DICOM Correction Proposal

STATUS	Letter Ballot
Date of Last Update	2024/01/14
Person Assigned	R Horn
Submitter Name	rjhorniii@gmail.com
Submission Date	2023/05/14

Correction Number CP-2308
Log Summary: Clarify Creator Digital Signature Profile
Name of Standard PS3.15
Rationale for Correction: The Creator Digital Signature profile is rather old, but It addresses the problem of tampering with SOP Instances from modalities. A recent review of the profile suggests some notes and clarifications are needed. We could engage in a more thorough IOD by IOD review of these requirements, but I propose we wait until actual use indicates a problem. For example, none of the additional attributes defined as part of modality specific modules for various optical modalities are included in the profile list. The attributes of General Image module and Image Pixel module are included. I do not recall whether this was by conscious design or not. The only one that caught my attention as potentially being a genuine problem is the omission of the Microscope Slide Layer Tile Organization Module from the profile. Maybe that one should be added, but I left it out of this CP.
Correction Wording:

Modify PS3.15 Annex C.2

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).

Note: Local rules and regulations may further restrict the hashing functions that are permitted. These regulations usually restrict the hashing functions that may be used by the SCP in creating a new signature on a new SOP Instance. For example, they may prohibit use of RIPEMD-160 and MD5. The regulations usually allow an SCU to verify an old signature that uses an algorithm that is now prohibited for new signatures. Implementations that support this profile will need to accommodate these local regulations.

As a minimum, an implementation shall include the following Attributes in generating the Creator RSA Digital Signature:

a. the SOP Class and Instance UIDs

…

ad. any Attributes of the Microscopy Bulk Simple Annotations Module that are present

Note: The requirement is upon attributes, and the use of Modules in the list above is for documentation brevity. For example, a SOP instance of an Encapsulated STL IOD will have all of the attributes of the Encapsulated Document module (used to encapsulate the STL file) signed. It will also have the attributes used in any icon images signed, because the icon images use attributes that are also attributes of the General Image Module and Image Pixel Module. The General Image Module and Image Pixel Module are not incorporated the Encapsulated STL IOD and do not appear in the list in PS3.3 Table A.85.1-1 Encapsulated STL IOD Modules.

The Digital Signature shall be created using the methodology described in the Base RSA Digital Signature Profile. Typically, the certificate and associated private key used to produce Creator RSA Digital Signatures are configuration parameters of the Application Entity set by service or installation engineers.

The SCP may include other attributes when generating the Creator RSA Digital Signature, and the SCU shall support verification of such signatures.