

# **e-health und Telematiksysteme im Gesundheitswesen**

Dietmar Bremser  
Sebastian Glandien

Eine Ausarbeitung im Rahmen des Seminars  
“Cross-Media”  
Prof. Dr. Rebensburg  
Universität Potsdam  
Sommersemester 2005

## **Zusammenfassung**

Die vorliegende Ausarbeitung illustriert den Prozess der Analyse der Anforderungen und Rahmenbedingungen des für das Jahr 2006 geplanten bundesweiten Einsatzes der Elektronischen Gesundheitskarte, über die Planung einer eigenständigen Architektur dieser Technologie bis hin zur Implementierung.

Vorrangiges Merkmal dieser Technologie sollte vor allem der Medienbruch sein, welcher an den Schnittstellen zwischen Technologien bei der Weitergabe von Daten oder dem Ruf von Funktionen auftritt und allgemein als „Cross-Media“ bezeichnet wird.

Folglich wird in den abschließenden Bemerkungen dieser Dokumentation nicht nur die hier vorgelegte Architektur einer Implementierung mit der gegenwärtigen Referenzarchitektur für eine elektronische Gesundheitskarte verglichen, sondern die hier vorgelegte Architektur hinsichtlich möglicher und vorhandener Medienbrüche diskutiert.

# Inhaltsverzeichnis

<b>1. Vorbetrachtungen</b>	<b>1</b>
<b>1.1 Telematik</b>	<b>1</b>
<b>1.2 Die elektronische Gesundheitskarte (eGK)</b>	<b>1</b>
1.2.1 Gesetzliche Grundlagen	1
1.2.2 Ziele der elektronischen Gesundheitskarte	3
<b>2. Technische Modelle für die elektronische Gesundheitskarte</b>	<b>4</b>
<b>2.1 Ein Überblick</b>	<b>4</b>
<b>2.2 Das Fraunhofer „Referenzmodell“</b>	<b>9</b>
<b>3. Von der Theorie zur Praxis</b>	<b>11</b>
<b>3.1 Szenarien für den Einsatz der elektronischen Gesundheitskarte</b>	<b>11</b>
3.1.1 Gegenwart	12
3.1.2 Patient als Datenträger	13
3.1.3 Datenanbieter Krankenkasse	14
3.1.4 Ärzte-(Daten-)Cluster	15
<b>3.2 Das eigenständige Konzept eines Gesundheitstelematik-Systems</b>	<b>16</b>
<b>3.3 Probleme bei der Implementierung</b>	<b>20</b>
<b>4. Ausblick</b>	<b>22</b>
<b>4.1 „The hidden problem: Cross-Media?“</b>	<b>22</b>
<b>4.2 „The obvious problem: work in progress!“</b>	<b>23</b>
<b>4.3 „The political problem: just think“</b>	<b>25</b>
<b>5. Literaturverzeichnis</b>	<b>28</b>

Für dieses Dokument nebst den begleitenden Materialien gelten bei einer nicht-wissenschaftlichen oder kommerziellen Verwendung zu Gunsten der Autoren Dietmar Bremser und Sebastian Glandien die Urheberrechtsbestimmungen der Bundesrepublik Deutschland zum Zeitpunkt der Niederlegung.

# 1. Vorbetrachtungen

Das Thema dieser Ausarbeitung wie auch der im Rahmen oben genannten Seminars vorgelegten Implementierung nebst Lastenheft war die **elektronische Gesundheitskarte**, in diesem Text abgekürzt auch **eGK**, für welche es galt die Anforderungen, hier besonders die gesetzlichen Rahmenbedingungen sowie die Interessen der beteiligten Parteien, zu eruieren, um darauf aufbauend in einem quasi-industriellen Prozess eine Software-Entwicklung zu betreiben.

Im Folgenden soll die eGK eingeordnet und ihre gesetzlichen Rahmenbedingungen erläutert werden.

## 1.1 Telematik

Die elektronische Gesundheitskarte ist als Technologie dem Bereich der Gesundheitstelematik, international: „health telematics“, zuzuordnen.

Der Begriff der Telematik konstruiert sich semantisch und technologisch aus der *Telekommunikation* und der *Informatik*, womit die Gesundheitstelematik nur eine Fokussierung des Einsatzbereiches dieses abstrakten Begriffes bedeutet.

Das „Telematik-Buch“[1, S. 23] beschreibt Gesundheitstelematik in Abgrenzung zur Telemedizin wie folgt:

Gesundheitstelematik bezeichnet Anwendungen von Telekommunikation und Informatik im Gesundheitswesen. Der etwas enger gefasste Begriff der Telemedizin, bezeichnet hingegen den Einsatz von Telematikanwendungen (Diagnostik, Konsultation, Radiologie, etc.) primär zur Überwindung einer räumlichen Trennung von Patient und Arzt oder zwischen mehreren Ärzten.

In diesen Teilbereich fällt auch das Projekt zur Umsetzung der elektronischen Gesundheitskarte. Die damit verbundenen Dienste spiegeln einen großen Teilbereich der Anforderungen und Bemühungen in der Telemedizin wieder. Das Wissen und die Entwicklung der Komponenten bildet somit eine der modernsten Projekte zur Umsetzung einer modernen Telematik-Infrastruktur

## 1.2 Die elektronische Gesundheitskarte (eGK)

Das Informationsblatt zur Einführung der elektronischen Gesundheitskarte des Bundesministerium für Gesundheit und Soziale Sicherung (BMGS) beschreibt die elektronische Gesundheitskarte (eGK) nicht nur als formalen Wechsel eines Ausweisdokumentes für den Krankenversicherten, sondern als grundlegenden technologischen Wandel für alle Geschäftsprozesse im deutschen Gesundheitssystem[**Fehler! Verweisquelle konnte nicht gefunden werden.**]:

„Ab 2006 wird die elektronische Gesundheitskarte die bisherige Krankenversichertenkarte ersetzen. Die Gesundheitskarte wird technisch so weiterentwickelt sein, dass sie in der Lage ist, neben ihren administrativen Funktionen auch Gesundheitsdaten verfügbar zu machen. ...“

Ferner klärt benanntes Informationsblatt darüber auf, welche Ziele und neuen Funktionalitäten, aber auch welche Vorteile mit diesem Projekt für den Patienten und Arzt (allgemein Heilberufler) verbunden sind.

### 1.2.1 Gesetzliche Grundlagen

Im Rahmen einer europäischen Initiative zur Harmonisierung des Gesundheitswesens sowie einer deutschen Initiative zur Modernisierung der Gesetzlichen Krankenversicherung wurden im § 291 a des Sozialgesetzbuches V (SGB V) die gesetzlichen Anforderungen zur elektronischen Gesundheitskarte mit Wirkung zum 01.01.2004 formuliert, welche ab dem 01.01.2006 an alle Versicherten der Gesetzlichen Krankenkassen abzugeben sind.

Der **Absatz 1** dieses Gesetz formuliert diese Motivation als „*Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz* der Behandlung“.

In **Absatz 2** sind die Pflichtanforderungen an die eGK, genauer alle obligatorisch auf der Karte zu speichernden Daten beschrieben, nämlich „die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form“, explizit von Rezepten, und die Versicherten-Daten, amtlich auch als „Krankenversicherungs-Berechtigungs-nachweis“ bezeichnet. Die Versicherten-Daten umfassen die ausstellende Krankenkasse, den Namen, das Geburtsdatum, die Anschrift des Versicherten wie auch seine Krankenversicherungsnummer, Versichertenstatus, das Gültigkeitsdatum, sein Geschlecht, sein Zuzahlungsstatus sowie die Speicherung eines Lichtbildes. Der Europäische Krankenschein E111 wird vorerst aber nicht in elektronischer Form gespeichert, sondern ist nur als „Sichtvermerk“ auf der elektronischen Gesundheitskarte vorgesehen.

Die eben beschriebenen Daten werden auch als administrativer Teil der elektronischen Gesundheitskarte bezeichnet, weil sie auf die überwiegend auf die Beziehung des Versicherten zu der ausstellenden Institution, der Gesetzlichen Krankenkasse, abstellen.

Der **Absatz 3** des benannten Gesetzes formuliert die Kann-Anforderungen, also jene Daten, welche auf der Karte erst nach Einwilligung des Versicherten zu speichern sind[3]:

1. medizinische Notfallversorgungsdaten (z.B. Blutgruppe, Allergien, Dialyse, Asthma, EKG, kritische Röntgenaufnahmen),
2. elektronischer Arztbrief (Befunde, Diagnosen, Therapieempfehlungen, Behandlungsberichte für einrichtungübergreifende fallbezogene Kooperation),
3. Arzneimitteldokumentation,
4. elektronische Patientenakte (Arztbriefe sowie Impfungen für fall- und einrichtungübergreifende Dokumentation),
5. freiwillige Daten von oder durch den Versicherten, (Fremdsprachenkenntnisse und Organspendenausweis)
6. in Anspruch genommene Leistungen und deren vorläufige Kosten nach § 305 Abs. 2 SGB V.

Die eben beschriebenen Daten des Absatz 3 werden auch als medizinischer Teil der elektronischen Gesundheitskarte bezeichnet, weil sie auf die überwiegend auf die Beziehung des Versicherten zu einem Heilberufler abstellen und damit vertrauliche und sensible Daten repräsentieren.

Im **Absatz 4** setzt der Gesetzgeber Grenzen für die Verarbeitung der Daten in dem Sinne, dass nur die notwendigen Daten zur Versorgung des Versicherten betroffen sein sollen.

Der **Absatz 5** regelt dann den Zugang zu den Daten für Heilberufler, indem von ihnen eine elektronischer Identitätsnachweis, die „Health Professional Card“ vorgehalten werden muss. Dieser Identitätsnachweis soll dann als Autorisierung für den Zugriff auf die elektronische Gesundheitskarte dienen.

Angemerkt sei hier, dass das Signaturgesetz (SigG) in seiner Fassung aus dem Jahre 2001 am Anfang des Jahres 2005 hinsichtlich der Regelungen für Aussteller von elektronischen Zertifikaten, auch als Trust-Center bekannt, erheblich verändert wurden. Obwohl der Gesetzgeber für die „Health Professional Card“ keine konkreten Autorisierungsmechanismen vorschreibt, also auch andere als eine „elektronische Signaturkarte“ ermöglicht, so haben sich die an der elektronischen Gesundheitskarte beteiligten Technologiefirmen wie „Giesecke + Devrient“ als Hersteller von Kartenlesesystemen offensichtlich auf einen derartigen Autorisierungsmechanismus und damit eine „Health Professional Card“ als Träger von den Heilberufler identifizierenden Zertifikaten eingestellt. Folglich liegt die Vermutung nicht fern, dass der §291a SGB V maßgebliches Motiv für die Änderung des SigG war.

Der **Absatz 6** weicht den impliziten Datenschutz des Absatz 3 wieder auf, indem hier laut Gesetz die Aussteller von elektronischen Gesundheitskarten gefordert sind, auf Anforderung des Versicherten alle gespeicherten Daten nach Absatz 3 zu löschen. Dies wird in der Praxis mit hoher Wahrscheinlichkeit bedeuten, dass Aussteller zum Stichtag 01.01.2006 auch die freiwilligen Daten nach Absatz 3 auf den Karten der Versicherten speichern werden und erst nach seinem Widerspruch löschen, obwohl der Absatz 3 an und für sich die Speicherung dieser Daten von der Einwilligung des versicherten abhängig macht.

Der **Absatz 8** verlagert die Datenhoheit auf die Seite des Patienten insofern, dass vom Versicherten nicht verlangt werden kann, einem anderen als den durch das Gesetz Berechtigten Zugriff auf die Daten zu ermöglichen.

Interessant in dem Gesetzgebungsprozess ist auch die Diskussion der Datenschützer um die Verantwortung für den Datenschutz, wobei die Datenschützer maßgeblich die Verantwortung für den Schutz der Daten nicht beim Versicherten sehen[3]:

Verantwortlich für den jeweiligen Datenverarbeitungsvorgang sind diejenigen Personen oder Stellen, die die personenbezogenen Daten für sich erheben oder weiter verarbeiten, egal ob sie dies selbst tun oder durch andere im Auftrag vornehmen lassen (§ 67 Abs. 9 SGB X, § 3 Abs. 7 BDSG, § 2 Abs. 3 LDSG SH). Verantwortliche Stelle kann die Krankenkasse sein (z.B. bei der Ausstellung der eGK oder Erhebung von Abrechnungsdaten, vgl. § 284 SGB V), der Arzt oder ein Krankenhaus, die z.B. Notfalldaten erfassen, ein elektronisches Rezept oder einen elektronischen Arztbrief ausstellen, oder der Apotheker, der ein elektronisches Rezept abrufen, um das Medikament auszugeben.

Die Zweiteilung der Anforderungen des Gesetzgebers an die eGK als Pflicht- und Kann-Anforderungen machen deutlich, dass auch Aspekte des Datenschutzes in das legislative Verfahren eingeflossen sind. Durch den Grundsatz der Freiwilligkeit, dass der Patient entscheiden kann welche Daten gespeichert und gelöscht werden und welche dem Leistungserbringer zugänglich gemacht werden, sollen zentral gespeicherte Datensammlungen vermieden werden.

Bei der gegenwärtigen Planung der elektronischen Gesundheitskarte wird davon ausgegangen, dass erst die Anforderungen des §291a, Absatz 2, SGB V, also des "Krankenversicherungs-Berechtigungsnachweises" und des elektronischen Patientenrezeptes, erfüllt werden und dann sukzessive mit den Kann-Anforderungen, beginnend mit der Arzneimitteldokumentation und den Notfalldaten fortgesetzt wird.

Grundsätzlich ist an dieser Stelle zu bemerken, dass die Anforderungen des Gesetzgebers nur eine „Datensicht“ bedeuten bzw. sich ausschließlich auf die anfallenden Daten beziehen und keinerlei Mechanismen bzw. konkrete Technologien beschrieben sind. Allerdings sind die Technologieträger gehalten, diese Mechanismen, insbesondere mit Fokus auf die Wahrung der Datenintegrität sowie des Datenschutzes, zu realisieren und nachvollziehbar zu gestalten.

### *1.2.2 Ziele der elektronischen Gesundheitskarte*

Zum besseren Verständnis des angestrebten Funktionsumfangs sollen nun zusammenfassend die angestrebten Ziele genannt werden.

Zum Nutzen aller Beteiligten wird eine Verbesserung der medizinischen Versorgung (u.a. der Arzneimittelsicherheit) angestrebt. Insbesondere die Patienten sollen hierbei von besseren patientenorientierten Dienstleistungen profitieren. So sollen Doppelbehandlungen vermieden werden und festgestellte Ursachen und Überempfindlichkeiten keine Komplikationen während späterer Behandlungen in Zukunft verursachen können. Gerade der Bereich Diagnose durch Röntgenaufnahmen ist ein Bereich, wo übermäßige körperliche Belastungen durch Röntgenstrahlung vermieden werden kann. Weiterhin steht im Mittelpunkt der

Bemühungen um die eGK die Stärkung der Eigenverantwortung, Mitwirkungsbereitschaft und -initiative der Patienten.

Es erübrigt sich die Anmerkung, dass die elektronische Gesundheitskarte mittels der Digitalisierung der Datenerfassung, -verarbeitung und -speicherung damit vollständig auf die Geschäftsprozesse in Krankenhäusern, Arztpraxen, Apotheken und sonstigen Einrichtungen der Heilberufe durchgreifen. Auf diese Weise findet eben nicht nur ein Wechsel eines Berechtigungsnachweises statt, sondern es ist auch ein technologischer, mit Kosten verbundener Wandel im Gesundheitswesen vonnöten, welcher auf Seiten der Vertreter der Heilberufe berechnete Kritik hervorruft.

Neben diesen wohlfeilen Zielen ist aber der Tenor seitens der Politik sehr viel eindringlicher, nämlich dass die Einführung der elektronischen Gesundheitskarte vor allem Kosteneffekte, im Sinne der Senkung von Kosten, hervorbringen soll. Die Steigerung der Wirtschaftlichkeit und Leistungstransparenz im Gesundheitswesen erhofft man vor allem mittels der Optimierung der Arbeitsprozesse sowie die Bereitstellung aktueller statistischer Daten zu erreichen. Der hin und wieder beklagte Missbrauch einer Versichertenkarte mittels „Doppelnutzung“ soll auf diese Weise ebenso eingedämmt werden[Fehler! Verweisquelle konnte nicht gefunden werden.].

## **2. Technische Modelle für die elektronische Gesundheitskarte**

In diesem Kapitel sollen die einzelnen Implementierungsansätze für eine elektronische Gesundheitskarte und die gegenwärtige Referenzarchitektur genauer eingegangen und die Vor- bzw. Nachteile analysiert werden.

Ein Konsens aller Technologieträger der Technologieträger der verschiedenen Implementierungsansätze ist der Einsatz oben benannter „elektronischen Signaturkarte“. Diese fungiert als Träger von Zertifikaten, welche ihren Inhaber identifizieren.

Dabei ist aber ein Unterschied zwischen der „Health Professional Card“ als reine „elektronische Signaturkarte“ für die Authentifizierung (elektronische Identitätsprüfung) und Autorisierung (elektronische Zugriffsberechtigungsprüfung) ihres Inhabers sowie der „electronic health card“ (elektronische Gesundheitskarte) als Berechtigungsnachweis des Inhabers und Gegenstand einer Autorisierung festzustellen.

Allerdings ist die technologische Plattform beider Identitätsnachweise die selbe, weshalb die „Health Professional Card“ wie auch die „electronic health card“ zur Gewährleistung der gesetzlichen Anforderungen und der damit eng verbundenen Sicherheitsziele als Mikroprozessorkarte, auch bekannt als SmartCard bzw. Cryptocard, realisiert wird. Diese Technologie verfügt damit über Funktionen zur Authentifizierung, Verschlüsselung und elektronischen Signierung realisiert werden.

In den nachfolgenden Kapiteln soll noch genauer auf die zentrale Komponenten Smartcard und deren Funktionalität im Umfeld der Infrastruktur eingegangen werden.

### **2.1 Ein Überblick**

Im Bereich der Telemedizin existierten lange vor den Bemühungen zur Umsetzung einer elektronischen Gesundheitskarte Projekte, welche sich mit der Vereinfachung und Optimierung von Geschäftsprozessen in Arztpraxen, Krankenhäusern und Kliniken beschäftigten. Bislang war eine Umsetzung der Konzepte entweder nur auf eine Region oder auf eine Institution beschränkt.

So wurde beispielsweise Anfang 2005 mit Unterstützung von Microsoft in der Notaufnahme im Klinikum Ingolstadt die manuelle Patientendatenerfassung auf ein elektronisches Verfahren umgestellt. Die behandelnden Ärzte wurden mit TabletPC ausgestattet und nutzen XML-basierte Formulare zur Eingabe aller relevanten Informationen. Die bisherigen

Papierdokumente konnten auf diese Weise ersetzt werden, aber auch die zeitnahe Über- bzw. Eintragung und der Austausch zwischen Ärzten und anderen Mitarbeitern wurde dadurch möglich. Besonders interessant war aber auch die Verkopplung der Datendomänen, etwa vom Krankenwagen und der Notaufnahme, so dass während des Transports des Patienten von der Unfallstelle zum Krankenhaus, seine Daten bereits erfasst, evtl. eine Vordiagnose erstellt und Behandlungsvorschläge übermittelt werden konnten.

Ein anderes beispielhaftes Szenario ist die Einführung einer elektronischen Patientenakte mit digitalem Archiv im Jahre 2001 im Berliner Klinikum für Minimal Invasive Chirurgie (MIC). Auch hier wurden TabletPC eingesetzt, um eine direkte Erfassung von Patientendaten oder Befunden direkt am Krankenbett zu ermöglichen[Fehler! Verweisquelle konnte nicht gefunden werden.].

Neben den hier aufgezeigten Projekten wurden auch in kleinerem Umfang bereits vor der gesetzgeberischen Initiative zur elektronischen Gesundheitskarte Projekt ins Leben gerufen, die sich mit der Organisation und dem Austausch von Patientendaten im Netzwerk beschäftigten. So schlossen sich Ärzte im so genannten „Ärzenetz Remscheid“ regional zusammen, um das Ziel der Interoperabilität und den Austausch von Patientendaten zu realisieren.

Die genannten Projekte haben auf diese Weise bereits vor einigen Jahren illustriert, dass Bestrebungen zur Digitalisierung von Daten sowie der elektronischen Verarbeitung selbiger in medizinischen Einrichtungen existieren. Die Beispiele ähneln in ihrem Funktionsumfang der elektronischen Gesundheitskarte, wobei sie sich entweder durch eine spezialisierte Domäne der Daten und die sie verarbeitenden Mechanismen oder die individuellen (qualifizierenden) Anforderungen der sie realisierenden Institutionen voneinander unterscheiden.

Der erste Meilenstein zur Übergabe einer ersten Spezifikation bzw. Lösungsarchitektur des bundesweit konzertierten Projektes zur Einführung der elektronischen Gesundheitskarte wurde auf der CeBIT 2005 erreicht[Fehler! Verweisquelle konnte nicht gefunden werden.]. Hier erfolgte die Übergabe durch die GEMATIK, einem institutionellen Überbau des BIT4Health-Konsortiums zur Spezifikation der elektronischen Gesundheitskarte. Neben dem Fraunhofer-Institut für Arbeitswirtschaft und Organisation wirken die IBM Deutschland GmbH, SAP Deutschland AG & Co. KG, InterComponentWare AG und die ORGA Kartensysteme GmbH mit. Die verabschiedete, fast 360 Seiten umfassende Spezifikation legt grundlegende Richtlinien zur Umsetzung der Sicherheitsanforderungen und -architektur, dem Informationsmodell sowie die Einordnung in die mitunter existierenden „Anwendungslandschaften“ fest. Die vorerst sehr abstrakte Sicht auf die zu implementierenden Teile der eGK legt folglich keine technischen Details fest und lässt den jeweiligen Entwicklern Spielraum zur Umsetzung.

Im Vorfeld der „offiziellen“ Spezifikation zur eGK wurde im Jahre 2004 auf der Fachmesse „medica 2004“ von selbigem Konsortium ein Prototyp vorgestellt, welcher die Pflichtenforderungen bzw. den administrativen Teil des §291a SGB V zuzüglich der Notfalldaten realisiert[6]. Diesbezüglich werden das Konsortium als auch die zuständigen Regierungsstellen kritisiert, dass nach der Präsentation auf der „medica 2004“ keine weiteren Ausschreibungen vorgenommen wurden, sondern die Anschlussverträge am 11.01.2005 unterzeichnet wurden[7].

Das Unternehmen „secunet AG“, dessen Hauptanteilseigner das Unternehmen „Giesecke + Devrient“ ist, stellte - wie oben bemerkt - auf der „medica 2004“ das Lesegerät für die beiden Kartentypen inklusive eines Konnektors, welcher ähnlich einem Router die Geschäftsstellen der Heilberufler mit dem geschützten Netzwerk verbinden soll[6]. Dabei ist der Konnektor keine vollständige Neuentwicklung, sondern entstammt einer Entwicklung[9, 10] mit dem

Bundesamt für Sicherheit in der Informationstechnik (BSI) für das Bundesverteidigungsministerium, dem so genannten „Führungsinformationssystem der Streitkräfte“ oder für die gesicherte Kommunikation des Auswärtigen Amtes mit seinen Botschaften im Ausland[11]. Die gemeinsam mit dem BSI entwickelte „Sichere Inter-Netzwerk Architektur (SINA)“ „verfügt ... in Deutschland über die NATO-Zulassung für die Übermittlung von Informationen bis zur Klasse SECRET[10, S.2]“ und mittlerweile auch mit der Klasse STRENG GEHEIM[11].

Dieser kurze Abriss macht deutlich, dass die Einführung der elektronischen Gesundheitskarte in Deutschland nicht nur zentralistisch koordiniert und monopolartig in Form von Konsortien bzw. Kartellen betrieben wird, sondern sich auch an quasi-militärischen Befehlshierarchien orientiert bzw. Technologien aus diesem Sektor als vertrauenswürdig und „sicher“ angesehen werden.

Es bleibt anzumerken, dass die secunet AG zusammen mit dem BSI auch an der Planung und Entwicklung der in Deutschland ab November 2005 auszugebenden biometrischen Ausweise beteiligt ist[12].

Als eine der acht Pilotregionen für die Erprobung der elektronischen Gesundheitskarte ist das Bundesland Rheinland-Pfalz zu nennen[13], welches unter dem Namen „Vita-X-Net“ den Einsatz eines elektronischen Patientenpostfachs und Rezepts in einer zentralistischen Client-Server-Architektur erprobt. Hierbei übernimmt ein am Zentralen Rechenzentrum in Hannover (RRZN) situerter Zentralrechner die Funktionen zur Speicherung und Verteilung der Patientendaten. Eine andere Testregion mit gleichem Ansatz ist in Flensburg, Schleswig-Holstein, zu finden.

Das Hauptproblem bei der Umsetzung der elektronischen Gesundheitskarte ist die Integration der Daten und der darauf zugreifenden Mechanismen in die bestehenden Praxis-Software und Krankenhausinformationssysteme. Diese praxisübergreifende Datenanpassung sollte auch dann reibungslos funktionieren, wenn nicht alle beteiligten Ärzte mit derselben EDV arbeiten. Zur Unterstützung der Anforderungen muss eine Vielzahl von offenen Standards berücksichtigt werden. Die Grundlage für die einzelnen Austauschformate bildet dabei XML. Von zentraler Bedeutung ist dabei xDT. So dient ADT zum Austausch von Abrechnungsdaten und BDT für Behandlungsdaten. Weitere Formate sind DICOM (Digital Imaging and Communications in Medicine) und PACS (Picture Archiving and Communication System) zur Speicherung (Digitales Archiv), Verteilung (Netzwerk) und die Anzeige (Workstations mit Monitoren oder Projektionssystemen) von Bilddaten in medizinischen Einrichtungen (Röntgen, MRT, CT, etc.).

*{Sebastian: bitte über den Text schauen, nach semantischen Schwächen suchen UND die Abkürzungen bitte ausschreiben!}*

Neben den der „offiziellen“ Spezifikation der elektronischen Gesundheitskarte existieren zwei verschiedene Ansätze, nämlich das „Ärztetz Remscheid“ und die fachgetriebene Standardisierung der Arbeitsgruppen der „Health Level 7 (HL7)“ sowie der „Clinical Document Architecture (CDA)“.

Das „Ärztetz Remscheid“[14] setzt als dezentrale bzw. regionale Lösung ebenfalls auf die IT-gestützte Patientenverwaltung, wobei sie sich deutlich als Vorläufer und Konkurrenz zur elektronischen Gesundheitskarte versteht[15]. Dabei fokussiert das Projekt auf die praxisübergreifende Koordination ärztlicher Behandlungsprozesse und damit die immer wichtiger werdende integrierte Versorgung. Resultat dieses Projektes ist demzufolge die elektronische Patientenakte und das „eRezept“. Der sichere, elektronische Datenaustausch spielte hierbei ebenfalls eine wichtige Rolle. Die Sicherheit dazu liefert einerseits die „medisign GmbH“ mit Hilfe einer Karte, der so genannten „medisign card“, welche als

Träger eines digitalen Zertifikates fungiert. Das digitale Zertifikat auf der Karte entstammt einer „Public Key Infrastructure“ bzw. einem „TrustCenter“, welche von der „DGN Service GmbH“<sup>1</sup> betrieben wird. Die Datenkomponenten der Karten ermöglichen auf diese Weise die Verschlüsselung und digitale Signatur und damit im Endeffekt die Wahrung der Integrität und des Schutzes der Daten bei ihrer Übertragung über das Internet. Zusätzlich erfolgt eine Abgrenzung der Kommunikation zwischen den Arztpraxen mittels eines „Virtual Private Networks“, das ebenfalls von der „DGN Service GmbH“ betrieben wird. Die Technologie zur Anbindung der Arztpraxen an das Netzwerk wird mittels eines Konnektor gewährleistet und ähnelt damit dem oben beschriebenen Konnektor der secunet AG. Problematisch in diesem Zusammenhang waren die sich sehr stark unterscheidenden Schnittstellen zur Kommunikation zwischen verschiedenen Software-Systemen in den Arztpraxen, welche mittels der Implementierung des proprietären Kommunikationsprotokolls „VDAP<sup>2</sup> Communication Standard (VCS)“ gelöst wurde. Mit Hilfe dieses Protokolles können Daten aus elektronischen Arztbriefen oder Krankenhausüberweisungen direkt in die elektronische Karteikarte einer Praxis gespeichert werden[16].

Allerdings bleibt auch hier zu bemerken, dass das „Ärztetz Remscheid“ von quasi-zentralistischen Strukturen getragen wird, denn die „DGN Service GmbH“ ist ein Tochterunternehmen der „APO-Bank“ [16], hinter welcher sich niemand anders als der für seinen kartellartigen Marktaktionismus<sup>3</sup> bekannte und relativ reformaverse Apothekerverband verbirgt. Insofern ist die „Konkurrenz“ des „Ärztetz Remscheid“ zur bundesweiten Infrastruktur der elektronischen Gesundheitskarte auch als Strategie zur Wahrung tradierter Strukturen zu Gunsten des Apothekerverbandes zu sehen. Es verwundert deshalb auch nicht, wenn der Identitätsnachweis der Ärzte und Apotheker, die „medisign Card“, auch für „Online-Banking“, „Online-Abrechnung“ sowie elektronische Unterschriften unter Verträge eingesetzt werden kann[17].

Eine zweite bemerkenswerte Lösung wird vor allem aus fachspezifischer Sicht von der „Health Level 7 (HL7)“ verfolgt, wobei diese deutlich mit einer Einschränkung der Datendomäne versehen ist[20]. Die Datendomäne bezieht sich hier nicht auf den administrativen Teil des §291a SGB V, sondern überwiegend auf alle in Krankenhäusern anfallenden Daten, welche nicht von dem Gesetz erfasst sind, dabei vor allem auf die Struktur der Dokumentationen von Befunden und medizinischer Forschung. Im weiteren bedeutet HL7 auch eine „Arbeitsanleitung“ für die Erfassung, Übermittlung und Verwaltung der in einem Krankenhaus anfallenden medizinischen Daten und impliziert damit auch technologische Notwendigkeiten, die aber von HL7 nicht erfasst werden.

HL7 ist auf diese Weise als Beschreibung der Geschäftsprozesse in Krankenhäusern zu verstehen und damit keine Konkurrenz zur Architektur der elektronischen Gesundheitskarte, sondern die notwendige Ergänzung zu selbiger, weil diese Daten von der Intention des §291a SGB V als „Anstoß zur Kosteneinsparung“ nicht erfasst sind. Allerdings sei hier darauf hingewiesen, dass genau wegen dieser disjunkten Datendomänen Brüche an den Schnittstellen der Software-Systeme im Gesundheitswesen und folglich auch Aspekte des „Cross-Media“ greifen.

Ergänzt wird HL7 durch Spezifikationen verschiedener Arbeitsgruppen, welche das mitunter hohen Datenaufkommen, etwa Röntgenbilder oder mikrobiologische Forschungsdokumente,

---

<sup>1</sup> DGN ist ein Akronym für das „Deutsche Gesundheitsnetz“.

<sup>2</sup> VDAP ist ein Akronym für den „Verband Deutscher Arztpraxis-Software-Anbieter“, <http://www.vdap.de>

<sup>3</sup> Am Ende des 20. Jahrhunderts geriet der Apothekerverband in die Kritik, weil er als Interessenvertretung auftritt, tatsächlich aber ein hochprofitables Unternehmen ist, das seine Gewinne vorrangig aus Zwangsmitgliedschaft und Marktzutrittsbarrieren für „freie“ Apotheken generiert.

strukturieren und formalisieren. Hier ist dann besonders das Unterprojekt „Standardisation of Communication between Information Systems in Physician Offices and Hospitals using XML (SCIPHOX)“ zu benennen, welches in 3 Phasen „die inhaltlichen Erfordernisse einer Kommunikation zwischen ambulanten und stationären Versorgungseinrichtungen analysiert[22]“ und auf Basis des ANSI-Standards der „Clinical Document Architecture (CDA)“ spezifiziert und realisiert.

Dabei beschreibt die CDA nur die Datenstruktur von klinischen Dokumenten[21]:

#### Klinische Dokumente

Ein CDA-Dokument ist ein klinisches Dokument, das Beobachtungen und Maßnahmen enthält und folgende Eigenschaften aufweist:

- Persistenz
- geregelte Verwaltung
- Möglichkeit zur Authentifizierung
- Ganzheit der Authentifizierung
- Lesbarkeit für das menschliche Auge (kein Binärformat)

Ein CDA-Dokument ist ein definiertes und komplettes Informationsobjekt, das Texte, Bilder, Klänge und andere multimediale Objekte enthalten kann. CDA-Dokumente sind in der Extensible Markup Language XML kodiert.

Die Phase I des SCIPHOX-Projektes ist mittlerweile abgeschlossen[22] und fokussierte vor allem auf den

Entlassungsbrief mit Diagnosen, Therapien, Informationen zur Weiterbehandlung und Medikation etc. nach Beendigung eines Krankenhausaufenthaltes für den niedergelassenen Arzt oder als Bericht bei Weiter- /Mitbehandlung durch einen niedergelassenen Kollegen und die Überweisung von Arzt zu Arzt oder eine Krankenseinweisung an die entsprechende Krankenhausabteilung andererseits

Die Phase II und III des SCIPHOX-Projektes „haben vor allem eine Ausbreitung der Anwendungsfälle zum Ziel gehabt: das eRezept, Informationsübermittlung im Rahmen der Dokumentationsbögen zur Qualitätssicherung (z. B. Diabetes mellitus) und Notfalldaten sind definiert und umgesetzt.“

Maßgeblich verantwortlich für die Spezifikation der Phase I des SCIPHOX-Projektes „zum standardisierten elektronischen Kurzbericht (Entlassungsbrief, Überweisung und Einweisung)“ war die deutsche Arbeitsgruppe „HL7-Benutzergruppe in Deutschland e.V. Technisches Komitee ‚XML-Anwendungen im Gesundheitswesen‘“, welche Mitte 2002 eine Working Draft vorlegte[23].

Abschließend seien an dieser Stelle noch einmal die verschiedenen Ansätze für die Umsetzung einer elektronischen Verwaltung von Patientendaten aufgelistet, vor allem auch, weil das Kapitel 3.1 auf den vorangegangenen Beschreibungen aufbauen wird:

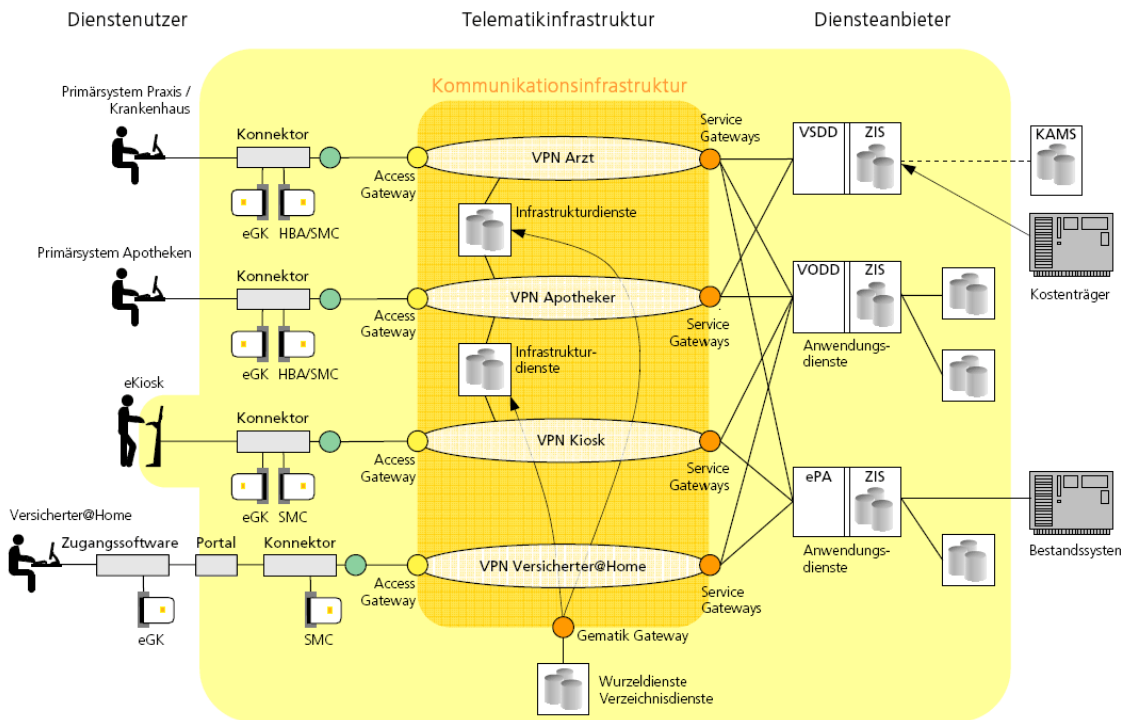
1. die „offizielle“, bundesweite Architektur der GEMATIK respektive des bit4Health-Konsortiums
2. die regionale, dezentrale Lösung des „Ärztenez Remscheid“, maßgeblich gestützt von der „DGN Service GmbH“ respektive der „APO-Bank“
3. die fachbezogene, institutionelle Lösung der „Clinical Document Architecture“ respektive der HL7-Working Group bzw. Arbeitsgemeinschaft SCIPHOX

## 2.2 Das Fraunhofer „Referenzmodell“

Das hier besprochene „Referenzmodell“ der deutschen Fraunhofer-Gesellschaft, ersehen aus Figure 1, kann in dem Sinne nur als „Referenz“ verstanden werden, als dass es einen Kompromiss zwischen den an der bundesweiten Einführung der elektronischen Gesundheitskarte Beteiligten, aber in keinem Fall eine idealisierte oder gar typische Architektur eines Dokumentenverteilsystems im Gesundheitswesen darstellt.

Das Modell teilt sich in die Bereiche Dienstenutzer, Telematikinfrastruktur und Diensteanbieter auf. Die Praxen bzw. das Krankenhaus, die Apotheken und der Zugang für die Versicherten werden als Klienten bzw. Dienstenutzer aggregiert. Der Zugriff erfolgt dabei über Konnektoren, die in Abhängigkeit von eGK, HBA und SMC (Secure Module Card) den Zugriff auf die Infrastruktur bereitstellen. Angebunden an den Konnektor ist eine VPN-Box, symbolisiert durch einen grünen Kreis, die den sicheren Kommunikationskanal für die „letzte Meile“ anbietet. Das gesicherte Kommunikationsnetz ist dann je nach Benutzergruppe bzw. Autorisation des anfragenden Nutzers disjunkt gestaltetem also etwa einem gesonderten VPN für Ärzte oder Apotheker. Die Aufgabe der Autorisation übernehmen die so genannten „Access Gateways“, welche nur registrierten und autorisierte Nutzern oder gar Zugangsknoten den Zugriff auf die zentral gelagerten Daten ermöglichen. Eine weitere Prüfung von Berechtigungen erfolgt an dem Zugangsknoten zu den Diensteanbietern, den „Service Gateways“. Entsprechende Tabellen sollen hier die Zugangskontrolle regeln, also aus für welche Kategorie eines VPN welche Dienste verfügbar sind.

Eine spezielle Rolle kommt hierbei dem „GEMATIK Gateway“ zu., welcher Verzeichnis- und Wurzeldienste zur Verwaltung und Konfiguration des Netzes vorhält und somit als zentrale Autorisierungsinstanz fungiert. Die genutzten Anwendungsdienste „Verordnungsdatendienst (VODD)“ oder „Patientenakten (ePA)“ sind hingegen verteilt realisiert. Alle Anwendungsdienste nutzen eine einheitliche und anwendungsübergreifende „Zugangs- und Integrationsschicht (ZIS)“. Die ZIS soll eine einheitliche Rechteverwaltung für den Zugriff auf die Daten und einen einheitlichen Zugang auf verteilte Datenspeicher, die so genannte Ortstransparenz gewähren. [24]



**Figure 1: Visualisierung des Fraunhofer „Referenzmodells“**

Offensichtlich verfolgt damit die Projektgruppe bit4Health ein zentralisiertes Datenmodell, das maßgeblich mit den Interessen der Krankenkassen konform geht[28]:

Bei der vor allem von den Krankenkassen favorisierten Server-Lösung fungiert die elektronische Gesundheitskarte nur als Schlüssel zu den Daten, die auf einem zentralen Server gespeichert werden.

Ergänzend zu diesem „Referenzmodell“ legte die Dachorganisation GEMATIK eine Reihe weiterer Spezifikationen vor, etwa das an HL7 orientierte „Informationsmodell“[25, S. 22], welches die Daten zur Identifikation der an der Architektur beteiligten Personenkreise, der Sicherheitsdaten, der medizinischen Daten oder Vertragsdaten beschreibt, oder die Sicherheitsanforderungen und Sicherheitsarchitektur[26].

Die Sicherheitsarchitektur der Projektgruppe „orientiert ... sich an dem internationalen ISO Standard 7498-2: OSI Basic Reference Model – Part 2“ [26, S.10].

Allerdings muss an dieser Stelle bemerkt werden, dass sowohl der von der Projektgruppe referenzierte Standard sowie die vorgelegte Sicherheitsarchitektur in keiner Weise als der Sicherheit zweckdienlich betrachtet werden kann.

Denn

1. der referenzierte Standard baut auf dem ISO Standard 7498-1 auf[27], welcher versucht, die mangelnde Spezifikation von Sicherheitsanforderung aus dem OSI-Referenzmodell für Netzwerkkommunikation nachträglich durch Addition einiger Sicherheitsmechanismen zu beheben; dabei ist in der Informatik bekannt, dass das OSI-Referenzmodell für Netzwerk-kommunikation auf der strikten Trennung von Funktionalität in Form von Schichten, jeweils mit einem Zweck der Datenverarbeitung versehen, basiert und damit ein Durchgriff oder Ruf von Funktionalität durch die Schichten nicht zulässig ist; allerdings sieht der ergänzende ISO-Standard 7498-1 je Schicht nur partielle Sicherungsmechanismen vor, die zudem wegen des Paradigmas des OSI-Referenzmodell für Netzwerkkommunikation nur auf einer Schicht und nicht über alle Schichten wirken,

2. die von der Projektgruppe vorgelegte Sicherheitsarchitektur ist zwar theoretisch ansatzweise konsistent formuliert, allerdings werden schon die „Sicherheitsobjekte“ „Benutzer, Passwort, Schlüssel“ oder „Privilegien“ unzulässigerweise miteinander, also effektiv die Beschreibung von Akteuren mit den Daten der Zugriffskontrolle vermischt werden und zudem die sorgfältig vorgenommene Trennung von Sicherheitsdiensten und Sicherheitsmechanismen zwischen- und untereinander in der Grundsatzentscheidung zur Architektur verwischt wird, so dass die Trennung software-technisch, aber nicht sicherheitstechnisch motiviert und in einem gewissen Sinn auch der Unzulänglichkeit des eben genannten OSI-Sicherheitsmodelles geschuldet ist[26, S. 17]: „es ist zu beachten, dass ein Sicherheitsdienst durch unterschiedliche Mechanismen realisiert werden kann und ein Sicherheitsmechanismus auch von unterschiedlichen Diensten verwendet wird.“

Ferner verstrickt sich die Projektgruppe bit4Health in weitere Inkonsistenzen, die deutlich darauf hinweisen, dass die Einführung der elektronischen Gesundheitskarte entweder wie die Einführung der Maut in Deutschland ein Debakel wird oder die komplexeren Probleme sehr kostenintensiv erst zur Laufzeit der von ihr vorgeschlagenen Architektur zu Tage treten werden[26, S. 20]:

Langzeitarchivierung ... Für die prioritären Anwendungen ist die Archivierung der Daten zurzeit nicht im Fokus. Eine Langzeitarchivierung findet ausschließlich in den IT-Systemen der Arztpraxen und stationären Einrichtungen sowie u.U. in den IT-Systemen der Kostenträger statt. ... Langzeitarchivierung z.Zt. noch nicht behandelt.

Dennoch können von Archivierungssystemen im Gesundheitswesen benötigte Dienste die von der Telematikinfrastruktur allgemein bereitgestellt werden, über eine einheitliche Schnittstelle genutzt werden ...

### **3. Von der Theorie zur Praxis**

Im Vorfeld der Planung einer eigenständigen Architektur, welche die Geschäftsprozesse in den Institutionen der Heilberufe auf Basis der elektronischen Gesundheitskarte unterstützen sollten, galt es die unterschiedlichen Implementierungsansätze zu kategorisieren.

Dabei fielen drei mögliche Geschäftsprozesse bzw. Szenarien für die Verarbeitung von Patientendaten auf:

1. der Patient als Datenträger im Sinne einer Datenhoheit des Patienten, welche bisher in keiner der im Kapitel 2 beschriebenen Implementierungen betrachtet wurde
2. die Krankenkasse als Datenträger, welche mittels des „Referenzmodells“ der Fraunhofer-Gesellschaft und damit über die Projektgruppe bit4Health auch bundesweit im Jahre 2006 realisiert wird
3. das Ärzte-(Daten-)Cluster im Sinne der Datenhoheit der Vertreter der Heilberufe, welche etwa mittels des Standards HL7 und CDA oder das „Ärztetz Remscheid“ realisiert wird

Diese Kategorisierung dient vor allem der Bestimmung der eigenständigen Architektur für eine elektronische Gesundheitskarte, welche hier besonders die Interessen der Beteiligten, vor allem der Vertreter der Heilberufe und des Versicherten, berücksichtigen soll.

Dabei soll ebenso das Interesse der Krankenkassen an einer nachvollziehbaren und authentischen Datenverarbeitung berücksichtigt werden, wobei die Krankenkassen diesbezüglich auf ihre gesetzlichen Aufgaben beschränkt werden sollen.

#### **3.1 Szenarien für den Einsatz der elektronischen Gesundheitskarte**

Die folgenden Unterkapitel sollen die in Kapitel 2 vorgestellten Realisierungen nach ihren systemtechnischen Motivationen kategorisieren und bewerten, um später für die Motivation und Annahmen der eigenständigen Implementierung des Projektes verständlicher zu machen.

### 3.1.1 Gegenwart

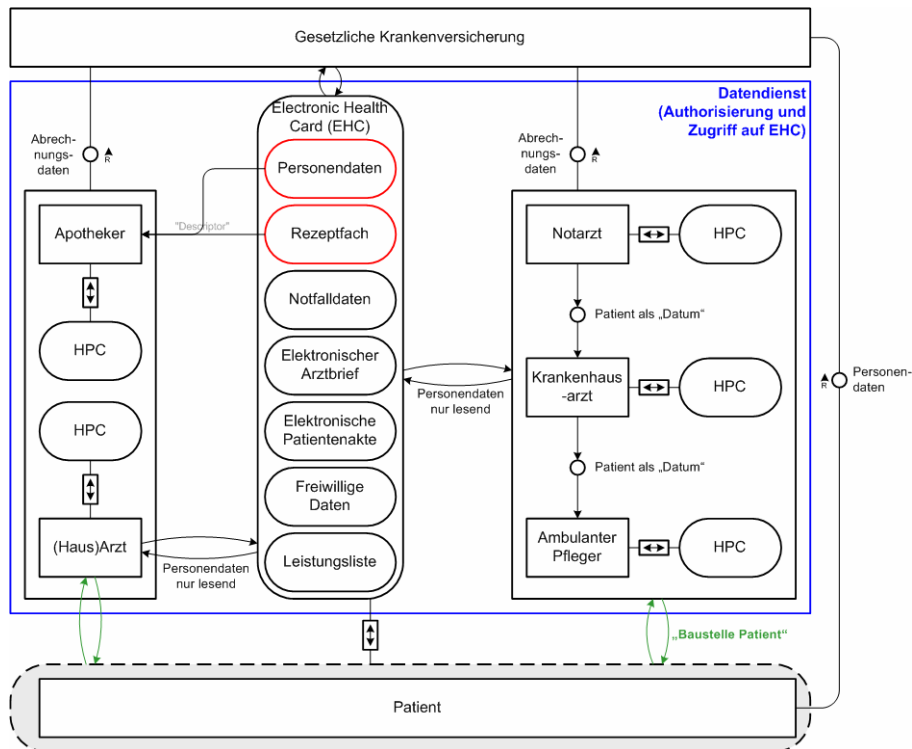
Zum aktuellen Zeitpunkt werden die Daten bei jedem Arzt, welcher eine entsprechende Behandlung durchgeführt hat, vor Ort gespeichert. Alle anderen am Versorgungskreis beteiligten Institutionen, etwa Krankenhäuser oder Apotheke, fordern vom entsprechenden (Haus-)Arzt die Daten in Papierform an oder erhalten sie über den Patienten. Die Identifikation des Patienten erfolgt im Moment noch über den Versicherungsausweis mit aufgedruckten den Vertragsdaten des Versicherten in Bezug zu seiner Krankenkasse sowie einem kleinen Satz an Daten, welche sich in einem kleinen Datenspeicher auf der Karte befinden.

Die Krankenversicherung hat in dieser Konstellation lediglich die Pflicht und das Recht, die Abrechnungsdaten in kodierter Form zu verwalten, aber keinen Zugriff auf die gesundheitlichen Stammdaten des versicherten, welche mitunter redundant bei verschiedenen Vertretern der Heilberufe liegen.

Ziel der aktuellen Bestrebungen um die eGK soll es sein, die gesamte Versorgung des Patienten mittels technischer Mechanismen zu verbessern, was die „allgegenwärtige“ Verfügbarkeit von Daten für zugriffsberechtigte Personen einschließt. Eine Umsetzung dieses Ansatzes scheitert vorrangig daran, dass eine zu starke Gebundenheit an die physischen Medien vorliegt, welche sich besonders auf die Latenz, die Lesbarkeit und die Beschaffungskosten der Daten von der Quelle zum Ziel auswirkt. Wichtige Daten sind deshalb im entscheidenden Moment, wie einem Notfall, nicht verfügbar. Eine unstrukturierte und verteilte Sammlung von Patientendaten, verteilt über alle behandelnden Ärzte, macht folglich bei zunehmendem Datenaufkommen eine Suche nahezu unmöglich.

Andererseits ist trotz der überwiegenden Nachteile die Wahrung der ärztlichen Schweigepflicht, sofern die medizinischen Daten lokal beim Arzt liegen, hier deutlich hervorzuheben.





**Figure 3: "Der Patient als Datenträger" (Syntax: FMC)**

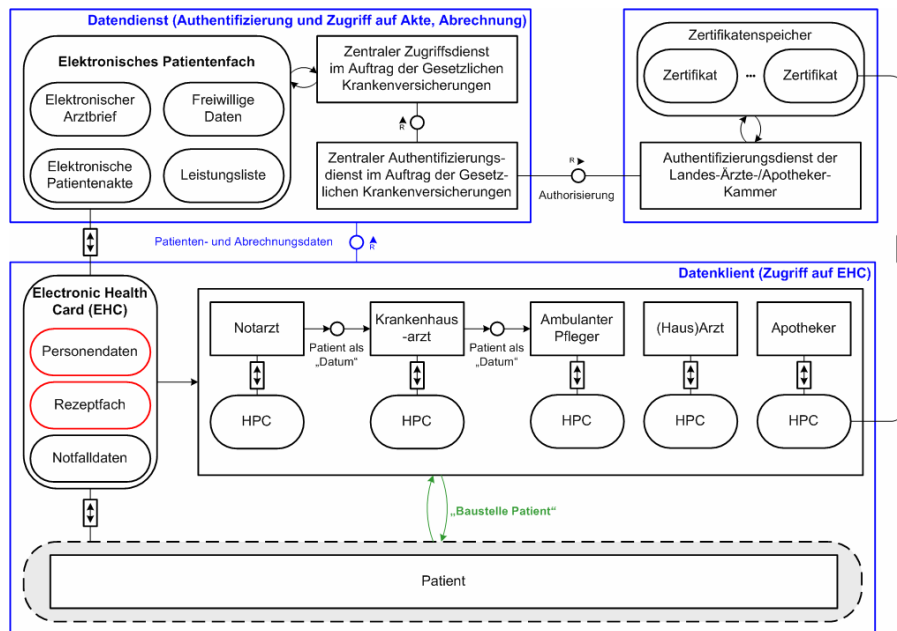
### 3.1.3 Datenanbieter Krankenkasse

Diese Lösung ist - wie bemerkt - der Gegenstand der Projektgruppe bit4Health und der Favorit der Gesetzlichen Krankenkassen, welche sie zentrale Instanz der elektronischen Verwaltung der Patientendaten etabliert. Auf der „electronic health card (EHC)“ residieren nur die Personen- und Notfalldaten, das Rezeptfach und als Datensatz formulierte „trigger“ einer weiterführenden Datenverarbeitung. Als Pedant zur EHC existiert die „health professional card (HPC)“, welche Vertretern der Heilberufe Zugriff auf die relevanten Patientendaten ermöglichen. Die Sicherung von Patienten- und Abrechnungsdaten erfolgt entgegen den vorhergehenden Ansätzen zentral in einem elektronischen Postfach auf einem Datenspeicher unter Ägide der Krankenkassen. Dieses Postfach soll den elektronischen Arztbrief, die Patientenakte und die Leistungsliste umfassen. Eine Autorisierung soll in diesem Fall ebenfalls durch einen zentralen Dienst, einem Zertifikatenspeicher respektive „TrustCenter“ realisiert werden.

Der Vorteil dieses Ansatzes gegenüber den vorhergehenden Szenarien ist die elektronische, allgegenwärtige Verfügbarkeit von Daten in der vollen Verantwortung der Gesetzlichen Krankenkassen, vor allem was haftungsrechtliche Fragen bezüglich der Sicherheitsmechanismen betrifft. Ein leichtere Verwaltung und bessere Kontrolle über die Versichertendaten ist ebenfalls eine nebenläufige Begleiterscheinung.

Allerdings führt dieses Szenario nicht unerhebliche Nachteile mit sich, die sich mitunter aus der eingesetzten Technik ergeben. So sind vor allem in Bezug auf die zu erwartende Datenlast am zentralen Datenspeicher verstärkt Maßnahmen zur Gewährleistung von Verfügbarkeit und Systemperformanz zu ergreifen. Ein weiterer Mangel dieses Szenarios betrifft den Datenschutz, vor allem was die Vertraulichkeit der Daten betrifft, weil ein Angriff gegen einen zentralen Datenspeicher leichter „zu fahren ist“ als ein Angriff gegen zahlreiche disjunkte und verteilte Datenspeicher, wie es etwa das Szenario des „Patienten als Datenträger“ vorgibt. Zudem ist es äußerst kritisch zu betrachten, dass mittels des hier

besprochenen und offensichtlich in Deutschland durchzusetzenden Szenarios die ärztliche Schweigepflicht aufgeweicht wird bzw. die ärztliche Schweigepflicht erhalten bleibt, aber an langer Hand dem Heilberufler jene Dokumente, über welche er Stillschweigen zu bewahren hat, entzogen werden.



**Figure 4: "Datenanbieter Krankenkasse" (Syntax: FMC)**

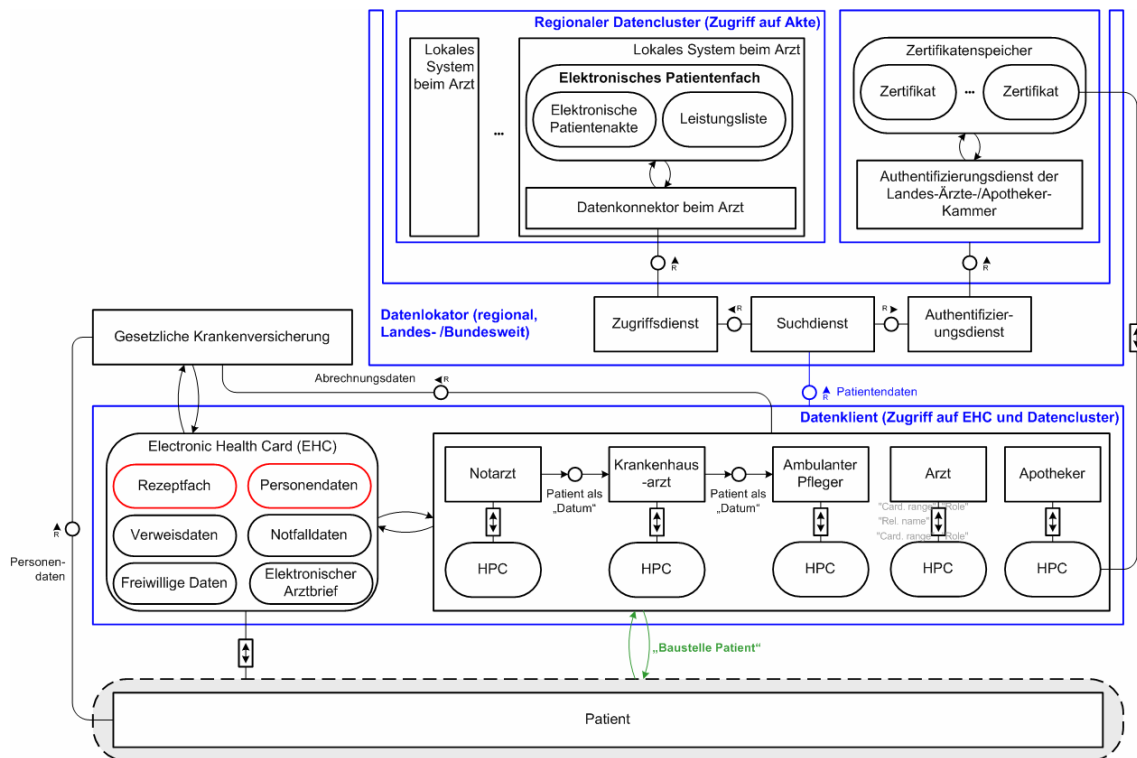
### 3.1.4 Ärzte-(Daten-)Cluster

Im letzten Szenario wird der verteilte Ansatz in einer speziellen Form aufgegriffen und ist fortwährend der Ansatz für die mit diesem Dokument beigegebene eigenständige Implementierung.

Es greift die Authentifikation des vorhergehenden Szenarios (3.1.3) in Form der nutzerseitigen Authentifikation mittels HPC und EHC zum Zugriff auf und der Veränderung von Patientendaten auf, kombiniert diese aber mit dem Szenario des „Patient als Datenträger“ (3.1.2). Versatzstücke des „Gegenwartsszenario“ (3.1.1) sind in diesem Szenario aber auch vorzufinden, indem die Daten auf kaskadierenden Speichern bei den Vertretern der Heilberufe(!) zur Verfügung stehen, so dass die Patientendaten auch nach regionalen oder fachlichen Aspekten verteilt gespeichert sein können. Der Zugriff auf die Daten wird durch einen Suchdienst sichergestellt, welcher die Authentizität des Anfragenden validiert und entweder die Adressen von Datensätzen oder von weiteren Suchdiensten vorhält. Zusätzlich zur veränderten Struktur der Datenspeicher werden die Datensätze auf der EHC gegenüber den vorhergehenden Szenarien anders organisiert. So finden sich auf der EHC neben den Patientendaten und dem Rezeptfach auch der elektronische Arztbrief, die Notfalldaten und die freiwilligen Daten an. Bei den Vertretern der Heilberufe befinden sich dann folglich nur noch die Elektronische Patientenakte und die Leistungsliste, womit die ärztliche Schweigepflicht wiederhergestellt ist. Wichtige Daten sind zudem im Notfall auch im schlechtesten Fall, etwa bei einem Ausfall von drahtlosen Verbindungen auf dem Lande zu einem zentralen Datenspeicher, wie sie das Szenario „Datenanbieter Krankenkasse“ vorgibt, beim Patienten verfügbar, wohingegen nicht permanent verfügbare Daten erst auf Abruf verfügbar sein müssen. Weitere Vorteile dieses Szenarios sind die Lastbalancierung der Daten und die zwangsweise komplexeren Angriffsszenarien, welche sich aus der Verteilung ergibt.

Allerdings sei angemerkt, dass die Verantwortung bzw. Haftung für Sicherheitsmechanismen dann bei den Vertretern der Heilberufe liegt und so nicht zu vertreten ist, wenn die

Heilberufler sich auf ihr Fach konzentrieren sollen. Folglich müssen dann die Entwickler von Software-Systemen für Heilberufe hier nicht nur in der Pflicht sein, wirksame Sicherungsmechanismen zu produzieren, sondern auch in der Haftung stehen.



**Figure 5: "Ärzte-(Daten-)Cluster" (Syntax: FMC)**

Als Konsequenz dieser Diskussion und im Vorfeld der Spezifikation einer eigenständigen Implementierung einer Architektur für die elektronische Gesundheitskarte zeichnete sich auf diese Weise ein klarer „Frontenverlauf“ dergestalt ab, dass die Krankenkassen eine bundesweite, zentrale Lösung präferieren, wohingegen die Ärzte sich eher für regionale, dezentrale und überschaubare Lösungen aussprechen. Die Krankenhäuser oder auch Kliniken interessieren sich hingegen sehr für eine zentrale hausinterne, auf ihre organisatorische Struktur zugeschnittene Lösung mit Kopplung nach außen.

Und die Informatiker ziehen auch aufgrund der datenschutzrechtlichen Einwände offensichtlich das „Daten-Cluster“ vor.

### 3.2 Das eigenständige Konzept eines Gesundheitstelematik-Systems

Im Folgenden soll nun kurz unsere prototypische Lösung zur Umsetzung und Lösung der elektronischen Gesundheitskarte aufgezeigt werden. Es werden nur grundlegende Merkmale, die zum Verständnis der Funktionsweise beitragen, vermittelt. Genauere Ausführungen und Betrachtungen zur spezifischen Umsetzung können in dem dieser Ausarbeitung beigegebenen Lastenheft nachgelesen werden.

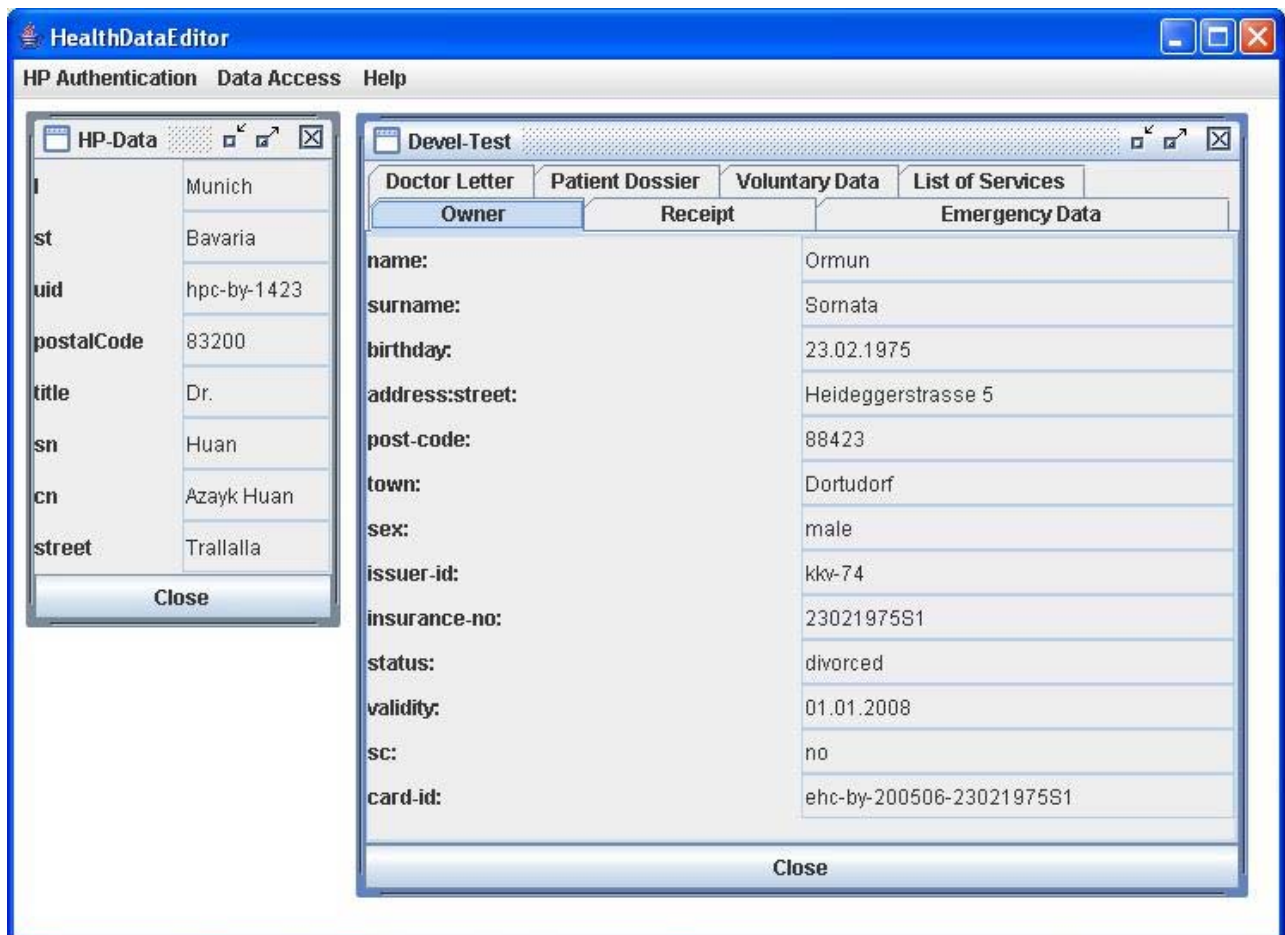
Es sei hier deutlich hervorgehoben, dass dieses Projekt beim Entwurf einer derartigen Architektur an den Interessen der an einer elektronischen Gesundheitskarte Beteiligten orientierte und im Gegensatz zu den offensichtlich rein software-technischen Ansätzen der Projektgruppe bit4Health nicht an den verfügbaren Technologien orientierte.

Aus diesem Grund floss sowohl des Szenarios des „Patienten als Datenträger“ in den Entwurf ein, aber auch die Idee, dass für andere Heilberufler ein bestimmter, vom Datenvolumen begrenzter Satz an Daten zum Abruf bereitsteht. Eine weitere Dimension eröffnet sich im Streitfall, etwa bei einem so genannten „Ärztepfusch“, für welche die Daten vertraulich und

revisionssicher bei einer Bundes- oder Landesbehörde eingelagert sind und erst nach einer Autorisierung durch den Patienten und dem Heilberufler einem Gericht zur Verfügung stehen. Als Seiteneffekt bleibt die Verantwortung und Haftung der Gesetzlichen Krankenversicherung auf ihre Aufgaben beschränkt, da sie einerseits ihre Abrechnungen auf diese revisionssicheren Daten beziehen können und andererseits keine zentralen Datenspeicher vorhalten müssen, auch wenn sie es gerne wollten.

Die Lösung ist eine Umsetzung des beschriebenen Szenarios eines „Daten-Clusters“. Sie gliedert sich grob in 5 Teile. Der Zugang zum gesamten System erfolgt über eine grafische Schnittstelle, wobei der Zugriff auf die Daten im System mittels der Autorisierung über die beiden Identifikatoren HPC und EHC im das Kartenlesegerät des Arztes erfolgt.

Der Koppler zwischen dem Kartenlesegerät, dem Arzt, gegebenenfalls der Krankenschwester, und dem Datenanbieter (Serverseite) realisiert die Benutzungsschnittstelle (Figure 6). Sie übernimmt die Präsentation, die Ver-/Entschlüsselung, die Signierung und den sicheren Netzwerkzugriff auf die Dienste. Nach Eingabe oder Änderung neuer Daten sollen sie mittels kryptographischer Werkzeuge an die entsprechenden Dienste geschickt werden. Eintrittspunkt für die Serverseitige Verarbeitung ist der Datenautorisierungsdiensteanbieter.



**Figure 6: Die grafische Oberfläche der eigenständigen Implementierung**

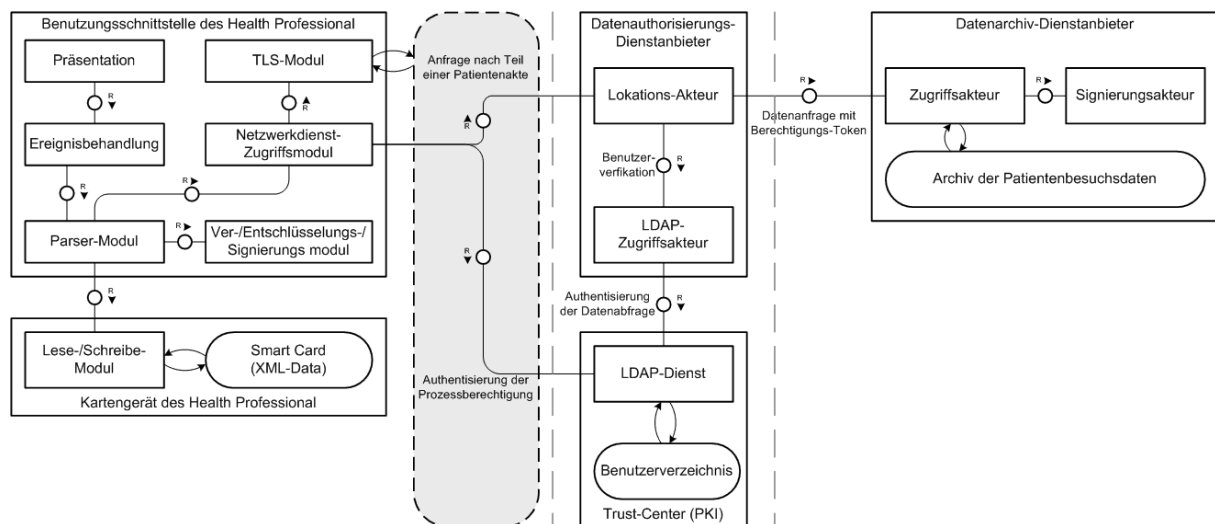
Der Datenautorisierungsdiensteanbieter übernimmt die Funktionalität zum Auffinden von angeforderten oder der Auswahl des Speicherortes für neue Dokumentationen von Besuchen des Versicherten bei Heilberuflern. Zusätzlich wird hier die Kontrolle des Zugriffes von Heilberuflern mit Hilfe eines Zertifikatenspeichers vorgenommen. Es wird von einer

regionalen Verteilung, etwa nach Bundesländern, der Datenarchive sowie der Zertifikatenspeicher ausgegangen.

Nach der Lokalisierung der entsprechenden Informationen erfolgt die Weiterleitung an den Datenarchiv-Diensteanbieter, welcher die endgültige und revisionssichere Speicherung der Daten vornimmt.

Zusätzlich zur Verteilung der Daten auf verschiedene Instanzen eines Datenarchives und ihrer Zugriffskontrolle muss auch die Integrität, also der Schutz vor unberechtigter oder zufälliger Manipulation, und die Vertraulichkeit, der Schutz vor unberechtigten Einblicken, gewahrt bleiben. Aus diesem Grund wurden an entsprechenden Stellen Mechanismen zur Verschlüsselung und digitalen Signatur eingeführt.

Grundlage des Schutz gegen die Einsicht in die Dokumentationen durch Dritte ist die asymmetrische Verschlüsselung. Der Patient bekommt damit die Möglichkeit „Herr“ über seine Daten zu sein, indem mittels des privaten bzw. öffentlichen Schlüssel die Arztbriefe oder Rezepte ent- bzw. verschlüsselt werden. Da das asymmetrische Schlüsselpaar nur auf der Smartcard des entsprechenden Besitzers resident ist, sind die mit diesen Schlüsseln chiffrierten Daten ebenso nur mit diesen Smartcards zu einem späteren Zeitpunkt wieder nutzbar. Entsprechend der Betrachtung der verschlüsselten Informationen als „kryptographischen Blob“ muss im Vorfeld festgelegt werden, was für die Abrechnung durch die Krankenversicherung zur späteren Identifizierung oder weiteren Verarbeitung notwendig ist. Zusätzlich zur Verschlüsselung ist eine digitale Signatur notwendig, damit eine eindeutige Verifikation und Revisionssicherung der Dokumentationen möglich wird. Dementsprechend signieren der Arzt, der Patient und das Datenarchiv die Dokumentationen vor der Einlagerung bzw. Speicherung. Der Archiv-Diensteanbieter spielt in diesem Zusammenhang eine zentrale Rolle. Er bestätigt als unabhängige Instanz die Richtigkeit der Daten beispielsweise gegenüber der Krankenkasse.



**Figure 7: Eigenständige Referenzarchitektur dieses Projektes (Syntax: FMC)**

Im Weiteren wird hier noch einmal ausdrücklich auf das dieser Ausarbeitung beigegebene Lastenheft verwiesen, welche ausführlich auf die Anforderungen an die Daten, Funktionen sowie Hard- und Software eingeht.

Die Umsetzung erfolgt für alle Bestandteile mit der Programmiersprache Java. Nach der Richtlinie von SUNs „Java Coding Style Guide“ erfolgte eine Trennung der Klassen entsprechend ihrer Funktionalität in Packages (Figure 8). Basis-Paket für die Graphische



### 3.3 Probleme bei der Implementierung

Bei der Implementierung der eben vorgestellten Architektur ergaben sich vereinzelt Probleme, welche vor allem möglichen Inkonsistenzen der verwandten Software-Werkzeuge selbst oder ihrer Dokumentation geschuldet sind.

Hier sollen aber nur jene Probleme beschrieben werden, welche die für die Architektur deutlichsten Konsequenzen hervorbrachten.

Bei der Vorbereitung der Komponenten bereitete der als Zertifikatenspeicher eingesetzte openldap-Server Probleme bei der Speicherung der Zertifikate.

Die von dem LDAP-Server verzeichnisartig verwalteten Benutzerinformationen über die Vertreter der Heilberufe basieren auf so genannten Schemata, welche im Standard X.500 definiert sind. Diese Schemata sind in Konfigurationsdateien mit sinngemäß gleicher Namensendung (.schema) organisiert.

Nun wurden alle benötigten Schemata eingebunden und konnten dann bei der Beschreibung der Benutzer verwendet werden, aber absurderweise konnten keine Zertifikate im Verzeichnis eingebunden werden. So enthält die relevante Datei „inetorgperson.schema“ das Attribut „uid“ genauso wie das Attribut „userCertificate“. Doch obwohl das Attribut uid problemlos im Verzeichnis, vor allem für die Authentifizierung, verwendet werden konnte, war die Benutzung des Attributes userCertificate nicht möglich bzw. die Benutzung wurde durch den openldap-Server verweigert. Die Dokumentationen schlugen vier Möglichkeiten vor, den Import aus einer separaten Datei oder als Zeichenkette bzw. Wert des Attributes, beide jeweils entweder als Bytestrom oder als ASCII-Dateibinstrom (Base64). Ein Tupel aus Attribut und Wert kann folglich so gestaltet sein

```
userCertificate;binary: MII...(weitere base64-kodierte Daten)
```

oder

```
userCertificate;binary:< file://certfile
```

Allerdings schlugen alle Versuche zum Import der Zertifikate fehl.

Dies ist insofern zu bedauern, da innerhalb der hier besprochenen Architektur

1. die Authentifizierung der Heilberufler gegenwärtig über ihre Benutzerkennung erfolgt und ein Vergleich des auf der HPC residenten Schlüssels mit dem im Zertifikat des Heilberufler enthaltenen Schlüssel, welche beide gleich sein müssen, den Authentifizierungs-Mechanismus „härten“ würden
2. ein Heilberufler auch Dokumentationen von anderen Heilberuflern einsehen könnte, wenn diese nur mit dem privaten Schlüssel des Heilberuflers verschlüsselt wurden und demzufolge mit dem öffentlichen Schlüssel des selbigen nebst den Schlüsseln des Patienten entschlüsselt werden könnten

Die Struktur der Dokumentationen wie auch der auf der EHC residenten Daten wurde, wie aus dem Lastenheft ersichtlich, in einer DokumentenTypDeklaration (DTD) formuliert, so dass dann tatsächliche Ausprägungen dieser Struktur dann als Dateien der eXtensible Markup Language (XML) vorliegen.

Die Wahl fiel wegen der oben beschriebenen notwendigen Revisionsicherung und Verschlüsselung auf den XML-Parser des Apache-Projektes, genannt Xerces.

Allerdings stellte sich die Implementierung des Parsers als nicht vollständig nachvollziehbar heraus, weil Zeilentrenner, also ein „newline“ nach einem Tag als eigenständiger Knoten ausgegeben wurde. Dies erhöhte die Komplexität und damit Laufzeit der Mechanismen, welche die Baumstruktur der Knoten einlas, und führte folglich auch zu Komplikationen, wenn nur Teilbäume der gesamten Baumstruktur ausgegeben werden sollten, also wegen der

Sonderstellung der Zeilentrenner anstelle des gewünschten Knotens ein unbenannter #name-Knoten zurückgegeben wurde.

Obwohl das Software-Paket „xml-security“ vom gleichen Entwicklerkreis stammt wie der Xerces-Parser, waren eine Mängel in der Integration der jeweiligen Werkzeuge offensichtlich.

So war die Signierung von Unterbäumen eines gesamten XML-Dokumentes problematisch, weshalb als „Workaround“ die zu signierenden Unterbäume als eigenständige XML-Dokumente erzeugt und signiert wurden und dann in das gesamte Dokument eingebunden wurden.

Das Projekt ging am Anfang noch von RFID-Technologien und Smartcards für das verschlüsselte Auslesen und Beschreiben der elektronischen Gesundheitskarte aus, was aber mangels verfügbarer Technologien und des gegenwärtigen Entwicklungsstadiums der elektronischen Gesundheitskarte verworfen wurde.

Folglich wurden die Gesundheitskarten respektive der Aspekt der Smartcards simuliert, indem auf USB-Speichergeräten gekapselte Datenspeicher für die Zertifikate und Schlüssel, der so genannte „keystore“ von SUN Java mitgeführt wurde. Allerdings verfügt das SUN-eigene Werkzeug `keytool`, welches für einen keystore Zertifikate und Schlüssel erzeugen kann, gegenwärtig nur über die Möglichkeit Zertifikate der Version 1 (X509.v1) zu erzeugen.

Aktuell wird aber der Einsatz von Zertifikaten der Version 3 (X509.v3), welche gegenwärtig nur durch das Werkzeug `openssl` der Open-Source-Gemeinde erzeugt werden können. Auf diese Weise ergaben sich Probleme der Interoperabilität zwischen `openssl` und dem Java-Werkzeug `keytool` beim Import der mittels `openssl` generierten Zertifikate in den keystore von SUN.

Wichtig ist noch zu bemerken, dass nur die Daten des Krankenversicherten bzw. Patienten in Form von XML-Dateien auf den USB-Speichergeräten abgelegt waren, nicht aber jene identifizierenden Daten des Heilberufers. Letztere waren in der Datenstruktur des Zertifikates erfasst, was letztlich auch mit dem Einsatz von Zertifikaten der Version 3 (X509.v3) zu verdanken ist.

Die Realisierung der Benutzerschnittstelle war eher zeitaufwändig, weil von Hand und nicht mittels eines UI-Builders kodiert, als kritisch. Es bleibt aber zu bemerken, dass JAVA Swing als Bibliothek für die Gadgets, also die Elemente der Benutzungsschnittstelle, in Bezug auf den Ressourcenverbrauch sowie das Laufzeitverhalten als nicht optimal anzusehen ist, weshalb bei zukünftigen Entwicklungen eine systemnähere Programmiersprache etwa C zu empfehlen wäre, obwohl man sich dann Performanzgewinne mit einer Dependenz vom Betriebssystem respektive dem vom Fenstersystem mitgelieferten Ressourcen, etwa TCL/TK oder GTK unter Linux oder die Win32-API von Windows, erkauft.

Die Kommunikation der Elemente der Benutzungsschnittstelle war unter JAVA Swing nicht einfach zu lösen, etwa, wenn ein Fenster an ein anderes Fenster Daten weiterleiten wollte oder ein Fenster ein weiteres Fenster erzeugen wollte, aber jedes Fenster vom Hauptfenster, dem „heavy-wight thread“ verwaltet werden musste. Nicht jede Kommunikation der Fenster untereinander ist mittels threads oder Ereignisbehandelnden Akteuren (event handler) lösbar, vor allem, wenn die Struktur der ausgetauschten Daten komplexer ist.

Letztlich ergaben sich beim Integrationstest der Komponenten Probleme der Interoperabilität zwischen den Betriebssystemen, trotzdem JAVA Plattforminteroperabilität verspricht.

So waren etwa Anfragen von einem MAC OS X-System gegen einen lokalen oder gegen einen auf einem Windows-Systeme residierenden LDAP-Server erfolgreich, dagegen nicht von einem Windows-System auf ein Mac OS X-Systemen. Die Vermutung, dass die Auflösung des Namens in eine IP-Adresse über die auf Windows-Systemen präsenten Datei

hosts.conf nicht möglich war, wurde falsifiziert, da Windows-Systeme untereinander eben solche Anfragen erfolgreich durchführen konnten.

Da die Verschlüsselung der Kommunikation zwischen der Benutzungsschnittstelle und dem LDAP-Server auf Basis von Zertifikaten vorgenommen wurde, die übrigens sowohl beim Server als auch auf der „simulierten“ Smartcard vorlagen, konnte die Kommunikation auch nicht nur über die IP-Adressen der Dienste erfolgen.

Denn das Zertifikat, das ein Dienst für eine Verschlüsselung der Kommunikation vorhält muss für eine menschenlesbare Adresse des Dienstes und nicht auf eine IP-Adresse ausgestellt sein.

Ein weiteres Problem ergab sich bei der Kommunikation einer auf einem Mac OS X-System residenten Benutzungsschnittstelle mit dem auf einem Windows-System residenten Datenautorisierungsdiensteanbieter, wenn eine Dokumentation des Besuches eines Versicherten bei einem Heilberufler eingelagert oder abgerufen werden sollte.

Das Datenarchiv war als Web-Service auf Basis von JBoss realisiert und gab an das Mac OS X-System Fehlermeldungen zurück, die das System trotz korrekt installierter Pakete nicht interpretieren konnte und folglich zu einem Laufzeitfehler führte. Der gleiche Aufruf zwischen den Komponenten auf Windows-Systemen führte nicht zu diesem fatalen Laufzeitfehler.

## **4. Ausblick**

Dieses letzte Kapitel soll die hier vorgelegte Implementierung aus der Sicht von Aspekten des Medienbruches analysieren, Perspektiven für selbige aufzeigen und in abschließenden Worten die Aktivitäten um die Einführung der elektronischen Gesundheitskarte in Deutschland bewerten.

### **4.1 „The hidden problem: Cross-Media?“**

Die Idee des Projektes lag in ihren Anfängen noch in dem Einsatz von Gesundheitskarten, welche mittels RFID ausgelesen und beschrieben werden sollten. Die Gründe für den Kurswechsel ergaben sich nicht nur aus den in Kapitel 3.3 beschriebenen technischen Hindernissen, sondern auch in Folge der Analyse der vorhandenen Realisierungen von Architekturen für eine elektronische Verwaltung von Patientendaten. Dabei sollte nicht nur den teils inkonsistenten und für Deutschland bundesweit zu erwartenden Ansatz der Projektgruppe bit4Health (vgl. auch Bewertungen in Kapitel 2.2 ) entgegengetreten, sondern dem etwas komplexeren Anforderungen der Vertreter der Heilberufe Rechnung getragen werden. Außerdem ermangelt der Entwurf der Sicherheitsarchitektur der Projektgruppe bit4Health, wie oben ausgeführt, jeglichen Ansatz einer umfassenden Absicherung von IT-Infrastrukturen, sondern fokussiert vor allem auf die funktionalen Anforderungen sowie die verfügbaren Technologien, welche dann selbst wegen nicht bedachter Seiteneffekte oder wegen nur partieller Wirksamkeit der eingesetzten Mechanismen häufig sicherheitsrelevante Probleme erst hervorrufen.

Eine Technologie, welche aber von der Anforderung an Sicherheit getrieben ist, sollte immer beim Geschäftsprozess und damit bei den Interessen der beteiligten Parteien ansetzen, da sich Sicherheit bezogen auf die Domäne des Geschäftsprozesse mitunter unterschiedlich und nicht vorkonfektioniert gestaltet, sondern Sicherungsmechanismen funktional auch häufig bei der Klärung von Haftungsfragen unterstützend wirken sollen. In diesem Fall hilft es dann nicht, unautorisierte Zugriffe auf geschützte Objekte lediglich abzuwehren, sondern vor allem autorisierte Zugriffe revisionssicher zu dokumentieren.

Aus dieser Sicht wird der Medienbruch und damit der Aspekt des „Cross-Media“ in der vorgelegten Implementierung deutlich.

Der Vollständigkeit halber seien die wesentlichen Merkmale von „Cross-Media“ noch einmal zitiert[29]:

Vision einer „omnipotenten“ Medienmaschine: ... **Inhalte liegen in verschiedenen Formaten auf verschiedenen Datenträgern an unterschiedlichen Orten** und sie werden von **unterschiedlichen Orten, unterschiedlichen Endgeräten** und Anwendern **gezeigt** bzw. abgerufen. ... **Es soll um den Aufbau von Netzstrukturen und die an diesen Netzstrukturen angeschlossenen Geräte** gehen. Die angeschlossenen Geräten können verschiedenste elektronische Geräte sein. ... Die Daten liegen in verschieden Formaten auf verschiedenen Servern.

Auch wenn der Medienbruch bei Einsatz von RFID-basierten Datenträgern offensichtlich und wohl kaum notwendigerweise zu begründen gewesen wäre, verfügt dieses Projekt ebenfalls über zahlreiche Medienbrüche.

**Verschiedene Formate:** die Dokumentation eines Versicherten bei einem Heilberufler liegt verschlüsselt und signiert im Datenarchiv vor, eine Referenz auf diese Dokumentation dagegen auf der Gesundheitskarte des Versicherten, und werden entschlüsselt und von der Signatur entledigt in der Benutzungsschnittstelle des Heilberuflers angezeigt;

die Benutzer halten jeweils auf den Datenträger zusätzlich identifizierende und zur Autorisierung verwendbare Daten, nämlich Zertifikate und Schlüssel vor, welche zumindest beim Heilberufler auch durch entfernte Rufe an das Trust-Center verifiziert werden

**Netzstruktur bzw. verschiedene Orte:** die Daten des Versicherten werden disjunkt an verschiedenen Orten gespeichert, nämlich die Dokumentation seines Besuches beim Heilberufler in einem Datenarchiv und die verbleibenden auf seiner elektronischen Gesundheitskarte

die den Heilberufler identifizierenden Daten liegen spiegelbildlich sowohl auf seinem Identitätsnachweis als auch im Trust-Center vor und werden validiert

**Verteilung der Dienste:** ergibt sich aus der Komponentenübersicht (vgl. Figure 7), also aus der Zerlegung von Rechten an der Ausführung der Benutzungsschnittstelle mittels Authentifizierung des Heilberuflers gegen das Trust-Center und dem Recht am Zugriff auf das Datenarchiv mittels Authentifizierung des Heilberuflers gegen den Datenauthorisierungsanbieter, welcher nach erfolgreicher Validierung die Anfrage an den Datenarchiv-Dienstanbieter weiterleitet;

hinzu kommt der beim Heilberufler lokal agierende Dienst des Kartenlesegerätes

**Verteilung der Daten:** analog zu Punkt „Netzstruktur bzw. verschiedene Orte“ die elektronische Dokumentation des Besuches eines Versicherten beim Heilberufler

#### **4.2 „The obvious problem: work in progress!“**

Das Kapitel 3.3 hat verschiedene Ansätze für eine zukünftige Weiterentwicklung dieses Projektes in einem wissenschaftlichen Umfeld gegeben, die vor allem technischer Natur sind, aber die Funktionalität und Verwertbarkeit des Projektes beträchtlich verbessern würde.

Allerdings stellt sich nicht nur die Frage, inwiefern sich das hier beschriebene Projekt in das „Referenzmodell“ einer Telematik für die elektronische Gesundheitskarte einfügt, sondern auch inwiefern es in Kontext des Gesundheitswesens oder einem anderen Kontext verwendbar wäre.

Zur Einordnung in den Kontext des „Referenzmodell“ bleibt zu sagen, dass aufgrund der groben Ausführungen eine Umsetzung dieses somit auch gegeben ist. Für die notwendige prototypische Präsentation war es wichtig alle Schichten, also Clientseite (Dienstenutzer),

Kommunikation (-infrastruktur) und Serverseite (Diensteanbieter), zu implementieren. Auch die Erweiterung und gleichzeitig die Verteilung der Daten auf mehrere Hosts und deren Lokalisierung lässt sich ebenfalls mit dem „Referenzmodell“ vereinbaren.

Bezüglich des Einsatzes des Projektes innerhalb einer Telematik für die elektronische Gesundheitskarte bleiben die Bemerkungen aus Kapitel 2, dass die Einführung der Gesundheitskarte nicht nur monopolistisch und konzertiert organisiert wurde und wird, folglich die Zuständigkeitsbereiche der einzelnen Mitglieder der Projektgruppe bIT4Health abgesteckt und vergeben sind, und ferner die Projektgruppe bIT4Health und das Bundesministerium für Gesundheit und Soziale Sicherung offensichtlich den Interessen der Gesetzlichen Krankenversicherungen an einem zentralen Datenspeicher erlegen ist oder eben die Gesetzlichen Krankenversicherungen und das Bundesministerium für Gesundheit den Interessen der Projektgruppe bIT4Health an einer schnellen und scheinbar billigen Lösung erlegen ist.

Genau dieser Ansatz wird aber nicht nur aus Sicht der Datenschützer[3] sondern wegen der nicht unbeträchtlichen Anlaufkosten und den bisher nicht zu kalkulierenden Folgekosten bei den Vertretern der Heilberufe[18] für weiteren Zündstoff sorgen.

Allerdings war jüngst zu lesen, dass für den Fall eines Wahlsieges der CDU/CSU-Fraktion im September 2005 das Projekt der Einführung der elektronischen Gesundheitskarte aufgeschoben wird[34]. In diesem Fall haben alle prächtig verdient, mit Ausnahme des Krankenversicherten - die beabsichtigte Kosteneinsparung ist damit schon im Ansatz zur Farce verkommen.

Abseits des Kontextes Gesundheitswesen kann das Projekte innerhalb von Handelsplattformen, etwa elektronische Auktionshäusern, zum Einsatz kommen, also überall dort, wo die Einlagerung von revisionssicheren und vertraulichen Dokumenten zweier Vertragsparteien durch unabhängige Dritte notwendig wird.

Allerdings sei explizit darauf hingewiesen, dass ein derartiger Einsatz nur dann Sinn macht, wenn sich die beiden Vertragsparteien lokal an einem Platz befinden und Identifikationsnachweise vorhalten können, welche den Nachweis der Identität garantieren können und deren kryptographische Mechanismen nicht kompromittiert wurden.

Dieser Fall könnte beispielsweise bei Geschäften mit Gebrauchsmaschinen, welche zwar elektronisch abgewickelt werden können, aber aufgrund der Spezialität der Ware vor allem im industriellen Sektor häufig mit persönlichen Besuchen des Käufers beim Verkäufer verbunden sind. Auf diese Weise können dann Käufer und Verkäufer ihren Willen bekunden und im Fall von Vertragsstreitigkeiten gegenüber einem Gericht auf Basis der revisionssicheren Dokumentationen ihre Ansprüche durchsetzen. Ebenso kann es sich bei der Erledigung von elektronischen Behördenvorgängen verhalten, wenn etwa eine Bewerbung auf eine öffentliche Ausschreibung, versehen mit der Signatur des Sachbearbeiters und des Bewerbers und verschlüsselt mit dem öffentlichen Schlüssel des Sachbearbeiters beim Amt hinterlegt wird.

Auf diese Weise können Streitigkeiten um den Eingang eines Dokumentes, seinen Inhalt oder die Authentizität einer Unterschrift behoben werden, denn eine elektronische Signatur ist bei Einsatz geeigneter Mechanismen immer noch schwerer zu fälschen als eine menschliche Unterschrift.

Abseits davon eröffnen derartige Ideen aber auch berechtigten Ängsten um einen Orwellschen Staat Tür und Tor, die hier aber nicht weiter ausgeführt werden, weil sie im Rahmen dieses Seminars zur Genüge diskutiert wurden.

### 4.3 „The political problem: just think“

Die Einführung der elektronischen Gesundheitskarte steht in einem Spannungsfeld von mitunter divergierenden Interessen. Offensichtlich ist, dass sie von keinem demokratischen Prozess geführt wurde, sondern in Anlehnung an Europäische Harmonisierungsvorhaben als ministerielles Vorhaben angestoßen wurde und so auch konzertiert vom Entwurf bis zur Realisierung durchgeführt wird.

Zwar wünscht angeblich die Mehrheit der Bundesbürger die mit der Einführung der elektronischen Gesundheitskarte verbundenen Vorteile, also die verbesserte Verfügbarkeit von Daten sowie die Integration aller Geschäftsprozesse des Gesundheitswesens für eine durchgängigere und nahtlose Versorgung, allerdings scheint es, dass die Diskussion um die entscheidenden Intentionen noch immer ungenügend kommuniziert wurden oder bewusst ungenügend kommuniziert werden.

Denn die elektronische Gesundheitskarte soll der Freisetzung von Einsparpotenzialen dienen, weshalb es fraglich erscheint, inwiefern ein vorerst kostenintensiver Technologieträger dazu geeignet sein soll, zumal sich die Gesetzlichen Krankenversicherungen bisher als relativ avers gegen jegliche Reform gezeigt haben. Die bisherigen Reformen der Deutschen Bundesregierung haben bisher nachweislich nicht die erhofften Effekte, vor allem zu Gunsten der Versicherten, erbracht und ein maßgeblicher Teil der Kostensteigerungen ist bisher nachweislich der Ausweitung des Personalstammes der Gesetzlichen Krankenversicherungen geschuldet. Nun kann außerhalb von sozialistischen Arbeitsstrukturen Technik Personal ersetzen, aber die Inbetriebnahme und Wartung von Technik erfordert auch Personal.

Da die Einführung der elektronischen Gesundheitskarte den Krankenkassen in einem gewissen Sinne von außen verordnet wurde und diese zwar gern die Vorteile aber nicht die Kosten der elektronischen Verwaltung von Patientendaten - vermittels des zentralen Datenspeichers - aufnehmen wollen, verfolgt auch diese Reform den falschen Ansatz.

Den Vorteil der elektronischen Gesundheitskasse würde Volker Grassmuck wahrscheinlich mit den Worten „Datenherr“ Krankenkasse beschreiben, die in Bezug auf die Vertraulichkeit der Daten des Versicherten nicht unerhebliche Konsequenzen nach sich ziehen.

Der Datenschutzbericht des Datenschutzberichtes des Landes Berlin konstatiert deshalb nicht ohne Grund im Jahre 2003[30, S. 78]:

Begleitet werden diese Maßnahmen durch die Einführung einer bundeseinheitlichen Krankenversichertennummer (§ 290 SGB V). Diese Krankenversichertennummer darf zwar nicht mit der Rentenversicherungsnummer identisch sein, stellt aber wegen ihrer bundesweiten Vereinheitlichung eine weitere Initiative zur Schaffung einer Personenkennziffer dar.

Dies erinnert nicht nur an US-amerikanische Verhältnisse, sondern auch an die als „menschenverachtend und diktatorisch“ konnotierten Verhältnisse in der DDR, in denen jede Reise eines Bürger mittels einer Personenkennziffer verfolgbar war.

Denn sie wird von Technik zur Kosteneinsparung motiviert und nicht von den Geschäftsprozessen im Gesundheitswesen.

Außerdem fällt auf, dass dem §291a SGB V jeglicher Bezug auf ein Europäisches Harmonisierungsvorhaben fehlt, das zumindest eine Regelung einer einheitlichen Sprache und ferner Struktur der Daten erfordern würde. Denn aus europäischer Sicht müsste eine deutsche elektronische Gesundheitskarte auch von nicht-deutschen, europäischen Software-Systemen gelesen werden können und folglich die Daten auch einem nicht-deutschen, europäischen Mediziner vor allem bei einem Notfall der vorgeblich reiselustigen Deutschen zur Verfügung stehen. Diese Sprache könnte dann entweder die Sprache der Mediziner, das Latein, oder im einfachsten Fall Englisch sein.

Dies weist aber darauf hin, dass die elektronische Gesundheitskarte vor allem ein nationales Unterfangen, wenn der Auslandskrankenschein E111 nur als Sichtvermerk auf der Berechtigungskarte vorliegt, womit die „integrierte Versorgung“ und „Verfügbarkeit von Daten“ de facto an der deutschen Grenze endet.

Ob dies nun ein erneuter Beleg der Inkompetenz der Akteure im politischen Tagesgeschäft und ein Argument gegen die indirekte Demokratie ist, wenn nur national und die Folgen eines Gesetzes nicht konsequent zu Ende gedacht werden, oder ob hier konsequentes Kalkül des Protektionismus der relativ teuren deutschen medizinischen Dienstleistungen gegen deutsche „Medizin-Touristen“ im Ausland die Feder führte, bleibt offen.

Allerdings spricht die späte Einsicht der Parlamentarier für die Aufnahme der Notfalldaten in den lokalen Bestand der elektronischen Gesundheitskarte[32], also ohne Abrufe der Daten von entfernten Dienste bei einer möglicherweise inexistenten Verbindung mit dem Internet, deutlich für den ersten Fall.

Neben der in Kapitel als nicht unkritisch diskutierten Vergabepaxis des Bundes bei der Einführung der elektronischen Gesundheitskarte ist festzustellen, dass in Deutschland nicht nur ein starker Hang zu zentralistischen Strukturen, sondern auch komplexen Komplettlösungen, die lediglich den Erfordernissen einer Gegenwart begegnet, existiert.

So wäre die Alternative eine schrittweise Einführung einer elektronischen Verwaltung von Patientendaten, etwa den Versichertendaten und dem elektronischen Rezept, gefolgt von weiteren medizinischen Daten, welche sich aus dem Dialog mit den Heilberuflern und Versicherten oder/und aus der Analyse der Geschäftsprozesse im Gesundheitswesen ergeben hätte, denkbar gewesen. Stattdessen wird ähnlich den deutschen Maut-Systemen eine neue Technologie „aus einem Guß“ geplant und stetig weiterentwickelt.

In den Niederlanden[32, S. 12]:

gibt es ... derzeit Feldversuche, die Versicherungskarte in die SIM-Karte des Mobiltelefons zu integrieren und diese mit einem Transponder auszustatten. Beim Arzt oder Apotheker wird eine verschlüsselte Verbindung aufgebaut und nach Eingabe der PIN können die Stammdaten ausgelesen und neue Daten für Rezepte gespeichert. Etwaig anfallende Praxisgebühren oder Zuzahlungen bei Medikamenten können dann bequem über die Telefonrechnung abgerechnet werden.

Es bleibt auch zu bemerken, dass Einführung von drahtlosen Technologien, etwa von RFDI-basierenden Gesundheitskarten eher den Bestrebungen der Industrie entsprechen und bei datenschutzrechtlichen Bedenken mit fadenscheinigen Argumenten abgeschmettert werden.

Denn einerseits sind RFID-Technologien nun nicht mehr als „sicher“ anzusehen, wenn etwa Forscher der Uni Baltimore im Jahre 2005 gemeinsam mit Experten der RSA Security den in den USA als Wegfahrsperre genutzten RFID-Transponder von Texas Instruments knacken[33] und andererseits Anleitungen für Angriffe auf SmartCards vielfach im World Wide Web bereitstehen.

Folglich ist das berührungslose Auslesen von der Daten von RFID-basierten Karten nur eine Vereinfachung möglicher Angriffsszenarien, weil damit weder der physische Kontakt zu Karte notwendig ist noch die Quelle eines Angriffes verifizierbar ist.

Zwar ist es zu begrüßen, dass der §291a SGB V sich sowohl auf den Datenschutz bezieht und den Missbrauch der Karten eindämmen will, aber weder die von Projektgruppe bit4Health vorgelegte Entwurf einer Sicherheitsarchitektur noch die Verwendung der Karten lassen darauf schließen, dass dieser Missbrauch tatsächlich verhindert werden könnte.

Denn einerseits sind die Zugangspasswörter für die elektronische Gesundheitskarte viel zu kurz (vgl. Ausführungen im Kapitel „Produktdaten“ des Lastenheftes) und andererseits ist die

„Ausleihe“ von Gesundheitskarten an Heilberufler mit krimineller Energie nicht ausgeschlossen. Das Gesetz wie auch die Projektgruppe BIT4Health sieht bisher keine Revisionssicherung vor.

Der Aspekt des Missbrauches wirft beim Einsatz von intransparenten und in Bezug auf die Projektgruppe BIT4Health auch inkonsistenten Sicherungsmechanismen mehr denn je die Frage nach der Verantwortung der Beteiligten am Datenschutz auf.

Denn ein Missbrauch von Daten kann auch ohne Wissen eines Heilberuflers bei unwirksamen oder nur partiell wirksamen Sicherungsmechanismen nach einem Angriff vorliegen. Und wenn der Heilberufler den Angriff und damit seine Unschuld nicht nachweisen kann, sind automatisch die Entwickler derartiger Architekturen gefragt. Zwar sind nach einer Umfrage[19] die Heilberufler Telematik-Systemen nicht abgeneigt (etwa 75%) und behalten sich deshalb auch die persönliche Entscheidungskompetenz für den Einsatz von Telematik-Systemen vor. Allerdings beschreiben 60% der befragten Heilberufler ihre EDV-Kenntnisse nur als durchschnittlich.

Aus diesem Grund und vor allem wegen der Idee der Arbeitsteilung sollte den Heilberuflern nicht auch noch die Haftung für den Datenschutz in dem zentralistischen Modell der Krankenkassen zugewiesen werden, sondern - wie bemerkt – den Entwicklern des Modells.

Letztlich sei angemerkt, dass vielleicht ein fundamentaler Fehler aller Realisierungen einer elektronischen Verwaltung von Patientendaten die Orientierung am Szenario des „home banking“ ist.

Denn, wie schon bemerkt, haben die Beteiligten dieser Realisierung im Gesundheitswesen andere und weitreichendere Interessen als den Durchlauf von Rechnungsposten, sondern eher der medizinischen Versorgung, welche durch eine verlässliche und vertrauliche Datenbasis gestützt wird. Und ferner sind an dem Geschäftsprozess mindestens zwei Parteien beteiligt, die im Dialog einen Heilplan entwerfen, welcher dann von anderen Parteien wie der Krankenkasse oder weiteren Vertretern der Heilberufe unterstützt wird. Folglich agiert dabei nicht wie beim „home banking“ ein Mensch über eine Maschine mit einer Bank, deren elementare Dateneinheit eines Geldsurrogates ist, sondern es agieren Menschen miteinander, die hintergründig von Maschinen mit komplexen und nicht atomisierbaren Daten unterstützt werden wollen.

## 5. Literaturverzeichnis

1. „Telemedizin und eHealth in Deutschland: Materialien und Empfehlungen für eine nationale Telematikplattform“, Dr. med. Frank Warda, Dr. med. Guido Noelle, DIMDI, 2002, [http://www.dimdi.de/static/de/ehealth/public/telematikbuch19\\_02\\_03\\_web.pdf](http://www.dimdi.de/static/de/ehealth/public/telematikbuch19_02_03_web.pdf)
2. „Bundesministerium für Gesundheit und Soziale Sicherung“, BMGS, Juni 2005, <http://www.bmgs.bund.de/>
3. „Die elektronische Gesundheitskarte“, Thilo Weichert, DuD - Datenschutz und Datensicherheit 28 (2004) 7, Datenschutzzentrum Schleswig-Holstein, S. 391 – 403, [http://www.datenschutzzentrum.de/medizin/gesundheitskarte/dud\\_gesundheitskarte.pdf](http://www.datenschutzzentrum.de/medizin/gesundheitskarte/dud_gesundheitskarte.pdf).
4. „Innovative Technologien und Lösungen für integrierte Versorgungsnetze im Gesundheitswesen“, Microsoft, CEBIT 2005, Mai 2005, [http://download.microsoft.com/download/d/f/3/df341408-6196-4082-9a52-9c3457a66e03/CeBIT05\\_PM\\_Health.doc](http://download.microsoft.com/download/d/f/3/df341408-6196-4082-9a52-9c3457a66e03/CeBIT05_PM_Health.doc)
5. „Dokumente der Rahmenarchitektur Version 1.1“, Deutsches Institut für Medizinische Dokumentation und Information, Mai 2005, [http://www.dimdi.de/static/de/ehealth/karte/technik/rahmenarchitektur/rahmen\\_aktuell.htm](http://www.dimdi.de/static/de/ehealth/karte/technik/rahmenarchitektur/rahmen_aktuell.htm)
6. „secunet präsentiert Telematik-Konnektor“, Pressemitteilung via OMNICARD, Dezember 2004, [http://www.omnicard.de/news/nl\\_04\\_12.pdf](http://www.omnicard.de/news/nl_04_12.pdf) sowie Pressemitteilung von der secunet AG selbst, Dezember 2004, [http://www.secunet.de/download/presse/20041124-pi\\_medica\\_konnektor-de.pdf](http://www.secunet.de/download/presse/20041124-pi_medica_konnektor-de.pdf).
7. „Elektronische Gesundheitskarte kommt pünktlich“, 11.01.2005, Regierung online, <http://www.bundesregierung.de/Politikthemen/Gesundheit-und-Soziales-9957/Elektronische-Gesundheitskarte.htm>.
8. „Elektronische Gesundheitskarte teurer als erwartet?“, Philipp Grätzel von Grätz, Telepolis, 19.05.2004, <http://www.telepolis.de/r4/artikel/17/17421/1.html>.
9. „Sichere Inter-Netzwerk Architektur (SINA)“, Bundesamt für Sicherheit in der Informationstechnik, <http://www.bsi.de/fachthem/sina/sysbesch/sysbesch.htm>.
10. „SINA VPN – höchste Sicherheit für elektronische Kommunikation“, secunet AG, 2003, [http://www.secunet.de/download/fs/fs\\_sina\\_d.pdf](http://www.secunet.de/download/fs/fs_sina_d.pdf).
11. „secunet AG: Großauftrag für SINA® Komponenten“, Ad-hoc-Meldung nach § 15 WpHG, 10. Mai 2005, Essen, <http://allpr.de/13313/Ad-hoc-Meldung-nach-%A7-15-WpHG-secunet-AG-Grossauftrag-fuer-SINA-Komponenten.html> sowie weitere Finanzmeldungen der secunet AG selbst, [http://www.secunet.de/content.php?ln=1&text=u\\_irpr\\_finanzmeldungen&mnl=202](http://www.secunet.de/content.php?ln=1&text=u_irpr_finanzmeldungen&mnl=202).
12. "Elektronische Ausweise und Biometrie", secunet AG, 30.03.2005, [http://www.secunet.de/download/fs/fs\\_d\\_050330\\_biometrie\\_und\\_epassport\\_v01.pdf](http://www.secunet.de/download/fs/fs_d_050330_biometrie_und_epassport_v01.pdf).
13. Web-Site des Pilotprojektes zur Einführung der elektronischen Gesundheitskarte: <http://www.gesundheitskarte-rheinland-pfalz.de>.
14. „Sicher vernetzt Ärzte unter sich“ med-online, S. 15, 01/2003.
15. „Elektronische Gesundheitskarte: Szenario mit bewährten Systemen“, dent-online, S. 24-25, 01/2005.

16. „Ärztenez Remscheid Praxisübergreifend kooperieren - aber sicher“, med-online 04/2004, S. 20
17. „medisign Card: Vertrauen ist gut verschlüsseln ist besser“, med-online, S. 18, 04/2004.
18. „Die Elektronische Gesundheitskarte kommt: Die Kassen verdienen - und wir sollen zahlen?“, Dr.Manfred Diensberg, Der Hausarzt, S. 34, 02/2004.
19. „Ärztebefragung: Bereit für Telematik?“, med-online, S. 19, 02/2004.
20. „Was ist HL7?“, HL7 Deutschland, 1999,  
<http://www.hl7.de/standards/wasisthl7kurz.html>
21. „Zusammenfassung zur Clinical Document Architecture (CDA)“, Dr. Kai U. Heitmann, Universität zu Köln, 27,03.2001,  
<http://www.sciphox.de/atwork/cda/ZusammenfassungCDA.pdf>.
22. „Sciphox Dokumenten-Kommunikation im Gesundheitswesen - Ein Überblick“, Arbeitsgemeinschaft Sciphox GbR mbH, 2005,  
[http://www.sciphox.de/ueber\\_uns/flyerallgemein.pdf](http://www.sciphox.de/ueber_uns/flyerallgemein.pdf).
23. „Phase I Kommunikationsumfang und -inhalt Spezifikation zum standardisierten elektronischen Kurzbericht (Entlassungsbrief, Überweisung und Einweisung)“, SCIPHOX v1.0 Working Draft 15 vom 12. Juni 2002,  
<http://www.sciphox.de/atwork/tools/WD-sciphox-v15.pdf>.
24. *Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte; Fraunhofer??*
25. „Erarbeitung einer Strategie zur Einführung der Gesundheitskarte, Informationsmodell“, Projektgruppe bit4Health, Version 1.1, 12. August 2004,  
[http://www.dimdi.de/static/de/ehealth/karte/download/b4h\\_informationsmodell\\_v1-1.pdf](http://www.dimdi.de/static/de/ehealth/karte/download/b4h_informationsmodell_v1-1.pdf).
26. „Erarbeitung einer Strategie zur Einführung der Gesundheitskarte, Sicherheitsarchitektur“, Projektgruppe bit4Health, Version 1.1, 12. August 2004,  
[http://www.dimdi.de/static/de/ehealth/karte/download/b4h\\_sicherheitsarchitektur\\_v1-1.pdf](http://www.dimdi.de/static/de/ehealth/karte/download/b4h_sicherheitsarchitektur_v1-1.pdf).
27. Patrik Schmid, Remo Ferrari. OSI-Sicherheitsarchitektur. Studienarbeit an der Hochschule für Technik Rapperswill (Schweiz), 1998.  
<http://www.ita.hsr.ch/studienarbeiten/arbeiten/WS98/SecurityTutorial/sicherheitsarchitektur.html> .
28. „Mit der eGK zum EKG“, Susanne Köhler, 03.05.2005,  
<http://www.gesundheit.de/medizin/gesundheitsystem/gesundheitspolitik/elektronisch-e-gesundheitskarte/printer.html>.
29. Beschreibung der Veranstaltung „Cross-Media“, <http://www.semanticmedia-showcase.de/WerkstattCM/CrossMedia/inhalte.htm>
30. Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2003, <http://www.datenschutz-berlin.de/infomat/dateien/jb/jb03.pdf>.
31. „Elektronische Gesundheitskarte: Ausschuss gibt grünes Licht“, Detlef Borchers, Heise-Newsticker, 14.04.2005, <http://www.heise.de/newsticker/meldung/58555>.
32. "RFID im Gesundheitswesen", Simon Schnell, Seminararbeit an der Universität Bayreuth, Rechts- und Wirtschaftswissenschaftliche Fakultät, Lehrstuhl für

Betriebswirtschaftslehre, Bayreuth, 03. Juni 2005, [http://wi.oec.uni-bayreuth.de/fileadmin/download/05\\_I/seminar/Thema%2017%20-%20Schnell.pdf](http://wi.oec.uni-bayreuth.de/fileadmin/download/05_I/seminar/Thema%2017%20-%20Schnell.pdf).

33. Kurznachrichten, pcGo, S. 16, 06/2005.

34. „Elektronische Gesundheitskarte: Weiterer Aufschub durch Bundestagswahl“, Detlef Borchers, Heise-Newsticker, 21.07.2005, <http://www.heise.de/newsticker/meldung/61920>