Eur Radiol (2006) 16: 753–758
DOI 10.1007/s00330-005-0019-y

G. Weisser
M. Walz
S. Ruggiero
M. Kämmerer
A. Schröter
A. Runa
P. Mildenberger
U. Engelmann

Standardization of teleradiology using Dicom-e-mail: recommendations of the German Radiology Society

Received: 1 June 2005
Revised: 29 July 2005
Accepted: 23 August 2005
Published online: 15 October 2005

G. Weisser (✉) · S. Ruggiero · A. Runa
Department of Clinical Radiology,
University Hospital Mannheim,
Theodor-Kutzer-Ufer 1-3,
68167 Mannheim, Germany
e-mail: gerald.weisser@rad.ma.uni-heidelberg.de

M. Walz
Medical Office for Quality Assurance in Radiology,
Hessen, Germany

M. Kämmerer · P. Mildenberger
Department of Radiology,
Johannes Gutenberg University Mainz,
Mainz, Germany

A. Schröter
CHILI GmbH,
Heidelberg, Germany

U. Engelmann
Division of Medical and Biological Informatics,
German Cancer Research Center,
Heidelberg, Germany

Abstract Until recently there has been no standard for an interoperable and manufacturer-independent protocol for secure teleradiology connections. This was one of the main reasons for the limited use of teleradiology in Germany. Various teleradiology solutions have been developed in the past, but the vast majority have not been interoperable. Therefore an ad hoc teleradiology connection was impossible even between partners who were already equipped with teleradiology workstations. Based on the evaluation of vendor-independent protocols in recent years the IT Working Group (AGIT) of the German Radiology Society set up an initiative to standardize basic teleradiology. An e-mail based solution using the Dicom standard for e-mail attachments with additional encryption according to the OpenPGP standard was found to be the common denominator. This protocol is easy to implement and safe for personalized patient data and fulfills the legal requirements for teleradiology in Germany and other countries. The first version of the recommendation was presented at the 85th German Radiology Convention in 2004. Eight commercial and three open-source implementations of the protocol are currently available; the protocol is in daily use in over 50 hospitals and institutions.

Keywords Teleradiology · Telemedicine · Internet · E-mail · Dicom · OpenPGP

Introduction

Teleradiology applications are in use worldwide for the exchange of medical images and-in many cases-of other clinical data. These applications use a variety of protocols, for example, Dicom, HTTP, FTP, and vendor-dependent protocols and security measures, to ensure image quality and data security. Additional functions including screen synchronization and interactive mouse control can ease applications such as teleconferences.

Until recently no international or German national standard existed for an interoperable and manufacturer independent protocol for secure teleradiology connections. The otherwise successful initiative of Integrating the Healthcare Enterprise (IHE) has also not yet provided a profile for teleradiology services (http://www.ihe.net/Resources/index.cfm#profiles). This is one of the main reasons for the lack of a widespread use of teleradiology in Germany.

Various teleradiology solutions have been developed, the vast majority of which are vendor dependent (e.g., [1–6]).

Establishing an ad hoc teleradiology connection (secure image transfer within several hours between previously unknown partners) has therefore almost always been impossible even with partners already equipped with teleradiology workstations. Initial attempts at standaridizing teleradiology in Germany were undertaken in an early phase of teleradiology by the Information Technology Working Group (AGIT) of the German Radiology Society (DRG) and by the Zentralverband Elektrotechnik-und Elektronikindustrie (ZVEI) in 1998 [7], before IHE was established. This did not lead to the recommendation of a specific protocol. The first use of e-mail in combination with radiological image transfer in Germany was reported in 1997 [8]. Since 2002 two projects financed by public funds in the German states of Rheinland-Palatinate and Baden-Württemberg have tested the use of vendor independent teleradiology protocols across a wide spectrum of applications, even for emergency teleradiology [9].

There are three major applications for teleradiology in European countries, each with its own technical requirements [10]:

- Consultations: emergency consultations such as neurosurgery and neurology, expert consultations in special areas such as pediatric radiology and neuroradiology
- Clinical communication and cooperative work: teleconferencing, teledemonstrations with the use of combinations of images and other datalike reports, aid of computer assisted therapy, cooperative work between radiology departments of different clinics, teleguided examinations, etc.
- Other applications: education, access to reference databases, scientific cooperation, product maintenance, external archiving, etc.

Specific types of teleradiology services are regulated in Germany by the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (RöV 1987, Verordnung über den Schutz vor Schäden durch Röntgenstrahlen, last changed on 30 April 2003; http://bundesrecht.juris.de/bundesrecht/r_v_1987/gesamt.pdf): Teleradiology operators require a permit from the authorities when no accredited radiologist is present at the time and location of the radiological examination if radiography is used. The regulation requires a number of quality management measures at the technical and organizational levels. Additionally, a working group of the Radiology Standards Committee (NAR, Normenausschuss Radiologie), a cooperative of the German Institute for Standardization (DIN, Deutsches Institut für Normung), and the DRG is working on a national standard for quality assurance in teleradiology.

The present regulations in Germany, the increasing demand on modern diagnostic imaging modalities, and the lack of experienced radiologists led to a growing number of institutions interested in these teleradiology services in recent years.

Several successful applications with legacy-free protocols were presented at a national Dicom workshop in Mainz, Germany, in July 2003 (http://www.uni-mainz.de/FB/Medizin/Radiologie/agit/berichte/dicom2003) [9]. Due to the protocol details these applications were still not interoperable. The participants agreed that an initiative to create a vendor-independent minimum standard for teleradiology in Germany would be very helpful. This became a task of the AGIT, German Radiology Society. The first results have been published in German [11]. This contribution describes the results of years 1 and 2 of the initiative.

Materials and methods

Eight working group meetings were organized between September 2003 and February 2005. The participants at the initial meeting in Mainz came from four universities, one national research center, four companies, and the Medical Office for Quality Assurance in Radiology of the German state of Hessen. By 2005 three other companies and one other university had joined the working group (http://www.tele-x-standard.de/html/mitglieder.html). Three connectathons (similar to the IHE connectathons; http://www.ihe.net/Resources/index.cfm#connectathon) were organized to reassure interoperability, the first one taking place in January 2004 in Mannheim. An online connectathon for testing connections to various vendors without the need of personal presence was organized in addition.

During the decision-making process additional experts from companies and universities were invited to discuss and clarify specific topics of the communication and standards (e.g., from OFFIS, Oldenburg, and from the GnuPG working group in Germany). Major companies were informed about the activities in the early phase and invited to join the group. The results of all meetings were published over a mailing list which was open to active and passive members of the working group. These mailings included the request for comments to specific parts of the protocol.

Results

At the first meeting in September 2003 the discussion led to the following consensus:

- The working group will try to find the common denominator for teleradiology connections with basic functionality (sending and receiving of images and related clinical data).
- The recommendation must comply with all applicable national and international laws about data security.
- The recommendation must be based on international standards.
- The recommendation must contain only legacy-free protocols and software.

- The solution must be easy to integrate in different workflows and IT settings.
- Adding a communication partner should be easy.
- Interoperability should be tested in connectathons.
- Advanced functions such as teleconferences, screen synchronization, and mouse control will be discussed in later versions.
- Web-based viewing will be discussed in later versions.
- The recommendation will not address specific organizational or workflow definitions.

Communication protocol

During the second meeting in November 2003 various technical solutions were discussed, including e-mail, SSH, SFTP, scp, TLS, VPN, and Dicom additions. Participants agreed that the e-mail protocol would be ideal for establishing ad hoc connections and would cause minimal problems with existing firewall policies at the major hospitals. Present knowledge regarding e-mail encryption and security in hospital administrations should minimize the efforts during installation and configuration. According to German law, electronically transfered patient data must be encrypted and signed (http://bundesrecht.juris.de/bundesrecht/r_v_1987/gesamt.pdf; http://bundesrecht.juris.de/bundesrecht/bdsg_1990/gesamt.pdf). The available algorithms (recommended cryptoalgorithms by the regulatory authority for telecommunications and post: http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/198.pdf) and solutions for encrypted e-mail communication as recommended by the Federal Office for Information Security in Germany are the OpenPGP standard and the S/MIME standard (Federal Office for Information Security in Germany, 2005, IT Baseline Protection Manual, p 5.63, Use of GnuPG or PGP; http://www.bsi.bund.de/english/gshb/manual/s/s05063.html; S/MIME: http://www.bsi.bund.de/english/gshb/manual/s/s05110.html). Due to the multiplatform availability and good interoperability the OpenPGP implementations PGP and GnuGP were chosen to for the beginning.

The following protocol was accepted unanimously:

- Basic protocol is an e-mail communication with additional encryption and signature.
- The mail client must support the MIME standard (RFC 2045/2046), multipart e-mail, message partial and the use of X-tags.
- The encrypted variants of the SMTP and POP3/IMAP4 protocols should be used.
- Dicom objects must be integrated as MIME attachments according to the Dicom Supplement 54 (http://medical.nema.org/Dicom/supps/sup54_pc.pdf).
- The encryption must be according to the OpenPGP standard using RFC2440 and RFC3156. Encryption methods with a MUST status in the standard must be used.
- Clients can send signed e-mails; clients must be able to receive signed e-mails (inline and detached signatures).
- The clients are not obliged to check the signature; they can ignore it.

This basic protocol was evaluated in the first connectathon in January 2004 with five different clients. After initial problems and some corrections interoperability was achieved between all five clients. In the following meetings and connectathons the following protocol addition was made:

- The built-in zip compression of the OpenPGP implementations should be used; no other compressions must be used for the attachments

Integration of non-Dicom data

The use of the e-mail protocol facilitates the integration of other types of data such as PDF documents, JPEG images, and text files. These file types can be attached to e-mail and are classified by their MIME type. Unfortunately, there is no standardized way to add patient information such as name and birthdate to these non-Dicom file types. Since the presented communication protocol is used mainly for teleradiology, a Dicom image is added to a patient data set in most of the cases. The Dicom header contains most of the relevant patient data, including name, birthdate, and patient identification number. Therefore a simple and convenient way to bind a series of data files together would be the existence of a common ID for all data files belonging to the same patient. This method can be used in a multipart message as well as with multiple e-mails with single attachments.

The working group established a private MIME tag, according to the MIME standard, to be used as a common ID. This ID should be set to the Study Instance UID of one of the related Dicom images. If no related Dicom image is present, the ID must be generated with a valid process similar to Dicom UIDs to reassure its uniqueness. A unique enterprise number can be ordered free of charge, if needed (Internet Assigned Numbers Authority, IANA; IANA-MIB@iana.org):

- All types of attachments are allowed as long as they represent a valid MIME type.
- Non-Dicom MIME types should contain a private tag "X-telemedicine-study ID"
- The tag must be the Dicom Study Instance UID from one of the corresponding Dicom images if such an image is part of the message
- If no Dicom image is present in the message, the tag must be created in a process to reassure its uniqueness.

Figure 1 summarizes the message format. The current version of the white paper is available at http://www.tele-x-standard.de.

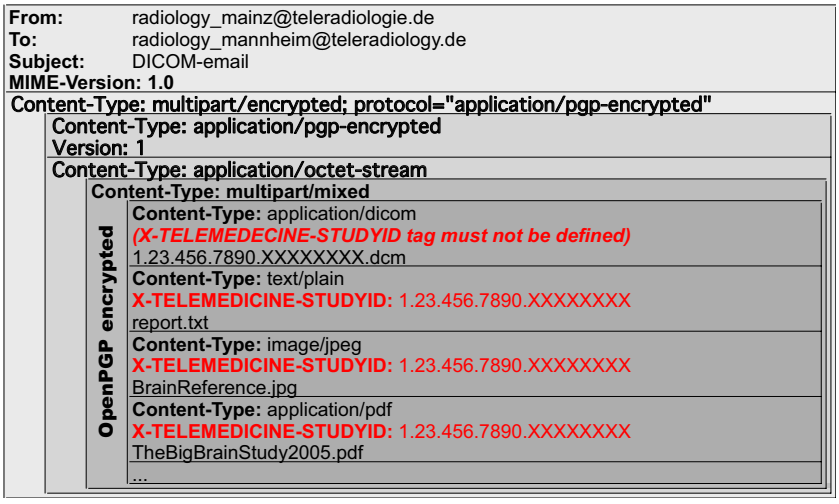

Fig. 1 Transfer syntax for data transfer of DICOM and non-DICOM data using e-mail

Key management and the AGIT key server

GnuPG and PGP create and use public and private keys in the form of pairs of keys. A message that has been encrypted with a public key or signed with the private key can only be decrypted with the corresponding private key or verified with the originator's public key. The public key can be revealed to anyone. Its purpose is to encrypt messages sent to the owner of the private key. To provide proof of unauthorized tampering and hence to protect messages against modification GnuPG and PGP use the originator's private key to calculate a cryptographic checksum for the message—the digital signature. Using the public key belonging to the message originator, every communication partner can determine whether the cryptographic checksum at the end of the message is valid or whether the message has been modified without authorization. To ensure security separate keys are usually used for encrypting and for digitally signing files. When using GnuPG or PGP it is advisable to use a combination of the two functions described above. To maximize security messages and files should generally first be signed with the sender's private key and then encrypted with the recipient's public key (http://www.bsi.bund.de/english/gshb/manual/s/s05063.html).

As yet there is no official Public Key Infrastructure (PKI) for health professionals in Germany, as in many other countries. Therefore the generation of key pairs for individual persons or groups is needed before any encryption and signature can be used. Local administrators can store their private keys and hand out the public keys to their communication partners. If used for ad hoc connections, the public keys must be exchanged beforehand. To ease the use of encryption and electronic signatures the German Radiology Society (DRG) built a PKI for members and interested individuals in 2004. This service is managed by the AGIT of the DRG with the help of the University Hospital in Mainz (http://www.radiologie-informatik.de/keyserver/). To date 150 signatures have been generated for individuals and institutions. The service can be used free of charge. The generated key pairs are signed with the root key of the DRG and are named and handed out after the check of an official ID (e.g., passport). Therefore a communication partner can check the validity of the received public key by checking the DRG signature. This method does provide a higher level of security since a tampered public key can be easily detected and can therefore be helpful in legal affairs. Nevertheless it does not reach the level of a qualified signature as defined by German law (Signaturgesetz SigG 2001; http://jurcom5.juris.de/bundesrecht/sigg_2001/gesamt.pdf), which follows the corresponding European regulations (99/93/EG, 99/93/EG; http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/esignatures_de.pdf).

Discussion

A wide range of protocols are presently in use for the purpose of secure teleradiology connections. The use, for example, of Virtual Private Networks (VPNs) in combination with Dicom transfers or the use of encrypted protocols such as https to access a common web server can provide data security for the transmission of patient data. For a given group of partners either of these solutions can be used to set up a reliable and secure network. Problems may occur if some partners are part of multiple networks or if ad hoc communications are needed. The use of VPNs will require the help of administrative staff on both sides for the time-consuming setup of a new connection. The use of a central server with https access helps to overcome this problem, but partners with different network connections may encounter problems integrating multiple user interfaces in their workflow. In addition, the use of one central server for data storage of different partners can lead to organizational problems.

The use of the communication protocol with encrypted e-mails as presented here can overcome many of these problems. The integration of the encrypted e-mail protocol into different workflows is currently evaluated in six teleradiology projects in the state of Baden-Württemberg [12, 13] (M. Walz, 2004, "Teleradiologieprojekte in Baden-Württemberg-Interoperabilität für die Notfallversorgung. 9. Sozialkonferenz: 4 Motoren für Europa"; http://www.sozialministerium.baden-wuerttemberg.de/sixcms/media.php/1442/Tagungsunterlagen%20der%209.%20Sozialkonferenz.pdf). These projects use four different communication protocols and different concepts for the integration into their HIS, RIS, and PACS environments. These efforst have already proved technically successful, and initial clinical results are expected at the end of 2005.

The protocol can be used for a variety of applications. Once the initial setup is completed, adding a new communication partner is simple and fast. The protocol allows the fully automated integration in a Dicom-based workflow with the use of Dicom e-mail converters; data can be sent and received with the standard Dicom workstation, modality, or PACS. Server-based gateways can forward other contents such as PDF and JPEG to specialized viewing applications or to the internal mailing system. Several commercial workstations with a multimedial integration of various filetypes and the support of the presented protocol are already available (http://www.tele-x-standard.de/html/mitglieder.html). The protocol can be used with a standard ADSL internet connection for receiving patient data at home, for example, for on-call services. Integration into telemedicine projects is easily achieved due to the well documented interface and simple protocol specifications.

Interoperability was one of the crucial points of the protocol. The use of connectathons similar to that in the IHE approach led to excellent interoperability and stability of all tested clients. The current status of the interoperability based on the tested systems can obtained online (http://www.tele-x-standard.de/html/connect/connect.html).

The protocol must be regarded as a national German standard for basic teleradiology, one which can also be used for demanding teleradiology applications such as emergency teleradiology. The national approach was chosen as the first step toward establishing an international standard. The transfer of this national standard into an IHE profile for teleradiology connections is one of the goals of year three of the initiative.

In contrast to our recommendation of the OpenPGP standard, both the Dicom framework and the IHE initiative chose the S/MIME encryption and signature standard. The reason for chosing OpenPGP was the interoperability problems of various S/MIME implementations in the past and the excellent interoperability and platform independence of the GnuPG and PGP tools. Current developments of the GnuPG tools support both standards OpenPGP and S/MIME. Therefore the use of both standards might be possible in future versions of the recommendation with minor additions, when stable versions of the tools are available. This will certainly ease the migration to an IHE compatible profile.

The use of e-mail with the Internet environment may cause instability due to spam mails, viruses, and worms spread over e-mails. When used for emergency teleradiology, additional measures are necessary to prevent malfunctions in the systems. However, the use of simple measures such as dedicated mail servers, SMTP authentication, and direct SMTP connections without mail relays have proven to be very reliable in routine clinical use of that protocol for more than 2 years [9, 12]. Even using these measures the protocol is not limited to the regional or national use; partners in the Middle East, the United States, and India have been integrated without problem. Special care must be taken to ensure the blocking of all executable e-mail content. No available clients execute any e-mail attachment. In 3 years of clinical use of this protocol and more than 400,000 e-mails transferred between the hospitals we have not encountered a single spam, virus, or worm e-mail.

The integration of non-Dicom data such as PDF and JPEG into the Dicom standard itself is in progress. Nevertheless the universal approach for the integration of all attachable formats in the presented protocol does not interfere with these attempts, since both possibilities can coexist without problems if the X-tag is defined.

Conclusion

The presented protocol for the use of Dicom e-mail in teleradiology establishes a national standard for basic teleradiology in Germany. It is easy to implement and allows a secure and legal use of Internet services for the worldwide transfer of personalized patient data. It can be used for a variety of applications, mainly for teleconsulation and, with technical supplements, even for demanding applications such as emergency teleradiology, but does not include teleconference functions.

Within 12 months the protocol obtained the support of eight companies, and three open-source implementations are available (http://www.tele-x-standard.de/html/mitglieder.html). Interoperability of these clients was successfully tested in 3 connectathons.

The protocol is in daily use in over 50 installations (Teleradiology Project of the Rhein-Neckar-Region; http://www.teleradiologie-rnd.de). It is currently being used for emergency teleradiology, second opinion, telework, and scientific communication.

Further additions with the support of notify mails, the access of clinical data over https, and other topics are planned for the next year of the initiative. The development of an IHE profile is a goal for the near future. The working group is open to all interested individuals, companies, and

organizations, and cooperation with international partners is welcome.

Acknowledgements This work was supported in part by the Zukunftsoffensive III of the Social Ministry of the state of Baden-Württemberg, Germany.

References

1. Engelmann U, Schroter A, Baur U, Werner O, Schwab M, Muller H, Bahner M, Meinzer HP, Boralv E, Goransson B (1998) The German teleradiology system MEDICUS: system description and experiences in a German field test. Eur J Radiol 26: 219–225
2. Stoger A, Giacomuzzi SM, Strohmayr W, Dessl A, Springer P, Buchberger W, Jaschke W (1996) Establishment of an emergency CT service by means of Teleradiology. Rofo-Fortschr Geb Rontgenstr Neuen Bildgeb Verfahr 165:520–523
3. Walz M, Bolte R, Lehmann KJ, Lutgemeier J, Georgi M (1999) Economic analysis of teleradiology applications with KAMEDIN. Stud Health Technol Inform 39:208–216
4. Engelmann U, Schwab M, Schröter A, Rusu P, Meinzer HP (2002) Evaluation of the CHILI teleradiology network 4 years after clinical implementation. Radiologe 42:87–93
5. Lienemann B, Hodler J, Luetolf M, Pfirrmann CW (2005) Swiss teleradiology survey: present situation and future trends. Eur Radiol (DOI: 10.1007/s00330-005-2764-3)
6. Boehm T, Handgraetinger O, Link J et al (2004) Evaluation of radiological workstations and web-browser-based image distribution clients for a PACS project in hands-on workshops. Eur Radiol 14:908–914
7. Walz M, Mildenberger P, Klose KJ (1999) Standardized image transmission: an important step in the direction of teleradiology and telemedicine. Radiologe 39:M77–M79
8. Ricke J, van der Donk E, Wolf M, Ostendorf, B, Hosten N, Zielinski C, Liebig T, Stroszczinski C, Lopez Hanninen E, Lemke AJ, Gillessen C, Gurvit O, Amthauer H, Kleinholz L, Bartelink H, Felix R (1997) Second opinion in online radiology via Internet: report on implementation and analysis of reliability of findings in sectional images. Aktuelle Radiol 7:50–55
9. Weisser G, Walz M, Koester C, Dinter D, Düber C (2002) New concepts in teleradiology with Dicom e-mail. Biomed Tech 47(Suppl 1):356–359
10. Walz M, Brill C, Bolte R, Cramer U, Wein B, Reimann C, Haimerl M, Weisser G, Lehmann KJ, Loose R, Georgi M (2000) Teleradiology requirements and aims in Germany and Europe: status at the beginning of 2000. Eur Radiol 10:1472–1482
11. Mildenberger P, Kämmerer M, Engelmann U, Ruggiero S, Klos G, Runa A, Schröter A, Weisser G, Walz M, Schütze B (2005) Teleradiologie mit DICOM E-Mail: Empfehlungen der @GIT. Rofo-Fortschr Geb Rontgenstr Neuen Bildgeb Verfahr 177:697–702
12. Engelmann U, Schroeter A, Schweitzer T, Meinzer HP (2002) The communication concept of a regional stroke unit network based on encrypted image transmission, the DICOM-Mail standard. In: Lemke HU, Vannier MW, Inamura K, Farman AG, Doi K, Reiber JHC (eds) CARS 2002. Springer, Berlin Heidelberg New York, pp 612–617
13. Engelmann U, Münch H, Schröter A, Meinzer HP. Jäckel A (ed) (2004) Von der bilateralen Teleradiologie zur Vernetzung von Regionen: der CHILI-Ansatz. Telemedizinführer Deutschland, Ausgabe 2005. Deutsches Medizin Forum, Ober-Mörlen, pp 265–269