Die Basiskonzepte der Sicherheitsarchitektur bei der Einführung der eGK

F. Fankhauser[1] T. Grechenig[2] D. Hühnlein[3] M. Lohmaier[4]

[1] Technische Universität Wien, florian.fankhauser@inso.tuwien.ac.at

[2] RISE - Research Industrial Systems Engineering F&E-GmbH
thomas.grechenig@rise-world.com

[3] secunet Security Networks AG, detlef.huehnlein@secunet.com

[4] Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
manfred.lohmaier@gematik.de

Zusammenfassung

Bei der Einführung der elektronischen Gesundheitskarte (eGK) in Deutschland und der dafür notwendigen Telematikinfrastruktur spielen Datenschutz und die Datensicherheit zentrale Rollen. Die grundsätzliche Konzeption der Sicherheitsarchitektur abgeleitet aus den Prämissen des Deutschen Datenschutzes und seinen Ausprägungen für persönliche Gesundheitsdaten werden dargestellt. Die Kernaspekte der Sicherheitsarchitektur der Telematikinfrastruktur (TI) für die Anwendungen der elektronischen Gesundheitskarte werden erläutert. Die im Feld sicherheitserzeugenden Komponenten werden anhand ihrer Rolle und Funktion in der Gesamtarchitektur erläutert.

1 Einleitung

Gemäß §291a SGB V muss die existierende Krankenversichertenkarte in Deutschland zur Verbesserung der Wirtschaftlichkeit, Qualität und Transparenz der medizinischen Behandlung zu einer elektronischen Gesundheitskarte (eGK) erweitert werden, durch die eine Vielzahl von Telematikanwendungen ermöglicht werden soll. Präziser formuliert wird dabei de-facto eine gesicherte, bundesweite und feingliedrige Telematikinfrastruktur für das Gesundheitswesen aufgebaut, bei der der eGK zwar eine nach außen hin deutlich sichtbare Rolle zukommt, diese gleichzeitig aber aus technischer Sicht nur eine von vielen Teilkomponenten darstellt. Neben den beiden Pflichtanwendungen gemäß §291a Abs. 2 SGB V (elektronisches Rezept und elektronischer Versicherungsnachweis) kann der Versicherte der Nutzung einer Reihe von freiwilligen Anwendungen gemäß §291a Abs. 3 SGB V (dem elektronischen Notfallausweis, dem elektronischen Arztbrief, Anwendungen zur Arzneimitteltherapiesicherheit, der elektronischen Patientenakte, dem Patientenfach und der Patientenquittung) zustimmen. Darüber hinaus ist die Telematikinfrastruktur offen für weitere Mehrwertdienste. Gemäß §291a Abs. 7 SGB V sind die Spitzenorganisationen der Leistungserbringer (Ärzte, Apotheker, etc.) und Kostenträger (Krankenkassen) für den Aufbau der für die Einführung und Anwendung der eGK notwendigen Informations-, Kommunikations- und Sicherheitsinfrastruktur

P. Horster (Hrsg.) · DACH Security · (2007) pp.

(Telematikinfrastruktur) verantwortlich. Hierfür wurde die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) gegründet, die

1. die technischen Vorgaben einschließlich eines Sicherheitskonzepts erstellen (§291b Abs. 1 Satz 1 Nr. 1 SGB V) und das notwendige Sicherheitsniveau der Telematikinfrastruktur gewährleisten muss (§291b Abs. 1 Satz 4 SGB V) sowie
2. die Interessen von Patientinnen und Patienten zu wahren und die Einhaltung der Vorschriften zum Schutz personenbezogener Daten sicherzustellen hat (§291b Abs. 2 SGB V).

Das vorliegende Papier beleuchtet kursorisch einige Aspekte des Datenschutzes und der Datensicherheit bei der Einführung der elektronischen Gesundheitskarte aus der Sicht der konkreten technischen Umsetzung.

Abschnitt 2 beleuchtet die wesentlichen Grundsätze des Datenschutzes bei der Einführung der eGK und skizziert deren Umsetzung. Abschnitt 3 widmet sich dem Überblick über die Sicherheitsarchitektur der geplanten Telematikinfrastruktur in der Form eines Ebenenmodells, das eine strukturierte Vorgehensweise bei IT-Sicherheitsrisiken und Umsetzungsmaßnahmen erlaubt. In Abschnitt 4 werden die technischen Kernkomponenten der Sicherheitsarchitektur sowie deren wesentliche Funktionen erläutert. Die wesentlichen Basiskonzepte werden dabei motiviert und systemisch dargestellt.

2 Wesentliche Datenschutzanforderungen

Die Telematikinfrastruktur richtet sich im Sinne des Gesetzgebers in Deutschland prioritär am Nutzen für den Patienten aus und alle Komponenten, Schnittstellen, Dienste und Prozesse der Gesundheitstelematik müssen daher an vornehmer Stelle den Erfordernissen des Datenschutzes und der Datensicherheit entsprechen. Natürlich gibt es dabei wirtschaftliche und operative Grenzen. Da es sich jedoch um eine bundesweite Gesamtsystematik handelt, die umfassende Volumen an hochpersönlichen Gesundheitsdaten genormt transportiert, ist im Sinne des Prinzips „Kettenstärke = Stärke des schwächsten Gliedes“ eine umfassende und nachhaltige Etablierung von Datensicherheitsprinzipien mit relativ hoher Striktheit beinahe unausweichlich: Kompromisse im Aufbau und im Betrieb sind in der IT ohnehin Legende. Im vorliegenden Fall der Wahrung von Grundrechten der Bürgerinnen und Bürger sind derartige Kompromisse allenthalben im Aufbau und im Test denkbar, nicht jedoch im Last- und Betriebsverhalten.

Die zu schaffenden technischen Verfahren bei der Einführung der elektronischen Gesundheitskarte richten sich dabei an folgenden Datenschutzgrundsätzen aus:

- Datenhoheit für den Versicherten

  Der Versicherte hat die Datenhoheit für alle seine Anwendungen und Gesundheitsdaten in der Telematikinfrastruktur. Ein Prinzip, das er heute nur theoretisch erleben kann. Praktisch liegen große Mengen an Informationstransaktionen vor, die für den Patienten selbst dann intransparent ablaufen, wenn er daran konkretes Interesse hätte. Eine geregelte Telematikinfrastruktur wird schrittweise sicherstellen können, dass der Patient die Datenhoheit letztlich auch praktisch besitzt. In der öffentlichen Diskussion wird hier oft fälschlich von der Gefahr des „gläsernen Patienten“ gesprochen. Faktisch liegt aber der Status des „daten-entrechteten Patienten“ vor. Die faktische und konkrete Etablierung der Da-

tenhoheit für den Patienten ist jedoch genau das Gegenteil des heutigen Status und ist faktisch das einzig brauchbare Mittel gegen den „gläsernen Patienten“.

- Freiwilligkeit

  Die Speicherung von Gesundheitsdaten ist grundsätzlich freiwillig und im Ermessen des Versicherten. Ohne die Einwilligung und Freigabe des Versicherten können die freiwilligen medizinischen Anwendungen nicht genutzt werden. Dieses Prinzip der Freiwilligkeit bewirkt zwar einen deutlichen Mehraufwand bei der Etablierung und eventuell einen verminderten Nutzen bestimmter Anwendungen, ist jedoch eine grundsätzlich notwendige Bedingung für die Akzeptanz einer derartigen Systematik. Eine Aushöhlung dieses Prinzips ist auch im Sinne des Vertrauens der Bürgerinnen und Bürger in die eGK-Systematik nicht zweckmäßig.

- Übernahme und Löschung von Daten

  Der Versicherte kann darüber entscheiden, welche seiner Gesundheitsdaten aufgenommen und welche gelöscht werden. Dies ist ein Prinzip, das als konkreter Umsetzungsaspekt des Hoheitsprinzips anzusehen ist.

- Übergabe von Daten

  Der Versicherte kann darüber entscheiden, ob und welche Daten er einem Leistungserbringer zugänglich macht. Auch dieses Konzept ist ein Konkretisierungsaspekt, wobei der Aufwand im Betrieb dafür in verschiedenen Bereichen durchaus aufwändig sein kann (z.B. Verstecken von Rezepten). Dieses Prinzip und seine Durchsetzung ist sowohl ein zu beachtendes Grundrecht als auch eine wesentliche Garantie, dass Schattentransaktionen im großen Ausmaß vermieden werden können: die Systematik bildet damit einfach das natürliche Verhalten der Patienten in bestimmten Fällen geeignet ab.

- Informations- und Leserecht

  Der Versicherte hat das Informations- und Leserecht, über seine gespeicherten Daten und alle diese Daten betreffenden Vorgänge. Dabei liefert letztlich erst die Etablierung einer geregelten Telematikinfrastruktur die technische Option der Lesbarkeit und Transparenz der den Patienten betreffenden Daten durch ihn selbst. Faktisch liegt dieses Recht heute nur sehr begrenzt vor.

- Allgemeine Datenschutzgrundsätze (Zweckbindung, Datensparsamkeit etc.)

  Neben den genannten eGK-spezifischen Datenschutzgrundsätzen sind selbstverständlich auch allgemeine Datenschutzgrundsätze (Zweckbindung, Datensparsamkeit etc.) zu berücksichtigen. Der Datenschutz in Deutschland ist zwar weltweit verglichen auf hohem Niveau, gleichzeitig ist abzusehen, dass andere Länder mit dem stetigen Wachstum der persönlichen Daten im Netz und dem daraus wachsenden Missbrauchspotential nachfolgen werden.

Über obige Grundsätze und deren Realisierung im Rahmen der Telematikinfrastruktur muss der Versicherte gemäß § 6c BDSG in allgemein verständlicher Form unterrichtet werden. Außerdem hat der Herausgeber der eGK dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen – z.B. in Form von eKiosk-Systemen – in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

Zur Umsetzung dieser Grundsätze tragen insbesondere folgende Bereiche bei:

- Rollen- und Berechtigungsmanagement

Die grundlegenden Rahmenbedingungen des Rollen- und Berechtigungskonzeptes für die auf der eGK gespeicherten Daten sind in §291a SGB V normiert. Beispielsweise ist in den Absätzen 4 und 5 festgelegt, dass auf bestimmte Daten nur Angehörige eines Heilberufes (z.B. Arzt oder Apotheker) mit Einverständnis des Versicherten zugreifen dürfen. Die technische Realisierung dieser gesetzlichen Anforderungen erfolgt durch die Card-to-Card-Authentisierung zwischen eGK und einem Heilberufsausweis (HBA), sowie einer PIN-Eingabe des Versicherten, durch die das Einverständnis dokumentiert wird. Für den Zugriff auf Daten, die nicht auf der eGK, sondern in verschlüsselter Form in entsprechenden Fachdiensten gespeichert werden, existieren entsprechende Online-Verfahren (z.B. unter Verwendung von Objekt- und Service-Tickets), durch die das gesetzlich normierte Berechtigungskonzept auch für Online-Szenarien umgesetzt wird.

- Versichertenzentrierter Audit-Service

  Gemäß §291a Abs. 6 Satz 2 SGB V ist für Zwecke der Datenschutzkontrolle zu gewährleisten, dass mindestens die letzten 50 Zugriffe auf die Daten des Versicherten protokolliert werden. Die Protokollierung des Zugriffs erfolgt auf der eGK sowie in einem versichertenzentrierten Audit-Service, in dem festgehalten wird wer, wann auf welche medizinische Daten zugegriffen hat. Durch technische Maßnahmen in der eGK (z.B. PIN) bzw. im Audit-Service (z.B. versichertenzentrierte Verschlüsselung) wird sichergestellt, dass ausschließlich der Versicherte Zugriff auf diese sensiblen Protokolldaten erhalten kann.

- Systeme zur Wahrnehmung der aktiven Versichertenrechte

  Ein wesentlicher Grundsatz bei der Einführung der eGK ist, dass der Versicherte die uneingeschränkte Hoheit über seine Daten behält – ohne die explizite Einwilligung des Versicherten können die freiwilligen Anwendungen (Notfalldaten, Arzneimitteldokumentation etc.) nicht genutzt werden. Außerdem kann der Versicherte selbst bestimmen, auf welche Daten/Dienste er einem bestimmten Heilberufler Zugriff gewährt. Deshalb ist es – unter Verwendung von eigens dafür in die internationale Normung eingebrachte Chipkartenkommandos (Activate Record und Deactivate Record) - beispielsweise möglich, eine auf der eGK gespeicherte Verordnung vor einem Heilberufler zu „verstecken“ und sie wieder sichtbar zu machen. Für die Wahrnehmung dieser Versichertenrechte werden dem Versicherten entsprechende kostenfrei nutzbare eKiosk-Systeme zur Verfügung stehen.

- Anonymisierung und Pseudonymisierung

  Ein wichtiger Aspekt für den Schutz personenbezogener Daten ist die Anonymisierung und Pseudonymisierung von Daten. Wie in Abschnitt 4.5 erläutert, wird die Identität des Versicherten in der Telematikinfrastruktur pseudonymisiert. Außerdem bleibt bei Versichertenstatusabfragen die Identität des Arztes gegenüber dem Versichertenstammdatendienst durch Einsatz eines vertrauenswürdigen Intermediärs (Broker) verborgen.

3 Das Schichtenmodell der Datensicherheit der eGK

Im Rahmen der Entwicklung des Sicherheitskonzeptes gemäß §291b Abs. 1 Satz 1 Nr. 1 SGB V wurde für die einzelnen Informationsobjekte und Komponenten in der Telematikinfrastruktur [gemGA] eine Schutzbedarfs-, Bedrohungs- und Risikoanalyse durchgeführt, auf deren Grundlage die notwendigen Sicherheitsmaßnahmen festgelegt wurden.

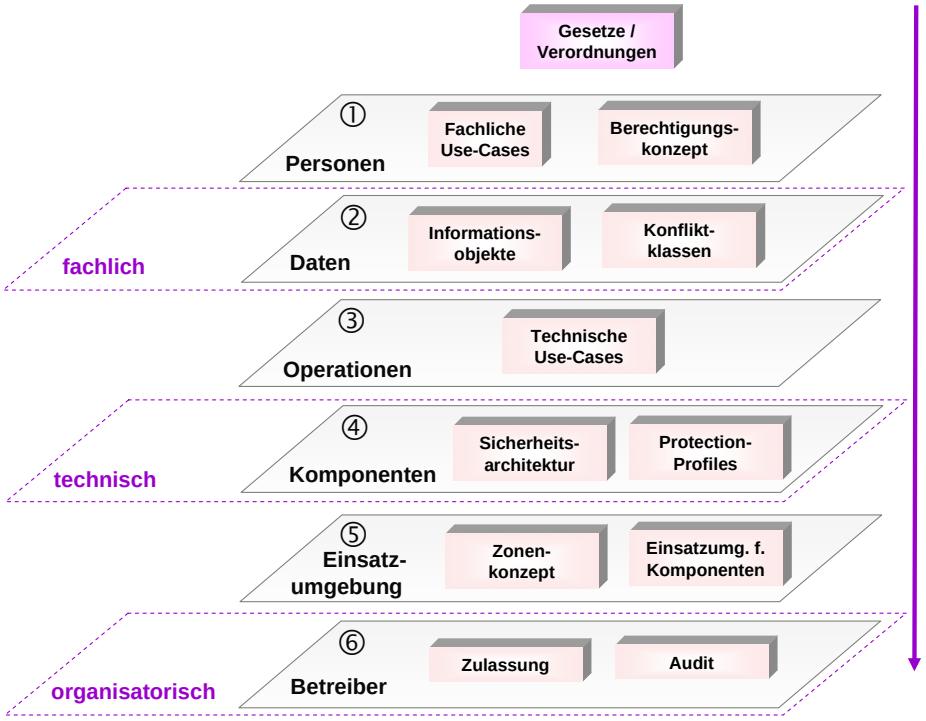

Abbildung 1: Schichtenmodell der Datensicherheit in der Telematikinfrastruktur

Diese Maßnahmen können drei unterschiedlichen konzeptiven Räumen (fachlich, technisch und organisatorisch) zugeordnet werden. Innerhalb der Konzept-Räume wird weitergehend auch danach unterschieden, wer die primären Adressaten dieser Maßnahmen sind (Personen, Daten, Operationen, Komponenten, Einsatzumgebung und Betreiber). Dieser Ansatz berücksichtigt damit den Umstand, dass Sicherheitsarchitekturen dynamischen Charakter haben und im Betrieb der laufenden Anpassung unterworfen werden. Bedrohungen und Risiken können laufend neu aus konkreter medizinischer Pragmatik erwachsen, sie entstehen aus klassischen IT-Angriffen oder folgen aus einer konkreten organisatorischen Handhabung, die sicherheitstechnische Relevanz erzeugt.

Analog zur Identifikation einer Bedrohung oder eines Angriffes liegt dessen Auflösung bzw. die zugehörige Lösungsmaßnahme ebenso im Scope der drei Konzept-Räume vor, wobei Risiko und Lösung nicht zwingend im Rahmen desselben Konzeptes gekoppelt werden müssen: z.B. kann eine Klasse von bestimmten technischen Risiken durchaus organisatorisch abgefangen werden. Dabei leiteten sich die fachlichen Anwendungsfälle und die zentralen Eckpfeiler des Berechtigungskonzepts aus den gegebenen rechtlichen Rahmenbedingungen (Gesetze, Verordnungen etc.) ab (dargestellt als Ebene 1 in Abb.1). Derartige Maßnahmen betreffen primär die handelnden Personen. Aus den fachlichen Anwendungsfällen leiteten sich die grundlegenden Informationsobjekte, entsprechende Konfliktklassen (Ebene 2, Daten) sowie die technischen Use-Cases (Ebene 3, Operationen) ab.

Aus der Betrachtung der technischen Abläufe folgte das Komponentenmodell (Ebene 4). Den einzelnen Komponenten wird hierbei ein entsprechender angemessener Schutzbedarf zugeordnet, wobei sich dieser in erster Näherung aus dem Maximum des Schutzbedarfs der in dieser Komponente verarbeiteten Daten ergibt. Für alle Komponenten erfolgt dabei eine grundlegende Bedrohungs- und Risikoanalyse. Für besonders sensible Komponenten (z.B. Chipkarten, Konnektor, Kartenterminal), deren systematische Position diese zum Sicherheitsträger

der TI macht, werden entsprechende Schutzprofile gemäß Common Criteria erarbeitet, deren Einhaltung als Voraussetzung für die sicherheitstechnische Zulassung der entsprechenden Komponenten dient.

Die Summe und technische Koppelung der sicherheitsrelevanten technischen Komponenten sowie deren normierte Interaktion wird als technische Sicherheitsarchitektur bezeichnet (Ebene 4, Komponenten). Die Kernkomponenten werden in Kapitel 4 dargestellt.

Die einzelnen Komponenten der Sicherheitsarchitektur sind systemisch im Umfeld der für sie vorgesehenen Einsatzumgebung als Sicherheitselemente zu bemessen (Ebene 5). Blackbox-Sicherheitsprüfungen aus diesem Umfeld bilden dabei den Prüfungs- und Risikoraum. Dabei werden die Komponenten mit ähnlichen Anforderungen an ihre technische und organisatorische Einsatzumgebung in einer entsprechenden gemeinsamen Sicherheitszone zusammengefasst. Die unterschiedlichen Zonen sind – z.B. durch entsprechende Firewalls – netzwerktechnisch und organisatorisch voneinander zu trennen. Grundsätzlich können notwendige Sicherheitsfunktionen durch eine Komponente selbst oder – sofern das in der Praxis zuverlässig realisierbar ist – durch entsprechende technische und organisatorische Maßnahmen in der Einsatzumgebung realisiert werden.

Hierbei ist eine systemische Asymmetrie zwischen dezentralen Komponenten (Chipkarten, Kartenterminals, Konnektor etc.) und zentralen Komponenten (Netzdienste, Broker, Fachdienste etc.) zuzulassen. An die Einsatzumgebung für dezentrale Komponenten bei den Leistungserbringern können kaum hohe homogene Anforderungen gestellt werden, weil es die logistischen Umsetzungsaufwände operativ und wirtschaftlich fast unmöglich machen. Deshalb stellen diese Komponenten die Sicherheitsmaßnahmen autark bereit. Bei den zentralen Komponenten, die in Rechenzentrumsumgebungen betrieben werden, können fast alle Sicherheitsanforderungen durch technische und organisatorische Maßnahmen des Betreibers (Ebene 6) realisiert werden.

Die zuverlässige Umsetzung dieser Maßnahmen wird im Rahmen des Zulassungsverfahrens sowie durch entsprechende Audits überprüft. Wesentlich dabei ist auch hier der Grundsatz, dass eine laufende Anpassung der Sicherheitsniveaus prinzipiell vorgesehen ist. Der Erbauer der Systematik (gematik) sollte dazu über die gesamte Aufbauphase die Souvereignität über die Systematik behalten, bis die homogene Bereitstellung der Sicherheitsmechanismen über die gesamte Telematik als gesichert anzusehen ist.

4 Die Kernkomponenten der Sicherheitsarchitektur

Im Rahmen der Einführung der elektronischen Gesundheitskarte ist vorgesehen, dass die Leistungserbringer im Gesundheitswesen über ihre bestehenden Primärsysteme (Praxisverwaltungssystem, Krankenhausinformationssystem, Apothekenverwaltungssystem u.ä.) die unterschiedlichen Dienste der Telematikinfrastruktur nutzen (vgl. Abbildung 2). Damit dies in ausreichend gesicherter Art und Weise geschehen kann, wurden von den IT-System- und Sicherheitsarchitekten mehrere teilweise im Feld bereits vorliegende systemische Komponenten mit entsprechenden Anforderungskatalogen vorgeschlagen: Primärsysteme, Dezentrale Komponenten, Zugangsnetz, Anwendungsinfrastrukturdienste, Public-Key-Infrastrukturen, Card-Application-Management-System (CAMS), Fachdienste, Mehrwertdienste.

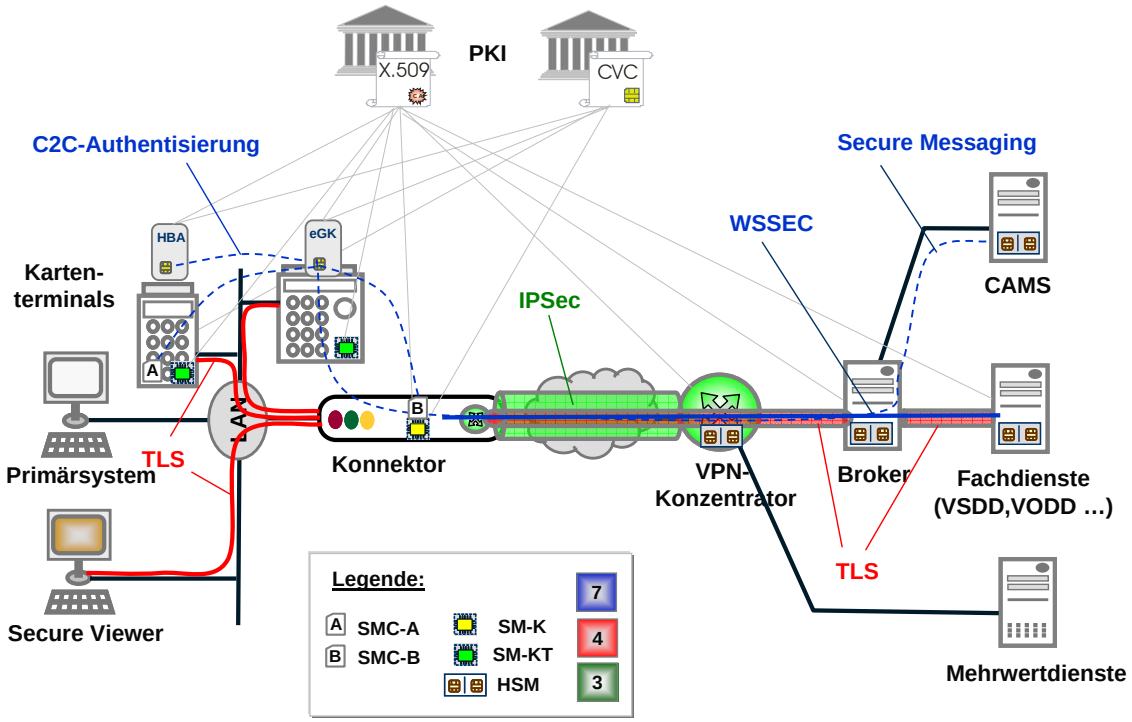

Abbildung 2: Sicherheitsarchitektur zur Einführung der eGK

4.1 Primärsysteme

Die Sicherheitsanforderungen an die Primärsysteme werden nicht durch die Telematikinfrastruktur vorgegeben. Das wäre logistisch inoperabel, da z.B. die Systeme bei den niedergelassenen Ärzten zahlreich sind und ungewöhnlich heterogen. Jedoch werden die Primärsysteme vor Angriffen aus der Telematikinfrastruktur konzeptiv dadurch geschützt, indem es nicht möglich ist Verbindungen aus der Telematikinfrastruktur zu den Primärsystemen aufzubauen. Das impliziert, dass die Leistungserbringer – wie bereits bisher – für ihre Umgebung selbst verantwortlich sind und die Vertraulichkeit und Integrität ihrer Systeme und der lokal gespeicherten und übertragenen medizinischen Informationen sicherstellen müssen. Dadurch bildet sich in der Sicherheitsarchitektur auch trefflich die zugrundeliegende rechtliche Verantwortlichkeit ab.

4.2 Dezentrale Komponenten

Um die Fachdienste der Telematikinfrastruktur (vgl. Abschnitt 4.7) nutzen zu können, werden die Primärsysteme (Größenordnung: 100.000 Arzt- und Zahnarztpraxen, 2.000 Krankenhäuser, 20.000 Apotheken) um sogenannte Konnektoren erweitert (siehe Abbildung 2). Dazu hat der Konnektor sowohl gesicherte Schnittstellen zu den Primärsystemen als auch zur Telematikinfrastruktur.

Der Konnektor besteht aus zwei logischen Teilkomponenten: dem Netzkonnektor und dem Anwendungskonnektor. Hierbei verbindet der Netzkonnektor die lokalen Netze der Leistungserbringer über ein IPSec-basiertes virtuelles privates Netz (VPN) (siehe [RFC2401] und folgende RFCs) in der Rolle eines VPN Clients mit dem VPN-Konzentrator der Telematikplattform. Die Hardware des Konnektors besitzt eine kryptographische Identität (SM-K),

die für die Prüfung der Integrität des Konnektors und für den Aufbau des IPSec-basierten VPN genutzt wird. Für die dynamische Vergabe von IP-Adressen für Konnektoren wird der PPP/IPCP-Mechanismus über L2TP genutzt. Neben der SM-K besitzt der Konnektor eine als PlugIn-Karte im ID-000-Format ausgeprägte Secure Module Card (SMC) Typ B [SMCSpek], die vom Anwendungskonnektor für die Authentifizierung auf Transport- [RFC2246] und Anwendungsebene [WSSec] genutzt wird.

Der Anwendungskonnektor fungiert als Applikations-Proxy zwischen den Primärsystemen der Leistungserbringer und den Fachdiensten der Telematikinfrastruktur. Er realisiert die Ansteuerung der primär involvierten Chipkarten (eGK und Heilberufsausweis (HBA)) über LAN-basierte [SICCT]-Terminals und fungiert hierbei als eine Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG. Hierbei besitzt der Konnektor selbst keine Anzeigekomponente, sondern überträgt bei Bedarf die darzustellenden Daten an das möglicherweise unsichere Primärsystem oder eine vertrauenswürdige Anzeigeeinheit (Secure Viewer).

Medizinische Daten wie z.B. Verordnungen werden durch den Anwendungskonnektor hybrid verschlüsselt und sie existieren somit innerhalb der Telematikinfrastruktur nur in verschlüsselter Form. Letzteres macht den Konnektor zu einer Art definiertes Sicherheitstor in die TI.

4.3 Zugangsnetz

Das Zugangsnetz dient in Verbindung mit den VPN-Konzentratoren der Telematikinfrastruktur zur sicheren Anbindung von zugelassenen Clients an diese. Dazu verbinden sich die Konnektoren über einen VPN-Tunnel mit der Telematikinfrastruktur. Die zu Grunde liegende Zugangsart (ISDN, ADSL, Standleitung,...) ist dabei neutral zu dieser Konzeption.

Die Netzwerk- und Transportschichten (OSI Layer 1-4) implementieren Authentifizierung und Autorisierung von maschinellen Kommunikationsendpunkten, sowie den Schutz der Vertraulichkeit und Integritätsschutz der übertragenden Daten. Die Nichtabstreitbarkeit und weitere Sicherheitsanforderungen werden ausschließlich durch Sicherheitsmaßnahmen in der Applikationsschicht sichergestellt (siehe auch [gemGA]).

Aus dem Zugangsnetz heraus erfolgt kein Verbindungsaufbau zum Konnektor. Alle Verbindungen bei den Leistungserbringern werden vom Konnektor initiiert. Das Zugangsnetz stellt nicht nur eine Verbindung zwischen den Netzen der Leistungserbringer und der Telematikinfrastruktur zur Verfügung, sondern soll auch Zugang zu Mehrwertdiensten bieten. Daher ist eine informationstechnische Trennung erforderlich. Diese informationstechnische Trennung zwischen Telematikanwendungen nach §291a SGB V und Mehrwertdiensten kann auf verschiedene Arten erfolgen. Es muss dabei jedoch sichergestellt sein, dass die Dienste der Telematikinfrastruktur aus dem Leistungserbringernetzwerk ohne Störung durch die Mehrwertdienste erreicht werden können.

Weitere Details zur Realisierung des Zugangsnetzes und der anderen Netze in der zentralen Telematikinfrastruktur sowie damit verbundene Sicherheitsaspekte sind in [gemNetz, gemNS] spezifiziert.

4.4 Anwendungsinfrastrukturdienste

Der Zugriff auf die Anwendungsservices der Fachdienste der Telematikinfrastruktur erfolgt über den Broker, der als Proxy fungiert. Er sorgt für die Lokalisierung von Diensten, das

Schreiben der versichertenzentrierten Auditlogs gemäß §291a Abs. 6 Satz 2 SGB V sowie bei Bedarf für die Anonymisierung bestimmter Fachdienstaufrufe (z.B. bei der Abfrage des Versichertenstatus am Versichertenstammdatendienst des zuständigen Kostenträgers).

Die Anonymisierung erfolgt in zwei Schritten. Zuerst werden Nachrichten aus der Telematikinfrastruktur (Telematik Core Messages), die anonymisiert werden sollen, vom Signature Validation Service (SVS) auf deren Gültigkeit überprüft. Dies geschieht durch die Prüfung der Signatur des Ausstellers der Nachricht. Ist diese Prüfung erfolgreich, wird diese Signatur in einem zweiten Schritt durch den Security Confirmation Service (SCS) bestätigt, indem an Stelle der ursprünglichen Signatur eine neue Signatur durch den SCS angebracht wird. Dadurch wird die Überprüfung der ursprünglichen Signatur bestätigt. Daraus folgt, dass die weiteren Dienste dem Broker vertrauen müssen. Da für viele Nachrichten die Rolle des ursprünglichen Senders wichtig ist, wird die Rolle (z.B. Arzt) in die Nachricht aufgenommen. Die genaue Identität des Leistungserbringers ist jedoch bewusst nicht mehr in der Nachricht enthalten, um das erwünschte Niveau der Anonymisierung zu erreichen.

Zugriffe auf die Fachdienste der Telematikinfrastruktur werden versichertenzentriert auditiert. Dadurch wird erreicht, dass Zugriffe auf medizinische Daten für Zwecke der Datenschutzkontrolle nachvollziehbar sind. Es wird jeweils protokolliert wer, wann auf welchen Dienst zugegriffen hat. Die einzelnen Einträge werden dabei im Audit-Service für den entsprechenden Versicherten verschlüsselt.

4.5 Public-Key-Infrastrukturen

In der Telematikinfrastruktur existieren verschiedene Public-Key-Infrastrukturen. Einerseits werden personalisierte X.509-Zertifikate zur Authentisierung, Verschlüsselung und zur Erstellung elektronischer Signaturen (Willenserklärung) angewendet. Zusätzlich gibt es Zertifikate, welche zu technischen Zwecken auch ohne PIN-Eingabe verwendet werden können. Aus Gründen des Datenschutzes, insbesondere zur Vermeidung der unnötigen Verwendung der „Klarnamen“ der Versicherten, wird bei einem Zertifikat im „CommonName“ eine pseudonyme Identität des Versicherten gewählt. Pseudonym-Zertifikate werden z.B. für den Nachweis, dass bei einer Verordnung die eGK eines Versicherten vorgelegen hat, eingesetzt (vgl. [gemX.509]).

Zudem werden CV-Zertifikate (Card-verifiable-Certificates, CVC [ISO7816-8] (Annex A)) verwendet. Das sind auf die für Chipkarten relevanten Informationen reduzierte Zertifikate, die eine Authentifikation einer Chipkarte gegenüber einer anderen Chipkarte (z.B. HBA/SMC gegen eGK) direkt auf Kartenebene ermöglichen. Durch kodierte Rollen im Datenfeld „Certificate Holder Authorization“ des CV-Zertifikats eines HBA bzw. einer SMC ist nach erfolgreicher C2C-Authentisierung der Zugriff auf Daten in der eGK (z.B. Notfalldaten) oder die Freischaltung eines Schlüssels (z.B. Einlösen einer elektronischen Verordnung) möglich. Entsprechende Zugriffe werden durch eine C2C-Authentisierung abgesichert, da der Zugriff auf diese Datenobjekte bzw. Schlüssel - wie in §291a Abs. 5 SGB V gefordert - nur autorisierten Personengruppen erlaubt ist. CV-Zertifikate dienen nur der Sicherstellung der notwendigen Zugriffsberechtigung (Security Environment) in der eGK entsprechend der durchzuführenden Aktion (z.B. Lesen einer auf der eGK oder auf einem Server gespeicherten Verordnung) (vgl. [gemCVC]).

CV-Zertifikate dienen darüber hinaus zur technischen Echtheitsprüfung auf Kartenebene, so dass es nicht möglich ist elektronische Gesundheitskarten zu „fälschen“. Weitere Informationen hierzu finden sich in [gemCVC].

In der Telematikinfrastruktur kommen zwei Typen von Secure Module Cards (SMC) mit CV-Zertifikaten zum Einsatz. Einerseits die SMC-A, die im Kartenterminal Verwendung findet, und die SMC-B im Konnektor. Auf letzterer sind außerdem X.509-Zertifikate für die Institution des Leistungserbringers gespeichert.

Um aktuelle Sperrinformationen für die X.509-Zertifikate zu erhalten, werden in der Telematikinfrastruktur OCSP-Responder eingesetzt.

4.6 Card-Application-Management-System (CAMS)

Für die Verwaltung der Kartenapplikationen existiert in der Telematikinfrastruktur das Card-Application-Management-System (CAMS). Mit Hilfe des CAMS werden die Applikationen auf der eGK verwaltet und Versichertenstammdaten bei Bedarf aktualisiert.

Das CAMS nutzt dazu symmetrische Schlüssel, die auf der eGK aufgebracht sind und für Zwecke des Secure Messaging gemäß [ISO7816-4] zwischen CAMS und eGK genutzt werden. Weitere Informationen zum CAMS finden sich in [gemCAMS].

4.7 Fachdienste

Die verschiedenen Anwendungen der elektronischen Gesundheitskarte werden durch so genannte Fachdienste realisiert, wobei grob die folgenden Fälle unterschieden werden können:

- Pflichtanwendungen (Versichertenstammdatenmanagement (VSDM) und Verordnungsdatenmanagement (VODM)).
- Freiwillige Anwendungen, die auf Wunsch der Versicherten freiwillig genutzt werden können (z.B. das Speichern von relevanten Notfalldaten im Rahmen des Notfalldatenmanagements (NFDM), das Speichern von Informationen für die Arzneimittelinteraktionsprüfung oder in eine elektronische Patientenakte).
- Anwendungen des Versicherten, die der Versicherte ohne Anwesenheit eines Leistungserbringers nutzen kann.

Alle fachlichen Geschäftsvorfälle zur Nutzung von medizinischen Daten und Anwendungen des Versicherten werden von den Primärsystemen initiiert. Über den Konnektor und die weiteren oben skizzierten Komponenten der Sicherheitsarchitektur gelangt eine Anfrage zur Speicherung oder zum Abruf von Informationen schließlich an den Fachdienst. Dieser authentifiziert die Anfrage, indem die entsprechenden Web-Service-Signaturen (des Versicherten, des Heilberuflers und/oder des Brokers) geprüft werden, so dass bei entsprechender Autorisierung der Zugriff gewährt wird.

In der Telematikinfrastruktur werden Berechtigungen durch Tickets abgebildet. Es wird zwischen Service- und Objekt-Tickets unterschieden, die Definition findet sich in [gemGA]: Service-Tickets realisieren die Autorisierung eines Versicherten für genau einen Leistungserbringer oder einen Vertreter zum Zugriff auf die medizinischen Daten des Versicherten in genau einem Fachdienst. Jedem medizinischen Objekt innerhalb eines Fachdienstes ist genau ein Objekt-Ticket zugeordnet. Objekt-Tickets enthalten die Entschlüsslungsinformation zum Zugriff auf die verschlüsselten medizinischen Daten und die Rechte für berechtigte Leis-

tungserbringer zum Zugriff auf das Objekt. Die vom Versicherten in den ausgestellten Service-Tickets dokumentierten Rechte werden in entsprechender Weise in das Objekt-Ticket übernommen.

Die Prüfung der Zugriffsberechtigung auf Fachdienste erfolgt einerseits durch die auf rechtlich vorgeschriebenen Regeln definierten Rollen (Heilberufler, Versicherte, etc.) und andererseits durch die in den Tickets dokumentierten Berechtigungen. Durch das Ausstellen von Service-Tickets kontrollieren Versicherte somit die Informationsflüsse zum und vom Fachdienst.

5 Zusammenfassung

In diesem Beitrag wurden die prinzipiellen Aspekte des Datenschutzes sowie die daraus abgeleiteten Konzepte der Datensicherheit bei der Einführung der elektronischen Gesundheitskarte kursorisch beleuchtet. Die Sicherheit der Telematikinfrastruktur wird durch unterschiedliche Maßnahmen auf verschiedenen fachlichen, technischen und organisatorischen Ebenen (vgl. Abbildung 1) gewährleistet. Der vorliegende Beitrag stellt dabei lediglich einen schmalen technischen Ausschnitt näher dar. Der interessierte Leser wird auf die umfassenden Spezifikationen der gematik verwiesen [gemSpek].

Referenzen

[BDSG] *Bundesdatenschutzgesetz:* http://www.gesetze-im-internet.de/bdsg_1990/index.html

[gemCAMS] gematik: *Einführung der Gesundheitskarte – Kartenmanagement eGK – Schnittstellenspezifikation Card Application Management Service*, Version 1.1.0 vom 02.03.2007, via http://www.gematik.de/upload/gematik_CMS_Karten_management_eGK_Schnittstellenspezifikation_CAMS_V1_1_0_1665.pdf

[gemCVC] gematik: *Einführung der Gesundheitskarte - PKI für CV-Zertifikate - Grobkonzept*, Version 1.1.0 vom 21.06.2006, via http://www.gematik.de/upload/gematik_PKI_CV-Zertifikate_Grobkonzept_V1_1_0_1566.pdf

[gemGA] gematik: *Einführung der Gesundheitskarte – Gesamtarchitektur*, Version 0.2.0 vom 16.11.2006, via http://www.gematik.de/upload/gematik_GA_Gesamtarchitektur_V0_2_0_1281.pdf

[gemNetz] gematik: *Einführung der Gesundheitskarte – Netzwerkspezifikation*, Version 1.2.0 vom 02.03.2007, via http://www.gematik.de/upload/gematik_INF_Netzwerkspezifikation_V1_2_0_1670.pdf

[gemNS] gematik: *Einführung der Gesundheitskarte – Spezifikation Netzwerksicherheit*, Version 1.0.0 vom 23.02.2007, via http://www.gematik.de/upload/ gematik_Inf_Netzwerksicherheit_V_1_0_0_1669.pdf

[gemSiko] gematik: *Einführung der Gesundheitskarte – Sicherheitskonzept*, Version 1.9.0 vom 03.04.2007

[gemSpek] gematik: *Spezifikationen zur Telematikinfrastruktur für die Einführung und Anwendung der elektronischen Gesundheitskarte*, via http://www.gematik.de (→ Release *n*)

[gemX.509] gematik: *Einführung der Gesundheitskarte* - Festlegungen zu den X.509 Zertifikaten der Versicherten, Version 1.2.0 vom 02.10.2006, via http://www.gematik.de/upload/gematik_PKI_X509_Zertifikate_des_Versicherten_eGK_V1_2_0_1567.pdf

[HBASpek] *Heilberufs-Ausweis und Security Module Card, Teil 2: HBA - Anwendungen und Funktionen*, Version: 2.1.0, via http://www.bmg.bund.de/nn_600148/SharedDocs/Gesetzestexte/Gesundheitskarte/HBA-D2,templateId=raw,property=publicationFile.pdf/HBA-D2.pdf

[ISO7816-4] *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*, ISO/IEC 7816-4, 2005

[ISO7816-8] *Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands*, ISO/IEC 7816-8, 1999

[RFC2246] T. Dierks, C. Allen: *The TLS Protocol - Version 1.0*, RFC2246, via http://www.ietf.org/rfc/rfc2246.txt

[RFC2401] S. Kent, R. Atkinson: *Security Architecture for the Internet Protocol*, RFC2401, via http://www.ietf.org/rfc/rfc2401.txt

[SGB V] *Sozialgesetzbuch – Fünftes Buch (V) – Gesetzliche Krankenversicherung*, via http://bundesrecht.juris.de/bundesrecht/sgb_5/

[SICCT] TeleTrusT e.V.: *Secure Interoperable ChipCard Terminal (SICCT)*, Version 1.1.0 vom 19.12.2006, via http://www.teletrust.de/fileadmin/files/publikationen/Spezifikationen/SICCT_Spezifikation_1.10.pdf

[SigG] *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*, via http://bundesrecht.juris.de/bundesrecht/sigg_2001/

[SMCSpek] *Heilberufs-Ausweis und Security Module Card, Teil 3: SMC - Anwendungen und Funktionen*, Version: 2.1.0, via http://www.bmg.bund.de/cln_041/nn_667298/SharedDocs/Gesetzestexte/Gesundheitskarte/HBA-D3,templateId=raw,property=publicationFile.pdf/HBA-D3.pdf

[WSSec] OASIS: *Web Services Security v1.0*, via http://www.oasis-open.org/specs/index.php#wssv1.0