DICOM Correction Item

Correction Number	CP-895
Log Summary: Password based encryption for media security	
Type of Modification Clarification	Name of Standard PS 3.15 2008
Rationale for Correction The current profile for providing file security on DICOM media uses CMS to encode files encrypted with certificate-based keys, which presupposes a priori knowledge of all recipients and a public key infrastructure. In practice this has proved to difficult to deploy. There is a user demand for a simpler, albeit potentially less secure, scheme, in which a password is used to encrypt and recover the content; such a password can be distributed separately from the media but to any number of recipients as appropriate. The IETF CMS S/MIME infra-structure provides for the use of such “password-based encryption”, originally specified in RFC 3211 “Password-based Encryption for CMS” and now referenced by RFC 3852, and support for this is added to the existing Basic DICOM Media Security Profile in PS 3.15, which in turn is inherited by the existing secure media application profiles. This profile was previously extended in CP 421 to add AES to the required list of content enryption mechanisms. Also, update the references for CMS to RFC 3852, which renders obsolete RFC 3369, which in turn made obsolete RFCs 2630 and references 3211.	
Sections of documents affected PS 3.15 2, D.1	
Correction Wording:	

Amend PS 3.15 Section 2 Normative References:

RFC 2849 The LDAP Data Interchange Format (LDIF)

RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000

RFC 3211 Password-based Encryption for CMS, December 2001

RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002.

RFC 3447 PKCS #1 RSA Cryptography Specifications Version 2.1, February 2003

Note: The RSA Encryption Standard is also defined in informative annex A of ISO/IEC 9796, and in Normative Annex A of the CEN/TC251 European Prestandard prENV 12388:1996.

RFC ~~3369~~3852 Cryptographic Message Syntax, ~~August 2002~~ July 2004

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

Amend PS 3.15 D.1:

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**, or password-based encryption and AES or Triple-DES,** for the key transport of the content-encryption keys. The encrypted content is a DICOM File that 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 ~~3369~~3852, 3370 and 3565. The enveloped data shall use RSA [RFC 3447]**, or password-based encryption using PBKDF2 [RFC 2898] for the key derivation algorithm and either AES or Triple-DES [RFC 3211],** for the key transport of 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-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.

In the case of password-based encryption using PBKDF2, the octet string that contains the password used to generate the key shall be limited to the encoding and the graphic character representation defined by the Default Character Repertoire.

Notes: 1. RSA key transport of 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.

4. The use of password-based encryption for key transport of content encryption keys is potentially less secure than certificate-based encryption, but may be useful when the list of recipients is not known a priori or when there is no public key infrastructure deployed. The security depends on the entropy of the password, which if user-selected can be quite low. RFC 3211 strongly recommends the use of a pass "phrase" rather than a single word, and RFC 2898 does not impose any practical length limit. Also, the method used to exchange the password or pass phrase also could have a significant impact on the level of security.

5. PBKDF2 as defined in RFC 2898 specifies the password to be "an octet string of arbitrary length whose interpretation as a text string is unspecified". For interoperability between the sender and recipient, both a character encoding scheme and a graphic character representation needs to be defined. ISO IR6 (US-ASCII), being the Default Character Repertoire for DICOM (see PS 3.5), is specified in order to avoid any potential ambiguity caused by the use of other character sets (such as UTF-8) that do not necessarily result in the same binary values for particular graphic character representation.

The graphic character representation of certain symbols in ISO IR6 is explicitly defined, even though the same binary representation may have a different graphic character representation in other 7-bit schemes. For example, in the version of ISO 646 used in Japan (ISO-IR 14 Romaji), 05/12 is represented as "¥" rather than backslash "\". It is the responsibility of the application to assure that the input method and display of such symbols to the user is mapped to the correct encoding, regardless of locale. I.e., if the password is "123\$", then it should be encoded as 03/01 03/02 03/03 05/12 02/04, regardless of whether the user types the backslash "\"(U+005C) on a Japanese or US keyboard; they should not be expected to type the "¥" (U+00A5) key on a Japanese keyboard, nor should 05/12 be displayed as "¥" if the password is displayed as text.

The restriction to the ISO IR 6 encoding and graphic character representation (rather than, for example, the minimal encoding of UTF-8) also eliminates the ambiguity introduced by homographs (characters that look the same but encode differently), and alternative encodings with the same meaning, such as the single German character "ß" (U+00DF) as opposed to the two-character "ss" (U+0073 U+0073), and the use of phonetic as opposed to ideographic representation of the same meaning, such as Japanese hiragana "ぞう" (U+305E U+3046) versus kanji "像" (U+50CF).

It is the responsibility of the application to prevent the user from creating passwords using characters that cannot be represented; e.g., on a Western European keyboard, the user should not be permitted to enter an accented character such as "é" (U+00E9) or "ö" (U+00F6), since there is no defined mapping of such characters to IS IR 6 characters (such as "e" or "o").