

Zentrale Verwaltung von Gesundheitskarten im stationären Krankenhausumfeld – Das IQ-Medi-LOG-Produkt als Alternative zu gematik-Konzepten

Die Einführung des Heilberufsausweises für medizinische Leistungserbringer stellt IT-Infrastrukturen, Aufbau- und Ablauforganisationen in Krankenhäusern vor große Herausforderungen. Der Beitrag stellt einen neuen Lösungsansatz und dessen Umsetzung in das Produkt IQ-Medi-LOG vor. Durch Einsatz einer multifunktionalen Smart Card ist eine bessere Integration des Heilberufsausweises in Krankenhausprozesse mit erhöhter Prozesseffizienz und Behandlungsqualität möglich. Die vorgeschlagene zentrale Verwaltung von Gesundheitskarten kann die Benutzerfreundlichkeit deutlich erhöhen. Durch die sichere Verwahrung von Gesundheitskarten in einem Chipkarten-Safe kann ein höheres Sicherheitsniveau erreicht werden. IQ-Medi-LOG kann als Basis für neue Mehrwertdienste wie Zeitabrechnungen oder mobile Visiten dienen.

DOI 10.1007/s11576-008-0133-y

Die Autoren

Dipl.-Inf. (Univ.) Christian Mauro

Technische Universität München
Lehrstuhl für Wirtschaftsinformatik (I 17)
Boltzmannstr. 3
85748 Garching b. München
Deutschland
mauro@in.tum.de

Univ.-Prof Dr. Jan Marco Leimeister

Universität Kassel
Fachgebiet Wirtschaftsinformatik
Nora-Platiel-Str. 4
34127 Kassel
Deutschland
leimeister@uni-kassel.de

Dipl.-Inf. (Univ.) Ali Sunyaev Dipl.-Inf. (Univ.) Dr. Helmut Krömer

Technische Universität München
Lehrstuhl für Wirtschaftsinformatik (I 17)
Boltzmannstr. 3
85748 Garching b. München
Deutschland
{sunyaev | krcmar}@in.tum.de

Eingereicht am 2007-12-27, nach zwei Überarbeitungen angenommen am 2008-08-08 durch Prof. Dr. Spann.

1 Einleitung

Das Gesetz zur Modernisierung des Deutschen Gesundheitswesens, das zum 2004-01-01 in Kraft getreten ist, sieht eine schrittweise Einführung der neuen elektronischen Gesundheitskarte (eGK) in der Bundesrepublik Deutschland vor. Die eGK wird mit ihrer Einführung die bisherige Krankenversichertenkarte ersetzen und ist im Gegensatz zur herkömmlichen Karte eine Smart Card, die einen eigenen Mikroprozessor enthält und damit sowohl wesentlich mehr Aufgaben erfüllen (z. B. mittels integrierter kryptographischer Funktionen) als auch Daten elektronisch speichern kann (gematik 2007a, S. 11). Dadurch soll sich der Versicherte eindeutig identifizieren und seinen Leistungsanspruch jederzeit nachweisen können. Neben der eGK wird der so genannte Heilberufsausweis (HBA) eingeführt, der den bisherigen Arztausweis ersetzt. Dabei handelt es sich ebenfalls um eine Smart Card, die (ggf. in Kombination mit der eGK) den Zugriff auf die Daten und Dienste der Telematik-Infrastruktur (s. Abschnitt 2.1) ermöglicht.

Aus diversen Vorarbeiten und Studien (vgl. z. B. die Übersicht in Bernat 2006) wird ersichtlich, dass die Einführung der elektronischen Gesundheitskarte insbesondere im Krankenhaus mit erheblichen Kosten verbunden sein wird. Ein möglicher Kostentreiber liegt in der Frage

nach einer sinnvollen Integration der neuen Komponenten in die vorhandene IT-Infrastruktur sowie in die administrativen und medizinischen Leistungserbringungsprozesse. Der vorliegende Artikel fokussiert auf eine Lösung zur Integration der neuen Karten in Krankenhausstrukturen und -prozesse.

Folgend werden zunächst die Anforderungen an eine solche Integrationslösung erhoben. Anschließend werden die bereits existierenden Integrationskonzepte der gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, <http://gematik.de/>) vorgestellt und bewertet. Nachdem gezeigt wurde, dass diese nur teilweise den zuvor dargestellten Anforderungen genügen, wird ein neues Lösungskonzept vorgestellt, das unter Berücksichtigung der Anforderungen entwickelt wurde und diese entsprechend erfüllt. Das Lösungskonzept ist in Form des Produkts „IQ-Medi-LOG“ der Firma COMPAREX Deutschland GmbH umgesetzt. Lösungskonzept und Produkt sollen anhand folgender Aspekte dargestellt werden:

- Eignung zur Integration von Gesundheitskarten in Krankenhausstrukturen, insb. da bisherige gematik-Konzepte die Anforderungen der Leistungserbringer nicht vollständig erfüllen.
- Betrachtung der eGK/HBA-Integration im Kontext organisatorischer Rahmenbedingungen und Adressie-

rung von Verbesserungen der Aufbau- und Ablaufstrukturen in Krankenhäusern.

- Analyse der Sicherheitsniveaus, benutzerfreundlichen Einsatzes sowie Wirtschaftlichkeit und Behandlungsqualität durch effizientere Prozesse.

Der Beitrag schließt mit einer Zusammenfassung der wichtigsten Ergebnisse sowie einem Ausblick auf zukünftige Entwicklungen.

2 Anforderungen an eine Integrationslösung für Gesundheitskarten

Eine Integrationslösung für HBA und eGK nebst deren neuen Funktionalitäten im Krankenhaus hat sich an Rahmenbedingungen durch die Telematik-Infrastruktur (Abschnitt 2.1), rechtlichen Anforderungen (Abschnitt 2.2) und insbesondere auch an Anforderungen aus der Praxis (d. h. der Leistungserbringer, Abschnitt 2.3) zu orientieren.

2.1 Rahmenbedingungen durch die Telematik-Infrastruktur

Die Hauptziele der Einführung der eGK sind die Kommunikationsverbesserung, die Senkung der Kosten sowie die Stärkung der Patientenrechte (Trill 2006). Zur Umsetzung dieser Ziele wird eine bundesweite IT-gestützte Infrastruktur aufgebaut. Entwickelt und betrieben wird diese Telematik-Infrastruktur von der gematik, die 2005 von der Selbstverwaltung gegründet wurde (Hornung et al. 2005). Eine ausführliche Darstellung der Telematik-Rahmenarchitektur findet sich in Frießem et al. (2005) oder Caumanns et al. (2006). Im Folgenden werden nur die zum Verständnis des Beitrags wichtigsten Aspekte vorgestellt.

Auf Seiten der Leistungserbringer werden die sog. dezentralen Komponenten der Telematik-Infrastruktur zum Einsatz kommen. Dazu gehören verschiedene Chipkarten (eGK, HBA und Secure Module Cards (SMC)), SICCT-Kartenterminals (Secure Interoperable Chip Card Terminal) sowie der sog. Konnektor, der die dezentralen Komponenten verbindet und für den Zugang zur zentralen Telematik-Infrastruktur zuständig ist.

Für die medizinische Leistungserbringung in Krankenhäusern bedeutet dies eine erhebliche Veränderung bestehender

Prozesse (bspw. Schweiger et al. 2007). Dies soll am Beispiel der Arztbriefschreibung verdeutlicht werden. Folgende Veränderungen ergeben sich in Bezug zum ursprünglichen Prozess:

- Das Ausstellen und Zustellen eines Arztbriefes benötigte bisher kein Eingreifen des Patienten. Nach Einführung der eGK muss entweder die Gesundheitskarte des Patienten verfügbar sein oder aber ein entsprechendes elektronisches Berechtigungsticket vorliegen.
- Der Arztbrief muss für die Zustellung nicht mehr gedruckt und postalisch versandt werden. Er wird in elektronischer Form abgelegt und ist direkt für den weiterbehandelnden Arzt verfügbar (entsprechende Berechtigungen vorausgesetzt).
- Die handschriftliche Unterschrift des Arztes wird durch eine qualifizierte elektronische Signatur (BSI 2006) ersetzt.

Neben den Erleichterungen in Bezug auf Druck, Zustellung und Zugriffsmöglichkeiten des Arztbriefes werden insbesondere die Ärzte mit Mehraufwänden belastet. Reichte bislang eine handschriftliche Unterschrift aus, die unabhängig von technischen Geräten schnell und unkompliziert geleistet werden konnte, ist nun eine elektronische Signatur nötig. Der Arzt muss sich also an einem Arbeitsplatz angemeldet, seinen HBA in einem Kartenlesegerät verfügbar gemacht und sich zudem gegenüber dem HBA authentifiziert haben. Für die Auslösung der Signatur muss anschließend ein weiteres Sicherheitstoken (in der Regel eine PIN) eingesetzt werden. Die konkrete Ausprägung und Intensität der daraus entstehenden Probleme hängen vom gewählten Integrationsansatz ab und werden in Abschnitt 3.3 im Detail behandelt.

2.2 Rechtliche Anforderungen

Die rechtlichen Anforderungen ergeben sich direkt aus gesetzlichen Vorschriften bzw. bindenden Spezifikationen der gematik (hierzu auch Mauro et al. 2008). Zentrale rechtliche Anforderungen sind hiernach:

- A1. Die Spezifikationen der gematik und die gesetzlichen Bestimmungen (insb. das Signaturgesetz und die Signaturverordnung) müssen eingehalten werden.

- A2. Sicherheitstoken (Medien und PINs) sowie insbesondere der HBA sind durch geeignete Maßnahmen vor dem Zugriff Dritter zu schützen. Es muss gewährleistet sein, dass nur berechtigte Personen die Funktionalitäten der Lösung nutzen können, um die Vertraulichkeit der hochsensiblen Patientendaten zu wahren.

2.3 Anforderungen aus der Praxis

Vertreter der Bundesärztekammer, der Kassenärztlichen Bundesvereinigung, der Kassenzahnärztlichen Bundesvereinigung, der Bundeszahnärztekammer, der Deutschen Krankenhausgesellschaft und der Bundesvereinigung Deutscher Apothekerverbände haben einen Forderungskatalog „Anforderungen der Leistungserbringer an eine anwenderorientierte und sichere Telematikinfrastruktur im Gesundheitswesen“ (BÄK et al. 2006) zusammengestellt und diesen Bundesgesundheitsministerin Ulla Schmidt vorgelegt. Im Wesentlichen lassen sich die dort zusammengeführten Anforderungen in drei Kategorien einteilen und somit zu folgenden weiteren Anforderungen zusammenfassen:

- A3. Zeitaufwand: Prozessdurchlaufzeiten sollen sich nicht unangemessen erhöhen. Andernfalls hätte dies neben einer breiten Ablehnung durch Leistungserbringer insbesondere auch Auswirkungen auf die Behandlungsqualität (weniger Zeit für den Patienten) bzw. ökonomische Nachteile zur Konsequenz. Ein zentraler Punkt ist hierbei die Vermeidung von Prozessverzögerungen durch häufiges Stecken von Chipkarten und der häufigen Eingabe von PINs.
- A4. Bedienkomfort: Eine einfache und komfortable Bedienung muss ermöglicht werden, um die Akzeptanz zu erhöhen. Einfache, intuitive Bedienbarkeit als wahrnehmbare Eigenschaften der technischen Innovation ist für die erfolgreiche Adoption und Diffusion zentral. Hierfür wird von den Leistungserbringern gefordert, dass der HBA über einen Arbeitstag hinweg an einer Stelle zentral gesteckt bleiben kann und die Daten der elektronischen Gesundheitskarte bzw. Telematik-Infrastruktur von allen Arbeitsplätzen einer Institution über die Eingabe einer PIN (oder vergleichbare Verfahren) möglich ist.

Hier steht eine Anzeige.



- A5. Ausfallsicherheit: Es gilt zu vermeiden, dass die Abläufe durch einen nicht funktionsfähigen HBA erheblich gestört werden können. Ein fehlender Informationszugriff würde sich insbesondere auch negativ auf die Behandlungsqualität auswirken, da Informationen die Entscheidungsgrundlage jeder Behandlung sind.

Zusätzlich zu diesen Forderungen der Leistungserbringerverbände wurden in einer Vorstudie mit 10 Krankenhausleitern auf Basis halbstandardisierter Leitfadeninterviews zu den Anforderungen an eGK- und HBA-Lösungen sowie anschließender standardisierter Onlinebefragungen von 372 Krankenhaus-IT-Leitern (Leimeister et al. 2008) folgende weitere Praxisanforderungen ermittelt:

- A6. Das System muss sich ohne größere individuelle Anpassungen in die verschiedenen bestehenden Umgebungen der Krankenhäuser integrieren lassen. Die Studie ergab, dass bei den 372 befragten Krankenhäusern mehr als 23 (22 zzgl. Eigenentwicklungen) verschiedene Krankenhausinformationssysteme (KIS) im Einsatz sind. Eine Anpassung aller KIS an ein eGK-/HBA-System bzw. die Anpassung eines eGK-/HBA-Systems an alle KIS ist daher kaum praktikabel.
- A7. Das eGK-/HBA-System muss sich in klinikspezifische Prozesse integrieren lassen. Die Prozessintegration ist ein wesentlicher Aspekt für effektive Informationssysteme im Gesundheitswesen (Beyer et al. 2006, S. 8).
- A8. Das eGK-/HBA-System soll zusätzliche Mehrwertdienste bieten können. Dies ist zur Akzeptanzförderung ebenso wie zur Erwirtschaftung zusätzlicher Einsparungen oder zusätzlicher Erlöse zur Gegenfinanzierung der zuvor benötigten Investitionen für das System notwendig und zweckmäßig. Dazu muss das System entsprechend flexibel und erweiterbar ausgelegt sein, auch um auf sich ändernde Rahmenbedingungen reagieren zu können.

Zusammenfassend gilt es auch bei der Einführung der eGK in das Krankenhausumfeld das Ziel effektiver Gesundheitssysteme zu erreichen, nämlich Arzt und Schwester in ihrer Arbeit optimal zu unterstützen und nicht neue, den Arbeitsprozess behindernde Tätigkeiten einzuführen (Haas 2005, S. 5).

3 Existierende Ansätze zur Verwaltung von Gesundheitskarten im Krankenhaus

Aus den Spezifikationen der gematik ergeben sich zwei verschiedene Ansätze für den Umgang mit Gesundheitskarten im Krankenhaus. Der eine basiert auf einer dezentralen, der andere auf einer zentralen Haltung der Karten. Der zentrale Ansatz ist dabei aus dem so genannten VerSA-Konzept entstanden. Beide Ansätze werden im Folgenden vorgestellt und bzgl. der zuvor aufgestellten Anforderungen bewertet.

3.1 Dezentraler Ansatz

Der dezentrale Ansatz ergibt sich implizit aus den von der gematik veröffentlichten Spezifikationen (insbesondere gematik 2007b und gematik 2007c). Er ist graphisch in **Bild 1** dargestellt.

An jedem Arbeitsplatz befindet sich ein von der gematik zertifiziertes SICCT-Kartenterminal. An Arbeitsplätzen, an denen potentiell eGK und HBA gleichzeitig gelesen werden müssen (z. B. in den Behandlungszimmern der Ambulanzen), ist ein Kartenterminal mit 2 Leseslots nötig. Die Kartenterminals sind direkt an das LAN angeschlossen (netzwerkfähige Kartenterminals). Die Möglichkeit eines „virtuellen Kartenterminals“ (gematik 2007d, S. 11) ist in **Bild 1** nicht dargestellt. Dabei wird das Terminal direkt an den Arbeitsplatzrechner angeschlossen und die SICCT-Schnittstelle über eine auf dem Rechner installierte Software an das LAN exportiert. Eine Anfrage bei den drei führenden Herstellern von Kartenterminals ergab aber, dass derzeit ausschließlich geplant ist, die SICCT-Schnittstelle direkt am LAN bereit zu stellen. Relevant ist dies in Hinblick auf anfallende Netzwerkinfrastrukturkosten, da für jedes SICCT-Kartenterminal ein Netzwerkport geschaffen werden muss.

Der Zugriff auf Kartenterminals bzw. die darin enthaltenen Karten erfolgt ausschließlich über den Konnektor. Dieser stellt auch die Verbindung zur zentralen Telematik-Infrastruktur her. Bei diesem Ansatz werden die Chipkarten direkt am Arbeitsplatz in das SICCT-Kartenterminal gesteckt. Bei einem Arbeitsplatzwechsel müssen die Chipkarten entsprechend mitgeführt werden.

3.2 Zentraler Ansatz / VerSA-Konzept

Das VerSA-Konzept (Verteilte Signatur Arbeitsplätze) wurde von der Bundesvereinigung Deutscher Apothekerverbände entwickelt. Es ist damit zwar aus den Bedürfnissen der Apotheken entstanden, dabei aber ausreichend allgemein gehalten, um es auch auf andere Bereiche des Gesundheitswesens übertragen zu können (bzw. allgemein auf vergleichbare Bereiche mit verteilten Signatarbeitsplätzen). Die Architektur des Ansatzes ist in **Bild 2** dargestellt.

Die Motivation für die Entwicklung dieses Ansatzes war, dass es im Gesundheitswesen (und insbesondere in Apotheken) in der Regel keine feste Zuordnung von Arbeitsplätzen zu Personen gibt (ABDA 2002, S. 2). Die Verwendung des dezentralen Ansatzes aus Abschnitt 3.1 hätte zur Folge, dass der Nutzer bei jedem Arbeitsplatzwechsel seinen HBA aus dem Lesegerät entfernen und in das Lesegerät des neuen Arbeitsplatzes stecken muss. Beim VerSA-Konzept werden daher die HBAe aller Angestellten in einem so genannten Server-Kartenterminal zentral gesteckt und von den Arbeitsplätzen entfernt bedient. Dazu wird eine sichere Verbindung (Trusted Channel) zwischen dem Kartenterminal am Arbeitsplatz und dem HBA aufgebaut. Zum Aufbau der sicheren Verbindung ist in jedem Kartenterminal eine SMC-A notwendig (ABDA 2002, S. 3 f.). Auf diese Weise können PINs sicher zum HBA übertragen werden.

Das Konzept wurde von der gematik übernommen und in die Spezifikationen als Möglichkeit zur entfernten PIN-Eingabe eingearbeitet (gematik 2007c, S. 67). Terminals sollen das Verfahren unterstützen, indem entsprechende Plug-In-Slots für SMCs angeboten werden (gematik 2007d, S. 23). Auch der Konnektor, betroffene Softwarekomponenten des Terminals sowie insbesondere die SMC sollen das Verfahren unterstützen (gematik 2007c, S. 66; TeleTrusT 2007, S. 67; Bundesärztekammer 2006, S. 7).

3.3 Bewertung der Ansätze

Der vorgestellte *dezentrale Ansatz* hat eine Reihe von Nachteilen:

- **Prozessineffizienz:** Der dezentrale Ansatz erfordert das häufige Stecken des HBA und die wiederholte Eingabe zweier verschiedener HBA PINs (für Authentifizierung und Signatur). Ein

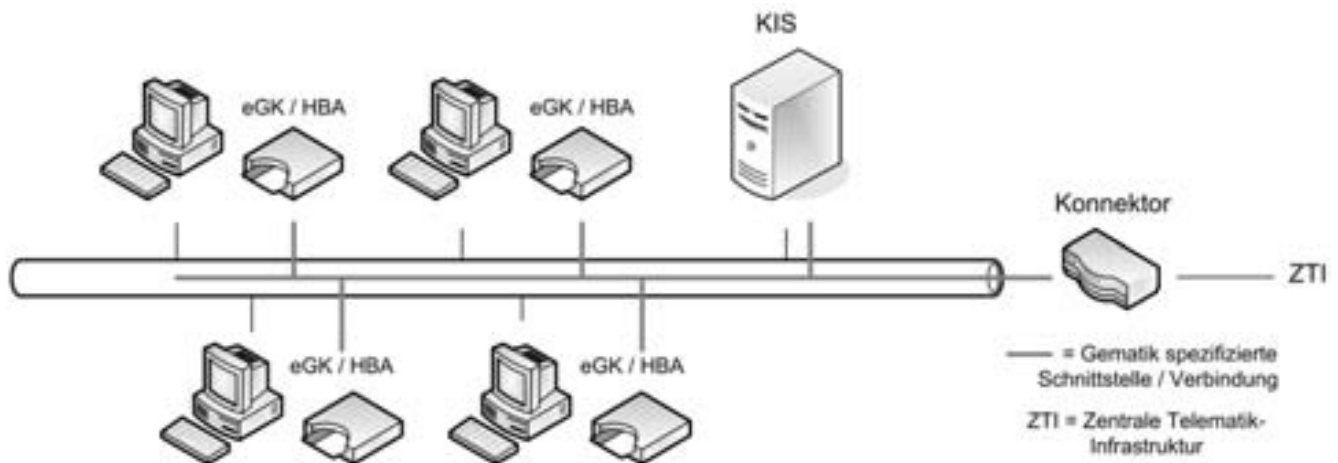


Bild 1 Dezentraler Ansatz

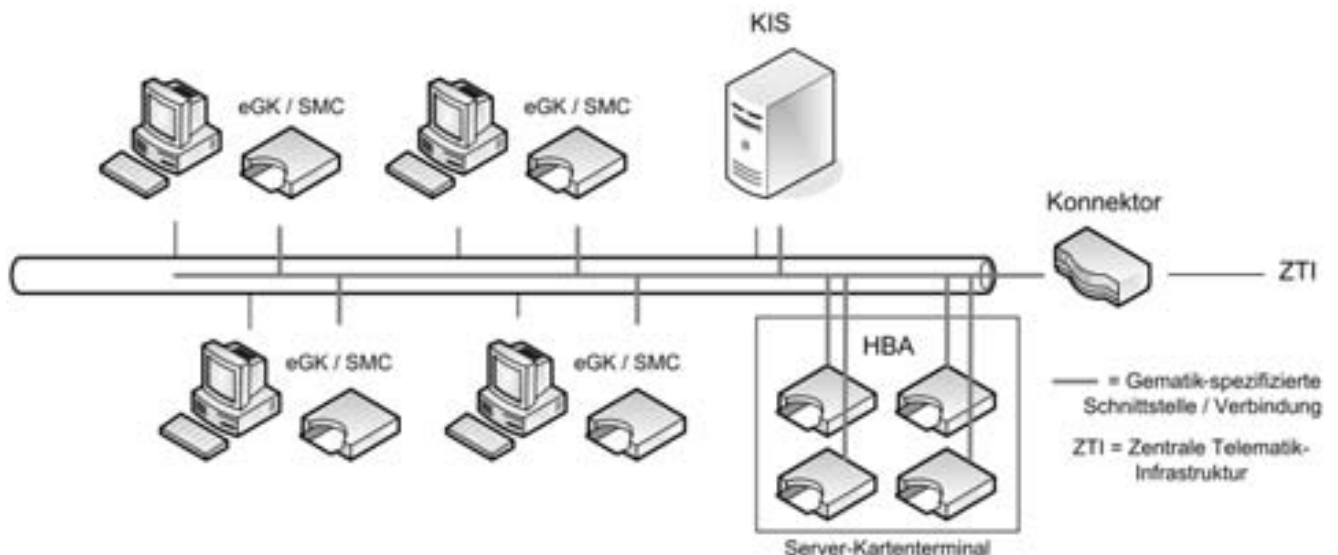


Bild 2 Zentraler Ansatz / VerSA-Konzept

noch ungünstigeres Szenario ergibt sich, wenn bereits eine weitere Chipkarte für das Single-Sign-On existiert, wie dies in einigen großen Krankenhäusern schon der Fall ist. In diesem Fall müsste der Anwender bei jedem Arbeitsplatzwechsel zwei Karten entnehmen und jeweils wieder neu stecken. Zudem wäre während des Arbeitsalltags die ständige Verwendung von drei verschiedenen PINs notwendig.

- Prozessunterstützung: Einige der klinikspezifischen Prozesse werden nur ungenügend unterstützt. Als Beispiel sei die mobile Visite (IT-gestützte Visite am Krankenhausbett) erwähnt. Für die Unterstützung dieses Anwendungsfalls wäre ein mobiles SICCT-Kartenterminal notwendig, wodurch weitere Kosten und Handlingprobleme entstehen.

- Benutzerunfreundlichkeit: Die o. g. Prozessineffizienz wirkt sich direkt auf die Benutzerfreundlichkeit aus, da der Anwender mit der Handhabung von Chipkarten und PINs belastet und damit in seinem Arbeitsfluss gestört wird.
- Wirtschaftlichkeit / Qualität: Durch die Ineffizienz der Prozesse ergeben sich direkte Nachteile auch bei der Wirtschaftlichkeit bzw. der Qualität. Je mehr Zeit der Heilberufler für die Bedienung von IT aufwenden muss, desto weniger Zeit bleibt für die Behandlung der Patienten. Bei gleichbleibender Qualität ist also ein verminderter Durchsatz anzunehmen bzw. umgekehrt bei gleichem Durchsatz eine verminderte Qualität. Daneben ist die Installation von SICCT-Terminals

für jeden Arbeitsplatz mit erheblichen Kosten verbunden (Anschaffungskosten, Netzwerkinfrastruktur und Wartungskosten). Ein weiterer Aspekt ist, dass der HBA durch das häufige Stecken einem starken Verschleiß ausgesetzt ist und daher eine erhöhte Austauschrate anzunehmen ist. Dadurch und auch durch die Gefahr, den HBA in einem Lesegerät zu vergessen, ergibt sich zudem die Notwendigkeit, einen Ersatz-HBA bereit zu halten.

- Sicherheitsaspekte: Muss der Heilberufler z. B. wegen eines Notfalls den Arbeitsplatz schnell verlassen, liegt es nicht fern, dass der HBA dabei im Kartenterminal vergessen wird. Gelangt der HBA dadurch in die Hände Dritter, sind Missbrauchsszenarien denkbar. Auch das Ausspähen der HBA-

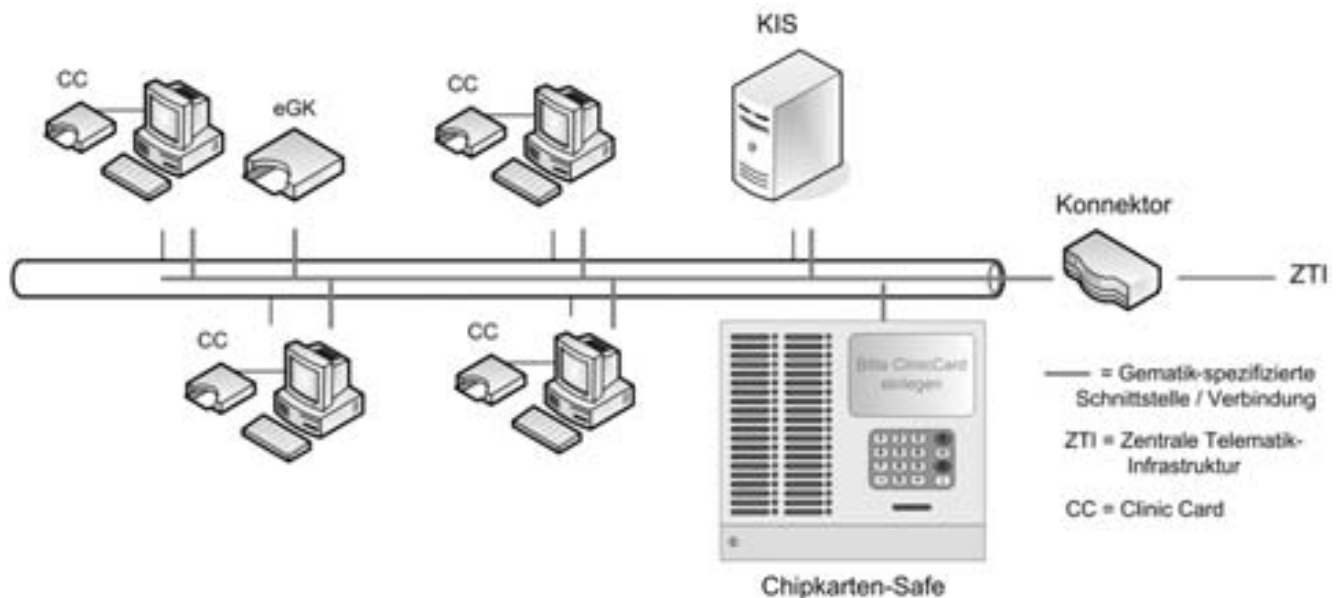


Bild 3 IQ-Medi-LOG-Konzept – Logische Architektur

PINs wird durch deren häufig wiederholte Eingabe erleichtert.

Das *VerSA-Konzept* ist vergleichsweise benutzerfreundlicher, da der HBA in einem Server-Kartenterminal verwahrt wird. Allerdings entsteht auch hier eine doppelte Anmeldeprozedur. Zum einen muss sich der Benutzer am Softwaresystem des Krankenhauses anmelden und zum anderen ist eine Authentifizierung gegenüber dem HBA nötig. Außerdem entstehen im Vergleich zum dezentralen Ansatz zusätzliche Kosten für die Anschaffung der Server-Kartenterminals und der SMCs. Davon abgesehen macht das VerSA-Konzept in seiner Dokumentation keine Aussagen über die technische Umsetzung. Die konkrete technische Ausprägung des Server-Kartenterminals bleibt unklar. Wie zuvor erwähnt müssen die Karten jedoch von einem SICCT-Kartenterminal gelesen werden, so dass es sich bei dem Server-Kartenterminal um ein Multi-Slot-SICCT-Kartenterminal handeln muss. Die Verwendung normaler SICCT-Kartenterminals wäre insofern problematisch, als dass zum einen eine Vielzahl an Terminals und zugehöriger Netzwerkports installiert werden müssten und zum anderen die sichere Verwahrung der Heilberufsausweise nicht gewährleistet wäre.

Ein genereller Nachteil beider Ansätze ist, dass sie nicht auf die Bedürfnisse von Krankenhäusern zugeschnitten sind. Die Konzepte gelten gleichermaßen für niedergelassene Ärzte, Apotheken und sonstige Einrichtungen, in denen das Lesen

von eGK und HBA notwendig ist. Aus diesem Grund werden von beiden Ansätzen neben der Einbindung der Karten keine klinikspezifischen Prozesse unterstützt. Aus dem gleichen Grund sind bei beiden Ansätzen auch keine Mehrwertdienste verfügbar.

Beide vorgestellten Ansätze erfüllen die zuvor erarbeiteten Anforderungen an eine eGK-/HBA-Lösung für Krankenhäuser nicht vollständig. Insbesondere bei der Benutzerfreundlichkeit, der schnellen Verwendbarkeit und dem Bereitstellen von krankenhausspezifischen Mehrwertdiensten sind deutliche Abstriche zu verzeichnen. Auch hinsichtlich Flexibilität und Erweiterbarkeit sind beide Ansätze stark verbesserungswürdig. Der dezentrale Ansatz zeigt zudem Schwächen in Bezug auf die Sicherheit. Das VerSA-Konzept geht mit seinem zentralen Ansatz erkennbar in eine vielversprechende Richtung. Im Folgenden wird daher ein Produkt vorgestellt, das zum einen die konkrete technische Ausprägung des Server-Kartenterminals umsetzt und zum anderen den VerSA-Ansatz zu einem ganzheitlichen Integrationskonzept erweitert und so die gestellten Anforderungen zu erfüllen versucht.

4 Der IQ-Medi-LOG-Ansatz: Architektur und Funktionalitäten

Das IQ-Medi-LOG-Lösungskonzept (in der Folge auch kurz Lösungskonzept)

basiert analog zu VerSA auf einer zentralen Haltung von Smart Cards und wird im Wesentlichen durch zwei Komponenten umgesetzt:

- Der Chipkarten-Safe (in der Folge auch kurz Safe genannt) ist eine zentrale Verwaltungseinheit für Smart Cards. In ihm werden Heilberufsausweise zentral und sicher (d. h. mit Entnahmeschutz) aufbewahrt.
- Die Clinic Card ist eine multifunktionale Smart Card. Sie soll die Funktionalitäten aller in einem Krankenhaus bereits vorhandenen Chipkarten oder berührungslosen Medien (z. B. für Kantinen, Zeiterfassung, etc.) vereinen. Zudem erfolgt mit ihr der Zugriff auf den im Safe befindlichen HBA inkl. Auslösung elektronischer Signaturen. Darüber hinaus kann sie für ein Single-Sign-On an allen klinischen Systemen verwendet werden.

Die Architektur sowie die Funktionalitäten des Systems werden in den folgenden Abschnitten vorgestellt.

4.1 Architektur

Das IQ-Medi-LOG-Konzept hat mit dem in Abschnitt 3.2 vorgestellten VerSA-Konzept einige Gemeinsamkeiten (vgl. **Bild 3**). Auch dort wurden die HBAs zentral deponiert und es erfolgte ein entfernter Zugriff von den Arbeitsplätzen aus. Es gibt jedoch fünf wesentliche Unterschiede:

- Es wird keine HBA-PIN über das Netzwerk übertragen.

- An den Arbeitsplätzen sind keine vollwertigen SICCT-Kartenterminals notwendig. Durch den Einsatz einer Proxy-Software können ausgewählte Standardlesegeräte eingesetzt werden. Eine Ausnahme bilden die Arbeitsplätze, an denen die eGK gelesen werden muss, z. B. an Aufnahme-Arbeitsplätzen. Dort müssen auch weiterhin vollwertige SICCT-Kartenterminals platziert werden.
- In den Lesegeräten am Arbeitsplatz sind keine SMCs notwendig.
- Die Lesegeräte sind immer direkt am Arbeitsplatz angeschlossen. Zusätzliche Netzwerkports sind daher nicht notwendig.
- Es wird eine multifunktionale Clinic Card eingesetzt.

Die ersten drei Punkte werden durch Nutzung von Funktionalitäten der Komfort-Signatur ermöglicht (s. Abschnitt 4.2). Die eGK wird derzeit nicht im Safe abgelegt, weil die endgültigen Abläufe und Rahmenbedingungen noch nicht klar sind. Die Lösung ist aber so flexibel angelegt, dass die eGK-Integration durch ein Software-Update ermöglicht werden kann.

Die Bedienung ist so einfach wie möglich gehalten. Nach dem Einlegen der Clinic Card wird der Benutzer aufgefordert, seinen HBA in den per LED markierten Leseslot einzuführen. Nach Abfrage der Authentifizierungs-PIN und der Signatur-PIN erhält der Benutzer seine Clinic Card zurück. Diese ist nun bereit für einen entfernten Zugriff auf den HBA. Zur Abmeldung legt der Benutzer seine Clinic Card ein und gibt die Clinic Card PIN ein. Hierauf erhält er seinen HBA zurück. Sollte sich der HBA in einem anderen Chipkarten-Safe befinden, wird dessen Lokalität angezeigt.

IQ-Medi-LOG bietet sich im Krankenhaus besonders in Kombination mit einer (ggf. existierenden) Thin-Client-Architektur (Jern 1998) an, da hier besonders einfach die Vorteile von IQ-Medi-LOG zum Tragen kommen können. Durch die so schon existierende zentrale Instanz zur Verwaltung der Benutzerzugriffe bleibt bei einer Unterbrechung am Client das angewendete Programm verfügbar und kann an jedem anderen Client im Netz fortgesetzt werden (Session-Übernahme). Diese zusätzlichen Funktionalitäten erhöhen insbesondere die Benutzerfreundlichkeit, wenngleich die Safelösung auch in anderen Architekturumgebungen eingesetzt werden kann.

4.2 Technische Realisierung

Die Details der technischen Realisierung befinden sich (bedingt durch die sich im Aufbau befindlichen gematik-Spezifikationen) noch im ständigen Wandel. Folgend werden zentrale technische Basisaspekte dargestellt.

Für die entfernte Nutzung des Heilberufsausweises werden Funktionalitäten der Komfortsignatur verwendet. Dadurch wird ermöglicht, dass die von der gematik definierten Schnittstellen genutzt werden können. Anpassungen an Konnektor oder Primärsystem sind nicht nötig. Für eine Darstellung der Kommunikationspfade sei daher auf gematik (2007c, S. 40) verwiesen.

Bei dem Chipkarten-Safe handelt es sich technisch gesehen um ein Multislot SICCT-Kartenterminal, das den Spezifikationen der gematik unterliegt bzw. entspricht. In einer IT-Landschaft eines Klinikums können mehrere Safes vorhanden sein, die auch verteilt aufgestellt werden können (z. B. an den Haupteingängen). Er ist in Varianten mit 20, 40 und 60 Slots verfügbar.

Für den Entnahmeschutz des Safes kommen so genannte Einzugleser (Rankl und Effing 1995, S. 257 f.) zum Einsatz, die (analog zu z. B. Bankautomaten) die Chipkarten vollständig aufnehmen. Die Entnahme eines Heilberufsausweises ist anschließend nur noch durch den Einsatz der zugehörigen Clinic Card möglich. Eine Ausnahme bilden die Mechanismen zur Entnahme von Karten im Falle eines Defekts (vgl. Abschnitt 4.3).

Die Clinic Card ist eine Prozessor-Chipkarte nach ISO 7816 mit kryptografischen Funktionen und Anwendungen für den entfernten HBA-Zugriff. Daneben werden MIFARE, LEGIC sowie Anwendungen für ein Single-Sign-On unterstützt. Bei der Signaturauslösung agiert die Clinic-Card-PIN als sog. Token im Sinne der BSI-Richtlinie TR-03115 (BSI 2007, S. 18 f.). Alternativ sind andere Authentifizierungsmechanismen wie z. B. RFID-Tags oder Biometrie denkbar.

4.3 Sicherheitskonzept

Für die Darstellung der technischen Sicherheit der Lösung ist eine detaillierte Beschreibung der internen Abläufe notwendig, die Gegenstand der gematik- und BSI-Zertifizierungen sind. Der folgende Abschnitt beschränkt sich daher auf

die Sicherstellung der Verfügbarkeit des Systems sowie auf allgemeine Sicherheitsaspekte. Alle Sicherheitsvorgaben finden sich im zugehörigen Common-Criteria-Dokument (Richter et al. 2007).

Nach empirischen Studien (Leimeister et al. 2008) ist die Verfügbarkeit der IT-Systeme für Krankenhaus-IT-Leiter das wichtigste Ziel bezogen auf den betriebswirtschaftlichen Beitrag der IT-Systeme. Verfügbarkeit ist auch für die Behandlungsqualität ein entscheidendes Kriterium, da medizinische Informationen die Entscheidungsgrundlage jeder Behandlung sind. Vor diesem Hintergrund sind insbesondere zentrale Konzepte kritisch zu betrachten, da der Ausfall einer Komponente weitreichende Folgen haben kann. Aus diesem Grund wurde für die Safelösung ein zweiteiliges Konzept entwickelt:

Der erste Teil des Konzepts soll die Wahrscheinlichkeit eines Ausfalls minimieren. Hierzu wird eine unterbrechungsfreie Stromversorgung innerhalb des Safes eingesetzt. Die Kartenleser wurden speziell für die Safelösung entwickelt und haben eine MTBF (Mean Time Between Failures) von 50.000 Stunden. Auch die anderen Komponenten sind entsprechend für einen 24/7-Dauerbetrieb ausgelegt. Der Kartenleser zum Auslesen der Clinic Card wird am meisten beansprucht, da dieser bei jedem Einlegen oder Entnehmen eines HBA genutzt wird. Aus diesem Grund kann bei Bedarf auf einen anderen Leser umgeschaltet werden.

Der zweite Teil des Konzepts befasst sich mit dem Ablaufplan im Falle eines Defekts. Wichtig ist hierbei, dass die in einem Safe befindlichen Heilberufsausweise schnellstmöglich wieder verfügbar gemacht werden müssen. Ist die Steuerungseinheit des Safes noch funktionsfähig, können die Kartenleser über eine Administrationsschnittstelle gesteuert werden. Andernfalls müssen die Chipkarten durch das Öffnen des Gehäuses zugänglich gemacht werden.

Von besonderer Bedeutung ist der Schutz der Heilberufsausweise vor dem Zugriff Dritter sowie die Manipulationssicherheit des Safes. Die Administrationsschnittstelle ist daher nur für autorisiertes Personal zugreifbar. Das Gehäuse ist durch ein Sicherheitsschloss geschützt und kann nur mit einem entsprechenden Schlüssel geöffnet werden. Darüber hinaus sind von außen keine Schrauben zugänglich, die das Öffnen des Gehäuses ermöglichen würden. Zur Erkennung von Mani-

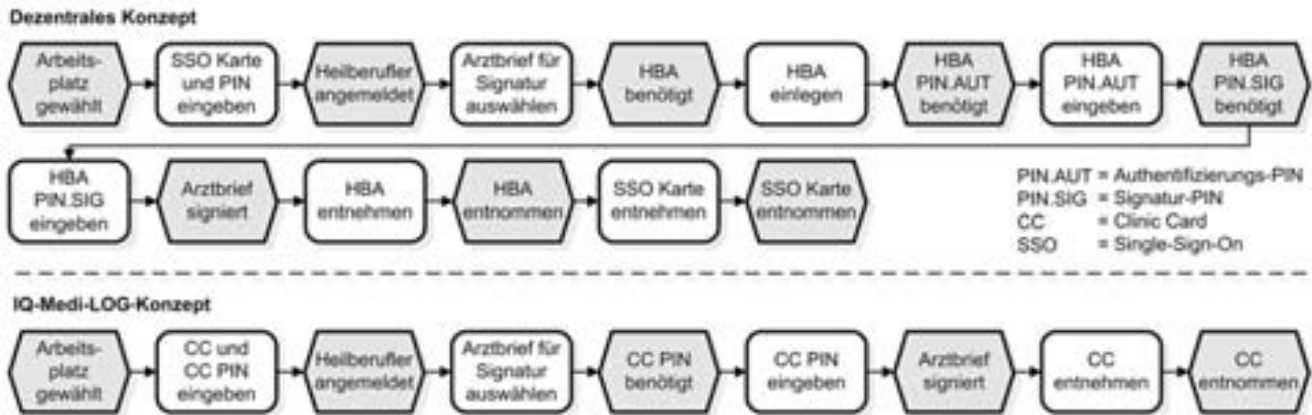


Bild 4 Prozessvergleich Arztbriefschreibung

pulationen ist das Gehäuse durch ein BSI-zertifiziertes Siegel geschützt, das sich bei Entfernung zerstört.

5 Bewertung des IQ-Medi-LOG-Lösungskonzepts

5.1 Konzeptuelle Bewertung

Anwendungen für die zentrale Aufbewahrung von Chipkarten für einen entfernten Zugriff gibt es derzeit im Zusammenhang mit Signaturservern (Hühnlein und Knosowski 2003, S. 304). Die Möglichkeiten der technischen Umsetzung finden in der Literatur wenig Beachtung, lassen sich aber anhand konkreter Produkte verschiedener Hersteller belegen. Beispielhaft erwähnt sei hier das cyberJack® Rack der Firma REINERSCT, welches pro Rack bis zu 13 Signaturkarten aufnehmen kann.

Auch der Einsatz von multifunktionalen Betriebsausweisen ist an sich nicht neu. Diese Thematik wird z. B. in Schröder (1995, S. 243 ff.) oder Arendt und Kafitz (2007) adressiert und findet sich auch in der Produktpalette einiger Hersteller wieder. Diesbezügliche Anwendungsgebiete gibt es viele. Neben dem Einsatz als Betriebsausweis seien hier beispielhaft multifunktionale Studentenausweise (Omar und Djuhari 2004) erwähnt.

Die Safelösung beinhaltet jedoch folgende wesentlichen Neuerungen:

- Verbindung von Betriebsausweis und Heilberufsausweis. Die Vorteile multifunktionaler Token sind bspw. in Arendt u. Kafitz (Arendt und Kafitz 2007) dargestellt. Durch den Heilberufsausweis würden diese Vorteile jedoch teilweise gemindert werden, da

der Arzt mit der Handhabung einer zusätzlichen Chipkarte belastet wird. Die Möglichkeit, den Betriebsausweis auch zur Steuerung eines zentral gesteckten Heilberufsausweises zu verwenden, ist neu. Dadurch ergeben sich insbesondere positive Effekte bzgl. der Benutzerfreundlichkeit und der Prozessintegration (vgl. 5.2).

- Sichere Verwahrung von Chipkarten. Bei existierenden Produkten zur zentralen Haltung von Chipkarten ist kein Entnahmeschutz umgesetzt. Diese eignen sich daher lediglich für den Betrieb in gesicherten Räumen oder gesicherten Serverschränken. Bei institutionellen Signaturkarten, die dauerhaft gesteckt bleiben und nicht manuell zugreifbar sein müssen, sind solche Lösungen ausreichend. Bei persönlichen Signaturkarten, die häufig entnommen werden müssen, ist dies jedoch nicht praktikabel. Durch die sichere Verwahrung der Karten werden völlig neue Einsatzszenarien möglich, die weit über die Domäne Gesundheitswesen hinausgehen (vgl. 5.5).
- Durch die sichere Verwahrung der Chipkarten und durch die Umsetzung des Safes als SICCT-Terminal im Sinne der gematik-Spezifikationen, ist das Produkt die aktuell einzig verfügbare Lösung zur konsequenten Anwendung des VerSA-Konzepts. Darüber hinaus werden zusätzliche Funktionalitäten angeboten, die das VerSA-Konzept zu einer ganzheitlichen Integrationslösung im Krankenhaus erweitern.

5.2 Benutzerfreundlichkeit und Prozessintegration

Bei der Entwicklung wurde besonderes Augenmerk auf die Anforderungen der

Leistungserbringer gelegt. Durch die Verwendung von nur einer Chipkarte und nur einer PIN für alle Belange, ist das System einfach und schnell zu bedienen. **Bild 4** verdeutlicht dies an einem realen Beispiel, indem der Prozess der Arztbriefschreibung des dezentralen Ansatzes dem des IQ-Medi-LOG-Ansatzes gegenübergestellt wird.

Sehr deutlich zeigen sich Mehraufwände beim dezentralen Ansatz durch die Handhabung verschiedener Karten und PINs. Eine weitere Verbesserung der Benutzerfreundlichkeit ließe sich z. B. durch den Einsatz von Biometrie erzielen.

Die Clinic Card fügt sich gut in die klinischen Prozesse ein. Deutlich wird dies auch vor dem Hintergrund serviceorientierter Architekturen. Die Telematik-Infrastruktur ist als serviceorientierte Architektur konzipiert (gematik 2007b, S. 44). Auch der Safe bietet mittels der Heilberufsausweise Signaturservices an. Aus technischer Sicht wurde dies im Bereich der elektronischen Signaturen mit Signaturservern bereits erfolgreich umgesetzt (Balfanz und Wendenburg 2003). Aus organisatorischer Sicht sind jedoch auch Vorgänge zu beachten, die der Anwender manuell durchführen muss, wie z. B. das Handling von Chipkarten, die Eingabe von PINs, das Anmelden am Arbeitsplatz, usw. Im Vergleich zu den existierenden Ansätzen wird der Anwender durch die Verwendung der Clinic Card ganzheitlich unterstützt, d. h. nicht nur beim Auslösen von Signaturen, sondern auch bei der Anmeldung am Arbeitsplatz und anderen Authentisierungsmechanismen im Krankenhaus (Kantine, Türschließsysteme, etc.). Durch die sichere Verwahrung des Heilberufsausweises wird der Anwender zudem bzgl. seiner Sorgfaltspflichten

Tab. 1 Zusammenfassung der Umsetzung der Anforderungen

| | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 |
|---------------------|----|----|----|----|----|----|----|----|
| Dezentrales Konzept | ++ | o | -- | -- | + | ++ | - | -- |
| VerSA-Konzept | ++ | ++ | o | o | + | ++ | - | -- |
| IQ-Medi-LOG | ++ | ++ | ++ | ++ | + | ++ | ++ | ++ |

++ = Voll umgesetzt, + = Überwiegend umgesetzt, o = Teils, teils umgesetzt, - = Überwiegend nicht umgesetzt, -- = Nicht umgesetzt

(im Sinne des § 6 Abs. 1 SigG) als Inhaber einer Signaturkarte entlastet.

5.3 Sicherheitsbewertung

Wie in Abschnitt 4.3 erwähnt, muss die technische Sicherheit – insbesondere die Konformität zu Signaturgesetz und Signaturverordnung – durch gematik- und BSI-Zulassungen sichergestellt werden. Bewertet werden im Folgenden die organisatorische sowie die Ausfallsicherheit. An dieser Stelle sei darauf hingewiesen, dass der HBA zur Nutzung von Funktionalitäten im Zusammenhang mit der Komfortsignatur in einem gesicherten Bereich betrieben werden muss. Diese ist in Form des Safes durch die Umsetzung des Entnahmeschutzes gegeben (BSI 2007, S. 10).

Bzgl. der organisatorischen Sicherheit ist die Gefahr des Kartenverlusts und PIN-Ausspähens zu betrachten. Die Gefahr des HBA-Verlusts ist weitgehend vernachlässigbar, da der HBA zu Beginn des Arbeitstages sicher verwahrt und damit nicht für Dritte zugreifbar ist. Auch das Ausspähen der HBA-PINs wird verhindert. Zum einen werden diese nur einmal am Tag am Safe eingegeben und zum anderen wird das Ausspähen durch die Bauweise des Safes (angelehnt an Bankautomaten) erschwert.

Die Gefahr des Verlustes der Clinic Card und auch die Gefahr des PIN-Ausspähens ist genauso hoch zu bewerten wie beim dezentralen Ansatz die Verlustgefahr des HBA bzw. der HBA-PINs. Kritisch anzumerken ist hierbei, dass bei Verlust der Clinic Card aufgrund der Multifunktionalität für kurze Zeit ein erhöhtes Missbrauchsrisiko besteht, ein generelles Problem von multifunktionalen Ausweisen. Demgegenüber stehen die Möglichkeit einer schnellen Kartensperrung, Kartenersetzung sowie der Vorteil, dass der Anwender nur auf ein einziges sicherheitskritisches Token zzgl. PIN achten muss. Ein HBA-Verlust ist zudem schwer-

wiegender zu bewerten, da hierbei institutionsübergreifende Missbrauchsszenarien denkbar sind, während die Clinic Card nur innerhalb genau eines Krankenhauses funktioniert. Zudem ist das Sperren und Ersetzen eines HBA ein komplexerer Prozess, der nicht allein innerbetrieblich geregelt werden kann.

Bzgl. der Ausfallsicherheit ist die Safelösung durch verschiedene technische Maßnahmen und Konzepte (s. Abschnitt 4.3) darauf bedacht, eine sehr hohe Verfügbarkeit zu gewährleisten bzw. im Falle eines Defekts die Verfügbarkeit schnellstmöglich wieder herzustellen. Kritisch anzumerken ist aber, dass die Wiederherstellung der Verfügbarkeit beim dezentralen Ansatz schneller möglich ist, da sich der HBA direkt im Zugriffsbereich des Arztes befindet.

5.4 Wirtschaftlichkeit / Qualität

Wirtschaftliche bzw. qualitative Vorteile ergeben sich durch verbesserte Prozesseffizienz (Krcmar 2005, S. 399) und die (kostengünstige) Unterstützung neuer Prozesse (z. B. mobile Visite). Zudem ergeben sich im Vergleich zu den gematik-Szenarien Einsparungen, da an den Arbeitsplätzen keine vollwertigen SICCT-Kartenterminals und keine zusätzlichen Netzwerkports notwendig sind. Demgegenüber stehen Anschaffungskosten für Safes und Clinic Cards. Die Marktpreise der zu den Lösungskonzepten notwendigen Hardware stehen aktuell noch nicht final fest. Es ist aber davon auszugehen, dass sich die initialen Kosten in etwa die Waage halten. Wirtschaftliche Vorteile sind daher vor allem längerfristig in Form von Prozesseffizienz und Qualität zu sehen.

5.5 Weitere Einsatzpotentiale

Der Einsatz des Safes als Speziallösung für das Krankenhaus wurde bereits ausführlich dargestellt. Weitere analoge

Einsatzmöglichkeiten in der medizinischen Domäne ergeben sich z. B. in der Apotheke, in Gemeinschaftspraxen oder anderen Institutionen, in denen mehrere Heilberufsausweise eingesetzt und Arbeitsplätze häufig gewechselt werden.

Aber auch in anderen Domänen gibt es Einsatzpotentiale für die Safelösung:

- Safe als Signaturserver: Als Signaturserver kann der Safe in den unterschiedlichsten Domänen zum Einsatz kommen. Beispielhaft sei hier die Massensignatur bei Scandienstleistern oder domänenübergreifend die Signatur von elektronischen Rechnungen erwähnt. Der Vorteil gegenüber existierenden Lösungen ist wiederum die sichere Verwahrung der Signaturkarten, da kein abgeschlossener Raum oder Ähnliches notwendig ist und die Inhaber ihre Karten problemlos einlegen und entnehmen können.
- Safe zur Verwahrung von Zugriffskarten: Die sichere Verwahrung von Chipkarten kann neben dem Einsatzgebiet für Signaturkarten auch für Zugriffskarten verwendet werden. Denkbar sind hier Szenarien in Hochsicherheitsbereichen, wobei die Entnahme und Rückgabe von Karten automatisiert kontrolliert und protokolliert werden kann. Auch die automatisierte Ausgabe von Zutrittskarten, z. B. im Hotelbereich, ist denkbar.

Da das Produkt und die zugehörigen Konzepte noch sehr neu sind, werden sich neben diesen ersten Ideen zukünftig sicherlich weitere Einsatzszenarien herauskristallisieren.

5.6 Umsetzung der Anforderungen

Das vorgestellte Konzept setzt sowohl alle Anforderungen der gematik-Spezifikationen als auch die gesetzlichen Bestimmungen (Anforderung A1) um. Durch die zentrale Haltung werden insbesondere der HBA und dessen PINs (einmalige Eingabe pro Tag, keine Übertragung über das Netzwerk) vor Verlust bzw. Ausspähen geschützt (Anforderung A2). Durch die Verwendung von nur einer Smart Card und einer PIN ergibt sich eine einfache und benutzerfreundliche Bedienung für effektivere Prozessabläufe (Anforderung 3 und 4). Ein weiterer Vorteil ist, dass beim Verlust einer Clinic Card oder im Falle des Ausspähens der Clinic Card PIN, diese einfach gesperrt und ersetzt werden kann. Dies gewährleistet in Zusammen-

Zusammenfassung / Abstract

Christian Mauro, Jan Marco Leimeister, Ali Sunyaev, Helmut Krömer

Zentrale Verwaltung von Gesundheitskarten im stationären Krankenhausumfeld – Das IQ-Medi-LOG-Produkt als Alternative zu gematik-Konzepten

Die gesetzlich vorgeschriebene Einführung des Heilberufsausweises (HBA) für medizinische Leistungserbringer stellt IT-Infrastrukturen, Aufbau- und Ablauforganisationen in Krankenhäusern vor große Herausforderungen. Der Beitrag stellt einen im Vergleich zu den von der gematik spezifizierten Ansätzen zur geplanten HBA-Integration in Krankenhausprozesse neuen Lösungsansatz vor, der im Produkt IQ-Medi-LOG umgesetzt ist. Hierdurch können die propagierten Effektivitäts- und Effizienzverbesserungspotenziale durch die elektronischen Gesundheitskarten vorteilhafter gehoben und eine Verbesserung des Kundenservice ermöglicht werden. Darüber hinaus bietet der Ansatz eine Grundlage für bisher noch nicht existierende Mehrwertdienstleistungen in Krankenhäusern. Anhand eines konzeptionellen Vergleichs kann die Vorteilhaftigkeit des neuen Ansatzes demonstriert werden. Abschließend werden weitere Anwendungspotenziale für diesen zentralen Ansatz zur Verwaltung von Gesundheitskarten dargestellt und ein Ausblick für die Weiterentwicklung gegeben.

Stichworte: Elektronische Gesundheitskarte (eGK), Heilberufsausweis (HBA), Krankenhaus, Gesundheitstelematik, eHealth, Integration

A Central Architecture and Solution for Health Smart Cards in Hospitals – The IQ-Medi-LOG Product as Alternative to gematik Concepts

The mandatory introduction of Health Professional Cards (HPC) in the German health care system induces major challenges for IT infrastructures as well as organisational structures in hospitals. This paper presents a new approach for integrating HPCs in hospital processes and infrastructures that is realized in the product IQ-Medi-LOG. The objective is to leverage efficiency and effectiveness potentials associated with the electronic health cards and to enable entirely new services in hospitals. Using a conceptual comparison the authors are able to show the advantages of this concept. In closing they outline further areas of application and future development trends.

Keywords: electronic health card, health professional card, hospital, health telematics, integration

hang mit den in Abschnitt 4.3 erläuterten technischen Vorkehrungen die Verfügbarkeit (Anforderung A5). Anpassungen am Primärsystem oder am Konnektor sind nicht nötig, da die von der gematik definierten Funktionalitäten bzw. Schnittstellen genutzt werden (Anforderung A6). Durch die Verwendung von nur einer Chipkarte für alle Belange gliedert sich das Konzept leichter in vorhandene Prozesse ein (Anforderung A7) und bietet zudem zahlreiche Möglichkeiten für Mehrwertdienste sowie Raum für Erweiterungen (Anforderung A8). Die Umsetzung der Anforderungen ist für die drei im Beitrag vorgestellten Konzepte zusammenfassend in **Tab. 1** dargestellt.

6 Zusammenfassung und Ausblick

Im vorliegenden Artikel wurde ein Lösungskonzept zur eGK/HBA-Integration in Krankenhäusern vorgestellt, das im Produkt IQ-Medi-LOG der Firma COMPAREX Deutschland GmbH umgesetzt ist. Wie in Abschnitt 3 gezeigt wurde, gibt es daneben zwei existierende Ansätze zur Integration von eGK/HBA in Leistungserbringerprozesse, die sich in den gematik-Spezifikationen finden, aber die Anforderungen der Leistungserbringer nicht vollständig erfüllen.

Während sich die existierenden Ansätze ausschließlich mit der eGK/HBA-Integration auseinandersetzen, adressiert die vorgestellte Lösung zusätzlich Prozessverbesserungen durch die Verwendung einer Clinic Card für Single-Sign-On, Schließsysteme, Kantinenabrechnung, etc. Zudem lassen sich durch die Erweiterbarkeit des Ansatzes weitere Mehrwertdienste entwickeln. Eine benutzerfreundliche und schnelle Bedienbarkeit des IQ-Medi-LOG-Systems wurde bei der Konzeption in den Vordergrund gestellt.

Viele der Ideen und Ansätze, die im Produkt IQ-Medi-LOG verwirklicht wurden, entstanden in enger Kooperation mit Partnern am Lehrstuhl für Wirtschaftsinformatik der Technischen Universität München. Für die nächsten Jahre sind vier zentrale Entwicklungen zu erwarten:

- a) Weiterentwicklung von Funktionalitäten. Die Erfahrungen aus den Testregionen werden weiteres Material für Erweiterungen und Optimierungen liefern. Nächster Schritt muss es daher sein, die vorgestellte Lösung im Feld zu erproben und zu evaluieren.

- b) Integration der eGK in das IQ-Medi-LOG-Produkt. Die eGK könnte bspw. bei der Aufnahme eines Patienten analog zum HBA zentral und sicher verwahrt werden und wäre damit während des Patientenaufenthalts durchgehend verfügbar. Hierzu sind jedoch noch prozesstechnische, rechtliche und auch Fragen hinsichtlich der Akzeptanz zu klären.
- c) Mehrwertdienste auf Basis des Safes. Der Chipkarten-Safe kann als Basis-Infrastruktur für weitere Dienste wie z. B. Fakturierung, Patientendienste, Zeiterfassung, etc. dienen. Hier gilt es zu evaluieren, welche Dienste weitere Mehrwerte im Krankenhaus liefern können.
- d) Entwicklung neuer Einsatzszenarien. Wie in Abschnitt 5.5 erwähnt, gibt es neben dem Gesundheitswesen eine Reihe von weiteren Domänen, die für den Einsatz des Safes in Frage kommen. Die Entwicklung von Konzepten und zusätzlichen Funktionalitäten für neue Einsatzszenarien wird zukünftig verstärkt verfolgt werden.

Auch wenn die Einführung der eGK viele Vorteile verspricht, ist die Zufriedenheit mit dem bisherigen Projektverlauf nicht optimal (Mentzini 2007). Im Gegensatz zu den Patienten ist die Akzeptanz der elektronischen Gesundheitskarte auf Seiten der Ärzteschaft noch gering (Trill 2007). Es wäre daher erfreulich, wenn das IQ-Medi-LOG-Konzept und weitere daraus resultierende Ideen zu einer Besserung dieser Situation beitragen könnten.

Literatur

- ABDA (2002): VERSA – Verteilte Signatur Arbeitsplätze: Ein Überblick. http://gematik.de/upload/gematik_KT_eHealth_Kartenterminal_V2_2_0_2427.pdf, Abruf am 2008-08-07.
- Arendt, H.; Kafitz, A. (2007): Starke Authentisierung mit Multifunktionstoken – Eine nächste Generation in Theorie und Praxis. In: *Datenschutz und Datensicherheit* 31 (3), S. 203–207
- BÄK; KBV; KZBV; BZÄK; DKG; ABDA (2006): Anforderungen der Leistungserbringer an eine anwenderorientierte und sichere Telematikinfrastruktur im Gesundheitswesen. <http://www.dkgev.de/pdf/1326.pdf>, Abruf am 2008-08-07.
- Balfanz, J.; Wendenburg, J.C.E. (2003): Digitale Signaturen in der Praxis – Leitfaden zur Prozessoptimierung und Kostenreduktion in Unternehmen und Behörden. AWV-Verlag, Eschborn.
- Bernnat, R. (2006): Endbericht zur Kosten-Nutzen-Analyse der Einrichtung einer Telematik-Infrastruktur im deutschen Gesundheitswesen. <http://www.ccc.de/crd/whistleblower-docs/20060731-Gesundheits telematik.pdf>, Abruf am 2008-08-07.
- Beyer, M.; Lenz, R.; Kuhn, K.A. (2006): Health Information Systems. In: *it – Information Technology* 48 (1), S. 6–11.
- BSI (2006): Grundlagen der elektronischen Signatur – Recht Technik Anwendung. <http://www.bsi.de/esig/esig.pdf#rechtliche>, Abruf am 2008-08-07.
- BSI (2007): BSI – Technische Richtlinie. Komfortsignatur mit dem Heilberufsausweis. <http://www.bsi.de/literat/tr/03115/BSI-TR-03115.pdf>, Abruf am 2008-08-07.
- Bundesärztekammer (2006): Heilberufsausweis und Security Module Card. Teil 3: SMC – Anwendungen und Funktionen. http://www.dimdi.de/dynamic/de/ehealth/karte/download-center/technik/kartenspezifikation/spez_testphase_archiv/spez_testphase_archiv_3_hba/hba-d3_v2-1-0.pdf, Abruf am 2008-08-07.
- Caumanns, J.; Weber, H.; Fellien, A.; Kurrek, H.; Boehm, O.; Neuhaus, J.; Kunsmann, J.; Struif, B. (2006): Die eGK-Lösungsarchitektur – Architektur zur Unterstützung der Anwendungen der elektronischen Gesundheitskarte. In: *Informatik Spektrum* 29, S. 341–348.
- Frießem, P.; Kalmring, D.; Reichelt, P. (2005): Lösungsarchitektur für die Einführung der elektronischen Gesundheitskarte und der auf ihr basierenden Anwendungen. In: *WIRTSCHAFTSINFORMATIK* 47 (3), S. 180–186.
- gematik (2007a): Einführung der Gesundheitskarte – Die Spezifikation der elektronischen Gesundheitskarte. Teil 3: Äußere Gestaltung. http://gematik.de/upload/gematik_eGK_Spezifikation_Teil3_V1_4_0_2257.pdf, Abruf am 2008-08-07.
- gematik (2007b): Einführung der Gesundheitskarte – Gesamtarchitektur. http://gematik.de/upload/gematik_GA_Gesamtarchitektur_V1_0_0_2302.pdf, Abruf am 2008-08-07.
- gematik (2007c): Einführung der Gesundheitskarte – Konnektorspezifikation. http://gematik.de/upload/gematik_KON_Konnektor_Spezifikation_V2_2_0_2429.pdf, Abruf am 2008-08-07.
- gematik (2007d): Einführung der Gesundheitskarte – Spezifikation eHealth-Kartenterminal. http://gematik.de/upload/gematik_KT_eHealth_Kartenterminal_V2_2_0_2427.pdf, Abruf am 2008-08-07.
- Haas (2005): Medizinische Informationssysteme und elektronische Krankenakten, Springer-Verlag, Berlin/Heidelberg.
- Hornung, G.; Goetz, C.; Goldschmidt, A. (2005): Die künftige Telematik-Rahmenarchitektur im Gesundheitswesen – Recht, Technologie, Infrastruktur und Ökonomie. In: *WIRTSCHAFTSINFORMATIK* 47 (3), S. 171–179.
- Hühnlein, D.; Knosowski, Y. (2003): Aspekte der „Massensignatur“. In: *Horster, P.* (Hrsg.): *Ta- gungsband D*A*CH Security*. IT-Verlag, S. 293–307.
- Jern, M. (1998): „THIN“ vs „FAT“ Visualization Client. In: *Proceedings of the Computer Graphics International*.
- Krcmar, H. (2005): *Informationsmanagement*. 4. Aufl., Springer, Berlin et al.
- Leimeister, J. M.; Klapdor, S.; Hörmann, C.; Krcmar, H. (2008): IT-Management in deutschen Krankenhäusern – Eine Bestandsaufnahme aus Sicht der IT-Entscheider. BoD Verlag, Norderstedt.
- Mauro, C.; Sunyaev, A.; Leimeister, J. M.; Schweiger, A.; Krcmar, H. (2008): A Proposed Solution for Managing Doctor's Smart Cards in Hospitals Using a Single Sign-On Central Architecture. In: *Proceedings of the Hawaii International Conference on System Sciences (HICSS 41)*.
- Mentzini, P. (2007): Die elektronische Gesundheitskarte – Made in Germany. In: *Jäckel, A.* (Hrsg.): *Telemedizinführer Deutschland*, Ausgabe 2007. Minerva, Ober-Mörlen, S. 27–28.
- Omar, S.; Djuhari, H. (2004): Multi-purpose student card system using smart card technology. In: *Proceedings of the Fifth International Conference on Information Technology Based Higher Education and Training (ITHET)*, S. 527–532.
- Rankl, W.; Effing, W. (1995): *Handbuch der Chipkarten*. Carl Hanser Verlag, München/Wien.
- Richter, T.; Witowski, N.; Weidner, J. (2007): *Common-Criteria-Dokument – Sicherheitsvorgaben zur Erreichung des EAL 3+*. Projekt: Elektronischer Chipkarten-Safe im Rahmen der Lösung IQ-Medi-LOG, COMPAREX Deutschland GmbH, Mannheim.
- Schröder, K.-W. (1995): *Zertifizierte Sicherheit für Chipkarten*. In: *Glade, A.; Reimer, H.; Struif, B.* (Hrsg.): *Digitale Signaturen & Sicherheitssensitive Anwendungen*. Vieweg, Braunschweig/Wiesbaden, S. 242–249.
- Schweiger, A.; Sunyaev, A.; Leimeister J. M.; Krcmar, H. (2007): *Toward Seamless Healthcare with Software Agents*. In: *Communications of the Association for Information Systems* 19 (33), S. 692–709.
- SigG (2001): *Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG)*. http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf, Abruf am 2008-08-07.
- SigV (2001): *Verordnung zur elektronischen Signatur (Signaturverordnung – SigV)*. http://www.gesetze-im-internet.de/bundesrecht/sigv_2001/gesamt.pdf, Abruf am 2008-08-07.
- TeleTrust (2007): *SICCT – Secure Interoperable ChipCard Terminal*. http://www.teletrust.de/fileadmin/files/publikationen/Spezifikationen/SICCT_Spezifikation_120.pdf, Abruf am 2008-08-07.
- Trill, R. (2006): eGK – ein Einstieg in die flächendeckende, Sektoren übergreifende Telematik? – Eine Betrachtung aus Krankenhaussicht. In: *Jäckel, A.* (Hrsg.): *Telemedizinführer Deutschland*, Ausgabe 2006. Minerva, Darmstadt, S. 10–14.
- Trill, R. (2007): *Gesundheitskarte – Akzeptanz drif- tet auseinander*. In: *Jäckel, A.* (Hrsg.): *Telemedizinführer Deutschland*, Ausgabe 2007. Minerva, Ober-Mörlen, S. 27–28.