```
<?xml version="1.0" encoding="utf-8"?>
<ServicePart Name="ADDRESSUPDATE" Action="SET">
  <Connection>
    <ID>1793.138131913.139</ID>
    <DisplayConnectionName>Hospital A</DisplayConnectionName>
    <Mailserver>Server</Mailserver>
    <Port>993</Port>
    <EmailAddress>dicom@hospital_a.com</EmailAddress>
    <GPGKeyID>A28DF952</GPGKeyID>
  </Connection>
</ServicePart>

<?xml version="1.0" encoding="utf-8"?>
<ServicePart Name="ADDRESSUPDATE" Action="REMOVE">
  <Connection>
    <ID>1793.138131913.139</ID>
  </Connection>
</ServicePart>
```

Fig. 1 Example of an XML message describing an address update

Using control messages for administrative tasks and constancy testing of DICOM e-mail based teleradiology networks

F. Schwind[1], H. Münch[1], A. Schröter[1], G. Weisser[2], H.-P. Meinzer[1,3], U. Engelmann[1,3]
[1]CHILI GmbH, Heidelberg, Germany
[2]Universitätsklinikum, Institut für Klinische Radiologie und Nuklearmedizin, Mannheim, Germany
[3]German Cancer Research Center, Division Medical and Biological Informatics, Heidelberg, Germany

Keywords Teleradiology · DICOM e-mail · PACS · Constancy testing

Purpose

DICOM e-mail is a wide used standard application in German teleradiology networks [1]. It is easy to admit new partners to the network, because all communication is done via dedicated servers for all participants. Only the e-mail connection must be configured and keys for encryption exchanged between partners [2].

One major drawback is the asynchronous communication, which makes it hard to trigger automated constancy tests between partners and generate protocols, which are required by the German authorities for legal reasons [3]. Furthermore it was up to now not possible to update changes in addresses or encryption keys automatically.

This paper presents a solution for automated constancy tests and the exchange of administrative data via e-mail, which was developed with the Working Group on Information Technology (Arbeitsgemeinschaft Informationstechnologie, @GIT) of the German Radiology Society (Deutsche Röntgengesellschaft, DRG) [4].

Methods

The newly developed DICOM e-mail service parts contain an XML body part describing the action, which should be interpreted and executed by the receiver. To ensure privacy, completeness and validity of the transferred e-mails, all communication must be encrypted PGP/GnuPG compatible and signed by the sender. The recipient has to decrypt the e-mail and check the validity of the signature. It is recommended to configure a whitelist with trusted partners for each allowed operation.

All participating hosts must support the message disposition notification (MDN) described in the @GIT Whitepaper v1.5 and RFC3798, RFC3462. While only complete messages can be notified by the receiver with the basic MDN, only one service part per e-mail is allowed at the moment.

To enable filtering of received messages, each service part message is identified by an unencrypted X-TELEMEDICINE-SERVICEPART tag, describing the action contained in the encrypted mail body. The tag value is either an ADDRESS- or KEYUPDATE or TESTTRANSFER for constancy test requests respectively PROTOCOL for constancy test results. The XML body, which is interpreted by the receiver, describes each action in detail.

Address and key updates

Figure 1 shows an example of an XML message for an address update where a new e-mail address is transmitted to all partners. Each XML service part is identified by a name (ADDRESSUPDATE) and an optional action (SET or REMOVE). The body of the service part is processed differently based on the found name and action. In case of an address update a new connection is added or updated if the given id already exists. If the action value REMOVE is set, the connection with the given id will be removed or disabled, depending on the implementation of the service part receiver.

After completing or denying the action, a MDN is send to the given e-mail address. For this purpose the existing @GIT error codes were extended with new messages matching the needs of service part messages including parser or update errors.

The service part KEYUPDATE works like the described ADDRESSUPDATE while only the complete PGP/GnuPG keyblock must be transmitted to add a new key. To remove an existing PGP/GnuPG key the key id must be transferred in a service part KEYUPDATE message using the action REMOVE.

Constancy tests

Service parts can also be used to trigger constancy tests between DICOM e-mail partners. The administrator of the network sends an e-mail containing a TESTTRANSFER request to a communication partner. The service part must contain the address and PGP/GnuPG key of the testdata receiver as well as the address and key of the protocol receiver. Additionally a test dataset id and an error timeout can be specified.

At the moment 17 datasets, matching common radiological studies, are predefined. It is possible to add new dataset as long as all partners use the same naming convention and support the requested imagetype.

After receiving the TESTTRANSFER request, the receiver sends the specified test data to the given connection partner. After all data is transferred correctly (which is ensured by using the described MDN mechanism) the test data sender generates a service part protocol and delivers it to the specified recipient using the service part type PROTOCOL (Fig. 2).

Each service part PROTOCOL is send in an XML format containing the transmission status (either COMPLETED or ABORTED if the given timeout was reached), the used test dataset id and mail count as well as the size and transfer time of each transmitted object. In case of errors during the constancy test all error codes and descriptions are included as well. Using this information, the protocol receiver is able to compile a complete constancy test protocol which is compliant with the German standard for quality assurance in teleradiology (DIN 6868-159).

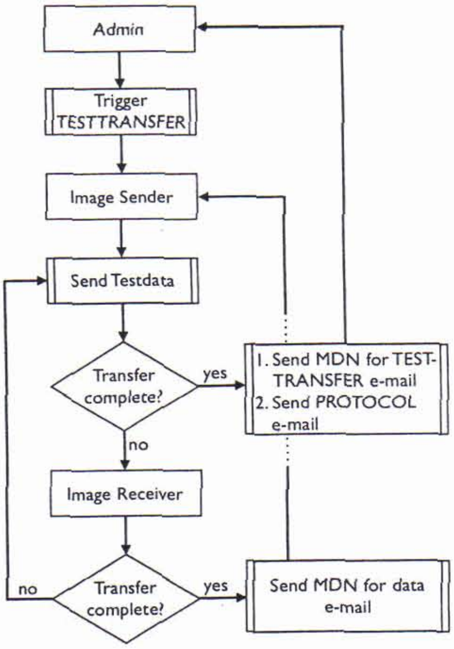

Fig. 2 Flowchart for constancy tests

Results

The authors implemented the described service part e-mails and tested them in a connect-a-thon with other members of the @GIT. The newly developed features extend the already existing "Guidelines for a standardized teleradiology data exchange v1.6" (Empfehlung für ein standardisiertes Teleradiologie Übertragungsformat) [5] and worked between multiple teleradiology clients and servers of different vendors. It was possible to trigger constancy tests between DICOM e-mail partners and propagate changes in address or encryption keys automatically between the participants.

Discussion

The newly defined and implemented extensions of the DICOM e-mail protocol simplify administrative tasks, such as public key updates, changes of e-mail addresses and quality measurements.

Teleradiology users in DICOM e-mail based networks can now easily analyze the quality of service by triggering constancy tests via DICOM e-mail while requesting the generated protocols simultaneously. It is now even possible to administrate such networks solely via DICOM e-mail, once the initial connection is setup correctly.

While only four service part messages are defined at the moment, these are easy extendable in the future to match the needs of upcoming DICOM e-mail teleradiology networks.

Conclusion

The implementation of the described methods enable automated time- and quality test for teleradiology networks, which communicate via DICOM e-mail. In addition it is possible to send administrative messages between DICOM e-mail partners. At the moment this guidelines are only used in Germany but might be useful in other countries as well, where the image communication is done via DICOM e-mail.

References

[1] Weisser G, Engelmann U, Ruggiero S, Runa A, Schröter, Baur S, Walz M. Teleradiology applications with DICOM-e-mail. Euro Radiol. 17(5) (2007) 1331–1340. doi 10.1007/s00330-006-0450-8.

[2] Engelmann U, Schroeter A, Schweitzer T, Meinzer HP. An architecture for secure exhange of medical images and reports based on mail, DICOM and public key encryption. Eur J Med Res 7 (Suppl. I) (2002) 22.

[3] Engelmann U, Seidel B. DIN 6868-159: A German standard for quality assurance in teleradiology. Int J CARS (2009) 4 (Suppl 1): S158–S159.

[4] Weisser G, Walz M, Ruggiero S, Kämmerer M, Schröter A, Runa A, Mildenberger P, Engelmann U, Standardization of teleradiology using Dicom e-mail: recommendations of the German Radiology Society. Eur Radiol. 2006 Mar;16(3):753–758.

[5] @GIT. Empfehlung für ein standardisiertes Teleradiologie Übertragungsformat: Version 1.6 (2010) www.tele-x-standard.de (Last access: 08.01.2012)