gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Whitepaper

Datenschutz und Informationssicherheit

Wie werden Gesundheitsdaten in der Telematikinfrastruktur geschützt?

INHALTSVERZEICHNIS

1 | EINLEITUNG

Das Whitepaper beschreibt die speziellen gesetzlichen Regelungen des Datenschutzes und der Informationssicherheit bezüglich der elektronischen Gesundheitskarte (eGK), die Datenschutz- und Informationssicherheitsstrategie der Telematikinfrastruktur (TI), deren Informationssicherheitsarchitektur sowie die Datenschutz- und Informationssicherheitsmaßnahmen der Anwendungen der TI.

Zielgruppe des Whitepapers sind insbesondere Versicherte und Heilberufler, die sich näher über den Datenschutz und die Informationssicherheit in der TI informieren möchten. Technische Details werden nur dann erklärt, wenn sie für das nähere Verständnis notwendig sind.

Die Anwendungen der TI werden stufenweise eingeführt. In der ersten Stufe sind dies die Anwendungen des Versichertenstammdatenmanagements (VSDM) und die sichere Kommunikation zwischen Leistungserbringern (KOM-LE).

Telematikinfrastruktur als sicheres digitales Gesundheitsnetz

Der Gesetzgeber hat die Spitzenverbände der Heilberufler[1] und der gesetzlichen Kostenträger im deutschen Gesundheitswesen im § 291a Sozialgesetzbuch (SGB) V damit beauftragt, ein sicheres digitales Gesundheitsnetz – die sogenannte Telematikinfrastruktur – in Deutschland aufzubauen.

Über dieses sollen Patientendaten sicher zwischen den berechtigten Teilnehmern ausgetauscht werden können. Sie nehmen diese Aufgabe durch die gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH wahr.

Rund 70 Millionen gesetzlich Versicherte [1], 180.000 niedergelassene Ärzte und Zahnärzte [2, 3], 20.500 Apotheken [4], 2.000 Krankenhäuser [5] und 118 Krankenkassen [6] werden die TI nutzen. Somit bietet die TI die sichere Basis für eine Vielzahl von medizinischen Anwendungen.

Datenschutz steht an erster Stelle

Diese neuen technischen Möglichkeiten der Informationstechnologie zum Austausch von medizinischen Informationen in der TI werfen Fragen im Bereich des Datenschutzes auf.

Versicherte müssen in jedem Fall darauf vertrauen können, dass das Arztgeheimnis weiterhin gewahrt bleibt. Denn nur so kann das Vertrauensverhältnis zwischen Heilberuflern und ihren Patienten aufrechterhalten werden, das für eine erfolgreiche medizinische Versorgung notwendig ist. Auch Heilberufler haben ein Interesse am Schutz der innerhalb der TI transportierten Daten. Als Berufsgeheimnisträger unterliegen sie besonders strengen Regelungen.

Der Gesetzgeber hatte daher zusammen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) spezielle Regelungen des Datenschutzes für die eGK formuliert. Diese ergänzen die geltenden Datenschutzregelungen, insbesondere des Bundesdatenschutzgesetzes und des SGB X. Datenschutz wird von der TI in ihrer Gesamtheit gewährleistet. Mit der eGK kontrolliert der Versicherte, wer auf seine Daten zu welchem Zeitpunkt zugreifen kann.

Die eGK leistet so einen entscheidenden Beitrag, den Datenschutz im Gesundheitswesen zu erhöhen und die Rechte der Versicherten zu stärken.

Hohes Informationssicherheitsniveau

Um diesen Datenschutzanforderungen gerecht zu werden und insbesondere die medizinischen Daten von Versicherten zu schützen, wird in der TI auf starke Informationssicherheitsmechanismen gesetzt.

Die sichere, verschlüsselte Kommunikation zwischen bekannten Kommunikationspartnern sowie der Schutz vor dem Zugriff auf sensible Informationen sind daher das Fundament der Telematikinfrastruktur. Ebenso ist der Grundsatz von zentraler Bedeutung, dass über das Internet kein Zugriff auf medizinische Daten möglich sein darf.

2 | GESETZLICHE REGELUNGEN

Der Gesetzgeber formuliert in den §§ 291a und 291b SGB V speziell für die eGK und die TI gesetzliche Regelungen des Datenschutzes und der Informationssicherheit. Dazu gehört, dass die gematik im Rahmen ihrer Aufgaben die technischen Vorgaben einschließlich eines Sicherheitskonzepts zu erstellen sowie die notwendigen Test- und Zertifizierungsmaßnahmen sicherzustellen hat.
Sie hat die Interessen von Versicherten zu wahren und sicherzustellen, dass die Vorschriften zum Schutz personenbezogener Daten eingehalten werden.

eGK dient als Versicherungsnachweis

Die eGK des Versicherten enthält die sogenannten Versichertenstammdaten (VSD) nach § 291 Abs. 2 Satz 1 SGB V. Mit diesen Daten (vgl. Kapitel 6) weist der Versicherte nach, dass er Leistungen der gesetzlichen Krankenversicherung in Anspruch nehmen kann. Sie unterscheiden sich nicht von den zuvor auf der Krankenversichertenkarte gespeicherten Daten und sind sowohl für den Nachweis des Anspruchs auf Leistungen der gesetzlichen Krankenkasse als auch für die Abrechnung dieser Leistungen durch den Heilberufler erforderlich. In Kapitel 4 wird im Detail erklärt, um welche Daten es sich bei den Versichertenstammdaten handelt.

Im Gegensatz zu den medizinischen Anwendungen ist die Speicherung der VSD auf der eGK für den Anspruchsnachweis gesetzlich verpflichtend und es bedarf daher keiner gesonderten Einwilligung des Versicherten.

Zugriff nur mit Heilberufsausweis

Neben den VSD können mittels der eGK in einer späteren Ausbaustufe auch medizinische Daten gespeichert werden. Auf diese medizinischen Daten sowie einen Teil der Versichertenstammdaten können nur Heilberufler mit einem entsprechenden Ausweis zugreifen. Hierzu zählen Ärzte, Zahnärzte, Psychotherapeuten, Apotheker oder – allgemein – Heilberufler und deren berufsmäßige Gehilfen. Je nach Anwendung kann der Zugriff zudem auf bestimmte Heilberuflergruppen beschränkt werden. Diese Zugriffsregelungen werden technisch durch das Zwei-Karten-Prinzip umgesetzt, das in Kapitel 4 erläutert wird. Wer keinem medizinischen Heilberuf angehört – bspw. Versicherungen, Banken oder Arbeitgeber –, darf und kann nicht auf die mit der eGK gespeicherten medizinischen Daten des Versicherten zugreifen. Dies gilt auch für den besonders geschützten Teil der VSD auf der eGK (vgl. Kapitel 6).

Medizinische Daten dienen der Patientenversorgung

Selbst Angehörige eines medizinischen Heilberufes dürfen die mittels der eGK gespeicherten medizinischen Daten nach § 291a Abs. 4 SGB V nicht für andere Zwecke als die medizinische Versorgung des Versicherten nutzen. So darf bspw. auch ein Betriebsarzt die Daten nicht einsehen, um die gesundheitliche Tauglichkeit eines Bewerbers zu überprüfen. Gesetzliche Sonderregelungen für die eGK im § 307b SGB V sehen für einen solchen Fall, in dem ein Zugriff nicht zum Zweck der medizinischen Versorgung erfolgt, sogar Freiheitsstrafen für den Heilberufler vor.

Der Gesetzgeber hat im § 97 StPO zudem den Beschlagnahmeschutz auf die eGK und die mit ihr gespeicherten Daten ausgeweitet. Mit dem Verbot der Sicherstellung wird auch in dieser Hinsicht gewährleistet, dass die Daten tatsächlich nur für den mit der eGK beabsichtigten Zweck – die medizinische Versorgung der Versicherten – verwendet werden.

Versicherte nutzen medizinische Anwendungen freiwillig

Die medizinischen Anwendungen der TI sind ein Angebot an Versicherte, aus dem sie frei auswählen können[2]. Erst nachdem der Versicherte sich für eine Anwendung entschieden hat, dürfen zu dieser Anwendung medizinische Daten erhoben, verarbeitet und genutzt werden.

Möchten Versicherte eine Anwendung nutzen, willigen sie darin gegenüber einem Arzt, Zahnarzt, Psychotherapeuten oder Apotheker gemäß § 291a Abs. 3 SGB V einmal schriftlich ein. Die eGK speichert einen Verweis auf die beim Heilberufler hinterlegte schriftliche Einwilligung.

Versicherte können die Einwilligung in eine medizinische Anwendung jederzeit widerrufen. Alle Daten

zu dieser freiwilligen Anwendung werden dann auf der eGK sofort gelöscht.

Versicherte behalten Datenhoheit

Entscheiden sich Versicherte später für eine zukünftige medizinische Anwendung der TI, bestimmen sie, welcher Heilberufler die Daten der medizinischen Anwendung wann nutzen darf, da vor jedem Zugriff ihr Einverständnis notwendig ist. Wenn der Versicherte nicht zustimmt, so erfolgt auch kein Zugriff auf seine Daten in der TI.

Der Versicherte wird daher grundsätzlich bei jedem Zugriff auf seine Daten in der TI aktiv eingebunden. Durch die Übergabe der eGK vom Versicherten an den Heilberufler und in späteren Ausbaustufen bei medizinischer Anwendung auch durch die Eingabe einer zusätzlichen PIN (persönliche Identifikationsnummer) stimmt der Versicherte einem Zugriff auf seine medizinischen Daten zu.

Die PIN der eGK ist eine persönliche, nur dem Versicherten bekannte Geheimnummer, wie er sie auch von Bankkarten, Handys u. Ä. kennt. Sie wird den Versicherten vor der Einführung von medizinischen Anwendungen in einer zukünftigen Stufe der TI durch ihre Krankenkasse mitgeteilt.

Die Eingabe der PIN zum Lesen der medizinischen Daten der eGK wird entsprechend den gesetzlichen Regelungen für bestimmte Anwendungen in Situationen, in denen der Versicherte dazu nicht in der Lage ist, entfallen. Dies betrifft bspw. Notfallsituationen, in denen das Lesen der auf der eGK gespeicherten Notfalldaten – falls der Versicherte dann diese zukünftige medizinische Anwendung nutzt – für den Arzt, Notfallsanitäter oder Rettungsassistenten auch ohne PIN-Eingabe des Versicherten möglich sein wird.

gematik hat keinen Zugriff auf Versichertendaten

Die gematik verantwortet den Aufbau der technischen Infrastruktur der TI. Sie ist zu keinem Zeitpunkt am Datentransport beteiligt. Das heißt, die gematik kennt die über die TI transportierten Daten von Versicherten nicht – weder die VSD noch die Daten einer zukünftigen medizinischen Anwendung der TI. Sie betreibt die Anwendungen der TI nicht und darf dies nach Gesetz auch nicht. Für Informationen zu den mittels der eGK gespeicherten Daten der Anwendungen der TI können sich Versicherte an ihre jeweilige Krankenkasse wenden. Soweit es um Daten von medizinischen Anwendungen geht, können die Heilberufler Auskünfte erteilen.

Alle Datenzugriffe für Versicherte erkennbar

Versicherte müssen nachvollziehen können, wer auf die mittels der eGK gespeicherten Daten zugegriffen hat. Nur so können sie ihre Datenschutzrechte wahrnehmen. Daher werden Zugriffe auf diese Daten des Versicherten auf der eGK protokolliert. Medizinische Daten selbst werden nicht in den Protokolldaten der eGK gespeichert.

Die Protokolldaten der eGK sind allein für den Versicherten bestimmt und werden vor unberechtigten Zugriffen geschützt (vgl. Abbildung 4). Von Bedeutung sind die Protokolldaten insbesondere für die zukünftigen medizinischen Anwendungen, bei denen Zugriffe auf medizinische Daten erfolgen können, wenn der Versicherte diese Anwendungen nutzt.

Daher ist vorgesehen, mit der Verfügbarkeit der ersten medizinischen Anwendung Möglichkeiten zur Einsichtnahme in das eGK-Protokoll für die Versicherten bereitzustellen.

Zulassung von Komponenten, Diensten und Anbietern

Neben den gesetzlichen Regelungen zur eGK legt der Gesetzgeber im § 291b SGB V auch Rahmenbedingungen für eine Verwendung von Komponenten und Diensten sowie die Teilnahme von Anbietern an der TI fest. So ist vorgeschrieben, dass die gematik Komponenten, Dienste und Anbieter zulassen muss, bevor diese in der TI angewendet werden oder teilnehmen dürfen.

Dies geschieht, wenn Funktionsfähigkeit, Interoperabilität und Sicherheit nachgewiesen sind. Bereits hier ist die enge Zusammenarbeit der gematik mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Prüfung der Informationssicherheit festgelegt.

3 | DATENSCHUTZ- UND INFORMATIONS-SICHERHEITSSTRATEGIE

Die Datenschutz- und Informationssicherheitsstrategie der TI legt die Vorgehensweise zur Erreichung des erforderlichen Datenschutz- und Informationssicherheitsniveaus fest.

Datenschutz und Informationssicherheit unterscheiden sich dabei in ihren Zielen. Datenschutz wahrt Persönlichkeits- und Freiheitsrechte; Informationssicherheit schützt Informationen. Im Gegensatz zum Datenschutz geht es bei der Informationssicherheit nicht zwangsläufig um personenbezogene Daten (sondern z.B. um Geschäftsgeheimnisse). Datenschutz und Informationssicherheit überschneiden sich jedoch, wenn die Informationssicherheit zum Schutz von personenbezogenen Informationen eingesetzt wird (z.B. Verschlüsseln von Patientendaten).

Der Gewährleistung des erforderlichen Datenschutz- und Informationssicherheitsniveaus in der TI dienen drei Grundsätze.

Die erstellten Konzepte zu Datenschutz und Informationssicherheit für eine Anwendung, eine Komponente bzw. einen Dienst der TI werden von datenschutzrechtlichen Aufsichtsbehörden oder Sicherheitsprüfstellen geprüft und bewertet.

Alle Spezifikationen der TI werden von der gematik veröffentlicht [7]. Durch die Veröffentlichung wird auch den Versicherten und weiteren Dritten eine Einsichtnahme ermöglicht.

Prüfung bei Zulassung

Bevor die verschiedenen technischen Komponenten und Dienste in der TI genutzt bzw. betrieben werden dürfen, müssen sie nach einem definierten Verfahren von der gematik zugelassen werden.

Eine der zwingenden Voraussetzungen dafür ist der Nachweis, dass die Produkte alle Anforderungen an den Datenschutz und die Informationssicherheit erfüllen.

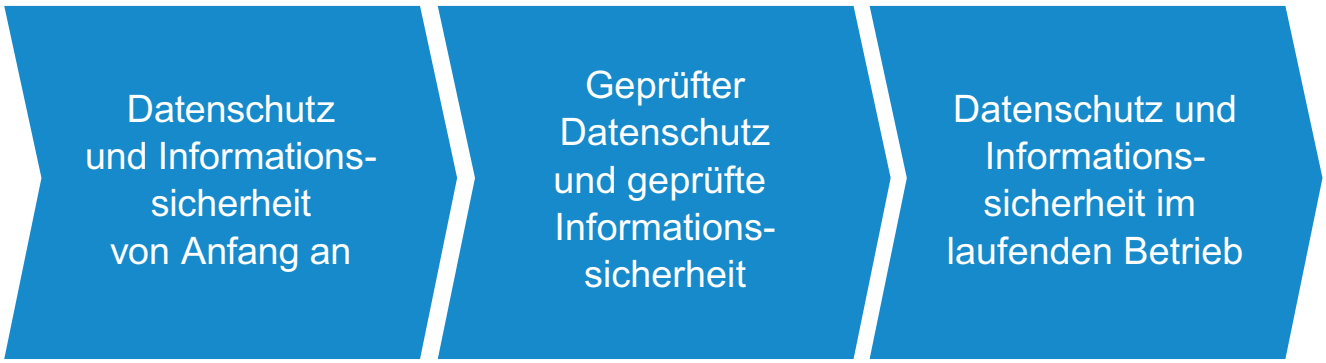


Abbildung 1: Datenschutz und Informationssicherheit werden im gesamten Lebenszyklus der TI berücksichtigt

Datenschutz und Informationssicherheit von Anfang an

Bei der Erstellung von Spezifikationen und der Entwicklung von Anwendungen, Komponenten und Diensten der TI werden bereits im Entwurfsstadium Datenschutz und Informationssicherheit berücksichtigt. Die Festlegungen und Maßnahmen der gematik zur Datensicherheit erfolgen in Abstimmung mit dem BSI und der BfDI.

Dieser Nachweis wird entweder durch eine Sicherheitsevaluation durch das BSI (bei technischen Geräten, wie etwa den Karten) oder durch ein Sicherheitsgutachten (bei zentralen Diensten) erbracht.

Die Vorgaben für die Prüfungen erstellen das BSI und die gematik. Die Prüfer der technischen Geräte müssen vom BSI, die Gutachter bei zentralen Diensten von der gematik anerkannte Sachver-

ständige sein. Zusätzlich testen die Hersteller und Anbieter sowie die gematik selbst die Komponenten und Dienste. Erst wenn alle Schritte erfolgreich durchlaufen wurden, kann eine Komponente zugelassen und in der TI eingesetzt bzw. ein Dienst in der TI betrieben werden.

Datenschutz und Informationssicherheit im laufenden Betrieb

Nachdem Komponenten und Dienste zugelassen und in Betrieb gegangen sind, muss deren datenschutzkonformer und sicherer Betrieb kontinuierlich überwacht werden, um das Datenschutz- und Informationssicherheitsniveau aufrechtzuerhalten. Dafür maßgeblich sind das Datenschutz- und Informationssicherheitsmanagementsystem (DSMS/ISMS) der TI.

Von besonderer Bedeutung im laufenden Betrieb sind hierbei zwei Dinge: Zum einen melden die Anbieter Datenschutzverstöße, Informationssicherheitsvorfälle und Risiken an die gematik. Zum anderen übermitteln Anbieter regelmäßig Kennzahlen, anhand derer die gematik Rückschlüsse auf das aktuelle Datenschutz- und Informationssicherheitsniveau ziehen kann. Im Einzelfall kann die gematik die Situation des Datenschutzes und der Informationssicherheit auch vor Ort beim Anbieter prüfen lassen.

4 | DIE ELEKTRONISCHE GESUNDHEITSKARTE

Im Hinblick auf den Datenschutz und die Informationssicherheit ist die eGK das wichtigste Instrument in der Hand des Versicherten.

4.1 Die elektronische Gesundheitskarte als Versicherungsnachweis

Die eGK dient als Nachweis, Leistungen der gesetzlichen Krankenversicherung in Anspruch nehmen zu können. Auf der eGK-Vorderseite befinden sich unter anderem der Name des Versicherten und dessen Krankenversichertennummer, die nach § 290 SGB V lebenslang gültig ist.

Abbildung 2: die Vorderseite der eGK und die Rückseite mit optionaler EHIC

Optional kann auf die Rückseite die europäische Krankenversichertenkarte (EHIC) aufgebracht werden, die innerhalb der EU als Berechtigungsnachweis dient. Um den Missbrauch bspw. einer gestohlenen eGK zu erschweren, zeigt die eGK zudem auf der Vorderseite ein Lichtbild des Versicherten. Davon ausgenommen sind eGKs von Kindern und Jugendlichen bis zum vollendeten 15. Lebensjahr und Versicherten, die an der Erstellung des Lichtbilds nicht mitwirken können, wie bspw. bettlägerige Patienten.

Die eGK ist jedoch kein rechtsgültiges Personaldokument, wie der Personalausweis. Es ist daher für die Krankenkassen nicht erforderlich, die Identität der Versicherten bei der Lichtbildübermittlung mit Hilfe eines Personaldokuments wie des Personalausweises zu prüfen. Die eGK speichert gemäß § 291 Abs. 2 Satz 1 SGB V die Versichertenstammdaten im Prozessorchip. Mit ihnen weist der Versicherte die Berechtigung zur Inanspruchnahme medizinischer Leistungen der gesetzlichen Krankenversicherung nach. Die VSD beinhalten hierfür die sogenannten administrativen Daten – z. B. Informationen zur Krankenkasse, zum Versicherungsschutz oder zur Kostenerstattung – sowie persönliche Angaben zum Versicherten wie den Namen, das Geburtsdatum, das Geschlecht und die Adresse. Zudem können sensible Informationen wie bspw. die Angabe zum Zuzahlungsstatus enthalten sein. Diese Daten sind vor unberechtigtem Lesen technisch geschützt (vgl. Abbildung 4). Der technische Schutz sensibler Informationen auf der eGK verbessert die Situation gegenüber der alten Krankenversichertenkarte.[3]

Auf dieser war ein Schutz der Daten technisch nicht vorgesehen und die Daten waren mit einem Kartenlesegerät frei auslesbar.

4.2 Die eGK als Bestandteil der TI

Zusätzlich zu den administrativen Daten wird es in späteren Ausbaustufen der TI möglich sein, mit Hilfe der eGK auch medizinische Daten zu speichern, falls der Versicherte dies wünscht. Auch hierfür sind bereits entsprechende Sicherheitsverfahren vorgesehen. In der ersten Einführungsstufe der TI werden den Versicherten jedoch noch keine freiwilligen Anwendungen angeboten.

eGK speichert digitale Schlüssel des Versicherten

Mit den auf der eGK gespeicherten digitalen Schlüsseln werden die Daten des Versicherten in der TI technisch geschützt. Für unterschiedliche Zwecke speichert die eGK hierzu auch verschie-

dene Schlüssel, etwa zum Ver- und Entschlüsseln von Daten, mit denen der Versicherte sich in der TI ausweist. Die sicherheitstechnischen Anforderungen an diese Schlüssel werden vom BSI entsprechend dem aktuellen Stand der Technik festgelegt. Auf dieser Grundlage werden die Karten von den Krankenkassen ggf. ausgetauscht, um ein gleichbleibendes Schutzniveau zu gewährleisten.

PIN und PUK des Versicherten

Sobald für den Versicherten medizinische Anwendungen in der TI zur Verfügung stehen, teilt die Krankenkasse dem Versicherten in einem PIN/PUK-Brief diese persönlichen Geheimnummern mit.

Die PIN ist sechsstellig und kann dann durch den Versicherten geändert werden. Der PUK besitzt acht Stellen und ist unveränderbar.

Wird dreimal nacheinander eine falsche PIN eingegeben, ist die eGK für weitere PIN-Eingaben gesperrt. Auf Objekte, die durch die PIN geschützt sind, kann in diesem Zustand nicht zugegriffen werden.

Mit dem PUK kann der Versicherte die Karte wieder entsperren. Nach zehnmaliger Eingabe des PUK ist die Karte endgültig für PIN-Eingaben gesperrt.

Schutz bei Verlust der eGK

Verliert der Versicherte seine eGK, sollte er dies unverzüglich seiner Krankenkasse melden. Die Krankenkasse sperrt dann die eGK. Ähnlich wie bei Bank- und Kreditkarten. Mit einer gesperrten Karte ist sowohl ein Zugriff auf die Daten als auch eine Inanspruchnahme von Leistungen nicht mehr möglich.

Zwei-Karten-Prinzip schützt medizinische Daten

Die ggf. mittels der eGK gespeicherten medizinischen Daten – ebenso wie die geschützten Versichertendaten (GVD, vgl. Kapitel 6) – sind durch ein sogenanntes Zwei-Karten-Prinzip geschützt.

Für diese Daten bedeutet dies, dass außer der eGK selbst gleichzeitig noch der Heilberufsausweis (HBA) eines Heilberuflers in ein Kartenterminal gesteckt sein muss.

Bei den medizinischen Anwendungen der späteren Ausbaustufen ist zudem für einen Zugriff auf die Daten grundsätzlich eine Autorisierung des Versicherten durch Eingabe der PIN seiner eGK erforderlich.

Dies ist mit einem Schließfach vergleichbar, das sich in der eGK befindet und das nur durch einen zusätzlichen Schlüssel – den HBA – und später auch die PIN der eGK, die nur der Versicherte kennt, geöffnet werden kann.

Durch das Zwei-Karten-Prinzip und ggf. zukünftig die PIN der eGK wird technisch verhindert, dass jemand mit einer gefundenen oder gestohlenen eGK Zugriff auf die medizinischen Daten und die GVD des Versicherten erhält.

Es verhindert aber auch, dass Versicherte gegen ihren Willen zur Übergabe der eGK gedrängt werden – etwa in einem Vorstellungsgespräch oder beim Abschluss einer Lebensversicherung. Allein der Besitz der eGK ist nicht ausreichend, auf die medizinischen Daten des Versicherten zugreifen zu können.

Damit auch Mitarbeiter von Ärzten, Zahnärzten und Apothekern sowie medizinisches Personal in Krankenhäusern auf die Daten des Versicherten im Rahmen der medizinischen Versorgung zugreifen

können, gibt es eine weitere Karte: die sogenannte Security Module Card Typ B (SMC-B). Eine SMC-B kann für eine Arztpraxis, Zahnarztpraxis, Apotheke oder ein Krankenhaus ausgestellt werden.

Sie dient genauso wie der HBA als Schlüssel. Mit ihr können die Mitarbeiter der entsprechenden medizinischen Institution auf genau die Daten des Versicherten zugreifen, auf die auch der HBA des Heilberuflers der jeweiligen Institution zugreifen kann (bspw. sind die Rechte einer SMC-B einer Zahnarztpraxis gleich denen eines HBA eines Zahnarztes).

Allerdings nur, wenn dies zuvor der entsprechende Arzt, Zahnarzt oder Apotheker genehmigt hat. Zum Erhalt des HBA müssen die Heilberufler ihre Berufsgruppenzugehörigkeit nachweisen.

Damit wird ausgeschlossen, dass Unbefugte einen Heilberufsausweis erhalten. Auch medizinische Institutionen müssen durch eine dritte Stelle – in der Regel eine übergeordnete Standesorganisation – bestätigt werden, bevor sie eine SMC-B erhalten.

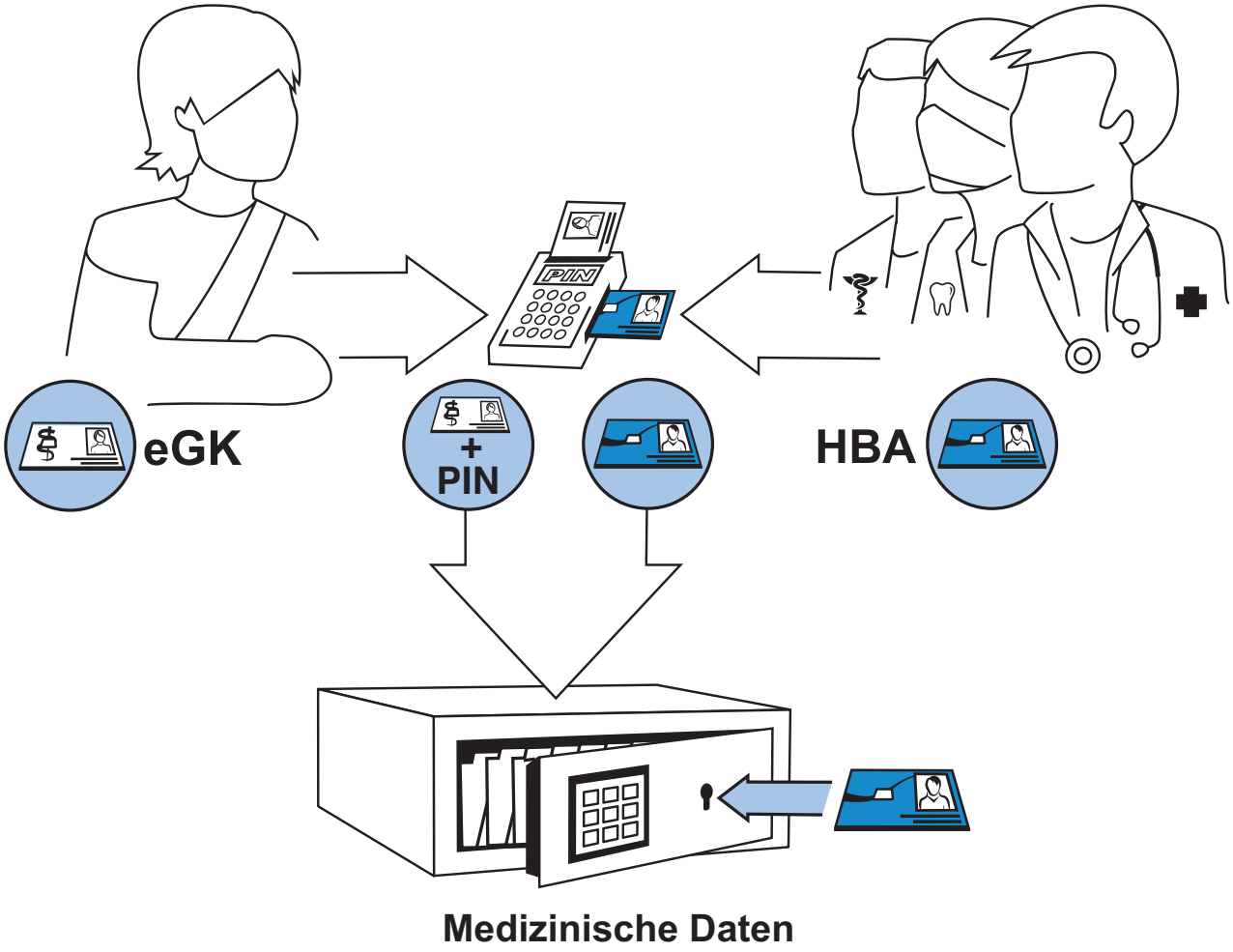


Abbildung 3: Zusammen mit einem HBA kann auf die medizinischen Daten des Versicherten zugegriffen werden

Daten sind technisch geschützt

Die eGK ist vergleichbar mit einem Aktenschrank mit verschiedenen Schließfächern für die Daten des Versicherten. Die Schließfächer unterscheiden sich dabei in der Art, wie sie zu öffnen sind.

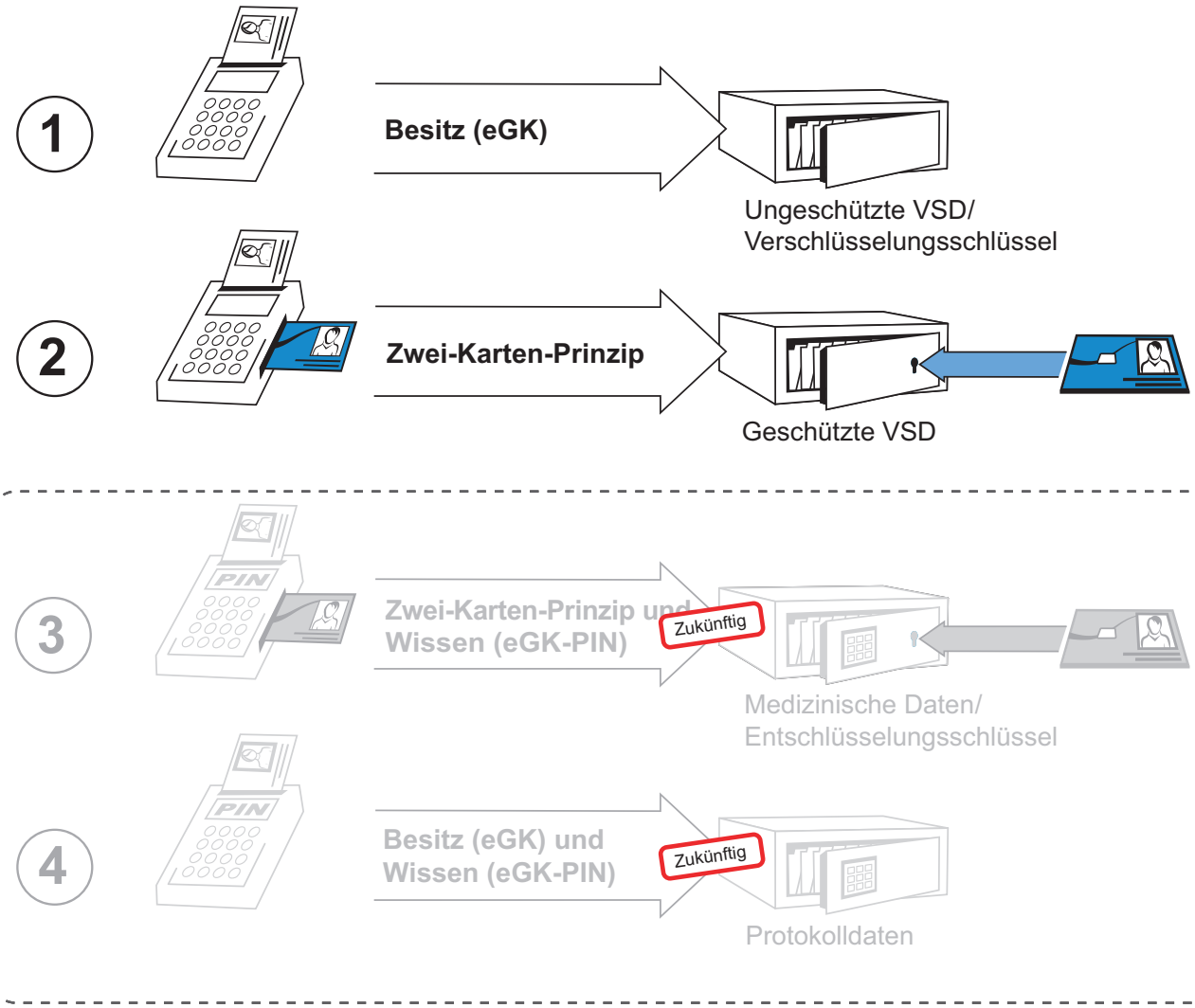


Abbildung 4: Die Daten auf der eGK sind unterschiedlich geschützt

1. Es gibt Fächer, die allein durch den Besitz der eGK geschützt sind (vgl. Abbildung 4). Diese sind somit von jedem zu öffnen, der die eGK und ein Kartenlesegerät mit dazugehöriger Software besitzt. Darin liegen z. B. die VSD des Versicherten, die zum Teil auch auf der eGK aufgedruckt sind.

2. Andere Fächer der eGK können zusammen mit einem HBA geöffnet werden – vorausgesetzt, dieser besitzt die dafür notwendigen Berechtigungen. Es handelt sich dabei um das bereits beschriebene Zwei-Karten-Prinzip (vgl. Abbildung 4). Anstelle des HBA kann hierzu auch die Institutionskarte SMC-B genutzt werden. In einem solchen Fach liegen z. B. die geschützten VSD.[3]

3. Zudem wird es in späteren Ausbaustufen Fächer geben, die nur zusammen mit einem HBA oder einer SMC-B mit den notwendigen Zugriffsrechten und einer zusätzlichen PIN-Eingabe des Versicherten geöffnet werden können (vgl. Abbildung 4). In einem solchen Fach liegt z. B. der Entschlüsselungsschlüssel des Versicherten.[4] Mit diesem Schlüssel werden die verschlüsselten Daten wieder zu einem lesbaren Klartext entschlüsselt. Diese Fächer sind auch für die medizinischen Daten des Versicherten in späteren Stufen der TI vorgesehen.

4. Schließlich wird es Fächer geben, die nur mit der PIN des Versicherten geöffnet werden können (vgl. Abbildung 4). In einem solchen Fach liegen z.B. die Protokolldaten der letzten 50 Zugriffe auf die Daten des Versicherten. Am Protokolleintrag erkennt der Versicherte, welcher Heilberufler zu welcher Zeit auf welche Anwendung zugegriffen hat.

5 | DIE INFORMATIONSSICHERHEITS-ARCHITEKTUR DER TI

Die Informationssicherheitsarchitektur der TI bildet sich sowohl in organisatorischen als auch in technischen Maßnahmen ab. In den folgenden Abschnitten werden die Komponenten und Dienste sowie deren Datenschutz- und Informationssicherheitsleistungen erläutert.

Unterscheidung in TI-Plattform und Fachanwendungen

Die TI unterscheidet zwischen der TI-Plattform (Abschnitt 5.1) und den Fachanwendungen (Abschnitt 5.2). Dabei bietet die TI-Plattform übergreifende, grundlegende Funktionalitäten und die Infrastruktur, die die Fachanwendungen nutzen können. Dies gilt auch für die Sicherheitsfunktionen in der TI.

Unterteilung in Zonen

Mittels der Zonen der TI ist geregelt, welche Komponenten und Dienste miteinander Daten austauschen dürfen. Abbildung 5 liefert eine grafische Übersicht über die Zonen der TI und ihre Verbindung zu den existierenden IT-Systemen der Heilberufler und den Bestandssystemen der Krankenkassen. Die in der Abbildung gezeigten Komponenten und Dienste werden im Folgenden näher erläutert.

5.1 Plattform der TI

Die TI-Plattform ist in die dezentrale und die zentrale TI-Plattform-Zone unterteilt.

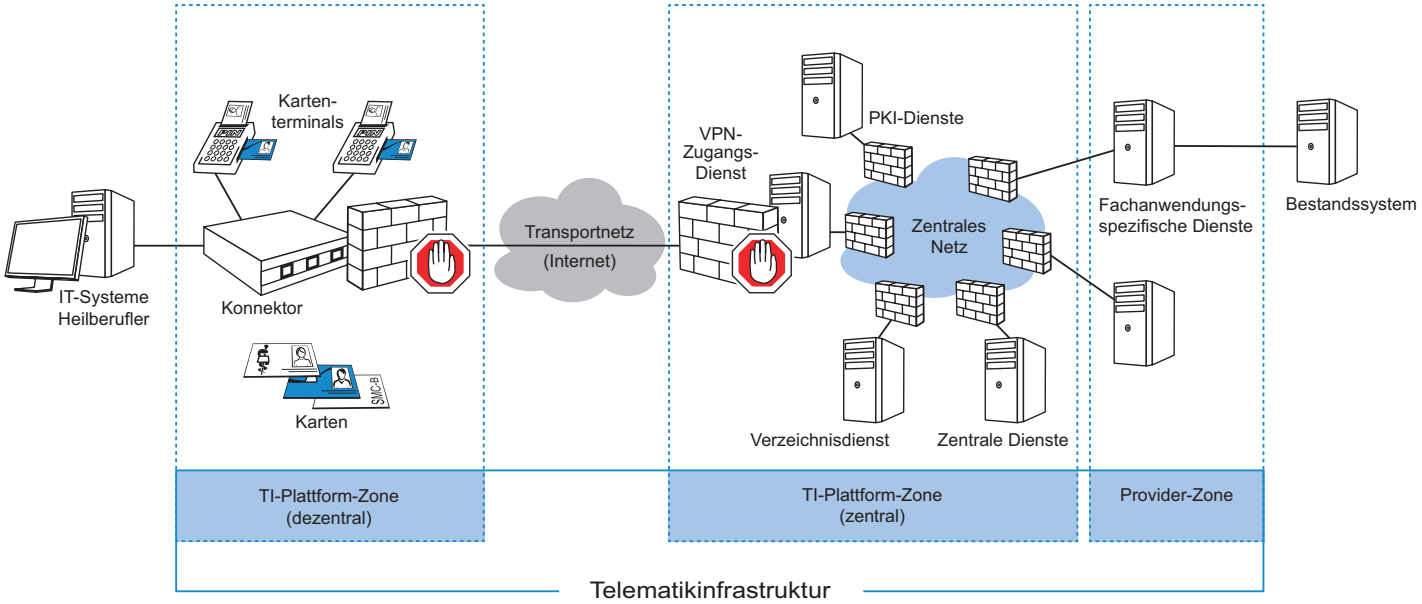


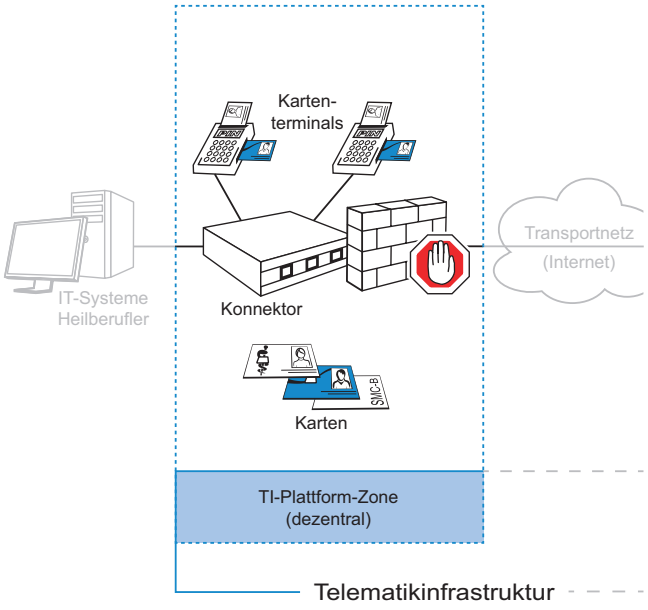
Abbildung 5: die Telematikinfrastruktur im Überblick

Die TI-Plattform liefert die Infrastruktur und stellt darauf aufbauende grundlegende Sicherheitsfunktionen wie bspw. Authentisierung, Signatur und Verschlüsselung zur Verfügung. Die Fachanwendungen müssen das für die durch sie verarbeiteten Informationen notwendige Sicherheitsniveau gewährleisten und nutzen dafür diese Funktionen der TI.

5.1.1 Dezentrale TI-Plattform

Die dezentrale TI-Plattform-Zone enthält die dezentralen Komponenten. Zu diesen gehören sämtliche Karten aller Beteiligten in der TI (eGK, HBA, SMC-B), Kartenterminals, der sogenannte Konnektor sowie Gerätekarten, die den Kartenterminals und Konnektoren eine eindeutige Identität zuordnen. Diese Komponenten kommen in den Umgebungen der Nutzer der TI zum Einsatz, also in den Arzt-

praxen, Krankenhäusern etc. All diese Komponenten müssen nach den Richtlinien des BSI geprüft werden, bevor sie zum Einsatz kommen dürfen. Damit können alle Beteiligten sicher sein, dass die Sicherheit der Daten, die mit den Komponenten verarbeitet werden, stets gewahrt ist.



Karten der Heilberufler

Neben der eGK gibt es weitere Karten in der TI. So besitzen Ärzte, Zahnärzte, Psychotherapeuten und Apotheker den elektronischen Heilberufsausweis. Für die Mitarbeiter in den Institutionen des Gesundheitswesens (Arztpraxis, Krankenhaus, Apotheke), die unter Aufsicht von HBA-Trägern arbeiten, gibt es die SMC-B (Institutionskarte).

HBA und SMC-B der Heilberufler ermöglichen den Zugriff auf medizinische Daten auf der eGK (siehe Kapitel 4). Dabei haben unterschiedliche Gruppen von Heilberuflern auch unterschiedliche Zugriffsrechte (abgestuftes Rollen- und Rechtekonzept). Ein Arzt hat bspw. andere Rechte als ein Apotheker. Dies kommt insbesondere bei den zukünftigen freiwilligen Anwendungen zur Geltung.

Technisch wird der Zugriff gewährt, nachdem sich der HBA oder die SMC-B gegenüber der eGK authentisiert hat (Zwei-Karten-Prinzip). Somit kann nur mit einem HBA bzw. einer SMC-B – sowie ggf. dem Einverständnis des Versicherten – auf Daten der eGK zugegriffen werden. Zur Nutzung seines HBA oder seiner SMC-B muss der Heilberufler eine PIN eingeben. Nur dann ist damit ein Zugriff auf Daten der eGK möglich. Daher ist eine gefundene oder gestohlene Karte eines Heilberuflers für den Zugriff auf eine eGK nutzlos.

Auf dem HBA befindet sich Schlüsselmaterial für eine qualifizierte elektronische Signatur (QES). Mit einer QES versichert der Heilberufler rechtsverbindlich, der Urheber der signierten Daten zu sein. Die QES ist das digitale Pendant zur handschriftlichen Unterschrift.

Wie bei der eGK wird auch bei HBA und SMC-B jede Kartengeneration vor der Ausgabe der Karten durch das BSI geprüft, um deren Sicherheit zu gewährleisten. Zudem werden – wenn dies für den Schutz vor neuartigen Bedrohungen notwendig werden sollte – Karten einer neuen Generation ausgegeben. Das garantiert, dass stets Karten in der TI zum Einsatz kommen, die dem aktuellen Stand der Technik entsprechen.

Zum Erhalt eines HBA bzw. einer SMC-B müssen die Heilberufler einen Nachweis ihrer Berufsgruppenzugehörigkeit erbringen. Damit wird ausgeschlossen, dass Unbefugte eine solche Karte erhalten.

Gerätekarten

Auch der Konnektor und die Kartenterminals besitzen eine eigene Karte. Dabei ist die Konnektorkarte (gSMC-K) fest in diesem verbaut und somit Teil des Konnektors. Die Karten der Kartenterminals (gSMC-KT) sind in diesen dauerhaft gesteckt, aber nicht in diesen fest verbaut. Die Gerätekarten werden bspw. für den Aufbau von geschützten Verbindungen (TLS) verwendet.

Kartenterminals

Die Kartenterminals sind die Bindeglieder zwischen der eGK sowie den Karten der Heilberufler und dem Konnektor. Sie stellen eine transportgeschützte (TLS-)Verbindung zum Konnektor her, sodass die Daten, die von den Karten gelesen bzw. auf die Karten geschrieben werden, unbefugten Personen nicht zur Kenntnis gelangen oder von diesen unbemerkt manipuliert werden können.

Die Kartenterminals für die TI werden als eHealth-Kartenterminals bezeichnet und besitzen ein PIN-Pad, ein Display und mindestens zwei Kartenschlitze, in die jeweils eine eGK und ein HBA bzw. eine SMC-B gesteckt werden können. Zusätzlich gibt es einen Kartenschlitz für die gSMC-KT. Da diese Karte nicht direkt in dem Gerät verbaut ist, wird sie mit einem fälschungssicheren Siegel überklebt, wodurch eine Manipulation am Gerät sofort erkennbar ist. Aufgrund der Verwendung moderner Transportverschlüsselung können keine Daten, die zwischen Karten im Kartenterminal und dem Konnektor ausgetauscht wurden, nachträglich entschlüsselt werden.

Das eHealth-Kartenterminal wird stationär aufgestellt – z. B. in einer Arztpraxis oder in einem Krankenhaus. Damit Heilberufler auch bei einem Hausbesuch oder in anderen Situationen außerhalb der Institution des Gesundheitswesens auf eine eGK zugreifen können, gibt es ein mobiles Kartenterminal. Dieses können Heilberufler zum Patienten mitnehmen, um dort dessen eGK auszulesen. Eine Aktualisierung der VSD ist mit einem mobilen Kartenterminal aktuell nicht möglich.

Konnektor

Die steuernde Komponente vor Ort bei den Heilberuflern ist der Konnektor, der mit den Kartenterminals und mit den IT-Systemen des Heilberuflers verbunden ist. Er stellt die für die Fachanwendungen notwendige Funktionalität (wie bspw. Verschlüsselung) zur Verfügung und bietet diesen und auch direkt dem Heilberufler Sicherheitsfunktionen an. Diese Funktionen können Heilberufler über ihre IT-Systeme nutzen. So können sie vom Konnektor Dokumente verschlüsseln lassen oder mittels ihres HBA über den Konnektor Informationen qualifiziert elektronisch signieren. Auch die bereits beschriebene gegenseitige Authentisierung zwischen Karten wird vom Konnektor gesteuert.

Der Konnektor bildet zudem auf dezentraler Seite den Zugang zur zentralen TI-Plattform. Er baut eine auf Netzebene gesicherte Verbindung (IPsec) zur zentralen TI-Plattform über das Transportnetz (Internet) auf. Sensible Daten, die über diese Verbindung transportiert werden, sind zusätzlich auf Transportebene geschützt (TLS).

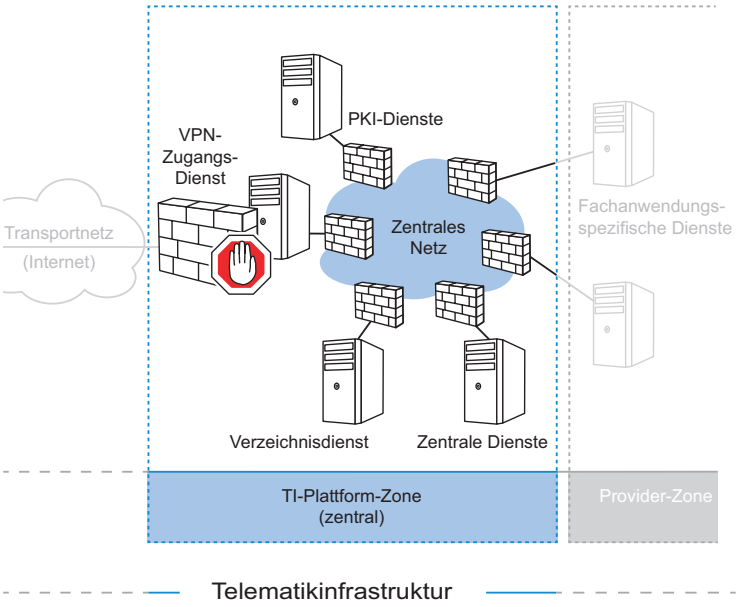
In seiner Funktion als Firewall auf Netz- und Anwendungsebene schützt der Konnektor sowohl die IT-Systeme der Heilberufler als auch die zentrale TI-Plattform. Auf Letzteres ist der Zugriff aus Endnutzersicht überhaupt nur mit einem Konnektor möglich. Die IT-Systeme der Heilberufler werden vor Angriffen aus dem Internet, aber auch vor unberechtigten Zugriffen aus der zentralen TI-Plattform geschützt. Der Anschluss an die TI bedeutet in keiner Weise einen Zugriff von zentralen Diensten der TI-Plattform auf das IT-System des Heilberuflers. Ohne die explizite Interaktion des Heilberuflers werden von seinem IT-System keine Informationen über ihn oder seine Patienten auf die eGK geschrieben oder an Dienste der TI übertragen.

Für die Anwendung VSDM ist dies auch nicht notwendig. Erst für zukünftige Anwendungen, etwa zur Pflege von Notfalldaten auf der eGK, werden medizinische Daten vom IT-System des Heilberuflers an den Konnektor und von dort aus auf die eGK übertragen – vorausgesetzt, der Heilberufler löst dies aus.

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

5.1.2 Zentrale TI-Plattform-Zone

Die zentrale TI-Plattform-Zone enthält die zentralen Dienste der TI-Plattform, welche die Anwendungen der TI mit grundlegenden, anwendungsunabhängigen Funktionalitäten unterstützen.



VPN-Zugangsdienst

Auf der Seite der zentralen TI-Plattform stellt der VPN-Zugangsdienst die Verbindung zwischen dezentraler und zentraler TI-Plattform dar. Bei ihm endet der VPN-Tunnel, der vom Konnektor aufgebaut wird. Dabei werden nur VPN-Verbindungen mit zuvor registrierten Konnektoren zugelassen. Für diese Registrierung beim VPN-Zugangsdienst ist zudem eine SMC-B notwendig. Dadurch können nur medizinische Institutionen mittels des Konnektors über den VPN-Zugangsdienst das zentrale Netz der TI und darüber die zentralen Dienste und fachanwendungsspezifischen Dienste (FAD) erreichen.

Zentrales Netz und Zugangspunkte

Das zentrale Netz der TI verbindet die zentralen Dienste, fachanwendungsspezifischen Dienste und die VPN-Zugangsdienste. Es handelt sich um ein geschlossenes Netz, zu dem der Zugang nur über sichere Zugangspunkte möglich ist. Die Dienste bzw. die Rechenzentren, in denen die Dienste betrieben werden, sind dabei direkt an das zentrale Netz der TI angebunden. Ein Zugriff auf das zentrale Netz der TI aus dem Internet ist somit nicht möglich.

PKI-Dienste

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

Die Identitäten der TI werden in einer Public Key Infrastructure (PKI) verwaltet. Technisch wird eine solche Identität durch ein asymmetrisches Schlüsselpaar – bestehend aus einem öffentlichen Schlüssel (Public Key) und einem dazugehörigen privaten Schlüssel – sowie ein Zertifikat realisiert. Das Zertifikat enthält neben dem öffentlichen Schlüssel Informationen zur Identität des Teilnehmers.

Eine vertrauenswürdige Stelle beglaubigt das Zertifikat und sichert zu, dass die Informationen zur Identität im Zertifikat richtig sind. Insbesondere wird also die Zugehörigkeit eines öffentlichen Schlüssels zu einer Identität beglaubigt. Entsprechend gelten für die Ausgabe von Zertifikaten in der TI besonders hohe Sicherheitsstandards. Diese Zertifikate zum Identitätsnachweis haben eine begrenzte Gültigkeitsdauer und können gesperrt werden.

Das Zertifikat und der öffentliche Schlüssel dürfen jedem in der TI bekannt sein. Den privaten Schlüssel hingegen besitzt allein der Teilnehmer. Der Schutz der Identität hängt unmittelbar mit der Geheimhaltung des privaten Schlüssels zusammen. Daher werden die privaten Schlüssel von Versicherten, Heilberuflern bzw. medizinischen Institutionen und dezentralen Komponenten ausschließlich auf einer Karte – also eGK, HBA bzw. SMC-B oder einer Gerätekarte – gespeichert. Hier sind sie vor dem Auslesen und vor unberechtigter Nutzung geschützt.

Die Identität eines TI-Teilnehmers wird genutzt, wenn dieser sich in der TI ausweist, für ihn verschlüsselt werden soll oder er signiert. Für jeden dieser Zwecke besitzt ein Teilnehmer ein separates Schlüsselpaar und dazugehöriges Zertifikat. Somit wird durch die Prüfung des Zertifikats eindeutig technisch sichergestellt, mit wem eine Kommunikation stattfindet, für wen etwas verschlüsselt wird

oder wer etwas signiert hat. Zudem ist den Teilnehmern der TI über ein gesondertes Zertifikat eine Rolle (bspw. „Arzt" oder „Apotheker") zugeordnet. Darüber wird das in Kapitel 5.1.1 erwähnte Rollen- und Rechtekonzept im Rahmen des Zwei-Karten-Prinzips umgesetzt, das unterschiedlichen Heilberuflerrollen jeweils nur die gesetzlich festgelegten und notwendigen Zugriffsrechte auf Daten der eGK gewährt.

Verzeichnisdienst

Der Verzeichnisdienst ist mit einem Telefonbuch für die TI vergleichbar. Er speichert Zertifikate von Heilberuflern und medizinischen Institutionen, mit denen Informationen für den jeweiligen Teilnehmer verschlüsselt werden können (Verschlüsselungszertifikat). Weiterhin können Informationen gespeichert werden, die spezifisch für eine Anwendung der TI benötigt werden. Ein Beispiel hierfür sind die in der Anwendung KOM-LE (vgl. Kapitel 7) benötigten E-Mail-Adressen von KOM-LE-Teilnehmern.

Die Speicherung von Informationen auf dem Verzeichnisdienst ist freiwillig. Die Informationen sind für jeden Teilnehmer der TI einsehbar.

Weitere zentrale Dienste

Neben den oben genannten Diensten sind in der TI-Plattform weitere Dienste, die Funktionen anbieten, die in jeder Kommunikations-IT-Infrastruktur benötigt werden. Hierzu gehören ein Zeitdienst für eine einheitliche Zeit in der TI sowie ein Namensdienst, um Dienste zu finden. Zudem gibt es einen Konfigurationsdienst, um Software und Konfigurationen der dezentralen Komponenten wie Konnektor und Kartenterminals zu aktualisieren.

5.2 Anwendungen der TI

Anwendungen der TI (z. B. VSDM, Kapitel 6) können aus mehreren Teilkomponenten bestehen. Falls zu einer Anwendung ein oder mehrere zentrale Dienste gehören, sind diese sogenannten fachanwendungsspezifischen Dienste der Provider-Zone zugeordnet. Aufgerufen werden FAD entweder von Clients, die auf Systemen der Heilberufler über die dezentrale TI-Plattform-Zone laufen, oder von Fachmodulen, die in den Konnektoren laufen. Daneben gibt es auch Anwendungen, die nur im Konnektor als Fachmodul realisiert sind und keinen FAD nutzen.

Der Konnektor lässt aus Gründen der Informationssicherheit den Zugriff auf die eGK nur für Fachmodule zu. Daher wird bei Anwendungen, die die eGK nutzen, stets ein von der gematik geprüftes Fachmodul im Konnektor verwendet.

Aus der Informationssicherheitsstrategie der TI folgt, dass Anwendungen der TI dafür verantwortlich sind, den notwendigen Datenschutz sowie die Informationssicherheit einzuhalten. Daraus resultiert, dass alle Anwendungen der TI entsprechend dem Schutzbedarf der durch sie verarbeiteten Informationsobjekte die erforderlichen Maßnahmen ergreifen und im Rahmen der Zulassung nachweisen müssen. Dabei sind auch die entsprechenden Vorgaben des Gesetzgebers zu beachten.

6 | VERSICHERTENSTAMMDATEN-MANAGEMENT

Eine erste Anwendung der TI ist das sogenannte Versichertenstammdatenmanagement (VSDM). Diese Anwendung ist gesetzlich vorgegeben. Die Krankenkasse kann mit dieser Anwendung die eGK eines Versicherten bei Änderungen an den Versichertenstammdaten (VSD) sicher über die TI aktualisieren. Dadurch muss die eGK in den meisten Fällen nicht durch die Krankenkasse ausgetauscht werden.

Krankenkassen aktualisieren VSD auf der eGK

Wenn die VSD auf der eGK eines Versicherten aktualisiert werden müssen, vermerkt die zuständige Krankenkasse dies auf dem Aktualisierungsstatusdienst (ASD[5]). Eine Aktualisierung ist bspw. notwendig, wenn sich die Anschrift des Versicherten oder sein Versichertenstatus – z. B. aufgrund eines Renteneintritts – ändert. Die zu aktualisierenden Daten werden von der Krankenkasse für den Aktualisierungsvorgang über einen weiteren Dienst – den Versichertenstammdatendienst (VSDD) – bereitgestellt.

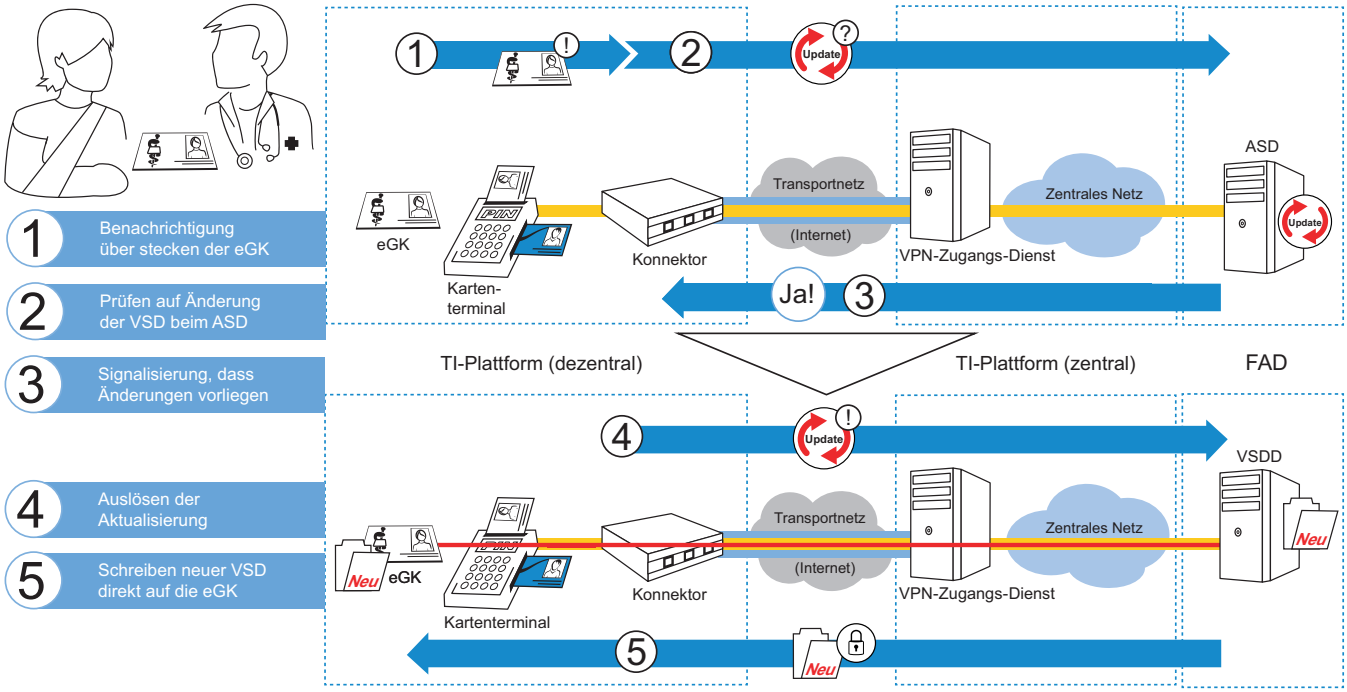


Abbildung 6: Die eGK wird mit den neuen VSD über einen sicheren Kanal über die TI aktualisiert

Sicherung auf Netzebene

Sicherung auf Transportebene

Sicherung auf Anwendungsebene

Gesetzlich geforderte Anwendung

Die Krankenkasse ist gesetzlich verpflichtet, die VSD auf der eGK ihrer Versicherten zu speichern (§ 291 Abs. 2 Satz 1 SGB V) und bei Bedarf zu aktualisieren (§ 291 Abs. 2b Satz 1 SGB V), da diese Daten für den Versicherten zum Nachweis seiner Anspruchsberechtigung sowie für die Abrechnung von Leistungen des Heilberuflers mit der gesetzlichen Krankenkasse erforderlich sind. Da die Krankenkassen gesetzlich zur Speicherung der VSD verpflichtet sind, ist hierfür – anders als bei freiwilligen medizinischen Anwendungen der TI – keine gesonderte Einwilligung des Versicherten erforderlich.

Bei der erstmaligen Inanspruchnahme einer Arztleistung im Quartal ist der Arzt verpflichtet, die eGK online zu prüfen. Hierbei wird beim Aktualisierungsstatusdienst geprüft, ob für die jeweilige Karte eine Aktualisierung vorliegt. Dies muss jedoch nur geschehen, sofern die eGK bei dem jeweiligen Arzt im laufenden Quartal bisher noch nicht geprüft wurde.

Dieser Vorgang verläuft über die auf Netzebene gesicherte Verbindung zwischen Konnektor und VPN-Zugangsdienst und ist zusätzlich auf Transportebene zwischen Konnektor und Aktualisierungsstatusdienst geschützt.

Müssen die VSD auf der eGK aktualisiert werden, wird zusätzlich zu den oben genannten Sicherheitsmaßnahmen eine auf Anwendungsebene gesicherte Verbindung (Secure Messaging) direkt zwischen der eGK und dem VSDD aufgebaut, auf dem die neuen VSD des Versicherten abgelegt sind.

Die Verbindung wird mit einem Schlüssel gesichert, der auf der eGK gespeichert ist und sonst nur der Krankenkasse des Versicherten bekannt ist. Der Schlüssel ist dabei für jede eGK einzigartig. Dadurch kann die abhör- und manipulationssichere Verbindung von einer Krankenkasse ausschließlich zu ihren eGKs aufgebaut werden. Die Krankenkasse schützt ihre IT-Systeme entsprechend den für sie geltenden Vorschriften des Datenschutzes nach SGB V und SGB X – und damit auch die in den IT-Systemen gespeicherten Schlüssel der eGK.

Die aktuellen VSD werden dann vom Versichertenstammdatendienst direkt zur eGK durch den sicheren Kanal transportiert (Ende-zu-Ende-Schutz) und dort gespeichert. Dank der sicheren Verbindung kann niemand unberechtigt die VSD einsehen. Auf der Transportstrecke über das Internet sind die Daten auf drei Ebenen geschützt: Netzebene, Transportebene und Anwendungsebene (vgl. Abbildung 6).

Auf der eGK wird protokolliert, wo die VSD zu welcher Zeit aktualisiert wurden. Zur Einführung medizinischer Anwendungen in späteren Stufen der TI wird es für Versicherte Möglichkeiten zur Einsicht in das eGK-Protokoll geben. Die Krankenkasse protokolliert in ihren Systemen ebenfalls, wann welche VSD auf welche eGK geschrieben wurden.

Arztbezug wird anonymisiert

Die Krankenkasse muss nicht wissen, wo die eGK eines Versicherten geprüft und falls erforderlich aktualisiert wurde. Sie muss lediglich wissen, um welche eGK es sich handelt. Die TI anonymisiert daher den Bezug zum Heilberufler so, dass die Krankenkasse nicht erkennt, von welchem Heilberufler aus die eGK durch den Fachdienst VSDM geprüft und aktualisiert wird.

Krankenkassen erteilen Auskunft

Krankenkassen müssen den Versicherten auf Anfrage über die auf der eGK gespeicherten Versichertenstammdaten und die durchgeführten Aktualisierungen Auskunft geben. Hierzu können Versicherte die bereits bestehenden Auskunftsprozesse der Krankenkassen weiterhin nutzen.

Die Krankenkasse ist als Herausgeberin der eGK zudem gesetzlich dazu verpflichtet, die Versicherten darüber zu informieren, wie sie ihre Datenschutzrechte ausüben können. Hierfür werden in einer späteren Ausbaustufe mit der Einführung medizinischer Anwendungen die Möglichkeiten zur Wahrnehmung des Auskunftsrechts – z. B. die Auskunft über die Zugriffe auf die mittels der eGK gespeicherten medizinischen Daten – bereitgestellt.

7 | SICHERE KOMMUNIKATION ZWISCHEN HEILBERUFLERN

Die Anwendung „Sichere Kommunikation zwischen Leistungserbringern[6] "(KOM-LE) ist eine Anwendung der TI, nutzt jedoch nicht die eGK. Es handelt sich um eine Anwendung für Heilberufler, die damit sicher – das heißt Ende-zu-Ende-verschlüsselt und mit gesicherter Authentizität der Kommunikationspartner – per E-Mail kommunizieren können.

Da die Anwendung nicht die eGK betrifft, ist sie nicht im Gesetz verankert. Heilberuflern ist freigestellt, ob sie die Anwendung nutzen.

Im Rahmen der Behandlung eines Patienten ist in vielen Fällen eine Kommunikation zwischen verschiedenen Heilberuflern notwendig. So müssen bspw. Röntgenbilder und Laborwerte dem behandelnden Arzt übermittelt werden oder Heilberufler, die an der Behandlung eines Patienten beteiligt sind, tauschen sich fachlich aus. KOM-LE bietet die technischen Voraussetzungen, dem Schutzbedarf sensibler Patientendaten gerecht zu werden.

Ausschließlich registrierte Teilnehmer

Die Anwendung KOM-LE ist allein Heilberuflern, medizinischen Institutionen und Leistungserbringerorganisationen vorbehalten. Dass nur diese berechtigten Teilnehmer KOM-LE verwenden, wird durch die notwendige Registrierung beim KOM-LE-Anbieter sichergestellt.

Bei dieser wird die Identität des Teilnehmers technisch über dessen Zertifikat geprüft.

Bei der Registrierung hinterlegen die Teilnehmer ein Passwort, das sie später bei der Nutzung beim KOM-LE-Fachdienst angeben müssen, um Nachrichten senden und empfangen zu können.

Ende-zu-Ende-Verschlüsselung

Wird bei kommerziellen E-Mail-Providern mit Verschlüsselung geworben, ist oftmals eine Transportverschlüsselung gemeint.

Dabei werden die E-Mails auf dem Versandweg zwischen den Kommunikationspunkten geschützt, damit niemand den Inhalt lesen kann, wenn er die E-Mail dazwischen abfängt. An den Kommunikationspunkten selbst liegt die E-Mail unverschlüsselt vor.

Einer dieser Punkte ist jedoch immer der E-Mail-Provider, da dort die E-Mails vorgehalten werden, bis der Empfänger diese abruft.

Der Provider kann (rein technisch betrachtet) in diesem Fall – auch wenn er besonders strengen Datenschutz- und Informationssicherheitsanforderungen unterliegt – alle gesendeten Nachrichten einsehen.

Dies steht bei medizinischen Daten im Widerspruch zur ärztlichen Schweigepflicht nach § 203 StGB.

Bei KOM-LE werden die Nachrichten daher vor dem Versand automatisch individuell für den/die Empfänger verschlüsselt.

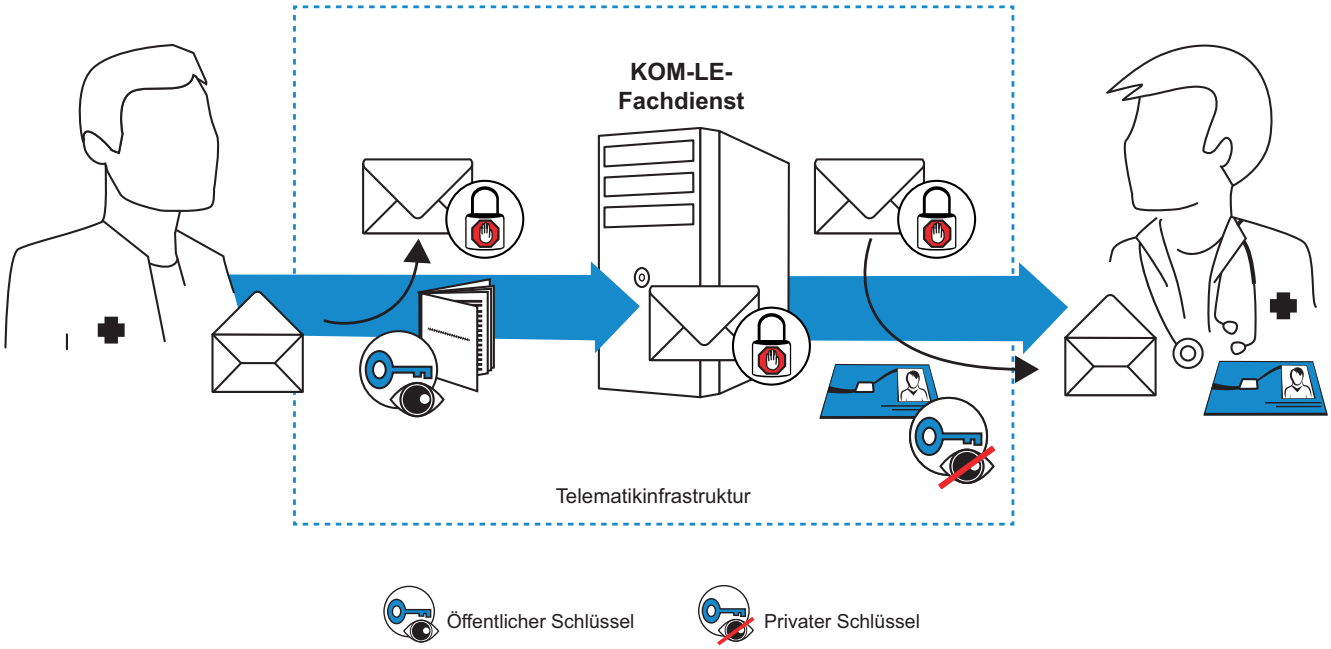
Nur ein rechtmäßiger Empfänger kann somit den Inhalt der Nachricht lesen. Der KOM-LE-Fachdienst, der als E-Mail-Provider fungiert, ist technisch nicht in der Lage, Nachrichten einzusehen.

Diese Daten können die KOM-LE-Teilnehmer vom Verzeichnisdienst der TI-Plattform abrufen.

Gesicherte Authentizität von Sender und Empfänger

Ausschließlich KOM-LE-Anbieter können für die registrierten Nutzer die KOM-LE-E-Mail-Adresse zu deren Verzeichniseintrag hinzufügen. Somit ist es unmöglich, einen gefälschten Eintrag zu erzeugen,

Abbildung 7: Ende-zu-Ende-Verschlüsselung bei KOM-LE



Dies schützt ebenfalls den KOM-LE-Anbieter. So kann er auch nicht unbeabsichtigt – etwa bei administrativen Tätigkeiten auf dem Server – medizinische Daten einsehen.

Auch sinkt damit für den Anbieter der technische und wirtschaftliche Aufwand, den er für den Schutz der E-Mails aufbringen müsste. Für die Ver- und Entschlüsselung wird das dafür vorgesehene kryptografische Material des HBA bzw. der SMC-B verwendet.

Um Nachrichten für einen Empfänger verschlüsseln zu können, ist der öffentliche Teil dieses Materials (das Verschlüsselungszertifikat des Empfängers) notwendig.

bei dem bspw. einem bestimmten Arzt (Name) eine falsche E-Mail-Adresse zugeordnet ist.

Zusätzlich wird vor dem Verschlüsseln von Nachrichten das aus dem Verzeichniseintrag ermittelte Verschlüsselungszertifikat auf Echtheit – also ob es sich um ein echtes Zertifikat der TI handelt – und Gültigkeit geprüft.

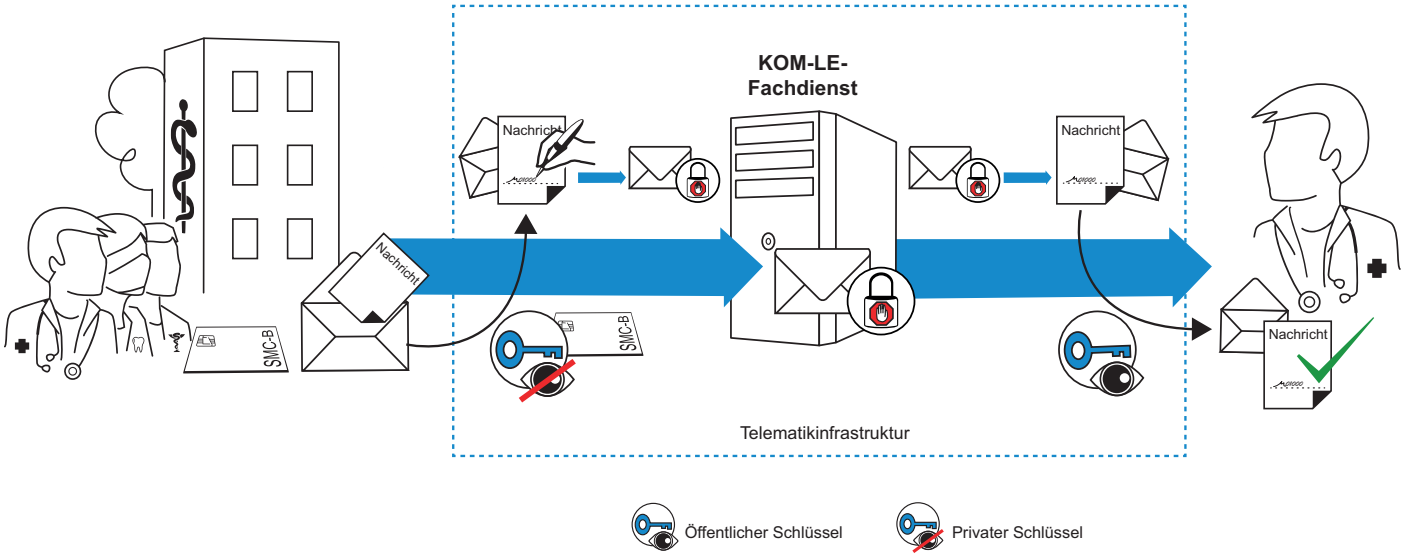
Die Nachrichten werden vor dem Versand automatisch signiert. Dazu wird das dafür vorgesehene kryptografische Material der SMC-B des Senders verwendet.

Der Empfänger kann daher sicher nachvollziehen, von welcher medizinischen Institution oder Organisation des Gesundheitswesens die Nachricht gesendet wurde. Zeitgleich wird durch die Signatur auch die Integrität der Nachricht geschützt, da Änderungen an den signierten Daten zwingend zu einem Fehler bei der Signaturprüfung führen.

Hier werden – wie bei anderen E-Mail-Providern – Nutzername und Passwort für das Senden und Empfangen abgefragt. Auch bekannte Funktionen wie bspw. das Anhängen von Dateien sind möglich.

Der Heilberufler muss also keine zusätzlichen Maßnahmen ergreifen, um mit Ende-zu-Ende-Sicherheit zu kommunizieren.

Abbildung 8: Sicherung der Authentizität und Integrität durch Signatur der KOM-LE-Nachricht



Automatische Informationssicherheit

Ähnlich wie beim Versichertenstammdatenmanagement durchläuft die Kommunikation zwischen Heilberuflern – neben der Sicherung auf Netz- und Transportebene – automatisch sämtliche bereits geschilderten Sicherheitsmaßnahmen durch den in das IT-System des Heilberuflers integrierten KOM-LE-Client. Ist die Anwendung beim Heilberufler eingerichtet, kann dieser mit seinem E-Mail-System wie gewohnt Nachrichten schreiben, senden, empfangen und lesen.

Selbstverständlich kann ein KOM-LE-Nutzer aber weitere Maßnahmen ergreifen und bspw. Dokumente, die an Nachrichten angehängt werden, vorher zusätzlich verschlüsseln oder qualifiziert elektronisch signieren.

8 | FAZIT

Die erste Ausbaustufe der TI legt den Grundstein für einen sicheren Austausch medizinischer Informationen. Auf dieser Grundlage werden in folgenden Ausbaustufen der TI weitere freiwillige medizinische Anwendungen eingeführt, die den Beteiligten benötigte medizinische Informationen aktuell, schnell und sicher zur Verfügung stellen.

Damit dieses Potenzial der TI zunehmend ausgeschöpft werden kann, sind für die sichere Vernetzung des Gesundheitswesens die nachhaltige Stärkung des Datenschutzes und Gewährleistung der Informationssicherheit unerlässliche Rahmenbedingungen für die TI als Datenautobahn.

gematik vernetzt das Gesundheitswesen – sicher

Die TI vernetzt das deutsche Gesundheitswesen und bietet die sichere Basis für eine Vielzahl von medizinischen Anwendungen.

Mit der Sicherstellung von Interoperabilität, Datenschutz und Informationssicherheit in der TI ist es zuverlässig möglich, Versichertenautonomie und informationelle Selbstbestimmung zu stärken.

Telematikinfrastruktur stärkt den Datenschutz – nachhaltig

Die Maßnahmen und Dienste des Datenschutzes der TI stehen allen Anwendungen der TI zur Verfügung. Die Entwickler von Anwendungen können das Datenschutzniveau in ihren Anwendungen in der TI so mit angemessenem Aufwand einfach erhöhen, ohne selbst Datenschutzmaßnahmen entwickeln zu müssen.

Die TI trägt somit nachhaltig dazu bei, die Datenschutzrechte der Versicherten zu stärken.

9 | QUELLENVERZEICHNIS

[1] GKV-Spitzenverband. Kennzahlen der gesetzlichen Krankenversicherung. Stand Januar 2016.
URL: https://www.gkv-spitzenverband.de/presse/zahlen_und_grafiken/gkv_kennzahlen/gkv_kennzahlen.jsp
(abgerufen am 4.3.2016)

[2] Bundesärztekammer. Ergebnisse der Ärztestatistik zum 31.12.2014.
URL: http://www.bundesaerztekammer.de/ueber-uns/aerztestatistik/aerztestatistik-2014/
(abgerufen am 29.7.2015)

[3] KZBV. KZBV-Jahrbuch 2014.
URL: http://www.kzbv.de/jahrbuch-2014.768.de.html
(abgerufen am 29.7.2015)

[4] ABDA. Die Apotheke – Zahlen, Daten, Fakten 2015.
URL: http://www.abda.de/uploads/tx_news/ABDA_ZDF_2015_Brosch.pdf
(abgerufen 29.7.2015)

[5] DKG. Überblick Krankenhausstatistik 2013. Stand 7.10.2014.
URL: http://www.dkgev.de/dkg.php/cat/5/title/Zahlen_%2526amp%253B_Fakten
(abgerufen am 29.7.2015)

[6] GKV-Spitzenverband. Krankenkassenliste. Stand 29.7.2015.
URL: https://www.gkv-spitzenverband.de/service/versicherten_service/krankenkassenliste/krankenkassen.jsp
(abgerufen am 29.7.2015)

[7] gematik. Spezifikation – Technische Vorgaben.
URL: http://www.gematik.de/cms/de/spezifikation/spezifikation_startseite.jsp
(abgerufen am 29.7.2015)

10 | ANMERKUNGEN

[1] Die Spitzenverbände der Heilberufler sind im Einzelnen Bundesärztekammer, Bundeszahnärztekammer, Deutscher Apothekerverband e. V., Deutsche Krankenhausgesellschaft e. V., Kassenärztliche Bundesvereinigung und Kassenzahnärztliche Bundesvereinigung.

[2] Einzige Ausnahme sind zukünftige elektronische ärztliche Verordnungen nach § 291a Abs. 2 Satz 1 Nr. 1 SGB V. Die Zulässigkeit hierfür basiert auf einer Vereinbarung zwischen der Kassenärztlichen Bundesvereinigung und dem Spitzenverband der Krankenkassen auf der Grundlage von § 87 Abs. 1 Satz 2 SGB V.

[3] Bis Heilberufler jedoch technisch so weit ausgestattet sind, dass sie auf den geschützten Bereich der eGK zugreifen können, sind die geschützten Versichertenstammdaten wie bei der bisherigen Krankenversichertenkarte frei zugänglich.

[4] Der Entschlüsselungsschlüssel kann niemals ausgelesen, sondern nur durch die Karte intern zum Entschlüsseln genutzt werden.

[5] In den Spezifikationen der gematik wird der ASD als Update Flag Service (UFS) bezeichnet.

[6] Der Begriff Leistungserbringer ist in diesem Kontext gleichbedeutend mit dem Begriff Heilberufler.

11 | ABKÜRZUNGSVERZEICHNIS

Kürzel	Erläuterung
ASD	Aktualisierungsstatusdienst
BfDI	Bundesbeauftragte/-r für den Datenschutz und die Informationsfreiheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSMS	Datenschutzmanagementsystem
eGK	elektronische Gesundheitskarte
FAD	fachanwendungsspezifischer Dienst
gSMC-K	Konnektorkarte
gSMC-KT	Karte der Kartenterminals
HBA	Heilberufsausweis
IPsec	Internet Protocol Security
ISMS	Informationssicherheitsmanagementsystem
KOM-LE	sichere Kommunikation zwischen Leistungserbringern
PIN	persönliche Identifikationsnummer
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key (persönlicher Entsperrungsschlüssel)
QES	qualifizierte elektronische Signatur
SGB	Sozialgesetzbuch
SMC-B	Security Module Card Typ B (Institutionskarte)
StPO	Strafprozessordnung
TI	Telematikinfrastruktur
TLS	Transport Layer Security
VSD	Versichertenstammdaten
VSDD	Versichertenstammdatendienst
VSDM	Versichertenstammdatenmanagement

IMPRESSUM

Herausgeber:
gematik Gesellschaft für Telematikanwendungen
der Gesundheitskarte mbH
Friedrichstraße 136 | 10117 Berlin

Redaktion:
Unternehmenskommunikation gematik, Berlin

Gestaltung:
Visuelle Kommunikation Hans Zierenberg, Hamburg
www.zierenbergundrode.de

Druck:
Laserline Druckzentrum Berlin GmbH & Co. KG, Berlin

Bildnachweis:
Infografiken: Ninieta Infografik, Berlin
www.zierenbergundrode.de
Kartengrafik: gematik GmbH, Berlin

Stand: April 2016

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Friedrichstraße 136 I 10117 Berlin I Tel: 030 / 400 41-0
Fax: 030 / 400 41-111 I info@gematik.de I www.gematik.de