



## ArchiSig - Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente

Prof. Dr. Paul Schmücker, Fachhochschule Mannheim,  
Windeckstraße 110, D-68163 Mannheim

Mannheim, 22.04.2004  
Tel.: 0621/292-6206

### **Stellungnahme des Verbundprojektes „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“ und der Arbeitsgruppe „Archivierung von Krankenunterlagen“ der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS) vom 22. April 2004 zur Rahmenarchitektur bit4health**

Sehr geehrte Damen und Herren,

Mitarbeiter des vom Bundesministerium für Wirtschaft und Arbeit geförderten Verbundprojektes „ArchiSig“ und der Arbeitsgruppe „Archivierung von Krankenunterlagen“ der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS) haben die Ergebnisse des Planungsauftrags bit4health kritisch zur Kenntnis genommen. Es kann festgehalten werden, dass die Vorbereitungen zur Einführung der elektronischen Gesundheitskarte einen großen Schritt vorangekommen sind. Der gesetzliche Rahmen wurde durch das Gesundheits-Modernisierungsgesetz geschaffen. Die Ergebnisse des Planungsauftrags bit4health stellen einen sinnvollen Rahmen für detaillierte funktionale, prozessorientierte, kommunikative, technische und organisatorische Spezifikationen zur Einführung und zum Betrieb der elektronischen Gesundheitskarte dar.

Nachfolgend möchten wir Ihnen primär einige Kommentare und Anregungen zu den Ergebnissen des Planungsauftrags bit4health bezüglich der beweiskräftigen und sicheren Langzeitsicherung elektronischer Dokumente übersenden.

Die Archivierung ist in dem bit4health-Konzept bisher ausdrücklich ausgeklammert (Sicherheitsarchitektur, Seite 16). Nach dem Teilkonzept „Sicherheitsanforderungen“, Seite 38 berücksichtigt das Kartenmanagement eine mittlere Lebensdauer der elektronischen Gesundheitskarte von ca. 5 Jahren. Hier stellt sich die Frage, ob es notwendig und geplant ist, die medizinischen Daten der alten Karte auf die neue Karte zu übernehmen.

In dem bit4health-Konzept ist nicht geklärt, wie lange die Daten auf der Gesundheitskarte karten- bzw. serverbasiert aufgehoben werden müssen und ob neben der Primärdokumentation im Krankenhaus und in den Arztpraxen Dokumentationen auf der Gesundheitskarte rechtlich erforderlich sind. Hat die Gesundheitskarte eine rechtliche Relevanz, wovon wir ausgehen, so sind eine Erzeugung und Verifikation von elektronischen Signaturen nicht ausreichend. Bei der Langzeitarchivierung elektronisch signierter Dokumente und Daten ergeben sich nämlich unter anderem folgende Problempunkte:

#### ArchiSig-Partner:

**Universitätsklinikum Heidelberg**  
Abt. Medizinische Informatik  
Abt. Innere Medizin

**Fraunhofer Gesellschaft**  
Institut für sichere Telekooperation,  
Darmstadt

**Niedersächsische Staatskanzlei,  
Hannover**  
Staatliche Archivverwaltung

**DATEV eG, Nürnberg**

**Universität Kassel**  
Projektgruppe Verfassungs-  
vertragliche Technikgestaltung

**IXOS Software AG,  
Grasbrunn / München**

**SECUDE Sicherheitstechnologie  
Informationssysteme GmbH,  
Darmstadt**

**Pergis Systemhaus GmbH,  
Ludwigshafen**  
Konsortialführer

**Fachhochschule Mannheim**  
Hochschule für Technik und  
Gestaltung, Lehrgebiet  
Medizinische Informatik

**Informatikzentrum  
Niedersachsen**  
Landesbetrieb

**T-Systems Austria  
GesmbH, Wien**  
Health Services

- Qualifizierte Signaturzertifikate sind zeitlich begrenzt verfügbar und prüfbar: 5 Jahre bei nicht akkreditierten Zertifizierungsdiensteanbietern, 30 Jahre bei akkreditierten Zertifizierungsdiensteanbietern.
- Kryptographische Algorithmen, die bei der Erzeugung der Signaturen verwandt werden, können mit der Zeit ihre Sicherheitseignung durch „Alterung“ verlieren.
- Informationen zu Sicherheitseignungen kryptographischer Algorithmen stehen den Betreibern von elektronischen Archivierungssystemen nicht in elektronisch auswertbarer Form zur Verfügung. Zur Zeit müssen diese dem Bundesanzeiger entnommen werden.
- Durch die Transformation signierter Dokumente in andere Dokumentenformate oder auf andere Datenträger wird der Beweiswert der ursprünglichen Signatur gemindert. Beispiele sind die Transformation von Papier auf elektronische Medien oder die Vorlage eines elektronisch signierten Dokumentes in Papierform.
- Die verfügbaren Signaturstandards sind insbesondere bezüglich Signaturerneuerung und Verifikationsdaten unzureichend.

Konzepte und Realisierungen zu diesen bisher ungelösten Anforderungen hat das Verbundprojekt „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente“ erarbeitet. Im Projekt „ArchiSig“ wurden unter anderem Konzepte und Module entwickelt für

- die Verifikationsdatenbeschaffung und -sicherung zu qualifizierten elektronischen Signaturen,
- die rechtzeitige und automatische Signaturerneuerung durch qualifizierte Zeitstempel,
- einen elektronischen Informationsdienst zur Sicherheit kryptographischer Algorithmen,
- elektronische Beglaubigungen von Transformationen und
- Verifikations- und Präsentationstools für signierte elektronische Dokumente.

Ist eine rechtliche Relevanz bei den auf der Gesundheitskarte gespeicherten Daten und Dokumente gegeben, wovon durchaus ausgegangen werden kann, so sind die ArchiSig-Konzepte anzuwenden, wenn die Integrität und Verbindlichkeit / Abstreitbarkeit von Dokumenten und Daten langfristig sichergestellt werden soll. Dies ist nur dann wirtschaftlich möglich, wenn insbesondere die Verifikationsdatenbeschaffung und -sicherung sowie die rechtzeitige und automatische Signaturerneuerung schon während des Signierens der Dokumente unterstützt wird.

In dem Teilkonzept „Standards und Initiativen im Gesundheitswesen“ fehlen einige Standards und gängige Verschlüsselungsverfahren wie z. B.

- a. Daten- und Dokumentenstandards: VITAL für Messdaten, LOINC für Laboruntersuchungen, ASCII und TIFF sowie PDF, ein Industriestandard, für Dokumente
- b. Signaturstandards: Electronic Signature Formats, basierend auf der „Cryptographic Message Syntax (CMS)“ sowie „XML Advanced Electronic Signatures“ (Spezifikationen des European Telecommunications Standards Institute (ETSI))
- c. Verschlüsselungsverfahren: Triple-DES, DES etc.

Ein breiter Einsatz der ArchiSig-Konzepte erfordert auch eine ausreichende Standardisierung von elektronischen Signaturen. Da Spezifikationen zur Integration der erforderlichen Verifikationsdaten in signierte Dokumente, zur Signaturerneuerung und für die Information über die Sicherheitseignung kryptographischer Algorithmen fehlen, hat das Projekt „ArchiSig“ Standardisierungsinitiativen ins Leben gerufen. Mit Unterstützung des ISIS-MTT-Boards wird derzeit eine nationale Standardisierung, im Rahmen der IETF (Internet Engineering Task Force) eine internationale Standardisierung durchgeführt. Die dringend erforderlichen Standardisierungsergebnisse werden noch in diesem Jahr erwartet.

In der bit4health-Rahmenarchitektur wurde leider der Einordnung der Elektronischen Gesundheitskarte in den Gesamtrahmen des Informationsmanagements des Gesundheitswesens nicht die notwendige Bedeutung beigemessen. Ein Nachteil der vorgelegten Rahmenarchitektur ist zum Beispiel, dass Redundanzen von Daten, Dokumenten und sonstigen Objekten im klinischen Umfeld aufgebaut werden, wobei das Beschreiben der Gesundheitskarten bzw. das Beliefern der serverbasierten Gesundheitsakten immense personelle und finanzielle Aufwände für die Krankenhäuser und Arztpraxen zur Folge hat. Hier gibt es riesige Einsparpotentiale z. B. durch die Vermeidung von Mehrfachablagen der Daten, Dokumente und sonstigen Objekten im Krankenhaus, in

Arztpraxen, auf Gesundheitskarten und in Gesundheitsakten. Bezüglich der Archivierung sollte ein behandlungsorientierte ökonomische Perspektive für die nächsten 15 Jahre entwickelt werden, die die Dokumentations-, Organisations- und Rechtsbedürfnisse aller beteiligten Parteien ohne einen Aufbau von vielfachen Redundanzen ermöglicht. Warum kann nicht eine kostengünstigere zentrale Speicherung der archivierten Daten und Dokumente für alle Beteiligten erfolgen? Die notwendigen Instrumente der Datensicherung und des Datenschutzes sind hierzu bereits verfügbar.

Die Dimension der medizinischen Dokumentation und Archivierung zeigt die folgende Modellrechnung: Wenn man davon ausgeht, dass jährlich 1 laufender Meter neuer Dokumente pro stationärem Bett bei 550.000 aufgestellten Betten im Akutbereich (ca. 2.200 Krankenhäuser) und durchschnittlich je 5.000 neue Seiten bei den 300.000 niedergelassenen Ärzten erzeugt werden, werden in Deutschland unter zusätzlicher Berücksichtigung von ca. 1.000 Rehabilitationseinrichtungen sowie der Pflegeeinrichtungen pro Jahr ca. 5 Milliarden neue Dokumente erzeugt. Für deren Archivierung entstehen aufgrund der bisherigen Erfahrungen Kosten in Höhe von ca. 2,5 Milliarden Euro.

Ein weiteres Beispiel für eine Kosteneinsparung stellt der bisher praktizierte konventionelle Arztbrief-, Befund- und Bildversand zu mitbehandelnden Institutionen dar. Dieser könnte grundsätzlich gemäß dem bit4health-Konzept abgewickelt werden. Was nutzt Wirtschaftlichkeit und der größtmögliche Gesamtnutzen für die Telematikinfrastruktur, wenn Zusatzkosten im klinischen Umfeld durch eine doppelte Bereitstellung von Informationen entstehen? Nach GMG ist der elektronische Arztbrief allerdings nur eine freiwillige Anwendung, die der Zustimmung des Patienten bedarf. Wie ist der Widerspruch zur heute gängigen Praxis zu verstehen, dass Arztbriefe, Befunde und Bilder ohne explizite Zustimmung des Patienten an externe klinische Institutionen nicht nur versandt werden, sondern in der Regel auch für die Weiterbehandlung benötigt werden.

Weitere Kosten können durch den Einsatz multifunktionaler Karten gespart werden, die sogar über das Gesundheitswesen hinaus eingesetzt werden können. Beispiele hierfür sind Bürgerkarten (eGovernment) oder Job-Karten. Multifunktionale Karten sollten auch den Bedürfnissen der medizinischen Einrichtungen gerecht werden, die über die Telematikplattform hinausgehen. Dies betrifft z. B. die Zufahrt zum Parkplatz, das Bezahlen in Mensa und Cafeteria oder der Zugang zu Räumen und Rechnersystemen.

Bei dem Studium und der Diskussion des bit4health-Konzeptes zeigt sich, dass eine sinnvolle Lösung eine Symbiose von Elektronischer Gesundheitskarte und serverbasierter Elektronischer Gesundheitsakte erfordert und dabei das Medium von nachrangiger Bedeutung ist. Dieser Grundsatz sollte auch in dieser Form in das Konzept übernommen werden. Aus diesem Grunde sollten die Möglichkeiten des Zusammenspiels von Patientenkarten und Patientenakten in dem bit4health-Konzept verbessert herausgearbeitet werden.

Die Definitionen zur Elektronischen Gesundheitskarte und zur Elektronischen Gesundheitsakte sind aus unserer Sicht zu wenig differenziert. Hierzu sollen die folgenden Ausführungen beitragen.

Krankengeschichte: Unter dieser versteht man die Sammlung aller medizinischen Informationen zu einer Person unabhängig vom Ort, der Zeit und dem Datenträger.

Patientenakte: Diese ist die Sammlung medizinischer Informationen zu einer Person in einer Institution. Hierzu zählen die Anamnese sowie diagnostische, therapeutische, pflegerische und administrative Maßnahmen. Die konventionellen Patientenakten können pro Krankenhaus, Klinik, Abteilung oder Funktionsbereich jahrgangsweise oder lebenslang angelegt werden.

Elektronische Patientenakte: Hierbei handelt es sich um eine auf digitalen Datenträgern (WORM, CD-ROM, DVD, ...) abgelegte und elektronisch verfügbare Patientenakte. Die verschiedenen Informationen werden über eindeutige Patientenidentifikationen miteinander verbunden. Für die Verwaltung, die Ablage, das Wiederauffinden und das Präsentieren von Informationen sind geeignete rechnerunterstützte Interaktions-, Speicher- und

Präsentationswerkzeuge erforderlich. Die elektronische Patientenakte wird durch medizinisches Personal im Krankenhaus oder der Arztpraxis aufgebaut und fortgeschrieben. Die gezielten Zugriffsmöglichkeiten auf die elektronische Patientenakte werden entscheidend durch den Grad der Strukturierung, Formalisierung und Metaisierung (z. B. Beschreibung der Inhalte durch Deskriptoren) der Daten und Dokumente bestimmt. Die Elektronische Patientenakte ist Bestandteil eines Krankenhausinformationssystems oder eines Praxissoftwaresystems.

Elektronische Gesundheitsakte:

Die elektronische Gesundheitsakte umfasst einen Teilausschnitt aus einer Krankengeschichte, der auf digitalen Datenträgern serverbasiert abgelegt ist, mehrere Institutionen an verschiedenen Orten betrifft und Dokumentationen des Patienten einbeziehen kann. Die Elektronische Gesundheitsakte wird über Schnittstellen aus verschiedenen Institutionen, aber auch durch die Eigendokumentation von Patienten beliefert. Dazu zählen auch Daten, die durch teure und gesundheitsbelastende Untersuchungen erzeugt wurden. Die elektronische Gesundheitsakte kann auch Daten aus dem Präventionsbereich wie Ernährungs- und Trainingspläne sowie vom Bürger übermittelte Daten von HomeCare-Devices (z. B. Blutzuckermesswerte) enthalten. Der Bürger hat damit die Möglichkeit, direkt auf sein Gesundheitsmanagement Einfluss auszuüben.

Ziele sind Gesundheitsakten für den Bürger, chronische Erkrankungen (z. B. Diabetes) oder die medizinische Versorgungsregion. Sie ermöglichen eine Kommunikation mit einem Gesundheitsbetreuer, eine einrichtungübergreifende Kommunikation sowie eine Unterstützung des Disease Management. Die Kommunikation erfolgt in der Regel orts- und zeitunabhängig über das Internet. Die elektronische Gesundheitsakte, die vorerst vorwiegend die für die Behandlung wichtigsten Informationen der Krankengeschichte umfasst, ist jederzeit verfügbar. Sie steht unter der Kontrolle des Patienten, soweit der Zugriff nicht gesetzlich geregelt ist.

Gemäß Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz - GMG) vom 14. November 2003 ist das Fünfte Buch Sozialgesetzbuch um § 67 und § 68 erweitert worden, um die Qualität und Wirtschaftlichkeit der Versorgung zu verbessern. Nach § 67 soll die papiergebundene Kommunikation unter den Leistungserbringern so bald und so umfassend wie möglich durch die elektronische und maschinell verwertbare Übermittlung von Befunden, Diagnosen, Therapieempfehlungen und Behandlungsberichten, die sich auch für eine einrichtungübergreifende fallbezogene Zusammenarbeit eignet, ersetzt werden. Die Krankenkassen und Leistungserbringer sowie ihre Verbände sollen den Übergang zur elektronischen Kommunikation finanziell unterstützen. Nach § 68 (Finanzierung einer persönlichen elektronischen Gesundheitsakte) können die Krankenkassen ihren Versicherten zu von Dritten angebotenen Dienstleistungen der elektronischen Speicherung und Übermittlung patientenbezogener Gesundheitsdaten finanzielle Unterstützung gewähren.

Elektronische Gesundheitskarte:

Im Gegensatz zu den o. a. Akten befindet sich die Elektronische Gesundheitskarte im persönlichen Besitz einer Person. Diese kann ebenfalls einen Teilausschnitt aus einer Krankengeschichte beinhalten, der von mehreren Institutionen an

verschiedenen Orten stammt. Auf der Gesundheitskarte sollen vorerst Verwaltungsdaten und Notfalldaten (Erkrankungen, Risikofaktoren, Medikation, ...) abgelegt werden. Ferner sollen u. a. auch das Elektronische Rezept, die Arzneimitteldokumentation, das Zuzahlungsmanagement, der Elektronische Arztbrief und elektronische Patientenaufzeichnungen unterstützt werden. Die Elektronische Gesundheitskarte soll außerdem als Europäische Krankenversichertenkarte zur Ablösung der Vordrucke E 111 und E 111b genutzt werden. Die Elektronische Gesundheitskarte dient dem asynchronen Datenaustausch über mehrere Institutionen an verschiedenen Orten. Sie wird auf Basis einer multifunktionalen Smartcard realisiert.

Digitales Archiv:

Eine Ansammlung von Elektronischen Patientenakten stellt in der Regel noch kein Digitales Archiv dar. Zusätzlich muss die ordnungsgemäße, revisionssichere und rechtlich anerkannte Aufbewahrung von Daten, Dokumenten, Bildern, Signalen etc. über einen Zeitraum von 30 Jahren und mehr sichergestellt werden.

Grundsätzlich sollte das bIT4health-Konzept den Patienten stärker in den Mittelpunkt stellen. Hierzu sind möglichst einfach bedienbare Benutzeroberflächen bereitzustellen, die selbsterklärend sind und keine Schulungen erfordern. Dieser letzte Punkt ist im Konzept anscheinend nicht ausreichend berücksichtigt. Die Notwendigkeit einer Schulung oder Einarbeitung bedeutet Nichtakzeptanz und Ablehnung eines Produktes, das möglichst von dem Großteil der Bevölkerung genutzt werden soll.

Zu einer Rahmenarchitektur gehören natürlich auch eine Kostenbetrachtung und eine umfangreiche Risikobewertung für die Durchführung des Projektes zur Einführung der elektronischen Gesundheitskarte. Zur Risikobewertung gehören auch Notfallkonzepte für alle beteiligten Gruppen. Die beiden Aspekte „Kostenbetrachtung und Risikobewertung“ können durchaus zu einem Scheitern von Projekten führen. Die Kostenbetrachtung sollte für alle beteiligten Institutionen Investitions- und Betriebskosten inklusive Personalkosten umfassen. Dies betrifft insbesondere auch die Krankenhäuser und die Arztpraxen.

Mit Spannung erwarten wir nun die Erarbeitung der Lösungsarchitektur und die Durchführung der ersten Modellprojekte. Hierzu bieten wir unsere Unterstützung an.

Bei dem Aufbau der Telematikplattform für das Gesundheitswesen wünschen wir uns allen viel Erfolg und verbleiben vorerst

mit herzlichen Grüßen  
Ihr



(Prof. Dr. Paul Schmücker)

Konsortialführer des Verbundprojektes „ArchiSig – Beweiskräftige und sichere  
Langzeitarchivierung digital signierter Dokumente“

Leiter der Arbeitsgruppe „Archivierung von Krankenunterlagen“ der Deutschen  
Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.  
(GMDS)