@GIT Initiative zur Standardisierung von Telemedizin

Empfehlung für ein standardisiertes Teleradiologie Übertragungsformat

Version 1.5
(Dezember 2005)

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

1. Inhaltsverzeichnis

2. Impressum

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

Titel : Empfehlung für ein standardisiertes Teleradiologie Übertragungsformat
Version : 1.5.01

Mitwirkende Arbeitsgruppenmitglieder in alphabetischer Reihenfolge:

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

Letzte Revision : 21.02.2006

3. Kontakt

Der Kontakt zu der Initiative kann jederzeit über nachfolgende eMail-Adresse hergestellt werden: *teleradiologie@drg.de*. Wir nehmen auf Wunsch auch gerne neue Interessenten in unseren Verteiler auf. Eine kurze formlose eMail 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 *URL* *http://www.tele-x-standard.de* der Öffentlichkeit zur Verfügung gestellt.

4. Copyright

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 1.5

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 hat (siehe Kapitel Mechanismus zur Überprüfung des vollständigen Empfangs auf der Seite des Empfängers).
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 (siehe Kapitel Mechanismen zur Überprüfung des vollständigen Datenempfangs auf der Absenderseite).
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 (siehe Kapitel Digitale Signatur (PGP / MIME)).

Autoren der Arbeitsgruppe

im Oktober 2005

7. Grundüberlegung

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

8. Mindestanforderungen an die Software

Transferdatentypen

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

MIME Standard

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

9. 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 Secure-Varianten der Mail-Protokolle (SMTP, POP3 bzw. IMAP4) unterstützt werden.

10. Verschlüsselung & Kompression

Die Verschlüsselung der Daten erfolgt OpenPGP kompatibel. Es dürfen nur die im PGP Standard enthaltenen „MUST“-Kriterien verwendet werden. 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/

11. 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 eMail-Verschlüsselung mit Signierung (combined method, RFC 3156, Kapitel 6.2)
- Daten mit einer abgetrennten Signatur, welche gemäß RFC 1847 PGP kompatibel verschlüsselt werden (encapsulation, RFC 3156, Kapitel 6.1).

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

Hinweis: GnuPG erstellt immer zuerst die Signatur und verschlüsselt diese anschließend mit den signierten Daten. Daraus ergibt sich, dass auch bei der „combined method“ die Daten zuerst entschlüsselt werden müssen und man erst dann die verborgene Signatur erhält. Um eventuellen „Mail-Bomben“ zu begegnen gibt es einen entsprechenden GnuPG-Schalter, der die maximale Outputgröße der entschlüsselten Datei beschränkt. Bei Überschreiten der voreingestellten Größe gibt GnuPG einen Fehler aus.

12. Transferformat

DICOM-Objekte

DICOM-Objekte werden in eine DICOM-eMail nach Suppl. 54 des DICOM-Standards überführt. Die neu entstandene DICOM-eMail wird OpenPGP kompatibel verschlüsselt und signiert (Abb. 1) [siehe Digitale Signatur (PGP / MIME)].

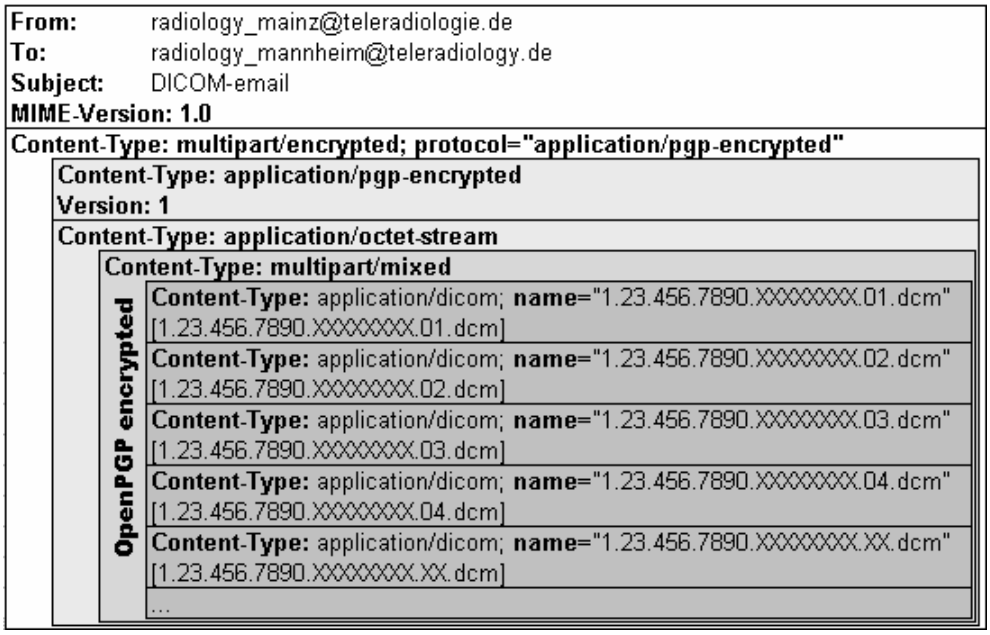

Abb. 1 – Transferformat für DICOM-Daten

Nicht-DICOM Daten

Nicht-DICOM Daten verfügen über keinen Header mit Patienteninformationen. Aus diesem Grund wurde, konform zum MIME Standard, ein X-Tag definiert. Dieses Tag lautet „X-TELEMEDICINE-STUDYID“. Diesem Tag wird die StudyInstanceUID [0020:000D] aus einem vorhanden DICOM-Header zugewiesen, damit die Zuordnung Daten <-> Studie erfolgen kann. Gibt es keine passende StudyInstanceUID muss eine neue erzeugt und den Daten zugeordnet werden (siehe Generierung von Identifikationsnummern (IDs)). Alle Nicht-DICOM Daten werden zusammen mit allen DICOM-Objekten OpenPGP kompatibel verschlüsselt und signiert (Abb. 2 – Transferformat für Nicht-DICOM-Daten). Es können damit auch Daten von unterschiedlichen Untersuchungen oder unterschiedlichen Patienten innerhalb einer einzigen eMail gemeinsam verschickt werden. Ebenso können zusammengehörige Daten in unterschiedlichen eMails 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** (Gebot der Eindeutigkeit).

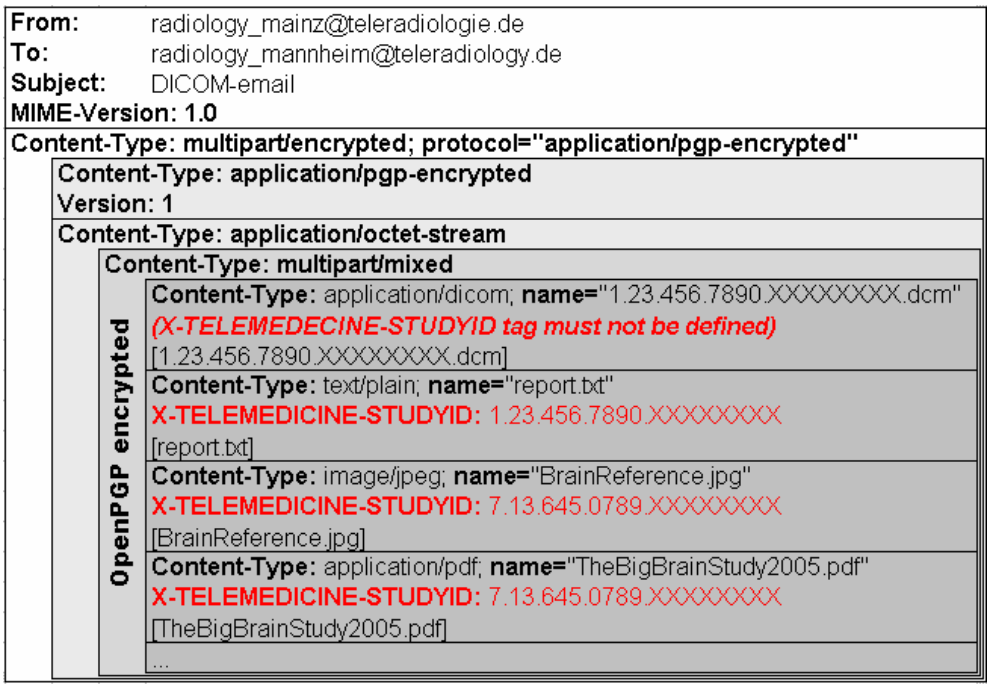

Abb. 2 – Transferformat für Nicht-DICOM-Daten

Message/Partial

In der Synopsis (Abb. 3 – Synopsis des Datentransfers) werden die Daten verschlüsselt als PGP/ MIME Multipart eMail verschickt. Im MIME Standard ist eine Auftrennung von größeren eMails in mehrere kleine eMails vorgesehen (message/ partial). Dies erfolgt entweder optional durch die Versandsoftware oder durch einen am Versand beteiligten eMail-Server (Abb. 3 ① message/ partial). Für den Empfangsprozess muss dies berücksichtigt werden, so dass dieser in der Lage ist, diese Anteile in die Ursprungsmail (Abb. 3 ②) zu überführen.

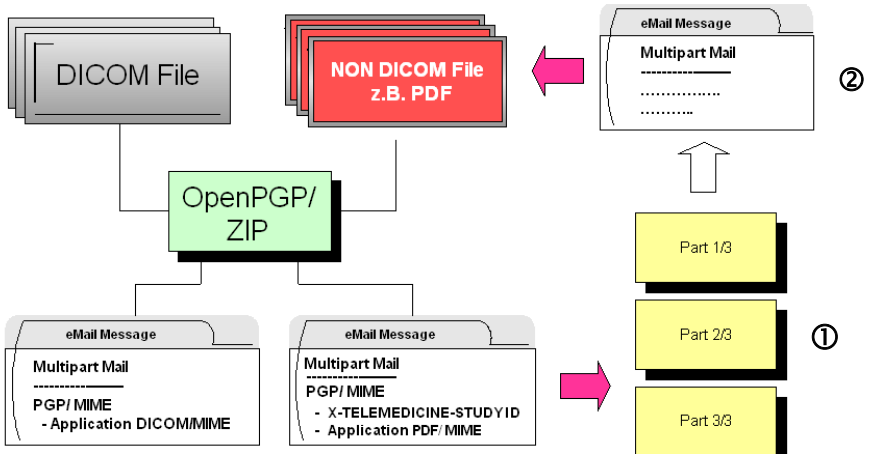

Abb. 3 – Synopsis des Datentransfers

Mechanismus zur Überprüfung des vollständigen Empfangs auf der Seite des Empfängers

Es werden vom Absender zusätzliche X-Tags 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 hat. Die Definition dieser X-Tags lehnt sich an den Mechanismus des MessagePartial an.

X-TELEMEDICINE-SETID = Eindeutige ID zur Kennzeichnung eines zusammengehörigen Satzes (Set) von eMails.

X-TELEMEDICINE-SETPART = Nummer der eMail innerhalb des zusammengehörigen Satzes.

X-TELEMEDICINE-SETTOTAL = Gesamtanzahl der eMails des zusammengehörigen Satzes.

Diese drei X-Tags repräsentieren keinen medizinischen Zusammenhang der Daten. Sie dienen ausschließlich der Kennzeichnung einer Serie von eMails, die vom Sender zusammenhängend verschickt wurden. Hiermit kann der Empfänger überprüfen, ob er diese Serie von eMails 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 werden sowohl außerhalb des PGP/MIME Containers als auch innerhalb eingesetzt [siehe Abb. 4]

2. X-TELEMEDICINE-SETID und X-TELEMEDICINE-SETPART müssen in jeder eMail verwendet werden. Nur die letzte eMail muss das X-Tag X-TELEMEDICINE-SETTOTAL enthalten.
3. Grundsätzlich sollten die Werte der verschlüsselt übermittelten X-Tags verwendet werden. Differieren diese mit den Werten der unverschlüsselt übermittelten X-Tags, sollte eine Warnmeldung an die Benutzer (z.B. Sender, Empfänger usw.) ausgegeben werden.

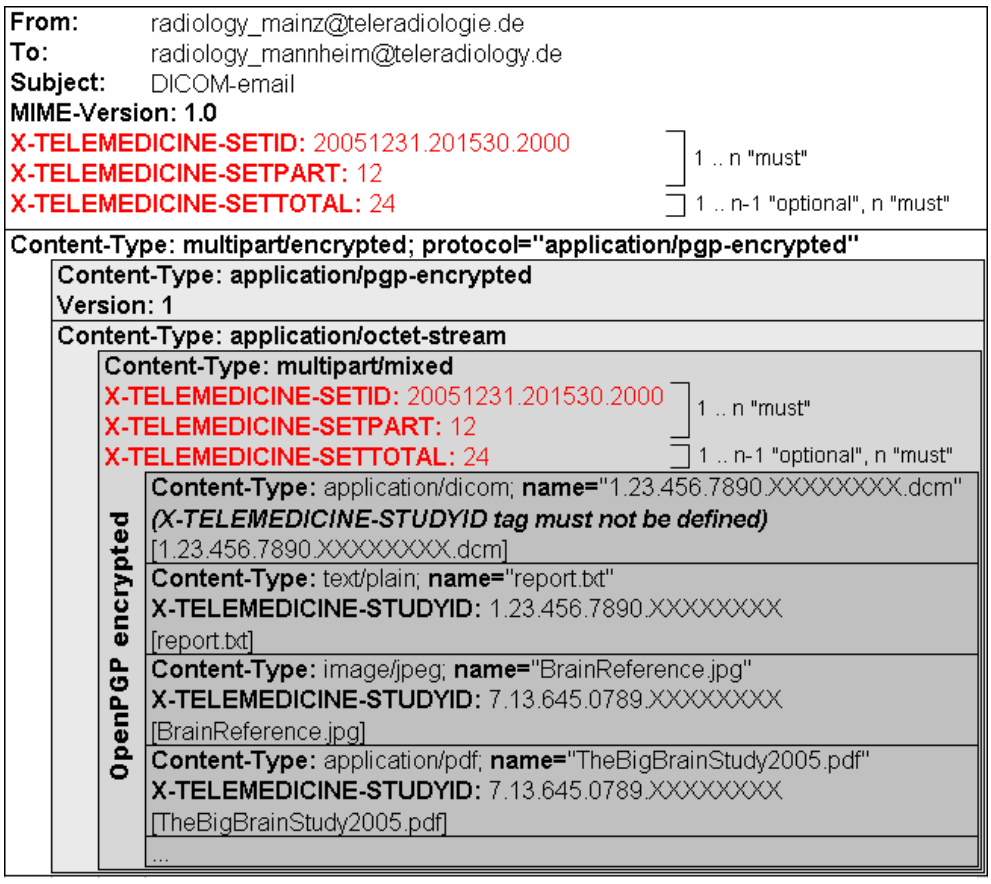

Abb. 4 – Kennzeichnung zusammengehöriger eMails

Mechanismen zur Überprüfung des vollständigen Datenempfangs auf der Absenderseite

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

Mechanismus 1

Zur Überprüfung des korrekten Versandes und Empfangs von eMails gibt der MIME-Standard gemäß des RFC 3798 die Möglichkeit der Anforderung sogenannter Disposition Notify Mails vor. Die Anforderung (*Disposition-Notification-To: Return_to_email_adresse*) wird im Mail-Header eingetragen. Damit wird auf der Empfängerseite der RFC-konforme Mechanismus zum Versand einer Empfangsbestätigung ausgelöst. Es sollte darauf geachtet werden, dass die Message-ID mit der Mail generiert wird und dies beispielsweise nicht dem Mailserver überlassen wird, da sonst für den Versender keine Möglichkeit besteht diese ID für den Abgleich mit den Notify eMails zu speichern. Die nachfolgende Abbildung 5 zeigt eine Beispiel-eMail.

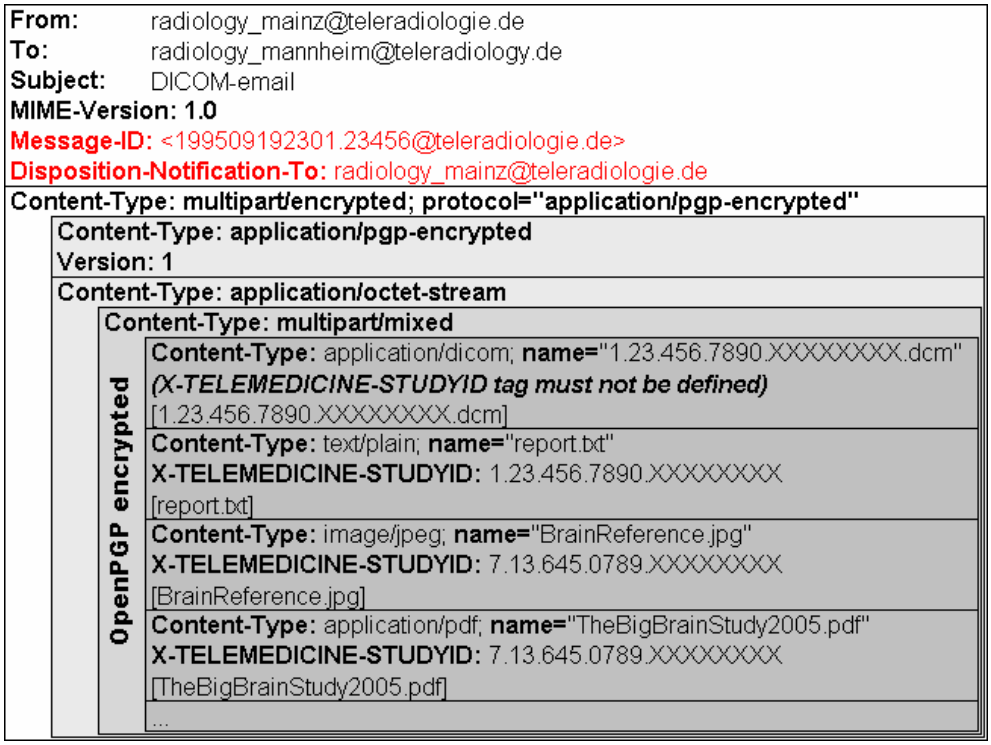

Abb. 5 – RFC konforme „Request for Notification“ eMail

Die Verwendung des RFC konformen Notify ergibt, dass sich

1. die Rückmeldungen immer auf die gesamte Mail beziehen und nicht auf den eigentlichen Inhalt und

2. werden die übermittelten Daten unverschlüsselt und unsigniert übertragen. Dies kann wiederum ein mögliches Angriffsziel für Manipulationen sein.

Mechanismus 2

Aus diesem Grund erlaubt der Mechanismus 2, dass für jeden Part des verschlüsselten PGP/MIME Containers jeweils getrennt die Anforderung einer Rückmeldung erfolgen kann. Hierfür wurden die X-Tags X-TELEMEDICINE-DISPOSITION-NOTIFCATION-KEYID und X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO eingeführt. Die beiden Tags können alternativ oder gemeinsam verwendet werden. X-TELEMEDICINE-DISPOSITION-NOTIFCATION-KEYID enthält die ID des PGP/ GnuPG Schlüssels, mit dem die resultierende Notify Mail verschlüsselt werden soll. X-TELEMEDICINE-DISPOSITION-NOTIFCATION-TO enthält die Return-eMail Adresse analog zu Disposition-Notification-To aus dem unverschlüsselten Teil. Sowohl die KeyID als auch die Return-eMail-Adressen können für alle Parts 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 1. zu der verschickten Mail und 2. zu jedem einzelnen verschickten Part einer 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.

Bei Verwendung des zweiten Mechanismus ist die Verwendung des Mechanismus 1 verpflichtend. Die unter Disposition-Notification-To angebene Adresse muss nicht mit den Werten von X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO 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 Adresse des unverschlüsselten Teil zu antworten (Disposition-Notification-To).

Eine gemeinsame Nutzung beider Methoden ermöglicht, dass die Option einer Statusrückmeldung erhalten bleibt, selbst wenn der PGP/MIME Container nicht zu öffnen ist. Die Abbildung 6 zeigt die Verwendung von beiden X-Tags. In Abbildung 7 wird die alleinige Verwendung von X-TELEMEDICINE-DISPOSITION-NOTIFICATION-TO gezeigt.

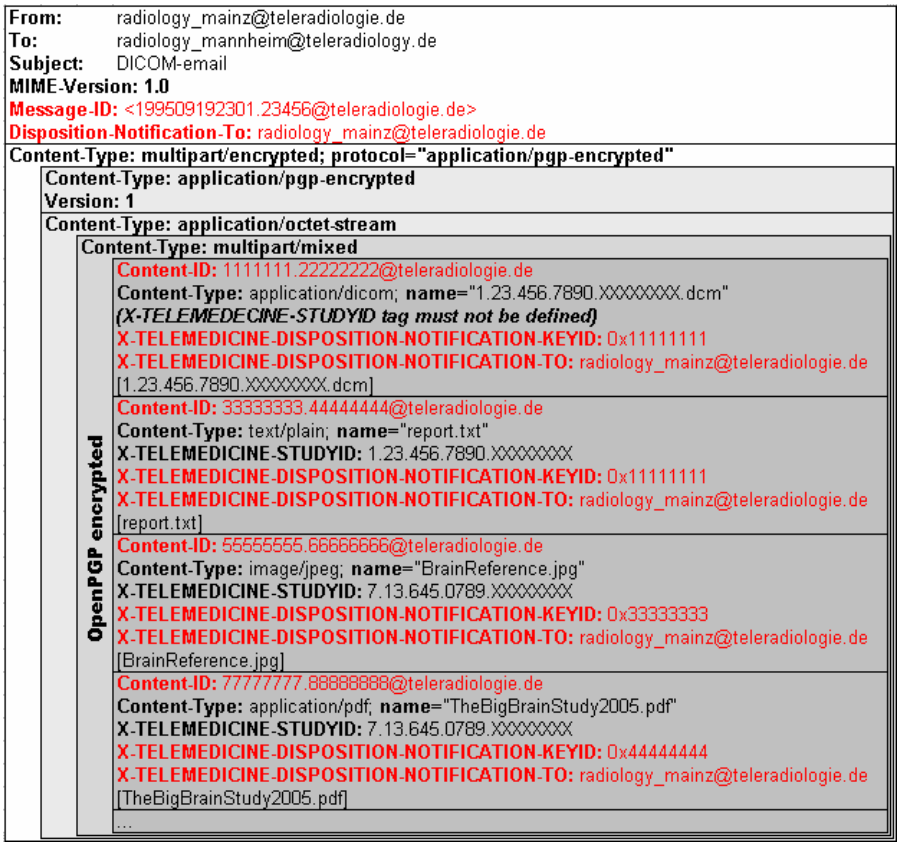

Abb. 6 –Inhaltsbezogene „Request for Notification“ eMail unter Verwendung der X-Tags für KeyID und Rücksendeemailadresse

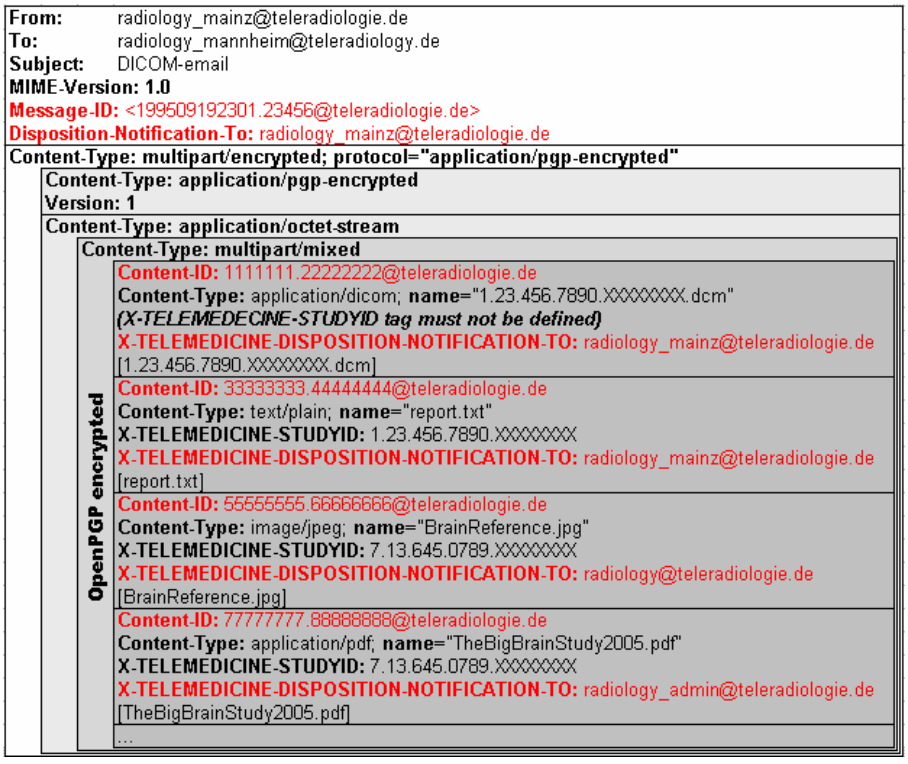

Abb. 7 –Inhaltsbezogene „Request for Notification“ eMail unter Verwendung des X-Tags der Rücksendeemailadresse

Rückmeldungsmail (Notify Mail)

Für die Antwortmail der beiden unterschiedlichen Anforderungsarten ist folgendes zu beachten: Grundsätzlich ist es dem Empfänger freigestellt, ob er eine Antwortemail verschickt. Bei der Verwendung von Mechanismus 1 kann genau eine Notification gesendet werden. Dabei wird eine Notify Mail, welche aus der nicht verschlüsselten Aufforderung (Mechanismus 1) resultiert, ebenso unverschlüsselt versendet. Die aus dem verschlüsselten Teil resultierenden Notify Mails werden entweder verschlüsselt oder unverschlüsselt verschickt. Dies richtet sich nach den verwendeten X-Tags im verschlüsselten Teil der Request-Mail. Wird das Tag X-TELEMECICINE-DISPOSITION-KEYID angegeben, so erfolgt die Rücksendung verschlüsselt. Fehlt die KeyID wird die Antwortmail unverschlüsselt verschickt, da so nicht sicher gewährleistet werden kann, dass der korrekte Schlüssel für den Versand verwendet wird.

Die verschlüsselten Notify eMails 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 8 und 9 zeigen das Beispiel einer nicht verschlüsselten Notify Mail (Abb. 8) und einer verschlüsselten, nicht RFC 3798 konformen Notify Mail (Abb. 9). Die Abbildungen zeigen das Grundgerüst. Die Inhalte der Mails werden durch die Statuscodes ausgedrückt. Diese werden im Kapitel Status behandelt.

Mechanismus 1 Notify

Die Notify Mail baut sich gemäß des RFC 3798 auf. Eine solche Mail gliedert sich in 2 Abschnitte: Header und multipart/report. Der 2. Abschnitt multipart/report wiederum ist in 3 Abschnitte (Parts) unterteilt: Part 1 – menschenlesbar, Part 2 – maschinenlesbar und Part 3 – Referenz auf die zugrunde liegende eMail. Der Part 3 ist optional und wird nicht verpflichtend von der Version 1.5 der hier vorliegenden Standardempfehlung gefordert. Die Antwortmail auf eine Anfrage (*Disposition-notification-to:*) erfolgt analog zu diesem Schema. In der Abb. 8 wird eine Beispielantwort auf die Anfrage aus Abb. 5 gezeigt. In diesem Fall gibt es die Rückmeldung, dass die empfangene Mail einen Fehler in der Syntax aufweist, der zu keinem verarbeitungsrelevanten Fehler geführt hat (Warning).

```
Date: Mon, 1 Jan 2009 00:19:00 (EDT) -0400
From: radiology_mannheim@teleradioloy.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/teleradiologie.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 corrupt mail syntax

--RAA14128.773615765/teleradiologie.de--
```

Abb. 8 – „Notify Mail“ nach RFC 3798

Mechanismus 2 Notify

Die Antwort auf die Rückmeldungsanforderung (Abb. 6) aus dem verschlüsselten PGP/MIME Container ergibt wiederum eine verschlüsselte Notify Mail. Diese ist folgendermaßen aufgebaut:

Der äußere Mailcontainer ist wie eine verschlüsselte eMail aufgebaut. In dem verschlüsselten Part 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 das Feld „X-TELEMEDICINE-ORIGINAL-CONTENT-ID“ anstatt dem Feld „Original-Message-ID“.

Die Abb. 9 zeigt ein Anwendungsbeispiel als Antwort auf die Anfrage aus Abb. 6.

```
From: radiology_mannheim@teleradioloy.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@ teleradioloy.de >
```

```
Content-Type: multipart/encrypted; protocol="application/pgp-
encrypted";
boundary="--=_NextPart_000_0027_01BF27A0.9BE21980/teleradioloy.de"

This is a multi-part message in MIME format.

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

Version: 1

----=_NextPart_000_0027_01BF27A0.9BE21980/teleradioloy.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/teleradiologie.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 corrupt mail syntax
%
%--RAA14128.773615765/teleradiologie.de--

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

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

* Die mit % eingeleiteten Zeilen sind in der echten Mail PGP verschlüsselt.

Abb. 9 – Notify Mail Antwort auf eine Anfrage aus dem PGP/MIME Container

Die Antwortmail aus der Anforderung aus Abb. 7 ergibt unverschlüsselte Antwort-eMails wie unter dem Mechanismus 1 in Abb. 8 gezeigt wird.

Statusmeldungen

Statusrückmeldungen werden gemäß des RFC3798 übergeben. Zur Verwendung kommen die Disposition Types „Displayed“ und „Deleted“. Als Konvention wurde vereinbart, dass „Keine Fehler“ und „Warnings“ 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 Disposition Types 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 **Code** wie in Anhang A definiert.

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

13. Generierung von Identifikationsnummern (IDs)

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 [siehe 7.Grundüberlegung].

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.

14. 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 eMail 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.

15. Geplante Weiterentwicklung

Einbringen der Ergebnisse in IHE

Die initial geplante Erstellung eines IHE Profils ist durch die Entwicklung von XDS in Frage gestellt worden. Zurzeit soll geprüft werden, inwieweit ein eigenes Profil sinnvoll ist bzw. die vorliegende Arbeit in bestehende Profile eingearbeitet werden können.

16. Mitgeltende Unterlagen

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

DICOM Standard

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

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

17. Anhang A

Die Fehlercodes werden in der getrennt erhältlichen Datei „Fehlercodes.pdf“ aufgelistet. Grundsätzlich sind diese in verschiedene Kategorien untergliedert. Die Codes werden von 0 bis n nummeriert und können beliebig viele Untercodes besitzen. Die nachfolgende Tabelle 1 ist ein Beispiel für den grundsätzlichen Aufbau der Fehlercodes. Jeder dieser Fehlercodes kann auf beliebiger Ebene benutzerspezifisch um .0 erweitert werden (z.B. siehe Code 2.1.0.2).

Kategorie	Code	Bedeutung
Undefined		
	0	vendor specific errors
Mail		
	1	general mail error
	1.1	mail was read before
	1.2	corrupt mail syntax
	1.2.1	corrupt mail syntax – empty body part
OpenPGP		
	2	general openpgp error
	2.1	no public key available
	2.2	key expired
	2.2.1	signing key expired (sender)
	2.1**.0.2**	**no public key available, no GPG installed**
	2.2.2	encryption key expired (receiver)
	2.3	valid signature from untrusted public key
Application		
	3.1	unknown mimetype not processed
	3.2	internal error
	3.2.1	attachement not processed
XTelemedicine		
	4	general x-tag error
	4.1	x-telemedicine-set tag error
	4.1.1	x-telemedicine-set tag error – missing intern

Tabelle 1: Beispielfehlercodes

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