DICOM Correction Item

Correction Number	CP-1059
Log Summary: Add SHA2 hash algorithms for digital signatures	
Type of Modification Addition	Name of Standard PS 3.3, 3.15 2009
Rationale for Correction The SHA2 family of hash algorithms (SHA256, SHA384, SHA512) have been requested for use with RSA digital signatures. Impact on Basic DICOM Media Security Profile: There are two approaches that can be taken. Either introduce a compatibility problem for the Basic DICOM Media Security Profile, or define a new profile. The new profile could be called the "Basic DICOM Media Security Profile – SHA2". The changes below show how we could modify the current profile. It adds the requirement for SHA256, SHA384, SHA512 support to the basic problem. This would invalidate existing readers of media. To make a new profile, a section D.2 Basic DICOM Media Security Profile – SHA2 would be added that copies all of D.1, with the additions shown below.	
Sections of documents affected PS 3.3 C.12.1.1.3, C.17.2.1 PS 3.15 C.1, C.4	
Correction Wording:	

Amend PS 3.3 C.12.1.1.3:

C.12.1.1.3 Digital Signatures Macro

This Macro allows Digital Signatures to be included in a DICOM Data Set for the purpose of insuring the integrity of the Data Set, and to authenticate the sources of the Data Set. Table C.12-6 defines the Attributes needed to embed a Digital Signature in a Data Set. This Macro may appear in individual sequence items as well as in the main Data Set of the SOP Instance.

Notes: 1. Each Item of a Sequence of Items is a Data Set. Thus, individual Sequence items may incorporate their own Digital Signatures in addition to any Digital Signatures added to the Data Set in which the Sequence appears.

2. The inclusion of this Macro in Sequence Items, other than as specified in this Part of the Standard, may be specified in an application-defined Standard Extended SOP Class or Private SOP Class (see PS3.2).

Table C.12-6
DIGITAL SIGNATURES MACRO ATTRIBUTES

Attribute Name	Tag	Type	Attribute Description
MAC Parameters Sequence	(4FFE,0001)	3	A sequence of one or more items that describe the parameters used to calculate a MAC for use in Digital Signatures.

…	…	…	…
>MAC Algorithm	(0400,0015)	1	The algorithm used in generating the MAC to be encrypted to form the Digital Signature. Defined Terms: RIPEMD160 MD5 SHA1 **SHA256** **SHA384** **SHA512** Note: Digital Signature Security Profiles (see PS 3.15) may require the use of a restricted subset of these terms.
…	…	…	…

Amend PS 3.3 C.17.2.1:

C.17.2.1 Hierarchical SOP Instance Reference Macro

…

Table C.17-3a
HIERARCHICAL SERIES REFERENCE MACRO ATTRIBUTES

…	…	…	…
Referenced SOP Sequence	(0008,1199)	1	References to Composite Object SOP Class/SOP Instance pairs that are part of the Study defined by Study Instance UID and the Series defined by Series Instance UID (0020,000E). One or more Items may be included in this sequence
…	…	…	…
>Referenced SOP Instance MAC Sequence	(0400,0403)	3	A MAC Calculation from data in the referenced SOP Instance that can be used as a data integrity check. Only a single Item shall be permitted in this Sequence. Note: This Attribute may be used in place of the Referenced Digital Signature Sequence Attribute (0400,0402), particularly if the SOP Instance does not have appropriate Digital Signatures that can be referenced.
…	…	…	…

>>MAC Algorithm	(0400,0015)	1	The algorithm used in generating the MAC. Defined Terms: RIPEMD160 MD5 SHA1 **SHA256** **SHA384** **SHA512** Note: Digital Signature Security Profiles (see PS 3.15) may require the use of a restricted subset of these terms.
…	…	…	…

Add to PS 3.15 Section 2 Normative References:

SHA-1 National Institute of Standards and Technology, FIPS Pub 180-1: Secure Hash Standard, 17 April 1995

SHA-2 National Institute of Standards and Technology, FIPS Pub 180-2: Secure Hash Standard, 1 August 2002

RFC 3851 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification

Amend PS 3.15 Digital Signature Profiles:

C.1 BASE RSA DIGITAL SIGNATURE PROFILE

The Base RSA Digital Signature Profile outlines the use of RSA encryption of a MAC to generate a Digital Signature. This Profile does not specify any particular set of Data Elements to sign. Other Digital Signature profiles may refer to this profile, adding specifications of which Data Elements to sign or other customizations.

The creator of a digital signature shall use one of the RIPEMD-160, MD5, ~~**or**~~ SHA-1 **or SHA-2 family (SHA256, SHA384, SHA512) of** hashing functions to generate a MAC, which is then encrypted using a private RSA key. All validators of digital signatures shall be capable of using a MAC generated by any of ~~**three**~~ **the** hashing functions specified (RIPEMD-160, MD5~~**, or**~~ SHA-1 **or SHA256, SHA384, SHA512**).

Note: The use of MD5 is not recommended by its inventors, RSA. See: ftp://ftp.rsasecurity.com/pub/pdfs/bulletn4.pdf

The MAC to be signed shall be padded to a block size matching the RSA key size, as directed in RFC 2437 (PKCS #1). The Value of MAC Algorithm (0400,0015) shall be set to either "RIPEMD160", "MD5", ~~**or**~~ "SHA1"**, "SHA256", "SHA384" or "SHA512"**. The public key associated with the private key as well as the identity of the Application Entity or equipment manufacturer that owns the RSA key pair shall be transmitted in an X.509 (1993) signature certificate. The Value of the Certificate Type (0400,0110) Attribute shall be set to "X509_1993_SIG". A site-specific policy determines how the X.509 certificates are generated, authenticated, and distributed. A site may issue and distribute X.509 certificates directly, may

utilize the services of a Certificate Authority, or use any reasonable method for certificate generation and verification.

If an implementation utilizes timestamps, it shall use a Certified Timestamp Type (0400,0305) of "CMS_TSP". The Certified Timestamp (0400,0310) shall be generated as described in "Internet X.509 Public Key Infrastructure; Time Stamp Protocols; March 2000".

…

C.4 STRUCTURED REPORT RSA DIGITAL SIGNATURE PROFILE

This profile defines a mechanism for adding Digital Signatures to Structured Reports or Key Object Selection Documents where there is no more than one Verifying Observer. Instances that follow this Digital Signature Profile shall include at least one Digital Signature at the top level of the Data Set.

…

All occurrences of Referenced SOP Instance MAC Sequence (0400,0403) shall have the Value of MAC Algorithm (0400,0015) set to either "RIPEMD160", "MD5", ~~**or**~~ "SHA1"**, "SHA256", "SHA384" or "SHA512"**.

The Digital Signature shall be created using the methodology described in the Base RSA Digital Signature Profile. The Application Entity shall determine the identity of the signatories and obtain their certificate through an application-specific procedure such as a login mechanism or a smart card. The conformance statement shall specify how the application identifies signatories and obtains certificates.

Note: Structured Report RSA Digital Signatures bear no direct relationship to other Digital Signatures. However, other Digital Signatures, such as the Creator RSA Digital Signature, may be used to corroborate the timestamp of a Structured Report RSA Digital Signature.

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**, SHA256, SHA384, or SHA512** as the digest algorithm and RSA as the signature algorithm, or
- be digested with SHA-1**, SHA256, SHA384, or SHA512** as digest algorithm, without application of digital signatures.

Note: The digest algorithm requirements will evolve as the threats evolve. As the digest requirements have changed, this profile has changed to include addition requirements.

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 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]**, SHA256, SHA384, or SHA512 [SHA-2]** 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”).