DICOM Correction Item

Correction Number	CP-421
Log Summary: Add AES to DICOM Secure Media and Attribute Encryption	
Type of Modification Addition	Name of Standard PS 3.15 2003
Rationale for Correction The Rijndael encryption system has been approved by the US government as a US replacement for the DES standard. CP-338 incorporated this replacement, known as AES, into a secure communications profile for TLS. AES has now been incorporated into the CMS standard by means of RFC- 3369, 3370, 3394, and 3565. Since CMS serves as the basis for DICOM Media Security and Attribute Level Confidentiality, these new RFCs allow us to bring AES into both of those domains, bringing them to parity with secure communications channels. The rationale for changing to AES is similar to that outlined in CP-338. RFC-3565 also includes references to RFC-3447, which replaces RFC-2437, and to RFC-3560, which adds protections based on RFC-3447 against the “million message attack”. All of these documents still incorporate the mechanisms defined in the predecessor documents, giving some level of backwards compatibility. However, they also add new mechanisms to improve resistance to attack and enhancements to algorithms, which may not be compatible with older implementations. In other words, writers need not change, but readers should be adapted to handle the new mechanisms.	
Sections of documents affected PS 3.15: Section 2, Section 4, Annex D, Annex E.1.1, Annex E.1.2	
Correction Wording:	

Change the RFC reference in Section 2, and add the additional references shown

RFC **~~2437~~3447**	PKCS #1 RSA Cryptography Specifications Version 2.**~~0~~1, February 2003**
RFC-**~~2630~~3369**	Cryptographic Message Syntax, **~~June 1999~~August 2002**
RFC-3370	**Cryptographic Message Syntax (CMS) Algorithms, August 2002**
RFC-3565	**Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS), July 2003**

Add the following abbreviation in Section 4

AES	**Advanced Encryption Standard**

*Make the indicated **~~deletions~~** and **insertions** in Annex D*

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 **either AES or** Triple-DES for content encryption and RSA for the key transport of **~~Triple-DES~~the** 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**s ~~2630~~3369, 3370, and 3565**. The enveloped data shall use RSA [RFC **~~2313~~3447**] for the key transport of **~~Triple-DES~~ the** content-encryption keys. **Creators of a Secure DICOM File conforming to this security profile may use either AES or Triple-DES for content-encryption. Readers claiming conformance to this profile shall be capable of decrypting Secure DICOM Files using either AES or Triple-DES. The AES key length may be any length allowed by the RFCs.** 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 **and Triple DES Content Encryption** in RFC-**~~2630~~3370, and for AES Content Encryption in RFC-3565**.

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**~~ **the** 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.

*Make the indicated **~~deletions~~** and **insertions** in item 4 of Annex E.1.1 De-identifier*

4. All instances of the Encrypted Attributes Data Set shall be encoded with a DICOM Transfer Syntax, encrypted , and stored in the dataset to be protected as an Item of the Encrypted Attributes Sequence (0400,0500). The encryption shall be done using RSA [RFC 2313] for the key transport of ~~**Triple-DES**~~ **the** content-encryption keys. **A de-identifier conforming to this security profile may use either AES or Triple-DES for content-encryption. The AES key length may be any length allowed by the RFCs.** 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 **and Triple DES Content Encryption** in RFC-~~**2630**~~**3370, and for AES Content Encryption in RFC-3565**.

   Notes: 1. Each item of the Encrypted Attributes Sequence (0400,0500) consists of two Attributes, Encrypted Content Transfer Syntax UID (0400,0510) containing the UID of the Transfer Syntax that was used to encode the instance of the Encrypted Attributes Data Set, and Encrypted Content (0400,0520) containing the block of data resulting from the encryption of the Encrypted Attributes Data Set instance.

   2. RSA key transport of ~~**Triple-DES**~~ **the** 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.

*Make the indicated **~~deletions~~** and **insertions** in Item 1 of Annex E.1.2 Re-identifier*

1. The application shall decrypt, using its recipient key, one instance of the Encrypted Content (0400,0520) Attribute within the Encrypted Attributes Sequence (0400,0500) and decode the resulting block of bytes into a DICOM dataset using the Transfer Syntax specified in the Encrypted Content Transfer Syntax UID (0400,0510). **Re-identifiers claiming conformance to this profile shall be capable of decrypting the Encrypted Content using either AES or Triple-DES in all possible key lengths specified in this profile.**

   Note: If the application is able to decode more than one instance of the Encrypted Content (0400,0520) Attribute within the Encrypted Attributes Sequence (0400,0500), it is at the discretion of the application to choose any one of them.