CARS 2002 – H.U. Lemke, M.W. Vannier; K. Inamura, A.G. Farman, K. Doi & J.H.C. Reiber (Editors)

The communication concept of a regional stroke unit network based on encrypted image transmission and the DICOM-Mail standard

Engelmann U[a], Schroeter A[a], Schweitzer T[b], Meinzer HP[a]

[a] German Cancer Research Center, Division Medical & Biological Informatics
Im Neuenheimer Feld 280, D-69120 Heidelberg, Germany
Mailto: U.Engelmann@DKFZ-Heidelberg.de
[b] Steinbeis-Transferzentrum Medizinische Informatik, Im Neuenheimer Feld 517,
D-69120 Heidelberg, Germany, URL: www.chili-radiology.com

Abstract

This paper describes the communication concept for a regional stroke network for the exchange of medical images and reports. The data transfer is realized with regular e-mail (SMTP). DICOM images are sent as DICOM compliant attachments. Private key encryption is used to ensure data security and privacy. All used protocols are standardized or de-facto standards and allow vendor-independent communication. Different problems and options of the concept realization are discussed.

Keywords: Teleradiology, DICOM, Security, SMTP, Stroke

1. Introduction

Time is one of the most important factors in the diagnosis, therapy and prognosis of apoplexy or stroke (time is brain!). The German federal state Rhineland-Palatinate (Rheinland-Pfalz) took the political decision to support the establishment of a state-wide competence network. The main purpose is to enable fast and reliable distribution of medical images for the purpose of stroke diagnosis and therapy.

The first step is establishing (and funding) of a pilot network connecting the referring hospitals in Neustadt and Worms with the competence centers in Ludwigshafen and Mannheim. Basic requirements have been defined in the request for proposals (RFP) which was organized by a health care consultant company (Pergis, Ludwigshafen, Germany) and a group of subcontracted teleradiology experts. Key requirements of the RFP were the following:

Full DICOM compliance for the exchange of data with imaging modalities. Storage of data in databases, advanced functions for the display and analysis of medical images from different modalities. This means, that not a dedicated special purpose communication system, but an integrated system was required.

The standard data transfer should be realized via E-Mail (SMTP) and the new DICOM supplement 54. The main reason for that was that e-mails can be sent through firewalls without any changes in their rule-sets. Another reason was the availability of standard encryption methods for e-mail.

The system should support autorouting and the automatic protocol conversion between DICOM and SMTP. All transmitted data must be encrypted. All communication channels must work with existing and future firewall solutions without security reductions.

Several teleradiology and PACS vendors submitted proposals. The selection process was based on the presentation of the solution and proof of concept with software demonstrations. The winner was the Steinbeis Transferzentrum Medizinische Informatik, a technology transfer company in Heidelberg, Germany, with a dedicated software architecture based on their CHILI (tele-) radiology product family.

2. Method

CHILI is a radiological workstation with powerful teleradiology functionality, supporting various protocols and de-facto standards for image distribution and interactive teleconferencing of medical images [1]. One important feature of the system is its security concept and the implemented data protection measures based on symmetric and public key encryption [2].

One of the supported transfer protocols is SMTP (simple mail transfer protocol). Thus, users can submit medical images and additional data as regular e-mails. They can also receive data in different formats (DICOM, JPEG, GIF, etc.) from communication partners who can submit images as attachments from a plain mail client only.

Most of the requested functionality of the RFP was already available in the CHILI software. Some additional features had to be implemented for the project, such as the automatic encryption/decryption of mails, and automatic protocol conversions between DICOM/SMTP. Data security measures, key management based on public key encryption and open standards have been implemented. The flexible protocol conversion to and from e-mail allows easy extension of the teleradiology network to other data types
and can provide the basis for a general telemedicine network.

3. Main concepts

The principle components of the network are shown in figure 1. Referring hospitals (without expertise in neuroradiology, neurology and neurosurgery) are equipped with one or several CHILI workstations (PCs running Linux). One is acting as a CHILI server and the other are CHILI clients. The server receives the images from the imaging modalities (e.g. CT), PACS or a DICOM workstation via DICOM protocol [3]. The server stores the data in a relational database. The CHILI clients are connected to this database and can view and process the stored data. Teleconferences between all CHILI workstations are possible.

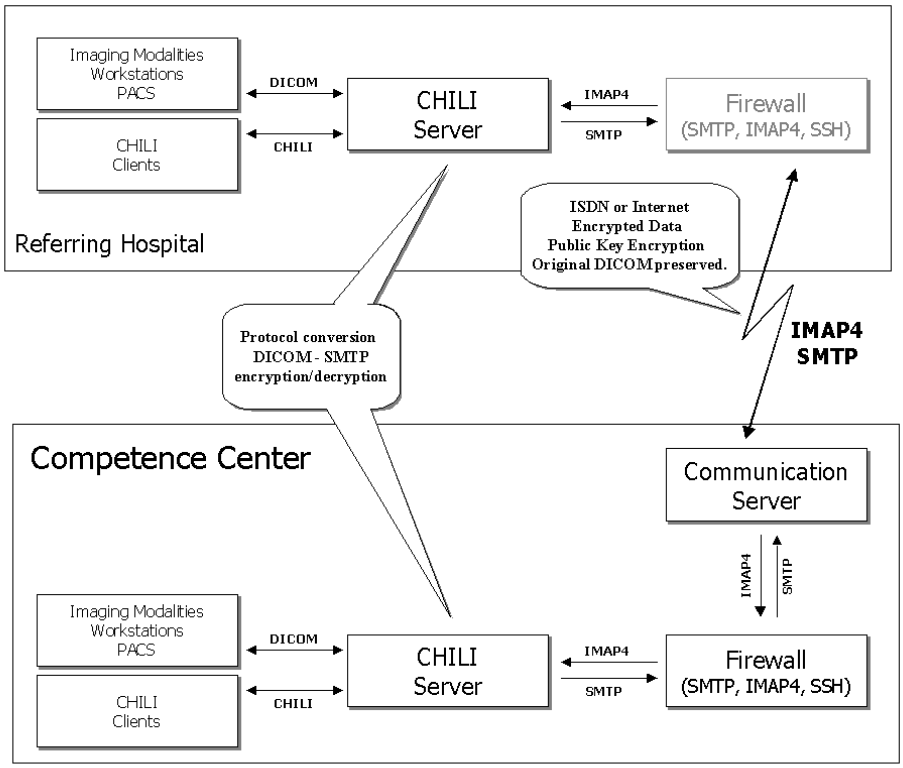

Figure 2. Protocols between the components

The data is submitted to the competence centers via e-mail, using the *Simple Mail Transfer Protocol* (SMTP) [4, 5]. The first versions of SMTP could only transfer 7-bit text messages. The *Multipurpose Internet Mail Extensions* (MIME) allows the transmission of multipart messages with many kinds of data [6]. The DICOM standard defines in supplement 54 the *DICOM MIME Type* [7]. This allows to transmit medical images via e-mail in a standardized way.

As DICOM images do contain patient data, it is not allowed (by different national and international laws) to transmit the data as clear text over unprotected communication lines. Thus, data protection measures have to be taken into account. One of the implemented methods of our communication concept is to encrypt and sign the mails, resp. parts of it. Galvin et al. define in RFC 1847: *Security Multiparts for MIME* how parts of e-mail can be signed and encrypted [8]. We used *MIME Security with OpenPGP* for the realization [9, 10]. The data is signed with the private key of the submitting person to protect authenticity and integrity of the data. The public key of the receiver is used to encrypt the data [2].

We have to take into account that we are submitting large amounts of data. The mail gateways usually limit the size of mails which are processed. Thus, all data is splitted into several mails of acceptable size automatically.

The submission process can be activated either by a user or automatically by a so-called autorouter. Different rules can be defined how and to whom the data should be sent and when. A problem is that no user is sitting at the workstation when data is sent automatically. This means that the submitted data cannot be signed by a person. Thus, we use a private key of the workstation (or institution) to create the signature of the data which protects authenticity and integrity of the data.

The transmission starts when the DICOM data has been converted into a set of encrypted e-mails. The CHILI server of the referring hospital (see figure 1) sends the data out to the external network (ISDN or Internet) over an optional firewall. The SMTP port of the firewall is usually open for data exchange.

The communication server at the competence center receives and temporary stores the incoming data from the referring hospitals. Usually, this server is located outside the hospital LAN in front of a firewall. The teleradiology servers inside the competence centers (behind the firewall) fetch the data periodically via IMAP from the communication server [11].

The fetched data is removed from the communication server and decrypted and re-converted into standard DICOM files and stored in the database of the local CHILI server. Visible and audible alarms inform the personnel of new incoming data which can be reported directly with the viewer of the CHILI workstation (client or server). The autoroutes can be configured to forward the data to one or several other workstations in the competence center. DICOM workstation can also query and retrieve data from the CHILI server.

Results and other information can easily be replied to the sender of the data via the user interface of the CHILI program. The digital signature of the reporting physician is used to ensure the authenticity of the report. The replies are again sent as encrypted e-mails to the communication server in front of the firewall. The CHILI server of the referring hospital is then fetching the answer and integrates the report into the local database where it is stored and viewed with the related series of the image data.

It is very important is to control the completeness and correctness of the data transfers. All transfers are logged at both sites. Furthermore, sender and receiver can see the progress of the data transfer. A meta-protocol has been implemented on top of SMTP for reliable and secure transfer of confirmations (logging!) and possible failure repair measures, such as autorouting to another competence center. Automatic fail over between the communications servers at different locations has been implemented in this way.

The realized CHILI system is not only a dedicated emergency tool. But also a radiological workstation which can be used for reporting in daily routine. Additional clients can be connected to the server if necessary. All clients can perform interactive teleconferences in-

house without the need of sending the data to the other workstation. Other options, such as long term archiving, distribution of images in the intranet, mobile clients, or 3D visualization modules [12,13] can be integrated into the "emergency system" easily.

4. Discussion

The system has been implemented as described. It is an open concept and based on standards. This ensures the data exchange with other systems. Nevertheless, there were from time to time several options possible. We used OpenPGP for the data encryption. An alternative to this was S/MIME [14]. We choose OpenPGP because it is at the current state easy to implement and as it was as popular as S/MIME. But the latter will be implemented later (see below).

Autorouting of data speeds up the transmission from the modality to the competence center. A limitation of this approach is, that the data is then signed by a machine with a machine signature instead of a person. We think that this is acceptable.

Another problem is when many people can be the receiver of the data. This means that the sender has to know the name of the person at the other side.

Currently, all public signatures are distributed by the CHILI system itself. The private keys are stored at the workstation and activated by a pass-phrase. The system is prepared to use digital signatures on cards, such as a health professional card. It is not yet clear which trust center will be chosen as provider for the certified signature cards. The price of the signatures is an important issue as a university hospital would need about 20-30 cards for the radiology department only. A budget has not been foreseen for this so far.

The *Sphinx project* launched by German authorities (BSI) aims to improve secure email exchange. The projects technological base is the protocol *TeleTrust e.V. MailTrusT Version 2*. This includes the standards S/MIME, X.509v3 and others [15]. Proprietary products are already on the way, but with the *project Ägypten* there is now also a Free Software solution going to be realized for popular mail user agents [16]. The integration of this software into our architecture is planned as well.

The aim of the *GNU Privacy Project* is to develop free encryption software for everybody [17]. This project is supported by two German ministries (Bundesministerium für Wirtschaft und Technologie and Bundesministerium des Inneren). It is planned to integrate the resulting free software tool *GNU Privacy Guard* as well into our realized infrastructure to achieve as much interoperability as possible.

5. Conclusion

The realized teleradiology network meets the requirements of the RFP for the stroke unit network. The network can easily be extended and scaled. Redundancy of all critical system components provides high availability.

The data security concept and flexible protocol conversion allow an easy extension of the teleradiology network to other data types. They can provide the basis for a general telemedicine network.

Acknowledgements

The pilot project *Teleradiology (Stroke-Unit in Rheinland-Pfalz)* is funded by the *Ministerium für Arbeit, Soziales, Familie und Gesundheit* in Mainz, Rheinland-Pfalz, Germany.

References

1. Steinbeis-Transferzentrum Medizinische Informatik. CHILI: Second Generation Teleradiology and Telecardiology. http://www.chili-radiology.com/.
2. Baur HJ, Engelmann U. Saurbier F, Schröter A, Baur U, Meinzer HP. How to deal with Security and Privacy Issues in Teleradiology. Computer Methods and Programs in Biomedicine, 53, 1 (1997) 1-8.
3. NEMA Standards Publication PS 3.1-15. Digital Imaging and Communications in Medicine (DICOM). National Electrical Manufacturers Association, 2101 L Street, N.W., Washington, D.C. 20037, 2000.
4. Resnick P (ed). RFP 2822: Internet Message Format. April 2001. http://www.ietf.org/rfc.html.
5. Wood D. Programming Internet Email. O'Reilly: Sebastopol 1999.
6. 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.
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.
8. Galvin J, Murphy S, Crocker S, Freed N. RFC 1847: Security multiparts for MIME: Multipart/signed and multipart/encrypted, October 1995. http://www.ietf.org/.
9. Elkins M, Del Torto D, Levien R, Roessler T. RFC 3156: Mime security with openPGP, August 2001. http://www.ietf.org/rfc.html.
10. Callas J, Donnerhacke L, Finney H, Thayer R. RFC 2440: OpenPGP message format, November 1998. http://www.ietf.org/rfc.html.
11. Mullet D, Mullet K. Managing IMAP . O'Reilly: Sebastopol 2000.
12. Engelmann U, Schröter A, Schwab M, Eisenmann U, Meinzer HP. Openness and Flexibility: From Teleradiology to PACS. In: Lemke HU, Vannier MW, Inamura K, Farman AG (Eds). CARS'99. Amsterdam: Elsevier (1999) 534-538.
13. Engelmann U, Schröter A, Schwab M, Eisenmann U, Bahner ML, Delorme S, Hahne H, Meinzer HP. The Linux-based PACS project at the German Cancer Research Center. Lemke HU, Inamura K, Farman AG, Doi K (Eds). CARS 2000: Computer Assisted Radiology and Surgery. Proceedings of the 14th International Congress and Exhibition. Amsterdam: Elsevier (2000) 419-424.
14. Ramsdell, B. RFC 2633: S/MIME Version 3 Message Specification, June 1999. http://www.ietf.org/rfc.html.
15. Bundesamt für Sicherheit in der Informationstechnik. Sphinx Project. http://www.bsi.de/aufgaben/projekte/sphinx/index.htm.
16. The GNU Privacy Guard. Projekt Ägypten. http://www.gnupg.org/aegypten/tech.en.html.
17. Das GNU Privacy Projekt (GnuPP). http://www.gnupp.de/start.html.