Digital Imaging and Communications in Medicine (DICOM)

Supplement 113 – Email Transport

Prepared by:

DICOM Standards Committee, Working Group 6

1300 N. 17th Street Suite 1752

Rosslyn, Virginia 22209 USA

VERSION: Final Text

August 24, 2006

Table of Contents

Foreword

There is a need to support the transmission of DICOM Composite SOP instances by email. One major use case is in the dental community, where a selection of dental images must be sent from one location to another. Email is preferred because they do not have a permanent network connection and because there are many ad hoc connections to establish on short notice. There is a similar requirement for transmission of images in locations where there is no reliable continuous network connectivity. Email provides this kind of connectivity without requiring a large IT staff to manage such connections. There is also a requirement to transmit other information such as instructions to the recipient in the email.

The DICOM instances may contain private health information that must be protected, so an adequate encryption mechanism must be provided for the email. The mechanism used must provide an envelope to convey the DICOM instances, a manifest indicating the intended list of images, plus any associated non-DICOM material, in a single package. There will be serious problems if a partial or damaged delivery can be mistaken for a complete package.

The sender and recipient will be using a wide variety of commercial email products for both the user agent and the transport agent. Some of these products do not contain code to perform special processing for DICOM objects. The user interface should require minimal interaction or training. The solution must permit the use of ordinary office automation tools.

There will also be DICOM aware applications that create and receive these emails, which must interoperate with the ordinary office automation tools.

The existing DICOM media profile for email transmission uses a MIME multipart related format that is difficult to create reliably by an ordinary user with ordinary office automation tools. Very few users understand how to manually create MIME multipart related messages. Some common office application email packages will not permit manual creation of such messages.

This supplement adds an email transport mechanism based on:

a. using a ZIP file to encode the DICOM File-set in a single DICOM attachment. This could be done using ZIP facilities that are provided by some email tools, by separately using an application to create the ZIP file, or by a DICOM aware application that has a ZIP creation facility. This is usually a “single click” activity.

b. sending the ZIP file as an ordinary email attachment. This can be done manually using the email tool’s “attach file” facility or by a DICOM aware application. This is either a single click or very few clicks operation depending on the particular tool.

c. encrypting the email using S/MIME. This capability is built into most email packages.

d. on the receiving side, detaching and extracting the ZIP file using either ordinary office applications or a DICOM aware program. This is usually a single click operation.

e. verifying the digital signature using ordinary office applications. This is sometimes fully automatic and sometimes single click.

This supplement addresses security by requiring the use of the S/MIME encryption, compression, and signature mechanisms. These are incorporated into all recent office automation user agents. This supplement does not address the PKI issues of signature certificate distribution, but the S/MIME tools

make use of the standard certificate format that is used by the various PKI systems. So it is adaptable and usable in any of the various PKI environments around the world. It will be necessary for local user groups, associations, or regulatory domains to specify how they will manage certificates for their local use. DICOM remains silent on those issues.

This supplement has a secure use profile that requires the use of encryption for messages sent by email, and requires that the messages be signed to attest to authorization to disclose the data to the recipient. Additional signatures can be added to these packages by other profiles, although there are no such other profiles at present. The approach selected does not address the selective signing of individual objects within the set of data that is sent. Selective signing is dealt with by other DICOM mechanisms.

This Supplement proposes changes to the following Parts of the DICOM Standard:

PS 3.11- Media Storage Application Profiles

PS 3.12- Media Formats and Physical Media for Media Interchange

PS 3.15 - Security and System Management Profiles

Digital Imaging and Communications in Medicine (DICOM)

Part 11: Media Storage Application Profiles

Part 11: Add Annex X – ZIP over Email

Annex X (Normative) – ZIP File over Email Interchange Profiles

X.1 PROFILE IDENTIFICATION

This Annex defines three Application Profiles for interchange of a DICOM Data Set, encapsulated in a ZIP File, through email.

Two Application Profiles support all defined Media Storage SOP Classes. These are intended to be used for the interchange of Composite SOP Instances via email for general purpose applications. Objects from multiple modalities may be included on the same email. The email may also include non-DICOM objects. One of these general profiles supports encryption of the email.

A detailed list of the Media Storage SOP Classes is defined in PS 3.4

The other application profile is specialized for dental applications and adds mandatory requirements for dental images to the general secure email profile.

The specific Application Profiles are shown in Table X.1-1:

Table X.1-1
STD-x-ZIP-MAIL Application Profiles

Application Profile	Identifier	Description
General Purpose ZIP Email	STD-GEN-ZIP-MAIL	Interchange of Composite SOP Instances by email.
General Purpose Secure ZIP Email	STD-GEN-SEC-ZIP-MAIL	Interchange of Composite SOP Instances by encrypted email.
Dental Radiograph ZIP Email	STD-DTL-SEC-ZIP-MAIL	Interchange of dental radiographic images by encrypted email

X.2 CLINICAL CONTEXT

These Application Profiles facilitate the interchange of images and related data through email.

The STD-GEN-ZIP-MAIL and STD-GEN-SEC-ZIP-MAIL profiles are intended for general purpose applications. They are not intended as a replacement for specific Application Profiles that may be defined for a particular clinical context. The STD-DTL-SEC-ZIP-MAIL profile is intended for the clinical context of the exchange of dental radiographs.

Note: It is possible to use email transport without using the encrypted secure profile. This would make sense for mailing DICOM objects that do not need protection.

X.2.1 Roles

X.2.1.1 File Set Creator

The role of File Set Creators shall be used by Application Entities that generate a File-set under any of the profiles listed in Table X.1-1. Typical entities that will use this role would include systems assigned to send images by email attachment to other systems. File Set Creators shall be able to generate the DICOMDIR directory file, and any supported DICOM Storage SOP Class Information Object files.

X.2.1.2 File Set Reader

The role of File Set Reader shall be used by Application Entities that receive a transferred File Set. File Set Readers shall be able to read the DICOMDIR directory file and all Information Objects defined for the specific Application Profiles, using the defined Transfer Syntaxes.

X.2.1.3 File Set Updater

The role of File Set Updater is not defined for these Application Profiles.

X.3 GENERAL CLASS PROFILE

X.3.1 STD-GEN-ZIP-MAIL and STD-GEN-SEC-ZIP-MAIL Abstract and Transfer Syntaxes

Applications interchanging data under the STD-GEN-ZIP-MAIL and STD-GEN-SEC-ZIP-MAIL profiles shall support the Information Object Definitions (IOD) and Transfer Syntaxes for the Media Storage SOP Class specified in Table X.3-1.

Table X.3-1
STD-GEN-ZIP-MAIL and STD-GEN-SEC-ZIP-MAIL SOP Classes and Transfer Syntaxes

Information Object Definition	Service Object Pair Class UID	Transfer Syntax and UID	FSC Requirement	FSR Requirement
Basic Directory	1.2.840.10008.1.3.10	Explicit VR Little Endian Uncompressed 1.2.840.10008.1.2.1	Mandatory	Mandatory
Composite Image & Stand-alone Storage	Refer to: PS 3.4 for SOPs UID definitions	Defined in Conformance Statement	Defined in Conformance Statement	Defined in Conformance Statement

Equipment claiming conformance to these Application Profiles shall list the subset of Media Storage SOP Classes and transfer syntaxes that it supports in its Conformance Statement.

X.3.2 Medium Format

The STD-GEN-ZIP-MAIL and STD-GEN-SEC-ZIP-MAIL application profiles shall use the ZIP File Media interchanged using the Email Media format as defined in PS3.12. This Email media shall comply with the following requirements:

a. The content shall be identified as: `Content-Type: application/zip`
b. The attachment shall be identified as: `id="DICOM.ZIP"; name="DICOM.ZIP"`
c. The disposition shall be: `Content-Disposition: attachment; filename="DICOM.ZIP"`
d. The email shall not be compressed.
e. The subject line shall contain the phrase: `DICOM-ZIP`

Note: An additional content type, file extension and file name may be defined by the Standard in the future to accomodate a DICOM specific zip file.

X.3.3 Directory Information in DICOMDIR

The Directory shall include Directory Records of PATIENT, STUDY, SERIES, IMAGE corresponding to the information object files in the File Set. All DICOM files in the File Set incorporating SOP Instances (Information Objects) defined for the specific Application Profile shall be referenced by Directory Records.

Note: 1. DICOMDIRs with no directory information are not allowed by these Application Profiles.

There may only be one DICOMDIR file per File Set. The Patient ID at the patient level shall be unique for each patient directory record in one File Set.

X.3.3.1 Additional Keys

No additional keys are specified.

X.3.4 Secure Transport

The Email Media interchange under the STD-GEN-SEC-ZIP-MAIL profile shall use the Secure Use of Email Transport profile specified in PS3.15.

X.4 DENTAL CLASS PROFILE

X.4.1 STD-DTL-SEC-ZIP-MAIL Abstract and Transfer Syntaxes

Applications interchanging data under the STD-DTL-SEC-ZIP-MAIL profile shall support the Information Object Definitions (IOD) and Transfer Syntaxes for the Media Storage SOP Class specified in Table X.3-2. File Set Creators for the STD-FTL-SEC-ZIP-MAIL shall support at least one of the optional IODs.

Table X.3-2
STD-DTL-SEC-ZIP-MAIL ABSTRACT AND TRANSFER SYNTAXES

Information Object Definition	SOP Class UID	Transfer Syntax and UID	FSC Requirement	FSR Requirement
Basic Directory	1.2.840.10008.1.3.10	Explicit VR Little Endian Uncompressed 1.2.840.10008.1.2.1	Mandatory	Mandatory
Digital Intra-oral X-Ray Image Storage – For Presentation	1.2.840.10008.5.1.4.1.1.1.3	Explicit VR Little Endian Uncompressed 1.2.840.10008.1.2.1	Optional	Mandatory
Digital X-Ray Image Storage – For Presentation	1.2.840.10008.5.1.4.1.1.1.1	Explicit VR Little Endian Uncompressed 1.2.840.10008.1.2.1	Optional	Mandatory

X.4.2 Medium Format

The STD-DTL-SEC-ZIP-MAIL application profile shall use the ZIP File Media interchanged using the Email Media format as defined in PS3.12. This Email media shall comply with the following requirements:

f. The content shall be identified as: `Content-Type: application/zip`

g. The attachment shall be identified as: `id="DICOM.ZIP"; name="DICOM.ZIP"`

h. The disposition shall be: `Content-Disposition: attachment; filename="DICOM.ZIP"`

i. The email shall not be compressed.

j. The subject line shall contain the phrase: `DICOM-ZIP`

Note: An additional content type, file extension and file name may be defined by the Standard in the future to accomodate a DICOM specific zip file.

X.4.3 Directory Information in DICOMDIR

The Directory shall include Directory Records of PATIENT, STUDY, SERIES, IMAGE corresponding to the information object files in the File Set. All DICOM files in the File Set incorporating SOP Instances (Information Objects) defined for the specific Application Profile shall be referenced by Directory Records.

Note: 1. DICOMDIRs with no directory information are not allowed by these Application Profiles.

There may only be one DICOMDIR file per File Set. The Patient ID at the patient level shall be unique for each patient directory record in one File Set.

X.4.4.1 Additional Keys

No additional keys are specified.

X.4.5 Specific Image Requirements for STD-DTL-SEC-ZIP-MAIL

For Digital Intra-oral X-Ray Image and Digital X-Ray Image Instances interchanged under the STD-DTL-SEC-ZIP-MAIL profile, the Attributes listed in Table X.4-1 used within the image instances shall take the values specified.

Table X. 4-1
STD-DTL-ZIP-MAIL - REQUIRED IMAGE ATTRIBUTE VALUES

Attribute	Tag	Value
Bits Allocated	(0028,0100)	If Bits Stored (0028,0101) is 8, then 8; otherwise 16.
Bits Stored	(0028,0101)	8, 10, 12 or 16

The Attributes listed in Table X.4-2 shall have their Types specialized.

Table X.4-2
STD-DTL-ZIP-MAIL - REQUIRED IMAGE ATTRIBUTE TYPES

Attribute	Tag	Type
Institution Name	(0008,0080)	2
Manufacturer's Model Name	(0008,1090)	2
Detector ID	(0018,700A)	2
Detector Manufacturer Name	(0018,702A)	2
Detector Manufacturer's Model Name	(0018,702B)	2

Note: These Type 3 attributes of the General Equipment and DX Detector Module are specialized in order to encourage FSC's to include values for them, recognizing that there are situations in which values may be unknown.

X.4.6 Secure Transport

The Email Media interchange under the STD-DTL-SEC-ZIP-MAIL profiles shall use the Secure Use of Email Transport profile specified in PS3.15.

Digital Imaging and Communications in Medicine (DICOM)

Part 12: Media Formats and Physical Media for Media Interchange

Add to Part 12 Section 2 Normative references

RFC 1939	Post Office Protocol - Version 3 (POP3)
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2046	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
RFC 2821	Simple Mail Transfer Protocol (SMTP)
RFC 3464	An Extensible Message Format for Delivery Status Notifications
RFC 3501	Internet Message Access Protocol - Version 4rev1 (IMAP4)
RFC 3798	Message Disposition Notification

ZIP File Format Specification, PKWARE , Inc.

Add to Part 12 Section 4 Symbols and abbreviations

IMAP4	Internet Message Access Protocol - Version 4
MIME	Multipurpose Internet Mail Extensions
POP3	Post Office Protocol - Version 3
SMTP	Simple Mail Transfer Protocol

Add Annex Y to Part 12

ANNEX Y (Normative) ZIP File Media

Y.1 DICOM MAPPING TO ZIP FILE

Y.1.1 DICOM File-set

One and only one DICOM File-set shall be contained in a ZIP File archive.

Each DICOM SOP Instance shall be encoded in accordance with the rules in PS 3.10.

Note: A ZIP File may contain files that are not referenced by the DICOMDIR, and which may be ignored by the DICOM application.

Y.1.2 DICOM File ID Mapping

The ZIP encoding preserves the hierarchical structure for directories and files within directories. Each volume has a root directory that may contain references to both files and subdirectories. Subdirectories may contain reference to both files and other subdirectories.

Y.1.2.1 File ID

PS 3.10 defines a DICOM File ID Component as a string of 8 characters from a subset of the G0 repertoire of ISO 8859.

Note: The use of long filenames is prohibited.

Filename extensions are not used in DICOM File ID Components, hence a File Identifier shall not contain a File Extension or the '.' that would precede such a File Extension.

The maximum number of levels of a pathname in a ZIP file-set shall be at most 8 levels, to comply with the definition of a DICOM File-set in PS 3.10.

Y.1.2.2 DICOMDIR

One and only one DICOMDIR File shall be present. The DICOMDIR shall be at the root directory of the File-set.

Note: The reason for the DICOMDIR is to serve as a manifest so that the recipient knows the full list of instances intended to be sent.

Y.2 LOGICAL FORMAT

The Zip file format shall be as described in the ZIP File Format Specification available from PKWARE. The following capabilities shall be used:

a. The ZIP encoding shall preserve the directory structure.

Note: This specification may be found at http://www.pkware.com/business_and_developers/developer/popups/appnote.txt.

Add Annex Z to Part 12

ANNEX Z (Normative) Email Media

Z.1 EMAIL MEDIA

This Media Format defines the interchange of other Media Formats, such as DICOM MIME or ZIP File, using email.

A Standard or Private Application Profile that uses this Email Media Format will specify the selection of the media profile to be transported.

A Standard or Private Application Profile that uses this Email Media Format specifies the MIME encoding requirements, to include:

a. The content identification to be used,
b. The attachment file identification to be used,
c. The disposition to be used,
d. Subject line content restrictions,
e. Other restrictions, especially use of MIME compression, encryption, and digital signatures.

Note: Subject lines are often modified automatically, e.g., by the addition of “Re:”. Other routing information such as “for Doctor Fred” is also often included. Automatic and human recognition of the special nature of this email can be improved by requiring that some phrase like “DICOM-ZIP” be part of the subject line.

Z.2 MEDIA INTERCHANGE APPLICATION ENTITIES

Z.2.1 Sender of the Email

The sender Application Entity composes an email and sends that email using a standard email transmission protocol.

The sender shall compose an email in compliance with RFCs 2045 and 2046, as a MIME Encoded email. RFC 2046 defines both MIME encoding and the mechanisms to be used for breaking up the email message if it is too large for the email system to send as a single email. The sender may request delivery acknowledgement and problem notification in accordance with RFCs 3464 and 3798, but shall be prepared for email recipients that do not implement RFCs 3464 and 3798. The sender shall send the email by means of Simple Mail Transfer Protocol (RFC 2821).

Note: The sender Application Entity does not need to be a single software program. For example, the attachment file may be created independently and then a generic email program used to manage attaching the file and sending the email.

Z.2.2 Recipient of the Email

The recipient Application Entity shall be able to receive an email by means of one or more of POP3 (RFC 1939), IMAP4 (RFC 3501), or SMTP (RFC 2821), and extract the attachment specified in the Application Profile. The recipient shall comply with RFC 2046, and may comply with RFCs 3464 and 3798.

Digital Imaging and Communications in Medicine (DICOM)

Part 15: Security and System Management Profiles

Add Part 15 Section 2 Normative references

RFC 3851	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification
RFC 3853	S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)

Add section B.X to Part 15

B.X SECURE USE OF EMAIL TRANSPORT

When a DICOM File Set is sent over Email transport in compliance with this profile the following rules shall be followed:

a. The File Set shall be an attachment to the email body.
b. The entire email (body, File Set attachment, and any other attachments) shall be encrypted using AES, in accordance with RFC 3851 and RFC 3853.
c. The email body and attachments may be compressed in accordance with RFC 3851.
d. The email shall be digitally signed by the sender. The signing may be applied before or after encryption. This digital signature shall be interpreted to mean that the sender is attesting to his authorization to disclose the information in this email to the recipient.

The email signature is present to provide minimum sender information and to confirm the integrity of the email transmission (body contents, attachment, etc.). The email signature is separate from other signatures that may be present in DICOM reports and objects contained in the File set attached to the email. Those signatures are defined in terms of clinical uses. Any clinical content attestations shall be encoded as digital signatures in the DICOM SOP instances, not as the email signature. The email may be composed by someone who cannot make clinical attestations. Through the use of the email signature, the composer attests that he or she is authorized to transmit the data to the recipient.

Notes: 1. This profile is separate from the underlying use of ZIP File or other File Set packaging over email.

2. Where private information is being conveyed, most country regulations require the use of encryption or equivalent protections. This Profile meets the most common requirements of regulations, but there may

be additional local requirements. Additional requirements may include mandatory statements in the email body and prohibitions on contents of the email body to protect patient privacy.