

Teleradiologie per DICOM-E-Mail: Der empfohlene Minimalstandard der Deutschen Röntgengesellschaft

U. Engelmann¹⁾, B. Schütze²⁾, A. Schröter³⁾,
G. Weisser⁴⁾, M. Walz⁵⁾, M. Kämmerer²⁾, P. Mildenerger²⁾

¹⁾Deutsches Krebsforschungszentrum, Abteilung Medizinische und Biologische Informatik,
Im Neuenheimer Feld 280, 69120 Heidelberg

²⁾Johannes Gutenberg-Universität Mainz, Klinik und Poliklinik für Radiologie

³⁾CHILI GmbH, Heidelberg

⁴⁾Institut für Klinische Radiologie, Universitätsklinikum Mannheim

⁵⁾Ärztliche Stelle für Qualitätssicherung in der Radiologie, Hessen

U.Engelmann@DKFZ.de

Diese Arbeit entstand in der Arbeitsgemeinschaft Informationstechnologie @GIT der Deutschen Röntgengesellschaft (DRG).

Da es bis heute keinen Standard für die Teleradiologie gibt, hat die Arbeitsgruppe Informationstechnologie (@GIT) der Deutschen Röntgengesellschaft (DRG) eine Initiative zur Entwicklung eines Minimalstandards für die Telemedizin gegründet. Als Basis wurde E-Mail gewählt, da sich hiermit leicht Ad-hoc-Verbindungen aufbauen lassen, praktisch jedermann den Einsatz gewohnt ist und Erweiterungen einfach zu implementieren sind. Der DICOM-Standard bietet die Möglichkeit, Bilder als MIME-Attachments an E-Mails anzuhängen, und somit Bilder im Originalformat übertragen zu können. Darüber hinaus müssen die gesetzlichen Anforderungen des Datenschutzes und der Ärztlichen Schweigepflicht beachtet und implementiert werden. Die erste Empfehlung der Arbeitsgruppe wurde auf dem 85. Röntgenkongress 2004 in Wiesbaden offiziell verabschiedet. Im Rahmen des Kongresses wurde dieser Arbeit der @Roentgenpreis 2004 verliehen. Heute sind verschiedene OpenSource-Implementierungen und kommerzielle Produkte auf der Basis dieser Empfehlung verfügbar und im täglichen klinischen Einsatz.

1 Einführung

Die Teleradiologie (ohne Radiologe am Untersuchungsort) wurde in Deutschland mit der Röntgenverordnung (RöV) 2002 erstmals definiert und unter bestimmten Voraussetzungen erlaubt [1]. Betreiber von Teleradiologieeinrichtungen benötigen eine Genehmigung der Aufsichtsbehörde, wenn kein Radiologe bei Untersuchungen unter Einsatz von Röntgenstrahlen am Ort der Untersuchung anwesend ist und die Bilder für diagnostische Zwecke zu einem anderen Ort übertragen werden. Die RöV fordert Qualitätssicherungsmaßnahmen auf technischer und organisatorischer Ebene. Eine Richtlinie zur Teleradiologie soll die Details regeln. Zusätzlich arbeitet ein gemeinsamer Fachausschuß (AA4/GA4) des Normenausschusses Radiologie der Deutschen Röntgengesellschaft (NAR) und des Deutschen Instituts für Normung (DIN) unter der Federführung des Erstautors an einer Norm für die Qualitätssicherung in der Teleradiologie.

Vorhandene Telematik-Anwendungen, wie die Teleradiologie, erlauben keinen hersteller-unabhängigen Datenaustausch mit integrierten Datenschutzmaßnahmen. Es gibt je-

U. Engelmann, B. Schütze B, A. Schröter A, Weisser G, Walz M, Kämmerer M, Mildenerger P. Teleradiologie per DICOM-E-Mail: Der empfohlene Minimalstandard der Deutschen Röntgengesellschaft. Aus: Steyer G, Tolxdorf T (eds). Proceedings Telemed 2005. bit for bit - Halbzeit auf dem Weg zur Telematikinfrastruktur. Berlin: Akademische Verlagsanstalt (2005) 102-107. (ISBN 3-89838-064-5)

doch eine Reihe von herstellerabhängigen Methoden und Produkten, die zeigen, dass dies möglich ist und dass ein herstellerunabhängiger Standard sinnvoll wäre [2]. Auf dem DICOM-Workshop im Juli 2003 wurden mehrere nicht miteinander kompatible Teleradiologielösungen vorgestellt. Während der Diskussion haben sich die Autoren darauf verständigt, eine Initiative zur Etablierung eines herstellerunabhängigen Standards für die Teleradiologie in Deutschland zu gründen. Die Aktivitäten sollten unter der Schirmherrschaft der Arbeitsgruppe Informationstechnologie (@GIT) der deutschen Röntgengesellschaft (DRG) stattfinden.

2 Material und Methoden

Das erste Treffen der Initiative fand im September 2003 statt. Die Gründungsmitglieder der Initiative kamen von drei Universitäten, einer Großforschungseinrichtung, vier Firmen und der Ärztlichen Stelle für Qualitätssicherung in der Radiologie Hessen. Dabei wurde das generelle Vorgehen der Initiative festgelegt: Die Entwicklung sollte, ähnlich wie bei der IHE-Initiative (Integrating the Healthcare Enterprise), organisiert werden [3]. In einem offenen Forum aus Anwendern und Industrievertretern sollten, soweit möglich, in mehreren Entwicklungsschritten vorhandene Standards verwendet werden. In sog. *Connectathons* sollten die korrekte Implementation und die Interoperabilität zwischen den Anwendungen getestet werden [4].

3 Ergebnisse

Die Arbeitsgruppe traf sich bis zum März 2005 insgesamt achtmal, um diesen Minimalstandard zu diskutieren und festzulegen. Das Vorgehen der Gruppe war dabei praxisorientiert: Die Lösung sollte sich einfach in den vorhandenen Workflow und in die IT-Infrastrukturen der Anwender integrieren lassen und mit vorhandenen Firewall-Architekturen und Sicherheitsregeln kompatibel sein. Hierfür wurden verschiedene technische Optionen und die Erfahrungen der Mitglieder der Gruppe berücksichtigt. Das Ergebnis war, dass nur eine Lösung auf der Basis von E-Mail den einfachen Aufbau von Ad-hoc-Verbindungen erlauben würde, ohne wesentlich in die Sicherheitseinstellungen der vorhandenen Firewalls eingreifen zu müssen.

3.1 DICOM MIME Type

Die Multipurpose Internet Mail Extension (MIME) definiert, wie Multimedia-Daten an E-Mails angehängt und übermittelt werden können [5, 6]. Das Supplement 54 des DICOM-Standards (*Supplement 54: DICOM MIME-Type*) spezifiziert, wie dies im Falle von DICOM-Bildern zu erfolgen hat [7, 8]. Daher bilden das SMTP-Protokoll, das DICOM Supplement 54 und weitere Requests for Comments (RFCs) [8] die Grundlage des vorgeschlagenen Standards.

3.2 Datenverschlüsselung

In Deutschland ist es nicht erlaubt Patientendaten unverschlüsselt über öffentliche Leitungen zu übermitteln [9]. Die Initiative beschloss daher, ein Verschlüsselungsverfahren anzuwenden. Die Wahl fiel auf das OpenPGP MIME-Format, das gleichzeitig auch noch

U. Engelmann, B. Schütze B, A. Schröter A, Weisser G, Walz M, Kämmerer M, Miltenberge P. Teleradiologie per DICOM-E-Mail: Der empfohlene Minimalstandard der Deutschen Röntgengesellschaft. Aus: Steyer G, Tolxdorf T (eds). Proceedings Telemed 2005. bit for bit - Halbzeit auf dem Weg zur Telematikinfrastruktur. Berlin: Akademische Verlagsanstalt (2005) 102-107. (ISBN 3-89838-064-5)

eine Kompression der Daten nach dem zip-Verfahren erlaubt [10]. PGP ist das weltweit am häufigsten eingesetzte Programm zur Verschlüsselung und digitalen Signatur. Es ist für alle gängigen Betriebssysteme verfügbar. GPG oder GnuPG [11] ist ein frei verfügbarer Nachfolger von PGP unter der GNU General Public Licence [12]. PGP und GPG werden vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) empfohlen [13].

Die PGP-Verschlüsselung basiert auf dem sog. Public-Key-Verfahren. Hierbei gibt es einen öffentlichen und einen geheimen Schlüssel. Der öffentliche Schlüssel wird potentiellen Kommunikationspartnern zur Verfügung gestellt. Der geheime Schlüssel verbleibt immer beim Besitzer und muss streng geheim gehalten werden. Um die Authentizität des Schlüssels und deren korrekte Zuordnung zu einer bestimmten Person zu gewährleisten, werden die öffentlichen Schlüssel von Dritten digital signiert. Durch gegenseitiges Beglaubigen der Schlüssel entsteht ein sog. *Web of Trust*. Dieses erfüllt allerdings nicht die Anforderungen des Informations- und Kommunikationsdienstegesetzes, bzw. des Signaturgesetzes [14], das die Verwaltung und Beglaubigung der Signaturen durch offizielle Zertifizierungsstellen (Trustzentren) erfordert. Außerdem sind nur Signaturen von natürlichen Personen vorgesehen, haben eine begrenzte Gültigkeit, können ungültig werden und müssen mindestens über einen Zeitraum von 30 Jahren aufbewahrt werden. Diese hohen Anforderungen resultieren natürlich in sehr hohen Kosten für den Aufbau der erforderlichen Infrastruktur und schließlich für die digitalen Signaturen.

3.3 Public-Key-Infrastruktur

Durch eine Public-Key-Infrastruktur (PKI) werden die Authentizität, Identität, Vertraulichkeit und Eindeutigkeit von elektronischen Daten nach dem aktuellen Stand der Technik gewährleistet. Dafür wird eine Infrastruktur für die Verwaltung und Verteilung von digitalen Signaturen aufgebaut [15, 16]. Public-Key-Infrastrukturen sind eine wichtige Voraussetzung für die Telemedizin.

Zurzeit gibt es in Deutschland keine Strukturen, um Ärzte mit qualifizierten Signaturen auszustatten. Entsprechende Projekte für den Aufbau von elektronischen Gesundheitskarten und elektronischen Heilberufausweisen befinden sich immer noch in der Planungs- bzw. Evaluationsphase [18]. Ihre Einführung ist frühestens für Anfang 2006 vorgesehen. Experten zweifeln allerdings an der Einhaltung dieses ehrgeizigen Zeitplans [19].

Aufgrund des Fehlens einer PKI, die eine wichtige Voraussetzung für Telemedizinanwendungen ist, hat die Deutsche Röntgengesellschaft (DRG) auf dem 85. Deutschen Röntgenkongress 2004 in Wiesbaden eine PKI-Initiative gegründet. Bei Veranstaltungen der DRG zertifiziert die DRG die PGP-Schlüssel von Mitgliedern und erzeugt bei Bedarf auch neue Schlüssel. Die signierten Schlüssel entsprechen einer *fortgeschrittenen Signatur* nach dem Signaturgesetz [14]. Die öffentlichen Schlüssel sind auf einem Schlüsselserver der Deutschen Röntgengesellschaft verfügbar und können dort manuell oder automatisch abgerufen werden [20]. Dieses Vorgehen stellt eine Alternative zum Aufbau einer projektspezifischen PKI dar. Die daraus resultierenden fortgeschrittenen Signaturen entsprechen aus juristischer Sicht einem Handschlag im Alltag [11].

3.4 Nicht-DICOM-Daten

DICOM-Dateien enthalten demographische Patientendaten, organisatorische und technische Daten, um die Untersuchung und den untersuchten Patienten eindeutig zu identifizieren. Diese eindeutige und standardisierte Zuordnung ist für andere Dateien (z.B. Word-

U. Engelmann, B. Schütze B, A. Schröter A, Weisser G, Walz M, Kämmerer M, Mildner P. Teleradiologie per DICOM-E-Mail: Der empfohlene Minimalstandard der Deutschen Röntgengesellschaft. Aus: Steyer G, Tolxdorf T (eds). Proceedings Telemed 2005. bit for bit - Halbzeit auf dem Weg zur Telematikinfrastuktur. Berlin: Akademische Verlagsanstalt (2005) 102-107. (ISBN 3-89838-064-5)

Dokumente, Excel-Tabellen, PDF-Dokumente) nicht zwingend gegeben. Daher wurde ein auf dem MIME-Standard beruhendes privates Mail-Tag „X-TELEMEDICINE-STUDYID“ definiert [21]. Der Zweck dieses Tags ist die eindeutige Zuordnung einer beliebigen Datei zu einer bestimmten Untersuchung und einem Patienten. Dieses Tag wird mit der weltweit eindeutigen StudyInstanceUID der dazugehörigen radiologischen Untersuchung gefüllt. Die StudyInstanceUID selbst steht im DICOM-Header der Bilddateien. Mit dieser pragmatischen Regelung kann eine eindeutige Zuordnung zwischen DICOM und nicht-DICOM-Daten hergestellt werden. Falls es keine dazugehörige radiologische Untersuchung gibt, kann nach definierten Regeln eine unabhängige StudyInstanceUID erzeugt werden [22].

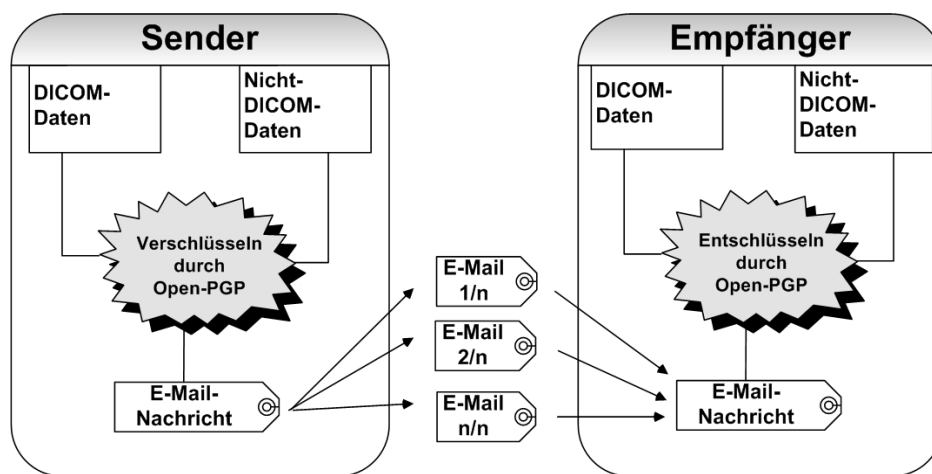


Abbildung 1: Das Prinzip von aufgeteilten, verschlüsselten DICOM-E-Mails

3.5 Aufteilung großer Datensätze

Beim Versand von umfangreichen medizinischen Bilddatensätzen per E-Mail müssen spezielle Vorkehrungen getroffen werden, denn E-Mail-Gateways begrenzen üblicherweise die Größe von E-Mails und leiten zu große Datensätze nicht weiter. Daher werden die Daten gem. dem MIME-Standard (message/partial) in mehrere Mails von akzeptabler Größe aufgeteilt (s. Abb. 1) [21].

3.6 Connectathons

Bisher haben drei Connectathons stattgefunden, bei denen sechs Softwarelösungen gegeneinander getestet wurden. Dabei mussten sieben verschiedene Szenarien mit unterschiedlichen Daten und Datenmengen durchgespielt werden. Die dabei gemachten Erfahrungen führten zu Verbesserungen in den getesteten Anwendungen und dienten der Überprüfung der entwickelten Konzepte. Die detaillierte und aktuelle Version des Standards und die Liste der Teilnehmer ist im Internet verfügbar [23].

U. Engelmann, B. Schütze B, A. Schröter A, Weisser G, Walz M, Kämmerer M, Mildnerge P. Teleradiologie per DICOM-E-Mail: Der empfohlene Minimalstandard der Deutschen Röntgengesellschaft. Aus: Steyer G, Tolxdorf T (eds). Proceedings Telemed 2005. bit for bit - Halbzeit auf dem Weg zur Telematikinfrastruktur. Berlin: Akademische Verlagsanstalt (2005) 102-107. (ISBN 3-89838-064-5)

3.7 Diskussion

Die Empfehlung, E-Mail als primäres Medium zur Übertragung von medizinischen Daten zu verwenden, kann natürlich auch kritisch gesehen werden. Die breite Verfügbarkeit und Standardisierung des E-Mail-Einsatzes sowie die Verfügbarkeit von Verschlüsselungsverfahren für vorhandene E-Mail-Clients waren die Gründe, E-Mail als beste Methode als (Minimal-) Standard für die Telemedizin zu verwenden. Zugleich stellt dieser Ansatz eine einfache Lösung für den Austausch von medizinischen Daten durch Firewalls dar, die auch für Ad-hoc-Verbindungen geeignet ist.

Heutzutage setzen viele Ärzte E-Mails ein. Dabei werden auch personenbezogene Daten übermittelt, obwohl sich die Anwender bewusst sind, dass eigentlich eine Verschlüsselung der Daten erforderlich ist. Das ist vermutlich darauf zurückzuführen, dass der Einsatz von Verschlüsselungsverfahren zu kompliziert erscheint. Die Empfehlung PGP/OpenPGP zu verwenden, das von vielen Programmen unterstützt wird und somit einfach einzusetzen ist, wird (hoffentlich) dazu führen, dass sich die Akzeptanz und der Einsatz von Verschlüsselungstechniken verbessern wird.

Der Einsatz von E-Mails und OpenPGP liegt dabei auf der Hand. Im einfachsten Fall benötigt der Empfänger einer E-Mail nach dem vorgeschlagenen Standard nichts weiter als ein E-Mail-Programm mit einem OpenPGP-Plug-in, um medizinische Bilder zu empfangen und entschlüsseln zu können. Entsprechende Plug-ins sind kostenlos für fast alle gängigen E-Mail-Clients im Internet verfügbar. Mehr Komfort bieten natürlich Workstations, in die der Versand und Empfang von verschlüsselten DICOM-Daten schon eingebaut ist. Hinweise zu entsprechenden Produkten sind auf der Homepage der Initiative zu finden [23].

Unsere Arbeit wird durch die Public-Key-Initiative der Deutschen Röntgengesellschaft (DRG) unterstützt. Die DRG agiert momentan als Trustcenter, das seinen Mitgliedern bei der Erstellung von digitalen Schlüsselpaaren hilft und die öffentlichen Schlüssel zertifiziert, solange noch keine elektronischen Heilberufsausweise, elektronische Gesundheitskarten und eine dazugehörige PKI verfügbar sind.

Somit kann schon heute jeder Radiologe sehr einfach eine digitale Signatur bekommen und diese für den spontanen telemedizinischen Datenaustausch auf der Basis des vorgeschlagenen Standards verwenden.

4 Zusammenfassung

Das vorgestellte Verfahren der verschlüsselten Datenübertragung per DICOM-E-Mail wurde nach der Erarbeitung der ersten Version von der Vollversammlung der @GIT formal verabschiedet. Auf dem Deutschen Röntgenkongress 2004 wurde diese Initiative mit dem @Röntgen-Preis der Deutschen Röntgengesellschaft ausgezeichnet. Damit liegt in Deutschland erstmalig ein Minimalstandard zum Austausch von medizinischen Bildern (und anderer Daten) vor. Auch gelegentlichen Nutzern steht damit eine preiswerte, aber dennoch sichere und standardisierte Methode der Teleradiologie zur Verfügung, die sowohl als Opensource-Lösung als auch von mehreren Firmen als Produkt angeboten wird.

Mehrere deutsche Krankenhäuser setzen diesen Standard heute bereits in der täglichen Routine ein [24].

Der beschriebene Standardisierungsprozess ist noch nicht beendet. Erweiterungen, an denen momentan gearbeitet wird, sind der Einsatz von digitalen Unterschriften der Ab-

U. Engelmann, B. Schütze B, A. Schröter A, Weisser G, Walz M, Kämmerer M, Mildner P. Teleradiologie per DICOM-E-Mail: Der empfohlene Minimalstandard der Deutschen Röntgengesellschaft. Aus: Steyer G, Tolxdorf T (eds). Proceedings Telemed 2005. bit for bit - Halbzeit auf dem Weg zur Telematikinfrastruktur. Berlin: Akademische Verlagsanstalt (2005) 102-107. (ISBN 3-89838-064-5)

sender und der Versand von Benachrichtigungsmails, die die Prüfung erfolgreich übermittelter Datenmengen, erlauben.

5 Danksagung

Die Initiative wurde teilweise aus Mitteln der Zukunftsoffensive III des Sozialministeriums Baden-Württemberg unterstützt.

6 Literatur

1. Verordnung über den Schutz vor Schäden durch Röntgenstrahlung (Röntgenverordnung - RöV). BGBl. 2003 Teil I Nr. 17 S.605, 5. Mai 2003. http://www.sidblume.de/info-rom/anl_gsi/roevo_f.htm. (2. März 2005).
2. Engelmann U, Schroeter A, Schweitzer T, Meinzer HP. The communication concept of a regional stroke unit network based on encrypted image transmission and the DICOM-Mail standard. In: Lemke HU, Vannier MW, Inamura K, Farman AG, Doi K, Reiber JHC (eds). CARS 2002. Heidelberg: Springer (2002) 612-617.
3. American College of Cardiology (ACC), Healthcare Information and Management Systems Society (HIMSS), Radiological Society of North America (RSNA): Integrating the Healthcare Enterprise IHE. <http://www.ihe.net/> (2. März 2005).
4. Mildenberger P, Kämmerer M, Engelmann U, Ruggiero S, Klos G, Runa A, Schröter A, Weisser G, Walz M, Schütze B. Teleradiologie mit DICOM eMail: Empfehlungen der @GIT. Fortschr. Röntgenstr. (2005) in print.
5. Borenstein N, Freed N. RFC 1521: MIME (Multipurpose Internet Mail Extensions) part one: Mechanisms for specifying and describing the format of Internet message bodies, September 1993. <http://www.ietf.org/rfc.html> (2. März 2005).
6. Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs), 2004. <ftp://ftp.rfc-editor.org/in-notes/rfc3461.txt> (2. März 2005).
7. DICOM Standards Committee, Digital Imaging and Communications in Medicine (DICOM). Supplement 54: DICOM MIME Type. http://medical.nema.org/Dicom/supps/sup54_pc.pdf. (2. März 2005).
8. Digital Imaging and Communications in Medicine (DICOM) - Application/dicom MIME Subtype Registration, 2004. <ftp://ftp.rfc-editor.org/in-notes/rfc3240.txt> (2. März 2005).
9. Mand E. Datenschutz in Medizinetzen. MedR 2003; 7: 393-400.
10. MIME Security with OpenPGP, 2004. <ftp://ftp.rfc-editor.org/in-notes/rfc3156.txt> (2. März 2005).
11. The International PGP Home Page, 2004. <http://www.pgpi.org/> (2. März 2005).
12. GNU General Public License, 2004. <http://www.gnu.org/copyleft/gpl.html> (2. März 2005).
13. Bundesamt für Sicherheit in der Informationstechnik - Einsatz von GnuPG oder PGP, 2004. <http://www.bsi.de/gshb/deutsch/m/m05063.html> (2. März 2005).
14. Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste. <http://www.netlaw.de/gesetze/iukdg.htm> (2. März 2005).
15. He Q, Sycara K, Su Z A Solution to Open Standard of PKI. LNCS 1998; 1438: 99-110.
16. Kent St. Rethinking PKI: What's Trust Got to Do with It? LNCS 2002; 2332: 398-399.
17. Brandner R, van der Haak M, Hartmann M, Haux R, Schmücker P. Electronic Signature for Medical Documents – Integration and Evaluation of a Public Key Infrastructure in Hospitals. Methods Inf Med 2002; 41: 321-330.
18. Deutsches Institut für Medizinische Dokumentation und Information DIMDI. eHealth. <http://www.dimdi.de/de/ehealth/> (2. März 2005).
19. Die Komplexität wird unterschätzt – Stellungnahme der Verbände und Fachgesellschaften zur IT im Gesundheitswesen. Krankenhaus Umschau 2004; 73(6): 484-485.
20. Keyserver der DRG, 2004. <http://www.radiologie-informatik.de/keyserver/> (2. März 2005).

U. Engelmann, B. Schütze B, A. Schröter A, Weisser G, Walz M, Kämmerer M, Mildenberge P. Teleradiologie per DICOM-E-Mail: Der empfohlene Minimalstandard der Deutschen Röntgengesellschaft. Aus: Steyer G, Tolxdorf T (eds). Proceedings Telemed 2005. bit for bit - Halbzeit auf dem Weg zur Telematikinfrastruktur. Berlin: Akademische Verlagsanstalt (2005) 102-107. (ISBN 3-89838-064-5)

21. Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types, 2004. <ftp://ftp.rfc-editor.org/in-notes/rfc2046.txt> (2. März 2005).
22. Medical Connections Home Page – Free UID Request, 2004. http://www.medicalconnections.co.uk/html/free_uid.html (2. März 2005).
23. @GIT Initiative zur Standardisierung von Telemedizin, 2004. <http://www.tele-x-standard.de> (2. März 2005).
24. Das Teleradiologie-Projekt Rhein-Neckar-Dreieck, 2004. <http://www.teleradiologie-rnd.de/> (2. März 2005).

U. Engelmann, B. Schütze B, A. Schröter A, Weisser G, Walz M, Kämmerer M, Mildenberge P. Teleradiologie per DICOM-E-Mail: Der empfohlene Minimalstandard der Deutschen Röntgengesellschaft. Aus: Steyer G, Tolxdorf T (eds). Proceedings Telemed 2005. bit for bit - Halbzeit auf dem Weg zur Telematikinfrastuktur. Berlin: Akademische Verlagsanstalt (2005) 102-107. (ISBN 3-89838-064-5)