Lösungsarchitektur für die Einführung der elektronischen Gesundheitskarte und der auf ihr basierenden Anwendungen

Die Autoren

Paul Frießem
Dirk Kalmring
Peter Reichelt

Paul Frießem
Dr. Dirk Kalmring
Peter Reichelt
Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT)
Bereich Sichere Prozesse und Infrastrukturen (SPI)
Schloss Birlinghoven
53754 Sankt Augustin
{paul.friessem | dirk.kalmring | peter.reichelt}@sit.fraunhofer.de

1 Telematikinfrastruktur für das deutsche Gesundheitswesen

Mit dem Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz, GMG) vom 2003-11-14 fiel der Startschuss für die Schaffung einer Telematikinfrastruktur für das gesamte deutsche Gesundheitswesen [Bund03]. Kernstück dieser Neuordnung ist die Einführung einer elektronischen Gesundheitskarte (eGK) und mehrerer auf ihr basierender Anwendungen (z. B. elektronisches Rezept, „eRezept"). Relevant sind hier vor allem die Änderungen der Paragraphen 67 und 291 des fünften Buches Sozialgesetzbuch (SGB V). § 67 schreibt vor, dass die papiergebundene Kommunikation (z. B. Rezept, Arztbrief) durch eine elektronische Kommunikation abgelöst werden soll. § 291 besagt, dass jeder Versicherte von seiner Krankenkasse eine Krankenversichertenkarte (KVK, seit 1993/94) und ab 2006-01-01 eine elektronische Gesundheitskarte erhält. Der durch das GMG neu geschaffene § 291a beinhaltet ausführliche Beschreibungen der eGK, z. B. welche Angaben gespeichert werden und wer auf die Daten der Karte zugreifen darf.

Die Spitzenverbände der gesetzlichen Krankenversicherung (GKV) und der Leistungserbringer im Gesundheitswesen (Ärzte, Zahnärzte, Krankenhäuser, Apotheken) haben den gesetzlichen Auftrag erhalten, bis zum Herbst 2004 dem Bundesministerium für Gesundheit und soziale Sicherung (BMGS) ein Konzept für die erforderliche Telematikinfrastruktur vorzulegen. Zu diesem Zweck entwickelte das Projektbüro der Selbstverwaltung protego.net (Projekt für Telematik der Gesundheitsorganisationen) eine Lösungsarchitektur.

Die Komplexität des Vorhabens ist außerordentlich hoch, gilt es doch rund 80.000.000 Patienten, 270.000 Ärzte, 77.000 Zahnärzte, 2.000 Krankenhäuser, 300 Krankenkassen sowie 22.000 Apotheken zu vernetzen und beispielsweise rund 700.000.000 Rezepte bzw. 900.000.000 Verordnungen im Jahr zu verarbeiten [Bund02]. Ziele der Einführung der eGK sind die Steigerung der Qualität der medizinischen Versorgung (z. B. Arzneimittelsicherheit), die Verbesserung der Wirtschaftlichkeit (vor allem mittels eRezept) und die Erhöhung der Leistungstransparenz im Gesundheitswesen. Die Ablauforganisation soll optimiert, aktuelle gesundheitsstatistische Informationen sollen bereitgestellt und die patientenorientierten Dienstleistungen sollen ver-

Kernpunkte

In Deutschland soll jeder Versicherte in der gesetzlichen Krankenversicherung ab 2006-01-01 eine elektronische Gesundheitskarte erhalten. Der Praxisbericht beschreibt den gegenwärtigen Stand der Systemarchitektur für die Telematikinfrastruktur, wie sie durch die Selbstverwaltung im Gesundheitswesen erarbeitet wird.

- Ziele bei der Einführung der Gesundheitskarte sind Qualitätssteigerung bei der medizinischen Versorgung, Verbesserung der Wirtschaftlichkeit und Leistungstransparenz im Gesundheitswesen.
- Die Vielzahl der Akteure sowie die Anforderungen aus rechtlicher, auch datenschutzrechtlicher, und technischer, auch sicherheitstechnischer Sicht führen zu einem hochkomplexen Vorhaben.
- Die Gesamtarchitektur basiert auf bestehenden Systemen, die über Konnektoren an die Telematikinfrastruktur mit ihren Diensten angebunden sind.

Stichworte: elektronische Gesundheitskarte (eGK), Heilberufeausweis (HBA), elektronisches Rezept, Gesundheitswesen, Telematikinfrastruktur, Lösungsarchitektur

Tabelle 1 Vergleich von KVK und eGK [Deut04]

	KVK	eGK
Verschlüsselung	nein	ja
Speichergröße	256 Byte	32.000–64.000 Byte
Signaturfähigkeit	nein	ja
Personalisierung	Vorderseite	Vorderseite/Rückseite
Passfoto	nein	ja
Gesundheitsdaten	nein	ja

bessert werden. Nicht zuletzt sollen die Eigenverantwortung der Patienten gestärkt sowie ihre Mitwirkungsbereitschaft und -initiative stimuliert werden. Tabelle 1 stellt KVK und eGK gegenüber.

Die Verwendung der 1993/94 eingeführten und ebenfalls per Gesetz durchgesetzten Krankenversichertenkarte als Legitimationsnachweis des Versicherten gehört heute ebenso wie die entsprechenden Kartenterminals zur täglichen Routine einer jeden Arztpraxis. Zwar konnten Prozesse verbessert und maschinenlesbare Belege eingeführt werden, eine Sektoren übergreifende elektronische Kommunikation (zu administrativen wie medizinischen Zwecken) ist allerdings nicht möglich.

§ 291a GMG schreibt für die im Zusammenhang mit der eGK zu speichernden Daten einen Pflichtteil („administrativer Teil“) und einen freiwilligen Teil („medizinischer Teil“) vor [Bund03]. Letzterer enthält Daten, die nur erhoben, gespeichert, verarbeitet und zugänglich gemacht werden, sofern der Versicherte dies wünscht. Der Pflichtteil enthält das eRezept, den europäischen Krankenschein E 111 und Versicherungsangaben. Letztere beinhalten die Bezeichnung der ausstellenden Krankenkasse, das Kennzeichen der örtlichen Kassenärztlichen Vereinigung (KV), den Familiennamen, den Vornamen, das Geburtsdatum, das Geschlecht, die Anschrift, die Krankenversichertennummer, den Versichertenstatus (z. B. Mitglied, Familienversicherter, Rentner), den Zuzahlungsstatus, den Beginn des Versicherungsschutzes, die Unterschrift und das Lichtbild des Versicherten sowie das Datum, zu dem die Karte ihre Gültigkeit verliert. Der freiwillige Teil umfasst eine Dokumentation der eingenommenen Arzneimittel, Notfallinformationen (z. B. Blutgruppe), zusätzliche Gesundheitsinformationen (z. B. aktuelle Diagnosen), den elektronischen Arztbrief (Mitteilungen) und die Patientenquittung, die den Patienten über die vom Arzt erbrachten Leistungen und deren voraussichtliche Kosten informieren soll. Ferner kann der Versicherte selbst Daten zur Verfügung stellen, wie z. B. Verlaufsprotokolle im Falle eines Diabetikers.

2 Einordnung der Arbeiten

Wie spätestens 1998 durch eine viel beachtete Studie zu Perspektiven der Telematik im Gesundheitswesen [Rola98] deutlich geworden ist, handelt es sich bei der Schaffung einer einheitlichen Telematikinfrastruktur für das Gesundheitswesen um einen volkswirtschaftlich wünschenswerten Schritt.

Staat, Selbstverwaltung und Industrie sind gefordert, einige Rollen sind durch das Gesetz vorgegeben. Das GMG verpflichtet die Selbstverwaltung, eine Informations-, Kommunikations- und Sicherheitsinfrastruktur für die Telematik im Gesundheitswesen zu vereinbaren. Das Resultat bedarf der Genehmigung durch das BMGS. Schafft es die Selbstverwaltung nicht, eine solche Vereinbarung zu treffen, werden deren Inhalte durch das BMGS festgelegt („Ersatzvornahme“, § 291a Abs. 7 SGB V).

Im Jahr 2003 initiierte das BMGS das Projekt bIT4health (better IT for health). Das beauftragte Industriekonsortium erarbeitete eine Rahmenarchitektur, in der generische Abläufe und wesentliche fachliche Regeln und Rollen, die organisatorischen und rechtlichen Anforderungen und das Zusammenwirken dargestellt werden [Bund04a]. Diese Arbeiten wurden durch eine Skizzierung der Lösungsarchitektur („Solution Outline“ [Bund04b]) ergänzt.

Die Selbstverwaltung begann 2004 mit der intensiven Arbeit an der Lösungsarchitektur. Ergebnis war eine technische Systemarchitektur als Grundlage für eine ausbaufähige Telematikinfrastruktur. Es wurden Basiskomponenten konzipiert, die an den erwarteten Zuwachs an Bedarf nach Gesundheitsanwendungen angepasst werden können. Die bekannten und erprobten Technologien reichen aus, um die erforderliche Infrastruktur zu gestalten.

Grundlage dieser Arbeiten bei protego.net waren der Planungsauftrag der Selbstverwaltung [Selb04] sowie die Rahmenarchitektur und die Solution Outline. Die Arbeiten entstanden in Zusammenarbeit mit der Fraunhofer-Gesellschaft (FhG) und der privaten Krankenversicherung (PKV) sowie unter Einbindung des BMGS. Die FhG war mit ihren Instituten SIT, IAO, ISST und IBMT beteiligt.

Die Arbeiten sind außerdem eingebettet in europaweite Maßnahmen. In 2002-06 beschloss der Europäische Rat den Aktionsplan eEurope 2005 [Euro02], der auch einen Schwerpunkt „eHealth“ enthält. Die Europäische Kommission fördert die Einführung einer Europäischen Krankenversicherungskarte und unterstützt die Standardisierung einer elektronischen Gesundheitsdatenarchitektur.

Der vorliegende Beitrag skizziert die von protego.net erarbeitete technische Systemarchitektur, ausgehend von den gesetzlichen Anforderungen, den Anforderungen aus den Geschäftsfällen und den IT-Sicherheitsanforderungen. Der Beitrag gibt einen Überblick über die Anwendungsdienste, die Infrastrukturdienste, den Konnektor zur Anbindung von Primärsystemen der Leistungserbringer und die grundlegenden Netzdienste.

3 Die technische Systemarchitektur

3.1 Die Anforderungen

Die von protego.net entwickelte Lösungsarchitektur genügt den Anforderungen des Gesetzgebers, den Anforderungen aus den Geschäftsfällen und den Anforderungen hinsichtlich der IT-Sicherheit [Proj04]. Die gesetzlichen Vorgaben umfassen neben dem oben zitierten GMG bzw. SGB V das Signaturgesetz (SigG) bzw. die Signaturverordnung (SigV) und das Bundesdatenschutzgesetz (BDSG). § 291a SBG V legt die Anwendungen fest, trifft aber keine Festlegung darüber, ob die Daten auf der Karte oder auf Servern gespeichert werden sollen. Speicherungs- und Transportverfahren werden ebenfalls nicht spezifiziert. Die medizinischen und administrativen Zugriffsrechte auf die Daten sind im GMG nur pauschal und abstrakt beschrieben. Der Gesetzgeber legt die Entscheidungsbefugnis in die Hand der Akteure der In-

frastruktur. Diese entscheiden gemäß den medizinischen bzw. praktikablen Abläufen. § 291 Abs. 2a SGB V schreibt Authentifizierung, Verschlüsselung und elektronische Signatur vor. Das SigG legt die möglichen Ausprägungen von Signaturen fest. Dem GMG ist zu entnehmen, dass die eGK für die Pflichtanwendungen keine „qualifizierte Signatur" gemäß SigG benötigt, also auch eine lediglich „fortgeschrittene Signatur" in Frage kommt. Abs. 5 Satz 3 legt fest, dass auf die Daten mittels der eGK nur in Verbindung mit einem elektronischen Heilberufeausweis (HBA) zugegriffen werden darf. Für den HBA ist eine qualifizierte Signatur verbindlich. Gemäß BDSG macht die Verarbeitung personenbezogener (also auch medizinischer) Daten eine gesetzliche Legitimation oder das Einverständnis des Betroffenen notwendig. In Bezug auf die Telematikinfrastruktur sind Anforderungen bzgl. des informationellen Selbstbestimmungsrechts, der Datenvermeidung bzw. -sparsamkeit, der Einwilligung und der Information des Versicherten zu beachten.

Die Anforderungen aus den Geschäftsfällen ergeben sich durch die beteiligten Akteure, die (veränderten) Geschäftsprozesse und die relevanten Anwendungen. Bei den Akteuren handelt es sich um Krankenversicherungen, Versicherte, Arzt- und Zahnarztpraxen, kassenärztliche Vereinigungen, Psychotherapeuten, stationäre Einrichtungen, sonstige Leistungserbringer (z. B. Heilmittelerbringer und -lieferanten) sowie Apotheken. Bei den Anwendungen sind insb. die Arzneimitteldokumentation, das eRezept, das Verordnungsmanagement, das Notfalldatenmanagement, das Versichertenstammdatenmanagement sowie geplante bzw. zukünftige Anwendungen (z. B. „ePatientenakte", „eArztbrief", „eEinweisung") zu berücksichtigen.

Die Anforderungen hinsichtlich der IT-Sicherheit leiten sich aus den Anforderungen an die Systemarchitektur (*Public Key Infrastructure* PKI, Authentisierungsverfahren, Zugriffsberechtigungen), den Anforderungen an die zuvor beschriebenen Anwendungen und grundsätzlichen Sicherheitsanforderungen ab. Grundsätzlich sind Rechtssicherheit, Revisionsfähigkeit, Nichtabstreitbarkeit des Datenempfangs, Zurechenbarkeit (Authentizität), Verfügbarkeit, Datenintegrität, Vertraulichkeit und die Steuerung abgestufter Nutzungsrechte zu garantieren. Für jedes einzelne System werden individuelle Sicherheitsziele durch eine Bedrohungs- und Risikoanalyse definiert und mittels technischer und organisatorischer Maßnahmen operationalisiert.

3.2 Die Gesamtarchitektur

Bild 1 liefert eine Gesamtsicht der Architektur mit den beteiligten Akteuren (an den Rändern des Bildes) und den Lösungskomponenten (im Inneren des Bildes).

Dem Patienten wird durch seine eGK die Nutzung der Telematikinfrastruktur ermöglicht. Er bzw. sie handelt über einen Patientenkiosk bzw. einen mit einem Kartenlesegerät ausgestatteten PC oder zusammen mit dem Leistungserbringer (in Verbindung mit dem jeweiligen HBA) über dessen „Konnektor". Der Konnektor stellt die Anbindung der Primärsysteme (z. B. einer Praxisverwaltungssoftware, PVS oder eines Krankenhausinformationssystems, KIS) an die Telematikinfrastruktur sicher. Die Krankenkassen fungieren als Herausgeber der eGK und kontrollieren ihren jeweiligen Versichertenstammdatendienst. Die Arztpraxen prüfen die Gültigkeit der eGK und die Anspruchsberechtigung des Versicherten. Sie stellen Verordnungen in das System ein. Der Heilberufeausweis des einzelnen Arztes ermöglicht eine genaue Zuordnung des Vorganges auch in Krankenhäusern und Gemeinschaftspraxen. Die Kassenärztlichen Vereinigungen als Dienstleister für die niedergelassenen Vertragsärzte stellen zentrale Sicherheitsdienste (https, Firewall, Viruswall), generische Daten- (Protokoll SOAP) bzw. Datei- (Format XML) Austauschdienste und eine Routingfunktionalität über den so genannten KV-Konzentrator bereit. Apotheken und Versandapotheken dispensieren das Rezept mit Zustimmung des Versicherten, d. h. über dessen eGK. Die Zustimmung erfolgt im Falle der Apotheke vor Ort, im Falle der Versandapotheke über ein WWW-Frontend bzw. den Patientenkiosk oder Patienten-PC. Durch die Dispensierung wird das Rezept in der Telematikinfrastruktur (innerer Bereich des Bildes) als dispensiert gekennzeichnet und dann über die konventionelle Datenfernübertragung (DFÜ) abgerechnet bzw. zur statistischen Auswertung weitergeleitet. Trustcenter verwalten die Zertifikate und stellen ihre Dienste über eine infrastrukturinterne PKI zur Verfügung.

Der jeweils aktuelle und signierte Stammdatensatz der Versicherten wird von den Krankenkassen über den Versichertenstammdatendienst (VSDD) bereitgestellt. Der Dienst ermöglicht eine Prüfung der Versichertendaten auf der eGK. Bei entsprechender Authentisierung kann eine gesicherte Aktualisierung der Daten auf der Karte erfolgen. Der Verordnungsdatendienst (VODD) verwaltet verschiedene Arten von Verordnungen (z. B. bzgl. Arzneien, Sehhilfen, Hörhilfen, Heilmitteln, Krankenbeförderungen) und erlaubt beliebig viele Speicherorte. Der Speicherort kann vom Versicherten, vom Verordnenden oder von der Krankenkasse während der Erstellung des Dokumentes festgelegt werden. Die Einstellung des Dokumentes erfolgt über den zentralen VODD. Die zweistufige Architektur ermöglicht einen besonderen Datenschutz für den Patienten. Versandapotheken werden ebenso unterstützt wie ein papierbasierter Fallback-Mechanismus. Der ebenfalls zweistufige Lokalisierungsdienst bestimmt aus der Krankenversichertennummer die Server für die Versichertenstammdaten und das Verordnungsdatenmanagement. Der hierarchische Objektidentifikatordienst (OID-Dienst) versorgt die gesamte Telematikinfrastruktur mit eindeutigen Identifizierern. Der Rollen- und Berechtigungsdienst stellt passende Zugriffsrechte für die beteiligten Akteure auf Daten und Dienste sicher. Die Vermittlung zwischen der Telematikinfrastruktur, den Primärsystemen und den Mikroprozessorkarten (über das jeweilige Kartenterminal) übernimmt der Konnektor. Er enthält also keine Anwendungslogik, sondern besteht lediglich aus Hardwarekomponenten und zertifizierten Softwaremodulen.

3.3 Die Dienste

Zu unterscheiden sind Anwendungsdienste (z. B. VODD), Infrastrukturdienste (z. B. Sicherheitsdienste), Netzdienste (auf TCP/IP-Basis) und der Konnektor. Aufgrund ihrer spezifischen Bedeutung für die Lösungsarchitektur werden im Folgenden der Konnektor, VSDD und VODD näher betrachtet. Die Bedeutung des VSDD und des VODD resultiert aus dem Umstand, dass das Management von Verordnungen und Versichertenstammdaten die prioritäre Anwendung der eGK ist. Da der Konnektor notwendig ist, um die Primärsysteme an die Telematikinfrastruktur anzubinden, besitzt er ebenfalls eine herausragende Funktion. Bild 2 fasst nochmals die oben beschriebene Position des Konnektors in der Architektur zusammen.

Der Konnektor besitzt Schnittstellen zu den Kartenterminals, zu den Primärsystemen und zum Telematiknetz. Grundsätzlich ist seine Operationalisierung als zusätzliche Hardware oder als ein weiteres Softwaremodul des Primärsystems möglich. In jedem Fall ist das in Bild 2 dargestellte „Toolkit" als Teil des Konnektors direkt mit dem Primärsystem verbunden. Die Visualisierung erfolgt somit mittels des

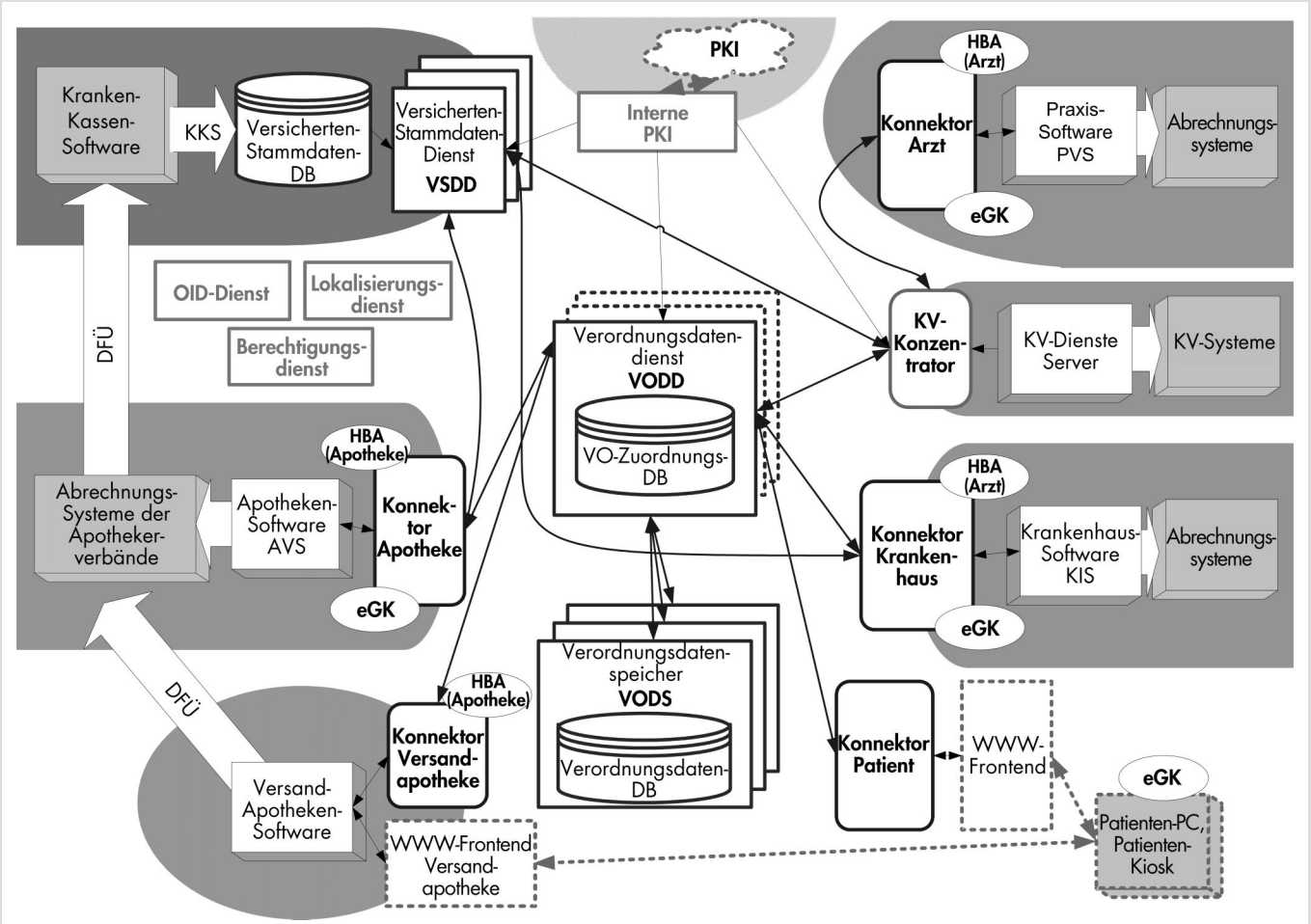

Bild 1 Überblick über die technische Systemarchitektur [Proj04]

Toolkit durch das Primärsystem. Die Primärsysteme rufen über den „Command Manager" Dienste auf, so dass z. B. Anfragen in das Telematiknetz weitergeleitet, Antworten empfangen, Daten auf die Karten geschrieben oder von dort gelesen werden können. Hierzu werden der VODD und der VSDD direkt aufgerufen. Dienste wie der Signatur-, der Vertraulichkeits- oder der Lokalisierungsdienst hingegen sind zwecks Daten-Caching sowohl im Telematiknetz als auch teilweise in den Konnektoren vorhanden. Der Authentifizierungsdienst erlaubt eine Authentifizierung der betreffenden Organisation innerhalb des Netzes. Im Sinne des Pull-Prinzips empfängt der Konnektor keine Daten aus dem Telematiknetz, sofern er sie nicht zuvor angefordert hat. Jede Kommunikation zwischen Primärsystem und Konnektor wird wiederum ausschließlich vom Primärsystem getriggert.

In Arztpraxen, Krankenhäusern und Apotheken stellt der Konnektor im Rahmen der Anmeldung des Versicherten die Kontrolle und ggf. die Aktualisierung der Versichertenstammdaten und des Zuzahlungsstatus in den Primärsystemen und auf der eGK sicher. Er garantiert die Signierung der Verordnungen, deren Transport vom ärztlichen Primärsystem auf den Verordnungsdatenserver und von dort in das System der Apotheke sowie die dortige Dispensierungsbestätigung per Signatur. Der Versicherte besitzt die Möglichkeit, einzelne Verordnungen für verschiedene einlösende Stellen sichtbar oder unsichtbar zu machen. Der Konnektor wandelt die Wünsche des Betroffenen in entsprechende Dienstaufrufe um.

Der in Bild 3 dargestellte Versichertenstammdatendienst ermöglicht den in § 291a GMG geforderten Abgleich von Kartendaten in Praxen, Krankenhäusern und Apotheken gegen den Datenbestand der Krankenkassen sowie die Aktualisierung dieser Daten auf der eGK. Es handelt sich dabei um alle Daten, die zur Dokumentation des jeweiligen Versicherungsverhältnisses und damit der Ansprüche des Versicherten gegenüber dem Kostenträger nötig sind. Konkret sind dies die persönlichen Daten des Versicherten, die Charakteristika des Vertragsverhältnisses und die Angabe, ob eine Zuzahlungsbefreiung gegeben ist. Die Versichertenstammdaten werden per VSDD von den Kassen verschlüsselt auf den Versichertenstammdatenservern gespeichert und dort in der jeweiligen Datenbankstruktur vom VSDD verwaltet. Schreibrecht besitzen lediglich die Kostenträger. Die Signatur der Anfrage des Konnektors eines Leistungserbringers wird durch den VSDD mittels PKI geprüft. Der Dienst prüft das Vorhandensein bzw. die Übereinstimmung von Krankenversicher-

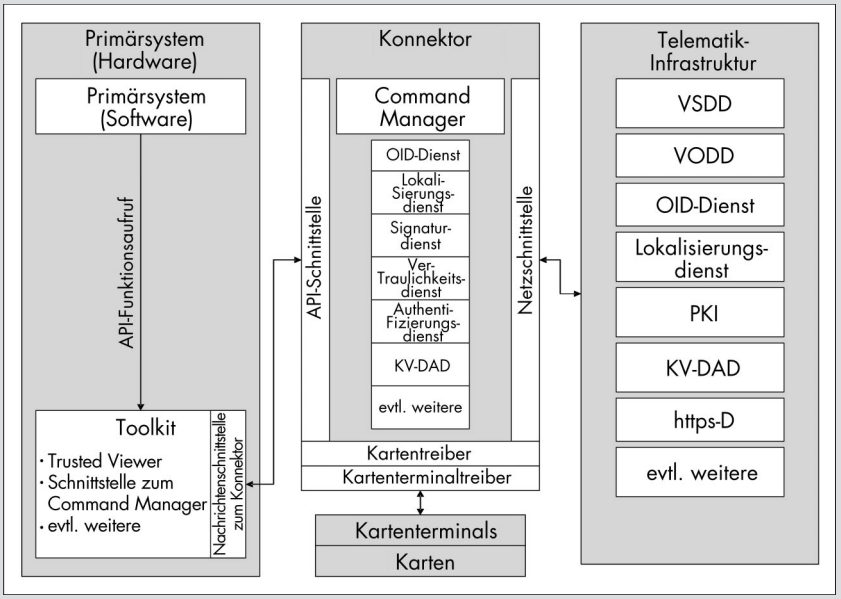

Bild 2 Komponenten des Konnektors und seine Rolle innerhalb der Lösungsarchitektur [Proj04]

tennummer (KVNr) und das Aktualisierungsdatum oder die Versionsnummer. Die Beantwortung erfolgt bei positivem Ergebnis der Prüfung der Konnektorsignatur und die Daten werden wiederum signiert und verschlüsselt zum Leistungserbringer übermittelt. Bei korrekter KVNr, aber veralterter Versionsnummer, erfolgt die Aktualisierung der Daten über den Konnektor des anfragenden Leistungserbringers. Alternativ ist eine Aktualisierung über den Patienten-Konnektor, z. B. am Patientenkiosk, vorgesehen. Da einzelne Kostenträger eigene Versichertenstammdatendienste betreiben werden, ermöglicht der zentrale Lokalisierungsdienst den Konnektoren das Auffinden des zuständigen VSDD. Die Lokalisierung erfolgt über das Institutionskennzeichen (IK) der Krankenversicherungen.

Die oben erläuterten Datensicherheits- und Datenschutzanforderungen besitzen für den Verordnungsdatendienst besonders große Relevanz. Daher wird der Dienst, wie in Bild 4 dargestellt, in zwei Ebenen realisiert. Ein Rückschluss von der Verordnung auf den Versicherten ist somit erheb-

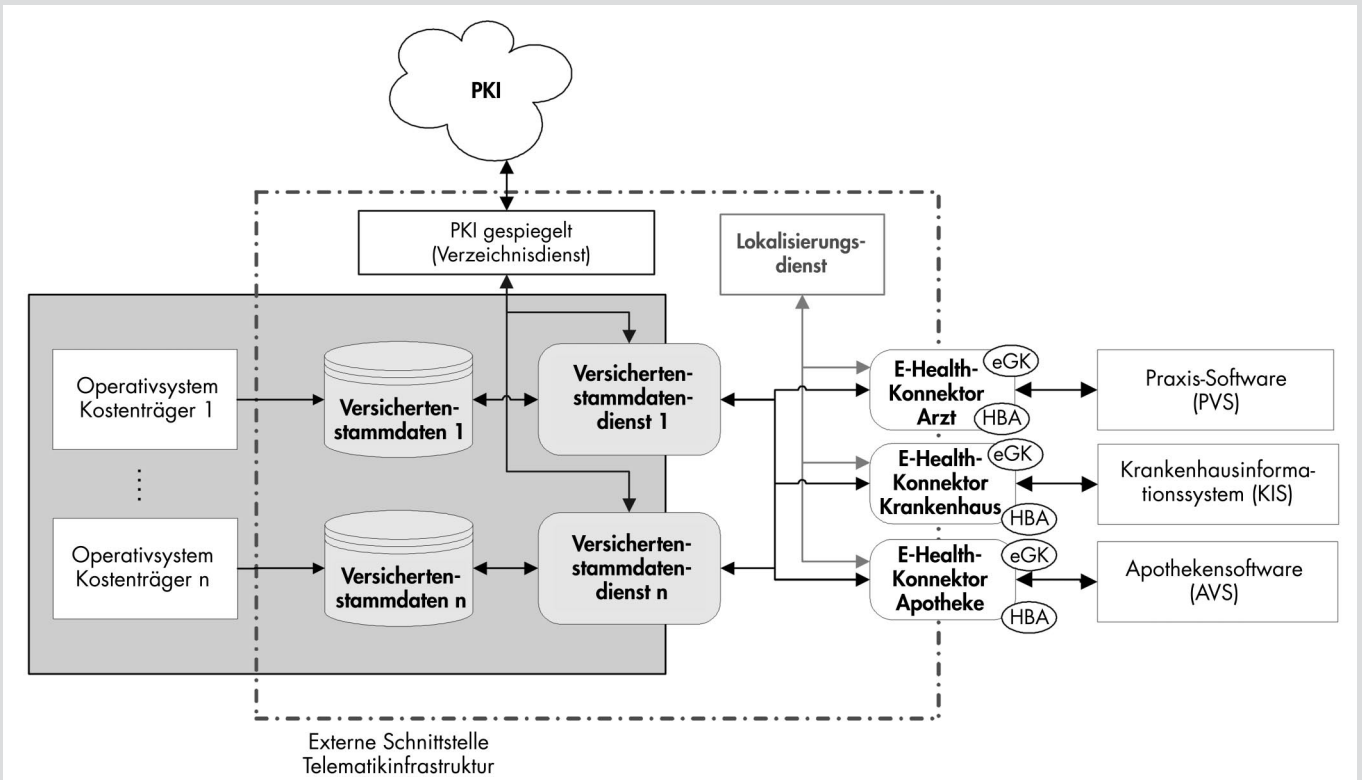

Bild 3 Einbettung des Versichertenstammdatendienstes in die Lösungsarchitektur [Proj04]

lich erschwert. Der Dienst gibt dem Versicherten weit reichende Vollmachten über die ihn betreffenden Dokumente, z. B. zur Unterdrückung der Anzeige einer Verordnung. Verarbeitet werden lediglich verschlüsselte Verordnungen. Sie werden mittels OIDs identifiziert. Vorstellbar ist, dass der Speicherort über die Zugehörigkeit zu einer bestimmten Krankenkasse, vom Patienten selbst oder durch den behandelnden Arzt festgelegt wird. Der VSDD führt mittels der PKI die Rechteprüfungen durch und ermöglicht eine Trennung des Managements der Dokumentverwaltungsdaten von der Speicherung des Dokuments. In seiner Zuordnungsdatenbank werden insbesondere der CardID, der OID der einzelnen Verordnung, der Identifizierer des als Speicherort für die Verordnung dienenden Servers, der Verordnungstyp, der momentane Status der Verordnung (sichtbar oder versteckt) und ein Verfallsdatum für den Zeitpunkt, an dem die Verordnung ihre Gültigkeit verliert, verwaltet. Der Verordnungsdatenspeicher kann durch mehrere Betreiber auf unterschiedlichen Servern realisiert werden. Diese Server sind ausfallsicher anzulegen. Sie kommunizieren über zweiseitig authentifizierte SSL-Kanäle. In ihrer Datenbank werden lediglich die verschlüsselte Verordnung selbst und der OID der Verordnung verwaltet.

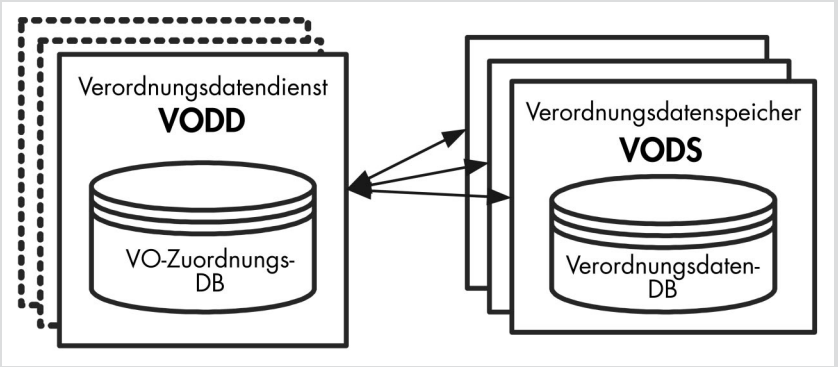

Bild 4 Verhältnis von VODD und VODS [Proj04]

4 Bewertung der Ergebnisse

Die erläuterte Systemarchitektur ist die Grundlage der noch zu beschließenden, endgültigen Lösungsarchitektur. Sie stellt wiederum eine Fortentwicklung der in Abschnitt 2 erläuterten Vorarbeiten von BMGS, Industrie und Selbstverwaltung dar. Der Umstand, dass das BMGS die Möglichkeit einer umfassenden „Ersatzvornahme“ [vgl. Abschnitt 2] Ende 2004 nicht wahrgenommen hat, impliziert, dass die dargestellte Architektur aus Sicht des Bundesministeriums grundsätzlich geeignet ist.

Die prinzipielle Eignung wird ebenfalls dadurch verdeutlicht, dass die Architektur Ausgangspunkt eines vom BMGS und der Selbstverwaltung gemeinsam getragenen Forschungs- und Entwicklungsauftrages an die Fraunhofer-Gesellschaft (2004-12 bis 2005-03) war [Frau04]. Die Ergebnisse dieser Spezifikationsarbeiten werden wiederum Ausgangspunkt für die 2005-01 gegründete Betriebsorganisation gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte) sein [Ärzt05].

Die vorgestellte Systemarchitektur ist an den gesetzlichen Anforderungen, den Anforderungen aus den Geschäftsfällen und den IT-Sicherheitsanforderungen ausgerichtet, das verdeutlicht Abschnitt 3. Das Ziel des Projektes, eine diesen Anforderungen genügende Architektur mit möglichst existierenden bzw. bereits vorhandenen Techniken zu entwerfen, kann als gelungen gezeichnet werden. Darüber hinaus folgt aus den Spezifikationen der einzelnen Dienste, dass der Aufbau eines separaten physischen Netzes für die Infrastruktur nicht notwendig sein wird. Die Sicherung der Dienste durch zertifikatbasierte kryptographische Verfahren sowie die Kapselung der Zugänge zum Netz erlauben den Betrieb eines hinreichend sicheren logischen Netzes.

Die angestrebte Lösungsarchitektur nähert sich den Anforderungen der Akteure des Gesundheitswesens, indem die mit den Anwendungen verbundenen Prozesse die Vorteile der neuen Technologie nutzen und gleichzeitig die heute üblichen Abläufe so wenig wie möglich verändern. Dies sei exemplarisch für die Patientensicht erläutert: Das Auslesen der Versichertenstammdaten kann ohne Eingabe einer PIN erfolgen; parallel zum eRezept ist die Ausgabe eines Papierbelegs an den Patienten vorgesehen („Patientenquittung“); der Versicherte kann einzelne Rezepte verbergen bzw. wieder sichtbar machen; seine Notfalldaten werden durch eine Speicherung auf der eGK jederzeit mobil verfügbar. Der Patient bleibt „Herr seiner Daten“.

Schließlich birgt die dargestellte Architektur ein hohes gesamtwirtschaftliches Innovationspotenzial. Neben den angestrebten Verbesserungen bei Transparenz, Qualität und Kosten im Gesundheitswesen

Abstract

Solution Architecture for the Adoption of the Patient Data Card and its Applications

In Germany it is intended that each insurant in the compulsory health insurance will get a Patient Data Card by 2006-01-01. This project report characterizes the present state of the system architecture for the telematics infrastructure elaborated by the self-administration of German health care. The introduction of the Patient Data Card aims at increasing the quality in medical care as well as improvement of cost effectiveness and transparency of health care output. The great deal of actors and the high amount of requirements concerning law including data privacy, and engineering including security and reliability cause a highly complex project. The overall system architecture is based on legacy systems which are connected to the telematics infrastructure and its new services by special modules.

Keywords: Patient Data Card (PDC), Health Professional Card (HPC), Electronic Prescription, Health Care, Telematics Infrastructure, Solution Architecture

kommt es erstmals in Deutschland zu einer massiven Anwendung von Smart Cards, verbunden mit einer entsprechend ausgebauten Public Key Infrastructure. Positive Wirkungen in andere Sektoren der deutschen Volkswirtschaft („Job Card“ u. Ä.) sind zu vermuten.

5 Ausblick

Die vorgestellte Architektur bildet den Ausgangspunkt für die weitere Detaillierung der interoperablen Lösungsarchitektur sowie zur Festlegung der Betreibermodelle, Entwicklung der zugehörigen Produkte und Dienstleistungen, zu den Tests im Labor und in den Testregionen und zum Roll-out der elektronischen Gesundheitskarte, des elektronischen Heilberufeausweises und der notwendigen Telematikinfrastruktur. Diese Arbeiten werden von BMGS und Selbstverwaltung gemeinsam getragen. Das BMGS, die Selbstverwaltung im deutschen Gesundheitswesen und die Fraunhofer-Gesellschaft haben dazu die nächsten Schritte vereinbart. Industrie, Patientenvertreter, Datenschutzbeauftragte, das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie die Wissenschaft werden an den Arbeiten intensiv beteiligt, um das „derzeit ehrgeizigste und größte IT-Projekt der Welt“ [Borc04] zu einem Erfolg zu führen.

Literatur

[Ärzt05] Ärzte Zeitung Newsletter: Neue Betriebsorganisation soll Start der Gesundheitskarte beschleunigen. http://www.aerztezeitung.de/docs/2005/01/12, 2005, Abruf am 2005-01-12.

[Borc04] *Borchers, Detlef:* Gesundheitskarte. Kampf dem Chipkartenbetrug. http://www.heise.de/newsticker/meldung/48927, 2004-07-07, Abruf am 2004-11-03.

[Bund02] Bundesministerium für Gesundheit und soziale Sicherung (BMGS): Statistisches Taschenbuch Gesundheit 2002. Bonn 2002.

[Bund03] Bundesrepublik Deutschland: Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG) vom 2003-11-14. Bundesgesetzblatt Nr. 55, Bonn 2003-11-19, S. 2190–2258.

[Bund04a] Bundesministerium für Gesundheit und soziale Sicherung (BMGS); Projektgruppe bIT4health: Erarbeitung einer Strategie zur Einführung der elektronischen Gesundheitskarte. Rahmenarchitektur für die Telematikinfrastruktur des Gesundheitswesens. http://www.dimdi.de/de/ehealth/karte/bit4health/ergebnisse/rahmen_aktuell.htm, 2004, Abruf am 2004-11-03.

[Bund04b] Bundesministerium für Gesundheit und soziale Sicherung (BMGS); Projektgruppe bIT4health: Solution Outline. Skizzierung der Lösungsarchitektur und Planung der Umsetzung. http://www.dimdi.de/de/ehealth/karte/bit4health/b4h_solutionoutline.pdf, 2004, Abruf am 2004-11-03.

[Deut04] Deutsches Institut für Medizinische Dokumentation und Information (DIMDI): Gesundheitskarte – bIT4health. http://www.dimdi.de/de/ehealth/karte/index.htm, 2004, Abruf am 2004-10-26.

[Euro02] Europäische Kommission: eEurope 2005. An Information Society for All. http://europa.eu.int/information_society/eeurope/2005/index_en.htm, 2002, Abruf am 2005-01-19.

[Frau04] Fraunhofer-Gesellschaft: Spezifikation einer Architektur zur Umsetzung der Anwendungen der Elektronischen Gesundheitskarte. Antrag für ein Forschungs- und Entwicklungsprojekt. München 2004.

[Proj04] Projekt für Telematik der Gesundheitsorganisationen (protego.net): Einführung der Telematik Infrastruktur. Überblick der Lösungsarchitektur. Bergisch Gladbach 2004.

[Rola98] Roland Berger & Partner GmbH: Telematik im Gesundheitswesen. Perspektiven der Telemedizin in Deutschland. Im Auftrag des Bundesministeriums für Bildung, Wissenschaft, Forschung und Technologie und in Zusammenarbeit mit dem Bundesministerium für Gesundheit. http://www.dimdi.de/de/ehealth/literatur/roland_berger_studie.zip, 1998, Abruf am 2004-01-13.

[Selb04] Selbstverwaltung im deutschen Gesundheitswesen (SV): Planungsauftrag für die flächendeckende Implementierung eines elektronischen Rezepts (eRezept) und eines elektronischen Arztbriefs (eArztbrief) einschließlich der Planung von Aufbau und Betrieb der notwendigen organisatorisch-technischen Infrastruktur. http://www.pkv.de/telematik/, 2004, Abruf am 2004-10-25.

Akronyme

AVS	Apothekenverwaltungssoftware
BDSG	Bundesdatenschutzgesetz
bIT4health	better IT for health
BMGS	Bundesministerium für Gesundheit und soziale Sicherung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CardID	Identifier der Gesundheitskarte
DB	Datenbank
DFÜ	Datenfernübertragung
DIMDI	Deutsches Institut für Medizinische Dokumentation und Information
eGK	Elektronische Gesundheitskarte
FhG	Fraunhofer-Gesellschaft
gematik	Gesellschaft für Telematikanwendungen der Gesundheitskarte
GKV	Gesetzliche Krankenversicherung
GMG	GKV-Modernisierungsgesetz
HBA	(elektronischer) Heilberufeausweis
HPC	Health Professional Card
https-D	https-Dienst
IAO	Institut für Arbeitswirtschaft und Organisation
IBMT	Institut für Biomedizinische Technik
IK	Institutionskennzeichen der Krankenversicherungen
ISST	Institut für Software- und Systemtechnik
IT	Informationstechnologie
KIS	Krankenhausinformationssystem
KV	Kassenärztliche Vereinigung
KV-DAD	KV-Datenaustauschdienst
KVK	Krankenversichertenkarte
KVNr	Krankenversichertennummer
OID	Object Identifier
PC	Personal Computer
PDC	Patient Data Card
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKV	Private Krankenversicherung
protego.net	Projekt für Telematik der Gesundheitsorganisationen
PVS	Praxisverwaltungssystem
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SigV	Signaturverordnung
SIT	Institut für Sichere Informationstechnologie
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
SV	Selbstverwaltung im deutschen Gesundheitswesen
TCP/IP	Transmission Control Protocol/Internet Protocol
VODD	Verordnungsdatendienst
VODS	Verordnungsdatenspeicher
VO-Zuordnungs-DB	Verordnungszuordnungsdatenbank
VSDD	Versichertenstammdatendienst
WWW	World Wide Web
XML	Extensible Markup Language