OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG
E-HEALTH LAB

REHA-TIKONSIL
TelematikInfrastruktur

Leitfaden zur Anbindung einer Reha-Einrichtung an die Telematikinfrastruktur

Digitales Rehabilitationskonsil mit Anbindung an die Telematik-Infrastruktur
(Reha-/TI-Konsil)

Autoren: Jennifer Wolter
Prof. Dr. med. Georgios Raptis

gefördert durch
Bayerisches Staatsministerium für
Gesundheit und Pflege

Inhaltsverzeichnis

1 Einleitung

Dieser Leitfaden wird im Rahmen des, durch das Bayerische Staatsministerium für Gesundheit und Pflege geförderten, Forschungsprojekts „Digitales Rehabilitationskonsil mit Anbindung an die Telematikinfrastruktur – Reha-/TI-Konsil“ erstellt. Die Inhalte des Leitfadens beruhen dabei einerseits auf Informationen seitens der Anbieter und Dienstleister der Telematikinfrastruktur (TI) sowie auf den Erfahrungen der am Projekt teilnehmenden Reha-Einrichtungen bei der Anbindung an die TI in ihrer Einrichtung.

Zur Zielgruppe des Leitfadens gehören sowohl Entscheidungsträger*innen (somit werden auch einige grundlegende Konzepte und Definitionen beschrieben sowie einige IT-technische Konzepte laienhaft erklärt) als auch Mitarbeiter*innen der IT-Abteilung von Reha-Einrichtungen.

Die Informationen in diesem Leitfaden wurden nach bestem Wissen recherchiert und widerspiegeln den Stand von Oktober 2022. Sollten Fehler enthalten sein oder neue Erkenntnisse vorliegen, bitten die Autoren um Rückmeldung. Eine neue, korrigierte Version wird dann bereitgestellt.

2 Grundvoraussetzungen für die Anbindung

Die TI soll alle Akteure des Gesundheitswesens vernetzen und den sektoren- und systemübergreifenden sowie sicheren Austausch von Informationen gewährleisten. Ziel ist eine sichere Datenautobahn des Gesundheitswesens, welche über die gematik GmbH im gesetzlichen Auftrag unter Beteiligung von privaten Anbietern errichtet und betrieben wird. Hierbei soll eine einheitliche sektorenübergreifende Plattform etabliert werden und somit ein sicherer Informationsaustausch zwischen den Gesundheitsdiensteanbietern ermöglicht werden. Die Stärkung des Datenschutzes und der Datensicherheit (inkl. Zertifizierung und Zulassung der technischen Komponenten) sowie die Etablierung eines digitalen Verzeichnisses stehen dabei im Vordergrund. Außerdem sollen somit IT-Inseln und Medienbrüchen vermieden und der flächendeckende Einsatz von Patientenanwendungen gewährleistet werden.

Die Telematikinfrastruktur ermöglicht viele, auch medizinische Anwendungen. Dazu gehören das Notfalldatenmanagement (NFDM), der elektronische Medikationsplan (eMP), die elektronische Patientenakte (ePA) und künftig auch die Patientenkurzakte, sowie eine auf E-Mail basierte Kommunikationsplattform (KIM), über die Praxen etwa eArztbriefe versenden und empfangen können. Das elektronische Rezept (eRezept) und die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) werden derzeit (Oktober 2022) ausgerollt.

2.1 Grundausstattung für die Nutzung der TI, Begriffsdefinitionen

Grundvoraussetzung für die TI ist ein Internetzugang; für bestimmte Anschlussarten (TI as a Service) ist ein möglichst breitbandiger und schneller Zugang notwendig. Auch die Klinik-Software muss angepasst werden, um über entsprechende Schnittstellen eine Verbindung zur TI zu ermöglichen und auf die Anwendungen der TI zugreifen zu können. Ein entsprechendes Software-Update ist die Grundvoraussetzung für alle weiteren Schritte der TI-Anbindung.

Folgende Komponenten sind notwendig für den Anschluss an die TI:

- Sicherer Zugangsdienst (VPN)
- Konnektor
- eHealth-Kartenterminals
- Institutionsausweis (SMC-B)
- Elektronische Heilberufsausweis (eHBA)

Ein **VPN-Zugangsdienst** ermöglicht den Akteuren des Gesundheitswesens den Zugang zur TI und zum Secure Internet Service[1]. Die Anbieter müssen von der gematik zugelassen sein. Jede Vorsorge- und Rehabilitationseinrichtung benötigt einen VPN-Zugangsdienst.

Aktuell sind 3 VPN-Zugangsdienste von folgenden Anbietern zugelassen:

- Arvato Systems Digital GmbH,
- T-Systems International GmbH,
- CompuGroup Medical Deutschland AG.

Es ist sinnvoll einen Zugangsdienst erst in Abstimmung mit einem Konnektor-Hersteller auszuwählen bzw. i.d.R. wird ein Zugangsdienst vom Konnektor-Hersteller oder Konnektor-Vertriebsdienstleister gleich mit angeboten oder vorgegeben.

Weitere Informationen zu VPN-Zugangsdiensten und den zugelassenen Produkten sind im Fachportal der gematik unter folgender URL enthalten:

https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/vpn-zugangsdienst

Der **Konnektor** ist eine Art „Router“ mit einem sehr hohen Sicherheitsniveau, der die Reha-Einrichtung mit dem digitalen Netz der TI verbindet. Er umfasst die Funktionalitäten eines VPN-Devices und eines Application Proxys. Der Konnektor stellt ein sogenanntes Virtuelles Privates Netzwerk (VPN) her, welches ermöglicht, Anwendungen unter Einsatz moderner Verschlüsselungstechnologien völlig abgeschirmt vom sonstigen Internet zu nutzen. Er steuert die Kartenterminals und die Chipkarten. Soll eine Anwendung in der Telematik-Infrastruktur von der Klinik-Software genutzt werden, wird der Zugriff darauf über den Konnektor vermittelt. Er muss von der gematik zugelassen und vom BSI zertifiziert sein. Die benötigte Anzahl und Dimension hängt von der Größe und Struktur der jeweiligen Institution ab. Aktuell (Oktober 2022) empfiehlt es sich die Beschaffung eines Konnektors PTV 5[2] oder

[1] Der **Secure Internet Service** ist ein sicherer Zugang zum Internet über die TI. Dabei wird der Netzwerk-Verkehr über Security Gateways geleitet, so dass bestimmte Bedrohungen möglichst abgewehrt werden können. Der Dienst ist kostenpflichtig.

[2] PTV5: Produkttyp-Version 5: gemäß Gematik-Spezifikationen hat jede Produkttyp-Version bestimmte Fähigkeiten, z.B. Unterstützung von Komfort-Signatur oder elektronische Patientenakte 2.0

höher, da dieser sowohl eine Komfortsignatur als auch die elektronische Patientenakte in der Stufe 2 unterstützt.

Komfortsignatur: Bei diesem Verfahren können Ärzt*innen mit ihrem Heilberufsausweis (eHBA) und einer einmaligen PIN-Eingabe für einen bestimmten Zeitraum jeweils bis zu 250 Signaturen freigeben. Die einzelnen Signaturen werden über die Klinik-Software ausgelöst.

Stapelsignatur: Ärzt*innen können mit der Stapelsignatur mehrere Dokumente gleichzeitig qualifiziert elektronisch unterschreiben. Sie signieren hierbei einmal mit ihrem eHBA und ihrer dazugehörigen PIN den gesamten vorbereiteten elektronischen Dokumentenstapel, zum Beispiel am Ende eines Praxistages.

Technische Informationen zum Konnektor – inkl. ein Konzept für die Inbetriebnahme und die Liste der zugelassenen Anbieter bzw. Konnektoren – können im Fachportal der gematik unter folgender URL abgerufen werden:

https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/konnektor

Die **eHealth-Kartenterminals** dienen zum Einlesen der elektronischen Gesundheitskarte, des elektronischen Heilberufsausweis (eHBA) sowie der Institutionskarte (SMC-B Reha). Sie müssen von der gematik zugelassen und vom BSI zertifiziert sein. Es wird eine Verbindung über das lokale Netzwerk mit dem Konnektor erstellt; die Einrichtung eines eigenen VLAN für die Kartenterminals ist ratsam. In einem Kartenterminal wird u.a. auch die SMC-B der Einrichtung eingesteckt (s. weiter unten). Die Kartenterminals können sowohl die elektronischen Gesundheitskarten als auch mit den Heilberufsausweisen steuern und somit Anwendungen der TI unterstützen. Die benötigte Anzahl hängt von der Größe und Struktur der Einrichtung ab. Aus der Anzahl der Kartenterminals ergibt sich die Anzahl zu beschaffender Konnektoren.

Die zugelassenen eHealth-Kartenterminals finden Sie im Fachportal der gematik:

https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/ehealth-kartenterminal

Angehörige der Heilberufe (z. B. Ärzte, Apotheker) weisen sich mit dem elektronischen Heilberufsausweis (**eHBA**) gegenüber der TI aus. Der eHBA ist eine personenbezogene Chipkarte mit kryptographischen Funktionen und ermöglicht den Ärzt*innen rechtsverbindliche qualifizierte elektronische Signaturen (QES) zu erstellen, z.B. für elektronische Arztbriefe. Für die Herausgabe ist die jeweilige Berufskammer z.B. bei Ärzten und Ärztinnen die jeweilige Landesärztekammer zuständig. Möglicher Einsatz im Rehabilitationsbereich ist im Entlass-Management und in den Prozessbereichen, in denen medizinische Dokumente rechtssicher digital unterschrieben werden müssen.

Die **SMC-B** (Security Module Card – Type B) ist ein Institutionsausweis. Neben ihrer Eigenschaft als Ausweis hat sie auch wesentliche Sicherheitsfunktionen. Die SMC-B Reha weist eine Vorsorge- und Rehabilitationseinrichtung gegenüber der TI aus, um eine Verbindung in der TI aufzubauen. Die Sektoren beauftragen Herausgeber für die Ausgabe der SMC-B. Die Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH (DKTIG) ist Herausgeber der SMC-B Reha.

Folgende Einrichtungen sind berechtigt, die SMC-B Reha zu bestellen:

- Vorsorge- und Rehabilitationseinrichtungen, mit denen ein Versorgungsvertrag nach §§ 111 Abs. 2 Satz 1, Abs. 3, § 111a Abs. 1 Satz 1 oder § 111c Abs. 1 SGB V besteht.
- Vorsorge- und Rehabilitationseinrichtungen der gesetzlichen Rentenversicherung, die Leistungen nach den §§ 15, 15a oder § 31 Abs. 1 Nr. 2 des Sechsten Buches erbringen.

Nach der Antragsfreigabe durch die DKTIG erfolgt die Personalisierung, Produktion und der Versand der SMC-B Karten und zugehörigen PIN Briefe durch von der DKTIG beauftragte und der gematik zugelassene Trusted Service Provider (TSP). Eine (Ersatz-) Ausstattung ggf. über 2 TSP, um beispielsweise Betreiberausfällen vorzubeugen, wird empfohlen. Es ist gesetzlich vorgeschrieben, dass eine SMC-B nur dann bestellt werden darf, wenn in der Rehabilitationseinrichtung ein eHBA (z.B. des ärztlichen Direktors) bereits vorhanden ist.

Jeder TSP bietet ein webbasiertes Antragsportal. Aktuell (Oktober 2022) sind lt. DKTIG folgende TSPs für die Ausgabe der SMC-B Reha zugelassen:

- D-Trust GmbH – Ein Unternehmen der Bundesdruckerei
- Stolle & Heinz Consultants GmbH & Co KG (SHC)

Die DKTIG stellt eine Checkliste mit Informationen für die Beantragung der SMC-B Reha zur Verfügung:

https://dktig.de/wp-content/uploads/2022/07/Checkliste_Antragstellung-SMC-B-Reha_V1.3.pdf

Die DKTIG vergibt im Zuge des Ausgabeprozesses der SMC-B Reha eine Telematik-ID als eindeutige Identifikationsnummer der Vorsorge- und Rehabilitationseinrichtung in der Telematikinfrastruktur. Die Einrichtung wird als Eintrag im Verzeichnisdienst der Telematikinfrastruktur mit einem Basisdatensatz und der Telematik-ID angelegt. Die Telematik-ID ist zwingende Voraussetzung für den korrekten Eintrag von KIM-Adressen im Verzeichnisdienst.

KIM (Kommunikation im Medizinwesen) ist eine Anwendung, mit der teilnehmende Institutionen in der Telematik-Infrastruktur miteinander kommunizieren können. KIM ermöglicht eine Kommunikation per E-Mail, sorgt jedoch u.a. für die Verschlüsselung und die Authentizität der Kommunikationspartner sowie die Integrität der ausgetauschten E-Mails. Über KIM werden auch TI-Anwendungen realisiert, wie die elektronische Arbeitsunfähigkeitsbescheinigung (eAU). Die Nutzung von KIM erfordert spezielle E-Mail-Adressen, die i.d.R. kostenpflichtig sind und mit der SMC-B verbunden werden.

2.2 Finanzierung der Kosten für die Anbindung von Reha-Einrichtungen an die TI

Das Patientendaten-Schutzgesetz (PDSG) hat die Möglichkeit einer Anbindung von Reha-Kliniken an die Telematik-Infrastruktur eingeführt. Die Anbindung ist dabei derzeit freiwillig. Lt. Einschätzung des Bundesverbands Deutscher Privatkliniken e.V. (vgl. Geschäftsbericht 2020/2021[3], S. 57) sollen die Gesamtkosten (inkl. interner Planungs- und Umsetzungsaufwand, Schulungen, Hard- und Software)

[3] Geschäftsbericht 2020/2021 BDPK, https://www.bdpk.de/fileadmin/user_upload/BDPK/Veroeffentlichungen/BDPK_Geschaftsbericht_2020_2021.pdf

auf durchschnittlich 90.000 Euro belaufen. Über eine Finanzierungsvereinbarung zwischen den relevanten Parteien der Selbstverwaltung (vgl. § 381 SGB V) sollen die dabei entstehenden „Ausstattungs- und Betriebskosten“ gemäß § 376 Satz 1 SGB V erstattet werden. Die Finanzierungsvereinbarung sollte bis zum 01.10.2020 unterzeichnet werden und ab dem 01.01.2021 gelten, ist jedoch aktuell (Oktober 2022) noch nicht unterzeichnet worden.

2.3 Vorgehensweise

Die folgenden Schritte sollten beachtet werden, wenn eine Reha-Einrichtung einen Anschluss an die TI realisieren möchte.

2.3.1 Entscheidung auf Management-Ebene

Die Entscheidung sollte auf strategischer Ebene gefällt werden. Motivation kann eine evtl. vorhandene Digitalisierungs-Strategie der Klinik sein. Konkret kann die Nutzung von TI-Anwendungen, wie der elektronischen Patientenakte oder die Möglichkeit über KIM zu kommunizieren eine Motivation sein. Ebenfalls als Motivation können Anwendungen von Drittanbietern fungieren, welche innerhalb der TI angeboten werden, z.B. das Reha-Konsil zur Betreuung von Reha-Patient*innen in Kooperation mit niedergelassenen Ärzt*innen. Eine zwingende Motivation wird eine evtl. künftige Pflicht zur TI-Anbindung und Nutzung von TI-Anwendungen für Reha-Einrichtungen sein, sollte sie gesetzlich vorgeschrieben werden.

Der TI-Anschluss ist mit Kosten und internem Personalaufwand verbunden. Diese Parameter sollten im Vorfeld recherchiert und eingeschätzt werden, um eine qualifizierte Entscheidung des Klinik-Managements zu ermöglichen.

2.3.2 Interne Projektinitialisierung

Ein internes Projektteam sollte gebildet werden. Notwendig ist die Einbindung der IT-Leitung, des kaufmännischen Managements und der ärztlichen Leitung. Es sollten Ansprechpartner gegenüber externen Anbietern und relevanten Organisationen bestimmt werden. Das Projektteam soll die internen personellen und finanziellen Ressourcen herausarbeiten und zunächst eine grobe Zeitplanung für das Vorhaben erstellen.

Die Erfahrungen aus unserem Forschungsprojekt haben eine Projektlaufzeit für den TI-Anschluss von durchschnittlich 3 - 6 Monaten mit einer sehr großen Varianz i.d.R. nach oben - motiviert durch außerplanmäßige Herausforderungen - ergeben. (Reguläre) Zeittreiber können sein:

- Laufzeiten für den eHBA-Antrag, motiviert durch Identifikation, Bearbeitung durch Ärztekammer und eHBA-Anbieter, Produktion, sichere Auslieferung von Karte und Transport-PIN sowie Freischaltung des eHBA beim Anbieter (Empfangsbestätigung)
- Zeit für die Erstellung und Umsetzung eines Angebots seitens Konnektoren-Dienstleister
- Evtl. Notwendigkeit einer öffentlichen Ausschreibung
- interne Planung und Umsetzung von Netzwerk-Konfigurationen (inkl. Firewalls und VLANs)
- SMC-B Beantragung und Laufzeit (Schritte ähnlich wie eHBA)
- Updates der Klinik-Software, um „TI-Readyness“ herzustellen

Außerplanmäßige Schwierigkeiten mit substantiellem Zeit-Impact im Projekt waren (abgesehen von der COVID-19 Pandemie):

- Langanhaltende Bestell- und Lieferschwierigkeiten von Konnektoren (z.B. aufgrund von Cyberangriffen oder Chipmangel)
- unverhältnismäßige Laufzeiten der HBA-Beantragung aufgrund eines laufenden Massen-Rollouts (welches sich jedoch regelmäßig bzw. alle 5 Jahren wiederholen wird)
- Notwendigkeit von größeren Umbaumaßnahmen in der IT-Infrastruktur einer Klinik (Modernisierung, fehlende Bereitstellung von notwendigen Upgrades)
- Interne Widerstände innerhalb einer Klinik, die bis zum Abbruch des Projekts führen können.

2.3.3 Ermittlung und Planung der internen Voraussetzungen

Für einen TI-Anschluss muss i.d.R. die Klinik-Software ertüchtigt werden. Die meisten Hersteller bieten Updates, welches die entsprechenden Funktionalitäten nachrüsten. Evtl. sind jedoch auch Upgrades erforderlich, falls eine ggf. eingesetzte, ältere Software-Version keine TI-Unterstützung durch ein Update ermöglicht. Solche Upgrades könnten auch Hardware-Aufrüstungen nach sich ziehen. Um den Bedarf und den Zeitaufwand zu ermitteln, muss der Software-Hersteller oder Vertriebspartner konsultiert werden. Zu den unmittelbaren Kosten des Updates (Einrichtung und ggf. wiederkehrende Kosten / Lizenzen) müssen auch interne Kosten und Personalzeit für ein Update oder Upgrade der Klinik-Software (und ggf. auch Hardware) mitgerechnet werden.

Die Klinik-Software muss für die Nutzung des Konnektors (für Krankenhäuser: auch für Interoperabilität beim Datenaustausch, Stichwort ISiK-ISiP) zugelassen sein. Eine Übersicht der zugelassenen Primärsysteme ist im Fachportal der Gematik unter „Bestätigungsübersicht Primärsysteme“ enthalten:

https://fachportal.gematik.de/zulassungs-bestaetigungsuebersichten

Zu den internen Voraussetzungen zählen auch Anpassungen in Firewall und das interne Netzwerk. Beispiele sind die Reservierung bestimmter IP-Adressbereiche für den Konnektor oder die Öffnung bestimmter Ports und Protokolle am Firewall. Diese können jedoch erst in Abstimmung mit einem Konnektor-Anbieter bzw. -Dienstleister ermittelt und geplant werden. Sie müssen erst mit Installation des Konnektors bzw. unmittelbar vorher aufgeführt werden.

2.3.4 Markterkundung und Angebotseinholung

Es werden die bereits oben definierten Komponenten für einen TI-Anschluss unmittelbar benötigt:

- Sicherer Zugangsdienst (VPN)
- Konnektor
- eHealth-Kartenterminals
- Institutionsausweis (SMC-B)
- Elektronische Heilberufsausweis (eHBA)

Für diese Komponenten gibt es eine überschaubare Anzahl von Anbietern. Die wichtigste Rolle nimmt hier der Konnektor-Anbieter, da dieser i.d.R. die Einrichtung der internen TI-Infrastruktur maßgeblich bestimmt und koordiniert.

Es gibt vier Arten von Konnektoren:

- (Hardware-) Konnektor, in der Art, wie er auch in einer Arztpraxis eingesetzt wird. Dafür fallen u.a. einmalige Kosten (aktuell ca. 2.500 € bis 3.500 € netto) für die Hardware an. I.d.R. können 25-50 Kartenterminals von einem Konnektor gesteuert werden (aus Performance-Gründen sollten 25 KTs nicht überschritten werden). Werden mehrere Konnektoren installiert (z.B. für Redundanz oder bessere Performance/Skalierung) muss die Zuordnung von Kartenterminals und klinischen Arbeitsplätzen an die Konnektoren per Konfiguration erfolgen; dafür ist eine Management-Software üblich.
- Krankenhaus-Konnektor: i.d.R. mehrere (meist 2) der o.g. Konnektoren in einem 19“ Gehäuse (1 HE), um mehr Redundanz und Performance zu gewährleisten.
- Highspeed-Konnektor: ist zwar spezifiziert, jedoch noch nicht zugelassen. Er entspricht einem Rechenzentrums-Konnektor mit einem High-Performance Hardware-Security-Modul (HSM, eine sehr performante „Chipkarte“ im 19“ Gehäuse) und ist für große Krankenhäuser relevant
- TI as a Service: der Konnektor wird nicht physisch vor Ort, sondern im Rechenzentrum des Anbieters betrieben. Die Klinik-Software und alle Kartenterminals werden mit ihm über ein VPN verbunden. Es fallen i.d.R. (!) keine einmaligen Kosten für den Kauf, sondern monatliche Kosten für die Dienstleistung des Betriebs an. Alle anderen Hardware-Komponenten (Kartenterminals, HBA, SMC-B) müssen jedoch weiterhin gekauft werden.

Ein Angebot eines Konnektor-Anbieters (bzw. eines autorisierten IT-Dienstleisters) enthält i.d.R. die Kosten für den Konnektor selbst, des Zugangsdienstes und optional von Kartenterminals, Lizenzen für eventuell vorhandene Management-Software für den Konnektor sowie KIM-Adressen. Es kann auch signifikante Projektkosten für die Einrichtung des Konnektors enthalten. Voraussetzung für ein Angebot ist die Bedarfsermittlung bzgl. des Mengengerüsts für Konnektoren, SMC-Bs und Kartenterminals. Diese hängen von der Größe (Bettenanzahl, Stationen) der Klinik, von der geplanten Nutzung von TI-Anwendungen sowie vom Verfügbarkeitskonzept (Redundanz für Konnektor und SMC-B) ab und sollten im Vorfeld mit dem Konnektor-Hersteller bzw. sein Dienstleister abgestimmt werden.

Auswahlkriterien für den Konnektor sind i.d.R.:

- Physischer Konnektor oder TI as a Service
- Ggf. Kompatibilität zu vorhandener Klinik-Software
- Preis inkl. Projektkosten und ggf. Kosten für Wartungsvertrag
- Weitere Faktoren, wie Zuverlässigkeit des Anbieters, der Hardware und der Software, Verfügbarkeit, Service, weitere angebotene Komponenten usw.

Gegenüberstellung physischer Konnektor vs. TI as a Service

Für einen physischen Konnektor fallen einmalig Anschaffungskosten an. Der Aufwand für Betrieb und Wartung fällt vor Ort an, zudem ist das Troubleshooting bei Fehlern intern durchzuführen. Nachteilig ist, dass bei einem Defekt am Konnektor außerhalb einer evtl. vorhandenen Garantiezeit die Kosten für die Neuanschaffung selbst zu tragen sind. Außerdem gibt es bei einem Ausfall längere Zeit keine Verbindung zur TI oder es müssen redundant zwei Konnektoren betrieben werden. Bei veränderten Anforderungen bezüglich z. B. höherer Last (Skalierung) müssen mehr Konnektoren beschafft werden und das Last-Management zwischen den Konnektoren muss intern erfolgen.

Bei TI as a Service wird der Konnektor nicht vor Ort betrieben, sondern outgesourct im Rechenzentrum eines spezialisierten Anbieters. Es gibt (i.d.R.!) keine einmaligen Anschaffungskosten, allerdings monatliche Betriebs- und Wartungskosten. Die Betriebsverantwortung, Wartung, Updates, Fehlerbehebung, Defekte, Ausfall und Skalierung von mehreren Konnektoren werden durch den Anbieter verantwortet. Nachteil ist die deutlich größere Netzwerkstrecke über das Internet und VPN, um den Konnektor zu erreichen. D. h. für jede Zugriff der Klinik-Software auf den Konnektors und insbesondere für jeden Chipkarten-Zugriff muss die Anfrage und Antwort über den Konnektor zum Anbieter laufen. Kritisch sind hier Use Cases von Anwendungen der Telematik-Infrastruktur, bei denen eine Freischaltung der elektronischen Gesundheitskarte durch die SMC-B oder eHBA erfolgt (kryptographische Card-to-Card Authentisierung, Zwei-Schlüssel Prinzip, z.B. beim Einlesen der Versichertenstammdaten). In diesem Fall läuft die gesamte (mehrstufige, bidirektionale) Kommunikation zwischen (lokal eingesteckter) eGK und SMC-B im Rahmen des kryptographischen Protokolls über das Netzwerk bis zum Anbieter. Ein weiterer potenzieller Nachteil ist, dass eine serielle Installation des Konnektors nicht möglich ist und dadurch der Konnektor nicht als Firewall für die Klinik eingesetzt werden kann. Die Klinik muss mit dem Internet verbunden werden, um den Konnektor zu erreichen, d.h. der Konnektor ist parallel angeschlossen. Dies ist aber nur dann relevant, wenn eine serielle Installation des Konnektors, die mit Einschränkungen in der Internet-Konnektivität der Klinik verbunden ist, geplant ist.

Aus betriebswirtschaftlicher und betrieblicher Sicht kann ein Anschluss via TI as a Service vorteilhaft sein (zumindest wenn keine hohe Einrichtungskosten berechnet werden), allerdings kann dies bei höherer Last und/oder schmalbandiger Verbindung bzw. großer Netzwerk-Latenz an Grenzen stoßen.

Dieser Aspekt sollte mit dem Anbieter im Vorfeld geklärt werden. Im Zweifel, d.h. bei hoher Last und/oder bekannt schlechter Internet-Verbindung, sollten vorab Tests durchgeführt werden.

Folgende Anbieter gibt es aktuell für physische Konnektoren:

- Compugroup Medical Deutschland AG (CGM)
- secunet Security Networks AG
- Research Industrial Systems Engineering (RISE) Deutschland GmbH

CGM und RISE bieten außerdem Konnektoren im Rechenzentrum als Dienstleistung an (TI as a Service). Es gibt jedoch weitere Unternehmen, welche TI as a Service anbieten und dafür physische Konnektoren der o.g. Anbieter einsetzen. Eine (evtl. nicht abschließende) Liste von TI as a Service Anbietern:

- akquinet GmbH
- Compugroup Medical (CGM)
- Research Industrial Systems Engineering (RISE) Deutschland GmbH
- SL.IS Services GmbH
- Arvato Systems GmbH
- Concat AG
- RED Medical Systems GmbH

Einige Anbieter werden durch Vertriebspartner vertreten, z. B. (Liste nicht abschließend):

Secunet

- Bechtle GmbH & Co. KG
- Deutsche Telekom AG
- IS4IT KRITIS GmbH
- Noventi Health SE
- mzd services GmbH
- ARVATO Systems Perdata GmbH (Bertelsmann)

RISE

- Telekonnekt GmbH
- medkonnekt GmbH (für den Rechenzentrumskonnektor)

2.3.5 Abstimmungen mit ausgewähltem Anbieter, Zuschlag

Nach der Beauftragung des ausgewählten Anbieters ist es wichtig die Schritte des Projektes abzustimmen und Termine für beispielsweise Ressourcenplanung und Installation festzulegen. Des Weiteren müssen die Anforderungen des Anbieters bzgl. interne Voraussetzungen (IP-Adressen, Ports am Firewall usw.) ermittelt und auch diese entsprechend eingeplant werden. Die Abstimmung, ob Management-Software für den Konnektor (z.B. bei mehreren Konnektoren) erforderlich ist, inkl. Lizenzen und Voraussetzungen werden ebenfalls abgestimmt und entsprechend beauftragt / installiert.

Es ist empfehlenswert bei der Beschaffung der Hard- und Software für den Anschluss an die TI auch gleich einen KIM-Dienst und entsprechende (ggf. mehrere) KIM-Adressen zu bestellen; i.d.R. werden diese als Paket von den Konnektor-Anbietern/Dienstleistern mit angeboten. KIM-Adressen können (mit Hilfe von Suchkriterien mehr oder weniger gut) im Verzeichnisdienst der Telematik-Infrastruktur gesucht werden, um KIM-Nachrichten zu verschicken. Die KIM-Adressen sollten auf Klinik- oder Stations- oder Arzt-Ebene abgestimmt werden. Bisher gibt es keine Vorgaben für die Namensgebung, allerdings ist es sehr vorteilhaft diese logisch aufzubauen und auch den Rückschluss auf die Reha-Einrichtung zuzulassen.

Als Beispiel:

- Luitpoldklinik-Heiligenfeld-Verw@heiligenfeld.kim.telematik
  Diese Adresse bezieht sich eindeutig auf die Einrichtung und ist gut im Verzeichnis zu finden.
- Praxis-1234567@i-motion.kim.telematik
  Diese Adresse ist nicht nachvollziehbar und bietet zudem ein großes Potential für Tippfehler.

Vor Beantragung der KIM-Adresse ist darauf zu achten, dass die Einrichtung bereits über eine Telematik-ID und einen Eintrag im Verzeichnisdienst der TI verfügt. Der Eintrag im Verzeichnisdienst wird im Rahmen der Initialbefüllung per E-Mail bestätigt. Die E-Mail enthält auch die Telematik-ID.

2.3.6 Schaffung der internen Voraussetzungen

Bevor der Anschluss beginnen kann müssen eventuell Updates an der Klinik-Software durchgeführt, um „TI-Ready“ zu werden. Dies sollte mit dem Anbieter der Klinik-Software abgestimmt werden. Eine Besonderheit stellt hier der KIM-Client dar. Theoretisch kann KIM sogar mit einem E-Mail Programm, wie Thunderbird bedient werden. Es ist jedoch ratsam, einen KIM-Client als Modul der Klinik-Software zu nutzen, damit geschützte E-Mails direkt aus der Klinik-Software heraus verschickt und empfangen werden können.

Das Netzwerk der Einrichtung muss vorbereitet werden, bevor der Konnektor installiert wird. Außerdem sollten Prüfungen durchgeführt werden, ob die späteren Routen in der aktuellen Netzwerk-Konfiguration möglich sind und auch sonst alle anderen Netzwerkvoraussetzungen (z.B. für den Konnektor reservierte IP-Adressen, VLAN-Einrichtung für Kartenterminals) gegeben sind.

Der Konnektor sollte von allen klinischen Arbeitsplätzen erreichbar sein, entsprechend sollte die VLAN- und Firewall-Konfiguration dies ermöglichen.

Die Schaffung der internen Voraussetzungen umfasst auch organisatorische und bauliche Voraussetzungen: Der Konnektor muss in einem geschützten Bereich, d.h. für Unbefugte nicht zugänglich, betrieben werden. Die Kartenterminals können laut Sicherheitszertifizierung Angriffe über eine max. Zeit von 10 Minuten widerstehen, d.h. sie müssen in einer Umgebung betrieben werden, in der sie für Unbefugte zwar zugänglich sein können jedoch nicht länger als 10 Minuten beaufsichtigt. Diese Voraussetzungen gelten ab der (sicheren) Lieferung der Komponenten. Die Komponenten dürfen zudem nur über die vom Hersteller definierten sicheren Lieferketten ausgeliefert werden, d.h. eine Bestellung über Drittquellen ist in Hinsicht auf ihre Sicherheitszertifizierung nicht möglich. Es sollte außerdem bedacht werden, ob Netzwerkdosen überall dort wo der Konnektor und die Kartenterminals betrieben werden. Sind VLANs in der Klinik eingerichtet werden, müssen sie entsprechend angepasst werden.

2.3.7 Bestellung HBA und SMC-B

Bevor das Kartenterminal in Betrieb genommen werden kann, muss erstmal die Bestellung für den HBA, i.d.R. als Erstes für den/die ärztliche/n Direktor*in, angestoßen werden. Die Bestellung des eHBA muss über die jeweilige Landesärztekammer initiiert werden und läuft dann über einen der folgenden Anbieter:

- D-Trust GmbH – Ein Unternehmen der Bundesdruckerei
- Medisign GmbH
- SHC+Care – Stolle & Heinz Consultants GmbH & Co KG
- T-Systems International GmbH

Sobald der eHBA in der Einrichtung vorliegt, kann die Bestellung der SMC-B Reha getätigt werden. Die Beantragung des Institutionsausweises erfolgt über die DKTIG, welche Herausgeber der SMC-B für Vorsorge- und Rehabilitationseinrichtungen ist. Sollte ein unterbrechungsfreier Betrieb des TI-Anschlusses kritisch sein, so sollte die redundante Bestellung der Karten (2. SMC-B, Ersatzausweis für den ärztlichen Direktor / die ärztliche Direktorin) erwogen werden.

Die Freischaltung der SMC-B Karte muss durch den Antragsteller im Antragsportal erfolgen. Hierfür wird das mit den Antragsunterlagen ausgegebene Freischaltepasswort benötigt. Mit der Freischaltung bestätigt der Antragsteller den Erhalt der SMC-B und den zugehörigen PIN Brief. Erst durch die Freischaltung der SMC-B wird die Eintragung der Basis- und Zertifikatsdaten in den elektronischen Verzeichnisdienst der TI, dem so genannten VZD, initiiert. Es ist zu beachten, dass ohne die Eintragung im VZD die KIM Adressen der Einrichtung nicht zugewiesen werden können.

Die Aktivierung der SMC-B erfolgt mittels des zur Karte gehörigen PIN bei der erstmaligen Nutzung im Kartenlesegerät.

Die SMC-B Reha kann nach Erhalt **zu einem beliebigen Zeitpunkt** initialisiert, d.h. mit Hilfe der PIN in Betrieb genommen werden. Dies ist bei SMC-B für Arztpraxen anders; diese müssen innerhalb von 14 Tagen nach Erhalt in Betrieb genommen werden, sonst werden sie automatisch gesperrt.

Sowohl für den HBA als auch für die SMC-B ist eine sichere Identifikation (z.B. über PostIdent) und Lieferung notwendig, sowie Bestätigung des Empfangs gegenüber dem Anbieter. Die Bearbeitungszeit des Antrages (bei der SMC-B Bestellung ab Eingang der Unterlagen bei der DKTIG) ab Bestellung dürfte mindestens zwei Wochen betragen, bei höherer Last der Anbieter (laufender Roll-Out oder Austausch nach 5 Jahren) auch deutlich länger.

2.3.8 Installation des Konnektors

Die Einrichtung des Konnektors ist sehr komplex, daher ist die Hilfe des Herstellers/Dienstleisters wichtig und i.d.R. notwendig. Beispiele für nicht selbsterklärende und naheliegende Installationsprozeduren, welche eine längere Suche in der Dokumentation erfordern, sind:

- Abweichung der Systemzeit des Konnektors zur aktuellen Zeit
- Abgelaufene CRL oder TSL im Konnektor
- Notwendigkeit einer Firmware-Update
- Fehlgeschlagenes Pairing eines Karten-Terminals

- IP-Adressbereiche im internen Netz, welche mit der Konfiguration des Konnektors nicht zusammenpassen

Es sollte ebenfalls mit dem Anbieter geklärt werden, ob eine Management-Software notwendig ist. Meist ist dies der Fall, wenn mehr als ein Konnektor installiert wird, um die Kartenterminals und die SMC-Bs einem Konnektor zuzuordnen und ein Lastmanagement zu etablieren. Zudem ist die Konfiguration der Klinik-Software für die Anbindung wichtig, um z.B. klinische Arbeitsplätze an Kartenterminals für die Komfortsignatur zuzuordnen. Die Möglichkeit einer TLS-Verbindung zwischen Konnektor und Klinik-Software sollte erwogen werden (Zertifikat ggf. vom Konnektor erstellen lassen). Die TLS-Konnektion zwischen Klinik-Software und Konnektor ist zwingend, wenn die Komfort-Signatur ermöglicht werden soll. Abgesehen davon muss die Komfort-Signatur explizit von der Klinik-Software unterstützt werden, weil die Auslösung der einzelnen Signaturen gemäß bestimmten Sicherheitsregeln von der Software erfolgen muss.

Die Installation weiterer Module und Updates der Klinik-Software sollte spätestens in dieser Phase erfolgen. Diese sollen die Use Cases der TI-Anwendungen unterstützen, welche für die Klinik im Vorfeld als relevant ermittelt wurden (z.B. elektronische Patientenakte) und umfassen insbesondere einen KIM-Client.

2.3.9 Netzwerk-Konfiguration

Um den Anschluss vollständig abzuschließen und den Konnektor vollumfänglich nutzen zu können müssen Firewall-Ports gemäß den Informationen des Anbieters freigeschalten werden. Die Firewall- und Router-Konfiguration kann neben naheliegenden Aktionen, wie Ports freischalten, auch ungewöhnliche Punkte enthalten, wie z.B. die Freischaltung am Router von URL-Aufrufen mit IP-Adressen statt FDQN-basierten URLs für die Aktualisierung von CRLs im Konnektor[4]. Die Dokumentation des Herstellers muss deshalb sehr genau beachtet werden; meist ist es wirtschaftlicher, eine professionelle Installation durch einen Dienstleister des Konnektor-Herstellers vornehmen und dokumentieren zu lassen.

Der Aufruf einer TI-Anwendung oder einer Anwendung eines Drittanbieters über die TI (z.B. Reha-Konsil) muss über den Konnektor erfolgen. Wenn der Konnektor im Parallelbetrieb eingesetzt wird, muss am entsprechenden PC eine statische Route gesetzt werden, sonst geht der Datenverkehr über den Router, bzw. Firewall der Klinik und kann die TI nicht erreichen.

Am entsprechenden (Windows-) PC die Kommandozeile (als Administrator ausführen!) öffnen und folgendes eingeben:

```
route add 100.102.160.0 MASK 255.255.0.0 xxx.xxx.xxx.xxx -p
```

Wobei `xxx.xxx.xxx.xxx` mit der IP Adresse des Konnektors zu ersetzen ist. Linux- und MacOS bieten ähnliche Befehle und Konfigurationen an.

Sollte der Konnektor hinter einer Firewall betrieben werden, muss noch geprüft werden, ob der ausgehende Datenverkehr für das IP-Subnetz der TI-Anwendungen freigeschaltet ist (100.102.160.0/29)

[4] vgl. https://www.secunet.com/fileadmin/user_upload/01_Seitencontent/Produkt-_und_Serviceseiten/konnektor/Kundeninformation_secunet-Konnektor_Lösung_CRL_Download.pdf

Des weiteren muss ggf. ein eigenes VLAN für die Verbindung zwischen Konnektor und Kartenterminal eingerichtet werden, damit beide Komponenten miteinander kommunizieren können und die Kartenterminals sonst von anderen internen Netzen abgeschottet sind. Dies ist nicht zwingend, jedoch ratsam und sollte gemäß der (Sicherheits-) Policy der Klinik entschieden werden.

2.3.10 Tests der Konnektivität und KIM-Tests

Der fertig installierte und konfigurierte Konnektor und die Konfiguration des Netzwerkes müssen getestet werden, um zu prüfen,

- ob eine Verbindung zur TI hergestellt werden kann.
- ob entsprechende Use Cases für TI-Anwendungen bedient werden können
- ob Anwendungen von Drittanbietern über die TI, wie beispielsweise das Reha-Konsil erreichbar sind.
- ob der Verzeichnisdienst der TI erreichbar ist
- ob die KIM-Clients den KIM-Dienst aufrufen kann. Es sollten einige Test-Mails via KIM versendet werden.

Insbesondere bei einer Anbindung via TI as a Service sollten auch Lasttests durchgeführt werden, um den Einfluss der Netzwerkverbindung zum Anbieter in der Kommunikation zum Konnektor zu ermitteln.

3 Bekannte Schwierigkeiten / Erfahrungsberichte

In diesem Kapitel werden praktische Erfahrungen und Herausforderungen von 5 Reha-Einrichtungen beschrieben, welche im Rahmen des Forschungsprojektes Reha-Konsil an die TI angeschlossen wurden. Es handelt sich dabei um die ersten Reha-Einrichtungen in Deutschland (mit Ausnahme von Reha-Einrichtungen, welche an Akut-Krankenhäuser angeschlossen sind), welche an die TI angeschlossen wurden.

Die Erstinstallation und Inbetriebnahme liefen mit Hilfe des Konnektor-Herstellers/Dienstleisters weitgehend reibungslos ab. Allerdings führten lange Lieferzeiten bei den Anbietern zu Verzögerungen. Grundsätzlich dauerte der Anschluss zwischen 3 – 6 Monate, das Einholen der Angebote dauerte in der Regel ca. 2 – 4 Wochen.

Die ersten Tests deckten Probleme auf, wie fehlende Freischaltungen von Ports. Bei Fehler müssen häufig Dienste oder der gesamte Konnektor neugestartet werden; die SMC-B muss neu initiier und freischaltet, sowie das Kartenterminal neu ein- und ausschaltet werden. Diese Problematiken sind bekannt und führen zu Betriebsproblemen. Bei Updates muss ebenfalls das Kartenterminal i.d.R. wieder neu startet werden. Ebenfalls haben Updates des Konnektors zu Fehler im Pairing mit dem Kartenterminal geführt, welches neu eingerichtet werden muss. Updates des Kartenterminals sind

ohne aussagekräftige Fehlermeldung fehlgeschlagen und konnten erst nach Löschen der Firmware-Cache durchlaufen. Solche Probleme sind nicht bei jedem Update aufgetreten, sondern punktuell.

Des Weiteren kann es zu Zertifikatsproblemen kommen, mit denen verschiedene Konnektoren unterschiedlich vorgehen, z.B. mit einem manuellen Austausch der TSL im Konnektor. Solche Schwierigkeiten in Konnektoren und Kartenterminals müssen von der Einrichtung intern gelöst werden, was ein funktionierendes Patch-Management voraussetzt.

Grundsätzlich ist der Aufwand der Einrichtung höher als erwartet; auch der Betrieb erzeugt Aufwand. Durchschnittlich werden 80 – 100 Personenstunden notwendig, um intern den Anschluss und die Einrichtung erfolgreich zu beenden.

Ein weiteres Problem hat ein Kartenterminal eines Herstellers (Orga 6141 online) betroffen, welches meist im Winter bei trockener Luft (hohe elektrostatische Aufladung) und bei bestimmtem Bodenbelag beim Stecken bestimmter eGKs (bei diesen eGKs wurde auf eine galvanische Trennung von kontaktbehafteter und NFC-Schnittstelle verzichtet) zum Absturz des Kartenterminals geführt hat[5]. Ein Aufsatz (eigentlich durch die Sicherheitszertifizierung verboten, hier ausnahmsweise möglich), welches die eGK erdet, musste installiert werden.

Letztendlich wird hier auch auf den Ablauf der internen Konnektorzertifikate nach spätestens 5 Jahre verwiesen, was nach heutigem Stand (jedoch noch offenem Ausgang) einen Austausch des Konnektors bedingt. Es kann jedoch davon ausgegangen werden, dass in 2027 die Einführung der TI2.0 so weit fortgeschritten sein sollte, so dass zu diesem Zeitpunkt ein Konnektor nicht mehr notwendig sein dürfte.

[5] vgl. https://www.heise.de/hintergrund/Probleme-in-Arztpraxen-NFC-Gesundheitskarten-legen-Kartenleser-lahm-7128666.html?seite=all