangsdienst-Anbieter angehalten, diese Störung an den betreffenden Anbieter des die Störung verursachenden TI-Dienstes zu melden, eine Lösung einzufordern und die Lösung zu validieren. Auch bei einer weitergeleiteten Störung übernimmt der VPN-Zugangsdienst Ihnen gegenüber weiterhin die Verantwortung für die Bearbeitung der Störung. **Er kann diese Verantwortung nicht an Dritte delegieren.**

Zur übergreifenden Störungsbearbeitung ist der Anbieter des von Ihnen beauftragten VPN-Zugangsdienstes in das übergreifende IT-Service-Management der TI (TI-ITSM) eingebunden. Der Support der Anbieter von Betriebsleistungen untereinander ist dabei durch ein übergreifendes Betriebskonzept der gematik geregelt (siehe [gemKPT_Betr]), das auf die spezifischen Anforderungen der TI ausgerichtet ist. Alle Anbieter von Betriebsleistungen stellen im TI-ITSM einen Single-Point-of-Contact (SPOC) zur Verfügung, der eingehende Tickets überprüft und bei positiver Validierung an den nachgelagerten internen Support (im Sinne eines 2nd/3rd-Level-Supports) weiterleitet sowie übergreifende Störungen an die verursachenden Anbieter meldet. Der Anbieter-Anbieter-Support ermöglicht eine schnelle und erfolgreiche Bearbeitung übergreifender Störungen.

Die gematik agiert im Rahmen des TI-ITSM als koordinierende und überwachende Instanz. Sie überprüft dabei die Einhaltung der zugesicherten Service Level. Als Eskalationsinstanz unterstützt sie zudem bei übergreifenden Störungen die Lösungsfindung.

Beachten Sie bitte, einen auf Ihren Bedarf und Ihre Kenntnisse ausreichenden Support für die Installation, den Betrieb und die Wartung von Konnektoren bei Ihrem Konnektor-Hersteller zu beauftragen bzw. die Konditionen dafür zu erfragen. Falls ein VPN-Zugangsdienst-Anbieter gewählt wurde, der die Nutzung und Administration von Konnektoren im Bundle anbietet, kann von diesem ebenfalls ein entsprechender Support abgerufen bzw. angefordert werden.

4.2 Installation und Inbetriebnahme

4.2.1 Vorbereitung und Durchführung

Einen Einstieg zur Vorbereitung des TI-Anschlusses bietet die „**Checkliste Dienstleister vor Ort**" (siehe fachportal.gematik.de/dvo). Obwohl diese auf die TI-Anbindung einer Arztpraxis eingeht, können Sie die Checkliste auch als Grundlage für die Anbindung Ihrer Institution verwenden.

Grundsätzliche Voraussetzung für eine TI-Anbindung ist ein funktionierender Internetanschluss. Mit den Installationsarbeiten am Konnektor können Sie zudem erst dann beginnen, wenn:

- eine SMC-B beantragt wurde,
- die PIN separat per Post zugesendet wurde und
- die Karte durch den Kartenherausgeber freigeschaltet wurde.

Ein stationäres Kartenterminal (eH-KT) ist ebenfalls obligatorisch.

4.2.2 Installationsszenarien – Allgemeine Informationen zur Anbindung des Krankenhaus-Netzes (LAN) an die TI

In der Regel liegen den möglichen Installationsszenarien zwei Anbindungsvarianten zugrunde – die **serielle Anbindung** („Reihenbetrieb") und die **parallele Anbindung** („Parallelbetrieb") (siehe Kapitel 4.2.2.1). Auf dem Fachportal der gematik finden Sie das Informationsblatt „Betriebsarten des Konnektors" (fachportal.gematik.de/dvo), das Ihnen weitere Szenarien aufzeigt.

Beachten Sie, dass im Folgenden grundsätzlich von einer vorhandenen strukturierten Gebäudeverkabelung und einer Verbindung zum Internet via Internet Access Gateway (IAG) ausgegangen wird. Des Weiteren darf in allen Szenarien die Installation bzw.

Inbetriebnahme des Konnektors ausschließlich in einem zutrittsgeschützten bzw. zutrittsbeschränkten Raum (siehe Kapitel 3.4.1) erfolgen.

Allgemeine Sicherheitshinweise für die Installation im Krankenhaus:

Sofern durch die Anbindung an die TI die Leistungserbringerumgebung erstmalig an das Internet angeschlossen wird, ist zu gewährleisten, dass notwendige Sicherheitsmaßnahmen zum Schutz der medizinischen Patientendaten etabliert werden. Weiterführende Informationen finden Sie unter:

- dkgev.de/datenschutz,
- kbv.de/html/datensicherheit.php
- bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

Beachten Sie, dass Sie bei der **Installation des Konnektors im Reihenbetrieb** und bei der Nutzung des „Sicheren Internet Service" (SIS) diese Sicherheitsmaßnahmen sinnvoll in das Gesamtsicherheitskonzept Ihres Krankenhauses integrieren müssen.

Sofern aufgrund der konkret vorliegenden IT-Landschaft **im Krankenhaus ein Parallelbetrieb des Konnektors** geplant wird, sind bei der Auswahl der erforderlichen Netzwerkkomponenten und der Netzwerkkonfiguration insbesondere die Umsetzungshinweise „NET: Netze und Kommunikation" des Bundesamtes für Sicherheit in der Informationstechnik (BSI, siehe vorstehenden Link) zu beachten, da im Parallelbetrieb das lokale Netz (LAN) des Krankenhauses nicht durch die Netzwerksicherheitsfunktionen des Konnektors geschützt wird.

4.2.2.1 Serielle Anbindung vs. Parallele Anbindung

Der Konnektor kann die IT-Systeme des Krankenhauses vor Angriffen aus dem Internet zusätzlich schützen, sofern Sie die Konfiguration „seriell" wählen. Unabdingbar ist dabei, dass mit der Installation eines Konnektors keinesfalls die in den medizinischen Einrichtungen bereits umgesetzten Sicherheitsmaßnahmen für den IT-Betrieb obsolet werden, z. B. sind ein dem Gefährdungspotential entsprechender separater Virenschutz und Maßnahmen zur Netzabsicherung erforderlich.

Serielle Anbindung („Reihenbetrieb")

Bei einer **seriellen Anbindung** befinden sich alle Komponenten im selben Netzwerk (LAN) und erhalten ausschließlich über den Konnektor Zugang zur TI. Durch die integrierte Firewall des Konnektors und der optionalen Einbindung des Sicheren Internet Service (SIS, siehe Kapitel 4.2.3.2) wird das LAN optimal vor unautorisierten Zugriffen von außen geschützt. Diese Betriebsart ist einfach zu konfigurieren und gewährleistet eine vertrauliche Übertragung medizinischer Daten.

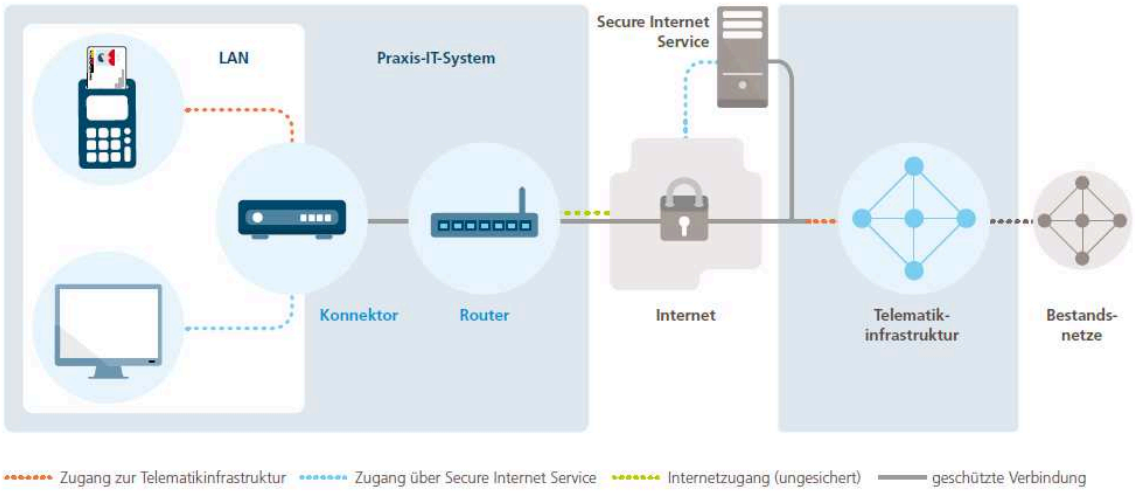

Abbildung 17: Schematische Darstellung der seriellen Anbindung

Parallele Anbindung („Parallelbetrieb")

Bei der **parallelen Anbindung** sind alle Komponenten mittels Netzwerkverteiler (Switch/Router) miteinander verbunden. Die Komponenten zur Verarbeitung medizinischer Daten nutzen den Konnektor, um die TI oder den optionalen SIS zu erreichen. Es ist daher zwingend notwendig, explizite Routen mit dem Ziel TI auf denjenigen Systemen zu konfigurieren, welche einen Zugriff auf die TI benötigen. Für die Namensauflösung von Zielsystemen in der TI muss entweder der jeweilige DNS-Request zum Konnektor gesendet werden oder ein entsprechendes Forwarding auf einem lokalen DNS-Server eingerichtet werden. Die restlichen Komponenten hingegen erhalten über den Router direkten Anschluss an das Internet. Ein bereits bestehendes LAN kann hierbei um den Konnektor ergänzt und weitergenutzt werden. Über den Router ist das Internet unabhängig vom Zugang zur TI und mit allen Diensten verfügbar. Dieses Netzwerk ist flexibel konfigurierbar.

Im Parallelbetrieb ist keine Komponente des LAN durch den Konnektor vor unautorisierten Zugriffen, bspw. Angriffen aus dem Internet, geschützt. Da der Konnektor im Parallelbetrieb nicht als Firewall im LAN fungiert, ist diese Betriebsart nur für medizinische Einrichtungen geeignet, die bereits ein LAN etabliert haben und über entsprechende Sicherheitsfunktionen gemäß den Standards des Bundesamtes für Sicherheit in der Informationstechnik verfügen.

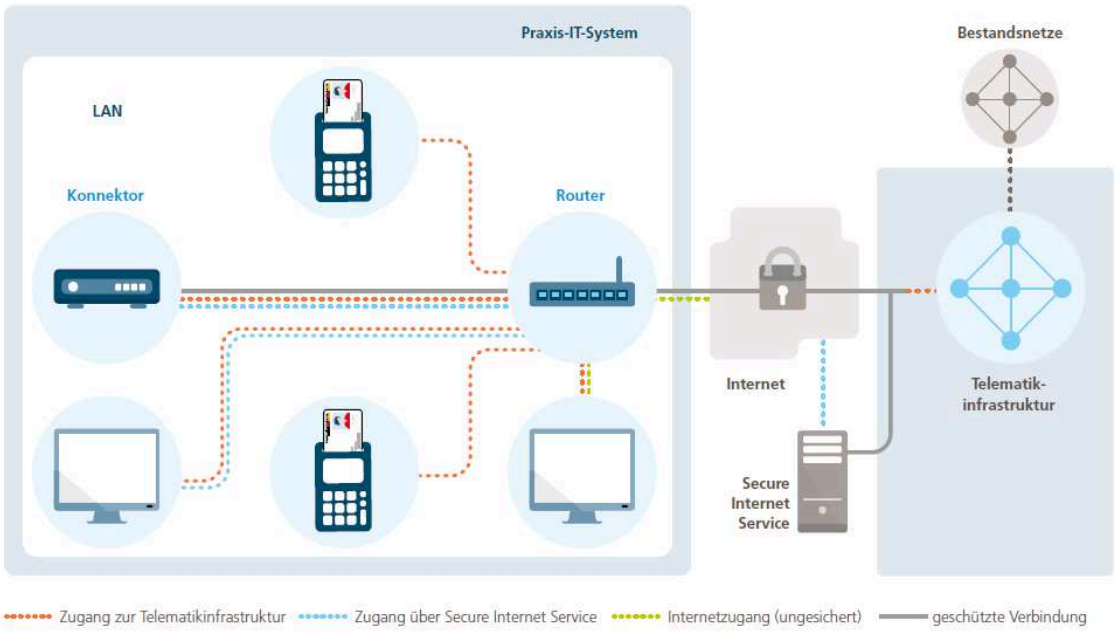

Abbildung 18: Schematische Darstellung der parallelen Anbindung

Weitere Installationsszenarien finden Sie im Anhang K des gematik-Dokuments [gemSpec_Kon], abrufbar im Fachportal der gematik bspw. unter fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/konnektor.

4.2.3 Nutzung wesentlicher TI-Dienste und Zugang zu Bestandsnetzen

Bevor Sie die Anbindung Ihres Krankenhauses an die TI vornehmen, sollten Sie die Anwender in Ihrem Hause (Ärzte, medizinisches Fachpersonal etc.) über die Nutzung der nachfolgenden Dienste informieren bzw. aufzeigen, wie die Zugriffe auf diese erfolgen.

4.2.3.1 VPN-Zugangsdienst (VPN-ZugD)

Ein **VPN-Zugangsdienst** (VPN-ZugD) ermöglicht den Leistungserbringern den Zugang zur TI und über den Secure Internet Service (SIS, siehe Kapitel 4.2.3.2) einen sicheren Internet-Zugang. Als Transportinfrastruktur zwischen dem Krankenhaus-LAN auf der einen Seite und dem VPN-ZugD auf der anderen Seite wird das Internet genutzt. Über diese Infrastruktur werden mittels IPsec-Tunnel zwischen den Konnektoren und dem VPN-ZugD gesicherte Verbindungen aufgebaut. Darüber hinaus erfolgt via VPN-ZugD u. a. die Registrierung und Freischaltung von Konnektoren.

Die derzeit von der gematik zugelassenen Konnektoren nutzen für die Kommunikation zur TI das IPv4-Protokoll. Für das WAN- bzw. LAN-Interface ist dabei ein Default-Wert von 1500 für die MTU-Size (Maximum Transmission Unit) vorgesehen. Diesen Wert können Sie über die jeweilige Managementschnittstelle des Konnektors konfigurieren.

Bei Anschluss an ein IPv6-Netz sollten Sie neben der Aktivierung von DS-Lite (Dual Stack Lite-Technik zum Tunneln von IPv4-Adressen in IPv6) beim Internet-Provider eine Reduzierung der MTU-Size auf den Wert 1400 vornehmen, um störende Paket-Fragmentierungen aufgrund des zusätzlichen Protokoll-Overheads zu verhindern.

Weitere Hinweise zu spezifischen Netzwerkinformationen der VPN-Zugangsdienst-Anbieter finden Sie unter https://fachportal.gematik.de/dvo.

4.2.3.2 Sicherer Internet Service (SIS)

Wie zuvor erwähnt, stellt der VPN-Zugangsdienst den Leistungserbringern zusätzlich einen **Sicheren** (oder Secure) **Internet Service** (SIS) zur Verfügung. Die Nutzung dieses ggf. für Sie kostenpflichtigen Services ist optional.

Durch die Verwendung eines SIS-Zugangs wird die Nutzung von Diensten im Internet sicherer. Generell werden vom SIS alle marktüblichen „State-of-the-Art"-Sicherheitsleistungen unterstützt, darunter bspw. Virenscanner, Firewall etc. Die Konfiguration der Sicherheitsleistung erfolgt zentral durch den Anbieter des VPN-Zugangsdienstes. Die Verbindung vom Krankenhaus zum SIS erfolgt über einen VPN-Kanal, der getrennt vom VPN-Tunnel zur TI aufgebaut wird.

Da die Kommunikation über den SIS auch Einschränkungen mit sich bringen kann, müssen Sie entscheiden, welches Installationsszenario den Ansprüchen Ihrer Anwender bei der Nutzung des SIS am besten gerecht wird. Dabei ist zu prüfen, ob die bisher genutzten Dienste auch über SIS noch funktionieren und ob es ggfs. auch individuelle Konfigurationsmöglichkeiten gibt bzw. notwendig sind (bspw. Nutzung SIS von allen PCs).

Bei der Wahl der passenden SIS-Anbindungsart prüfen Sie insbesondere folgende Punkte:

Bestandsaufnahme der Kommunikation zum Internet

- Auflistung aller Anwendungen und Dienste mit den dazugehörigen TCP/UDP-Ports pro Anwendung.
- Auflistung dedizierter Verbindungen, bspw. VPN-Tunnel zu anderen Standorten.
- Auflistung dedizierter Verbindungen aus dem Internet in das lokale Netzwerk, z. B. Remote Zugriff für Fernwartung.

Kommunikationsbewertung

- Werden Standardanwendungen, bspw. http, https, FTP, SMTP, SMTPS, POP3, POP3S, IMAP und IMAPS unterstützt.

Verbindungen in das Netzwerk des Krankenhauses

- Die Sicherheitsrichtlinien für den SIS erlauben keinen Verbindungsaufbau in das Krankenhaus-LAN. Deshalb sind Verbindungen, die aus dem Internet in Richtung lokales LAN aufgebaut werden, mit der SIS-Nutzung nicht mehr möglich. In diesem Fall müssen Sie prüfen, ob es alternative Möglichkeiten gibt.

Sonderfall: Klärung mit dem VPN-Zugangsdienstanbieter

- Im SIS wird ein Applikation Layer Gateway (ALG) eingesetzt, das für jede Anwendung einen Proxy bereitstellt. Wenn eine Anwendung nicht über einen Standardport kommuniziert, muss eine entsprechende Konfiguration am ALG vorgenommen werden. Aktuell ist ein Proxy-Satz im ALG konfiguriert, welcher durch den Betreiber des VPN-Zugangsdienstes definiert wird. Nutzen die bestehenden Anwendungen jedoch nicht die standardisierten TCP/UDP-Ports, müssen diese Verbindungen aus dem lokalen Netzwerk individuell betrachtet werden. Ggf. müssen Sie sich mit dem Anbieter des VPN-ZugD zur Klärung in Verbindung setzen.

  Weiterführende Informationen zum SIS finden Sie im gematik-Dokument [gemSpec_VPN_ZugD], das Sie auf dem Fachportal der gematik abrufen können.

4.2.3.3 Bestandsnetze

Neben der TI existieren im deutschen Gesundheitswesen weitere Netzwerkverbunde, sog. **Bestandsnetze**, die teilweise bereits vor der TI entstanden sind. In den Bestandsnetzen werden Leistungserbringern und Krankenhäusern unterschiedliche Fachanwendungen bereitgestellt.

Die verfügbaren Bestandsnetze können Sie über das Management-Interface des Konnektors einsehen. Dabei sind die Bestandsnetzanbindungen standardmäßig aktiviert.

Die genaue Vorgehensweise für die Anbindung der Bestandsnetze über den Konnektor erfolgt herstellerspezifisch.

Bitte beachten Sie unbedingt, dass die angebundenen Bestandsnetze (aAdG-NetG) mit einer öffentlichen IP-Adresse an die TI angeschlossen werden. Für die Erreichbarkeit dieser Bestandsnetze über die TI sind daher im Anschlussszenario „Parallelbetrieb" entsprechende Routen in Richtung Konnektor notwendig. Die Namensauflösung für die Zielsysteme im Bestandsnetz erfolgt über DNS-Server im Bestandsnetz. Daher ist es notwendig. dass die DNS-Requests für diese Ziele im Bestandsnetz zum Konnektor geleitet werden.

4.2.4 Mandantenkonfiguration

An die Mandantenkonfiguration gibt es pro Fachanwendung unterschiedliche Anforderungen:

- VSDM, NFDM, eMP: keine TI-spezifischen Anforderungen
- ePA: Berechtigungen auf die ePA werden über die Telematik-ID einer SMC-B einem Mandanten (identifiziert über die Mandanten-ID) zugeordnet. Dadurch können datenschutzrechtliche Zugriffsberechtigungen bzw. -beschränkungen innerhalb von Krankenhäusern auf die ePA übertragen werden.

Die **Anwendung ePA erfordert** (anders als NFDM) eine an die Mandantentrennung eines Krankenhauses **angepasste Verwaltung von SMC-Bs bzw. Mandanten**. Für eine funktionierende ePA muss zwischen der Mandanten-ID, die im Informationsmodell des Konnektors konfiguriert wird, und der Telematik-ID eine 1:1-Beziehung vorliegen. **Das bedeutet, dass für einen (ePA-)Mandanten im Konnektor die zugeordneten SMC-Bs eine identische Telematik-ID aufweisen müssen.** Der diesen SMC-Bs zugeordnete Mandant hat dann dieselben Zugriffsrechte auf die ePA eines Versicherten, in Abhängigkeit der Berechtigung, die dieser Institution (Telematik-ID) vom Versicherten erteilt wurde.

Bei geeigneter Beantragung von SMC-Bs für das Krankenhaus können Sie damit die im Krankenhaus vorhandenen bzw. geplanten internen Zugriffsberechtigungen abbilden (Mandantentrennung). Die Freigabe von Zugriffsrechten auf die ePA erfolgt auf Basis der Telematik-ID der den Arbeitsplätzen zugeordneten SMC-Bs.

Im Vorfeld einer Mandantentrennung müssen unterschiedliche SMC-Bs mit je eigenen Telematik-IDs pro Mandant beantragt sein, falls dies ihrem Mandantentrennungskonzept entspricht.

Die Telematik-ID wird im Informationsmodell des Konnektors der SMC-B und den betroffenen Arbeitsplätzen zugeordnet. Dadurch wird sichergestellt, dass erteilte Zugriffsberechtigungen zu einer faktischen Zugriffsmöglichkeit an den vorgesehenen Arbeitsplätzen führt.

4.2.5 Notwendige Einstellungen von DNS-Verweisen und Routern im Umgang mit Zertifikatsprüfungen

Werden durch den Client einer TI-Fachanwendung (Browser oder Rich-Client) TI-Zertifikate genutzt bzw. durch die Fachanwendung verwendet, so ist Folgendes zu beachten:

Der „Default-Vertrauensraum" von Browsern ist zunächst das „Internet". Ist der im (vom Server der Fachanwendung empfangene) Zertifikat enthaltene FQDN[20] keine Internetadresse und somit das ausgestellte Zertifikat nicht von einer Zertifikatsstelle ausgestellt, der der Client vertraut, so kann der Client grundsätzlich melden, dass das Zertifikat aus keinem bekannten Vertrauensraum stammt. Zum Beispiel, indem er die Meldung „Vertrauen Sie diesem Zertifikat?" anzeigt.

Handelt es sich um ein von einer Internet-Zertifikatsstelle ausgestelltes Zertifikat, so wird der Browser diese Meldung nicht anzeigen.

Sollte es mit Hilfe des FQDN bei einer TI-Fachanwendung zu einer Überprüfung des Zertifikats kommen (CA- oder OCSP-Abfrage), muss ein angesprochener lokaler DNS-Server statt ins Internet auf den Konnektor verweisen. Lokale DNS- und Routingeinstellungen müssen also für TI-spezifische FQDN auf den Konnektor bzw. in die TI verweisen.

Bei Rich-Clients existiert das Problem zwar ebenfalls, es kann aber programmtechnisch gelöst werden. Der Rich-Client kann in seinem Verhalten, im Gegensatz zu Browsern, durch seinen Programmierer entsprechend eingestellt werden, um in der beschriebenen Situation angemessen zu reagieren.

4.2.6 Allgemeine Hinweise zur erfolgreichen Installation

Anhand der folgenden Punkte können Sie allgemein überprüfen, ob die Installation und somit der Anschluss an die TI auf technischer Ebene erfolgreich verlaufen ist:

KIS

Die Einrichtung einer Verbindung zwischen einem KIS und einem Konnektor folgt den jeweiligen Herstellervorgaben. Allen Einrichtungsszenarien ist jedoch gemein, dass das KIS für den Nachweis einer erfolgreichen Installation die „Bereitschaft" des Konnektors überprüft. Dazu fragt das KIS bspw. das Vorhandensein aller benötigten Schnittstellen sowie aller Karten ab. Erst wenn diese Bereitschaft vom Konnektor bestätigt wird, kommunizieren KIS und Konnektor miteinander. Dies erkennen Sie daran, dass im Primärsystem der Konnektor angezeigt wird.

Dabei ist zu beachten, dass der Konnektor sowohl als „online" (mit der TI verbunden) als auch als „offline" (kein Zugang zur TI) angezeigt werden kann.

Konnektor und Kartenterminal

Um zu überprüfen, ob der Konnektor erfolgreich installiert wurde, öffnen Sie einen Browser und geben Sie dort die IP-Adresse des Konnektors ein. Hier sehen Sie das Management Interface des Konnektors. Sobald Sie die VPN-Zugangsdaten über das Management Interface eingegeben haben, kann der Konnektor beim VPN-ZugD registriert und ein Tunnel vom Konnektor zum VPN-ZugD aufgebaut werden. Das Management Interface des Konnektors zeigt Ihnen auch an, ob die Kartenterminals gepairt und verbunden bzw. funktionsbereit sind, also als „online" angezeigt werden.

[20] Fully-Qualified Domain Name, vollqualifizierter Name einer Domain

Verwendung der Prüfkarte eGK

Um zu überprüfen, ob die Installation von Primärsystem, eHealth-Kartenterminal (eH-KT) und Konnektor in Bezug auf die Fachanwendung VSDM und die Konfiguration der dezentralen Komponenten erfolgreich war, stecken Sie die Prüfkarte eGK in das eH-KT. Am Primärsystem wird daraufhin ein Versichertenstammdatensatz mit einer fiktiven Identität als Ergebnis der Prüfung der Versichertenstammdaten angezeigt (siehe nachfolgende Tabelle):

Tabelle 2: Beispiel für Anzeige der Prüfkarten-eGK-Daten im Primärsystem

Versicherten_ID	**Prüfkartennummer** [siehe Aufdruck der Prüfkarte]
Nachname	**„Ort"**
Vorname	**„Dienstleister"**
Vorsatzwort	**„vor"**
Geburtsdatum	19800101 – [01.01.1980]
Geschlecht	„X" [unbestimmtes Geschlecht]
Straße	„Friedrichstraße"
Hausnummer	136
Ort	„Berlin"
Postleitzahl	10117
Versicherungsschutz Beginn	20000101 – [01.01.2000]
Kostentraeger	109500969
Kostentraegerlaendercode	„D" [Deutschland]
Kostentraeger/Name	„Test GKV-SV"
Versichertenart	1 [Mitglied]
Kostenerstattung (alle)	0
WOP	83 [Brandenburg]
Zuzahlungsstatus/Status	0 [von der Zuzahlungspflicht nicht befreit]
Selektivvertraege (alle)	9
Selektivvertraege/Art	0000
Alle weiteren Angaben	„" [leer]

Eine vollständige Onlineprüfung und -aktualisierung der Versichertenstammdaten kann mit der Prüfkarte eGK G2 nicht durchgeführt werden, da ihre Daten – im Gegensatz zu den Daten einer eGK eines Versicherten – keiner realen Krankenversicherung zugeordnet sind. Ab der Prüfkarte eGK G2.1 wird zusätzlich eine „teilweise" Onlineprüfung durchgeführt.

Beim Initiieren des Auslesens der Prüfkarte eGK im KIS führt das Fachmodul VSDM des Konnektors auch eine OCSP-Abfrage durch und erhält im Erfolgsfall eine Meldung „Ok". Diese Information wird im Ablaufprotokoll des Fachmoduls VSDM dokumentiert. Das Ablaufprotokoll kann über die Administrationsschnittstelle des Konnektors eingesehen werden.

Darüber hinaus werden über die Administrationsschnittstelle des Konnektors weitere Prüfmöglichkeiten angeboten, so z. B. die Abfrage des Status einer etablierten VPN-

Verbindung. Über die genaue Umsetzung dieser Prüfmöglichkeiten informieren die Administrationshandbücher der Konnektor-Hersteller.

Beim Auslesen der Prüfkarte eGK kann optional ein Prüfungsnachweis mit dem Ergebnis der Onlineprüfung angefordert werden. Da bei der Prüfkarte der Generation G2 kein Fachdienst VSDM zur Verfügung steht, erzeugt das Fachmodul VSDM den Prüfungsnachweis mit dem Ergebnis 3 („Aktualisierung VSD auf eGK technisch nicht möglich"). Das Ergebnis 3 gibt für sich allein keinen Aufschluss darüber, ob eine Verbindung zur TI aufgebaut werden konnte oder nicht. Dazu müssen Sie das Ablaufprotokoll und ggf. das Fehlerprotokoll des Fachmoduls VSDM hinzuziehen und analysieren.

Ab der Prüfkarte eGK G2.1 steht ein VSDM UFS-Dienst zur Verfügung. Anfragen über den Konnektor werden, für diese eGKs immer mit dem Prüfungsnachweis mit dem Ergebnis 2 quittiert („Keine Aktualisierung VSD auf eGK erforderlich"), was ebenfalls im Ablaufprotokoll des Fachmodul VSDM protokolliert wird. Dadurch wird attestiert, dass die Gültigkeitsprüfung der Prüfkarte eGK vom OCSP-Server und die Verbindung vom Konnektor über das Intermediär zum Fachdienst VSDM erfolgreich waren.

4.2.7 Verwendung der Prüf-eGK

Die Prüf-eGK ist eine Versicherte-ungebundene eGK, die in der PU für Prüfzwecke eingesetzt werden kann. Ihre Nutzung ist in [gemSysL_PK_eGK] erläutert (Dokument befindet sich demnächst auf dem Fachportal der gematik unter dem Titel „Systemspezifischer Prüfleitfaden mit der Prüfkarte eGK".

Für KH hat die Prüfkarten eGK den Vorteil nicht in der RU testen zu müssen, was für KH mit erheblichem Aufwand verbunden ist. Bereits mit der Prüfung VSDM mit Prüf-eGK lässt sich die Funktionsfähigkeit der Infrastruktur (Konnektor, Kartenterminals, VPN-Zugangsdienst, SMC-B, Routing) sicherstellen.

4.2.7.1 Einsatz von HBA und SMC-B

Die Prüfkarten eGK werden mit den echten HBA und SMC-B verwendet. Während dies bei der SMC-B kein praktisches Problem darstellt, muss für Prüfungen und Schulungen, die einen HBA erfordern (QES für NFDM/EMP, eAU, eRP), ein „friendly" Arzt seinen HBA zur Verfügung stellen.

Da zumindest Schulungen der QES hauptsächlich Ärzte betreffen, gehen wir davon aus, dass eine entsprechende Nutzung eines Arzt-HBA möglich sein sollte.

Hinweis: Einen Prüf-HBA und eine Prüf-SMC-B wird es in absehbarer Zeit nicht geben. Dies hätte zur Folge:

- *dass sämtliche HBA-Signaturen, die heute standardisiert sind, eine entsprechende Markierung als „Prüfsignatur" bekommen und gleichzeitig alle signaturauswertenden Systeme diese Prüfsignatur als solche erkennen, somit nicht mehr dem Standard folgen,*
- *dass zusätzlich eine Prüfkarte HBA oder SMC-B in ihrem Funktionsumfang erheblich eingeschränkt werden müsste, um ein Missbrauch mit echten Versicherten-eGKs zu unterbinden, was wiederum zu keiner effektiven oder sinnvollen Nutzung dieser Leistungserbringer-Prüfkarte führen würde.*

4.3 KIM-Integration

Damit KIM in einem Krankenhaus eingesetzt werden kann, ist es zunächst notwendig, einen von der gematik zugelassenen KIM-Anbieter zu finden, der auch das KIM-

Clientmodul bereitstellt und bei Integration, Installation und Inbetriebnahme sowie bei technischen Problemen entsprechende Lösungen und Support anbietet.

Für die Nutzung von KIM in einem Krankenhaus bestehen u.a. folgende Anwendungsfälle, die Sie bei der Planung einer Kommunikationsarchitektur berücksichtigen können:

Ausgehender KIM-Verkehr, d.h. Versand einer Nachricht eines Krankenhaus-Arztes (persönliches KIM-Postfach) oder aus einem Gruppen- bzw. Funktionspostfach des Krankenhauses:

- an einen externen Arzt mit optionalem Anhang ohne Patientenzuordnung,
- Versand einer Nachricht eines Krankenhaus-Arztes an einen externen Arzt mit LDT3-Anhang (mit Patientenzuordnung),
- Versand einer Nachricht eines Krankenhaus-Arztes an ein Gruppen- bzw. Funktionspostfach eines externen Krankenhauses mit optionalem Anhang ohne Patientenzuordnung,
- Versand einer Nachricht eines Krankenhaus-Arztes an ein Gruppen- bzw. Funktionspostfach eines externen Krankenhauses mit LDT3-Anhang (mit Patientenzuordnung),
- Versand einer elektronischen Arbeitsunfähigkeitsbescheinigung an die zuständige Krankenkasse bei Entlassung des Patienten zur externen Weiterbehandlung,
- intersektorale Entlass- oder Überleitungsinformationen aus dem Krankenhaus in eine Pflegeeinrichtung.

Einkommender KIM-Verkehr, d.h. Nachricht von einem externen Arzt oder aus einem externen Gruppen- bzw. Funktionspostfach:

- an einen Arzt des Krankenhauses mit optionalem Anhang ohne Patientenzuordnung,
- an einen Arzt des Krankenhauses mit LDT3-Anhang (mit Patientenzuordnung)
- an ein Gruppen- bzw. Funktionspostfach des Krankenhauses ohne Patientenzuordnung mit anschließender interner Verteilung,
- an ein Gruppen- bzw. Funktionspostfach des Krankenhauses mit LDT3-Anhang (inkl. Patientenzuordnung),
- intersektorale Entlass- oder Überleitungsinformationen aus einer Pflegeeinrichtung an das Krankenhaus.

Die Einbindung von KIM in die bestehenden Prozesse und IT-Systeme stellt ein Krankenhaus vor mehrere und ggf. sehr komplexe Herausforderungen, die einer sorgfältigen Planung und Konzeptionierung sowie der Planung einer ggf. stufenweisen Einführung und Inbetriebnahme bedürfen. Im Folgenden können nur einige wesentliche und übergreifende Herausforderungen angesprochen werden, da sich die aufbauorganisatorischen, prozessualen und technischen Ausgangssituationen in den Krankenhäusern sehr stark voneinander unterscheiden (können).

4.3.1 Schutzerfordernisse und Ausfallsicherheit

Wie bereits aus den Ausführungen des Kapitels 2.4.6 hervorgeht, ermöglicht KIM bei der Übertragung von KIM-Nachrichten die Erreichung der IT-Schutzziele Verfügbarkeit, Vertraulichkeit und Authentizität. Die über KIM aus Ihrem Krankenhaus versendeten Nachrichten werden vom KIM-Clientmodul verschlüsselt und signiert und von dort sicher über die TI bis zum KIM-Fachdienst des Empfängers transportiert. Das KIM-Clientmodul

des Empfängers wiederum nimmt die Signaturprüfung vor und entschlüsselt die Nachricht. Alle KIM-Teilnehmer sind im VZD der TI gelistet, zur sicheren Übertragung der Nachrichten werden die PKI-Komponenten der TI verwendet. Sämtliche Verbindungen sind zusätzlich TLS-verschlüsselt. Alle bei diesem Nachrichtenverkehr beteiligten KIM-Fachdienste der unterschiedlichen KIM-Hersteller und deren KIM-Clientmodule sind von der gematik zugelassen, die KIM-Fachdienste werden dabei sicher in der Provider Zone der TI von zugelassenen KIM-Anbietern betrieben.

Auch die Erreichung des IT-Schutzzieles Integrität wird bei KIM vorausgesetzt, da die Erzeugung der KIM-Nachrichten in der Consumer Zone der TI unter Verwendung der Komponenten der Secure Consumer Zone erfolgt. Dennoch ist nicht vollständig auszuschließen, dass über KIM Schadsoftware oder Viren verteilt bzw. versendet werden. Dies geschieht beispielsweise unwissentlich und unbeabsichtigt, da ggf. das Clientsystem des Absenders von Schadsoftware infiziert ist und die Infizierung bisher unentdeckt blieb.

Als IT-Dienstleister des Krankenhauses müssen Sie daher im Rahmen einer Überprüfung der bestehenden Sicherheitsanforderungen und des bisherigen Sicherheitskonzepts entscheiden, in welcher Weise in Ihrem Krankenhaus über KIM eingehender Nachrichtenverkehr überprüft werden muss. Des Weiteren müssen Sie entscheiden, an welcher Stelle welche Schutzmaßnahmen zu ergreifen sind. Ggf. ist es ratsam, ein- und ausgehenden KIM-Nachrichtenverkehr an zentraler Stelle auf Schadsoftware und Viren zu untersuchen. Dazu müssen Sie planen, wie und mittels welcher Systeme diese Untersuchung erfolgen soll und ob bereits vorhandene Sicherheitssysteme und Vorkehrungen nachgenutzt werden können.

Da über KIM einkommende E-Mails erst hinter dem KIM-Clientmodul unverschlüsselt vorliegen, kann erst ab hier eine zentrale Untersuchung und Analyse der Inhalte der einkommenden KIM-Nachrichten auf Schadsoftware und Viren vorgenommen werden. Dies sollte auf einem separaten System erfolgen, bevor die Nachrichten bzw. der Inhalt der Nachrichten weitergeroutet bzw. weiterverarbeitet werden. Daher kann es ggf. erforderlich sein, das KIM-Clientmodul als Proxy auf einer separaten Appliance zu betreiben und die KIM-Nachrichten-Prüfung ebenfalls auf einer vorgeschalteten separaten Appliance in einem getrennten, geschützten Netzsegment des Krankenhaus-LANs vorzunehmen, um dort die erforderlichen Schutzmaßnahmen durchführen zu können. Beachten Sie dabei, dass das **KIM-Clientmodul keine persistente Speicherung der Nachrichteninhalte erlaubt**.

Des Weiteren müssen Sie klären, welcher Schutzbedarf in Ihrem Krankenhaus für das Versenden von KIM-Nachrichten besteht und welche Schutzmaßnahmen Sie hierzu ergreifen müssen (z. B. data-loss-prevention). Beachten Sie, dass beim Versenden von KIM-Nachrichten eine Überprüfung der Nachrichteninhalte nur vor dem KIM-Clientmodul möglich ist (vom absendenden Client-System ausgesehen), da ab hier die Nachrichteninhalte verschlüsselt übermittelt werden.

Ein weiterer wichtiger Punkt besteht in der Klärung, wie Sie die Ausfallsicherheit der KIM-Anbindung erhöhen können. Bei SMC-B gebundenen KIM-Adressen sollten Sie darauf achten, dass nicht durch Ausfall einer einzigen SMC-B, eines einzigen Kartenterminals oder eines Konnektors der gesamte KIM-Verkehr für längere Zeit lahmgelegt wird. Zu jeder SMC-B basierten KIM-Adresse sollte demzufolge mindestens eine Ersatz-SMC-B vorhanden sein, die bei Ausfall sofort gesteckt und dem Konnektor bekannt gemacht werden kann.

Bei Verfolgung eines **fachabteilungs-getriebenen Modells** (siehe Kapitel 3.2.2.4) sind bei Ausfall einer SMC-B, eines Kartenterminals oder eines Konnektors zunächst „nur" die entsprechend zugeordneten Fachabteilungen betroffen. Um eine Ausfallsicherheit zu schaffen, sollte jeder single-point-of-failure ausgeschlossen werden,

was bedeutet, dass Sie im Rahmen des Architekturkonzepts entsprechende Redundanzen einplanen sollten.

Im Falle der Realisierung des **anwendungsgetriebenen Modells** (siehe Kapitel 3.2.2.3) können beispielsweise in einem Rechenzentrum zwei SMC-Bs in zwei Kartenterminals einem KIM-Konnektor zugeordnet werden. Um eine Konnektor-Redundanz zu ermöglichen, kann ein zweites, redundantes KIM-Client-Modul bzw. eine zweite Clientmodul-Instanz eingerichtet werden, an die ein separater Konnektor angebunden ist, an dem ggf. wiederum zwei SMC-Bs in zwei Kartenterminals angeschlossen sein können. Dabei müssen Sie darauf achten, dass für jede für den KIM-Nachrichtenverkehr verwendete Telematik-ID entsprechend zugeordnete SMC-Bs einzusetzen sind. Falls mehrere Telematik-IDs verwendet werden, vervielfacht sich entsprechend der Einsatz der (redundanzsichernden) SMC-Bs.

Des Weiteren müssen Sie darauf achten, wie schnell die Auslastung des von Ihnen eingesetzten Konnektors erreicht wird. Beachten Sie hierbei, dass eine KIM-Nachricht, z. B. an ein Funktionspostfach eines anderen Krankenhauses, gegebenenfalls mehrfach verschlüsselt wird (siehe auch Kapitel 2.4.6#Abschnitt „Mehrere SMC-Bs pro Telematik-ID"). Folgen Sie daher den Vorgaben und Empfehlungen des Konnektor-Herstellers. Denken Sie daran, dass erst mit Umsetzung der KIM-Version 1.5.1 ein KIM-Clientmodul gleichzeitig mehrere Konnektoren ansprechen kann, sofern Ihr KIM-Anbieter dies entsprechend umgesetzt hat.

Bei der Einrichtung persönlicher Postfächer auf HBA-Basis ist darauf zu achten, dass bei Ausfall des HBAs die an dieses Postfach adressierten KIM-Nachrichten nicht mehr entschlüsselt werden können. Um eine unterbrechungsfreie persönliche Zustellung zu ermöglichen, kann beispielsweise im Falle des Ausfalls oder des Verlusts des HBA im Registrierungsdienst des KIM-Anbieters die vorhandene KIM-Adresse auf eine separate SMC-B (mit separater Telematik-ID) „übertragen" werden. Ein solches Vorgehen darf natürlich nur in Übereinstimmung mit den in Ihrem Krankenhaus geltenden Datenschutzvorgaben erfolgen und sollte von den entsprechenden Verantwortlichen bestätigt werden.

4.3.2 Festlegung der KIM-Adressen und Routing einkommender KIM-Nachrichten

Im Rahmen Ihres Kommunikationskonzeptes müssen Sie festlegen, welche KIM-Adressen Sie im VZD registrieren möchten. Dabei sind folgende Rahmenbedingungen durch den VZD der TI gegeben (siehe auch Kapitel 2.4.6):

- KIM-Adressen können ausschließlich über den Registrierungsdienst des beauftragten KIM-Anbieters im VZD der TI eingetragen werden,
- im VZD werden KIM-Adressen einer Telematik-ID zugeordnet,
- es können zu einer Telematik-ID maximal 100 KIM-Adressen registriert werden,
- eine KIM-Adresse darf im VZD nur ein einziges Mal vorkommen und kann daher immer nur zu einer Telematik-ID eingetragen werden,
- jeder HBA weist eine eigene Telematik-ID auf,
- im Gegensatz dazu können mehrere SMC-Bs zu einer Telematik-ID geführt werden,
- die Telematik-IDs von HBAs und von SMC-Bs sind disjunkt, d.h. eine Telematik-ID kann entweder einen HBA oder eine oder mehrere SMC-Bs repräsentieren,
- ein Krankenhaus kann durch mehrere Telematik-IDs repräsentiert werden, wenn bspw. eine oder eine Gruppe von Fachabteilungen eigene Institutionskennungen erhalten sollen,

- eine KIM-Adresse kann, unabhängig von der Telematik-ID, als eine persönliche Adresse oder eine Funktions- bzw. Gruppenpostfachadresse benannt werden.

Bei der Festlegung der KIM-Adressen sind folgende Fragen zu klären:

- Welche Funktionspostfach-Adressen sollen im VZD registriert werden (bspw. getrennt nach Fachabteilungen) und wie lautet die zutreffende Bezeichnung?
- Wie viele Funktionspostfächer sollen eingerichtet werden und unter welchen Telematik-IDs?
- Wenn persönliche Postfächer registriert werden sollen: Wie wird sichergestellt, dass bei Abwesenheit entsprechende KIM-Abwesenheitsnotizen eingetragen werden?
- Wie erfolgt die interne Bearbeitung der an ein Postfach adressierten eingehenden Nachrichten (persönliches Postfach, Gruppenpostfach, Verteiler)? Welche Personen erhalten Zugriff auf dieses Postfach? Wie können Mehrfach-Bearbeitungen eingehender Nachrichten vermieden werden?
- Wie erfolgt die Herstellung des Patientenkontextes bei eingehenden KIM-Nachrichten?

Des Weiteren müssen Sie klären, wohin und in welcher Weise über KIM eingehende Nachrichten in Ihrem Krankenhaus intern geroutet und den Empfängern zur Verfügung gestellt werden. Eine allgemein gültige Vorgehensweise kann an dieser Stelle nicht dargestellt werden. Grundsätzlich lassen sich folgende Vorgehensweisen unterscheiden:

- Eingehende KIM-Nachrichten werden dem Nutzer integriert in einem Client des Primärsystem zur Verfügung gestellt,
- die Zustellung erfolgt über das bereits in Ihrem Krankenhaus etablierte E-Mail-System und/oder
- es findet eine automatisierte Verarbeitung einkommender Nachrichten direkt innerhalb einer krankenhausinternen Fachanwendung statt (z. B. anhand der Dienstkennung).

Selbstverständlich sind auch Mischformen denkbar und sinnvoll. So eignet sich eine automatisierte Weiterverarbeitung von Nachrichten nur bei bestimmten Dienstkennungen. Für diese Nachrichten kann dann möglicherweise auf eine klassische Zustellung der ursprünglichen Nachricht an das adressierte Empfänger-Postfach vollständig verzichtet werden.

Eine weitere Fragestellung betrifft das Mapping der über den VZD der TI adressierbaren E-Mail-Adressen und auf die in Ihrem Krankenhaus-Verzeichnis geführten E-Mail-Adressen. Haben Sie vor, einkommende KIM-Nachrichten auf bereits bestehende Postfächer des im Krankenhaus etablierten E-Mail-Systems zuzustellen, so müssen Sie die Nachrichten auf diese Zieladressen routen. Am erfolgversprechendsten ist ein solches Routing, wenn der KIM-Anbieter hierzu ein entsprechendes zentrales Mapping-Verwaltungsmodul anbietet (dazu besteht keine normative Verpflichtung seitens gematik). Dies gilt insbesondere für das Mapping personengebundener KIM-Adressen (KIM-Adresse ist einem HBA zugeordnet).

Weiterhin müssen Sie festlegen, ob eine KIM-Nachricht, die an ein im VZD angegebenes Funktionspostfach gerichtet ist, zusätzlich einem definierten Adressatenkreis persönlich zugestellt werden soll. Ggf. können Sie dabei auf ein bereits bestehendes Konzept bzw. Regelungen zurückgreifen, zumal wenn für die Zielpostfächer das bereits etablierte E-Mail-System verwendet werden soll.

Beachten Sie auch, dass bei einkommenden KIM-Nachrichten beim Nutzer bzw. dem verwendeten Clientsystem auch eine entsprechende KIM-Referenz erhalten bleibt, um

die Quelle und den Übermittlungsweg transparent zu halten und beispielsweise eine direkte Antwort über den gleichen Übermittlungsweg erfolgen kann.

Für die Versendung von KIM-Nachrichten sind u.a. folgende Fragen zu klären:

- Welche Primär- bzw. Clientsysteme sind an den KIM-Nachrichten-Verkehr anzubinden?
- Wie und zu welchem Zeitpunkt wird die korrekte KIM-Adresse aus dem VZD ermittelt? Kann dies innerhalb der beteiligten Clientsysteme automatisiert erfolgen (z. B. beim Versand einer elektronischen Arbeitsunfähigkeitsbescheinigung an die Krankenkasse oder eines Entlassungsbriefs an den Hausarzt des Patienten)? Wie kann eine Verknüpfung zwischen der im Primärsystem enthaltenen Arztadresse (bspw. automatisiert über einen KBV-Eintrag ermittelt) mit einer KIM-Adresse hergestellt werden?
- Wie kann der VZD an einen vorhandenen Mail-Client angebunden werden (bspw. über LDAP)?
- Wie kann automatisiert eine korrekte KIM-Adressierung erfolgen? Welche Möglichkeiten bietet das Primärsystem?
- Wie können für den KIM-Benutzer Medienbrüche vermieden werden?
- Wie werden Nicht-Zustellungs-, Abwesenheits- und sonstige Fehler-Meldungen (automatisiert) verarbeitet?

Für das IP-Routing müssen Sie beachten, dass Sie das Routing vom KIM-Client-System zum (KIM-)Konnektor administrativ einrichten müssen. Falls Sie über ein Standard-Gateway verfügen, über das jeglicher Internet-Verkehr abgewickelt wird, würden – ohne entsprechende Änderung – sämtliche Anfragen zunächst über das Standard-Gateway ins Internet geroutet und die Anfragen liefen ins Leere. Da die KIM-Client-Systeme aller Wahrscheinlichkeit nach in ganz unterschiedlichen Netzwerksegmenten betrieben werden, müssen Sie, falls in Ihrem Krankenhaus **kein eigenes DNS** betrieben wird, **auf** den **Layer3-fähigen Komponenten** in Ihrem Netzwerk **statische Routen** zum KIM-Konnektor **einrichten**. Falls der KIM-Nachrichtenverkehr über mehrere Konnektoren abgewickelt wird, müssen ggf. mehrere Routen eingerichtet bzw. der jeweils zutreffende Konnektor adressiert werden.

4.3.3 Nutzung eines etablierten E-Mail-Systems zur Versendung von KIM-Nachrichten

Bei der Versendung von KIM-Nachrichten müssen Sie sicherstellen, dass vom Client-System die an das KIM-Clientmodul zu übergebenden Aufruf-Parameter korrekt und vollständig sind und dem jeweiligen Kontext entsprechen. Wir gehen davon aus, dass i.d.R. das Client-System ihres Primärsystems oder der Fachanwendung eine KIM-integrierende Funktion aufweist und die für das Versenden einer KIM-Nachricht erforderliche Funktionalität integriert ist. Ggf. ist es aber erforderlich, ein separates Kommunikationssystem aufzusetzen, dass den ein- und ausgehenden KIM-Nachrichten zentral steuert (z. B. bei ausgehenden Nachrichten automatisiert die Dienstkennung und korrekte KIM-Adressierung vornimmt).

Wenn Sie die Versendung von KIM-Nachrichten über das bei Ihnen etablierte E-Mail-System ermöglichen sollen, müssen Sie festlegen:

- wie der Nutzer einen Empfänger aus dem VZD auswählt und
- wie die für die KIM-Kommunikation erforderlichen Parameter an den E-Mail-Client übergeben werden, um im Rahmen von KIM eine Nachricht über das KIM-Clientmodul versenden zu können. Beispielsweise muss zusätzlich zum Benutzernamen (KIM-Mail-Adresse) der Aufrufkontext für den Konnektor bei

SMTP- bzw. POP3-Login angegeben werden. Dazu müssen Sie festlegen, ob und in welcher Weise Sie diese zusätzlichen, kontextbezogenen Daten in Ihrem E-Mail-System verwalten können (z. B. über Plug-In-Lösungen).

Weiterhin ist zu beachten, dass die KIM-Anwendung ggf. nicht sämtliche E-Mail-Funktionen des bei Ihnen bereits etablierten E-Mail-Systems unterstützt und umgekehrt, auch die Funktion „Zustell- oder Lesebestätigung einfordern" nicht durch alle E-Mail-Clients unterstützt werden.

Beachten Sie auch, dass Sie für das Empfangen und das Versenden von KIM-Nachrichten unterschiedliche Wege und Systeme zwischen Nutzer (und seinem Client-System) und dem KIM-Clientmodul einsetzen können.

4.3.4 Zusammenfassung

Hier noch einmal eine Übersicht der wichtigsten Aspekte, die Sie bei der Einrichtung von KIM beachten sollten:

- Planung und Festlegung des KIM-bezogenen Architekturkonzepts sowie Festlegung einer Einführungsstrategie (inkl. Konnektor- und SMC-B-Architektur).
- Herstellung des Patientenbezugs eingehender KIM-Nachrichten.
- Korrekte, zutreffende Adressierung ausgehender Nachrichten.
- Feststellung des Schutzbedarfs über KIM übermittelten Nachrichten, getrennt nach einkommenden und ausgehenden Nachrichten.
- Festlegung und Umsetzung der Schutzmaßnahmen des KIM Nachrichtenverkehrs, getrennt nach einkommenden und ausgehenden Nachrichten und Integration in das übergreifende Sicherheitskonzept.
- Festlegung der Maßnahmen zur Ausfallsicherheit und Lastverteilung (Konnektor, Kartenterminal, SMC-B).
- Mapping der im VZD geführten und adressierbaren E-Mail-Adressen mit den im Krankenhaus verwendeten E-Mail- oder sonstigen Zieladressen.
- Festlegung der Client-Systeme bzw. Zielpostfächer für die Zustellung einkommender KIM-Nachrichten sowie für die Erzeugung ausgehender KIM-Nachrichten (unter Berücksichtigung automatischer Verarbeitungs- und Erzeugungsvorgänge für ausgewählte Nachrichtentypen gemäß Dienstkennung).
- Bei Weiterverwendung etablierter E-Mail-Postfächer: Mapping der im VZD geführten und adressierbaren E-Mail-Adressen mit den im Krankenhaus verwendeten E-Mail- oder sonstigen Zieladressen und Umsetzung des entsprechenden Routings, ggf. getrennt nach einkommenden und ausgehendem KIM-Nachrichtenverkehr und unter Berücksichtigung der Dienstkennung.
- Festlegung von Verteilern bei Funktionspostfächern z. B. nach Fachrichtung / Abteilung.
- Integration KIM-relevanter Funktionalität bei Nutzung des etablierten E-Mail-Systems zum Empfang und zur Versendung von KIM-Nachrichten (Zugriff auf VZD, kontextbezogene Parameterübergabe, Fehlerhandling, serverseitiges Verwaltungstool).
- Festlegung der Maßnahmen zum IP-Routing (TI-relevanter-Datenverkehr muss über die KIM-Konnektoren geroutet werden).
- Verknüpfung von ausgehenden KIM-Nachrichten mit Patientenbezug und ggf. Ablage in ePA.

4.4 Schutzmaßnahmen ePA

Die Fachanwendung ePA wird für Benutzer in einem Krankenhaus weitestgehend durch das Primärsystem, also das KIS, umgesetzt. Die KIS-Hersteller sind dabei angehalten, die im Implementierungsleitfaden ePA [gemILF_PS_ePA] für die Primärsysteme definierten Anforderungen zu erfüllen. Da die Daten in der ePA Ende-zu-Ende verschlüsselt eingestellt werden, kann beim Herunterladen von Dokumenten aus der ePA eines Versicherten nicht ausgeschlossen werden, dass dort Schadsoftware enthalten ist. Aufgrund der Ende-zu-Ende-Versschlüsselung können die Dokumente jedoch nicht an zentraler Stelle auf mögliche Schadsoftware geprüft werden (z. B. durch den Anbieter des ePA-Aktensystems). Daher kann eine Absicherung gegen mögliche Schadsoftware in heruntergeladenen Dokumenten erst im Primärsystem erfolgen.

Als IT-Dienstleister oder IT-Verantwortlicher des Krankenhauses müssen Sie daher sicherstellen, dass eine Infizierung des Primärsystems und weiterer Systeme durch geeignete Schutzmaßnahmen ausgeschlossen wird. Zwar wird im vorgenannten Implementierungsfaden das Primärsystem dafür verantwortlich gemacht, geeignete Maßnahmen zum Schutz des Primärsystems und der Leistungserbringer-Umgebung durchzuführen, dennoch werden diese Maßnahmen immer erst in Abstimmung mit den IT-Verantwortlichen und Administratoren des Krankenhauses umgesetzt werden können. Geeignete Maßnahmen, bei deren Umsetzung Sie involviert sein können, sind:

- Laden und Extraktion der Dokumente in einer geschützten Umgebung, z. B. einer Sandbox und Untersuchung/Analyse durch geeignete Sicherheits- und Schutzsysteme,
- vor der Anzeige eines Dokumentes Sonder-und Meta-Zeichen im Dokument für die jeweilige Anzeigesoftware mit einer geeigneten Escape-Syntax entschärfen (als Schutz z. B. gegen Injection-Angriffe aus [OWASP Top 10#A1],
- Information der Benutzer, dass Dokumente Schadsoftware enthalten können und welche Maßnahmen der Benutzer zum Selbstschutz vornehmen bzw. beachten muss (Aufnahme in die Sicherheitsbelehrung).

Auch vor dem Hochladen von Dokumenten aus der Umgebung Ihres Krankenhauses in die ePA eines Versicherten kann es ggf. aufgrund von Compliance-Anforderungen erforderlich sein, die Dokumente bzw. deren Inhalte zu überprüfen (Stichwort: data loss prevention). Welche Anforderungen im Detail bestehen und befolgt werden müssen, können die in Ihrem Krankenhaus dazu beauftragten Verantwortlichen bzw. Organisationseinheiten beantworten bzw. Hinweise geben.

Achten Sie darauf, sämtliche für die Fachanwendung ePA zu etablierenden Schutzmaßnahmen in das übergreifende Datenschutz- und Sicherheitskonzept bzw. Information Security Management System (ISMS) Ihres Krankenhauses in Abstimmung mit den entsprechenden Anlaufstellen und Verantwortungsbereichen zu integrieren.

4.5 Wesentliche Betriebsaufgaben und Wartung – Supportaufgaben nach Anschluss an die TI

4.5.1 Firmware-Aktualisierung bei Kartenterminals und Konnektoren

Weder Konnektoren noch Kartenterminals sollten mit veralteter Firmware betrieben werden. Die notwendigen Firmware-Aktualisierungen eines Konnektors bzw. Kartenterminals können manuell oder automatisiert über den **Konfigurationsdienst** (auch: Konfigurations- und Software-Repository, kurz: KSR) durchgeführt werden. Dabei bietet der KSR zusätzlich die Funktion „Aktualisierungsplan". Mit Hilfe des Aktualisierungsplans können Updates noch besser gesteuert werden. Hierbei müssen Sie insbesondere folgende Punkte beachten:

- Führen Sie die Aktualisierung zeitnah durch, wenn der Konnektor/das Kartenterminal eine/n „Software-veraltet"-Meldung/Hinweis anzeigt.
- Installieren Sie Software-Updates erst nach einer entsprechenden Validierung.
- Verwenden Sie ausschließlich freigegebene, offiziell verfügbare, signierte Firmware-Versionen.
- Führen Sie Updates für Konnektor und Kartenterminal(s) bei Bedarf gemeinsam bzw. zeitgleich aus.
- Aktualisieren Sie ggf. die Liste der verfügbaren Bestandsnetze.

Denken Sie daran, dass Sie den Konnektor nur dann aktualisieren, wenn das Primärsystem die Funktionalität, die der Konnektor nach der Aktualisierung anbietet, auch unterstützt. Ggf. muss dazu vorab eine Aktualisierung des Primärsystems vorgenommen werden. Bei Problemen während der Aktualisierung wenden Sie sich an den zuständigen Support und/oder konsultieren Sie das jeweilige Handbuch.

Weitere Informationen zu Herstellern von Kartenterminals und Konnektoren finden Sie unter: https://fachportal.gematik.de/dvo.

4.5.2 Konfigurationsverwaltung von Konnektoren

Die **Konfigurationsverwaltung** eines Konnektors ermöglicht die Sicherung einer bestimmten Konnektorkonfiguration bzw. die Wiederherstellung auf einen gewünschten Stand der Konnektorkonfiguration. Dies ist zum Beispiel dann notwendig, wenn ein Konnektor auf Werkseinstellung zurückgesetzt oder ein Konnektor ausgetauscht wird. Dabei ist der Export bzw. Import von Konfigurationsdaten nur mit entsprechender Berechtigung möglich. Darüber hinaus erfordert jeder Export bzw. Import die Dokumentation im Betriebsführungshandbuch mit Unterschrift des ausführenden Administrators, also im Regelfall Ihre Unterschrift.

Generell müssen Sie mindestens folgende Punkte beim Export von Konnektor-Konfigurationsdaten beachten:

- der Export der Daten erfolgt herstellerspezifisch

und

- das für den Import benötigte Passwort, das auf dem PC-Bildschirm angezeigt wird, muss geschützt notiert oder heruntergeladen werden.

Überdies gelten die herstellerspezifischen Vorgaben.

Generell müssen Sie mindestens folgende Punkte beim Import von Konnektor-Konfigurationsdaten beachten:

- der Import der Daten erfolgt herstellerspezifisch,
- es wird das Import-Passwort abgefragt

und

- ein Neustart des Konnektors ist erforderlich.

Auch hier gelten darüber hinaus die herstellerspezifischen Vorgaben.

4.5.3 Sperrprozess und Außerbetriebnahme eines Konnektors

4.5.3.1 Sperrung eines Konnektors

Wenn ein Konnektor gesperrt werden muss, ist es wichtig, dass Sie so schnell wie möglich handeln. Darum sollten Sie bereits beim Anschluss Ihres Krankenhauses Leistungserbringer (und weitere autorisierte Mitarbeiter) über den Ablauf informieren.

Werden **Manipulationen** am Konnektor (bspw. Beschädigungen am Siegel bzw. Gehäuse des Konnektors) **angenommen** oder wurde der Konnektor **gestohlen**, sollte dies schnellst möglich erkannt werden (können) und dem zuständigen Support mitgeteilt werden. Dies sollten alle Beschäftigten des Krankenhauses, welche physischen Zugang zum Konnektor haben, wissen. Bitte legen Sie auch fest, welche Daten bei entsprechender Meldung bereitgehalten bzw. mitgeteilt werden müssen und welche weiteren Schritte der zutreffende Support einleiten bzw. unternehmen muss. Lesen Sie dazu auch das (Administrator-)Handbuch Ihres Konnektorherstellers bzw. die geltenden VPN-ZugD-Vertragsunterlagen.

Auch bei einer Manipulation wird das weitere Vorgehen vornehmlich durch die Vorgaben im (Administrator-)Handbuch bestimmt. **Bei einem Diebstahl muss jedoch der Konnektor (bzw. die gSMC-K) auf jeden Fall gesperrt werden.** Jeder Konnektor-Hersteller hat zu diesem Zweck einen Sperr-Prozess aufgesetzt. Des Weiteren muss der VPN-Zugangsdienst-Anbieter informiert werden. Auch der VPN-ZugD-Anbieter hat einen Prozess, um den TI-Zugang für einen bestimmten Konnektor zu sperren.

Um die **Sperrung eines Konnektors** einzuleiten, müssen Sie mindestens die **Seriennummer des Konnektors** für die Kommunikation mit dem Konnektorhersteller und **zusätzlich die Vertragsdaten** (Kunden-/Vertragsnummer) für die Kommunikation mit dem VPN-Zugangsdienst bereithalten. **Ggf.** werden die **Daten der SMC-B**, mit der der Konnektor registriert wurde, abgefragt. Der konkrete Sperrprozess kann zwischen den verschiedenen Konnektorherstellern bzw. VPN-ZugD-Anbietern variieren.

4.5.3.2 Außerbetriebnahme eines Konnektors

Bei einer **planmäßigen Außerbetriebnahme** eines Konnektors (z. B. bei einer Fehlfunktion oder einem Modellwechsel) de-registrieren Sie das Gerät gemäß Herstellervorgaben. Anschließend führen Sie einen Reset durch und informieren den VPN-Zugangsdienst-Anbieter.

Sie müssen den de-registrierten und zurückgesetzten Konnektor gemäß den Sicherheitsvorgaben entsorgen. Informieren Sie sich zu diesem Zweck beim jeweiligen Support-Anbieter bzw. beachten Sie die Vorgaben des jeweiligen (Administrator)-Handbuches.

4.5.4 Austausch von Kartenterminals

Stationäre bzw. mobile Kartenterminals müssen ausgetauscht werden, wenn die Sicherheitsvorgaben der TI verletzt werden. Dazu gehören – wie beim Konnektor – Manipulationen am Kartenlesegerät (bspw. Siegel bzw. Gehäuse des Kartenterminals sind beschädigt) sowie Diebstahl. Bei Diebstahl oder Verlust eines Kartenterminals oder einer gSMC-KT allein müssen Sie das Pairing im Konnektor für das betroffene Kartenterminal/die betroffene gSMC-KT aufheben. Dadurch können sich Kartenterminal und Konnektor nicht mehr miteinander verbinden.

Beim Austausch von stationären Kartenterminals müssen Sie mindestens folgende Punkte beachten:

- das Pairing mit dem Konnektor muss aufgehoben werden,

- die gSMC-KT muss entfernt werden,
- das neue KT muss eingerichtet und mit dem Konnektor verbunden werden
- ggf. muss die Konfiguration oder der Softwarestand des KIS aktualisiert werden.

Beim Austausch von mobilen Kartenterminals (mobKT) müssen Sie mindestens folgende Punkte beachten:

- das alte mobKT muss im Primärsystem abgemeldet werden
- das neue mobKT muss im Primärsystem eingerichtet werden.

4.5.5 Hinweise zu möglichen Störungen und deren Beseitigung

Wenn die eGK, der HBA oder die SMC-B nicht wie vorgesehen funktionieren, müssen sich die Inhaber – also Versicherter oder Leistungserbringer – an den 1st-Level-Support des jeweiligen Kartenherausgebers (siehe Kapitel 3.2) wenden.

Fehler können Sie auch mit Hilfe von Logfiles des Konnektors analysieren und beheben. Hierzu sehen Sie bitte im jeweiligen (Administrator-)Handbuch nach.

4.5.6 Ansprechpartner für weitere Fragen zu Komponenten des dezentralen TI-Bereiches

Bei Fragen zu einem Kartenterminal, einem Konnektor oder Ihrem Primärsystem sowie von Releases, Firmware, Versionsständen und Funktionsumfang (Releasenotes) sowie zu Fragen zum Zusammenspiel verschiedener TI-Komponenten im dezentralen TI-Bereich setzen Sie sich bitte mit dem jeweiligen Hersteller oder IT-Dienstleister in Verbindung. Weitere Informationen stehen Ihnen im Fachportal der gematik zur Verfügung (https://fachportal.gematik.de/hersteller-anbieter).

Die gematik wird **nur bei systemischen Fehlern**, also bei reproduzierbaren Fehlern, die im Zusammenspiel eines TI-Produktes mit TI-Komponenten unterschiedlicher Hersteller auftreten, hinzugezogen. Die gematik koordiniert in diesem Fall die Fehleranalyse gemeinsam mit den betroffenen Herstellern bzw. Anbietern. Üblicherweise wird die gematik vom Dienstleister/Anbieter, der Ihr Krankenhaus betreut, informiert. Sollte dies nicht geschehen, erreichen Sie die Experten der gematik unter über das Kontaktformular https://fachportal.gematik.de/kontakt.

5 TI-Anwendungen aus Prozesssicht im Krankenhaus

Bei der Inanspruchnahme von Leistungen im Krankenhaus können drei Varianten unterschieden werden:

1. **Inanspruchnahme stationärer Leistungen** (vollstationär, vor-, nachstationär oder teilstationär):
    a. als zeitlich geplante Inanspruchnahme oder
    b. als ungeplante, z. B. durch einen Notfall veranlasste Inanspruchnahme.
2. **Inanspruchnahme ambulanter Institutionsleistungen des Krankenhauses**:
    a. an Institutsambulanzen des Krankenhauses (insbesondere Hochschulambulanzen, psychiatrische Institutsambulanzen, sozialpädiatrische Zentren etc.),
    b. als ambulante Notfallbehandlung.
3. **Inanspruchnahme ambulanter Leistungen ermächtigter Krankenhausärzte:**

Aus diesen Varianten können Szenarien (Prozessabläufe) abgeleitet werden, deren mögliche Interaktion mit den Anwendungen der TI im Folgenden betrachtet wird.

Tabelle 3: Mögliche Verwendung von TI-Anwendungen in den verschiedenen Szenarien

Szenario	VSDM	NFDM	eMP/AMTS	ePA	KIM	E-Rezept
Patient wird in der Notaufnahme aufgenommen.		X	X	X		
Elektiver Patient wird stationär aufgenommen (medizinische Aufnahme).	X	(X)	X	X		
Patient wird entlassen (Entlassmanagement)			X	X	X	X

5.1 Szenario: Patient wird in der Notaufnahme aufgenommen

In diesem Szenario erfolgt im Krankenhaus initial meist eine Klassifikation nach dem Manchester-Triage-System. Ein Patient, der mit der Triagestufe „grün" klassifiziert wurde, kann seinen „grundsätzlichen" Gesundheitszustand über eine Einsicht in die ePA an den behandelnden Arzt vermitteln. Während dieser Phase der Behandlung ergäbe sich damit die Nutzung von Notfalldaten, Medikationsdaten und Ärztebriefe sowie weitere Dokumentarten.

5.1.1 NFDM

Im Falle, dass ein Patient mit der Triagestufe „rot" klassifiziert wird (nach Manchester Triage System – MTS), kann ein schneller und sicherer Zugriff auf den NFD der eGK erfolgen (siehe nachfolgende Abbildung).

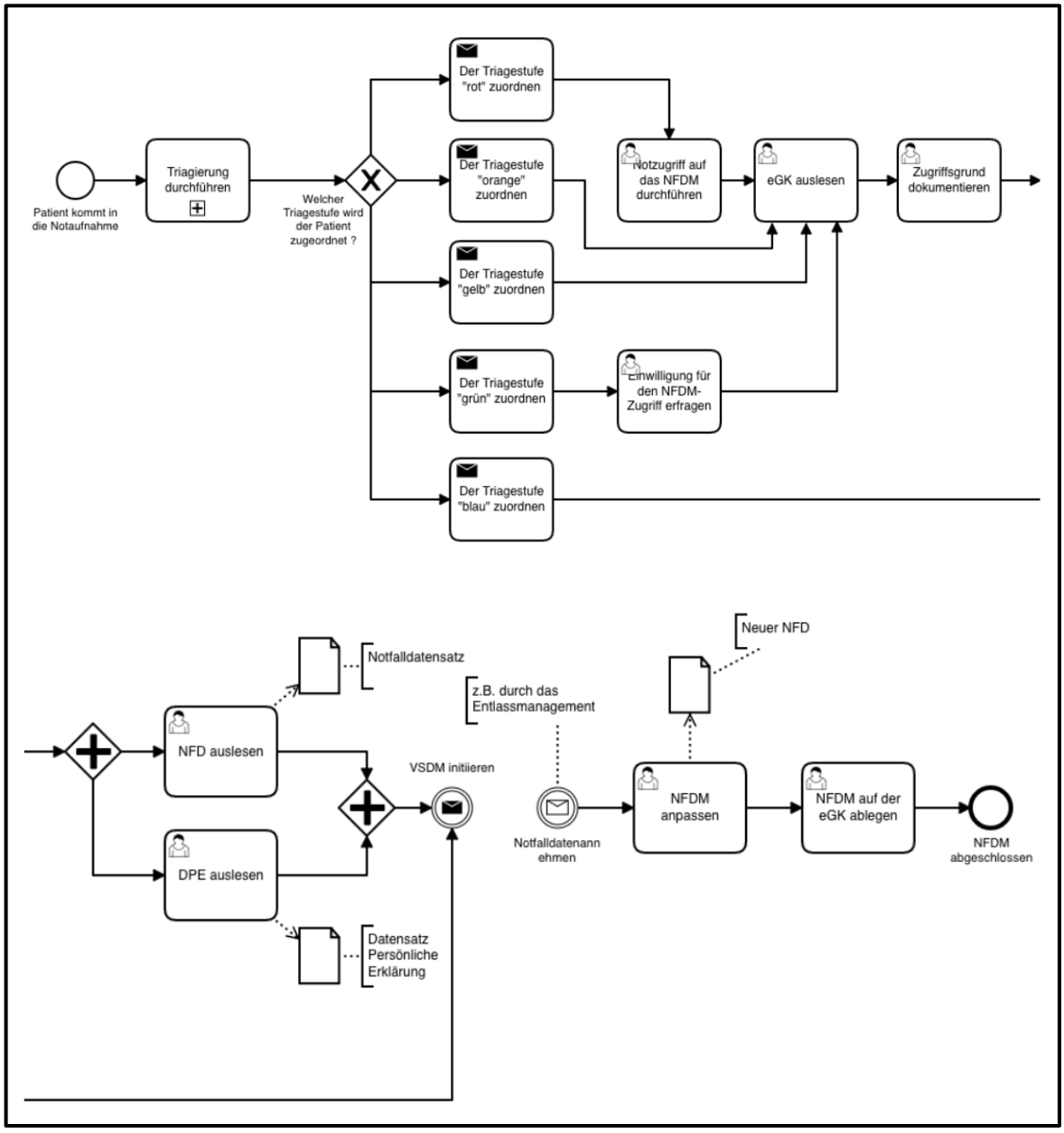

Abbildung 19: NFDM-Zugriff in der Patientenaufnahme (Bsp.)

Mittels NFDM erhält der Arzt sofort Zugriff auf die notfallrelevanten medizinischen Informationen des Patienten, die zur Abwendung eines ungünstigen Krankheitsverlaufs genutzt werden können.

Mit dem NFD soll eine möglichst gezielte Diagnostik und Therapie unterstützt werden. Das ist insbesondere dann von Vorteil, wenn für die Behandlung anamnestische Angaben entscheidend sind, die sonst nicht oder nicht vollständig erhoben werden können.

Ebenfalls ist es in diesem Szenario dann möglich, auf den DPE Informationen über das Bestehen und den Ablageort von Patientenverfügung, Vorsorgevollmacht und dem Organspendeausweis zu erhalten.

5.1.2 ePA

Um eine Berechtigung auf die Dokumente in die ePA zu bekommen, ist es notwendig, eine Einwilligung vom betreffenden Patienten einzufordern und ihn über dieses Vorhaben aufzuklären. Die Berechtigung kann über eine Ad-hoc-Berechtigung im jeweiligen KIS-Modul erfolgen. Dafür ist es notwendig, die eGK in ein eHealth-KT zu stecken und vom Patienten eine Ad-hoc-Berechtigung inkl. Angabe der Berechtigungsdauer anzufordern.

Der Patient bestätigt diese Anfrage über ePA-FdV und entscheidet, ob die Zugriffberechtigung für ausgewählte oder alle Dokumente freigegeben wird. Mit dem „Institutionsmodell" (siehe Kapitel 3.2.2.4), kann der Patient einen flächendeckenden Zugriff innerhalb der Institution auf die Dokumente seiner ePA gewähren.

Bei dem Abrufen von freigegebenen Dokumenten sollten diese aus Gründen der Nachweisbarkeit in die Primärdokumentation überführt werden, da die Daten nur bedingt persistent vom Patienten gehalten oder zur Verfügung gestellt werden.

Im Verlauf der weiterführenden Behandlung innerhalb des Krankenhauses können die neuen Dokumente (wie Arztbriefe) in die ePA eingestellt werden.

5.2 Szenario: Elektiver Patient kommt in die stationäre Aufnahme

5.2.1 VSDM

Die Aktualitätsprüfung der VSD kann im Kontext der Patientenaufnahmeanwendung im KIS erfolgen (siehe Abbildung 20). Dazu sind in den Organisationsbereichen des Krankenhauses geeignete Patientenaufnahmearbeitsplätze erforderlich, z. B.:

- zentrale Patientenaufnahme,
- dezentrale Patientenaufnahme (Station, Notaufnahme) und
- Ambulanzen, sofern dort eine Aufnahme zur stationären Weiterbehandlung erfolgt.

Die Durchführung einer Aktualitätsprüfung kann für einzelne Arbeitsplätze konfiguriert werden und dabei die arbeitsteilige Prozessgestaltung in Krankenhäusern gewährleisten. Wenn die Gültigkeitsprüfung der eGK und Aktualisierung der VSD bei jeder Krankenhausaufnahme durchgeführt wird, liegen aktuelle Versicherteninformationen und Informationen zum Status des Versichertenverhältnisses wesentlich frühzeitiger vor als über die Routinedatenübermittlung nach § 301 SGB V. Das frühzeitige Vorliegen von aktuellen Informationen zum Versicherungsstatus bietet auch in solchen Fällen einen Prozessvorteil, in denen bei der Aufnahme des Patienten die Verteilung in den stationären oder ambulanten Bereich erst noch aussteht. Das Einlesen der VSD ist ein optionaler administrativer Prozess, der im Krankenhaus in der Regel getrennt von medizinischen Prozessen ausgeführt wird, aber durchaus auch in medizinischen Organisationsbereichen (z. B. auf den Stationen) erfolgen kann.

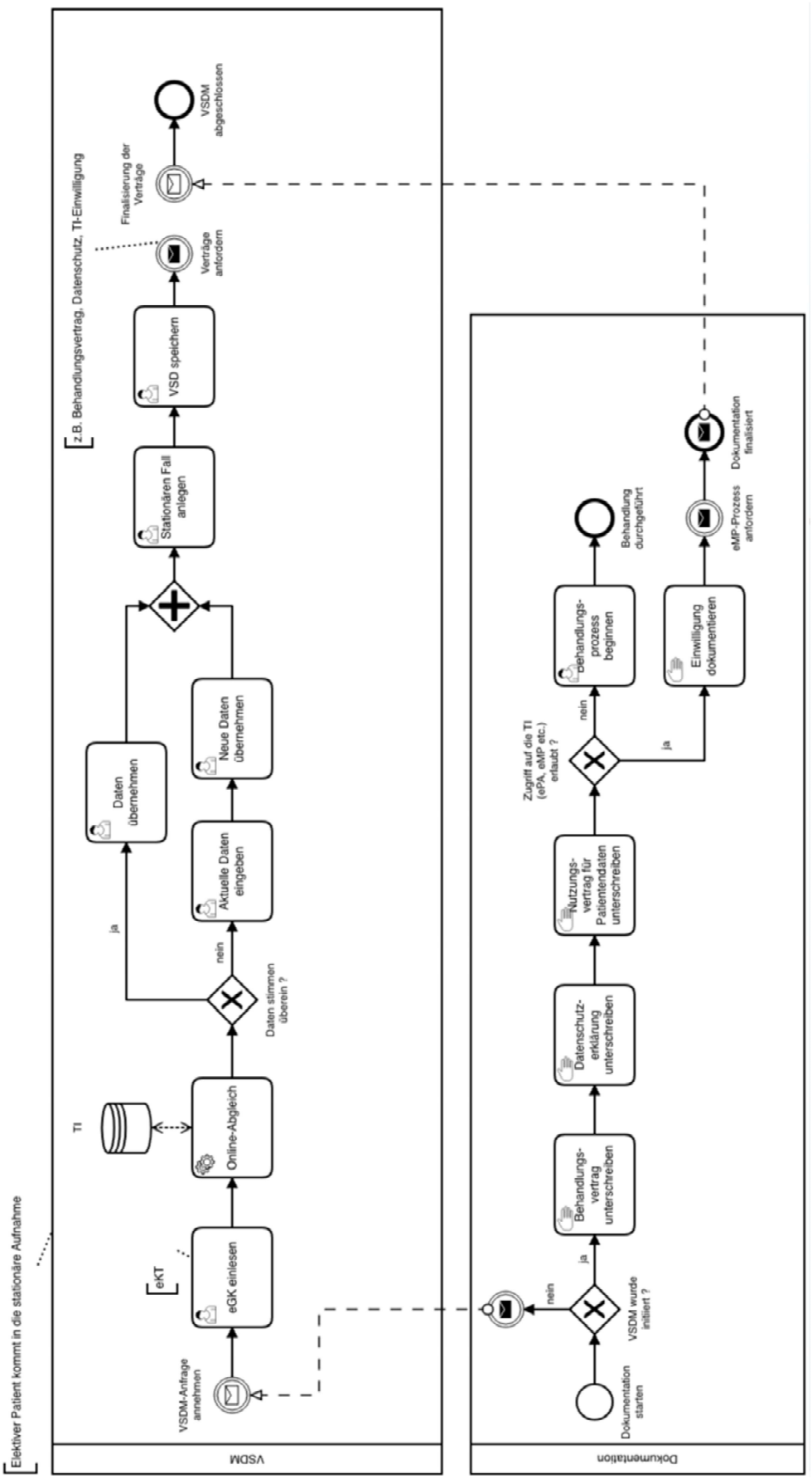

Abbildung 20: VSD-Abgleich und Dokumentation in der Patientenaufnahme (Bsp.)

Nach Aktualitätsprüfung der eGK und Einlesen der VSD ist eine Datenübernahme in die Patientendatenverwaltung erforderlich, um als Grundlage für die weitere Leistungsdokumentation und spätere Abrechnung dienen zu können.

Eine Konfiguration der Frequenz der Online-Prüfung, die auch bei Folgebesuchen im Quartal die Authentizität der eGK online prüfen lässt, ist geeignet, Missbrauch zu vermeiden.

Zum Nachweis der durchgeführten Online-Prüfung wird ein Prüfungsnachweis erzeugt. Gemäß § 291a Abs. 1 SGB V sind auch die im Krankenhaus an der vertragsärztlichen Versorgung teilnehmenden Ärzte und Einrichtungen bei der erstmaligen Inanspruchnahme ihrer Leistungen durch einen Versicherten im Quartal angehalten, die Gültigkeit der eGK und Aktualität der darauf gespeicherten Versichertendaten zu prüfen. Die Durchführung der Prüfung wird auf der eGK gespeichert (Prüfnachweis) und ist Bestandteil der an die kassen(zahn)ärztliche Vereinigung zu übermittelnden Abrechnungsunterlagen.

Die Prüfung auf Notwendigkeit einer Aktualisierung der eGK sowie eine ggf. erforderliche Aktualisierung kann – nach entsprechender Konfigurationseinstellung – beim Einlesen der eGK vollautomatisch ohne Nutzerinteraktion durchgeführt werden. Anhand aktualisierter Versichertenstammdaten der eGK können erneuerte Daten (z. B. Versicherungsstatus, Adresse) ins KIS übernommen werden.

5.2.1.1 Technische Rahmenbedingungen

Die Unterstützung der Inanspruchnahme von Leistungen des VSDM erfolgt in einer Konfiguration, die alle eGK-Kartenzugriffe SMC-Bs zuordnet, die für Mandanten stehen.

Die Mandantenkonfiguration am Konnektor muss bei Bedarf geeignet sein, die drei Szenarien der Leistungsinanspruchnahme zu unterstützen. Die Arbeitsplatzverwaltung von Konnektor und Primärsystem (KIS) muss insbesondere in Bezug auf die Mandanten konfiguriert werden (siehe Kapitel 4.2.4).

Eine Abbildung der Mandanten auf die interne Mandantenverwaltung des Krankenhauses ist ratsam. Insbesondere muss an Kontaktpunkten im Krankenhaus, an denen über Kartenterminals VSD eingelesen werden, die SMC-B des jeweils zuständigen Mandanten erreichbar sein. Falls es eine Mehrzahl von Mandanten gibt, muss eine Auswahl zwischen den betroffenen Mandanten über das KIS erfolgen können. Bei einer dezentralen Aufnahmeorganisation im Krankenhaus oder bei nächtlichen stationären Aufnahmen oder Aufnahmen an Wochenenden kann es spezielle Arbeitsplätze geben, bei denen eine Auswahl unter mehreren Mandanten standardmäßig an einem einzelnen speziellen Arbeitsplatz erforderlich ist.

5.2.2 Elektronischer Medikationsplan (eMP/AMTS)

Im Rahmen der Aufnahme der medizinischen Daten eines Patienten im Krankenhaus (z. B. im Vorfeld einer stationären Behandlung) macht es ggf. Sinn, einen auf der eGK des Patienten vorhandenen eMP auszulesen und in das Primärsystem zu überführen, so dass diese Daten für den weiteren Behandlungsverlauf genutzt werden können. Im Verlauf der Behandlung kann der Leistungserbringer dann entscheiden, ob eine Aktualisierung der eMP-Daten erforderlich ist und diese – in Abstimmung mit dem Patienten – entsprechend veranlassen (beispielsweise im Rahmen des Entlassmanagements). Verfügt der Patient noch über keinen eMP auf seiner eGK, kann der Leistungserbringer, falls die Behandlung dies medizinisch ermöglicht und eine weitergehende Medikation erforderlich ist, in Abstimmung mit dem Patienten einen entsprechenden Datensatz anlegen.

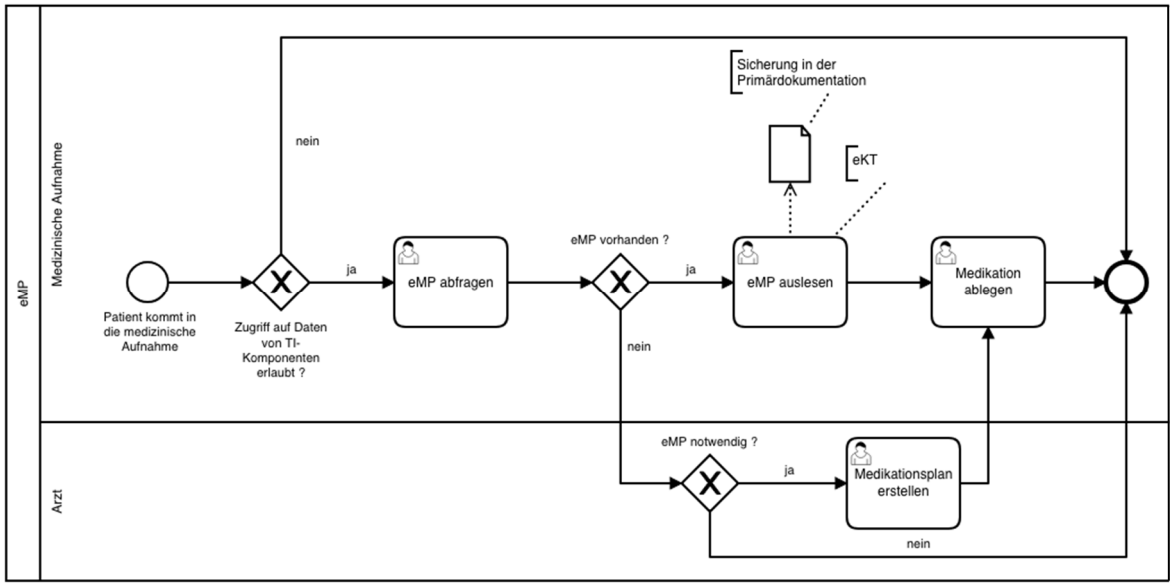

Abbildung 21: eMP bei der medizinischen Aufnahme (Bsp.)

5.2.3 ePA

Zum Zeitpunkt der stationären Aufnahme eines Versicherten ist es möglich, dass dieser Zugriffrechte auf seine ePA erteilt (TI-Einwilligung). In dieser Phase der Behandlung ergibt sich die Möglichkeit, Einsicht in vorhandene Dokumentationen über den Krankheitsverlauf zu erlangen. Freigegebene Daten sollten nach Möglichkeit in die Primärdokumentation überführt werden.

Die Freigabe der Dokumente kann, je nach Struktur des Krankenhauses, einer oder mehreren fachärztlichen Stationen zugewiesen werden, oder aber dem gesamten Krankenhaus im Rahmen einer einmaligen Freigabeprozedur (siehe Kapitel 3.2.2.3. f.).

Die im Verlauf der Behandlung erstellten Dokumentationen können ebenfalls simultan zu der Behandlung oder im Rahmen des Entlassmanagements in die ePA über das KIS-Modul geschrieben werden (siehe Abbildung 22 auf der nächsten Seite).

5.2.3.1 Technische Rahmenbedingungen

Für die o.g. ePA-Anwendungsfälle ist es nicht erforderlich, einen HBA zu nutzen. Dennoch kann für das Einstellen von Dokumenten optional eine Signierung mittels dem HBA durchgeführt werden. Eine Berechtigungsvergabe auf Dokumente der ePA ist nur dann umsetzbar, wenn der Patient die Berechtigung direkt auf dem Frontend seines Smartphones vornimmt (über die entsprechende App).

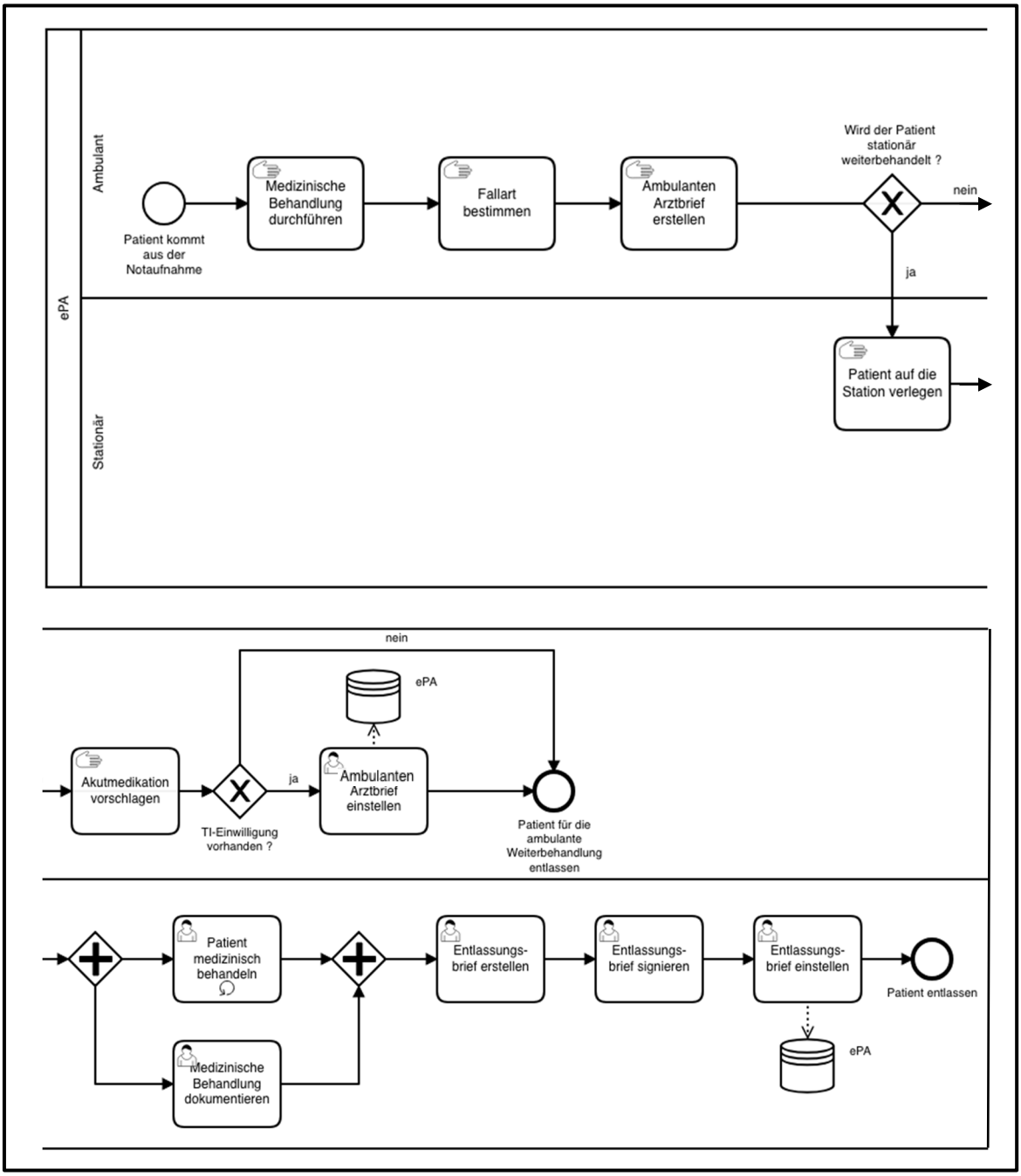

Abbildung 22: Dokumente in ePA einstellen (Bsp.)

5.3 Szenario: Ein Belegarzt führt eine Operation in einem Belegklinikum durch

Unabhängig davon, welche TI-Anwendungen von einem Belegarzt genutzt werden, sollte die Anwendung mittels einer separaten SMC-B und einer vom Krankenhaus abweichenden Telematik-ID erfolgen und organisatorisch vom Rest des Krankenhauses trennbar sein.

5.4 Szenario: Ein Patient erhält bei seiner Entlassung ein Entlassrezept

Zum Zeitpunkt der Entlassung eines Patienten kann im Rahmen des Entlassmanagements ein Entlassrezept in Form eines E-Rezeptes ausgestellt werden.

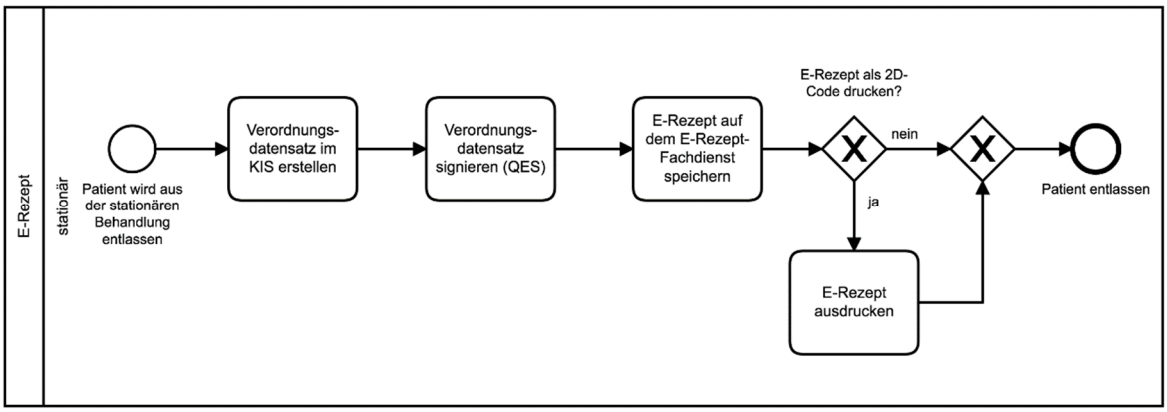

Abbildung 23: Prozess des E-Rezeptes im Entlassmanagement (Bsp.)

Um ein E-Rezept zu erzeugen, wird im KIS ein Verordnungsdatensatz erstellt. Zur Erstellung der Signatur wird der Verordnungsdatensatz um eine über die TI bezogene Rezept-ID ergänzt. Die qualifizierte elektronische Signatur (QES) kann ein Leistungserbringer ausschließlich per HBA erzeugen, nicht per SMC-B. Dabei kann die Einzel-, Stapel- oder Komfortsignatur genutzt werden. Anschließend wird das E-Rezept auf dem E-Rezept-Fachdienst gespeichert. Der Patient kann das E-Rezept in einer Apotheke seiner Wahl einlösen. Soll optional ein Ausdruck des E-Rezeptes für den Patienten erstellt werden, wird im KIS ein E-Rezept-Token erzeugt, das dann im Krankenhaus als 2D-Code zusammen mit weiteren Zusatzinformationen ausgedruckt werden kann.

Die Informationen des E-Rezeptes können im Rahmen des Entlassmanagements in den elektronischen Medikationsplan (eMP) übernommen werden (siehe Kap. 5.2.2).

5.5 Szenario: Ambulante Behandlung eines Patienten mit Zytostatika oder parenteralen Zubereitungen

Für die Behandlung erstellt ein Arzt einen Therapieplan und verordnet mit Hilfe des E-Rezepts die für die Behandlung notwendigen Medikamente. Die Verordnung selbst unterscheidet sich hierbei nicht vom Ablauf der Entlassrezepte.

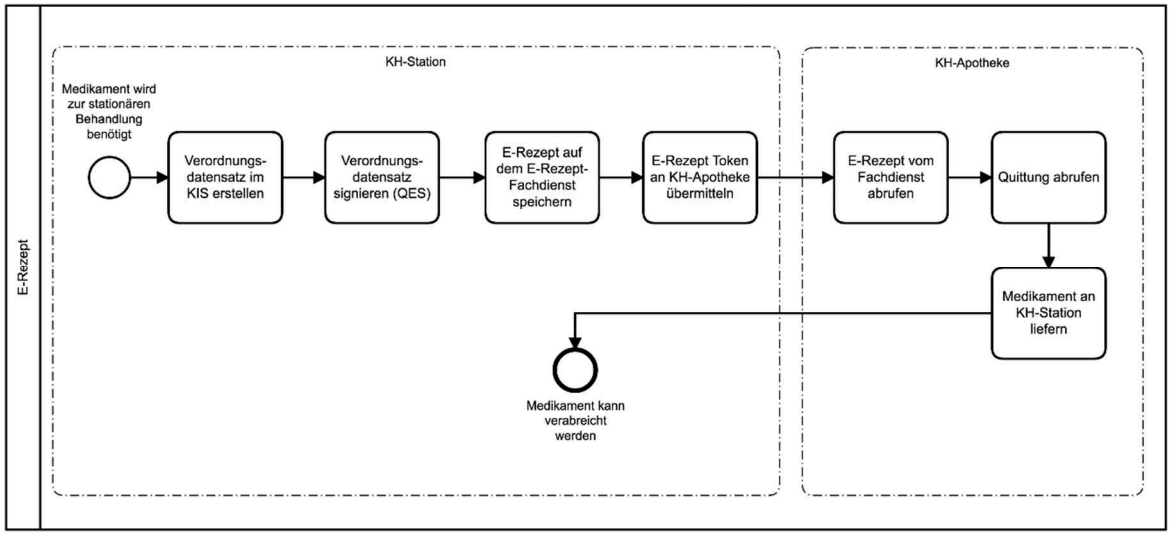

Abbildung 24: Beispielhafter Prozess des E-Rezeptes zur Behandlung mit Zytostatika oder parenteraler Zubereitung

Einen Sonderfall stellen E-Rezepte für die ambulante Behandlung eines Patienten mit Zytostatika und parenteralen Zubereitungen dar. Diese werden nicht von Patienten in die Apotheke überbracht und eingelöst, sondern der Token für diese E-Rezepte wird direkt vom behandelnden Arzt an die Apotheke übermittelt. Für die Übersendung des Tokens kann ein sicheres Verfahren der TI (z.B. KIM) verwendet werden. Im Kontext des Krankenhauses sind auch weitere Übertragungswege über das KIS möglich.

Die Apotheke liefert das Medikament an den behandelnden Arzt aus, der anschließend das Medikament verabreicht. Der Patient verzichtet an dieser Stelle auf sein Recht der freien Apothekenwahl. Dies ist im Behandlungsvertrag zwischen Patient und Krankenhaus festzulegen.

Sofern die Apotheke, die das E-Rezept gegenüber der Krankenkasse abrechnet, nicht zugleich auch die Apotheke ist, die das Medikament herstellt, ist weiterhin die Dokumentation der herstellenden Apotheke zu beachten. Die Informationen zur Herstellung werden künftig nicht mehr auf dem Rezept abgedruckt, sondern elektronisch an die abrechnende Apotheke übergeben. Die Details zu den Inhalten und zur Übergabe der Informationen werden zwischen GKV-SV und DAV unter Einbeziehung der DKG festgelegt. Die Abrechnung von E-Rezepten findet nicht im Rahmen der Fachanwendung E-Rezept über die TI statt.

5.6 Szenario: Übersendung von Entlassdokumentation bei der (Rück-) Einweisung eines behandelten Patienten in eine Pflegeeinrichtung

Wird ein Patient nach einer Krankenhausbehandlung direkt (wieder) in eine Pflegeeinrichtung übergeben überstellt, erstellt das Krankenhaus die notwendige Entlassdokumentation bzw. einen Pflegeüberleitungsbogen. Diese enthalten u. a. relevante Daten zur Behandlung des Patienten, Informationen zum Vitalzustand oder auch wichtige Hinweise für die weitere Betreuung in der Pflegeeinrichtung. Diese Informationen werden via KIM direkt an die aufnehmende Pflegeeinrichtung und parallel an den behandelnden Hausarzt versendet.

Idealerweise haben sich Krankenhaus und Pflegeeinrichtung auf eine standardisierte Datenstruktur geeinigt, so dass die Informationen auch direkt in das Primärsystem der aufnehmenden Einrichtung eingelesen werden können.

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
aAdG	andere Anwendungen des Gesundheitswesens
aAdG-NetG	andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens
aAdG-NetG-TI	Andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens
ALG	Application Layer Gateway
AMTS	Arzneimitteltherapiesicherheit
API	Application Programming Interface
C2C	card to card (Authentifizierungsverfahren)
DKTIG	Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH
DVO	Dienstleister vor Ort
eAU	elektronischen Arbeitsunfähigkeitsbescheinigung
eGK	elektronische Gesundheitskarte
eH-KT	eHealth-Kartenterminal (stationär)
eMP	elektronischer Medikationsplan
E-Rezept	Elektronisches Rezept
FAD	Fachanwendungsspezifischer Dienst
FHIR	Fast Healthcare Interoperability Resources
FQDN	Fully Qualified Domain Name
gSMC-K	gerätespezifische Security Module Card – Typ Konnektor
gSMC-KT	gerätespezifische Security Module Card – Typ Kartenterminal
HBA	Heilberufsausweis
HL7	Health Level Seven International
IAG	Internet Access Gateway
ICCSN	Integrated Circuit Card Serial Number
KIM	Kommunikation im Medizinwesen (vormals KOM-LE)
KIS	Krankenhausinformationssystem
KOM-LE	siehe KIM
KSR	Konfigurations- und Software-Repository
MobKT	Kartenterminal, mobiles
NFD	Notfalldaten
NFDM	Notfalldatenmanagement
OCSP	Online Certificate Status Protocol
OWASP	Open Web Application Security Project
PN	Prüfnachweis

Kürzel	Erläuterung
PVS	Praxisverwaltungssystem (wird in diesem Dokument synonym zu Primärsystem und KIS verwendet)
SIS	Sicherer (oder Secure) Internet Service
SMC-B	Security Module Card – Typ B (Institutionskarte)
SPOC	Single-Point-of-Contact
SÜV	Sicheres Übermittlungsverfahren (siehe KIM)
TI	Telematikinfrastruktur
TI-ITSM	IT-Service-Management der TI
TSP	Trust Service Provider
VPN-ZugD	VPN-Zugangsdienst
VSD	Versichertenstammdaten
VSDM	Versichertenstammdatenmanagement
WANDA	Weitere Anwendungen (siehe auch aAdG, aAdG-NetG, aAdG-NetG-TI)
WOP	Wohnortprinzip

A2 – Glossar

Das vollständige Glossar finden Sie auf der Homepage der gematik (siehe gematik.de/glossar). Dieses kann auch vollständig als pdf-Datei heruntergeladen werden.

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 – Referenzierte Dokumente

A5.1 – Dokumente der gematik

[Quelle]	Herausgeber: Titel (jeweils in der aktuell veröffentlichten Version)
[gematik_Checkliste_DVO]	gematik: Checkliste Dienstleister vor Ort
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemILF_PS]	gematik: Implementierungsleitfaden Primärsysteme
[gemILF_PS_AMTS]	gematik: Implementierungsfaden Primärsysteme – elektronischer Medikationsplan/AMTS-Datenmanagement
[gemILF_PS_ePA]	gematik: Implementierungsfaden Primärsysteme – Elektronische Patientenakte (ePA)
[gemILF_PS_eRp]	gematik: Implementierungsleitfaden Primärsysteme – E-Rezept
[gemILF_PS_NFDM]	gematik: Implementierungsfaden Primärsysteme – Notfalldaten-Management (NFDM)
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemKPT_Betr]	gematik: Betriebskonzept Online Produktivbetrieb
[gemSpec_Aktensystem]	gematik: Spezifikation des Aktensystems
[gemSpec_FD_eRp]	gematik: Spezifikation E-Rezept-Fachdienst
[gemSpec_Kon]	gematik: Spezifikation Konnektor
[gemSpec_VPN-ZugD]	gematik: SpezifikationVPN-Zugangsdienst
[gemSysL_eRp]	gematik: Systemspezifisches Konzept E-Rezept
[gemSysL_NFDM]	gematik: Systemspezifisches Konzept Notfalldaten-Management (NFDM)

A5.2 – Anlagen und Internetreferenzen

[Quelle]	Herausgeber: Titel, Link
Anlage 1 zum Kapitel „Vorbereitung und Durchführung“	gematik: „Checkliste Dienstleister vor Ort“, abrufbar unter https://fachportal.gematik.de/dvo/

[Quelle]	Herausgeber: Titel, Link
Anlage 3 zum Kapitel 4.2.2	gematik: „Hinweise zu den Betriebsarten für Konnektoren“, abrufbar unter https://fachportal.gematik.de/informationen-fuer/krankenhaeuser
Informationsmaterialien zum Online-Produktivbetrieb	gematik: „Allgemeine Informationsmaterialien zum Online-Produktivbetrieb “, abrufbar unter https://www.gematik.de/mediathek/publikationen/
Konzepte und Spezifikationen der gematik	https://fachportal.gematik.de/downloadcenter
Webauftritte der gematik	www.gematik.de fachportal.gematik.de
HL7	hl7.de
OWASP	owasp.org/www-project-api-security/