xPIPE – Reception of DICOM Data from any Sender via the Internet

Abstract

Purpose: Various technologies have been established for DICOM data exchange in radiology. In addition to the patient CD, online transfers via VPN (virtual private network) or DICOM email are common practice. However, dedicated network solutions are generally not appropriate for data exchange with occasional and spontaneous partners due to missing infrastructure at the partner institutions and/or complex setup procedures. The purpose was to develop a practical solution to complement the established technologies to allow users worldwide to transfer images without registration.

Materials and Methods: The development of the xPIPE system is based on Java and various software libraries. A client hosted on a web-site enables sending DICOM data to a receiving system of the hospital.

Results: The new xPIPE system creates a gateway to a receiving hospital which is accessible from any point worldwide, giving other hospitals, clinics and patients a simple and secure method to transmit DICOM data without intermediate storage on external servers.

Conclusion: The system was deployed at the University Hospital Münster and subsequently widely used even without information events and training. Data protection during transfer is ensured by the use of signatures and encryption. From the user’s perspective the system has only minor technical requirements and can be used with minimal setup effort.

Key Points:

- There is a need for DICOM receiving systems for connecting occasional and spontaneous partners.
- A successful solution has to minimize the complexity for the partners.
- The developed xPIPE system provides an option for simple and secure DICOM data transmission.
- Availability of such receiver systems may reduce the risk of using insecure transmission paths.

Citation Format:


Zusammenfassung

gänzung der etablierten Technologien, die ohne Voranmeldung jedem weltweiten Nutzer den Bild-
versand ermöglicht.


Ergebnisse: Das entwickelte xPIPE-System schafft ein weltweit erreichbares Gateway in das Kran-
enhaus und bietet damit beliebigen Partnern (Kliniken, Arztpraxen oder Patienten) eine Mög-
llichkeit der einfachen und gleichzeitig sicheren Übermittlung von DICOM-Daten ohne Zwischen-
speicherung auf externen Servern.
The following demands were made of the xPIPE system prior to its development:

- Transmission of DICOM data from any sender to the University Hospital Münster
- Optional notification of the recipient per e-mail
- Secure transmission
- Minimum setup effort
- Simple operation

A client that receives data from the sender and can securely transfer the data via the Internet to a server at the University Hospital Münster was developed for this purpose. Fig. 1 shows the basic data flow.

The xPIPE client was developed in Java and uses the Pixelmed DICOM Toolkit (http://www.pixelmed.com) for processing DICOM data and the HTTPS protocol for encrypted transmission. The client is distributed per Java Web Start technology. The client can thus be launched directly via a link on a provider website (see Fig. 2). The only requirement for the sender is a Windows or Mac OS X operating system with installed Java Runtime Environment. Detailed instructions, technical data, and contact information are available for the user on the provider website parallel to the client.

Once the client has been launched, a data privacy statement is displayed. If the user accepts the statement, the graphical user interface launches (see Fig. 3). The sender’s contact information (name and e-mail address) is queried in steps 1 and 2. The recipient can be optionally notified per e-mail in steps 3 and 4. The DICOM data is then selected via a selection dialog. Data can be imported from any medium (CD, DVD, USB stick or hard disk). The so-called DICOMDIR, a directory defined in the DICOM standard, e.g. for patient CDs, is used to identify the DICOM files. If this is not available, the DICOM files are identified on the basis of a recursive search of the directory tree. Transfer to the recipient is performed via the “Start transfer” button. The current status and a final report can be viewed under point 7.
The RSNA Clinical Trial Processor (http://mircwiki.rsna.org) is used as the recipient. This open source project of the Radiological Society of North America provides the option of processing DICOM data via so-called pipelines. Pipelines can be comprised of different import services, processor services, and export services. A pipeline consisting of an HTTPS import service and a DICOM export service was created for the xPIPE system. Since only DICOM data received per HTTPS needs to be transmitted, a processor service is not necessary. However, an expanded HTTPS import service was implemented for the desired functionality of e-mail notifications. In addition to DICOM data, the HTTPS import service also receives notification data per HTTPS and sends.

Fig. 2 xPIPE website of the University Hospital Münster.

Fig. 3 The graphical user interface of the xPIPE client.
corresponding e-mails via the internal hospital e-mail server.

For security reasons the Clinical Trial Processor is operated in the so-called DMZ (demilitarized zone) of the network. Systems within the DMZ accessible via the Internet are separated from the internal network by a firewall. To be able to dispense with opening of the firewall for DICOM image transmission, the Clinical Trial Processor offers a polling option. An additional Clinical Trial Processor in the internal network actively queries the Clinical Trial Processor in the DMZ for new DICOM data for transfer and then transmission. Since the establishing of a connection is initiated from the internal network, i.e., the connection is established in the direction of the DMZ, the firewall can remain closed for all connections from the DMZ in the direction of the internal network.

A temporary storage including a web viewing system is used for providing the DICOM data. Via a link in the notification e-mails, the received data can thus be called up and displayed directly at all workstations. Images can be optionally transferred from the temporary memory to the PACS for archiving at any time. Fig. 4 shows the complete internal data flow.

Different aspects are taken into consideration with respect to the protection of transmitted patient data. Data confidentiality during transfer via the Internet can be ensured by using encryption via HTTPS protocol. This is an encrypted direct connection between the xPIPE client and the RSNA Clinical Trial Processor which spans all intermediate transfer systems and networks including the Internet.

In addition, it is important to also check the authenticity of the receiving system. By using official X.509 certificates for operation of the HTTPS import service of the Clinical Trial Processor, it can be ensured that the provided xPIPE client data can only be sent to the designated server at the University Hospital Münster. Moreover, it must be ensured that the xPIPE client used by the user was provided by the University Hospital Münster and has not been manipulated by a third party. The xPIPE client was protected in this regard via code signing also using an official X.509 certificate.

The xPIPE system has been in operation at the University Hospital Münster since the middle of November 2013. After initial test operation only in radiology, use was expanded to additional departments by June 2014. University-wide use at the University Hospital Münster began in August 2014. Fig. 5 shows the increase in the frequency of use during the introduction phase.

Moreover, it would be conceivable to establish additional xPIPE systems outside the University Hospital Münster. After setting up an xPIPE receiving system, additional hospitals and clinics could offer an adapted xPIPE client under their own logo via an independent website. The product and necessary services can be acquired from the University Hospital Münster via a cooperative agreement.

Fig. 4 The data flow in the University Hospital Münster.

Fig. 5 Amount of data transmitted via xPIPE (number of patients).
Risk evaluation

The use of official certificates and state-of-the-art encryption makes it possible to protect patient data. However, as in the case of all encryption techniques, absolute protection cannot be achieved. The HTTPS protocol also has a history of security vulnerabilities that are counteracted with constant further development. However, the xPIPE system has a security advantage compared to web servers that can be accessed with any browser. It uses its own client so that for example older protocols or ones known to be insecure do not need to be offered for reasons of compatibility. Therefore, use of the SSL 3 protocol and the RC4 encryption method is not available. Moreover, in relation to authentication of the sender, not using manual assignment of login data does not result in a disadvantage but rather ensures the desired ease of use of the system. However, as in the case of all services offered via the Internet, possible hacking scenarios should be taken into consideration and the risk should be evaluated.

It is conceivable that hackers could overload the xPIPE system by sending large quantities of data or could overload the downstream temporary storage. The risk can be initially decreased by offering a large network, server, and storage infrastructure. Moreover, attacking systems can be blocked as needed on an acute basis by corresponding firewall configurations or whitelist/blacklist IP lists in the Clinical Trial Processor. The import service of the CTP was expanded to include a data monitor as an additional protection measure. This monitors the incoming data quantities and can inform the user via login with user name and password, was intentionally not used in contrast to many established solutions. Personal authentication of the sender is not conceivable any way since the available options for verifiable identification are extremely limited. Identification solutions, e.g. the electronic personal ID for online identification introduced in Germany, are not widely used. A standardized global system is not available. Moreover, in relation to authentication of the sender, not using manual assignment of login data does not result in a disadvantage but rather ensures the desired ease of use of the system. However, as in the case of all services offered via the Internet, possible hacking scenarios should be taken into consideration and the risk should be evaluated.

Summary

On the whole, the xPIPE system offers a simple and secure option for transmitting DICOM files. Patient data is protected against attack by third parties at all times. From the user’s perspective the system has only minor technical requirements and can be used with minimal setup effort. Technologies such as VPN or DICOM e-mail are to be given preference for data exchange with fixed partners, due to the possible integration in the hospital workflow and the bidirectional communication. However, xPIPE meets the need for simple data exchange with an unlimited number of temporary partners and thus allows global communication. In addition, it reduces the risk of the often observed use of insecure paths of transmission such as e-mail and messenger services. It is therefore a useful addition to established technologies for DICOM transmission.

The simple use without special know-how and dedicated access paths has quickly made xPIPE a product that has accelerated and simplified workflows at the University Hospital Münster and is equally valued by referring physicians and patients.

References

1 Mildenberger P, Kotter E, Riesmeier J et al. The DICOM-CD-Project of the German Radiology Association – an Overview of the Content and Results of a Pilot Study in 2006. Fortschr Röntgenstr 2007; 179: 676–682