Ein Beitrag zur Entwicklung von kostenneutralen Internet-Lösungen für die Praxis

B. Schütze[1)], M. Kroll[1)], T. Geisbe[2)], H.-D. Lipinski1[)], T.J. Filler[3)]

1) Fachhochschule Dortmund, Fachbereich Medizinische Informatik
2) Universität Witten/Herdecke, Institut für Radiologie und MikroTherapie
3) Universität Münster, Institut für Anatomie (Klinische Anatomie)

Sachfremde Leistungen	Millionen Euro			
	1998	1999	2000	2001
Forschung/Ausbildung/Investitionen	4.074,00 €	10.026,00 €	9.931,00 €	10.203,00 €
Gutachten und Koordination	640,00 €	659,00 €	669,00 €	691,00 €
Transporte	3.192,00 €	3.326,00 €	3.454,00 €	3.613,00 €
Verwaltungsleistungen	10.987,00 €	11.406,00 €	11.577,00 €	11.951,00 €
Waren / Einkauf	54.976,00 €	55.733,00 €	57.291,00 €	60.363,00 €
Gesamt	**73.869,00 €**	**81.150,00 €**	**82.922,00 €**	**86.821,00 €**

Tabelle 1: Kosten sachfremder Leistungen im Gesundheitswesen
Quelle: Statistisches Bundesamt, http://www.destatis.de/themen/d/thm_gesundheit.htm

Kosten im Gesundheitswesen	Millionen Euro			
	1998	1999	2000	2001
Gesamtkosten	211.027,00 €	214.270,00 €	218.784,00 €	225.931,00 €
ambulante Einrichtungen	95.445,00 €	98.110,00 €	100.411,00 €	105.086,00 €
stationäre/teilstationäre Einrichtungen	80.717,00 €	83.448,00 €	85.315,00 €	86.725,00 €
Anteil Sachfremde Leistungen an den Gesamtkosten	**35,00%**	**37,87%**	**37,90%**	**38,43%**

Tabelle 2: Kosten im Gesundheitswesen
Quelle: Statistisches Bundesamt, http://www.destatis.de/themen/d/thm_gesundheit.htm

Einleitung
Bei den laufend steigenden Ausgaben im Gesundheitswesen (siehe Tabelle 2) und den gleichzeitig immer geringeren verfügbaren finanziellen Ressourcen müssen neue Wege zur Verbesserung der Patientenversorgung bei gleichzeitiger Vermeidung erhöhten Ressourcenverbrauches. Da für sachfremde Leistungen, d.h. Leistungen die nicht direkt mit der Patientenbehandlung involviert sind (Transportkosten, Bestellungen usw.), fast 40 % der Gesamtkosten im gesundheitswesen entfallen (siehe Tabelle 1), bietet hier das Medium Internet mit seinen Möglichkeiten des Datenaustausches hervorragende Möglichkeiten.
Im vernetzten Gesundheitssystem haben Partner bei der Patientenbehandlung, z.B. Krankenhaus und niedergelassene Ärzte, die Möglichkeit, eine gemeinsame Datenbasis bzgl. der angefallenen Patientendaten (Patientenstammdaten, diagnostische und therapeutische Daten, ...) zu nutzen. Die kostengünstigste Möglichkeit der Datenübertragung bietet hier das Medium Internet, da heutzutage fast jede Klinik eine Standleitung besitzt und die meisten Arztpraxen über DSL an das World Wide Web angeschlossen sind.
In der Radiologie ist der Einsatz von Open-Source-Software als Picture Archiving and Communication System (PACS) oder als Betrachtungsstation für DICOM-Bilddaten schon länger bekannt[1, 2]. Diese Arbeit zeigt, dass mit Open-Source-Software eine im Vergleich zu kommerziellen Anbietern kostengünstigere Lösung zur Verteilung der nach dem deutschen Datenschutzrecht als höchst schützenswürdig einzustufenden Patientendaten gefunden werden kann.[3]

Material und Methode
Die Übermittlung medizinischer Daten, z.B. Befunde und Bilddaten muss den rechtlichen Rahmenbedingungen genügen. Hieraus resultiert die Forderung, dass die Daten mit sicheren kryptographischen Methoden verschlüsselt werden, sobald öffentliche Übertragungsmedien (Internet, Telefonleitungen, usw.) benutzt werden[5]. Weiterhin muss der Arzt, bei dem die medizinischen Patientendaten angefallen sind, vorher festlegen, welche Daten von wem eingesehen werden dürfen. Generell gilt das Prinzip der Datenvermeidung und des Datenschutzes auch bei der Zurverfügungstellung von Daten. Es müssen so wenige Daten wie notwendig anderen zur Einsicht gegeben werden. Außer dem Patienten darf nur ein mitbehandelnder Mediziner bzw. eine vom Patienten legitimierte Person in die für die Mitbehandlung notwendigen bzw. die bereitgestellten Daten Einblick erhalten. Verantwortlich für die Zuteilung ist außer dem Patienten der „Besitzer“ der Patientendaten: der behandelnde Arzt, der das Informationssystem verwendet. Aus Gründen des Datenschutzes muss er die Daten aktiv an seinen Kollegen versenden. Der umgekehrte Weg der Kollege holt sich die Daten aus der Datenbank ist nicht gestattet. Die Alternative ist die aktive Freischaltung einzelner Daten im Informationssystem durch den behandelnden Arzt nach Rücksprache mit dem behandelten Patienten, so dass der mitbehandelnde Arzt nur die speziell für ihn aufbereiteten Daten sehen kann. Eine Ausnahme bildet hier der Patient selbst, der selbstverständlich alle ihn betreffenden Daten sehen darf.
Zur Übermittlung der Patientendaten mittels eMail erfolgt die Verschlüsselung der medizinischen Nutzdaten durch eine schnelle symmetrische Verschlüsselung mit einem als sicher anerkannten Verfahren, z.B. AES oder Twofish. (Siehe Abbildung 1) Die Nutzung von Public-Key-Verfahren wie z.B. PGP verbieten sich, da nach deutschem Recht der private Schlüssel beschlagnahmt werden und damit das Schweigerecht / die Schweigepflicht des Arztes nicht länger aufrecht gehalten werden kann[6].
Um die Patientendaten bei der Benutzung eines Webinterfaces mit einer Verbindung zu einem Informationssystem zu schützen, müssen die Daten ebenfalls durch kryptographische Methoden geschützt werden:
- Integritätssicherung: Um sicherzustellen, dass die übertragenen Daten nicht zufällig oder absichtlich verfälscht worden sind, können die Daten mit einer kryptographischen Prüfsumme versehen werden.
- Verschlüsselung: Um die Vertraulichkeit der übertragenen Daten sicherzustellen, können symmetrische (z.B. AES, Twofish) oder asymmetrische (z.B. RSA, Elliptische Kurven) Verschlüsselungsverfahren benutzt werden.
- Quittierung: Zur Quittierung kann der Empfänger aus den empfangenen Daten einen Hashwert bilden und diesen anschließend digital signiert als Empfangsquittung zurücksenden. Hierdurch kann der Sender nachweisen, dass
  - die Quittung vom Empfänger stammt (digitale Signatur) und
  - dieser die Quittung nur durch Kenntnis der übermittelten Daten erstellen konnte (Hashwert).
  - Durch Verwendung von dynamischen Schlüsseln, Transaktionsnummern oder Zeitstempeln kann sichergestellt werden, dass wiedereingespielte manipulierte Nachrichten als solche erkannt und abgelehnt werden.

Die vorgenannten Maßnahmen sichern nicht die eingesetzten Rechner bzw. die Datenbank mit den medizinischen Nutzdaten vor unbefugten Manipulationen. Hier ist die einzige Möglichkeit zur Verhinderung von Manipulationen der Einsatz einer Firewall. Dabei werden im wesentlichen zwei Mechanismen unterschieden: Paketfilter und Application Level Gateway (Proxy Gateways)[4].

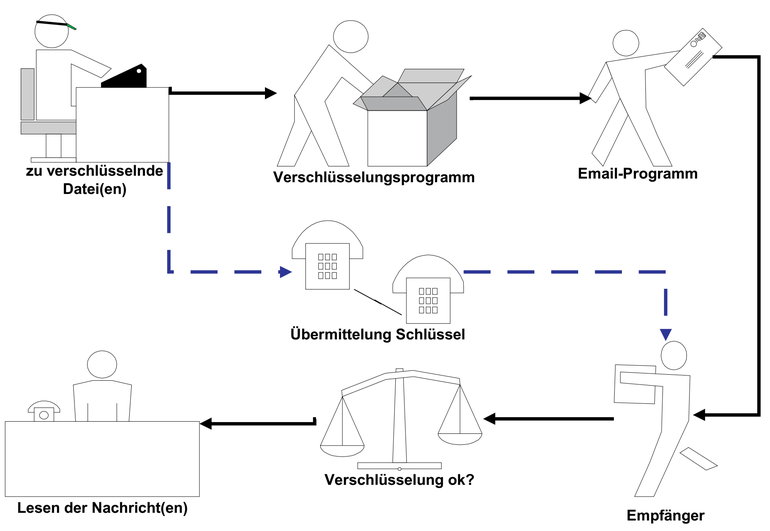

Abbildung 1: Versendung von Patientendaten mittels eMail

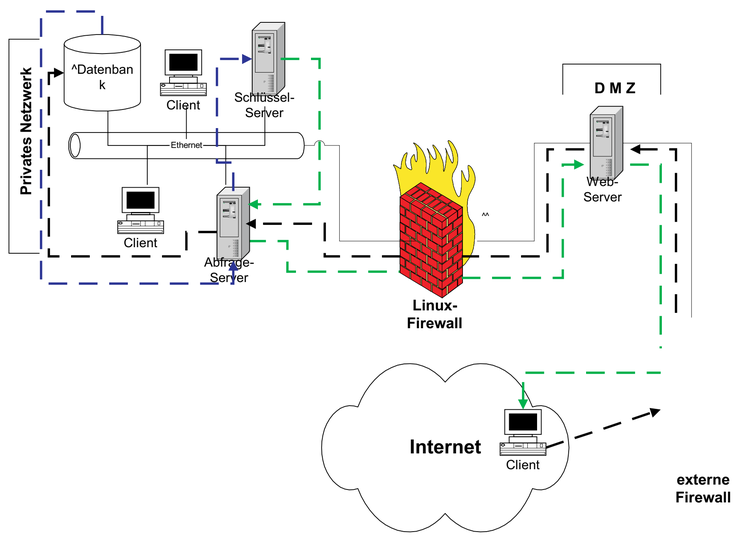

Abbildung 2: Abfrage an Informationssystem in der Medizin aus dem Internet

Ergebnisse
Zur Übersendung von Daten mittels eMail bietet sich ein Programm, welches zum einen eine sichere Verschlüsselung mittels AES anbietet und zum anderen die zu sichernden Daten komprimiert und zusammen mit dem Entschlüsselungsprogramm zu einer ausführbaren Datei („exe-Datei“) zusammenfasst, bietet die Firma „DataRescue“ kostenlos im Internet an[7]. Das Programm heißt „aCrypt+“, daher ist eine Eigenentwicklung hier nicht notwendig.
Der Internet-Server, der das Webinterface zur Abfrage der Patientendaten aus dem medizinischen Informationssystem zur Verfügung stellt, ist durch eine externe Firewall, die eine Kommunikation nur über den Port 80 gestattet, für WWW-Anfragen erreichbar. Die Kommunikation erfolgt mittels SSL. Die bei der Kommunikation genutzte SSL-Verbindung wird von einem Überwachungsserver protokolliert. Auf dem Webserver selbst wird durch die Anfrage ein CGI-Skript gestartet, welches eine Kommunikation auf einem nicht-privilegierten Port (> 1024) mit einem durch die interne Firewall geschützten Kommunikations-Server aufbaut. Der Kommunikations-Server fungiert als Abfrage-Client, d.h. hier wird die eigentliche SQL-Abfrage an das medizinische Informationssystem durchgeführt. Für die Implementierung der Server wurde das Betriebssystem Linux genutzt, die Firewall, der Webserver wie auch der Überwachungsserver nutzt Open-Source-Software. (Siehe Abbildung 2)

Diskussion/Schlussfolgerungen
Open-Source-Software erfüllt alle Anforderungen, die an eine sichere Übermittlung von Gesundheitsdaten mit dem Medium Internet gestellt werden müssen. Sowohl eine Firewall wie auch die Möglichkeit Patientendaten aus medizinischen Datenbanken abzufragen können mittels des Betriebssystems Linux und anderer Open-Source-Software realisiert werden. Die eingesparten Kosten bei der Anschaffung der Software bedingen auf der anderen Seite eine Einarbeitung in die Benutzung der entsprechenden Software. Diese Personalkosten sind jedoch zu relativieren, da viele Positionen wie z.B. ein IT-Leiter im Krankenhaus schon zur Verfügung steht, d.h. die Kosten fallen nicht zusätzlich an. Bei kleineren Krankenhäusern oder Arztpraxen ohne eigene EDV-Abteilung empfiehlt sich der Zusammenschluss zu einem telematischen Verbund mit einem externen Dienstleister, welcher die Wartung der Firewall sowie die Programmierung der Internet-Präsentation der Patientendaten übernimmt.
Fazit: Im Vergleich zu den anschaffungskostenträchtigen kommerziellen Lösungen für die rechtsbedingten Sicherungssysteme für die Patientendaten in der Teleradiologie sind die kostenlosen Open-Source-Lösungen wenigstens gleich leistungsfähig.

Literatur
1. Langer S.G. OpenRIMS:
   An Open Architecture Radiology Informatics Management System.
   J Digit Imaging 2002; 15(2):91-7
2. Marzola P, Da Pra A, Sbarbati A, Osculati F.
   A PC-based workstation for processing and analysis of MRI data.
   MAGMA 1998;7(1):16-20
3. Bergmann L., Möhrle R., Herb A.
   Datenschutzrecht, Teil III Kommentar zum Bundesdatenschutzgesetz.
   Richard Boorberg Verlag, 2002
4. Bundesamt für Sicherheit in der Informationstechnik [Online].
   2000 Feb 25 [zitiert 2003 März 22]; Verfügbar unter
   http://www.bsi.bund.de/literat/tagung/cebit00/vt_071.htm
5. Bundesamt für Sicherheit in der Informationstechnik [Online] .
   2002 Sep 9 [zitiert 2003 März 22]; Verfügbar unter
   http://www.bsi.bund.de/esig/basics/techbas/krypto/index.htm
6. Schütze B., Geisbe Th., Grönemeyer D.H.W., Filler T.J.
   Sicherer elektronischer Datenaustausch durch Electronic Mail.
   Telemed 2002;
7. DataRescue [Online].
   2003 Feb 24 [zitiert 2003 März 22];
   Verfügbar unter http://www.acrypt.com
8. Meyer A. Wer verdient wie viel?
   Ergebnisse der c't-Gehaltsumfrage.
   C't 2002; 6: 110 117

Kontaktanschrift:
Bernd Schütze
Fachhochschule Dortmund
eMail: schuetze@medizin-informatik.org
http://www.medizin-informatik.org