Anschluss medizinischer Einrichtungen an die Telematikinfrastruktur – Ein Überblick für Dienstleister vor Ort (DVO)

Version:	2.4.0
Revision:	
Stand:	11.07.2022
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemInfo_Anschluss_TI_DVO]

Dokumentinformationen

Änderungen zur Vorversion

Die Änderungen zur Vorversion können Sie der nachfolgenden Übersicht entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	21.03.18		freigegeben	gematik
			Ergänzung von Informationen zur neuen Prüfkarte eGK in den Kapiteln 3.2.6 und 4.4	gematik
2.0.0	12.10.18		freigegeben	gematik
2.1.0	24.10.18		Korrekturen in Kapitel 3.2.6 und 4.4	gematik
2.2.0	28.08.19		Aktualisierung der referenzierten Links. Ergänzungen zum Thema IT-Sicherheit in den Kapiteln 4.2 und 4.2.1 sowie zum Thema Netzwerk im Kapitel 4.3.1	gematik
2.2.1	20.11.19		Ergänzung im Kapitel 4.2 „Allgemeine Sicherheitshinweise für die Installation in der Leistungserbringerumgebung“	gematik
2.3.0	02.06.21	4.2.2,4.3.4	Ergänzung Konfiguration des Informationsmodells (KIM, E-Rezept) Hinweis zur Konfiguration im Netzwerk allgemeine Aktualisierung von Abbildungen, Verlinkungen und Paragraphen im gesamten Dokument	gematik
2.4.0	11.06.22		Korrekturen in Kapitel 1.1.1, 2.1 und A5.2	gematik

Hinweise zum Dokument

„Anschluss medizinischer Einrichtungen an die Telematikinfrastruktur – Ein Überblick für Dienstleister vor Ort (DVO)“ richtet sich an Dienstleister, die von **Leistungserbringern**, bspw. von Ärzten, mit dem Anschluss an die Telematikinfrastruktur bzw. dem damit zusammenhängenden IT-Support beauftragt werden.

Das vorliegende Dokument gibt Ihnen eine erste Übersicht über die Rolle bzw. Aufgaben eines Dienstleisters vor Ort, erklärt die Grundzüge der Telematikinfrastruktur und stellt kurz die gematik vor. Überdies finden Sie hier grundlegende Informationen zur Installation

bzw. Inbetriebnahme von Konnektoren. Abschließend erfahren Sie mehr über Betriebsaufgaben und Wartungsaspekte.

Wenn Sie sich für Detailfragen interessieren, geben Ihnen blaue Infoboxen am Ende eines Themenabschnittes eine Übersicht über weiterführende Informationen, bspw. in Spezifikationen und Konzepten der gematik.

Beachten Sie, dass dieses Dokument **nicht** die Lektüre von (Administrator-) Handbüchern, die u. a. im Lieferumfang von Konnektoren enthalten sind, **ersetzt**.

Da Krankenhäuser in der Regel über eine IT-Abteilung verfügen, die den Anschluss an die Telematikinfrastruktur ohne externe Dienstleister einrichtet, geht das Dokument nicht explizit auf diesen Leistungserberbringer ein. Ungeachtet dessen sind die Angaben in diesem Dokument auch für diesen Leistungserbringer weitgehend übertragbar.

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

Inhaltsverzeichnis

1 Der DVO als Supportdienstleister im dezentralen Bereich der Telematikinfrastruktur

1.1 Einleitung

Als Dienstleister vor Ort, kurz: DVO, spielen Sie bei der Digitalisierung des deutschen Gesundheitswesens eine wesentliche Rolle: Sie schließen Praxen von Ärzten, Zahnärzten und psychologischen Psychotherapeuten an die Telematikinfrastruktur (TI) an. Mit diesem Ziel gehen verschiedene Aufgaben einher. Einen Überblick über diese Aufgaben finden Sie im Kapitel 1.1.1.

Als DVO sind Sie in der Regel auf selbstständiger Basis tätig. Sie erhalten Aufträge zum Anschluss an die TI von **Leistungserbringern** (LE), also bspw. Ärzten, Zahnärzten und psychologischen Psychotherapeuten.

1.1.1 DVO – Rollenverständnis und Aufgaben

Die Bezeichnung **Dienstleister vor Ort** dürfen nur Personen führen.

Wenn Sie mit der Einrichtung eines TI-Zuganges beauftragt werden, zählen zu Ihren Hauptaufgaben:

- die Planung und Vorbereitung eines Vor-Ort-Termins (inklusive der Beschaffung der notwendigen dezentralen TI-Komponenten (s. dazu auch 3.1), falls vom Leistungserbringer gewünscht),
- die Installation und Inbetriebnahme von dezentralen TI-Komponenten (insbesondere von Konnektoren und Kartenterminals, s. Kapitel 3.2.4 und 3.4),
- die Dokumentation der Installation bzw. Inbetriebnahme,
- die Wartung von dezentralen TI-Komponenten sowie
- die Störungssuche, -meldung und ggf. -beseitigung.

Sie sind – neben Ihren allgemeinen IT-Support-Aufgaben – zudem dafür zuständig, Störungen im **dezentralen Bereich der TI** (s. auch Kapitel 2.2) zu beheben. Bei Störungen im **zentralen Bereich der TI** müssen Sie sich, insofern Sie selbstständig tätig sind, an den User Helpdesk des **VPN-Zugangsdienstes**[1] (s. Kapitel 4.3.1) wenden.

Aufgrund Ihres Aufgabenprofils sind Sie auch Ansprechpartner für Leistungserbringer und deren Mitarbeiter für die unterschiedlichsten Fragen zur TI. Hier kann es hilfreich sein, bspw. das Informationsmaterial der gematik zu kennen. Es ist abrufbar unter: https://www.gematik.de/newsroom/mediathek

[1] Beachten Sie, dass der Leistungserbringer Vertragspartner des VPN-Zugangsdienstanbieters ist.

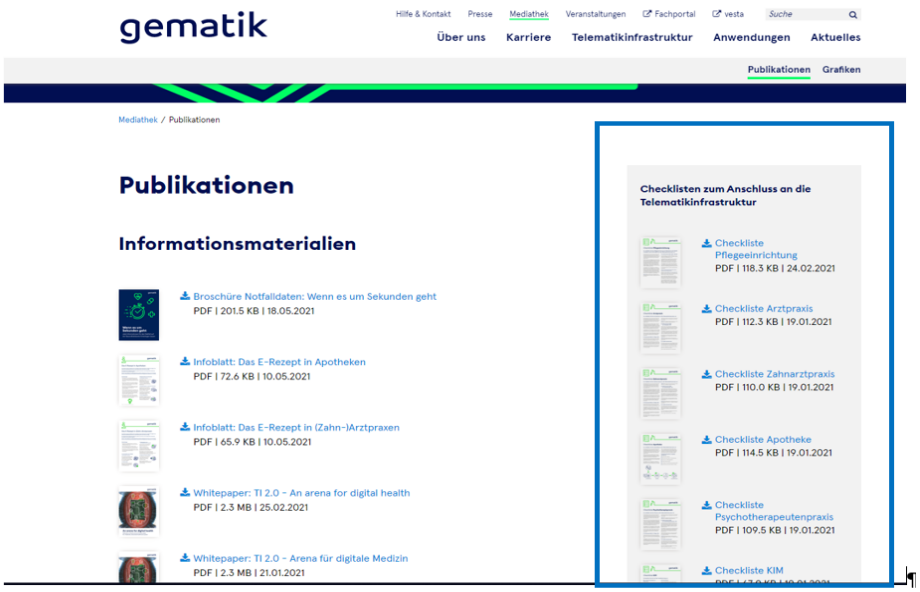

Abbildung 1: Beispielhafter Ausschnitt des gematik-Webauftrittes mit Überblick über das allgemeine Informationsmaterial zum Online-Produktivbetrieb für Leistungserbringer (Stand: Juni 2021)

Grundsätzlich gilt: Wie weit sich Ihr Verantwortungsbereich im Detail erstreckt, wird individuell vertraglich zwischen Ihnen und dem Leistungserbringer geregelt.

1.1.2 Erforderliche Fachkenntnisse eines DVO

Um als (selbstständiger) Dienstleister vor Ort tätig zu werden, benötigen Sie keine gesonderte Zertifizierung. Dennoch sollten mindestens die nachfolgenden Kenntnisse zu Ihrem Fachrepertoire gehören:

- Kenntnisse der typischen IT-Infrastruktur in **Leistungserbringerinstitutionen** (LEI), z. B. Arzt- und Zahnarztpraxen)
- Kenntnisse der Installation/Funktionsweise gängiger Primärsysteme[2] in Leistungserbringerinstitutionen; Erfahrung in der Softwareimplementierung medizinischer Verwaltungssysteme von Vorteil
- Erfahrung in der Netzwerktechnik und mit Netzwerkprotokollen
- Kenntnisse in der Absicherung von Netzwerkumgebungen
- Kenntnisse der Datenschutzbestimmungen sowie
- Erfahrung in der strukturierten Analyse und Behebung von Fehlern.

1.1.3 Überblick über die Supportstruktur der TI

Ein wesentlicher Bestandteil der Telematikinfrastruktur ist deren dienstleisterübergreifende Supportstruktur. Um als DVO Ihre Supportaufgaben in vollem Umfang wahrnehmen zu können, sollten Sie die TI-Supportstruktur kennen.

[2] IT-Systeme, die bei einem Leistungserbringer eingesetzt werden und sich unter dessen administrativer Hoheit befinden, werden im TI-Kontext als Primärsysteme bezeichnet. Dazu gehören Praxisverwaltungssysteme (PVS), Apothekenverwaltungssysteme (AVS) oder Krankenhausinformationssysteme (KIS).

Die Supportstruktur sieht vor, dass unterschiedliche TI-Komponenten (s. auch Kapitel 3) von verschiedenen Rollen angeboten bzw. betrieben werden können. Diese Rollen unterteilen sich im Wesentlichen in:

- **Anbieter**
  (Anbieter sind Unternehmen, die Dienste/Services für Anwender oder andere Servicenehmer offerieren, welche sie gegenüber dem Anwender/Servicenehmer verantworten.)

und

- **Hersteller**
  (Hersteller sind Unternehmen, die ein TI-Produkt, also Geräte oder Software, gemäß den Spezifikationen der gematik (s. auch Kapitel 2.1) herstellen. Hersteller übernehmen die Produkthaftung gemäß den gesetzlichen Vorgaben sowie den Produkt-Support. Sie unterscheiden sich von Anbietern insbesondere dadurch, dass das verantwortete Produkt kein IT-Service ist.)

Die betriebliche Koordination dieser Rollen liegt in der Verantwortung der gematik.

Die Supportstruktur ermöglicht die schnelle Bearbeitung von Störungen. Dies erfolgt über den 1st- und 2nd/3rd-Level-Support, wobei der 1st-Level-Support auch als Anwendersupport bezeichnet wird.

Der Leistungserbringer (Anwender) hat dabei die Wahl,

- den Anschluss an die TI eigenständig vorzunehmen (Der Anwender besorgt sich die notwendigen TI-Komponenten und schließt einen Vertrag mit einem **VPN-Zugangsdienst-Anbieter**.)

oder

- einen DVO und einen VPN-Zugangsdienst-Anbieter zu beauftragen.

Störungen auf der zentralen Seite werden über den 1st-Level-Support des VPN-ZugD-Anbieters aufgenommen, Störungen auf dezentraler Seite hingegen löst der VPN-Zugangsdienstanbieter nicht. Diese muss der Leistungserbringer eigenständig beheben bzw. Sie als DVO beauftragen.

Jeder Anbieter wird in das IT-Service-Management der TI (TI-ITSM) eingebunden. Somit nimmt er an einem auf die spezifischen Anforderungen der TI ausgerichteten ITSM-Framework teil. Hierüber besteht die Möglichkeit, bei übergreifenden Störungen[3] Tickets einzustellen. Dazu muss ein Anbieter einen Single Point of Contact (SPOC) sowohl für den nachgelagerten Anwendersupport (im Sinne eines 2nd/3rd-Level-Supports) als auch für den erforderlichen providerübergreifenden Support einrichten.

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.

[3] Übergreifende Störungen sind Störungen, für deren Behebung mehrere TI-ITSM-Teilnehmer involviert werden müssen. In diesem Fall muss eine von der gematik koordinierte Informationsübermittlung an alle beteiligten TI-ITSM-Teilnehmer eingeleitet werden.

Weiterführende Informationen zur Supportstruktur der TI

Weiterführende Informationen zur Supportstruktur der TI finden Sie im gematik-Dokument „Betriebskonzept Online-Produktivbetrieb (OPB)“ [gemKPT_Betr], abrufbar im Fachportal der gematik.

2 Die sichere Vernetzung des deutschen Gesundheitswesens – Vorstellung der gematik und der TI

2.1 Die gematik – Kurzvorstellung des Unternehmens und des gesetzlichen Auftrages

Die Gesellschaft für Telematik Anwendungen der Gesundheitskarte mbH, kurz: **gematik**, wurde 2005 in Berlin gegründet. Das Wirkungs- und Aufgabenfeld der gematik ist per Gesetz festgeschrieben. Gemäß § 291a SGB V[4] bzw. § 311 SGB V ist sie u. a. verantwortlich für die Einführung und die Weiterentwicklung der Telematikinfrastruktur, der elektronischen Gesundheitskarte (eGK) (s. dazu auch Kapitel 3.2.4) sowie zugehöriger Fachanwendungen.

Die gematik untersteht der Selbstverwaltung des deutschen Gesundheitswesens – vertreten durch die Spitzenorganisationen der Leistungserbringer und Kostenträger im deutschen Gesundheitswesen. Diese Spitzenorganisationen agieren zusammen mit dem Bundesministerium für Gesundheit (BMG) als Gesellschafter der gematik.

Die Rechtsaufsicht über die gematik obliegt laut SGB V dem BMG.

Weitere Informationen zur gematik und zum gesetzlichen Auftrag der gematik

Weiterführende Informationen zur gematik bzw. ihrem gesetzlichen Auftrag erhalten Sie unter den folgenden Links:

https://www.gematik.de/newsroom/mediathek

§ 291a SGB V – Elektronische Gesundheitskarte (gibt u. a. die Anforderungen, Aufgaben und Ziele der eGK sowie Anforderungen an die TI vor).

§ 311 SGB V – Gesellschaft für Telematik (benennt u. a. die Aufgaben der gematik)

2.2 Die Telematikinfrastruktur – Das sichere Netz des deutschen Gesundheitswesens

Die **Telematikinfrastruktur** ist eine bundesweite, interoperable und sektorübergreifende Informations-, Kommunikations- und Sicherheitsinfrastruktur.

Mithilfe der TI können zukünftig alle für eine medizinische Behandlung relevanten Informationen schnell und zuverlässig ausgetauscht werden – und zwar genau dann, wenn sie gebraucht werden. Auf diese Weise trägt die TI zu einer nachhaltigen Verbesserung der medizinischen Versorgung von Versicherten bei. Gleichzeitig kann die Telematikinfrastruktur so einen Beitrag dazu leisten, die Transparenz, Qualität und Wirtschaftlichkeit im Rahmen von Versorgungsituationen zu fördern.

Die Abbildung 2: Schematische Darstellung des Gesamtsystems der TI zeigt die TI aus Netzwerksicht.

[4] Fünftes Sozialgesetzbuch

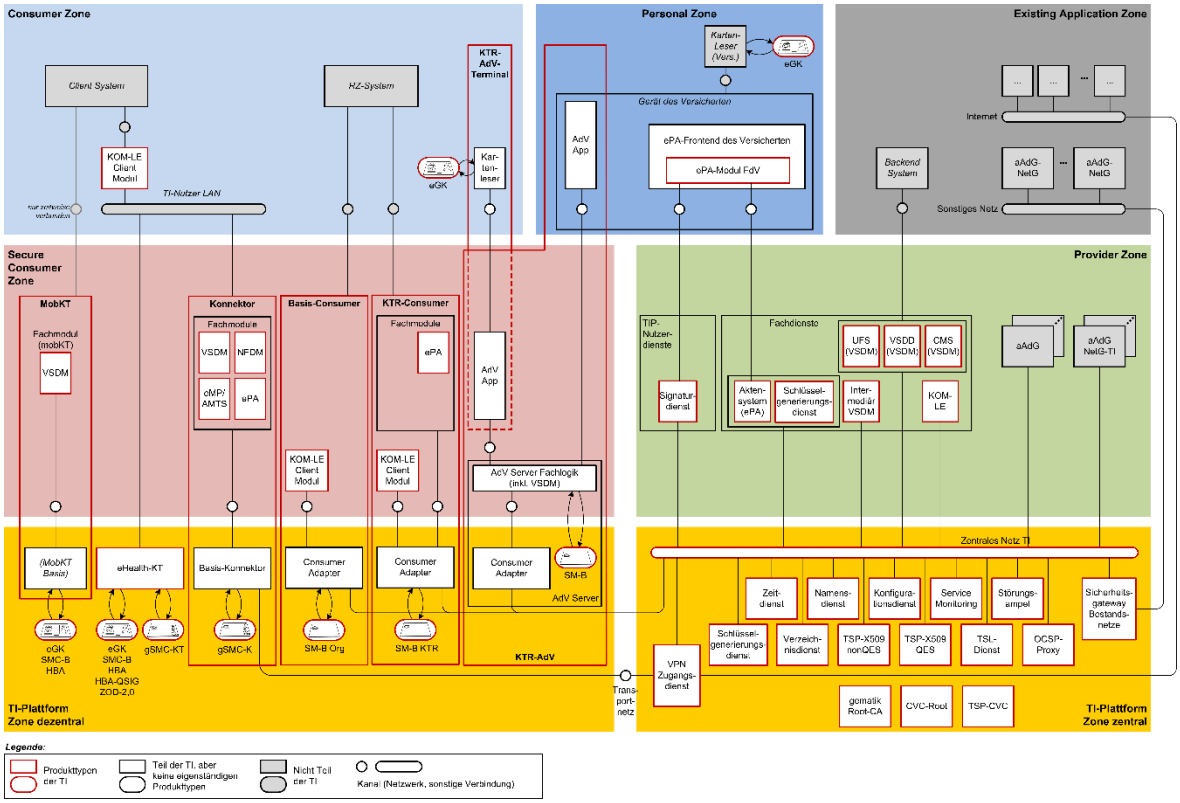

Abbildung 2: Schematische Darstellung des Gesamtsystems der TI[5]

Als DVO arbeiten Sie in der **TI-Plattform Zone dezentral** sowie in der **Consumer Zone** (s. Abbildung 2: Schematische Darstellung des Gesamtsystems der TI). Demzufolge müssen Sie insbesondere mit den **dezentralen Komponenten**, z. B. Konnektor und Kartenterminal, vertraut sein (s. Kapitel 3).

Weiterführende Informationen zur Architektur der Telematikinfrastruktur

Weiterführende Informationen zum Aufbau der Telematikinfrastruktur finden Sie im gematik-Dokument „Konzept Architektur der TI-Plattform“ [gemKPT_Arch_TIP], abrufbar im Fachportal der gematik.

2.2.1 Fachanwendung Versichertenstammdatenmanagement (VSDM)

Mit dem Anschluss an die TI ermöglichen Sie die Nutzung der ersten administrativen TI-Fachanwendung: **das Versichertenstammdatenmanagement** (VSDM). Diese Fachanwendung ist gesetzlich verpflichtend und umfasst die Daten des Versicherten gemäß § 291 Abs. 2 SGB V, die für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung sowie der Abrechnung mit den Leistungserbringern notwendig sind.

[5] Im vorliegenden Dokument werden nicht alle in dieser Abbildung gezeigten Abkürzungen erklärt. Diese Komponenten sind in Ihrer täglichen Arbeit als DVO im Regelfall nicht relevant. Da aber nicht gänzlich ausgeschlossen werden kann, dass Sie bspw. im Rahmen von Fehlermeldungen oder Störungen mit diesen Komponenten konfrontiert werden, sind sie hier informativ aufgeführt. Ausführliche Informationen erhalten Sie bei Bedarf u. a. in dem gematik-Dokument „Konzept Architektur der TI-Plattform“.

Zu diesen sogenannten Stammdaten gehören beispielsweise:

- Name
- Geburtsdatum sowie
- Anschrift.

Mithilfe des VSDM kann überprüft werden, ob ein Anspruch auf Leistungen einer gesetzlichen Krankenversicherung besteht.

Wenn sich diese Daten bei einem Versicherten ändern, können die gesetzlichen Krankenversicherungen mit dieser Fachanwendung die eGK sicher über die TI aktualisieren. Somit entfällt unter Umständen der kostspielige und zeitaufwendige Austausch der eGK[6].

[6] Im Bedarfsfall, bspw. bei Verlust, kann eine eGK auch gesperrt werden, um einen Missbrauch der Karte zu verhindern.

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

3.1 Dezentrale Komponenten – Allgemeine Informationen

Unter den Begriff **dezentrale Komponenten** fallen die TI-Komponenten, die in den Leistungserbringerinstitutionen (kurz: LEI), also bspw. den Arztpraxen, lokal aufgestellt und installiert werden oder – wenn es um Smartcards (auch: Chipkarten) geht – dort „angewendet" werden (s. auch Abbildung 2: Schematische Darstellung des Gesamtsystems der TI)

Zu den dezentralen TI-Komponenten zählen Smartcards, stationäre und mobile Kartenterminals sowie Konnektoren. Nachfolgend werden diese Komponenten (auch **Produkte** genannt) näher vorgestellt.

Dezentrale TI-Komponenten werden von verschiedenen Herstellern produziert und vertrieben. Dabei dürfen Sie **ausschließlich von der gematik zugelassene Komponenten** bei der Einrichtung eines Zuganges zur TI verwenden.

Weiterführende Informationen zu zugelassenen TI-Komponenten

Eine Übersicht über von der gematik zugelassene TI-Komponenten finden Sie im gematik-Fachportal unter https://fachportal.gematik.de/zulassungs-bestaetigungsuebersichten

3.2 Smartcards – Allgemeine Informationen

Als **Smartcards** bzw. Chipkarten werden im TI-Kontext Mikroprozessorkarten bezeichnet, die mit einem Betriebssystem – das sog. Card Operating Systems (COS) für Dateiverwaltung, Prozesssteuerung, Befehlssatz etc. – laufen.
In der TI werden die folgenden Kartentypen eingesetzt:

- Security Module Card – Typ B/Praxisausweis (SMC-B)
- gerätespezifische Security Module Card – Typ Kartenterminal (gSMC-KT)
- gerätespezifische Security Module Card – Typ Konnektor (gSMC-K)
- Heilberufsausweis (HBA)
- elektronische Gesundheitskarte (eGK).

Gebunden sind diese Smartcards entweder an Personen – wie eGK und HBA –, an Leistungserbringerinstitutionen – wie SMC-B – 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 mittels Card-to-Card-Authentisierung nachweist.

Smartcards werden 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.

Zusätzlich zu diesen Smartcards gibt es die Prüfkarte eGK (s. Kapitel 3.2.6). Sie ermöglicht es, die erfolgreiche Installation dezentraler Komponenten der TI zu prüfen.

3.2.1 Security Module Card – Typ B (SMC-B) (Praxisausweis)

Eine **Security Module Card – Typ B** (SMC-B) wird durch die kassenärztlichen/kassenzahnärztlichen Vereinigungen herausgegeben und dient als Praxisausweis bzw. Institutionsausweis. Sie ermöglicht den Zugriff einer berechtigten Leistungserbringerinstitution (bspw. Praxen) auf die TI, d. h., ohne SMC-B baut der Konnektor keine Verbindung zur TI auf.

Eine SMC-B hat zwar wie der Heilberufsausweis und die elektronische Gesundheitskarte (s. Kapitel 3.2.4 und 3.2.5) Scheckkartenformat (Format ID-1), jedoch weist die SMC-B um den Chip herum einen vorgestanzten Bereich auf. Dieser ist so groß wie die SIM-Karte für Mobiltelefone (Format ID-000). Je nach Größe des Kartenslots des eHealth-Kartenterminals (s. auch Kapitel 3.3) kann die SMC-B in „voller Größe" (Format ID-1) eingesetzt werden oder muss aus dem vorgestanzten Bereich der Plastikkarte herausgebrochen werden. Im Gegensatz zur gSMC-KT (s. Kapitel 3.2.2)-KT wird diese Smartcard nicht mit einem Slotsiegel geschützt.

Auf der SMC-B werden folgende Daten gespeichert:

- Integrated Circuit Card Serial Number (kurz: ICCSN, eindeutige/weltweit einmalige Kennnummer)
- Name der Leistungserbringerinstitution[7]
- Betriebsstättennummer[7]
- Art der Praxis (bspw. psychotherapeutische Praxis)[8].

Solange eine freigeschaltete SMC-B im Kartenterminal steckt, kann der Leistungserbringer auf Fachanwendungen, bspw. VSDM, zugreifen und u. a. Versichertenstammdaten auf der eGK lesen oder aktualisieren.

Als DVO benötigen Sie diese Karte bei der Ersteinrichtung des Konnektors, bei der erstmaligen Registrierung beim VPN-Zugangsdienst (s. auch Kapitel 4.3.1) und bei möglichen Störungen im Verbindungsaufbau zur der Telematikinfrastruktur.

[7] Diese Angaben stehen nicht auf den SMC-Bs für zahnmedizinische Institutionen.

[8] Das heißt, dass eine Zuordnung der Institution zu einer Berufsgruppe sowie dem entsprechenden Berechtigungsprofil möglich.

*Bitte informieren Sie ggf. den Leistungserbringer darüber, dass er die SMC-B **rechtzeitig vor dem Anschlusstermin** der Leistungserbringerinstitution an die TI bei einem von der gematik zugelassenen Kartenhersteller [9,10] beantragen muss. In der Regel sollte dies **circa vier Wochen vor dem Anschlusstermin** erfolgen. Bindend sind die jedoch die aktuellen Fristen des jeweiligen Kartenherstellers. Beachten Sie, dass die SMC-B zum Anschlusstermin zwingend freigeschaltet sein muss.*

3.2.2 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 Karten werden mit dem Kartenterminal geliefert.

Im Gegensatz bspw. zum HBA werden gSMC-KTs nicht speziell für den einzelnen Leistungserbringer als personalisierte Smartcard hergestellt. Die gSMC-KT muss nach Einstecken in den Slot des Kartenterminals durch ein Slotsiegel geschützt werden. Dieses Slotsiegel ist im Lieferumfang enthalten. Sie bringen es im Beisein des Leistungserbringers an. Ggf. muss dieses Slotsiegel vom Leistungserbringer unterschrieben werden.

Eine gSMC-KT ist so groß wie die SIM-Karte für Mobiltelefone (Format ID-000). Ggf. muss sie aus einer größeren Karte (Scheckkartenformat) aus einem vorgestanzten Bereich um den Chip herum herausgebrochen werden.

3.2.3 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 (s. Kapitel 4.3.1) sowie den anderen TI-Komponenten, z. B. einem HBA. Im Gegensatz zu den anderen Chipkarten ist die gSMC-K fest – und somit nicht sichtbar – im Konnektor (s. Kapitel 3.4) durch den Hersteller verbaut.

Weiterführende Informationen zu Chipkarten

Weiterführende Informationen zu den Chipkarten finden Sie im Fachportal der gematik unter „Smartcards in der TI“.

3.2.4 Heilberufsausweis (HBA)

Ein **Heilberufsausweis (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 aber auch digital mit dem HBA ausweisen. Ferner können Leistungserbringer mit dem HBA Daten verschlüsseln und signieren. Der HBA ermöglicht zudem den Zugriff auf Daten auf der eGK.

[9] Bitte beachten Sie, dass Zahnärzte u. U. ihre SMC-B direkt über die kassenzahnärztliche Vereinigung beantragen können.

[10] Diese Hersteller werden im TI-Kontext auch als **Trust Service Provider** (TSP) bezeichnet.

© Bundesärztekammer

Abbildung 3: Muster für eine HBA-Vorderseite (gemäß Bundesärztekammer)

© Bundesärztekammer

Abbildung 4: Muster für eine HBA-Rückseite (gemäß Bundesärztekammer)

Für die erste Fachanwendung VSDM (s. Kapitel 2.2.1) wird der HBA nicht benötigt. Erst bei künftigen Anwendungen kommt der HBA in der TI zum Einsatz.

3.2.5 Elektronische Gesundheitskarte (eGK)

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

Auf der eGK sind persönliche Informationen eines Versicherten bzw. Angaben zu seiner Mitgliedschaft in der Krankenversicherung gemäß § 291 Abs. 2 SGB V digital gespeichert oder aufgedruckt (s. dazu auch Abbildungen Abbildung 5 und Abbildung 6, wobei die Abbildung der Europäischen Krankenversicherungskarte auf der Rückseite der eGK optional ist).

Allgemeine Versichertenstammdaten (wie Vorname und Name) können der eGK ohne technische Hilfsmittel abgelesen werden. Geschützte Versichertenstammdaten hingegen können erst durch eine Card-to-Card-Authentisierung ausgelesen werden.

Die eGK

- ermöglicht u.a. die Authentisierung des Versicherten bzw. Authentifizierungsprozesse in der TI

und

- bietet einen sehr hohen Schutz für kryptographische Identitäten und Fachdaten, indem sie selbstständig prüft, ob der Zugriff auf diese Informationen gestattet werden darf.

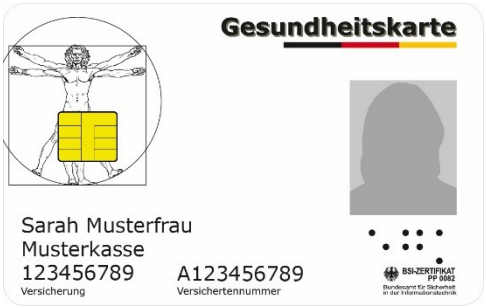

Abbildung 5: Muster für die Vorderseite einer eGK

Abbildung 6: Muster für die Rückseite einer eGK

Als DVO werden Sie unter Umständen bei einem fehlerhaften eGK-Lesevorgang von einem Leistungserbringer oder seinen Mitarbeitern konsultiert. In diesem Fall prüfen Sie zunächst die TI-Funktionalität beim Leistungserbringer. 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 (s. dazu auch Kapitel 5.5 und 5.6).

3.2.6 Prüfkarte eGK

Im Gegensatz zu den zuvor genannten Smartcards ist die Prüfkarte eGK keine Chipkarte, die im regulären Versorgungsalltag von Leistungserbringern oder Versicherten genutzt wird. Die Prüfkarte eGK dient DVOs als Hilfsmittel, mit dem sie nachweisen können, dass die Anbindung einer Einrichtung an die TI erfolgreich war. 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 Primärsystem korrekt auf die eGK zugreifen können. Darüber hinaus können Sie mit der Prüfkarte eGK kontrollieren, ob die Installation von Primärsystem, eHealth-Kartenterminals (Kapitel 3.3) und Konnektor (Kapitel 3.4) in Bezug auf die Fachanwendung VSDM und die Konfiguration der dezentralen Komponenten erfolgreich war (siehe auch Kapitel 4.4).

Wie Abbildung 7 zeigt, lässt sich die Prüfkarte eGK leicht von einer eGK unterscheiden. Eine Verwechselung mit der eGK eines Versicherten ist somit ausgeschlossen.

Abbildung 7: Muster für die Vorderseite einer Prüfkarte (eGK)[11]

Die Prüfkarte eGK zeichnet sich durch

- eine für Prüfzwecke eindeutig definierte Institutskennung (Test-IK)

sowie

- die Verwendung von Personalisierungsdaten fiktiver Identitäten aus.

Hinweis:
Die Prüfkarte eGK kann im Fachportal der gematik kostenpflichtig erworben werden. Die Prüfkarte stellt eine Hilfestellung zur Überprüfung des erfolgreichen Anschlusses einer medizinischen Einrichtung an die TI dar. Sie ist keine Voraussetzung zur erfolgreichen Anbindung an die TI.

3.3 Kartenterminals – Allgemeine Informationen

Im Rahmen der TI werden zwei Arten von Kartenterminals unterschieden: **stationäre** und **mobile Kartenterminals** – auch „**Kartenlesegeräte**" genannt. Mithilfe der Kartenterminals können u. a. Daten auf einer eGK gelesen werden.

3.3.1 Stationäre Kartenterminals (KT)

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

BCS-Kartenterminals

Während des Anschlusstermins können Sie in der Leistungserbringerinstitution auf die älteren BCS-Kartenterminals stoßen. Diese wurden im Rahmen des sog. Basis-Rollouts der TI verwendet. Sie verfügen über einen USB-Anschluss und werden via Primärsystem gesteuert. BCS-Kartenterminals können nicht mit dem Konnektor verbunden werden. Somit können Sie nicht in der TI genutzt werden.

[11] Die Rückseite der Prüfkarte eGK ist weiß.

Unter Umständen werden Sie gebeten, das Modell zu entsorgen.[12] Wenn dies der Fall ist, setzen Sie bitte das Kartenlesegerät auf die Werkseinstellung zurück.

eHealth-Kartenterminals

Im Gegensatz zu den BCS-Kartenterminals werden die eHealth-Kartenterminals nicht mehr lokal über PCs betrieben. eHealth-Kartenterminals können vom Konnektor erkannt und somit via LAN-Verbindung gesteuert werden. Zu diesem Zweck muss ein eHealth-Kartenterminals mit einem Konnektor bekannt gemacht, also **gepairt** werden. Grundsätzlich können bei Bedarf mehrere eHealth-Kartenterminals innerhalb einer Leistungserbringerinstitution mit einem Konnektor gepairt werden. Hierzu müssen diese Kartenlesegeräte im sog. „Infomodell" des Konnektors administriert werden.[13] Der Konnektor kann dann erkennen, wo welches eHealth-Kartenterminal steht.

eHealth-Kartenterminals 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 eHealth-Kartenterminals 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 zukünftige Zugriff auf die medizinischen Gesundheitsdaten wird im Rahmen der TI ebenfalls über das sog. „Zwei-Schlüssel-Prinzip" geregelt. In groben Zügen dargestellt, bedeutet dies: Ein Zugriff auf diese geschützten Daten kann nur dann erfolgen, wenn sich sowohl der Leistungserbringer (mittels HBA als 1. Schlüssel) als auch der Versicherte (mittels eGK als 2. Schlüssel) authentisieren. Für den Zugriff auf geschützte Daten kann zusätzlich die Eingabe der PIN in einem Kartenlesegerät durch den Versicherten erforderlich sein.

Grundsätzlich gilt: Beachten Sie die herstellerspezifischen Angaben in den jeweiligen (Administrator-)Handbüchern.

3.3.2 Mobiles Kartenterminal (mobKT)

Ein **mobiles Kartenterminal** (mobKT) kommt – wie die Bezeichnung bereits andeutet – außerhalb von Leistungserbringerinstitutionen zum Einsatz. Ein mobKT erlaubt es einem LE, Versichertendaten von der eGK auszulesen und zwischenzuspeichern. Später können diese Daten von einem mobKT in das Primärsystem des LE übertragen werden. Hierzu wird das mobile Kartenterminal lokal an einen PC angeschlossen.

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

[13] 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.

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.

Eine Übersicht über zugelassene mobKT finden Sie unter https://fachportal.gematik.de/zulassungs-bestaetigungsuebersichten im gematik-Fachportal.

3.4 Konnektor – Allgemeine Informationen

Ein **Konnektor** als zentraler Bestandteil der TI verbindet die IT-Systeme der Leistungserbringer über ein Transportnetz (typischerweise das Internet via sicherer VPN-Verbindung) mit der TI. Darüber hinaus ermöglicht er dem Primärsystem den sicheren Zugriff auf die Karten (HBA, SMC-B, eGK) über die netzwerkfähigen stationären eHealth-Kartenterminals. Außerdem schützt der Konnektor das lokale Netzwerk eines Leistungserbringers und die dort installierten Clientsysteme vor Angriffen aus der TI – und umgekehrt, die TI vor Angriffen aus einem lokalen Netzwerk.

Als Schnittstelle stellt er 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 Firewall und eines VPN-Clients. Hierbei ist zu beachten, dass für einen Zugang zur TI die Registrierung und die Freischaltung des Konnektors bei einem **VPN-Zugangsdienst**-Anbieter nötig ist (s. Kapitel 4.3.1)

Der Konnektor muss bei der Installation für seine Einsatzumgebung entsprechend der Vorgaben im jeweiligen Handbuch konfiguriert werden.

3.4.1 Hinweise zu Installationsvorkehrungen

Ein Konnektor – sowie die Netzwerkkomponenten Switch und Internet Access Gateway (IAG), bspw. Router mit DSL-/Kabelmodem – darf gemäß Sicherheitsvorgaben der gematik nur in einem zugriffsgeschützten bzw. zugriffsbeschränkten Bereich aufgestellt werden.

Dieser Bereich muss den physischen Schutz des Geräts gegen Angriffe sicherstellen und somit den unberechtigten Zugriff verhindern.

Demnach können nur Leistungserbringer sowie von ihm autorisierte Personen auf den Konnektor zugreifen.

Zu solchen vor dem physischen Zugriff geschützten Bereichen zählen bspw.:

- ein verschließbarer Schrank oder ein vergleichbar gesichertes Objekt

oder

- abschließbare Räume in der Leistungserbringerinstitution.

Befolgen Sie bei der Wahl eines geeigneten zugriffsgeschützten Bereiches die herstellerspezifischen Vorgaben aus dem jeweiligen (Administrator-)Handbuch.

Ungeachtet dessen kann ein Konnektor eigene zusätzliche Mechanismen wie bspw. eine Firewall aufweisen, die Manipulationen und Angriffe erschweren, 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 zumindest folgende Sicherheitsmerkmale vor einer Installation gründlich überprüfen:

- 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?[14]

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 (s. dazu auch Kapitel 5.3).

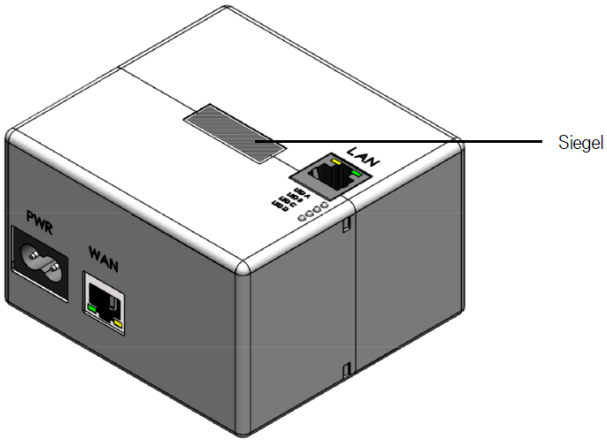

Abbildung 8: Beispielhafte Darstellung für die Siegelplatzierung auf einem Konnektor

Der Konnektor ist – nicht zuletzt aufgrund seiner komplexen Funktionalität – die dezentrale Komponente mit dem höchsten Konfigurationsaufwand. Bitte beachten Sie darum die Anweisungen im herstellerspezifischen (Administrator-)Handbuch.

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

4 Installation und Inbetriebnahme – Von der Terminvorbereitung zum Anschluss an die TI

4.1 Vorbereitung und Durchführung des Termins

Im Anhang dieses Dokumentes finden Sie die „**Checkliste Dienstleister vor Ort**", die Sie dabei unterstützt, den TI-Anschluss-Termin in einer Leistungserbringerinstitution vorzubereiten und durchzuführen. Sie listet alle benötigten Karten, Anträge und PINs auf, nennt die Mindestvoraussetzungen vor Ort und weist Sie auf wichtige Punkte hin, die Sie mit dem Leistungserbringer vor der Einrichtung des Zuganges absprechen müssen.

Bitte beachten Sie, dass diese Checkliste gezielt auf die TI-Anbindung einer Arztpraxis eingeht, zum Beispiel dann, wenn die Rede von „Praxisverwaltungssystem" oder generell „Praxisbetrieb" die Rede ist. Dennoch können Sie die Checkliste problemlos für die Anbindung anderer Leistungserbringerinstitutionen verwenden.

Grundsätzlich gilt jedoch: Ein funktionierender Internetanschluss in der Leistungserbringerinstitution ist zwingend. Die Installation kann zudem erst stattfinden, wenn:

- der Leistungserbringer die SMC-B beantragt hat,
- er anschließend die PIN separat per Post erhalten und
- dann die Karte über das Portal des Kartenherstellers freigeschaltet hat.

Komponenten wie bspw. das stationäre Kartenterminal und den Konnektor hingegen bringen Sie als DVO – insofern nichts anderes vereinbart wurde – zum Anschlusstermin mit.

4.2 Installationsszenarien – Allgemeine Informationen zur Anbindung des LE-Netzwerkes an die TI

In Regel liegen den möglichen Installationsszenarien zwei Anbindungsvarianten zugrunde – die serielle Anbindung und die parallele Anbindung (s. Kapitel 4.2.1). Auf Basis dieser Varianten können Sie unterschiedliche Installationsszenarien realisieren. In der Anlage 3 finden Sie das „Informationsblatt Betriebsarten Konnektor", das Ihnen weitere Szenarien aufzeigt.

Beachten Sie, dass grundsätzlich von einer vorhandenen strukturierten Gebäudeverkabelung und einer Verbindung zum Internet via Internet Access Gateway (IAG) ausgegangen wird. Daneben darf in allen Szenarien die Installation bzw. Inbetriebnahme des Konnektors ausschließlich in einem zugriffsgeschützten/-beschränkten Raum (s. Kapitel 3.4.1) erfolgen.

Allgemeine Sicherheitshinweise für die Installation in der Leistungserbringerumgebung:

Sofern durch den Anschluss an die Telematikinfrastruktur die Leistungserbringerumgebung erstmalig an das Internet angeschlossen wird, ist hierbei zu gewährleisten, dass notwendige Sicherheitsmaßnahmen zum Schutz der medizinischen und zahnmedizinischen Patientendaten etabliert werden. Weiterführende Informationen finden Sie unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Bitte beachten Sie, dass auch bei der Installation des Konnektors im Reihenbetrieb und auch bei der Nutzung des „Sicheren Internet Service" (SIS) diese Sicherheitsmaßnahmen sinnvoll in das Gesamtsicherheitskonzept der Leistungserbringerumgebung integriert werden müssen.

Sofern aufgrund der konkret vorliegenden IT-Landschaft beim Leistungserbringer ein Parallelbetrieb des Konnektors erforderlich ist, sind bei der Auswahl der erforderlichen Netzwerkkomponenten und der nachfolgenden Netzwerkkonfiguration besonders der Baustein und die Umsetzungshinweise „NET: Netze und Kommunikation" https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html zu beachten, da im Parallelbetrieb das Leistungserbringernetz (LAN) nicht durch die Netzwerksicherheitsfunktionen des Konnektors geschützt wird.

4.2.1 Serielle Anbindung vs. Parallele Anbindung

Der Konnektor kann die Systeme der Leistungserbringer, die daran angeschlossen sind, vor Angriffen aus dem Internet zusätzlich schützen, sofern die Konfiguration „seriell" gewählt wird. Sehr wichtig ist aber, dass mit der Installation eines Konnektors keinesfalls die in den medizinischen Einrichtungen bereits umgesetzten Sicherheitsmaßnahmen für den IT-Praxisbetrieb obsolet werden, so dass z. B. Virenschutz oder die Netzabsicherung nach wie vor unerlässlich sind.

Serielle Anbindung (auch „Reihenbetrieb" genannt)

Bei einer **seriellen Anbindung** befinden sich alle Komponenten im selben LEI-Netzwerk (LAN) und erhalten Zugang über den Konnektor zur TI. Durch die integrierte Firewall des Konnektors und den optionalen SIS (s. auch Kapitel 4.3.2) wird das LAN optimal vor unautorisierten Zugriffen von außen geschützt. Diese Betriebsart ist leicht zu konfigurieren und gewährleistet eine vertrauliche Übertragung medizinischer Daten.

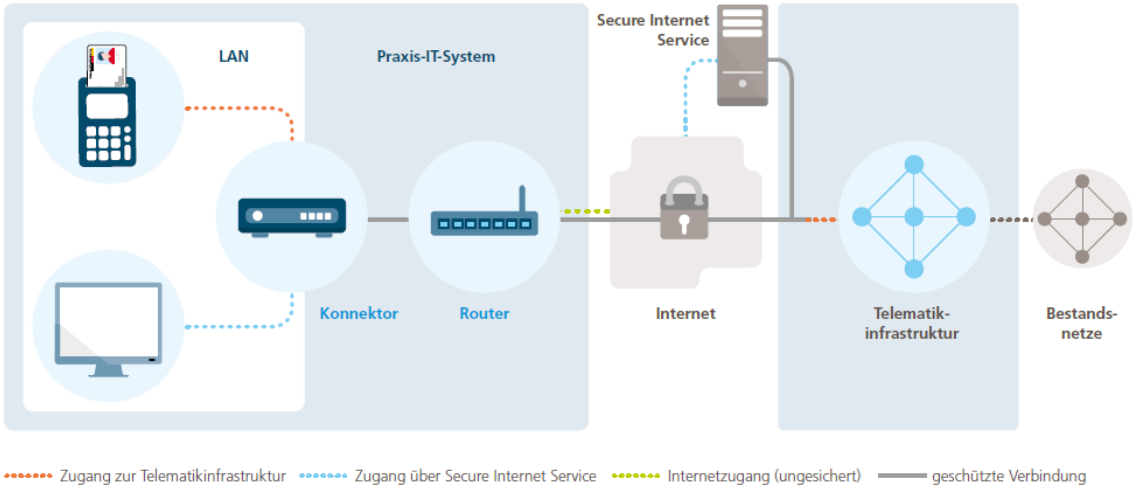

Abbildung 9: Schematische Darstellung der seriellen Anbindung

Parallele Anbindung (auch „Parallelbetrieb" genannt)

In der **parallelen Anbindung** sind alle Komponenten mittels Netzwerkverteiler (Switch/Router) miteinander verbunden. Die Komponenten zur Verarbeitung medizinischer Daten nutzen den Konnektor, um die Telematikinfrastruktur oder den optionalen SIS zu erreichen. 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 (nur SIS/nur Internet/SIS plus Internet).

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.

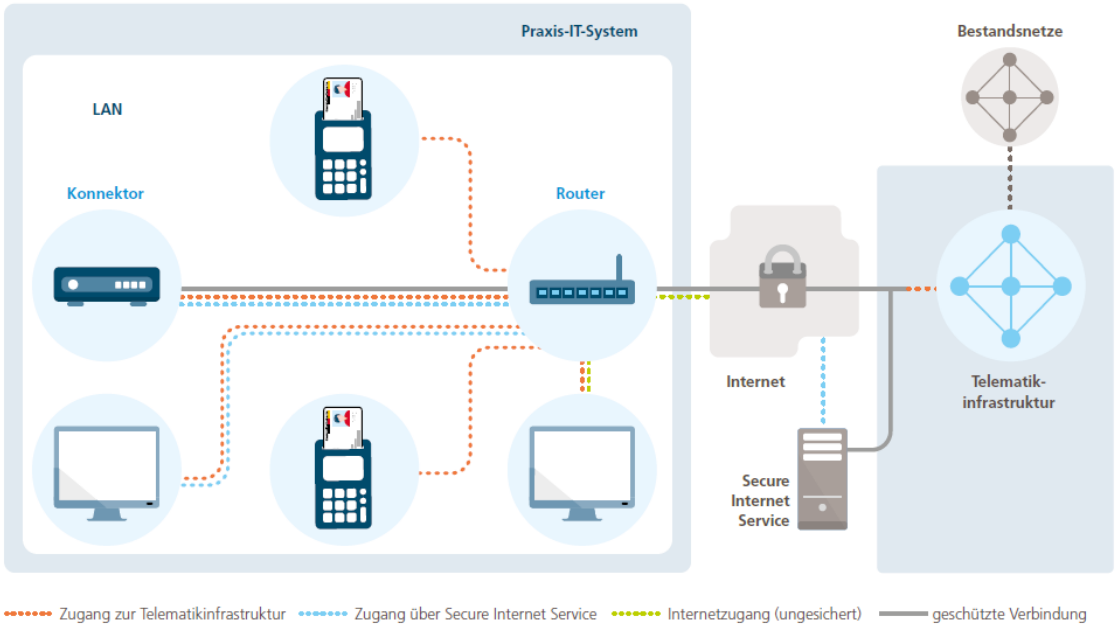

Abbildung 10: Schematische Darstellung der parallelen Anbindung

Weiterführende Informationen zu Installationsszenarien

Weiterführende Informationen zu Installationsszenarien finden Sie im Anhang K des gematik-Dokumentes „Spezifikation Konnektor“ [gemSpec_Kon], abrufbar im gematik-Fachportal.

4.2.2 Konfiguration des Informationsmodells

Der Konnektor steuert den Zugriff auf die angeschlossenen Kartenterminals und darin gesteckte Karten über die Parameter `Mandant`, `ClientSystemID`, `WorkplaceID` und im Falle des HBAs `UserID`. Im Konnektor werden hierfür Kennungen konfiguriert, die auch im Primärsystem hinterlegt werden müssen, damit dieses die Kennungen in den Funktionsaufrufen an den Konnektor einbauen kann.

Der Mandant wird dabei mit einer Institutionskarte (SMC-B) verknüpft. Die `ClientSystemID` repräsentiert eine Anwendung, die `WorkplaceID` hingegen einen Arbeitsplatz. Die an einem Arbeitsplatz direkt verwendeten Kartenterminals werden dem Arbeitsplatz als lokale Kartenterminals zugeordnet. Damit aus einem Arbeitsplatzkontext auf ein Kartenterminal zugegriffen werden kann, dass z. B. in einem Rechnerraum steht, muss dieses als RemoteKT konfiguriert werden. Durch das Remote-PIN-Verfahren kann die PIN-Freischaltung einer Karte in einem RemoteKT über das lokale Kartenterminal eines Arbeitsplatzes erfolgen. Detaillierte Informationen entnehmen Sie bitte dem Handbuch des Konnektors.

4.2.2.1 Auswirkungen der Komfortsignatur auf das Informationsmodell des Konnektors

Wenn die KIM[15]-Adresse nur für die Institution verwendet wird, also nur die SMC-B für die KIM-Ver-/Entschlüsselung verwendet wird, gibt es keine Wechselwirkung mit dem Informationsmodell, das im Konnektor konfiguriert ist.

Wenn die KIM-Adresse für eine Person verwendet wird, also der HBA für die Ver-/Entschlüsselung verwendet wird, muss Folgendes beachtet werden:

Für den **Signaturclient des Primärsystems** und die **KIM-Clients** (Mailclient und Clientmodul) müssen Sie unterschiedliche ClientSystemIDs im Informationsmodell des Konnektors konfigurieren. Der Grund ist, dass bei der Komfortsignatur für den HBA eine lange UserID verwendet wird, die sich regelmäßig ändert, im KIM-Clientmodul jedoch eine UserID statisch hinterlegt wird. Durch die Verwendung unterschiedlicher ClientSystemIDs ist das unabhängig voneinander möglich. Andernfalls kommt es zu Fehlermeldungen beim Zugriff auf den HBA.

4.2.3 Absicherung der Verbindung zwischen Clients und Konnektor

Gemäß der Sicherheitsrichtline der Kassenärztlichen Bundesvereinigung (KBV) muss die Kommunikation zwischen Primärsystem und Konnektor per TLS gesichert werden. Um die Komfortsignatur des Konnektors nutzen zu können, ist es technisch notwendig, dass der Konnektor dieses mit den folgenden Konfigurationsparametern durchsetzt:

```
ANCL_TLS_MANDATORY= enabled

ANCL_CAUT_MANDATORY= enabled

ANCL_CAUT_MODE=CERTIFICATE | PASSWORD
```

Diese Konfiguration wirkt auf alle Clients (Primärsystem (SOAP, ggf. CETP), KIM-Clientmodul, Mail-Client(LDAPs)...) wie in [gemSpec_Kon#TAB_KON_852] und [gemSpec_Kon#TAB_KON_860] angegeben. Daher müssen Sie prüfen, ob alle Clientsysteme TLS unterstützen und die Möglichkeit bieten, ein Zertifikat oder username/password für eine Clientauthentifizierung zu hinterlegen.

Bei `ANCL_CAUT_MODE=CERTIFICATE` muss sich auch der Mailclient für die Verzeichnisdienstabfrage (LDAPs) authentifizieren, bei `ANCL_CAUT_MODE=PASSWORD` wird im LDAP keine Clientauthentifizierung durchgeführt.

Hierfür müssen Sie in den Clients und im Konnektor zueinander passende Authentifizierungsgeheimnisse hinterlegen.

4.3 Nutzung wesentlicher TI-Dienste und Zugang zu Bestandsnetzen

Noch bevor Sie den Leistungserbringer an die TI anschließen, sollten Sie ihn über die Nutzung der nachfolgenden Dienste informieren bzw. dem Leistungserbringer aufzeigen, wie er Zugriff auf die Bestandsnetze hat.

[15] Abkürzung für die Fachanwendung „Kommunikation im Medizinwesen“ (sicherer E-Mail-Dienst für das Gesundheitswesen)

4.3.1 VPN-Zugangsdienst (VPN-ZugD)

Ein **VPN-Zugangsdienst** (VPN-ZugD) ermöglicht den Leistungserbringern den Zugang zur TI und zum Secure Internet Service (SIS, s. auch Kapitel 4.3.2), der wiederum ein integraler Bestandteil des VPN-ZugD ist. Als Transportinfrastruktur zwischen dem Netz des Leistungserbringers auf der einen Seite und dem VPN-ZugD auf der anderen Seite wird dabei das Internet genutzt. Über diese Infrastruktur werden gesicherte Verbindungen von den Konnektoren der Leistungserbringer zu einem VPN-Zugangsdienst aufgebaut. Darüber hinaus erfolgt via VPN-ZugD u. a. die Registrierung und Freischaltung von Konnektoren.

In der TI wird ein VPN-Zugang mittels eines IPsec-Tunnels zwischen Konnektor und VPN-ZugD realisiert. Voraussetzung hierfür ist eine funktionierende Internetverbindung. Die Vertraulichkeit und Integrität der übertragenen Daten wird durch den Einsatz kryptographischer Maßnahmen sichergestellt.

Die derzeit von der gematik zugelassenen Konnektoren nutzen für die Kommunikation zur Telematikinfrastruktur das IPv4-Protokoll. Für das WAN- bzw. LAN-Interface ist dabei ein Default-Wert von 1500 für die MTU-Size (Maximum Transmission Unit) vorgesehen. Dieser Wert kann vom Administrator über die jeweilige Managementschnittstelle des Konnektors konfiguriert werden.

Bei Anschluss an ein IPv6-Netz sollte 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 erfolgen, um störende Paket-Fragmentierungen aufgrund des zusätzlichen Protokoll-Overheads zu verhindern.

Ein VPN-Zugangsdienst darf nur von einem von der gematik zugelassenen Anbieter betrieben werden. Der hierfür notwendige Vertrag wird zwischen Leistungserbringer und dem Anbieter geschlossen.

Aktuelle Hinweise zu spezifischen Netzwerkinformationen der VPN-Zugangsdienst-Anbieter finden Sie auf der DVO-Seite des gematik-Fachportals.

4.3.2 Secure Internet Service (SIS)

Wie zuvor erwähnt, stellt der VPN-Zugangsdienst den Leistungserbringern zusätzlich einen Zugang zum **Secure Internet Service** (SIS) zur Verfügung. Für Leistungserbringer ist die Nutzung dieses ggf. kostenpflichtigen Services optional.

Durch die Verwendung eines SIS-Zugangs wird Nutzung von Diensten im Internet sicherer. Dies bedeutet, dass eingehende Verbindungen aus dem Internet ggf. durch Blacklists unterbunden werden. Die Inhalte der Kommunikation werden zudem auf etwaige Schadsoftware überprüft.

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 Leistungserbringer 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 den Leistungserbringer dazu beraten, welches Installationsszenario seinen Ansprüchen bei der Nutzung des SIS am besten gerecht wird. Der Leistungserbringer muss zusammen mit Ihnen entscheiden, ob seine bisher genutzten Dienste auch über SIS noch funktionieren und ob es ggfs. auch individuelle Konfigurationsmöglichkeiten gibt (bspw. Nutzung SIS von allen PCs).

Als DVO müssen Sie den Leistungserbringer zu den Vor- und Nachteilen dieser Anbindungen beraten (s. auch Kapitel 4.2.1)

Bei der Wahl der passenden SIS-Anbindungsart helfen die folgenden Aspekte:

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

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

Verbindungen in das Netzwerk des Leistungserbringers

- Die Sicherheitsrichtlinien für den SIS erlauben keinen Verbindungsaufbau in das Netzwerk des Leistungserbringers. 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 Standard Port 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 Anwendungen des Leistungserbringers jedoch nicht die standardisierten TCP/UDP-Ports, müssen diese Verbindungen aus dem lokalen Netzwerk individuell betrachtet werden. Ggf. müssen Sie sich mit dem VPN-ZugD zur Klärung in Verbindung setzen.

Weiterführende Informationen zu SIS

Weiterführende Informationen zur Integration von SIS/Konnektor finden Sie im gematik-Dokument „Spezifikation Konnektor“ [gemSpec_Kon], abrufbar im Fachportal der gematik.

4.3.3 Bestandsnetze

Neben der Telematikinfrastruktur existieren im deutschen Gesundheitswesen weitere Netzwerkverbunde. Hierzu gehören bspw. die **Bestandsnetze**, die bereits vor der TI entstanden sind. Hier werden Leistungserbringern bspw. unterschiedliche Fachanwendungen bereitgestellt.

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

4.3.4 Hinweise zur Konfigurationen im Netzwerk

Zum zweiten Halbjahr 2021 gibt es neue Anwendungen, die Anpassungen bei der TI-Anbindung erfordern.

4.3.4.1 DNS-Auskunft für offene Fachdienste der TI

Damit offene Fachdienste der TI funktionieren, muss das Primärsystem Anfragen zur Namensauflösung der Domäne

```
*.telematik
```

an den Konnektor stellen. Der DNS-Dienst des Konnektors liefert eine entsprechende Namensauflösung.

In Umgebungen mit Reihenschaltung ist das gegeben.

Für alle anderen Umgebungen ist eine der folgenden Lösungen umzusetzen.

1. **Lösung**: In der Umgebung wird ein DNS-Resolver verwendet, auf dem ein Domain-Forewarding eingerichtet werden kann. Hier wird ein Forewarding zum Konnektor eingetragen.
2. **Lösung**: In der Umgebung wird eine DNS-Resolver verwendet, der kein Domain-Forewarding unterstützt (z. B. Fritzbox). Es kann aber ein DNS-Server konfiguriert werden. Wird hier nun der Konnektor eingetragen, werden alle DNS-Anfragen an den Konnektor gesendet. Wenn der Konnektor ausfällt, ist allerdings das Internet für diese Umgebung nicht mehr erreichbar.
3. **Lösung**: Auf dem Primärsystemrechner werden domainspezifische DNS-Server konfiguriert (z. B. Windows: NameResolutionPolicyTable; iOS: /etc/resolver/). Wenn das Primärsystem diese Konfiguration vornimmt, sind durch Sie als DVO keine Anpassungen notwendig.

Zu vermeiden ist die Auflösung der relevanten Namen über die Hosts-Datei des Systems. Diese Lösung umgeht die Lastverteilung des DNS. Auch betriebliche Änderungen der IP-Adressen führen unweigerlich zu Störungen.

4.3.4.2 Namensauflösung E-Rezept (DRAFT)

Für die Dienste des E-Rezeptes unter `*.splitdns.ti-dienste.de` kann eine Namensauflösung sowohl im Internet erfolgen als auch über den Konnektor. Es wird dabei ein IP-Adresse aus dem Bereich der offenen Fachdienste zurückgemeldet.

4.3.4.3 Routen in die Telematikinfrastruktur

Das E-Rezept, KIM sowie weitere Dienste der TI werden von Clients aus der Umgebung des Leistungserbringers direkt angesprochen. Damit das funktioniert, muss ein Routing zum Konnektor für folgende Netzbereiche eingerichtet werden (gemSpec_Net#GS-A_4029-01)

- offene Fachdienste oder Dienste eines SÜV[16] 100.102.0.0/17, 100.103.0.0/16
- aAdG und aAdG NetG-TI (WANDA) 100.102.128.0/17

[16] Sicheres Übermittlungsverfahren

- Bestandsnetze öffentliche Adressen siehe Bestandsnetze.xml.
  Die aktuellen Bestandsnetze können über die Administrationsoberfläche des Konnektors eingesehen werden.

In Umgebungen mit Reihenschaltung oder in Umgebungen, die den Konnektor als Default-Gateway nutzen, wird das Routing durch den Konnektor gewährleistet.

Für alle anderen Umgebungen ist eine der folgenden Lösungen umzusetzen:

- Einrichtung statischer Routen für die Netzbereiche zum Konnektor auf dem Default-Gateway des Netzes (z. B. Internetgateway Fritzbox o.ä.)
- Einrichtung statischer Routen auf dem Primärsystem-Rechner. Die Einrichtung dieser Routen können von Installationsroutinen der Primärsysteme durchgeführt werden.

Um wiederholten Konfigurationsaufwand zu vermeiden, sollten die Routen für die kompletten Adressbereiche eingerichtet werden. Damit ist das Routing bereits für neue Dienste oder bei Änderungen der IP-Adressen gegeben.

Weitere Informationen finden Sie auf GitHub unter https://github.com/gematik/api-erp/blob/master/docs/ti_configuration.adoc

4.4 Allgemeine Hinweise zur erfolgreichen Installation

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

Primärsystem

Die Einrichtung einer Verbindung zwischen einem Primärsystem und einem Konnektor folgt den jeweiligen Herstellervorgaben. Allen Einrichtungsszenarien ist jedoch gemein, dass das Primärsystem für den Nachweis einer erfolgreichen Installation die „Bereitschaft" des Konnektors überprüft. Dazu fragt das Primärsystem bspw. das Vorhandensein aller benötigten Schnittstellen sowie aller Karten ab. Erst wenn diese Bereitschaft vom Konnektor bestätigt wird, kommunizieren Primärsystem 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 (s. auch Kapitel 4.2). Das Management Interface des Konnektors zeigt Ihnen auch an, ob die Kartenterminals gepairt und verbunden bzw. funktionsbereit sind, also als „online" angezeigt werden.

Verwendung der Prüfkarte eGK

Um zu überprüfen, ob die Installation von Primärsystem, eHealth-Kartenterminal und Konnektor in Bezug auf die Fachanwendung VSDM und die Konfiguration der dezentralen

Komponenten erfolgreich war, stecken Sie die Prüfkarte eGK in das eHealth-Kartenterminal. Am Primärsystem wird daraufhin ein Versichertenstammdatensatz mit einer fiktiven Identität als Ergebnis der Prüfung der Versichertenstammdaten angezeigt (s. nachfolgende Tabelle):

Tabelle 1: Beispiel für Anzeige der Prüfkarten-eGK-Daten im Primärsystem

Versicherten	**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 nicht durchgeführt werden, da ihre Daten – im Gegensatz zu den Daten einer eGK eines Versicherten – keiner realen Krankenkasse zugeordnet sind.

Beim Initiieren des Auslesens der Prüfkarte eGK im Primärsystem 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. Das Fachmodul VSDM erzeugt 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. Es muss das Ablaufprotokoll und ggf. das Fehlerprotokoll des Fachmoduls VSDM analysiert werden.

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

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 automatisch 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. Sie müssen hierbei 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 Software,
- führen Sie Updates für Konnektor und Kartenterminal(s) bei Bedarf gemeinsam aus und
- aktualisieren Sie ggf. die Liste der verfügbaren Bestandsnetze.

Beachten Sie, dass Sie den Konnektor nur aktualisieren, wenn das Primärsystem diese Aktualisierung unterstützt. Ggf. muss 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.

5.2 Konfigurationsverwaltung von Konnektoren

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

Generell sind mindestens folgende Punkte beim Export von Konnektor-Konfigurationsdaten zu beachten[17]:

- der Export der Daten erfolgt herstellerspezifisch

und

[17] Es gelten für den Export und den Import überdies die herstellerspezifischen Vorgaben.

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

Generell sind mindestens folgende Punkte beim Import von Konnektor-Konfigurationsdaten zu beachten:

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

und

- der Neustart des Konnektors ist erforderlich.

5.3 Sperrprozess und Außerbetriebnahme eines Konnektors

5.3.1 Sperrung eines Konnektors

Wenn ein Konnektor gesperrt werden muss, ist es wichtig, dass so schnell wie möglich gehandelt wird. Darum sollten Sie bereits beim Anschluss einer Leistungserbringerinstitution den Leistungserbringer (und autorisierte Mitarbeiter der Leistungserbringerinstitution) über den Ablauf informieren.

Werden **Manipulationen** am Konnektor (bspw. Beschädigungen am Siegel bzw. Gehäuse des Konnektors) erkannt oder wurde der Konnektor **gestohlen**, muss sich der Leistungserbringer (oder ein autorisierter Mitarbeiter) mindestens an den jeweiligen Support-Anbieter wenden. Ggf. wird der Leistungserbringer (oder sein Mitarbeiter) Sie bitten, dies zu übernehmen. Welchen Daten (vom Leistungserbringer oder seinen Mitarbeitern) zu diesem Zweck bereitgehalten werden müssen, entnehmen Sie bitte dem (Administrator-)Handbuch bzw. den Vertragsunterlagen.

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, muss der Leistungserbringer (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-Zugangsdienstanbietern variieren.

Weitere herstellerspezifische Informationen können Sie dem jeweiligen (Administrator-)Handbuch entnehmen.

5.3.2 Außerbetriebnahme eines Konnektors

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

Sie müssen den deregistrierten 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.

5.4 Austausch von Kartenterminals

Stationäre bzw. mobile Kartenterminals müssen ausgetauscht werden, wenn die Sicherheitsvorgaben der TI verletzt werden. Dazu gehören – wie auch 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 als DVO mindestens folgende Punkte beachten[18]:

- 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

und

- ggf. muss die Konfiguration oder der Softwarestand des Primärsystems aktualisiert werden.

Beim Austausch von mobilen Kartenterminals müssen Sie als DVO mindestens folgende Punkte beachten:

- das alte mobKT muss im Primärsystem abgemeldet werden

und

- das neue mobKT muss im Primärsystem eingerichtet werden.

5.5 Hinweise zu möglichen Störungen und deren Beseitigung

Wenn die elektronische Gesundheitskarte, der Heilberufsausweis oder der Praxisausweis nicht wie vorgesehenen funktionieren, müssen sich die Inhaber – also Versicherter oder Leistungserbringer – an den 1st-Level-Support des jeweiligen Kartenanbieters (s. Kapitel 3.2) wenden.

Im Anhang finden Sie zudem ein „Merkblatt zum Umgang mit Störungen bei der Nutzung der TI". Dieses Merkblatt zeigt Ihnen auf einen Blick, welche Fehler auftreten können, warum sie auftreten können und wie sie behoben werden können.

Darüber hinaus besteht die Möglichkeit, mithilfe von Logfiles des Konnektors Fehler zu analysieren und zu beheben. Hierzu sehen Sie bitte im jeweiligen (Administrator-) Handbuch nach.

[18] Es gelten für den Export und den Import zudem die herstellerspezifischen Vorgaben.

Weiterführende Informationen zu Fehlermeldungen

Weiterführende Informationen zu Fehlermeldungen können Sie dem gematik-Dokument „Implementierungsleitfaden Primärsysteme“ [gemILF_PS] entnehmen, abrufbar im Fachportal der gematik.

5.6 Ansprechpartner für weitere Fragen zu Kartenterminals oder Primärsystemen

Bei Fragen zu **Kartenterminal**, **Software** oder zum Zusammenspiel verschiedener TI-Komponenten setzen Sie sich bitte mit dem jeweiligen Hersteller in Verbindung.

Hierfür steht Ihnen eine Übersicht über Ansprechpartner für die Themenbereiche stationäre/mobile Kartenterminals sowie Primärsysteme zur Verfügung unter https://fachportal.gematik.de/zulassungs-bestaetigungsuebersichten

Die gematik ist Ihr Ansprechpartner bei systemischen Fehlern, also bei reproduzierbaren Fehlern, im Zusammenspiel eines Produktes mit Komponenten verschiedener Hersteller. Die gematik koordiniert in diesem Fall die Fehleranalyse gemeinsam mit den betroffenen Herstellern.

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
ALG	Application Layer Gateway
DVO	Dienstleister vor Ort
eGK	elektronische Gesundheitskarte
eMP	elektronischer Medikationsplan
gSMC-K	gerätespezifische Security Module Card – Typ Konnektor
gSMC-KT	gerätespezifische Security Module Card – Typ Kartenterminal
HBA	Heilberufsausweis
IAG	Internet Access Gateway
KT	Kartenterminal (stationär)
KSR	Konfigurations- und Software-Repository
mobKT	mobiles Kartenterminal
OCSP	Online Certificate Status Protocol
NFDM	Notfalldatenmanagement
SIS	Secure Internet Service
SMC-B	Security Module Card – Typ B
TSP	Trust Service Provider
TI	Telematikinfrastruktur
TI-ITSM	IT-Service-Management der Telematikinfrastruktur
VPN-ZugD	VPN-Zugangsdienst
VSDM	Versichertenstammdatenmanagement
WOP	Wohnortprinzip

A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 – Referenzierte Dokumente

A5.1 – Dokumente der gematik

[Quelle]	Herausgeber: Titel (jeweils in der aktuell veröffentlichten Version)
[gem_Betriebliche_Rolle_gematik_OPB]	gematik: Betriebliche Rolle der gematik im Online-Produktivbetrieb,
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar
[gemKPT_Betr]	gematik: Betriebskonzept Online-Produktivbetrieb (OPB)
[gemSpec_Kon]	gematik: Spezifikation Konnektor
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemILF_PS]	gematik: Implementierungsleitfaden Primärsysteme

A5.2 – Weiterführende Informationen

[Quelle]	Herausgeber: Titel, Link
Anlage 1 zum Kapitel „Vorbereitung und Durchführung des Termins“	gematik: „Checkliste Dienstleister vor Ort“ https://fachportal.gematik.de/dvo, abrufbar unter Stand: September 2020
Anlage 2	entfallen

[Quelle]	Herausgeber: Titel, Link
Anlage 3 zum Kapitel „Installationsszenarien – Allgemeine Informationen zur Anbindung des LE-Netzwerkes an die TI“	gematik: „Hinweise zu den Betriebsarten für Konnektoren“, abrufbar unter https://fachportal.gematik.de/dvo, Stand Juni 2019
Informationsmaterialien zum Online-Produktivbetrieb	gematik: „Allgemeine Informationsmaterialien zum Online-Produktivbetrieb “, abrufbar unter https://www.gematik.de/newsroom/mediathek
Konzepte und Spezifikationen	https://fachportal.gematik.de/ → Dokumentensuche oder Downloadcenter (Releases)
Webauftritt der gematik	www.gematik.de