@GIT Initiative

zur Standardisierung

von Telemedizin

Empfehlung

für ein standardisiertes

Teleradiologie Übertragungsformat

Version 1.6

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

1. Inhaltsverzeichnis

2. Impressum

Initiative zur Standardisierung von Telemedizin der Arbeitsgemeinschaft Informationstechnologie der Deutschen Röntgengesellschaft
E-Mail: teleradiologie@drg.de
URL: http://www.tele-x-standard.de

Titel: Empfehlung für ein standardisiertes Teleradiologie Übertragungsformat
Version: 1.6

Mitwirkende Arbeitsgruppenmitglieder (in alphabetischer Reihenfolge)

Name	Organisation	Versionen
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
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

Letzte Revision: 30.06.2010

3. Kontakt

Der Kontakt zu der Initiative kann jederzeit über nachfolgende E-Mail-Adresse hergestellt werden: *teleradiologie@drg.de*. Wir nehmen auf Wunsch auch gerne neue Interessenten in unseren Verteiler auf. Eine kurze formlose E-Mail genügt.

Selbstverständlich werden alle Daten streng vertraulich behandelt. Insbesondere eine Weitergabe an Dritte erfolgt nicht.

Die Ergebnisse der Initiative werden über das Internet unter der Adresse *http://www.tele-x-standard.de* der Öffentlichkeit zur Verfügung gestellt.

4. Copyright

Das Copyright der Empfehlungen liegt bei der Deutschen Röntgengesellschaft.

Diese hat jedoch kein Recht, die Ergebnisse zu veräußern oder das Lizenzmodell (Public Domain) zu ändern. Kostenbeiträge für Drucksachen etc. können erhoben werden.

5. Präambel

Die @GIT Initiative zur Standardisierung von Telemedizin hat sich zu dem Zweck der Entwicklung einer Empfehlung für ein für die Teleradiologie geeignetes Kommunikationsprotokoll zusammengefunden. Die Mitglieder setzen sich aus verschiedenen universitären Einrichtungen, Forschungseinrichtungen und Industrievertretern zusammen. Jeder, der einen Beitrag leisten möchte, kann der Gruppe beitreten.

Die Ergebnisse sind jetzt und in Zukunft für die Allgemeinheit frei verfüg- und nutzbar (Public Domain).

6. Vorwort zur Version 1.6

Die vorliegende Version 1.6 der Standardempfehlung steht ganz im Zeichen der Unterstützung administrativer Tätigkeiten.

Seit dem 01.03.2009 gibt es in Deutschland eine neue Norm zu Abnahme- und Konstanzprüfung in der Teleradiologie nach Röntgenverordnung (DIN 6868-159). Diese stellt die Anforderungen an den technischen Ablauf und die Rahmenbedingungen für die Durchführung von Teleradiologie nach Röntgenverordnung (RöV). Ein wesentlicher Bestandteil sind die Empfehlungen zur Funktions- und Übertragungszeitkonstanzprüfung teleradiologischer Einrichtungen. Insbesondere in Netzwerken, die nicht nur Software eines Herstellers einsetzen stellen diese Anforderungen die Betreiber vor neue Herausforderungen. Eine weitere Herausforderung entsteht durch das Zusammenwachsen bestehender Netzwerke. Die Grundandforderung besteht hier in einem herstellerübergreifenden Austausch von Kommunikationsdaten.

Als eine Lösung für diese Anforderungen werden mit der Version 1.6 sogenannte Service Part E-Mails eingeführt. Basierend auf den bisher in den Versionen 1.1 und 1.5 verwendeten Standards können nun folgende Szenarien durch die @GIT Teleradiologie Standardempfehlung abgebildet werden:

1. Die herstellerübergreifende Kommunikation der nach DIN 6868-159 notwendigen Daten zur Konstanz- und Funktionsprüfung.
2. Der herstellerübergreifende Austausch von PGP/ GnuPG-Schlüsseldaten.
3. Der herstellerübergreifende Austausch von Adressdaten.

Die Rückmeldungen über die durchgeführten Aktionen werden nach dem, in der Version 1.5 beschriebenen Benachrichtigungsmechanismus verschickt.

Autoren der Arbeitsgruppe

im Juni 2010

7. Vorwort zur Version 1.5

Mit der Version 1.1 ist bereits eine Möglichkeit des herstellerunabhängigen Datentransfers ermöglicht worden. In der vorliegenden Version 1.5 sind zusätzlich folgende Erweiterungen behandelt:

1. Mechanismus zur Überprüfung des vollständigen Empfangs auf der Seite des Empfängers. Hierzu werden vom Absender zusätzliche Informationen den Datenpaketen hinzugefügt, die beim Empfang auf Seiten des Empfängers ausgewertet werden können. Hierdurch kann ein Empfänger sicherstellen, dass er tatsächlich alle vom Absender gesendeten Datenpakete empfangen.
2. Mechanismus zur Überprüfung des vollständigen Empfangs auf der Seite des Absenders. Hierzu werden vom Empfänger Bestätigungsmeldungen mit definiertem Status an den Absender versendet. Hierdurch kann ein Absender sicherstellen, dass alle versendeten Datenpakete auch tatsächlich beim Empfänger angekommen sind.
3. Mechanismus zur Überprüfung der Authentizität des Absenders und der Integrität der Datenpakete. Hiermit können Veränderungen der Datenpakete durch Dritte erkannt werden und unerwünschte Datenpakete können abgewiesen werden.

Autoren der Arbeitsgruppe

im Oktober 2005

8. Errata

8.1 Version 1.5

8.1.1 Fehler in Abbildung - Empfangsbestätigung nach RFC 3798

Das nachfolgend aufgeführte Beispiel enthält einen Fehler im maschinenlesbaren Abschnitt bei der Trennung zwischen Header und Body (siehe Pfeil in Abb. 1 – Fehlerhafte Empfangsbestätigung nach RFC 3798). Hier müßte eine Trennung durch Einfügen einer Leerzeile nach dem Content-Type herbeigeführt werden. Dieser Fehler muß ab der Umsetzung der Standardempfehlung Version 1.6 in der Software (gemäß Beispiel Abb. 9 – Empfangsbestätigung nach RFC 3798) behoben werden.

```
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

 An dieser Stelle ist Freitext möglich

--RAA14128.773615765/teleradiology.de
content-type: message/disposition-notification
Reporting-UA: post.teleradiology.de; Mailprogramm 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--
```

Abb. 1 – Fehlerhafte Empfangsbestätigung nach RFC 3798

9. Grundüberlegung

Die vorgestellte Empfehlung basiert auf der Annahme, dass der E-Mail Versand mit verschlüsselten Daten den kleinsten gemeinsamen Nenner für einen sicheren Austausch von nicht anonymisierten oder pseudonymisierten medizinischen Daten darstellt.

10. Mindestanforderungen an die Software

10.1 Transferdatentypen

Grundsätzlich muss jeder Datentyp (DICOM & Nicht-DICOM) übertragen werden können. Wird ein Datentyp empfangen, den die Software nicht verarbeiten kann, sollten diese Daten an ein anderes Programm weitergeleitet oder zwischengespeichert werden. In jedem Fall darf der Empfang unbekannter Objekte nicht zu einem Empfangsabbruch führen.

10.2 MIME Standard

Unterstützung des MIME Standards[1], insbesondere von Multipart Mail, Message Partial sowie die Verwendung von X-Tags.

11. Erweiterte Anforderungen an die Software

Die zum Zeitpunkt der Entstehung dieses Dokuments noch ausstehenden Richtlinie Teleradiologie bzw. eine entsprechende DIN Norm wird voraussichtlich eine zusätzliche Leitungsverschlüsselung fordern. Für den Einsatz der Software zum Zweck der Teleradiologie nach Röntgenverordnung sollten daher zusätzlich die Sicherheitsvarianten der Mail-Protokolle (SMTP, POP3 bzw. IMAP4) unterstützt werden.

12. Verschlüsselung & Kompression

Die Verschlüsselung der Daten erfolgt OpenPGP kompatibel (RFC 4880). Die Verwendung der in OpenPGP enthaltenen ZIP-Kompression ist optional, die Nutzung des Kompressionsverfahrens wird aber bei einer größeren Transferdatenmenge empfohlen.

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

13. Digitale Signatur (PGP/MIME)

PGP/ GnuPG können sowohl zur Verschlüsselung als auch zur Signierung von Daten verwendet werden. Im Rahmen dieser Empfehlung werden gemäß RFC 3156 und RFC 1847 folgende beide Verfahren empfohlen:

- Gleichzeitige E-Mail-Verschlüsselung mit Signierung. (RFC 3156, Kapitel 6.2 - *Combined method*)
- Daten mit einer abgetrennten Signatur, welche gemäß RFC 1847 OpenPGP kompatibel verschlüsselt werden. (RFC 3156, Kapitel 6.1 - *Encapsulation*)

Es ist für den Datentransfer nach der vorliegenden Standardempfehlung ab Version 1.5 verpflichtend, die Daten mit einer der beiden Methoden zu signieren und zu verschlüsseln.

14. Transferformat

14.1 DICOM-Daten

DICOM-Daten werden in eine DICOM E-Mail nach Suppl. 54 des DICOM-Standards überführt. Die neu entstandene DICOM E-Mail wird OpenPGP kompatibel verschlüsselt und signiert (Abb. 2) (siehe Kapitel 13 - *Digitale Signatur (PGP/MIME)*).

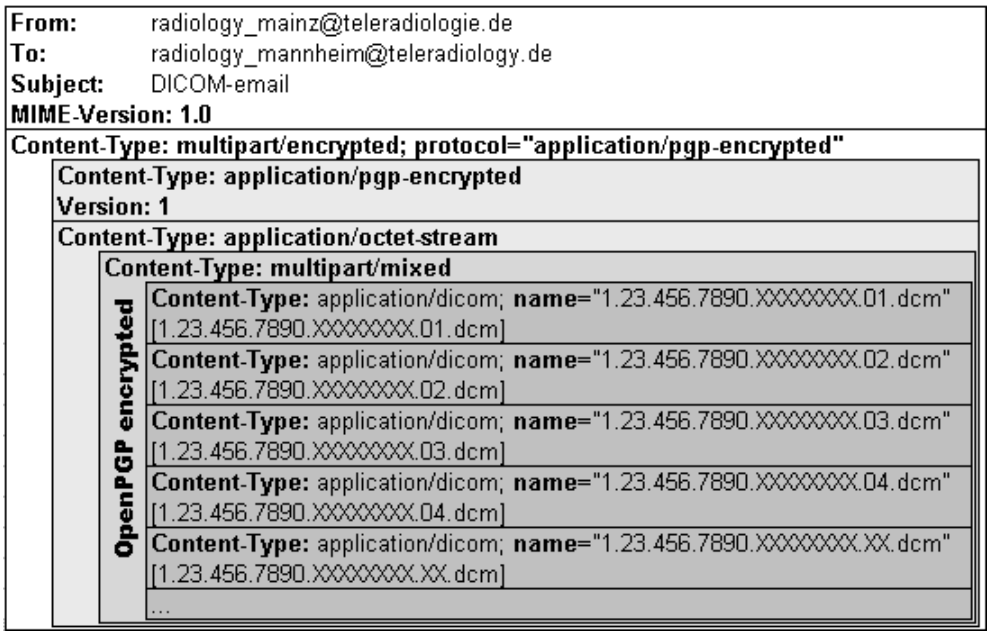

Abb. 2 – Transferformat für DICOM-Daten

14.2 Nicht-DICOM-Daten

Verwendete X-Tags: X-TELEMEDICINE-STUDYID

Nicht-DICOM-Daten verfügen über keinen Header mit Patienteninformationen. Aus diesem Grund wurde, konform zum MIME Standard, ein neues X-Tag *X-TELEMEDICINE-STUDYID* definiert. Diesem Tag wird die StudyInstanceUID [0020:000D] aus einem gegebenfalls vorhanden DICOM-Header zugewiesen um die Zuordnung zwischen Nicht-DICOM Daten und einer DICOM Studie zu ermöglichen. Gibt es keine passende DICOM Studie oder StudyInstanceUID muss eine neue UID erzeugt und den Nicht-DICOM Daten zugeordnet werden (siehe Kapitel 16 - Generierung von Identifikationsnummern). Alle Nicht-DICOM Daten werden zusammen mit allen DICOM-Daten OpenPGP kompatibel verschlüsselt und signiert (Abb. 3 – Transferformat für Nicht-DICOM-Daten). Es können damit auch Daten von unterschiedlichen Untersuchungen oder unterschiedlichen Patienten innerhalb einer einzigen E-Mail gemeinsam verschickt werden. Ebenso können zusammengehörige Daten in unterschiedlichen E-Mails verschickt werden, die Zuordnung erfolgt dabei immer über die entsprechende StudyInstanceUID (bei DICOM-Daten) und die *X-TELEMEDICINE-STUDYID* (bei Nicht-DICOM-Daten).

Eine Verwendung der *X-TELEMEDICINE-STUDYID* bei DICOM-Daten ist nicht zulässig und muss auf Empfängerseite ignoriert werden. (Gebot der Eindeutigkeit)

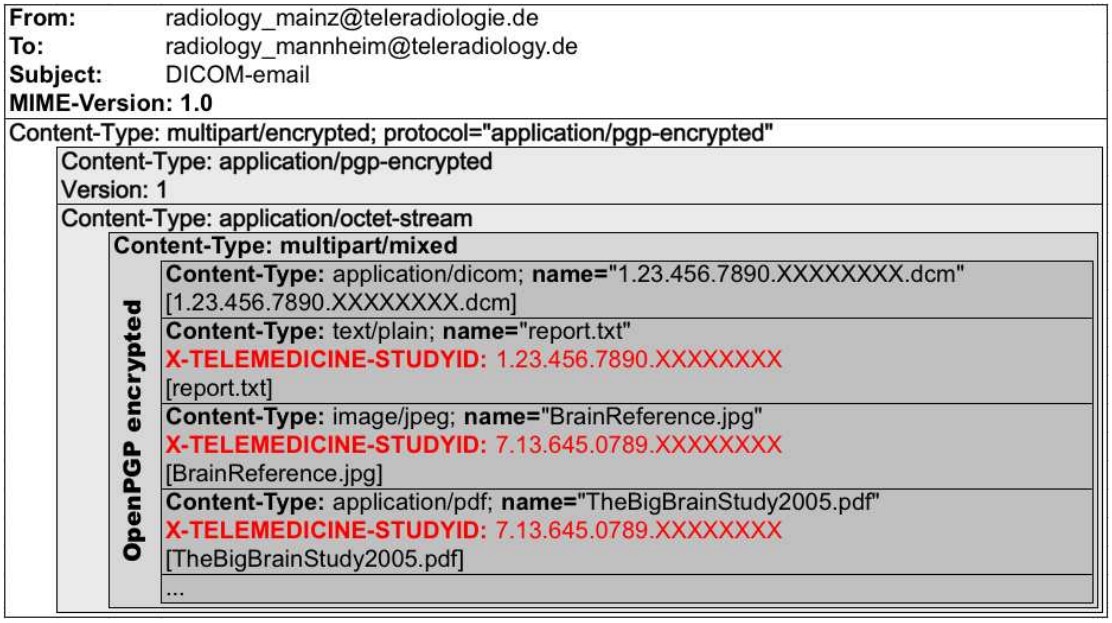

Abb. 3 – Transferformat für Nicht-DICOM-Daten

14.3 Message/Partial

In der Synopsis (Abb. 4 – Synopsis des Datentransfers) werden die Daten verschlüsselt als PGP/MIME Multipart E-Mail verschickt. Im MIME Standard (RFC 2046, Kapitel 5.2.2 - *Partial Subtype)* ist eine Auftrennung von größeren E-Mails in mehrere kleine E-Mails vorgesehen (message/partial). Dies erfolgt entweder durch die Versandsoftware oder durch einen am Versand beteiligten Mail-Server (Abb. 4 ① message/partial). Für den Empfangsprozess muss dies berücksichtigt werden, so dass dieser in der Lage ist, die einzelnen Teile wieder in die Ursprungsmail (Abb. 4 ②) zu überführen.

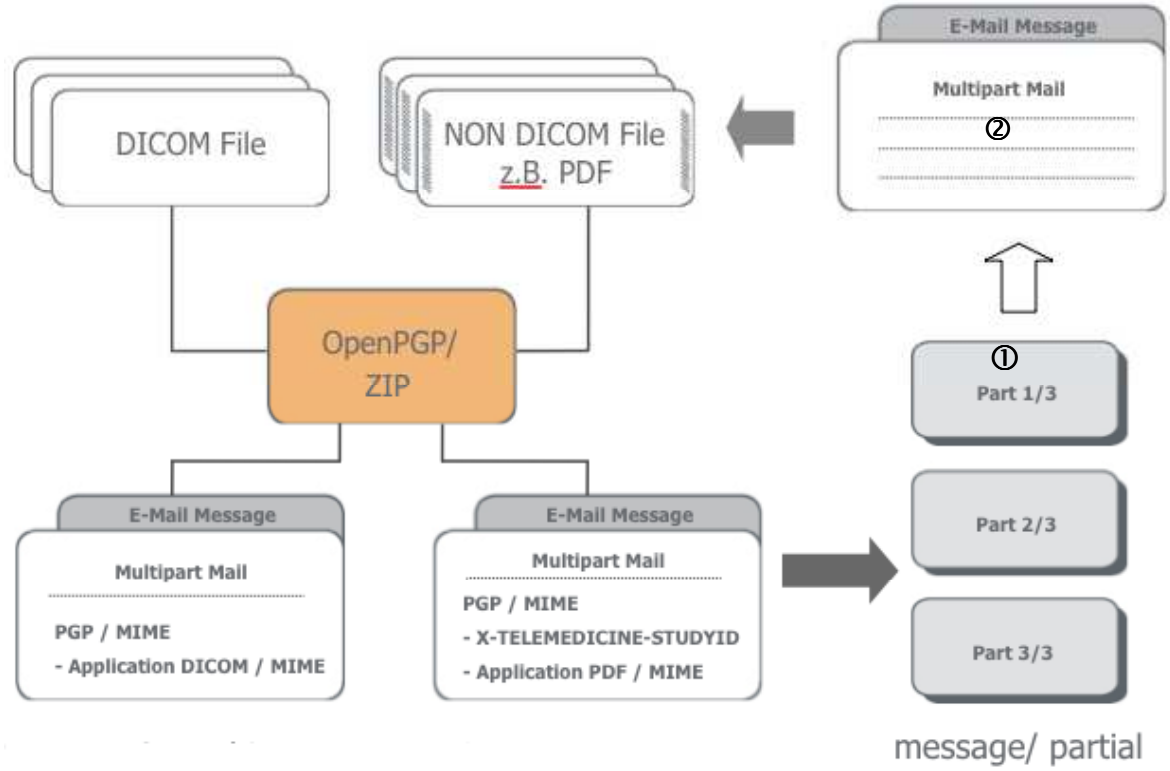

Abb. 4 – Synopsis des Datentransfers

14.4 Mechanismus zur Überprüfung des vollständigen Empfangs auf der Seite des Empfängers (optional)

Verwendete X-Tags: X-TELEMEDICINE-SETID, X-TELEMEDICINE-SETPART, X-TELEMEDICINE-SETTOTAL

Es werden vom Absender zusätzliche X-Tags den Datenpaketen hinzugefügt, die auf Seiten des Empfängers ausgewertet werden können. Hierdurch kann ein Empfänger sicherstellen, dass er tatsächlich alle vom Absender gesendeten Datenpakete empfangen hat. Die Definition dieser X-Tags lehnt sich an den

Mechanismus des „message/partial“ an (RFC 2046, Kapitel 5.2.2 - *Partial Subtype*).

X-TELEMEDICINE-SETID = Eindeutige ID zur Kennzeichnung eines zusammengehörigen Serie von E-Mails.

X-TELEMEDICINE-SETPART = Nummer der E-Mail innerhalb des zusammengehörigen Serie.

X-TELEMEDICINE-SETTOTAL = Gesamtanzahl der E-Mails des zusammengehörigen Serie.

Diese drei X-Tags repräsentieren keinen medizinischen Zusammenhang der Daten. Sie dienen ausschließlich der Kennzeichnung einer Serie von E-Mails, die vom Sender zusammenhängend verschickt wurden. Hiermit kann der Empfänger überprüfen, ob er diese Serie von E-Mails vollständig erhalten hat. Für die Verwendung ist zu beachten, dass die X-Tags optional einzusetzen sind. Werden sie verwendet, so gilt müssen folgende Regeln beachtet werden:

1. Die X-Tags können sowohl außerhalb des PGP/MIME Containers als auch innerhalb eingesetzt (Abb. 5 – Kennzeichnung zusammengehöriger E-Mails).
2. *X-TELEMEDICINE-SETID* und *X-TELEMEDICINE-SETPART* müssen in jeder E-Mail verwendet werden.
3. *X-TELEMEDICINE-SETTOTAL* muss in der letzten E-Mail des Sets vorhanden sein und ist in allen übrigen E-Mails optional.
4. Grundsätzlich sollten die Werte der verschlüsselt übermittelten X-Tags verwendet werden. Differieren diese mit den Werten der unverschlüsselt übermittelten X-Tags, sollte eine Warnmeldung ausgegeben werden.

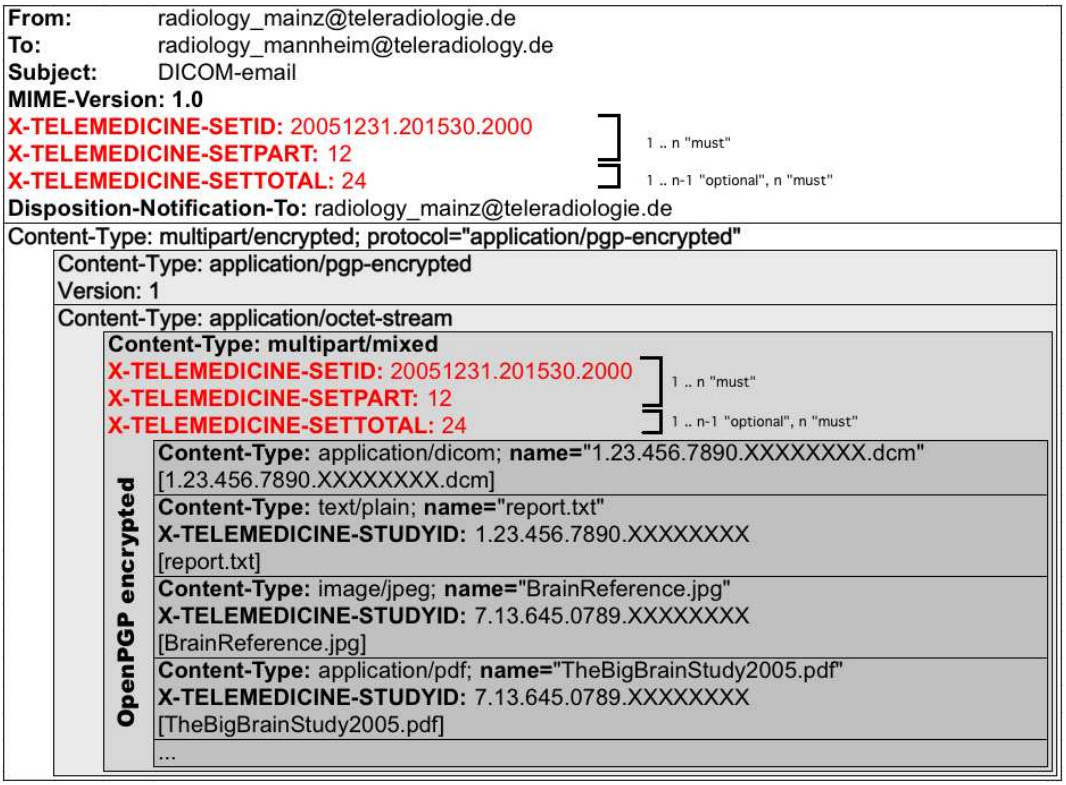

Abb. 5 – Kennzeichnung zusammengehöriger E-Mails

14.5 Mechanismen zur Überprüfung des vollständigen Datenempfangs auf der Seite des Absenders

Die Standardempfehlung umfasst zwei Mechanismen. Der Mechanismus 1 stellt hierbei die Minimalvariante dar und sollte von MIME-Standard konformen E-Mail Programmen verwendet werden können. Der Mechanismus 2 kann ergänzend verwendet werden.

14.5.1 Mechanismus 1 - MIME-Bestätigung (verpflichtend)

Verwendete Tags: DISPOSITION-NOTIFICATION-TO

Zur Überprüfung des korrekten Empfangs von E-Mails gibt der MIME-Standard gemäß des RFC 3798 die Möglichkeit der Anforderung von Benachrichtigungs-E-Mails.
Die Anforderung (*DISPOSITION-NOTIFICATION-TO: Benachrichtigungsadresse*) wird dem Mail-Header hinzugefügt. Damit wird auf der Empfängerseite der RFC-konforme Mechanismus zum Versand einer Empfangsbestätigung ausgelöst.

Die nachfolgende Abb. 6 zeigt eine Beispiel E-Mail.

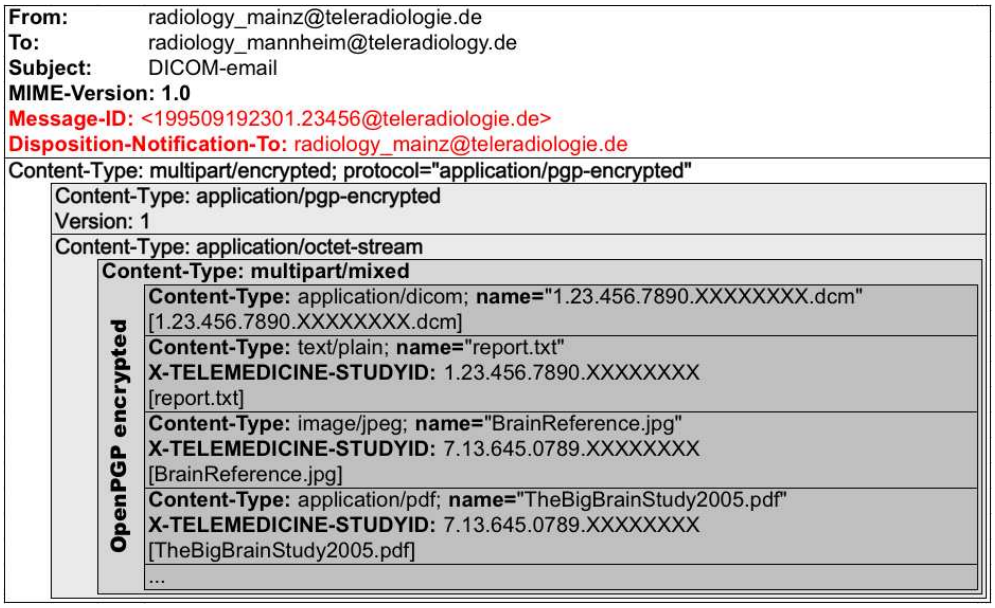

Abb. 6 – RFC konforme Anforderung einer Empfangsbestätigung

Die Verwendung einer RFC konformen Benachrichtigung ergibt, dass

1. sich die Rückmeldung immer auf die gesamte Mail bezieht und nicht auf den eigentlichen Inhalt.
2. die übermittelten Daten unverschlüsselt und unsigniert übertragen werden. Dies kann wiederum ein mögliches Angriffsziel für Manipulationen sein.

14.5.2 Mechanismus 2 - X-TELEMEDICINE-Bestätigung (optional)

Verwendete X-Tags: X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO, X-TELEMEDICINE-DISPOSITION-NOTIFCATION-KEYID

Um die angesprochenen Schwächen von Mechanismus 1 auszugleichen, erlaubt der Mechanismus 2, dass für jeden Teil des verschlüsselten PGP/MIME Containers jeweils getrennt die Anforderung einer Empfangsbestätigung erfolgen kann. Hierfür wurden die X-Tags *X-TELEMEDICINE-DISPOSITION-NOTIFCATION-TO* und *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-KEYID* eingeführt. *X-TELEMEDICINE-DISPOSITION-NOTIFCATION-TO* enthält die Benachrichtigungsadresse analog zur *DISPOSITION-NOTIFCATION-TO* Adresse aus Mechanismus 1. *X-TELEMEDICINE-DISPOSITION-NOTIFCATION-KEYID* enthält die ID des PGP/ GnuPG Schlüssels, mit dem die resultierende Antwort-E-Mail verschlüsselt werden soll. Die Verwendung dieses Tags ist optional. Sowohl die Benachrichtigungsadressen als auch die Schlüssel IDs können für alle Teile unterschiedlich sein. Bei Einsatz dieser Tags ist die Verwendung einer Content-ID gemäß RFC 2392 verpflichtend. Aufgrund der

geforderten globalen Eindeutigkeit der IDs kann hiermit eine eindeutige Zuordnung zu der verschickten Mail und zu jedem einzelnen Teil der Mail hergestellt werden. Da sich die Rücksendeadresse aus beiden Tags ergeben kann, wurde festgelegt, dass bei Angabe von beiden Tags grundsätzlich der Wert in *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO* als Rücksendeadresse verwendet werden sollte.

Die unter *DISPOSITION-NOTIFCATION-TO* angegebene Adresse muss nicht mit den Werten der *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO* Adresse übereinstimmen. Beide müssen aber gültige Rücksendeadressen enthalten. Bei Verwendung von Mechanismus 2 sollten primär die Rücksendeadressen aus dem verschlüsselten Teil (*X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO*, *X-TELEMEDICINE-DISPOSITION-NOTIFCATION-KEYID*) verwendet werden. Es ist als Fallbackvariante aber auch möglich an die DISPOSITION-NOTIFCATION-TO Adresse des unverschlüsselten Teil zu antworten.

Bei Verwendung von Mechanismus 2 ist die Verwendung des Mechanismus 1 verpflichtend. Dies stellt sicher, dass die Option einer Statusrückmeldung erhalten bleibt, selbst wenn der PGP/MIME Container nicht zu öffnen ist. Abb. 7 zeigt die Verwendung von beiden X-Tags. In Abb. 8 wird die alleinige Verwendung von *X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO* gezeigt.

Abb. 7 – Inhaltsbezogene Bestätigungsanforderung unter Verwendung der X-Tags für Schlüssel ID und Rücksendeadresse

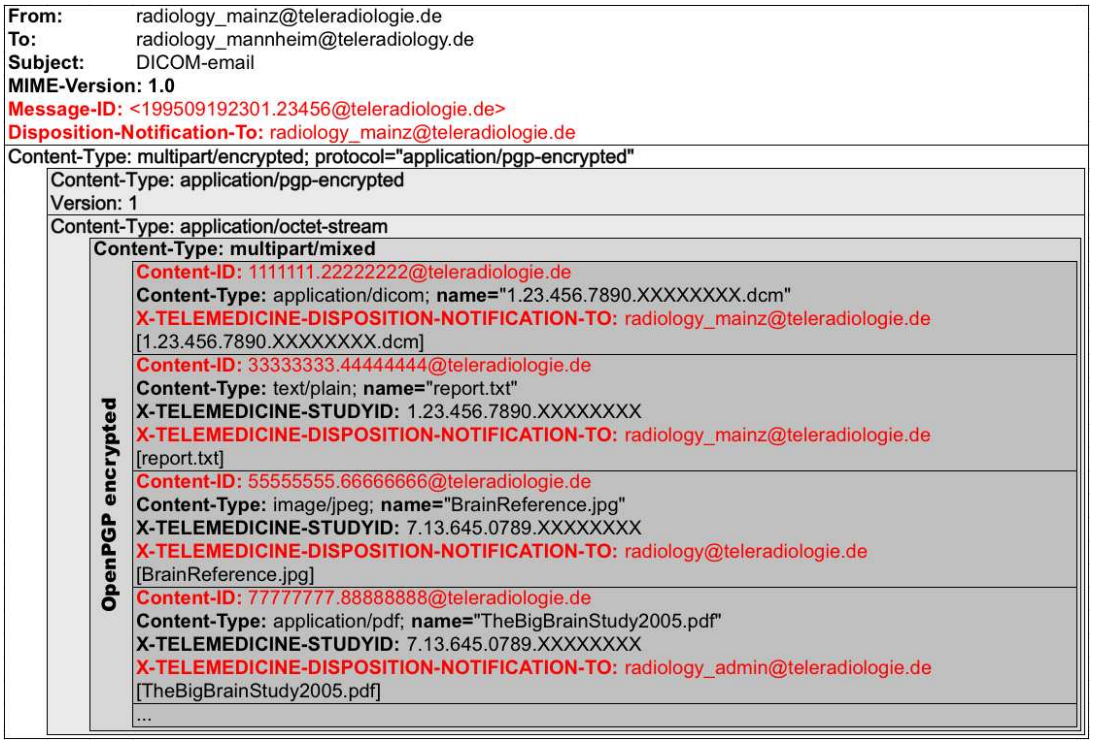

Abb. 8 – Inhaltsbezogene Bestätigungsanforderung unter Verwendung des X-Tags der Rücksendeadresse

14.6 Empfangsbestätigung (optional)

Für die Antwort-E-Mail der beiden unterschiedlichen Anforderungsarten ist folgendes zu beachten: Grundsätzlich ist es dem Empfänger freigestellt, ob er eine Antwort-E-Mail verschickt. Bei der Verwendung von Mechanismus 1 kann genau eine Bestätigung gesendet werden. Dabei wird eine Bestätigungs-E-Mail, welche aus der nicht verschlüsselten Aufforderung (

Mechanismus 1) resultiert, ebenso unverschlüsselt versendet. Die aus dem verschlüsselten Teil resultierenden Bestätigungs-E-Mails werden entweder verschlüsselt oder unverschlüsselt verschickt. Dies richtet sich nach den verwendeten X-Tags im verschlüsselten Teil der Anforderungs-E-Mail. Wird das Tag *X-TELEMEDICINE-DISPOSITION-KEYID* angegeben, so erfolgt die Rücksendung verschlüsselt. Fehlt die Schlüssel ID wird die Antwort-E-Mail unverschlüsselt verschickt, da so nicht sicher gewährleistet werden kann, dass der korrekte Schlüssel für den Versand verwendet wird.

Die verschlüsselten Bestätigungs-E-Mails müssen die Content-ID enthalten. Da es das Feld Original-Content-ID nicht gibt, wurde hierfür das Feld *X-TELEMEDICINE-ORIGINAL-CONTENT-ID* eingeführt. Die nachfolgenden Abbildungen zeigen das Beispiel einer nicht verschlüsselten Bestätigungs-E-Mail (Abb. 9) und einer verschlüsselten, (nicht RFC 3798 konformen) Bestätigungs-E-Mail (Abb. 10). Die Abbildungen zeigen das Grundgerüst. Die Inhalte der Mails werden durch die Statuscodes ausgedrückt. (siehe Kapitel 14.9 - *Statusmeldungen*).

14.7 Empfangsbestätigung - Mechanismus 1

Verwendete Tags: DISPOSITION-NOTIFICATION-TO, ORIGINAL-MESSAGE-ID

Die Bestätigungs-E-Mail baut sich gemäß des RFC 3798 auf. Eine solche E-Mail gliedert sich in zwei Abschnitte: Header und „multipart/report“-Body. Der Body ist wiederum in drei Abschnitte unterteilt:

- Teil 1 – menschenlesbar
- Teil 2 – maschinenlesbar
- Teil 3 – Referenz auf die zugrunde liegende E-Mail.

Der Teil 3 ist optional. Die Antwort-E-Mail auf eine Anfrage (*DISPOSITION-NOTIFICATION-TO*) erfolgt analog zu diesem Schema. In Abb. 9 wird eine Beispielantwort auf die Anfrage aus Abb. 6 gezeigt. In diesem Fall gibt es die

Rückmeldung, dass die empfangene E-Mail einen Fehler in der Syntax aufweist, der zu keinem verarbeitungsrelevanten Fehler geführt hat (Warning).

Die Anforderung aus Abb. 8 ergibt eine unverschlüsselte Antwort-E-Mail wie unter dem Mechanismus 1 in Abb. 9 gezeigt wird.

```
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

 An dieser Stelle ist Freitext möglich

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

Reporting-UA: post.teleradiology.de; Mailprogramm 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--
```

Abb. 9 – Empfangsbestätigung nach RFC 3798

14.8 Empfangsbestätigung - Mechanismus 2

Verwendete X-Tags: X-TELEMEDICINE-DISPOSITION-NOTIFICATION, X-TELEMEDICINE-ORIGINAL-CONTENT-ID

Die Antwort auf die Rückmeldungsanforderung (Abb. 7) aus dem verschlüsselten PGP/MIME Container ergibt wiederum eine verschlüsselte Bestätigungs-E-Mail. Diese ist folgendermaßen aufgebaut:

Der äußere Mailcontainer ist wie eine verschlüsselte E-Mail aufgebaut. In dem verschlüsselten Teil befindet sich ein MIME-Part mit dem Content-Type „multipart/report“. Der Report-Type ist „message/x-telemedicine-disposition-notification“, dieser entspricht dem Content-Type des zweiten Teils des Reports.

Dieser Content-Type ist analog zu „message/disposition-notification“ definiert, enthält statt der Original-Message-ID das Feld X-TELEMEDICINE-ORIGINAL-CONTENT-ID.

Die Abb. 10 zeigt ein Anwendungsbeispiel als Antwort auf die Anfrage aus Abb. 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
%
% An dieser Stelle ist Freitext möglich
%
%--RAA14128.773615765/teleradiology.de
%content-type: message/X-TELEMEDICINE-DISPOSITION-NOTIFICATION
%
%Reporting-UA: post.teleradiology.de; Mailprogramm 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--
```

* Die mit % eingeleiteten Zeilen sind OpenPGP kompatibel verschlüsselt.

Abb. 10 – Bestätigungs-E-Mail als Antwort auf eine Anfrage aus dem PGP/MIME Container

14.9 Statusmeldungen

Statusrückmeldungen werden gemäß des RFC 3798 übergeben. Zur Verwendung kommen die Benachrichtigungstypen „Displayed“ und „Deleted“. Als Konvention

wurde vereinbart, dass „Keine Fehler“ und „Warnungen“ unter „Displayed“ zusammengefasst werden. Damit wird festgelegt, das „Deleted“ mit einem Fehler einhergeht, der entweder einen erneuten Datentransfer nach sich zieht oder so schwerwiegend ist, dass ein erneuter Datentransfer keinen Sinn macht.

Zugelassene Kombinationen von Statusmeldungen und Benachrichtigungstypen sind:

1. Kein Fehler festgestellt
   disposition-field=Disposition:*automatic-action/MDN-sent-automatically*;**displayed**
   –[**kein warning, error- oder failure-field zulässig**]

2. Kein verarbeitungsrelevanter Fehler festgestellt
   disposition-field=Disposition:*automatic-action/MDN-sent-automatically*;**displayed/warning**
   warning-field = "Warning" ":" *text –[**mindestens ein warning-field verpflichtend**]
   –[**kein error- oder failure-field zulässig**]

3. Verarbeitungsrelevante Fehler festgestellt, Mail erneut senden
   disposition-field=Disposition:*automatic-action/MDN-sent-automatically*;**deleted/error**
   error-field = "Error" ":" *text –[**mindestens ein error-field verpflichtend**]
   warning-field = "Warning" ":" *text –[**warning-field optional**]
   –[**kein failure-field zulässig**]

4. Verarbeitungsrelevante Fehler festgestellt, Mail nicht erneut senden
   disposition-field=Disposition:*automatic-action/MDN-sent-automatically*;**deleted**
   failure-field = "Failure" ":" *text –[**mindestens ein failure-field verpflichtend**]
   error-field = "Error" ":" *text –[**error-field optional**]
   warning-field = "Warning" ":" *text –[**warning-field optional**]

Die als *text in den Beispielen aufgeführten Platzhalter enthalten nur den eindeutigen Statuscode wie im Anhang definiert. (siehe Kapitel 19 - *Anhang Übersicht aller X-TELEMEDICINCE Tags*)

Die Zuordnung eines Statuscodes zu einer der Kategorien „Warning“, „Error“ oder „Failure“ bleibt dem Absender der Benachrichtigung überlassen.

15. Service Part E-Mails

Ziel der Service Part E-Mails ist es die bisherige @GIT Teleradiologie Standardempfehlung (Versionen 1.1 und 1.5), um die Möglichkeit Arbeitsabläufe herstellerübergreifend durchführen zu können, zu erweitern. Die Kommunikation soll weiterhin über die bisher verwendeten Standards (siehe Kapitel 18.- *Mitgeltende Unterlagen*) abgebildet werden.

Folgende Szenarien werden durch die Service Part E-Mails unterstützt:

1. Die herstellerübergreifende Kommunikation der nach DIN 6868-159 notwendigen Daten zur Übertragungszeitkonstanz- und Funktionsprüfung.
2. Der Austausch und das Management von PGP/ GnuPG-Schlüsseldaten.
3. Der Austausch und das Management von Adressdaten.

15.1 Grundbedingung für alle Service Part E-Mails:

1. Alle Service Part E-Mails müssen verschlüsselt und signiert werden. Dies erfolgt RFC konform (RFC 3156 und RFC 1847) nach dem durch die @GIT Teleradiologie Standardempfehlung ab Version 1.5 beschrieben Mechanismus (siehe Kapitel 13 - *Digitale Signatur (PGP/MIME)* und Kapitel 14 - Transferformat).
2. Die Antworten auf die Service Part E-Mails sollen durch den Benachrichtigungs-Mechanismus 1 (siehe hierzu Standardempfehlung ab Version 1.5) abgebildet werden. Hierfür wurden die bisher bestehenden Errorcodes (siehe Kapitel 20 - *Anhang Errorcodes*) entsprechend erweitert.

Empfehlung: Zur Vorbeugung von Missbrauch sollte der Empfänger eine Whitelist (z.B. basieren auf Schlüssel IDs) für die Abarbeitung der Service Part E-Mails führen.

15.2 Aufbau von Service Part E-Mails

Alle Service Part E-Mails enthalten das X-Tag *X-TELEMEDICINE-SERVICEPART*, welches die auszuführende Aktion näher beschreibt. Hierdurch wird erreicht, dass E-Mails schon aussortiert werden können, ohne den Inhalt des XML-Dokuments zu verarbeiten. (Bsp: *X-TELEMEDICINE-SERVICEPART: ADDRESSUPDATE*)

Weiterhin enthält jede Service Part E-Mail genau ein XML-Dokument mit folgendem Aufbau:

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

Abb. 11 - XML Struktur Service Part E-Mail

Das Attribut *Name* definiert den Service Part, und das optionale Attribut *Action* enthält weitere Anweisungen. (Bsp: Name=“addressupdate“ Action=“remove“)

15.3 Szenario Konstanzprüfungen nach DIN 6868-159

Für die Umsetzung dieses Szenarios gibt es zwei Service Part E-Mails die verpflichtend zu implementieren sind:

1. Die Auslöse-E-Mail
2. Die Protokoll-E-Mail

Für die Verwendung beider Service Part E-Mails gilt zusätzlich zu den Grundbedingungen:

1. Die für die Konstanzprüfungen notwendigen Prüfbilder werden aus einem, durch die Kommunikationspartner zu definierenden Datenpool entnommen.
2. Es können jede Art von Daten verwendet werden.
3. Die Prüfstrecken beziehen sich immer auf den Weg zwischen zwei DICOM E-Mail Knoten.
4. Als PGP/ GnuPG Schlüssel ID ist die KeyID (8 stellige Hexadezimalnotation) des Hauptschlüssels zu verwenden.

Erst im Zusammenspiel des Service Part Auslöse-E-Mail Mechanismus mit dem Mechanismus der Service Part Protokoll-E-Mail können die herstellerübergreifenden Konstanzprüfungen, wie durch die DIN 6868-159 beschrieben, sinnvoll umgesetzt werden. Einen typischen Ablauf beschreibt das nachfolgende Flussdiagramm. Es zeigt einen möglichen Ablauf der Leitungsgeschwindigkeitsprüfung zwischen den Kommunikationspartnern B und C. Die Prüfung wird durch den Administrator A initiiert. Das bedeutet, der Versand der Prüfbilddaten erfolgt zwischen B und C. Das Kommunikationsprotokoll soll anschließend durch den Kommunikationspartner B an Administrator A übermittelt werden.

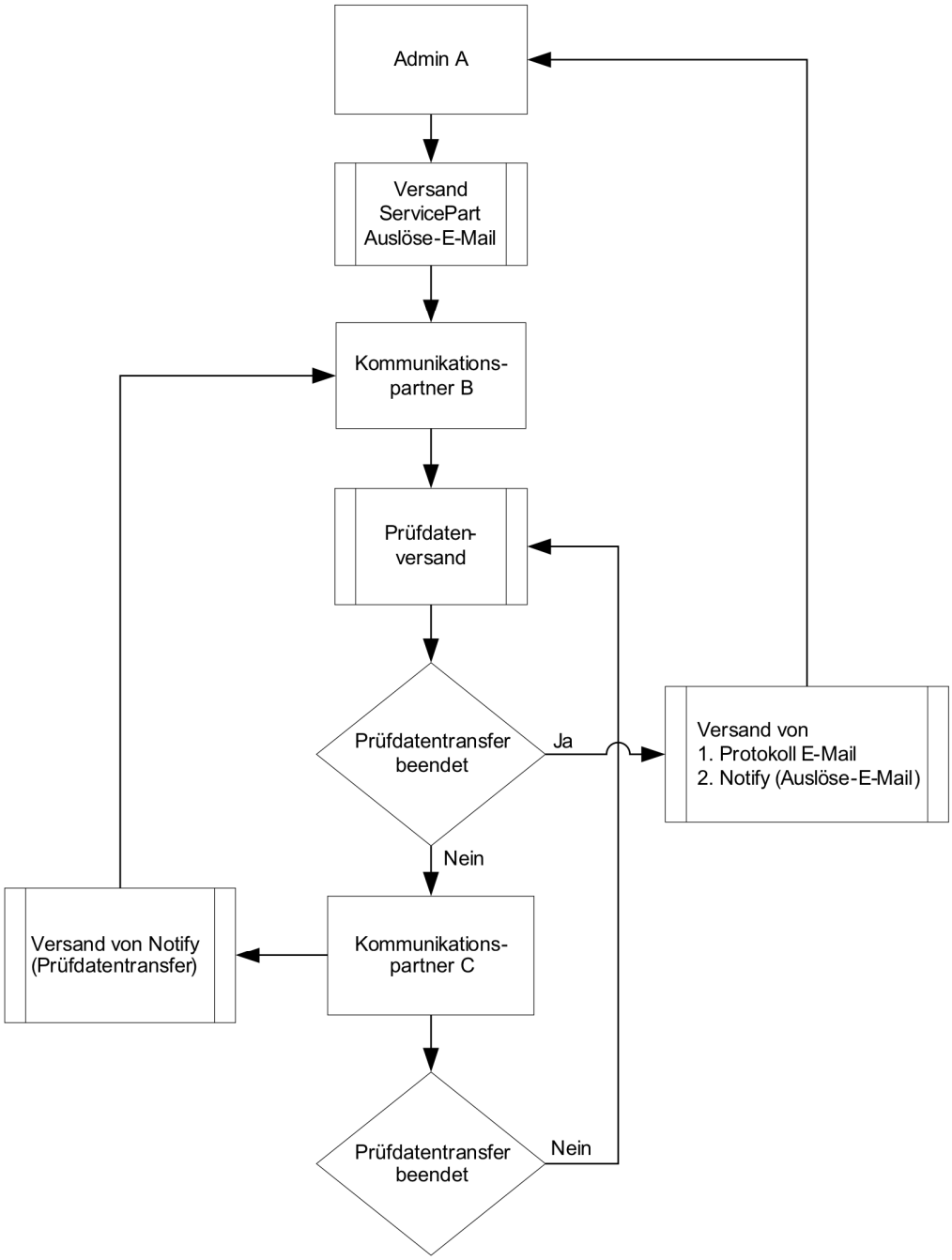

Abb. 12 – Ablaufbeispiel Konstanzprüfung durch Service Part Auslöse-E-Mail

15.4 Service Part Auslöse-E-Mails

Verwendete X-Tags: X-TELEMEDICINE-SERVICEPART:TESTTRANSFER, DISPOSITION-NOTIFICATION-TO

Durch die Auslöse-E-Mails können zwei Vorgänge ausgelöst werden:

1. Es wird ein nachgeschalteter Vorgang gestartet, der die Versendung des in der Auslöse-E-Mail benannten Prüfdatensatzes zur Folge hat.
2. Es kann die Rücksendung einer Bestätigungs-E-Mail ausgelöst werden.

Eine Auslöse-E-Mail weist folgende zusätzlichen Charakteristika auf:

1. Einfügen der Tags *X-TELEMEDICINE-SERVICEPART:TESTTRANSFER* und *DISPOSITION-NOTIFICATION-TO* im Mail-Header.
2. Anhängen einer XML Datei (text/xml) im Mailbody, nach der folgenden XML-Struktur.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="TESTTRANSFER" Action="QOSCHECK">
 <TestDataReceiver>
  <EmailAddress />  <- E-Mail Adresse des Datenempfängers
  <GPGKeyID />  <- (optional)
 </TestDataReceiver>
 <ProtocolReceiver> <- (optional)
  <EmailAddress />  <- Empfänger E-Mail Adresse der Protokoll-E-Mail
  <GPGKeyID />  <- (optional)
 </ProtocolReceiver>
 <TestDataSetID /> <-  [z.B. TESTDATASET_1 (siehe Anhang Prüfdatensatz IDs)]
 <ErrorTimeOut /> <- (optional) Zeitspanne in Sekunden ab wann spätestens das Protokoll verschickt
                     werden soll.
</ServicePart>
```

Abb. 13 – XML Struktur Service Part Auslöse-E-Mail

Der Wert des Attributs *Action* legt fest, welche Aktionen durch eine Auslöse-E-Mail initiiert werden. Das Attribut kann folgenden Wert annehmen:

1. QOSCHECK – hierdurch wird eine Leitungskonstanzprüfung nach DIN 6868-159 ausgelöst.

Der Knoten *TestDataSetID* beschreibt, welcher festgelegte Datensatz übertragen werden soll und darf nur einmal vorkommen. *TestDataSetID* kann folgende Werte annehmen:

1. Die im Anhang *Prüfbilddatensatz IDs* vorgegebenen Werte
2. Ein frei wählbare, maximal 64 Zeichen lange alphanumerische ID eines beliebigen, zu definierenden Prüfbilddatensatzes.

Auf eine Auslöse-E-Mail kann es zwei Antworten durch den E-Mail Empfänger geben:

1. Den Versand einer Bestätigungs-E-Mail (Mechanismus 1) an den Versender der Auslöse-E-Mail nach Beendigung des Prüfdatenversands.
2. Den Versand einer Protokoll-E-Mail an den in der Auslöse-E-Mail spezifizierten Empfänger. Diese Mail beinhaltet eine XML Protokolldatei als Anhang.

Nachfolgend wird ein Beispiel für ein Auslöse-E-Mail aufgeführt.

```
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;
%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--
```

* Die mit % eingeleiteten Zeilen sind OpenPGP kompatibel verschlüsselt.

Abb. 14 – Beispiel Service Part Auslöse-E-Mail

Durch diese Beispiel-E-Mail sollten folgende Aktionen ausgelöst werden:

1. Die Empfängerseite verschickt den festgelegten Funktionsprüfungs-datensatz (TESTDATASET_1) an die E-Mail Adresse DrMeyer@homeoffice.de. Zur Verschlüsselung wird der Schlüssel mit der KeyID AA76CA08 verwendet.
2. Der Versand der Protokoll XML Datei (siehe unten) erfolgt an die E-Mail Adresse admin@teleradiologie.de. Zur Verschlüsselung wird der Schlüssel mit der KeyID D4762A08 verwendet.
3. Der Versand der Bestätigungs-E-Mail erfolgt gemäß Mechanismus 1 (Seite 22) mit der Nachricht über den Erfolg bzw. Misserfolg des Testtransfers an die Adresse radiology_mannheim@teleradiology.de.

15.5 Service Part Protokoll-E-Mails

Verwendete X-Tags: X-TELEMEDICINE-SERVICEPART:PROTOCOL

Die Implementierung der Service Part Protokoll-E-Mails ist verpflichtend und wird durch die zuvor beschriebene Auslöse-E-Mail angefordert. Die Protokoll-E-Mail weist folgende zusätzliche Charakteristika auf:

1. Der Mail-Header wird um das X-Tag *X-TELEMEDICINE-SERVICEPART:PROTOCOL* erweitert.
2. Es darf immer nur genau eine Protokolldatei pro Service Part Protokoll-E-Mail verschickt werden.

Die Protokoll-E-Mail wird nach der Übermittlung der Prüfdaten automatisch versand.

Der schematische Aufbau einer solchen E-Mail ist der nachfolgenden Abb. 15 zu entnehmen.

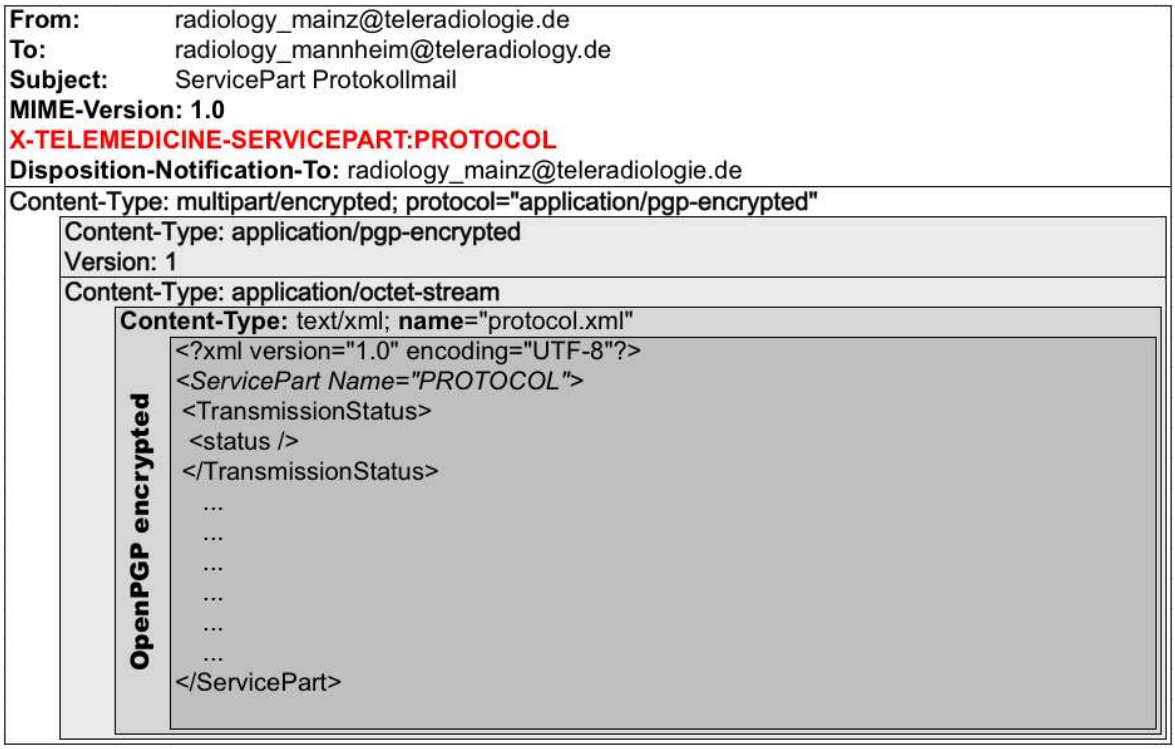

Abb. 15 – Schema Service Part Protokoll-E-Mail

Die XML Struktur der Protokolldatei wird in der nachfolgenden Abb. 16 dargestellt.

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

  <TransmissionStatus />   <- Es sind die Zustände COMPLETED, ABORTED möglich
  <TestDataSetID />   <- ID des verschickten Testdatensatzes

  <ObjectsSent>
    <Count />    <- Anzahl der versendeten Objekte
  </ObjectsSent>

  <ObjectsReceivedConfirmed> <- Zusammenfassung aller DatagramMail Knoten
   <Count />   <- Anzahl der versendeten und bestätigten Objekte
   <Time />   <- Gesamtübertragungszeit vom Versand des ersten Datenpackets bis zum Empfang der
                 letzten Bestätigungsmail für alle bestätigten Objekte, in Sekunden
   <MailSize />   <- Gesamtgröße aller bestätigten E-Mails, in Byte
   <ObjectSize /> <- Gesamtgröße aller bestätigten Objekte, in Byte
  </ObjectsReceivedConfirmed>

  <DataSender>
    <EMailAddress />   <- E-Mail Adresse des Prüfdaten Versenders
  </DataSender>

  <DataRecipient>
    <EMailAddress />   <- E-Mail Adresse des Prüfdaten Empfängers
  </DataRecipient>

  <ProtocolRecipient>
   <EMailAddress />   <- E-Mail Adresse des Protokoll Empfängers
  </ProtocolRecipient>

  <ErrorTimeOut />   <- Zeitspanne, in Sekunden, ab wann bei einer Empfangsstörung
                        von einem Fehler ausgegangen wird

  <DatagramMail EMailMessageID="">   <- Dieser Block kann beliebig häufig wiederholt werden
   <ErrorID />   <- Im Fehlerfall: Hier steht der Errorcode gemäß der Errorcode Liste ansonsten opt.
   <EMailContentID />   <- opt. ContentID bei Multipart Mails sofern vorhanden
   <StartDateTime />   <- Startdatum und -zeit der Datenübertragung (Format yyyymmddhhmmss)
   <NotifyDateTime />   <- Empfangsdatum und -zeit der Bestätigungs-E-Mail
                           (Format yyyymmddhhmmss)
   <MailSize />   <- Gesamtgröße der übertragenen E-Mails, in Byte
   <ObjectSize />   <- Gesamtgröße der übertragenen Objekte, in Byte
  </DatagramMail>

</ServicePart>
```

Abb. 16 – XML Struktur Service Part Protokoll

15.6 Szenario Schlüsseldatenaustausch

Verwendete X-Tags: X-TELEMEDICINE-SERVICEPART:KEYUPDATE, DISPOSITION-NOTIFICATION-TO

Zu den essentiellen administrativen Tätigkeiten in einem telemedizinischen Netzwerk gehört das Management der GPG-Schlüsseldaten. Durch die vorliegende Version der @GIT Standardempfehlung wird eine

herstellerübergreifende, automatisierte Durchführung ermöglicht. Die Umsetzung des Schlüsselmanagements ist verpflichtend.

Für das Schlüsselmanagement werden folgende Aktionen unterstützt:

1. Das Hinzufügen bzw. Aktualisieren von Schlüsseln.
2. Das Zurückziehen von Schlüsseln.

Der Header der Service Part E-Mail wird um das X-Tag *X-TELEMEDICINE-SERVICEPART:KEYUPDATE* erweitert. Die nachfolgende XML Struktur wird als Datei mit dem Content-Type „text/xml“ angehängt. Optional kann der Tag *DISPOSITION-NOTIFICATION-TO* zum Anfordern einer Bestätigungs-E-Mail eingefügt werden.

Auch hier gilt, dass pro Service Part E-Mail nur eine XML-Datei mit nur einer Verbindung übertragen werden darf.

15.6.1 Schlüssel Hinzufügen oder Aktualisieren

Hierfür muss das Attribut *Action* der nachfolgenden XML Struktur den Wert *„SET“* gesetzt bekommen.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="KEYUPDATE" Action="SET">
 <PublicKeyASCIIData />  <- öffentlicher, ASCII codierter GPG-Schlüsselteil
</ServicePart>
```

Abb. 17 – XML Struktur zum Hinzufügen eines Schlüssels

15.6.2 Schlüssel Zurückziehen

Hierfür muss das Attribut *Action* der nachfolgenden XML Struktur den Wert *„REMOVE“* gesetzt bekommen.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="KEYUPDATE" Action="REMOVE">
 <GPGKeyID />  <- GPG KeyID des ungültigen Schlüssels
</ServicePart>
```

Abb. 18 – XML Struktur zum zurückziehen eines vorhandenen Schlüssels

15.7 Szenario Adressdatenaustausch

Verwendete X-Tags: X-TELEMEDICINE-SERVICEPART:ADDRESSUPDATE, DISPOSITION-NOTIFICATION-TO

Der Austausch der Kommunikationsdaten ist eine weitere wichtige Aufgabe für das Management eines Telemedizinnetzwerks. Nachfolgend wird beschrieben, wie dies durch die @GIT Standardempfehlung unterstützt wird. Die Umsetzung des Adressdatenaustauschs ist verpflichtend.

Für das Adressdatenmanagement werden zwei Tätigkeiten unterstützt:

1. Das Hinzufügen bzw. Aktualisieren von Kommunikationsdaten.
2. Das Löschen von Kommunikationsdaten.

Der Header der Service Part E-Mail wird um das X-Tag *X-TELEMEDICINE-SERVICEPART:ADDRESSUPDATE* erweitert. Die nachfolgende XML Struktur wird als Datei mit dem Content-Type „text/xml“ angehängt. Optional kann der Tag *DISPOSITION-NOTIFICATION-TO* zum Anfordern einer Bestätigungs-E-Mail eingefügt werden.

Auch hier gilt, dass pro Service Part E-Mail nur eine XML-Datei mit nur einer Verbindung übertragen werden darf.

15.7.1 Adressdaten Hinzufügen und Ändern

Hierfür muss das Attribut *Action* der nachfolgenden XML Struktur den Wert *„SET“* gesetzt bekommen.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="ADDRESSUPDATE" Action="SET">
 <Connection>
  <ID />  <- (opt.) eindeutige Kennung eines Kommunikationswegs
  <DisplayConnectionName />  <- für den Benutzer sichtbarer Verbindungsname
  <Mailserver />  <- (opt.) Angabe des E-Mailversandservers
  <Port />  <- (opt.) Mailversandport
  <EmailAddress />  <- Empfänger E-Mail Adresse
  <GPGKeyID />  <- GPG KeyID des zu verwendenden Verschlüsselungsschlüssels
 </Connection>
</ServicePart>
```

Abb. 19 – XML Struktur Adressdatenaustausch

Hinweis: Ohne Verwendung des optionalen ID Tags ist eine spätere Änderung oder Entfernung der Kommunikationsdaten nicht möglich.

15.7.2 Adressdaten Löschen

Hierfür muss das Attribut *Action* der nachfolgenden XML Struktur den Wert „*REMOVE*“ gesetzt bekommen.

```
<?xml version="1.0" encoding="UTF-8"?>
<ServicePart Name="ADDRESSUPDATE" Action="REMOVE">
 <Connection>
  <ID />  <- Eindeutige Kennung eines Kommunikationswegs
 </Connection>
</ServicePart>
```

Abb. 20 – XML Struktur Adressdatenaustausch

16. Generierung von Identifikationsnummern

16.1 Hinweis

Es wird an dieser Stelle nochmals darauf hingewiesen, dass im Zusammenhang mit der Telemedizin Identitifikationsnummern (z.B. *X-TELEMEDICINE-STUDYID*, *X-TELEMEDICINE-SETID*) keinerlei Rückschlüsse auf die Patientenidentität erlauben dürfen.

16.2 DICOM UID

Die für die Erstellung gültiger DICOM UIDs notwendigen DICOM-Root-UIDs können kostenfrei oder kommerziell über das Internet bezogen werden. Entsprechende Adressen werden auf der Webseite der Initiative zur Standardisierung von Telemedizin *http://www.tele-x-standard.de/* vorgehalten.

17. Online Connect-a-thon Server

Für die Überprüfung von Implementierungen der hier vorliegenden Empfehlung wurde ein Server eingerichtet, auf dem Transferdaten von den verschiedenen, an den Offline Connect-a-thons teilnehmenden Herstellern bzw. von deren Produkten liegen. Der Zugriff erfolgt über das Internet. Eine Zugangsberechtigung sowie die Konfigurationsdaten sind via E-Mail bei *teleradiologie@rad.ma.uni-heidelberg.de* zu beziehen. Auf diese Weise können jederzeit Online Connect-a-thons durchgeführt werden.

Es wurde vereinbart, dass die Teilnehmer der Online Connect-a-thons bei Rückfragen durch andere Teilnehmer innerhalb von 2-3 Tagen antworten.

18. Mitgeltende Unterlagen

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 Deutsche Gesetze

- Verordnung über den Schutz vor Schäden durch Röntgenstrahlen („Röntgenverordnung“) - Neugefasst durch Bek. v. 30. 4.2003 I 604

- Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz, SigG) - Stand: Geändert durch Art. 1 G v. 4. 1.2005 I 2
- Verordnung zur elektronischen Signatur (Signaturverordnung) - Stand: Geändert durch Art. 2 G v. 4. 1.2005 I 2

19. Anhang Übersicht aller X-TELEMEDICINCE Tags

X-TELEMEDICINE-STUDYID

Zur Zuordnung von Nicht-DICOM Daten zu Studien

X-TELEMEDICINE-SETID

Zur Kennzeichnung eines zusammengehörigen E-Mail Sets

X-TELEMEDICINE-SETPART

Zur Kennzeichnung eines Teils eines E-Mail Sets

X-TELEMEDICINE-SETTOTAL

Zur Kennzeichnung des letzten Teils eines E-Mail Sets, bzw. die Gesamtzahl aller Teile

X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO

X-Telemedicine Benachrichtungsadresse

X-TELEMEDICINE-DISPOSITION-NOTIFCATION-KEYID

X-Telemedicine Benachrichtungsschlüssel

X-TELEMEDICINE-ORIGINAL-CONTENT-ID

Orignal-Content-ID für verschlüsselte Bestätigungs-E-Mails

X-TELEMEDICINE-SERVICEPART

X-Telemedicine Tag für Servicpart Operationen

20. Anhang Errorcodes

Code	Bedeutung
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-attachement-error
1.3.1	mail-attachement-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

Applikation

3	application-error
3.1	application-extern-error
3.2	application-intern-error
3.2.1	application-intern-attachement-error
3.2.1.1	application-intern-attachement-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

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

Jeder Fehlercode kann benutzerdefiniert / applikationsspezifisch mit „.0“ erweitert werden.

Bsp.: 2.1.0.2 (mgl. Bedeutung: no public key available, no GPG installed)

Vorschläge für weitere Codes sind über die Webseite der Initiative
http://tele-x-standard.de
einzureichen

21. Anhang Prüfdatensatz IDs

Bedingungen:

1. Die Prüfdatensatz ID kann aus max. 64 alphanumerischen Zeichen bestehen.
2. Es können beliebig viele Prüfbilddatensätze definiert werden.
3. Die vorgegebenen IDs sowie die Möglichkeit zur Definition beliebiger weiterer Prüfbilddatensätze sind verpflichtend zu implementieren.

Prüfdatensatz ID	**Beschreibung**
TESTDATASET_1	Funktionsprüfdatensatz (für die tgl. Funktionsprüfung gem. DIN 6868-159)
TESTDATASET_2	Größter Prüfbilddatensatz oder Äquivalent (für die mtl. Leitungskonstanzprüfung gem. DIN 6868-159)
TESTDATASET_CT_HEAD	Prüfbilddatensatz CT-Schädel
TESTDATASET_CT_NECK	Prüfbilddatensatz CT-Hals
TESTDATASET_CT_THORAX	Prüfbilddatensatz CT-Thorax
TESTDATASET_CT_ABDOMEN	Prüfbilddatensatz CT-Abdomen
TESTDATASET_CT_UPPER_EXTREMITY	Prüfbilddatensatz CT-Obere Extremitäten
TESTDATASET_CT_LOWER_EXTREMITY	Prüfbilddatensatz CT-Untere Extremitäten
TESTDATASET_CT_JOINTS	Prüfbilddatensatz CT-Gelenke
TESTDATASET_CT_HAND	Prüfbilddatensatz CT-Hand
TESTDATASET_CT_FOOT	Prüfbilddatensatz CT-Fuss
TESTDATASET_CT_FULLBODY_TRAUMA	Prüfbilddatensatz CT-Ganzkörper / Trauma
TESTDATASET_CT_ANGIO_ABDOMEN	Prüfbilddatensatz CTA-Abdomen
TESTDATASET_CT_ANGIO_EXTREMITIES	Prüfbilddatensatz CTA-Extremitäten
TESTDATASET_CR_THORAX	Prüfbilddatensatz konventionelle Röntgenaufnahmen Thorax
TESTDATASET_CR_ABDOMEN	Prüfbilddatensatz konventionelle Röntgenaufnahmen Abdomen
TESTDATASET_CR_EXTREMITIES	Prüfbilddatensatz konventionelle Röntgenaufnahmen Extremitäten