Digital Imaging and Communications in Medicine (DICOM)

Supplement 51: Media Security

DICOM Standards Committee, Working Group 14 Security

1300 N. 17th Street

Rosslyn, Virginia 22209 USA

VERSION: Final Text

10 Sep 2001

This is a draft document. Do not circulate, quote, or reproduce it except with the approval of NEMA

Please send comments to Howard Clark, NEMA (how_clark@nema.org)

CONTENTS

FOREWORD

This supplement addresses the following aspects of security defined in ISO 7498-2 at the level of DICOM media storage:

- Data Confidentiality – the property that information is not made available or disclosed to unauthorized individuals, entities or processes,
- Data Integrity – the property that data has not been altered or destroyed in an unauthorised manner,
- Data Origin Authentication – the corroboration that the source of data received is as claimed,

This supplement defines:

- a framework for the protection of DICOM Files for Media Interchange by means of an encapsulation with a cryptographic "envelope". This is concept is called *Secure DICOM File* throughout this document.
- a means of communicating the encryption keys to the intended recipients by means of key transport, key agreement or symmetric key-encryption key schemes,
- an industry standard symmetric encryption algorithm for protection of encrypted attributes (Triple-DES);

This supplement adds Attribute definitions and conformance requirements to PS 3.10, PS 3.11 and PS 3.15 for implementing the Media Security functions.

The Cryptographic Message Syntax (CMS)

The Cryptographic Message Syntax (CMS), RFC 2630, has been standardized by the Internet Engineering Task Force as the successor of the proprietary PKCS#7 specification ("public key cryptography standard #7"), in a similar way toTLS being the standardized successor of the proprietary SSL3 protocol. CMS defines an encapsulation syntax for data protection of arbitrary messages. It supports digital signatures, message authentication codes, and encryption. The syntax allows multiple encapsulation, so one encapsulation envelope can be nested inside another. CMS supports a variety of architectures for certificate-based key management. In particular, the X.509v3 certificates required for secure DICOM network communication over TLS (Supplement 31) as well as for digital signatures (draft Supplement 41) can also be used with CMS, which means that the same public key infrastructure can be used for all DICOM security extensions (also including the draft Supplement 55). CMS is very flexible in allowing a large number of cryptographic algorithms and key sizes to be used, depending on the capabilities of the implementation.

CMS differs from the TLS protocol recommended in Supplement 31 in being a security specification for store-and-forward communication such as e-Mail or storage media interchange. Unlike the protocol data units of the TLS protocol, each CMS encrypted block of data (e. g. DICOM file) is self-contained, with all necessary auxiliary data being part of the encoded data. This also means that there is no dynamic negotiation of supported security functions (key sizes, algorithms etc.) in CMS. Therefore, a careful "profiling" of the standard (an approach similar to the DICOM media storage application profiles) is required if interoperability should be guaranteed. This supplement addressed this need by defining a Media Storage Security Profile that requires certain CMS structures and algorithms to be supported by conforming implementations.

WHY CMS?

In the late 1990s, the European Union sponsored a number of research projects on IT security standards in the framework of the “Information Society Initiative in Standardization” (ISIS). Among these projects were also two healthcare related projects, “Health Care Security and Privacy in the Information Society” (MEDSEC) and “Secure Medical Record Information Communication” (SEMRIC). Both projects, independently from each other, came to the conclusion that PKCS#7 was the most appropriate specification for security encapsulation of store-and-forward messages in health care. This resulted in the creation of the CEN Prestandard ENV 13608-2 “Health Informatics - Security for healthcare communication - Part 2: Secure data objects” which recommends the Cryptographic Message Syntax, being the standardized successor of PKCS#7, for use with secure store-and-forward communication of healthcare data. Building on this work, DICOM WG14 has also selected CMS as the security envelope syntax for encapsulating DICOM files.

It should be noted that CMS is also used outside the DICOM world: Version 3 of the S/MIME specification for secure e-Mail (RFC 2633) is based on CMS, which means that most Web browsers support CMS. Other uses include the “DCE Public Key Certificate Login“ Specification from the Open Group. CMS has also been proposed for secure HL7 messaging.

1 ADDITIONS TO PS 3.10

ITEM 10.1 AMEND THE FOLLOWING TEXT IN SECTION 1 (SCOPE AND FIELD OF APPLICATION)

This Part specifies:

b. a DICOM File Format supporting the encapsulation of any Information Object Definition;

c. a Secure DICOM File Format supporting the encapsulation of a DICOM File Format in a cryptographic envelope;

~~c.~~**d.** a DICOM File Service providing independence from the underlying media format and physical media. The policies specific to the DICOMDIR file used to store the Media Storage Directory Service/Object Pair Class are also addressed.

This Part is related to other parts of the DICOM Standard in that:

- **PS 3.15, Security Profiles defines a number of profiles for use with Secure DICOM Media Storage Application Profiles. The Media Storage Security Profiles specify the cryptographic techniques to be used for each Secure DICOM File in a Secure Media Storage Application Profile.**

ITEM 10.2 ADD THE FOLLOWING REFERENCES TO SECTION 2

ISO 7498-2, Information processing systems - Open Systems Interconnection - Basic reference Model - Part 2: Security Architecture

RFC-2630, Cryptographic Message Syntax, June 1999

ITEM 10.3 AMEND THE FOLLOWING TEXT IN SECTION 3.1

3.1 Reference Model Definitions

This Part of the Standard is based on the concepts developed in ISO 7498-1 and makes use of the following terms defined in it:

a. Application Entity;
b. Application Process;
c. Service or Layer Service;
d. Transfer Syntax.

This Part of the Standard makes use of the following terms defined in ISO 7498-2:

a. Data Confidentiality

Note: The definition is “the property that information is not made available or disclosed to unauthorized individuals, entities or processes.”

b. Data Origin Authentication

Note: The definition is “the corroboration that the source of data received is as claimed.”

c. Data Integrity

Note: The definition is “the property that data has not been altered or destroyed in an unauthorized manner.”

ITEM 10.4 ADD THE FOLLOWING NEW DEFINITIONS IN SECTION 3.8

Secure DICOM File: A DICOM File that is encapsulated with the Cryptographic Message Syntax specified in RFC 2630.

Secure File-set: A File-set in which all DICOM Files are Secure DICOM Files.

Secure Media Storage Application Profile: A DICOM Media Storage Application Profile that requires a Secure File-set.

ITEM 10.5 AMEND THE FOLLOWING TEXT IN SECTION 6.2.3

The DICOM Data Format Layer includes ~~four~~ six elements of specification:

a. DICOM Media Storage SOP Classes and associated Information Object Definitions;

b. The DICOM File Format;

c. The Secure DICOM File Format;

~~c~~**d**. The DICOM Media Storage Directory SOP Class;

~~d~~**e**. DICOM Media Storage Application Profiles**;**

f. DICOM Security Profiles for Media Storage.

ITEM 10.6 ADD THE FOLLOWING TEXT TO SECTION 6.2.3.2

The encapsulation of a DICOM File in a Secure DICOM File shall follow the specifications of Section 7.4 of this Part. These encapsulation rules define a mechanism for creating a Secure DICOM File by encapsulating an unprotected DICOM File as payload within a secure envelope.

ITEM 10.7 AMEND THE FOLLOWING TEXT IN SECTION 6.2.4

Media Storage Application Profiles shall include:

a. The description of the need addressed by the Application Profile (e.g., cardiac, echography, angiography) and its context of application;

b. The selection, at the Data Format Layer, of a number of specific IODs and associated SOP Classes. For standard DICOM SOP Classes, this shall be done by reference to PS 3.4 of the DICOM Standard. These SOP Classes, like any other DICOM SOP Classes are assigned a unique registered UID. For each SOP Class it shall be stated if its support is required or optional within the context of this profile;

c. The selection of a specific Media Format definition. This is done by reference to PS 3.12 of the DICOM Standard which specif~~y~~ies the selected Physical Medium, a specific associated Media Format and the mapping of this Media Format (or file system) services onto the DICOM File Service;

d. The selection of appropriate Transfer Syntaxes;

e. The selection of a specific Security Profile. This is done by reference to PS 3.15 of the DICOM Standard which specifies the cryptographic algorithms to be used to encapsulate the DICOM Files of the DICOM File Set into Secure DICOM Files. If a Media Storage Application Profile selects no Security Profile, then the Application Profile is unsecure and the Secure DICOM File Format shall not be used with that Application Profile;

~~e.~~ **f.** Other choices facilitating interoperability such as specific limits (e.g., maximum file sizes, if necessary, support of options, if any).

ITEM 10.8 AMEND FIGURE 6.2-2

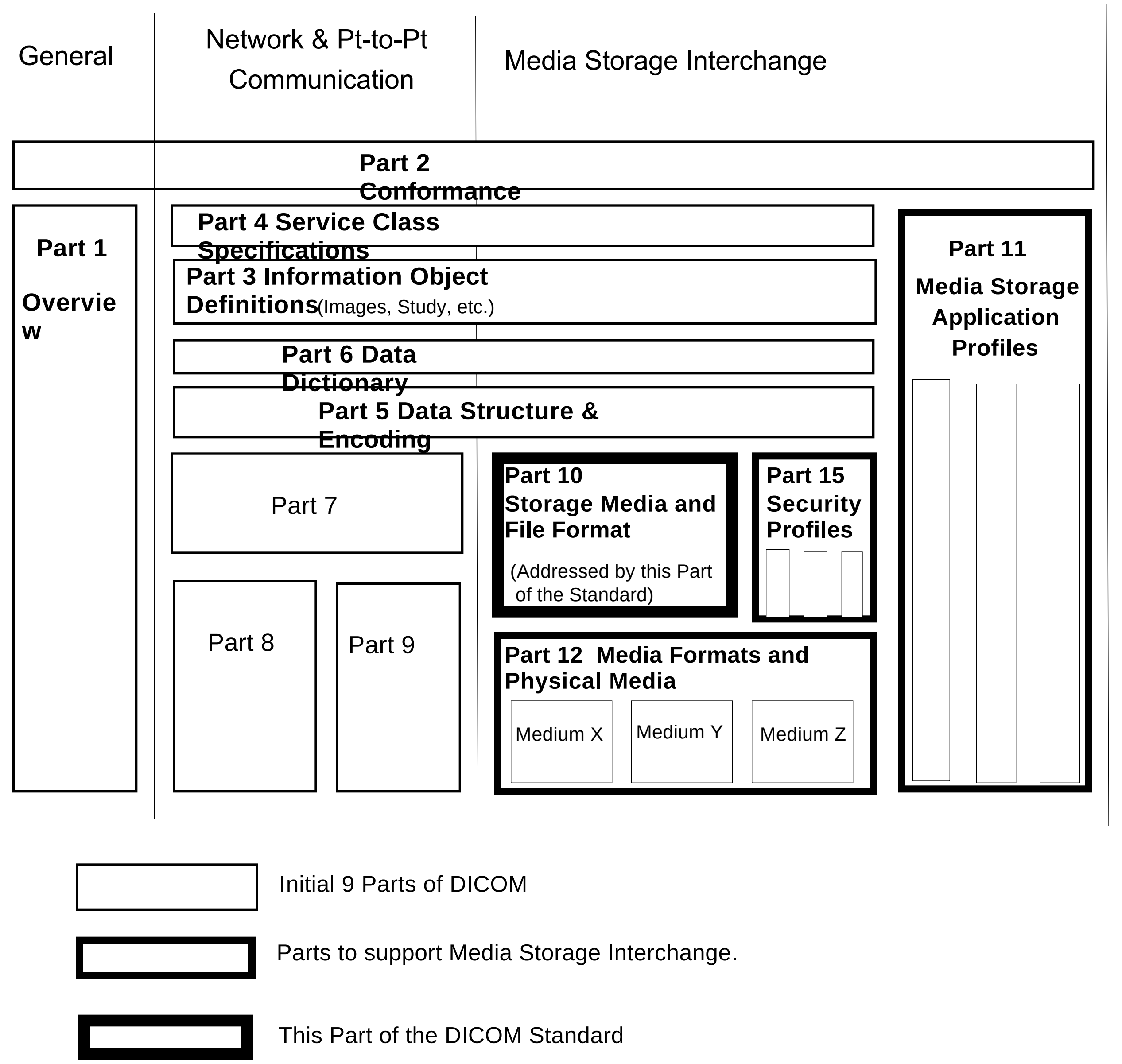
General
Network & Pt-to-Pt Communication
Media Storage Interchange
Part 2 Conformance
Part 1 Overview
Part 4 Service Class Specifications
Part 3 Information Object Definitions(Images, Study, etc.)
Part 6 Data Dictionary
Part 5 Data Structure & Encoding
Part 7
Part 8
Part 9
Part 10 Storage Media and File Format
(Addressed by this Part of the Standard)
Part 15 Security Profiles
Part 11 Media Storage Application Profiles
Part 12 Media Formats and Physical Media
Medium X
Medium Y
Medium Z
Initial 9 Parts of DICOM
Parts to support Media Storage Interchange.
This Part of the DICOM Standard

Figure 6.2-2
Media Storage and DICOM Parts

ITEM 10.9 DELETE THE FOLLOWING TEXT IN SECTION 7.3

~~**Note: This version of DICOM PS 3.10 does not address media interchange security beyond the Media and File access control services that a selected Medium Format may support. The requirements for security management, beyond the efficient capabilities provided by the Physical Media Layer and/or the Media Format Layer may be considered in future versions of DICOM Media Storage Standards..**~~

ITEM 10.10 ADD THE FOLLOWING NEW SECTION 7.4

7.4 Secure DICOM FILE FORMAT

A Secure DICOM File shall contain a single DICOM File encapsulated with the Cryptographic Message Syntax as defined in RFC 2630. Depending on the cryptographic algorithms used for encapsulation, a Secure DICOM File can provide one or more the following security properties:

- Data Confidentiality (by means of encryption)
- Data Origin Authentication (by means of certificates and digital signatures)
- Data Integrity (by means of digital signatures)

In addition, a Secure DICOM File offers the possibility to communicate encryption keys and certificates to the intended recipients by means of key transport, key agreement or symmetric key-encryption key schemes.

2 ADDITIONS TO PS 3.11

ITEM 11.1 ADD THE FOLLOWING TEXT IN SECTION 1 (SCOPE AND FIELD OF APPLICATION)

This Part is related to other parts of the DICOM Standard in that:

- **PS 3.15, Security Profiles defines a number of profiles for use with Secure DICOM Media Storage Application Profiles. The Media Storage Security Profiles specify the cryptographic techniques to be used for each Secure DICOM File in a Secure Media Storage Application Profile.**

ITEM 11.2 ADD THE FOLLOWING REFERENCES TO SECTION 2

ISO 7498-2, Information processing systems - Open Systems Interconnection - Basic reference Model - Part 2: Security Architecture

RFC-2630, Cryptographic Message Syntax, June 1999

ITEM 11.3 ADD THE FOLLOWING TEXT TO SECTION 3.1

3.1 Reference Model Definitions

This Part of the Standard makes use of the following terms defined in ISO 7498-2:

a. Data Confidentiality

Note: The definition is “the property that information is not made available or disclosed to unauthorized individuals, entities or processes.”

b. Data Origin Authentication

Note: The definition is “the corroboration that the source of data received is as claimed.”

c. Data Integrity

Note: The definition is “the property that data has not been altered or destroyed in an unauthorized manner.”

d. Key Management

Note: The definition is “the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.”

ITEM 11.4 AMEND THE FOLLOWING TEXT IN SECTION 3.7

3.7 DICOM media storage and file format definitions

This part of the standard makes use of the following terms defined in PS 3.10 of the DICOM Standard:

a) Application Profile

b) DICOM File Format

c) DICOM File Service

d) DICOM File

e) DICOMDIR File

f) File

g) File ID

h) File Meta Information

i) File-set

j) Media Storage Model

k) Secure DICOM File

l) Secure Media Storage Application Profile

ITEM 11.5 AMEND THE FOLLOWING TEXT IN SECTION 6

A DICOM Application Profile specifies:

a. which SOP Classes and options must be supported, including any required extensions, specializations, or privatizations

b. for each SOP Class, which Transfer Syntaxes may be used

c. what information should be included in the Basic Directory IOD

d. which Media Storage Service Class options may be utilized

e. which roles an application may take: File-set Creator, File-set Reader, and/or File-set Updater

f. which physical media and corresponding media formats must be supported

g. whether or not the DICOM Files in the File-set shall be Secure DICOM Files

h. which Media Storage Security Profile must be used for the creation of Secure DICOM Files

ITEM 11.6 AMEND FIGURE 6-1 IN SECTION 6

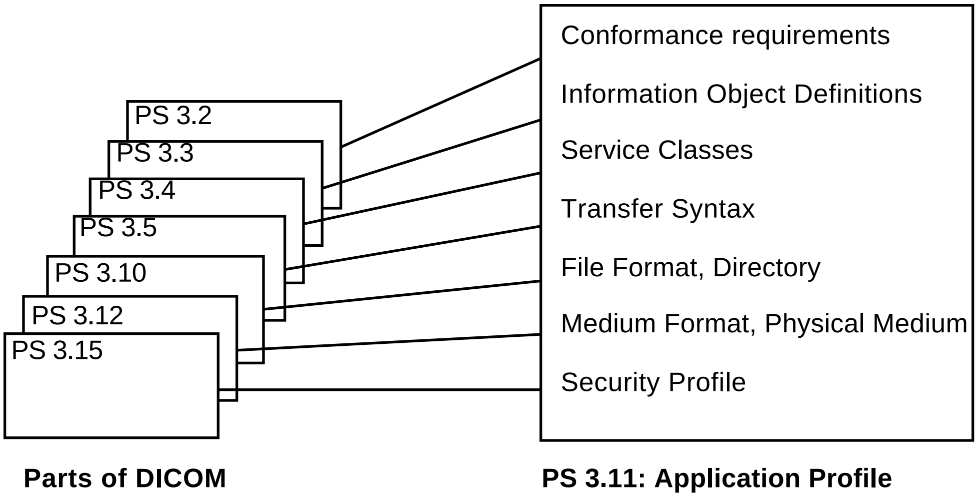

Figure 6-1
RELATIONSHIP BETWEEN AN APPLICATION PROFILE AND PARTS OF DICOM

ITEM 11.7 AMEND THE FOLLOWING TEXT IN SECTION 6

An Application Profile is organized into the following major parts:

a. The name of the Application Profile, or the list of Application Profiles grouped in a related class

b. A description of the clinical context of the Application Profile

c. The definition of the Media Storage Service Class with the device Roles for the Application Profile and associated options

d. Informative section describing the operational requirements of the Application Profile

e. Specification of the SOP Classes and associated IODs supported and the Transfer Syntaxes to be used

f. The selection of Media Format and Physical Media to be used

g. If the Directory Information Module is used, the description of the minimum subset of the Information Model required

h. Other parameters which need to be specified to ensure interoperable media interchange

i. Security parameters which select the cryptographic techniques to be used with Secure Media Storage Application Profiles

ITEM 11.8 ADD THE FOLLOWING TEXT IN SECTION 8

SECURITY Parameters - Section X.3.5

Section X.3.5 is optional; if absent, the Application Profile is unsecure and the Secure DICOM File Format shall not be used for any DICOM File in the File-set.

If present, this section defines the Media Storage Security Profile to be used for encapsulating *all* DICOM Files in the File-set, including the DICOM Directory. If this section is present, the Application Profile is called *Secure Media Storage Application Profile*.

ITEM 11.9 AMEND THE FOLLOWING TEXT IN ANNEX D, SECTION D.1

D.1 Profile Identification

This Annex defines an Application Profile Class potentially inclusive of all defined Media Storage SOP Classes. This class is intended to be used for the interchange of Composite SOP Instances via CD-R and DVD-RAM media for general purpose applications. Objects from multiple modalities may be included on the same media.

A detailed list of the Media Storage SOP Classes that may be supported is defined in PS 3.4.

Table D.1-1 STD-GEN Profiles

Application Profile	**Identifier**	**Description**
General Purpose CD-R Interchange	STD-GEN-CD	Handles interchange of Composite SOP Instances such as Images, Structured Reports, Presentation States and Waveforms.
General Purpose Interchange on DVD-RAM Media	STD-GEN-DVD-RAM	Handles interchange of Composite SOP Instances such as Images, Structured Reports, Presentation States and Waveforms.
General Purpose Secure CD-R Interchange	**STD-GEN-SEC-CD**	**Handles interchange of Composite SOP Instances such as Images, Structured Reports, Presentation States and Waveforms. Offers confidentiality, integrity and, depending on the File-set creator's choice, data origin authentication.**
General Purpose Secure Interchange on DVD-RAM Media	**STD-GEN-SEC-DVD-RAM**	**Handles interchange of Composite SOP Instances such as Images, Structured Reports, Presentation States and Waveforms. Offers confidentiality, integrity and, depending on the File-set creator's choice, data origin authentication.**

The identifier for this General Purpose Image Exchange profile class shall be STD-GEN.

Equipment claiming conformance to this Application Profile shall list the subset of Media Storage SOP Classes that it supports in its Conformance Statement.

Note: Since it is not required to support all Media Storage Classes the user should carefully consider the subset of supported Media Storage SOP Classes in the Conformance Statements of such equipment to establish effective object interchange.

ITEM 11.10 AMEND THE FOLLOWING TEXT IN ANNEX D, SECTION D.3.2

D.3.2 Physical Medium And Medium Format

The STD-GEN-CD **and STD-GEN-SEC-CD** application profiles require~~s~~ the 120 mm CD-R physical medium with the ISO/IEC 9660 Media Format, as defined in PS3.12.

The STD-GEN-DVD-RAM **and STD-GEN-SEC-DVD-RAM** application profile**s** require~~s~~ the 120 mm DVD-RAM medium, as defined in PS 3.12.

ITEM 11.11 ADD THE FOLLOWING SUBSECTIONS IN ANNEX D, SECTION D.3

D.3.4 Other Parameters

Not applicable.

D.3.5 Security Parameters

The STD-GEN-SEC-CD and STD-GEN-SEC-DVD-RAM application profiles require that all DICOM Files in the File-set including the DICOMDIR be Secure DICOM Files encapsulated in accordance with the requirements of the Basic DICOM Media Security Profile as defined in PS 3.15.

Note: These Application Profiles do not place any consistency restrictions on the use of the Basic DICOM Media Security Profile with different DICOM Files of one File-set. For example, readers should not assume that all Files in the File-set can be decoded by the same set of recipients. Readers should also not assume that all secure Files use the same approach (hash key or digital signature) to ensure Integrity or carry the same originators’ signatures.

3 ADDITIONS TO PS 3.15

ITEM 15.1 ADD THE FOLLOWING REFERENCES TO SECTION 2

RFC-2313	**PKCS #1: RSA Encryption, Version 1.5, March 1998.**
RFC-2630	**Cryptographic Message Syntax, June 1999**
ANSI X9.52	**American National Standards Institute. ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation. 1998.**
SHA-1	**National Institute of Standards and Technology, FIPS Pub 180-1: Secure Hash Standard, 17 April 1995**

ITEM 15.2 ADD THE FOLLOWING NEW SUBSECTION TO SECTION 6

6.4 MEDIA STORAGE SECURITY PROFILES

An implementation may claim conformance to one or more Media Storage Application Profiles which in turn require conformance to one or more Media Storage Security Profiles.

Note: An implementation may not claim conformance to a Media Storage Security Profile without claiming conformance to a Media Storage Application Profile.

A Media Storage Security Profile includes the following specifications:

a. What aspects of security are addressed by the profile.
b. The restrictions on the types of DICOM Files that can be secured, if any.
c. How the DICOM Files will be encapsulated and secured.

Media Storage Security Profiles are specified in Annex D.

ITEM 15.3 ADD THE FOLLOWING NEW ANNEX TO PS 3.15 SECURITY PROFILES

ANNEX D– MEDIA STORAGE SECURITY PROFILES (NORMATIVE)

D.1 Basic DICOM MEDIA SECURITY Profile

The Basic DICOM Media Security Profile allows encapsulation of a DICOM File into a Secure DICOM File such that the following aspects of security are addressed:

- confidentiality,
- integrity,
- data origin authentication (optional).

This profile specifies the use of Triple-DES for content encryption and RSA for the key transport of Triple-DES content-encryption keys. The encrypted content is a DICOM File which can either

- be signed with one or more digital signatures, using SHA-1 as the digest algorithm and RSA as the signature algorithm, or
- be digested with SHA-1 as digest algorithm, without application of digital signatures.

D.1.1 Encapsulation of a DICOM File in a Secure DICOM File

A Secure DICOM File conforming to this security profile shall contain an Enveloped-data content type of the Cryptographic Message Syntax defined in RFC 2630. The enveloped data shall use RSA [RFC 2313] for the key transport of Triple-DES content-encryption keys. The Triple-DES key length is 168 bits as defined by ANSI X9.52. Encoding shall be performed according to the specifications for RSA Key Transport in RFC-2630.

The encrypted content of the Enveloped-data content type shall be of the following choices:

- Signed-data content type;
- Digested-data content type.

In both cases, SHA-1 [SHA-1] shall be used as the digest algorithm. In case of the Signed-data content type, RSA [RFC 2313] shall be used as the signature algorithm.

Notes: 1. RSA key transport of Triple-DES content-encryption keys is specified as a requirement in the European Prestandard ENV 13608-2: Health Informatics - Security for healthcare communication – Part 2: Secure data objects.

2. No requirements on the size of the asymmetric key pairs used for RSA key transport are defined in this profile.

3. No requirements or restrictions on the use of the SignedAttributes element of the Signed-data content type's SignerInfo structure are defined in this profile. SignedAttributes might for example be used to specify the signing time or SMIME capabilities, as required by ENV 13608-2.