DICOM Correction Proposal

<table>
<thead>
<tr>
<th>STATUS</th>
<th>Letter Ballot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Last Update</td>
<td>3/25/2021</td>
</tr>
<tr>
<td>Person Assigned</td>
<td>Rob Horn</td>
</tr>
<tr>
<td>Submitter Name</td>
<td>Rob Horn</td>
</tr>
<tr>
<td>Submission Date</td>
<td>20201112</td>
</tr>
</tbody>
</table>

Correction Number: CP-2092

Log Summary: Update MAC Algorithms

Name of Standard
PS3.15

Rationale for Correction:
The list of MAC algorithms does not include the full list of algorithms approved by NIST. It contains those listed in FIPS-180 but not all of those listed in FIPS-202.

"Base RSA Digital Signature Profile" and "Structured Report RSA Digital Signature Profile" specify MAC algorithm restrictions. The Profiles "Authorization RSA Digital Signature Profile" and "Creator RSA Digital Signature Profile" do not constrain the MAC algorithms. The second two are updated to have the same algorithm list as the first two.

Note: If a Profile is needed to identify support for the SHA-3 algorithms that will be done by a separate work item and supplement.

Add to Part 3, Section 2.3 Internet Engineering Task Force (IETF)


Add to Part 3, Section 2.5 United States National Institute of Standards and Technology (NIST)


Update Part 3, Section C.12

Part 3

Table C.12-6. Digital Signatures Macro Attributes
Update Section C.12.1.3.1.2 Signature

C.12.1.3.1.2 Signature

To generate the MAC, Data Elements referenced either explicitly or implicitly by the Tags in the Data Elements Signed (0400,0020) list shall be encoded using the Transfer Syntax identified by the MAC Calculation Transfer Syntax UID (0400,0010) of the MAC Parameters Sequence (0400,0010) Item where the Data Elements Signed Attribute (0400,0020) appears. Data shall be formed into a byte stream and presented to the MAC Algorithm (0400,0015) for computation of the MAC according to the following rules:

The following bullet items are paragraphs in the current standard. Make them bullet items without changing the contents.

- For all Data Elements except those with a VR of SQ or with a VR of OB with an undefined length, all Data Element fields, including the Tag, the VR, the reserved field (if any), the Value Length, and the Value, shall be placed into the byte stream in the order encountered.

- For Data Elements with a VR of SQ or with a VR of OB with an undefined length, the Tag, the VR, and the reserved field are placed into the byte stream. The Value Length shall not be included. This is followed by each Item Tag in the order encountered, without including the Value Length, followed by the contents of the Value for that Item. In the case of an Item within a Data Element whose VR is SQ, these rules are applied recursively to all of the Data Elements within the Value of that Item. After all the Items have been incorporated into the byte stream, a Sequence Delimitation Item Tag (FFFE,E0DD) shall be added to the byte stream presented to the MAC Algorithm, regardless of whether or not it was originally present.

The MAC Algorithm (0400,0015) may be chosen either from the Defined Terms in Table C.12-6a or another algorithm can be identified.

Table C.12-6a Defined Terms for MAC Algorithm (0400,0015)

<table>
<thead>
<tr>
<th>Defined Term</th>
<th>Reference</th>
</tr>
</thead>
</table>

....

>MAC Algorithm (0400,0015) 1 The algorithm used in generating the MAC to be encrypted to form the Digital Signature. See Table C.12-6a Defined Terms for MAC Algorithm (0400,0015).

Defined Terms
RIPEMD160
MD5
SHA1
SHA256
SHA384
SHA512

Note
Digital Signature Security Profiles (see PS3.15) may require the use of a restricted subset of these terms.
<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Tag</th>
<th>Type</th>
<th>Attribute Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;&gt;MAC</td>
<td>(0400,0015)</td>
<td>1</td>
<td>The algorithm used in generating the MAC to be encrypted to form the Digital Signature.</td>
</tr>
</tbody>
</table>

- Defined Terms
  - RIPEMD160
  - MD5
  - SHA1
  - SHA256
  - SHA384
  - SHA512

- Note
  - Digital Signature Security Profiles (see PS3.15) may require the use of a restricted subset of these terms.
Update Part 15, Annex C.1 Base RSA Digital Signature Profile

The MAC data 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", "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 [ITU-T 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 [ITU-T X.509] certificates are generated, authenticated, and distributed. A site may issue and distribute [ITU-T X.509] certificates directly, may utilize the services of a Certificate Authority, or use any reasonable method for certificate generation and verification.

Update C.2 Creator RSA Digital Signature Profile

The creator of a DICOM SOP Instance may generate signatures using the Creator RSA Digital Signature Profile. The Digital Signature produced by this Profile serves as a lifetime data integrity check that can be used to verify that the pixel data in the SOP instance has not been altered since its initial creation. An implementation that supports the Creator RSA Digital Signature Profile may include a Creator RSA Digital Signature with every SOP Instance that it creates; however, the implementation is not required to do so.

The signature shall use one of the RIPEMD-160, MD5, 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 the hashing functions specified (RIPEMD-160, MD5, SHA-1 or SHA256, SHA384, SHA512).

C.3 AUTHORIZATION RSA DIGITAL SIGNATURE PROFILE

The technician or physician who approves a DICOM SOP Instance for use may request the Application Entity to generate a signature using the Authorization RSA Digital Signature Profile. The Digital Signature produced serves as a lifetime data integrity check that can be used to verify that the pixel data in the SOP instance is the same that the technician or physician saw when they made the approval.

The signature shall use one of the RIPEMD-160, MD5, 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 the hashing functions specified (RIPEMD-160, MD5, SHA-1 or SHA256, SHA384, SHA512).