@GIT Initiative

“Standardizing

Telemedicine”

Recommendation

for a Standardized

Teleradiology Transmission Format

Version 1.6.1

www.tele-x-standard.de
teleradiologie@drg.de

1 Index

2 Imprint

Initiative “Standardizing Telemedicine”
Working Group on Information Technology of the German Radiology Society
(Arbeitsgemeinschaft Informationstechnologie der Deutschen Röntgengesellschaft)
E-mail: teleradiologie@drg.de
URL: http://www.tele-x-standard.de

Title: Recommendation for a Standardized Teleradiology Transmission Format
Version: 1.6.1

2.1.1.1 Contributing members of the working group (in alphabetical order)

Name	Organization	Versions
Baur, Stefan	Curagita AG, Heidelberg	1.1,1.5
Engelmann, Uwe	Deutsches Krebsforschungszentrum, Heidelberg	1.1,1.5,1.6
Kämmerer, Marc	VISUS GmbH, Bochum	1.1,1.5,1.6
Klos, Gordon	Klinik für Radiologie, Uniklinik Mainz	1.1,1.5,1.6
Köster, Claus	GI Gesundheitsinformatik GmbH	1.1,1.5,1.6
Kreisel, Roman	Abasoft EDV-Programme GmbH	1.6
Mildenberger, Peter	Klinik für Radiologie, Uniklinik Mainz	1.1,1.5,1.6
Münch, Heiko	CHILI GmbH, Heidelberg	1.1,1.5
Pelikan, Ernst	Universitätsklinikum Freiburg, Klinikrechenzentrum	1.1,1.5
Philipps, Mario	Steinhart Medizinsysteme GmbH	1.1,1.5,1.6
Ruggiero, Stephan	Institut für Klinische Radiologie, Universitätsklinikum Mannheim	1.1,1.5
Runa, Alain	Institut für Klinische Radiologie, Universitätsklinikum Mannheim	1.1,1.5
Schneeberg, Sven	VISUS GmbH, Bochum	1.6
Schröder, Stephan	CHILI GmbH, Heidelberg	1.1,1.5
Schröter, Andre	CHILI GmbH, Heidelberg	1.1,1.5
Schütze, Bernd	http://www.medizin-informatik.org/	1.1,1.5,1.6
Schwind, Florian	CHILI GmbH, Heidelberg	1.6
Walz, Michael	Ärztliche Stelle für Qualitätssicherung in der Radiologie Hessen	1.1,1.5,1.6
Weisser, Gerald	Institut für Klinische Radiologie, Universitätsklinikum Mannheim	1.1,1.5,1.6
Westermann, Michael	GI Gesundheitsinformatik GmbH	1.1,1.5,1.6

Last revised: 05. April 2013

3 Contact

The initiative can be contacted at any time via the following e-mail address: *teleradiologie@drg.de*. Interested parties will be added to our mailing list upon request.

All personal data will be treated as strictly confidential. No personal information will be passed on to a third party.

Results generated by the Initiative will be made available to the public on the Internet at *http://www.tele-x-standard.de*.

4 Copyright

5 Preamble

Members of the @GIT Initiative “Standardizing Telemedicine” have joined with the intention of developing a recommendation for a communication protocol suitable for teleradiology. The members come from various academic and research institutions as well as from the industry. Anyone interested in contributing can join the group.

Results are accessible to, and can be used by, the public without restrictions, now and in the future (Public Domain).

6 Preface – Version 1.6.1

This is the first English version of the Recommendation for a Standardized Teleradiology Transmission Format. In comparison to version 1.6 it has been translated from German and errors have been corrected (cf. 9 Errata).

The authors of the Working Group,

March 2013

7 Preface – Version 1.6

The present version 1.6 of the recommendation is about the support of administrative tasks and quality testing.

A German standard for quality assurance in teleradiology (DIN 6868-159) was published in March 2009. Since then it is required to perform quality and constancy tests when sending data in teleradiology networks in accordance with the Röntgenverordnung (RöV, German X-Ray Ordinance). Particularly in heterogeneous networks with software from different manufacturers these requirements present a new challenge to perform the requested tests automatically. The basic task here is the exchange and processing of communication data across multiple vendors.

A second challenge is the convergence of existing networks. It becomes necessary to not only exchange DICOM images but also administrative messages between partners to enable the administration of growing networks.

In order to meet these new requirements, so-called Service Part e-mails are added in version 1.6. Based on the previous standard recommendations introduced in versions 1.1 and 1.5, the following scenarios can be presently covered:

1. Vendor independent communication of the required data for quality and constancy tests according to DIN 6868-159.
2. Exchange of PGP/GnuPG key data across vendors.
3. Exchange of address data across vendors.

Confirmations for completed actions are sent in accordance with the notification mechanisms described in version 1.5.

The authors of the Working Group,

June 2010

8 Preface – Version 1.5

Version 1.1 has already enabled the transfer of DICOM and NON-DICOM data across different vendors using the e-mail protocol. The present version 1.5 covers the following additional extensions:

1. A mechanism verifying the reception and completeness of data on the side of the receiver. For this purpose, additional information is added by the sender to the data packets, which can be analyzed, upon receipt.
2. A mechanism verifying the reception and completeness of data on the side of the sender. For this purpose, confirmation notifications are sent back to the sender, by the receiver, which include a defined status.
3. A mechanism verifying the authenticity of the sender and the integrity of the data packets. This allows identification of modifications on data packets by third parties, and refusal of acceptance for unwanted data packets.

The authors of the Working Group,
October 2005

9 Errata

9.1 Version 1.5

9.1.1 Error in Figure – MDM according to RFC 3798

The following example contains an error in the machine-readable paragraph where header and body are delimited (cf. arrow in Fig. 1 – Incorrect confirmation of receipt according to RFC 3798). A delimiter needs to be introduced here by adding a new line after the Content-Type. This error needs to be corrected in the software starting with the adoption of the standards recommendation version 1.6 (in accordance with the example Fig. 9 – Confirmation of Receipt according to RFC 3798).

```
Date: Mon, 1 Jan 2009 00:19:00 (EDT) -0400
From: radiology_mannheim@teleradiology.de
Message-Id: <2323423432019.12345@teleradiology.de>
Subject: Disposition notification
To: radiology_mainz@teleradiologie.de
MIME-Version: 1.0
Content-Type: multipart/report; report-type=disposition-notification;
boundary="RAA14128.773615765/teleradiology.de"

--RAA14128.773615765/teleradiology.de

 Here is the spot for additional optional text

--RAA14128.773615765/teleradiology.de
content-type: message/disposition-notification
Reporting-UA: post.teleradiology.de; Mailprogram 1.1
Final-Recipient: rfc822; radiology_mainz@teleradiologie.de
Original-Message-ID: <199509192301.23456@teleradiologie.de>
Disposition:automatic-action/MDN-sent-automatically;displayed/warning
Warning: 1.2

--RAA14128.773615765/teleradiology.de--
```

Fig. 1 – Incorrect confirmation of receipt according to RFC 3798

9.1.2 Errata in text chapter 15.4.2.1.2 Request Receipt Mechanism 2 - X-TELEMEDICINE confirmation (optional)

X-TELEMEDICINE-DISPOSITION-NOTIFCATION-TO should read *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO.* The same applies to *X-TELEMEDICINE-DISPOSITION-NOTIFCATION- KEYID* which should read *X-TELEMEDICINE-DISPOSITION-NOTIFICATION- KEYID*

As of version 1.6.1 both spellings of the x-tags must be supported. From version 1.8 onwards only the corrected spelling will be valid.

9.1.3 Errata in table 20. Appendix Error Codes

1.3	mail-attachement-error -> mail-attachment-error
1.3.1	mail-attachment-corrupt -> mail-attachment-corrupt
3.2.1	application-intern-attachement-error ->application-intern-attachment-error
3.2.1.1	application-intern-attachement-not-processed -> application-intern-attachment-not-processed

10 Basic consideration

The recommendation is based on the assumption that the exchange of e-mails with encrypted data provides the smallest common denominator for a secure exchange of non-anonymized or non-pseudonymized data.

11 Minimum requirements for the software

11.1 Datatype transfer

In general it has to be possible to transmit any type of data (DICOM and NON-DICOM). If the receiving software cannot handle a particular type of data it should be forwarded to another application or stored temporarily. In any case, receipt of unknown objects must not lead to an abortion of the data transmission.

11.2 MIME Standard

The software must support of the MIME Standard[1], in particular Multipart Mail, Message Partial, as well as use of X-tags.

12 Extended requirements for the software

The secure variants of the e-mail protocols (SMTP, POP3 or IMAP4) should be supported.

13 Encryption & compression

Encryption of data must be compatible to OpenPGP (RFC 4880). The use of compression as defined in RFC 4880 is optional but recommended. A guideline for the encryption key length and algorithm, which is considered as secure, was published by the German Federal Office for IT Security[2].

14 Digital signature (PGP/MIME)

PGP/GnuPG can be used for encrypting as well as for signing of data. In the context of this recommendation, the following two methods are recommended in accordance with RFC 3156 and RFC 1847:

[1] In particular RFC2045/46 (MIME Part 1&2), RFC3156 (MIME Security with OpenPGP); Source: http://www.ietf.org/

[2] https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

- E-mail encryption combined with signature (RFC 3156, chapter 6.2 – *Combined method*)
- Data with a separate signature, which is encrypted compatible to the OpenPGP standard in accordance with RFC 1847. (RFC 3156, chapter 6.1 – *Encapsulation*)

In accordance with the present recommendation from version 1.5, it is for the transfer of data to sign and encrypt the data using one of these two methods.

15 Transfer format

15.1 DICOM data

DICOM data is transformed into a DICOM E-MAIL in accordance with Suppl. 54 of the DICOM Standard and must be multipart/mixed. The resulting DICOM E-MAIL is encrypted and signed compatible to the OpenPGP standard (Fig. 2) (cf. Chapter 14 – *Digital signature (PGP/MIME)*).

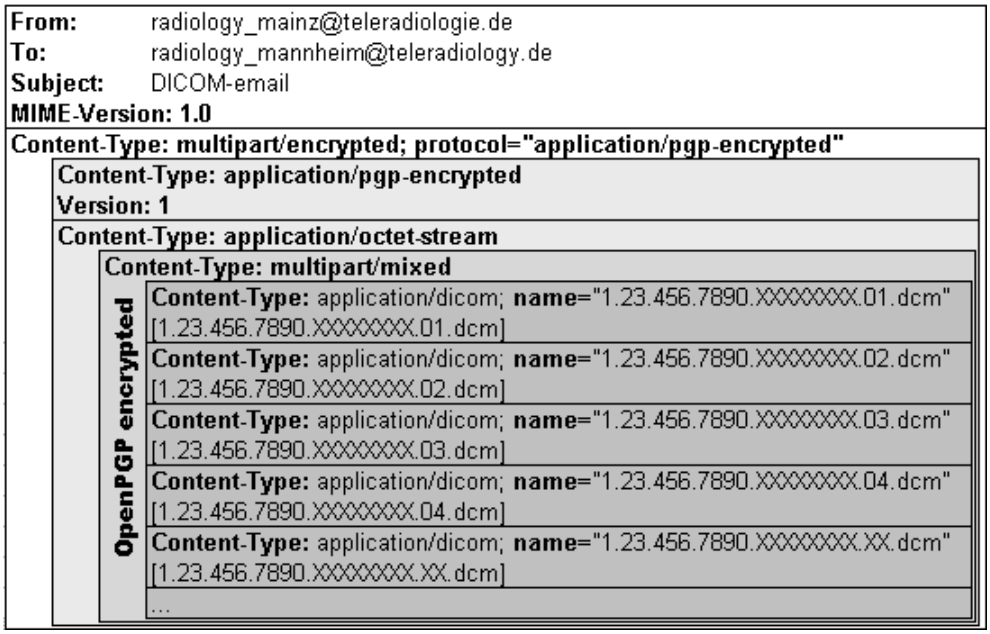

Fig. 2 – Transfer format for DICOM data

15.2 NON-DICOM data

Used X-tags: X-TELEMEDICINE-STUDYID

NON-DICOM data does not contain a header with patient information. For this reason, a new tag *X-TELEMEDICINE-STUDYID* has been defined, conforming to the MIME Standard. This tag is used to transmit the StudyInstanceUID in order to

assign a NON-DICOM object to a DICOM study. In case there is no suitable DICOM study or StudyInstanceUID, a new UID needs to be generated and assigned to the NON-DICOM data (cf. Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.** Generating identification numbers). All NON-DICOM data is encrypted and signed in compliance with the OpenPGP standard together with all DICOM data (Fig. 3 – Transfer format for). This allows the transmission of multiple exams or multiple patients together within a single e-mail. It is also possible to send associated data in different e-mails while the matching is done via the respective StudyInstanceUID (in the case of DICOM data) and *X-TELEMEDICINE-STUDYID* (in the case of NON-DICOM data).

Use of the *X-TELEMEDICINE-STUDYID* for DICOM data is not permitted and must to be ignored on the part of the receiver. (Rule of unambiguousness)

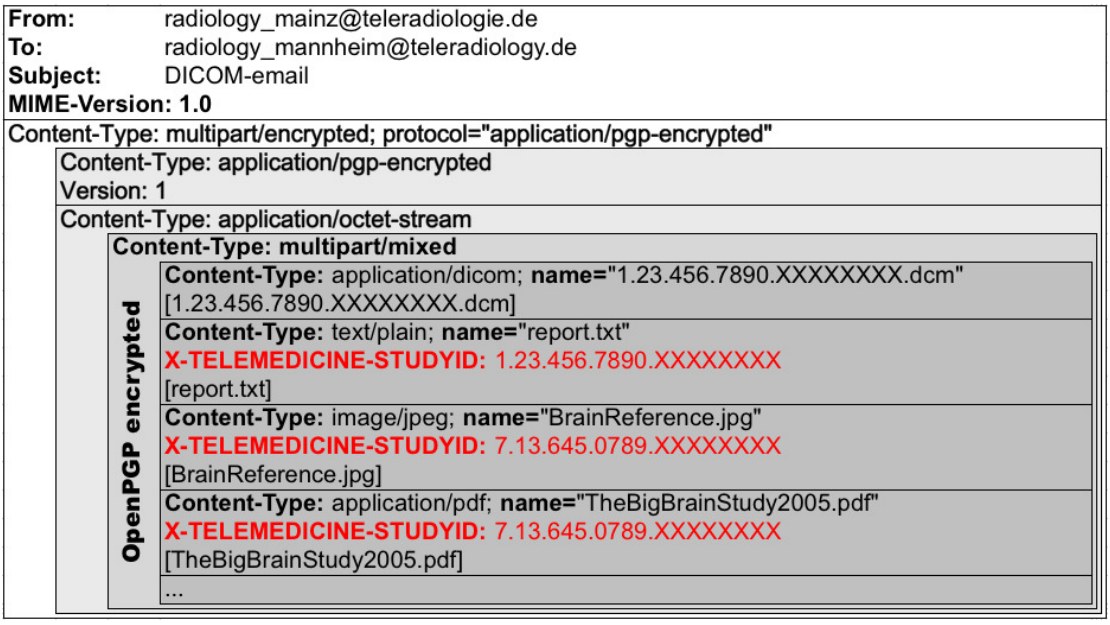

Fig. 3 – Transfer format for NON-DICOM data

15.3 Message/Partial

In the overview (Fig. 4 – Overview of data transfer) data is sent encrypted as a PGP/MIME Multipart e-mail. The MIME Standard (RFC 2046, Chapter 5.2.2 - *Partial Subtype)* provides a mechanism for the splitting large e-mails into multiple smaller parts (message/partial). This is done either by the sending software or by a mail server involved in the transmission process (Fig. 4 ① message/partial). The receiver must be capable of detecting the received splitted e-mail parts and assembling them into the original e-mail (Fig. 4 ②).

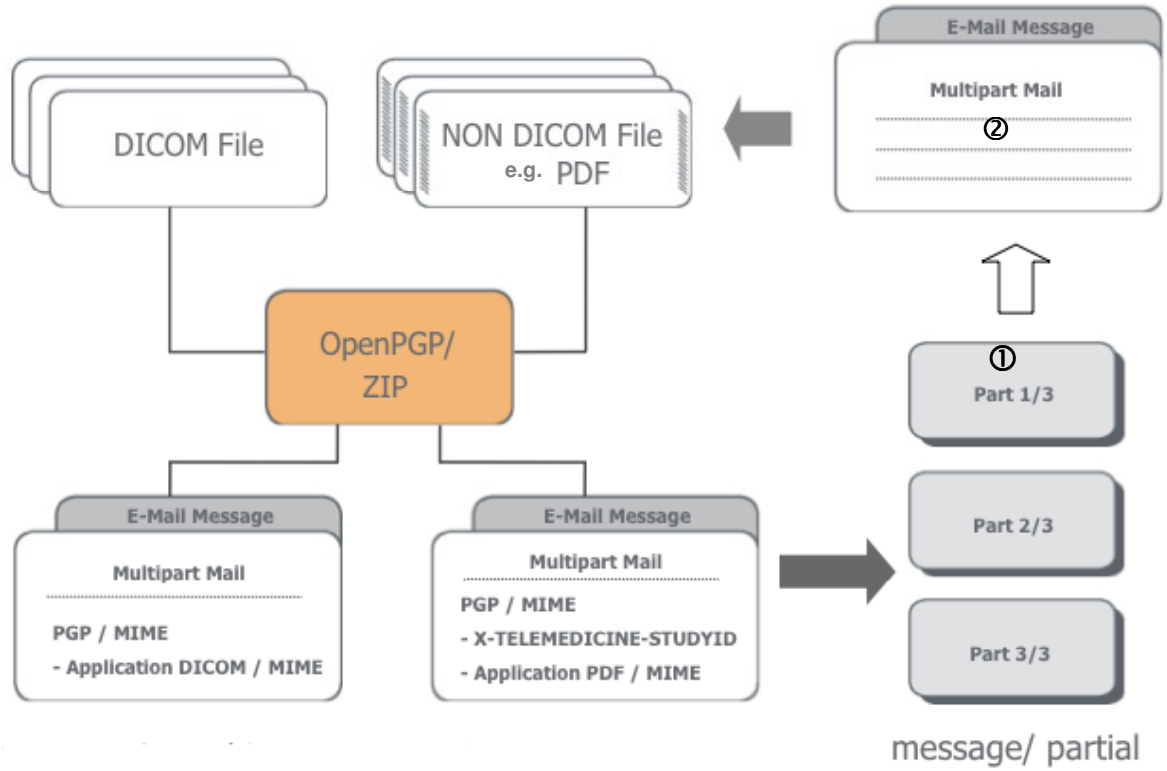

Fig. 4 – Overview of data transfer

15.4 Mechanisms to verify completeness of transmitted data

While sending data as DICOM E-MAIL via a mail server both the sender and receiver must be able to verify the completeness of the transmitted data.

On the sender side this means to know if an e-mail has reached the destination. On side of the receiver it is useful to know how many e-mails were sent and how many can be expected in this transfer.

15.4.1 On the side of the receiver (optional)

Used X-tags: X-TELEMEDICINE-SETID, X-TELEMEDICINE-SETPART, X-TELEMEDICINE-SETTOTAL

The sender adds additional X-tags to the data packets, which can be interpreted on the receiver side. This allows the receiver to verify that he has received all data packets sent. The definition of these X-tags follows the „message/partial“ mechanism (RFC 2046, Chapter 5.2.2 – *Partial Subtype*).

X-TELEMEDICINE-SETID = Unique ID to label a set of associated e-mails.

X-TELEMEDICINE-SETPART = Number of an e-mail within a set of associated e-mails.

X-TELEMEDICINE-SETTOTAL = Total number of associated e-mails in a set.

These three X-tags do not represent any medical correlation of the data. They only group associated e-mails and allow the receiver to verify whether he has received the complete set of e-mails. The use of the X-TELEMEDICINE-SET is optional. In case it is used the following rules must apply:

1. The X-tags can be used out- and inside of the PGP/MIME containers (Fig. 5 – Labeling e-mails belonging together)
2. *X-TELEMEDICINE-SETID* and *X-TELEMEDICINE-SETPART* must be used in each e-mail.
3. *X-TELEMEDICINE-SETTOTAL* has to be present in the last e-mail of the set while it is optional in all the other e-mails.
4. X-tags should always be part of the encrypted e-mail body. In cases they differ from unencrypted X-tags a warning message should be issued.

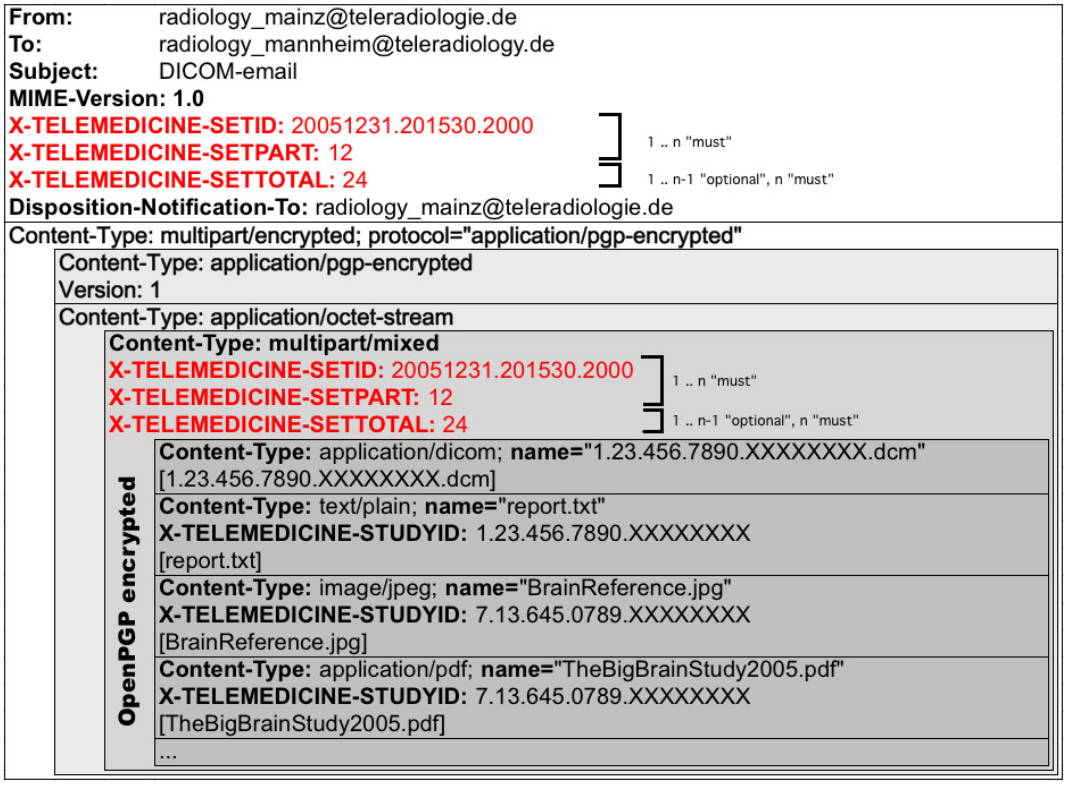

Fig. 5 – Labeling e-mails belonging together

15.4.2 On side of the sender

On the sender side the verification procedure for a complete data transmission consists of two dependent steps (First: Request for a receipt on data reception, Second: Returning the requested receipt to the sender).

Therefore the standard recommendation contains two mechanisms. The first represents the minimum variant and should be suitable for use with e-mail applications conforming to the MIME Standard. The second mechanism adds a notification feature for the individual e-mail parts rather than for the entire e-mail. Mechanism 2 is for complementary purposes.

15.4.2.1 Request for receipt

15.4.2.1.1 Request Receipt Mechanism 1 – MIME Message Disposition Notification (mandatory)

Used MIME-Tags: DISPOSITION-NOTIFICATION-TO

To verify the correct receipt of e-mails, the MIME-Standard provides the option to request notification e-mails (RFC 3798,). The request (*DISPOSITION-NOTIFICATION-TO: notification address*) is added to the e-mail header. This triggers, on side of the receiver, the mechanism of sending a message disposition notification conforming to the RFC.

The subsequent Fig. 6 shows a sample e-mail.

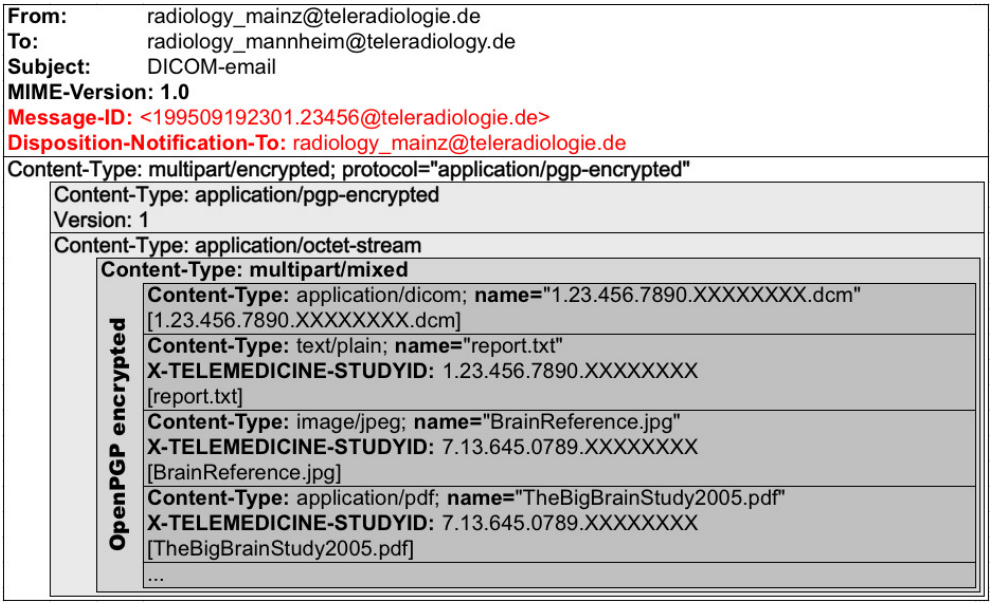

Fig. 6 – Request for confirmation of receipt conforming to RFC

Use of a notification conforming to the RFC results in the following:

1. The confirmation always refers to the entire e-mail and not to its content.
2. The data transferred is transmitted without encryption or signature. This may present a potential target to manipulations.

15.4.2.1.2 Request Receipt Mechanism 2 - X-TELEMEDICINE confirmation (optional)

Used X-tags: X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO, X-TELEMEDICINE-DISPOSITION-NOTIFICATION-KEYID

In order to overcome the weaknesses mentioned regarding Mechanism 1, Mechanism 2 allows a separate request to confirm the receipt for each part of the encrypted PGP/MIME container. For this purpose, the X-tags *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO* and *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-KEYID* were introduced. *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO* contains the notification address equivalent to the *DISPOSITION-NOTIFICATION-TO* address from Mechanism 1. *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-KEYID* contains the key ID of the PGP/GnuPG to encrypt the resulting e-mail reply. The use of this tag is optional. The notification addresses as well as the key IDs can be different for all parts. If these tags are used it is mandatory to set a content ID conforming to RFC 2392. Due to the required global uniqueness of the IDs it is possible to map each e-mail been sent and any of its containing parts to a receipt. While the return e-mail address can result from either Address- or KeyID-tag the *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO* tag must be used if both are present.

The address set with *DISPOSITION-NOTIFICATION-TO* does not have to match the one specified in *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO*. However, both must contain valid return e-mail addresses. If mechanism 2 is used, the return addresses from the encrypted part (*X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO*, *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-KEYID*) should primarily be used. The unencrypted address from DISPOSITION-NOTIFCATION-TO should only be used as fallback.

In case Mechanism 2 is choosen it is mandatory to use Mechanism 1 as well. This enables the reception of error messages even if the e-mail part could not be decrypted. Fig. 7 illustrates the use of both X-tags. Fig. 8 shows the use of *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO* only.

Fig. 7 – Content-related request for message disposition notification using the X-tags for key ID and return address

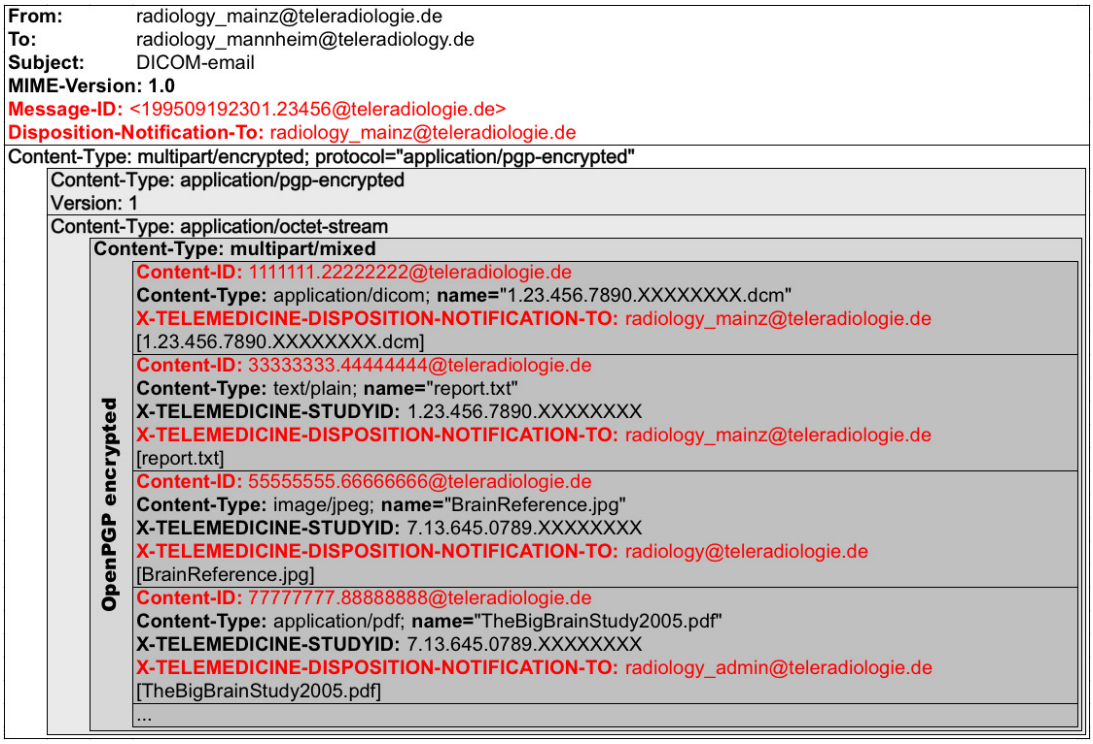

Fig. 8 – Content-related request for message disposition notification using the X-tag for return address only

15.4.2.2 Reply on data reception (optional)

While message disposition notification can always be requested the receiver of the e-mail can always choose to discard the request, which is discouraged by this recommendation.

In cases Mechanism 1 (cf. Chapter 15.4.2.1.1) is used, according to the MIME standard exactly one confirmation can be sent. This confirmation e-mail results from the unencrypted notification request and is also to be sent as an unencrypted message.

Confirmation e-mails resulting from the encrypted part (Mechanism 2, cf. Chapter 15.4.2.1.2) are sent either as encrypted or unencrypted messages. This depends on the X-tags used in the encrypted part of the notification request e-mail. In case the *X-TELEMEDICINE-DISPOSITION-KEYID* tag is used the notification should only be encrypted if the key ID is known to the receiver and the key is present.

The encrypted confirmation e-mails must contain the content ID. Due to the missing Original-Content-ID field for e-mail parts the X-tag *X-TELEMEDICINE-ORIGINAL-CONTENT-ID* has been introduced. The basic structure of the messages is shown in the following examples of unencrypted (**Fehler! Verweisquelle konnte nicht gefunden werden.**) and encrypted confirmation e-mails (not conforming to RFC 3798) (

Fig. 10). The status of the transfer is expressed by its status codes (cf. Chapter 15.4.2.2.3 – Status notifications) which are used for both kinds of message disposition notifications.

15.4.2.2.1 Reply on data reception – Mechanism 1

Used X-Tags: DISPOSITION-NOTIFICATION-TO, ORIGINAL-MESSAGE-ID

The reply e-mail is compatible to RFC 3798 and is divided into header and „multipart/report“ body. The body contains three parts:

- Part 1 – human readable (mandatory)
- Part 2 – machine readable (mandatory)
- Part 3 – reference to the original e-mail (optional)

The e-mail reply to a disposition notification request (*DISPOSITION-NOTIFICATION-TO*) is always a “multipart/report” message.

Fehler! Verweisquelle konnte nicht gefunden werden. shows a sample reply to the disposition notification request from Fig. 6. In this case, the return message indicates that the previously received e-mail contains a syntax error which has led to no error relevant in processing (Warning).

```
Date: Mon, 1 Jan 2009 00:19:00 (EDT) -0400
From: radiology_mannheim@teleradiology.de
Message-Id: <2323423432019.12345@teleradiology.de>
Subject: Disposition notification
To: radiology_mainz@teleradiologie.de
MIME-Version: 1.0
Content-Type: multipart/report; report-type=disposition-notification;
boundary="RAA14128.773615765/teleradiology.de"

--RAA14128.773615765/teleradiology.de

 Optional text goes here

--RAA14128.773615765/teleradiology.de
content-type: message/disposition-notification

Reporting-UA: post.teleradiology.de; Mailprogram 1.1
Final-Recipient: rfc822; radiology_mainz@teleradiologie.de
Original-Message-ID: <199509192301.23456@teleradiologie.de>
Disposition: automatic-action/MDN-sent-automatically;displayed/warning
Warning: 1.2

--RAA14128.773615765/teleradiology.de--
```

Fig. 9 – Message disposition notification according to RFC 3798

15.4.2.2.2 Reply on data reception – Mechanism 2

Used X-tags: X-TELEMEDICINE-DISPOSITION-NOTIFICATION, X-TELEMEDICINE-ORIGINAL-CONTENT-ID

The reply to a message disposition notification request (Fig. 7) from the encrypted PGP/MIME container results in an encrypted confirmation e-mail.

The external e-mail container is built like an encrypted e-mail. The encrypted part contains a MIME part with the content type „multipart/report“. The report type is “message/x-telemedicine-disposition-notification” which matches the content type of the report part.

This content type is defined analog to „message/disposition-notification“ and contains the field X-TELEMEDICINE-ORIGINAL-CONTENT-ID.

Fig. 10 shows a reply example to the request from Fig. 7.

```
From: radiology_mannheim@teleradiology.de
To: radiology_mainz@teleradiologie.de
Subject: Disposition notification
Date: Mon, 1 Jan 2009 15:15:35 +0100
MIME-Version: 1.0
Message-ID: <199509192301.23456@teleradiology.de >
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";
boundary="--=_NextPart_000_0027_01BF27A0.9BE21980/teleradiology.de"

This is a multi-part message in MIME format.

----=_NextPart_000_0027_01BF27A0.9BE21980/teleradiology.de
Content-Type: application/pgp-encrypted

Version: 1

----=_NextPart_000_0027_01BF27A0.9BE21980/teleradiology.de
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.1*

%MIME-Version: 1.0
%Content-Type: multipart/report;
%              report-type=X-TELEMEDICINE-DISPOSITION-NOTIFICATION;
%boundary="RAA14128.773615765/teleradiology.de"
%
%--RAA14128.773615765/teleradiology.de
%
% Here is the spot for additional optional text%
%--RAA14128.773615765/teleradiology.de
%content-type: message/X-TELEMEDICINE-DISPOSITION-NOTIFICATION
%
%Reporting-UA: post.teleradiology.de; mail program 1.1
%Final-Recipient: rfc822; radiology_mainz@teleradiologie.de
%X-TELEMEDICINE-ORIGINAL-CONTENT-ID: 1111111.2222222@teleradiologie.de
%Disposition: automatic-action/MDN-sent-automatically;displayed/warning
%Warning: 1.2
%
%--RAA14128.773615765/teleradiology.de--

-----END PGP MESSAGE-----

----=_NextPart_000_0027_01BF27A0.9BE21980/teleradiology.de--
```

* Lines starting with % are PGP/GnuPG encrypted.

Fig. 10 – Confirmation e-mail as a reply to a request from the PGP/MIME Container

15.4.2.2.3 Status messages

Status messages are used as defined in RFC 3798 but only the two notification types “Displayed” and “Deleted” are employed. Per definition “No Errors” and “Warnings” are subsumed as “Displayed”. All processing errors are grouped in the status “Deleted” including errors which either result in retransfer of data or severe errors where data must not be resent.

The following combinations of status notifications and notification types are allowed:

1. no error ascertained
   disposition-field=Disposition:*automatic-action/MDN-sent-automatically*;**displayed**
   –[**no warning, error or failure field allowed**]

2. no error ascertained relevant for processing
   disposition-field=Disposition:*automatic-action/MDN-sent-automatically*;**displayed/warning**
   warning-field = "Warning" ":" *status –[**at least one warning field mandatory**]
   –[**no error or failure field allowed**]

3. Errors ascertained relevant for processing, resend e-mail
   disposition-field=Disposition:*automatic-action/MDN-sent-automatically*;**deleted/error**
   error-field = "Error" ":" *status –[**at least one error field mandatory**]
   warning-field = "Warning" ":" *status –[**warning field optional**]
   –[**no failure field allowed**]

4. Errors ascertained relevant for processing, do not resend e-mail
   disposition-field=Disposition:*automatic-action/MDN-sent-automatically*;**deleted**
   failure-field = "Failure" ":" *status –[**at least one failure field mandatory**]
   error-field = "Error" ":" *status –[**error field optional**]
   warning-field = "Warning" ":" *status –[**warning field optional**]

The wildcards indicated as *status contain the status code as defined in the Appendix. (cf. Chapter 19 – *Appendix Overview of all X-TELEMEDICINE Tags*)

Whether an error is marked as “Warning”,“Error”, or “Failure” is defined by the sender of the notification.

16 Service Part e-mails

The goal of Service Part e-mails is to extend the existing @GIT Teleradiology standard recommendation (versions 1.1 and 1.5) by adding the option to support workflows across vendors. The communication of Service Parts follows the rules of the previous used standards (cf. Chapter 18 – *Further applicable documents*).

The following scenarios are supported by the Service Part e-mails:

1. Communication of data required for time constancy and function testing according to DIN 6868-159.
2. Exchange and management of PGP/GnuPG key data.
3. Exchange and management of address data.

16.1 Basic requirements for all Service Part e-mails

1. All Service Part e-mails must be encrypted and signed compatible to RFC (RFC 3156 and RFC 1847), in accordance with the mechanism defined by the @GIT Teleradiology Standard Recommendation version 1.5 (cf. Chapter 14 – *Digital signature (PGP/MIME)* and Chapter 15 – Transfer format).
2. The replies to the Service Part e-mails must be generated based on the notification mechanism chapter 15.4.2.1.1 Request Receipt Mechanism 1 – MIME Message Disposition Notification (mandatory). For this purpose, the existing error codes (cf. Chapter 20 – *Appendix Error Codes*) have been extended accordingly.
3. The content type of XML data must be text/xml.
4. Service Parts must be send as multipart/mixed.

Recommendation: In order to avoid misuse, the receiver should maintain a whitelist (based on e.g. key IDs) for the processing of Service Part e-mails.

16.2 Structure of Service Part e-mails

All Service Part e-mails contain the X-tag *X-TELEMEDICINE-SERVICEPART* which describes the requested action. This allows filtering of e-mails without

processing the content of the XML document. (Example: *X-TELEMEDICINE-SERVICEPART: ADDRESSUPDATE*)

Each Service Part e-mail contains exactly one document structured as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="" Action=""> <--Action is optional
...
</ServicePart>
```

Fig. 11 - XML structure Service Part e-mail

The attribute *Name* defines the Service Part, and the optional attribute *Action* contains a detailed action. (Example: Name="addressupdate" Action="remove")

16.3 Scenario constancy tests conforming to DIN 6868-159 (mandatory)

To realize this scenario, there are two Service Part e-mails whose implementation is mandatory:

1. The trigger e-mail
2. The protocol e-mail

In addition to the basic requirements, the following requirements must be met:

1. The test data required for the constancy tests are taken from a data pool, which is defined by the partners in the communication.
2. All types of data can be used.
3. The tested communication is always between two DICOM E-MAIL nodes.
4. For the PGP/GnuPG key ID the 8-digit hexadecimal notation of the main key must be used.

A useful realization of the cross-vendor constancy tests as described by DIN 6868-159 is only possible by the interaction of the Service Part trigger e-mail mechanism with the Service Part protocol e-mail.

A typical process is illustrated by the following flowchart. It shows a potential process for the test of the transfer speed between the communication partners B and C. The test is initiated by administrator A. This means that the transfer of test data is done between B and C. Subsequently, the communication protocol is transmitted by the communication partner B to the administrator A.

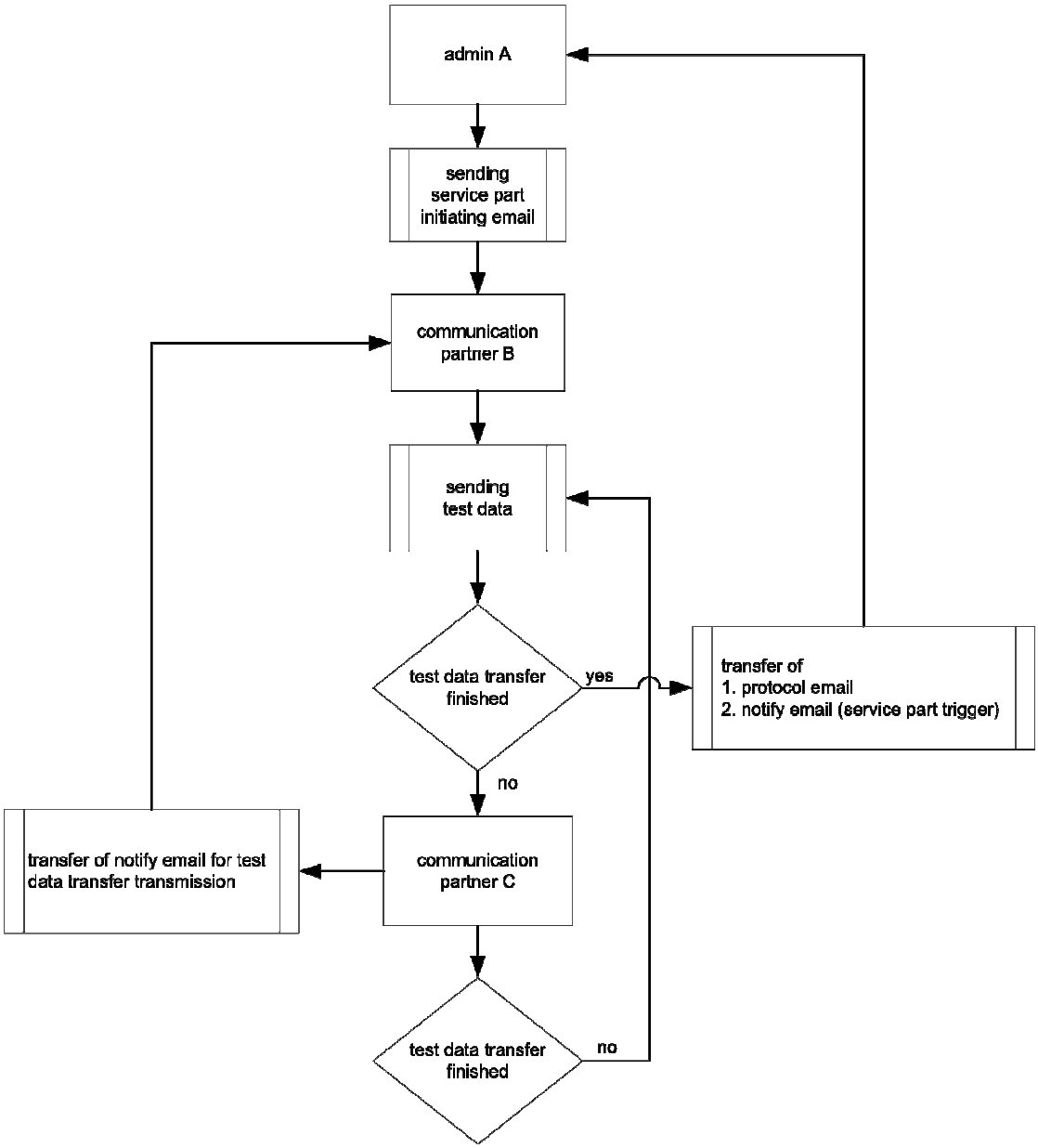

Fig. 12 – Sample process: constancy test by Service Part trigger e-mail

16.4 Service Part trigger e-mails

Used X-tags: X-TELEMEDICINE-SERVICEPART:TESTTRANSFER, DISPOSITION-NOTIFICATION-TO

Trigger e-mails can be used to initiate two processes:

1. A test transfer between to partners using the specified test data.
2. Generation of a confirmation e-mail.

A trigger e-mail has the following additional data:

1. *X-TELEMEDICINE-SERVICEPART:TESTTRANSFER* and *DISPOSITION-NOTIFICATION-TO* in the e-mail header.
2. Attachment of a XML file (text/xml) to the e-mail body using the following XML structure.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="TESTTRANSFER" Action="QOSCHECK">
 <TestDataReceiver>
  <EmailAddress />   <- E-mail address of the data receiver
  <GPGKeyID />   <- (optional)
 </TestDataReceiver>
 <ProtocolReceiver> <- (optional)
  <EmailAddress />   <- Protocol e-mail receiver address
  <GPGKeyID />   <- (optional)
 </ProtocolReceiver>
 <TestDataSetID /> <- [e.g. TESTDATASET_1 (cf. Appendix Test Data Set IDs)]
 <ErrorTimeOut /> <- (optional) timeout in [s] for sending the test protocol
</ServicePart>
```

Fig. 13 – XML structure Service Part trigger e-mail

The value of the attribute *Action* defines which actions are initiated by a trigger e-mail. The attribute can have the following value:

1. QOSCHECK – this triggers a constancy test according to DIN 6868-159.

The node *TestDataSetID* describes which defined data set should be transmitted, and must occur only once. *TestDataSetID* can have the following values:

1. The values defined in the Appendix Test Data Set IDs
2. An alphanumeric ID of max. 64 characters, freely selectable, of any test data set to be defined by the test partners.

There can be two responses to a trigger e-mail:

1. Dispatch of a confirmation e-mail (15.4.2.2.1 Reply on data reception – Mechanism 1) to the sender of the trigger e-mail when the test transmission is complete.
2. Dispatch of an e-mail protocol to the receiver specified in the trigger e-mail. This e-mail contains an XML protocol file as an attachment.

The following Fig. 14 – Example of a Service Part trigger shows an example of a trigger e-mail.

```
From: radiology_mannheim@teleradiology.de
To: radiology_mainz@teleradiologie.de
Subject: Request for testtransfer
Date: Mon, 1 Jan 2009 15:15:35 +0100
MIME-Version: 1.0
Message-Id: 83BF3401-0840-4268-83CD-610AF6259FD6@teleradiology.de
X-TELEMEDICINE-SERVICEPART: REQUEST-FOR-TESTTRANSFER
Disposition-Notification-To: radiology_mannheim@teleradiologie.de
Content-Type: multipart/encrypted; protocol="application/pgp-encrypted";
boundary="01BF27A0.9BE21980/teleradiology.de"

--01BF27A0.9BE21980/teleradiology.de
Content-Type: application/pgp-encrypted

Version: 1

--01BF27A0.9BE21980/teleradiology.de
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.1*

%Content-Disposition: attachment; filename="ServicePart.xml"
%Content-Type: text/xml; // application/xml is also valid but not recommended
%Content-Transfer-Encoding: quoted-printable
%
%<?xml version="1.0" encoding="UTF-8"?>
%<ServicePart Name="TESTTRANSFER" Action="QOSCHECK">
%  <TestDataReceiver>
%   <EmailAddress>DrMeyer@homeoffice.de</EmailAddress>
%   <GPGKeyID>AA76CA08</GPGKeyID>
%  </TestDataReceiver>
%
%  <ProtocolReceiver>
%   <EmailAddress>admin@teleradiology.de </EmailAddress>
%   <GPGKeyID>D4762A08</GPGKeyID>
%  </ProtocolReceiver>
%
%  <TestDataSetID>TESTDATASET_1</TestDataSetID>
%</ServicePart>

-----END PGP MESSAGE-----

--01BF27A0.9BE21980/teleradiology.de--
```

* The lines marked % are PGP/OpenPGP encrypted.

Fig. 14 – Example of a Service Part trigger e-mail

This sample e-mail should trigger the following actions:

1. On side of the receiver, the defined function test data set (TESTDATASET_1) is sent to the e-mail address DrMeyer@homeoffice.de. For encryption the key with the KeyID AA76CA08 is used.
2. The protocol XML file (cf. Fig. 15 – Schematic structure Service Part protocol) is sent to the e-mail address admin@teleradiologie.de. For encryption the key with the KeyID D4762A08 is used.

3. Dispatch of the confirmation e-mail is done with Mechanism 1 (15.4.2.2.1 Reply on data reception – Mechanism 1) including the message regarding the success or failure of the test transfer to the address radiology_mannheim@teleradiology.de.

16.5 Service Part protocol e-mails (mandatory)

Used X-tags: X-TELEMEDICINE-SERVICEPART:PROTOCOL

The implementation of the Service Part protocol e-mail is mandatory, and is requested by the trigger e-mail described above. The protocol e-mail has the following additional data:

1. The e-mail header is extended by the X tag *X-TELEMEDICINE-SERVICEPART:PROTOCOL*.
2. Only one protocol file per Service Part protocol e-mail must be sent.

The protocol e-mail is sent automatically upon transmission of the test data. The schematic structure of this e-mail is shown by the following Fig. 15.

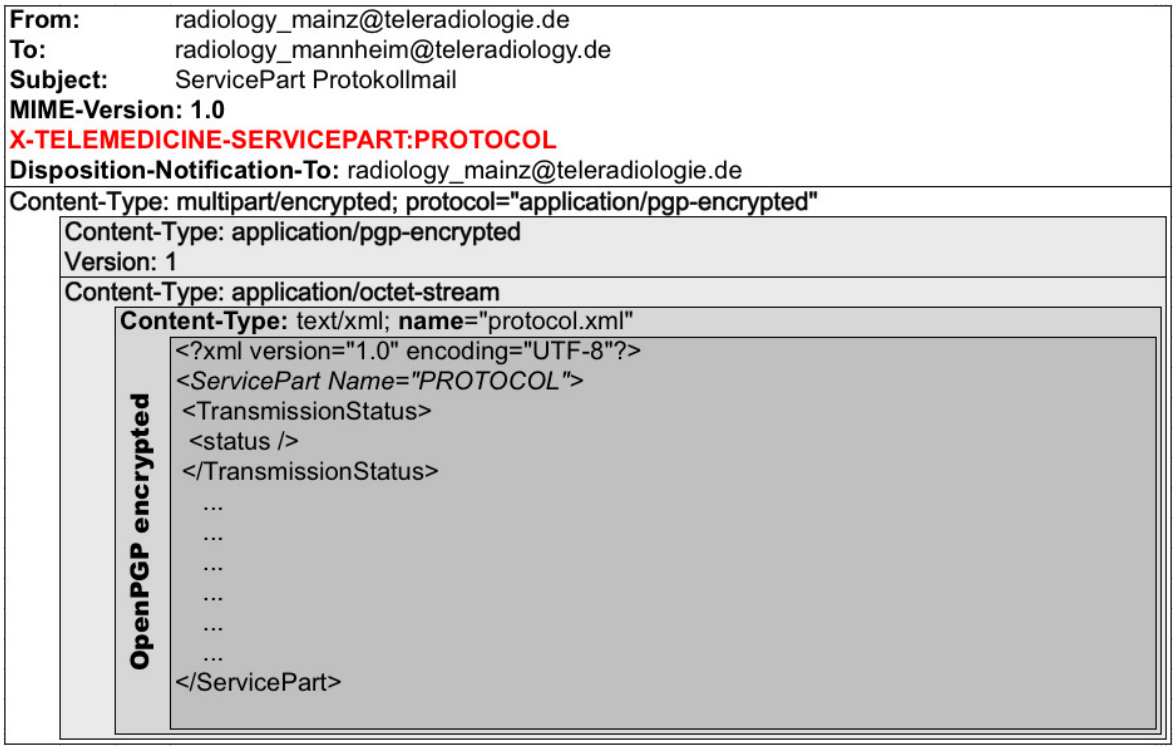

Fig. 15 – Schematic structure Service Part protocol e-mail

The XML structure of the protocol file is shown by the following Fig. 16.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="PROTOCOL">

  <TransmissionStatus />   <- Possible states are COMPLETED, ABORTED
  <TestDataSetID />   <- ID of the transfered testdata set

  <ObjectsSent>
    <Count />    <- Count of the transfered objects
  </ObjectsSent>

  <ObjectsReceivedConfirmed> <- Summary of all DatagramMail nodes
   <Count />   <- Count of transfered and verified objects
   <Time />   <- Transmission period (beginning with the transfer of the data package and ending with
                 the last verification e-mail) in seconds
   <MailSize />   <- Size combined of all verified e-mails in Byte
   <ObjectSize /> <- Size combined of all verified objects in Byte
  </ObjectsReceivedConfirmed>

  <DataSender>
    <EMailAddress />   <- e-mail address of the testdata set sender
  </DataSender>

  <DataRecipient>
    <EMailAddress />   <- e-mail address of the testdata set receiver
  </DataRecipient>

  <ProtocolRecipient>
   <EMailAddress />   <- e-mail address of the protocol receiver
  </ProtocolRecipient>

  <ErrorTimeOut />   <- Period in seconds, defining when receiving disturbances are to be regarded as
                        errors.

  <DatagramMail EMailMessageID="">   <- This block can be repeated arbitrary
   <ErrorID />   <- In case of an error: The tag contains the error code according to the error code list.
                    The tag is optional in the absence of an error.
   <EMailContentID />   <- opt. ContentID for Multipart Mails
   <StartDateTime />   <- Data transmission start date and time (Format yyyymmddhhmmss)
   <NotifyDateTime />   <- Notify e-mail receiving date and time (Format yyyymmddhhmmss)
   <MailSize />   <- Total size of all transmitted e-mails in Byte
   <ObjectSize />   <- Total size of all transmitted objects in Byte
  </DatagramMail>

</ServicePart>
```

Fig. 16 – XML structure Service Part protocol

16.6 Scenario exchange of key data (mandatory)

Used X-tags: X-TELEMEDICINE-SERVICEPART:KEYUPDATE, DISPOSITION-NOTIFICATION-TO

The management of the GPG key data is part of the essential administrative tasks in a telemedicine network. The present version of the @GIT Standard Recommendation enables cross-vendor realization. The implementation is mandatory.

For the key management, the following actions are supported:

1. Adding or updating of keys.
2. Withdrawal of keys.

The *X-TELEMEDICINE-SERVICEPART:KEYUPDATE* tag is added to the e-mail header. The subsequent XML structure is attached as a file (content type „text/xml“). The *DISPOSITION-NOTIFICATION-TO* tag can be used to request a confirmation e-mail.

Only one XML file per Service Part e-mail must be transmitted.

16.6.1 Adding or updating keys

To add or update keys the *Action* of the following XML structure needs to be given the value *“SET”*.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="KEYUPDATE" Action="SET">
 <PublicKeyASCIIData />  <- ASCII armored Public GPG Key
</ServicePart>
```

Fig. 17 – XML structure for adding a key

16.6.2 Withdrawal of keys

For removing a key the *Action* of the following XML structure needs to be given the value *„REMOVE“*.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="KEYUPDATE" Action="REMOVE">
 <GPGKeyID />  <- GPG KeyID of the invalid key
</ServicePart>
```

Fig. 18 – XML structure for withdrawal of an existing key

16.7 Scenario exchange of address data (mandatory)

Used X-tags: X-TELEMEDICINE-SERVICEPART:ADDRESSUPDATE, DISPOSITION-NOTIFICATION-TO

The exchange of communication data is a further important task for the management of a telemedicine network. Realization of the exchange of address data is mandatory.

For the management of address data, the following two actions are supported:

1. Adding or updating communication data.
2. Erasing communication data.

The header of the Service Part e-mail is extended by the X-tag *X-TELEMEDICINE-SERVICEPART:ADDRESSUPDATE*. The subsequent XML structure is attached as a file (content type „text/xml“). Optionally the tag *DISPOSITION-NOTIFICATION-TO* can be used to request a confirmation e-mail.

Only one XML file per Service Part e-mail must be transmitted.

16.7.1 Adding and changing address data

To add or update address data the attribute *Action* of the following XML structure needs to be given the value *„SET“*.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="ADDRESSUPDATE" Action="SET">
 <Connection>
  <ID />  <- (opt.) ambiguous identifier of a specific communication channel
  <DisplayConnectionName />  <- Communication channel name as displayed to the user
  <Mailserver />  <- (opt.) IP or FQDN of the SMTP e-mail server
  <Port />  <- (opt.) SMTP Port
  <EmailAddress />  <- Receiver e-mail address
  <GPGKeyID />  <- GPG KeyID of the public GPG key to be used for this connection
 </Connection>
</ServicePart>
```

Fig. 19 – XML structure exchange of address data

Note: In case the optional ID tag is not used, it is not possible to modify or erase communication data at a later time.

16.7.2 Erasing address data

To remove address data the attribute *Action* of the following XML structure needs to be given the value *„REMOVE“*.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="ADDRESSUPDATE" Action="REMOVE">
 <Connection>
  <ID />  <- ambiguous identifier of a specific communication channel
 </Connection>
</ServicePart>
```

Fig. 20 – XML structure exchange of address date

17 Generating identification numbers

17.1 Advice

Please note that in the context of the telemedicine identification numbers (e.g. *X-TELEMEDICINE-STUDYID*, *X-TELEMEDICINE-SETID, …) must not* allow any inferences regarding identity of patients.

17.2 DICOM UID

The DICOM-Root-UIDs required for the generation of valid DICOM UIDs can be obtained free of charge via Medical Connections (http://www.medicalconnections.co.uk/Free_UID) or commercially at the official institution responsible for your country.

18 Further applicable documents

18.1 RFC

- RFC1652 - SMTP Service Extension for 8bit-MIMEtransport
- RFC1734 - POP3 AUTHentication command
- RFC1846 - SMTP 521 Reply Code
- RFC1847 - Security Multiparts for MIME: Multipart/Signed and Multipart/ Encrypted
- RFC1939 / STD0053 - Post Office Protocol - Version 3
- RFC2034 - SMTP Service Extension for Returning Enhanced Error Codes
- RFC2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
- RFC2046 - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
- RFC2195 - IMAP/POP AUTHorize Extension for Simple Challenge/Response
- RFC2392 - Content-ID and Message-ID Uniform Resource Locators
- RFC2554 - SMTP Service Extension for Authentication
- RFC2595 - Using TLS with IMAP, POP3 and ACAP
- RFC2821 - Simple Mail Transfer Protocol
- RFC3030 - SMTP Service Extensions for Transmission of Large and Binary MIME Messages
- RFC3156 - MIME Security with OpenPGP
- RFC3206 - The SYS and AUTH POP Response Codes
- RFC3207 - SMTP Service Extension for Secure SMTP over Transport Layer Security
- RFC3462 - The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages
- RFC3798 - Message Disposition Notification
- RFC4880 - OpenPGP Message Format

18.2 DICOM Standard

- DICOM Standard, Suppl. 54 - DICOM MIME Content-Type

18.3 German Regulations

- Verordnung über den Schutz vor Schäden durch Röntgenstrahlen („Röntgenverordnung“, *German X-ray Ordinance*) – Revised Version Announced 30 April 2003 I 604
- Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz, SigG, *Law on the General Requirements for Electronic Signatures*) – Status: Modified by Art. 1 G, 4 January 2005 I 2
- Verordnung zur elektronischen Signatur (Signaturverordnung, *Electronic Signature Ordinance*) – Status: Modified by Art. 2 G, 4 January 2005 I 2

19 Appendix Overview of all X-TELEMEDICINE Tags

19.1.1.1 X-TELEMEDICINE-STUDYID

For mapping of NON-DICOM data with DICOM studies

19.1.1.2 X-TELEMEDICINE-SETID

For grouping of associated e-mail to sets

19.1.1.3 X-TELEMEDICINE-SETPART

To identify an e-mail belonging to a set

19.1.1.4 X-TELEMEDICINE-SETTOTAL

To identify the last e-mail belonging to a set (total number of all parts)

19.1.1.5 X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO

To request X-Telemedicine notifications to this e-mail address

19.1.1.6 X-TELEMEDICINE-DISPOSITION-NOTIFICATION-KEYID

To request encrypted X-Telemedicine notifications for this GPG keyid

19.1.1.7 X-TELEMEDICINE-ORIGINAL-CONTENT-ID

Original content ID for encrypted confirmation e-mails

19.1.1.8 X-TELEMEDICINE-SERVICEPART

To identify Service Part operations

20 Appendix Error Codes

Code	Meaning
Undefiniert	
0	vendor specific errors
Mail	
1	mail-error
1.1	mail-receipt-error
1.1.1	mail-receipt-failed
1.1.2	mail-receipt-was-read-before
1.2	mail-syntax-error
1.2.1	mail-syntax-header-error
1.2.1.1	mail-syntax-header-contentid-error
1.2.1.1.1	mail-syntax-header-contentid-missing
1.2.1.2	mail-syntax-header-dispo_to-error
1.2.1.2.1	mail-syntax-header-dispo_to-missing
1.2.1.3	mail-syntax-header-contenttype
1.2.1.3.1	mail-syntax-header-contenttype-missing
1.2.2	mail-syntax-body-error
1.2.2.1	mail-syntax-body-empty
1.2.2.2	mail-syntax-body-missing
1.3	mail-attachment-error
1.3.1	mail-attachment-corrupt
1.4	mail-mimetype-error
1.4.1	mail-mimetype-not-processed
1.4.2	mail-mimetype-not-supported
1.5	mail-security-error
1.5.1	mail-security-signature-error
1.5.1.1	mail-security-signature-missing
1.5.2	mail-security-encryption-error
1.5.2.1	mail-security-encryption-missing
1.6	mail-message/partial-error
1.6.1	mail-message/partial-part-error
1.6.1.1	mail-message/partial-part-missing
1.6.1.2	mail-message/partial-part-twice
1.6.1.3	mail-message/partial-part-header-error
1.6.1.3.1	mail-message/partial-part-header-id-error
1.6.1.3.1.1	mail-message/partial-part-header-id-missing
1.6.1.3.2	mail-message/partial-part-header-number-error
1.6.1.3.2.1	mail-message/partial-part-header-number-missing
1.6.1.3.3	mail-message/partial-part-header-total-error
1.6.1.3.3.1	mail-message/partial-part-header-total–missing
OpenPGP	
2	gpg-error
2.1	gpg-signature-error

2.1.1	gpg-signature-bad
2.1.2	gpg-signature-expired
2.2	gpg-key-error
2.2.1	gpg-key-expired
2.2.1.1	gpg-key-expired-sender
2.2.1.2	gpg-key-expired-receiver
2.2.2	gpg-key-revoked
2.2.2.1	gpg-key-revoked-sender
2.2.2.2	gpg-key-revoked-receiver
2.2.3	gpg-key-trust-error
2.2.3.1	gpg-key-trust-undefined
2.2.3.2	gpg-key-trust-never
2.2.3.3	gpg-key-trust-marginal
2.2.4	gpg-key-missing-error
2.2.4.1	gpg-key-missing-public
2.2.4.2	gpg-key-missing-private
2.2.5	gpg-key-signature-error
2.2.5.1	gpg-key-signature-expired
2.2.5.2	gpg-key-signature-revoked
2.3	gpg-passphrase-error
2.3.1	gpg-passphrase-bad
2.3.2	gpg-passphrase-missing
2.4	gpg-decryption-error
2.4.1	gpg-decryption–failed

Application

3	application-error
3.1	application-extern-error
3.2	application-intern-error
3.2.1	application-intern-attachment-error
3.2.1.1	application-intern-attachment-not-processed
3.2.2	application-intern-mimetype-error
3.2.2.1	application-intern-mimetype-unknown
3.2.2.2	application-intern-mimetype-not-processed
3.3	application-permission-error

XTelemedicine

4	x-telemedicine-error
4.1	x-telemedicine-studyid-error
4.1.1	x-telemedicine-studyid-missing-for-nondicom
4.1.2	x-telemedicine-studyid-not-allowed-for-dicom
4.2	x-telemedicine-set-tag-error
4.2.1	x-telemedicine-set-tag-content-differs
4.2.2	x-telemedicine-set-tag-intern-error
4.2.2.1	x-telemedicine-set-tag-intern-missing
4.2.2.2	x-telemedicine-set-tag-intern-id-error
4.2.2.2.1	x-telemedicine-set-tag-intern-id-missing
4.2.2.3	x-telemedicine-set-tag-intern-part-error
4.2.2.3.1	x-telemedicine-set-tag-intern-part-missing
4.2.2.4	x-telemedicine-set-tag-intern-total

4.2.2.4.1	x-telemedicine-set-tag-intern-total-missing
4.2.3	x-telemedicine-set-tag-extern-error
4.2.3.1	x-telemedicine-set-tag-extern-missing
4.2.3.2	x-telemedicine-set-tag-extern-differs
4.2.3.3	x-telemedicine-set-tag-extern-id-error
4.2.3.3.1	x-telemedicine-set-tag-extern-id-missing
4.2.3.3.2	x-telemedicine-set-tag-extern-id-differs
4.2.3.4	x-telemedicine-set-tag-extern-part-error
4.2.3.4.1	x-telemedicine-set-tag-extern-part-missing
4.2.3.4.2	x-telemedicine-set-tag-extern-part-differs
4.2.3.5	x-telemedicine-set-tag-extern-total-error
4.2.3.5.1	x-telemedicine-set-tag-extern-total-missing
4.2.3.5.2	x-telemedicine-set-tag-extern-total-differs
4.3	x-telemedicine-disposition-notification-tag-error
4.3.1	x-telemedicine-disposition-notification-tag-keyid-error
4.3.1.1	x-telemedicine-disposition-notification-tag-keyid-missing
4.3.2	x-telemedicine-disposition-notification-tag-to-error
4.4	x-telemedicine-contentid-error
4.4.1	x-telemedicine-contentid-missing

ServiceParts

5	servicepart-error
5.1	servicepart-protocol-error
5.1.1	servicepart-protocol-creation-error
5.2	servicepart-testtransfer-error
5.2.1	servicepart-testtransfer-testdataset-not-found
5.2.2	servicepart-testtransfer-testimages-not-found
5.3	servicepart-keyupdate-error
5.3.1	servicepart-keyupdate-addkey-error
5.3.2	servicepart-keyupdate-updatekey-error
5.3.3	servicepart-keyupdate-removekey-error
5.4	servicepart-addressupdate-error
5.4.1	servicepart-addressupdate-addaddress-error
5.4.2	servicepart-addressupdate-updateaddress-error
5.4.3	servicepart-addressupdate-removeaddress-error
5.5	servicepart-unsupported

Each error code can be extended by ".0" (user defined / application specific).

Example: 2.1.0.2 (potential meaning: no public key available, no GPG installed)

Proposals for further codes can be submitted using the website:
http://tele-x-standard.de

21 Appendix Test Data Set IDs

Requirements:

1. The test data set ID must consist of max. 64 alphanumeric characters.
2. Any number of test diagram data sets can be defined.
3. It is mandatory to implement the defined IDs as well as the possibility to add any further test diagram data sets.

Test Data Set ID	Descriptions
TESTDATASET_1	Function test data set (for the daily function test in accordance with DIN 6868-159)
TESTDATASET_2	Largest test diagram data set or equivalent (for the monthly constancy test according to DIN 6868-159)
TESTDATASET_CT_HEAD	Test data set CT head
TESTDATASET_CT_NECK	Test data set CT neck
TESTDATASET_CT_THORAX	Test data set CT thorax
TESTDATASET_CT_ABDOMEN	Test data set CT abdomen
TESTDATASET_CT_UPPER_EXTREMITY	Test data set CT upper extremities
TESTDATASET_CT_LOWER_EXTREMITY	Test data set CT lower extremities
TESTDATASET_CT_JOINTS	Test data set CT joints
TESTDATASET_CT_HAND	Test data set CT hand
TESTDATASET_CT_FOOT	Test data set CT foot
TESTDATASET_CT_FULLBODY_TRAUMA	Test data set CT full body/trauma
TESTDATASET_CT_ANGIO_ABDOMEN	Test data set CTA abdomen
TESTDATASET_CT_ANGIO_EXTREMITIES	Test data set CTA extremities
TESTDATASET_CR_THORAX	Test data set conventional X-ray images thorax
TESTDATASET_CR_ABDOMEN	Test data set conventional X-ray images abdomen
TESTDATASET_CR_EXTREMITIES	Test data set conventional X-ray images extremities