Digital Imaging and Communications in Medicine (DICOM)

Supplement XXX: Cryptography Update for Digital Signature and Media Storage Security

Prepared by: Alexander Zhang, Essien Ge, Jeroen Medema, Rob Horn

DICOM Standards Committee, Working Group 14 (Security)

1300 N. 17th Street, Suite 900

Rosslyn, Virginia 22209 USA

Status: Draft Proposal

Developed pursuant to DICOM Work Item 2025-12-A

Table of Contents

Document History

2026/01/19	Version 01	Alexander Zhang, Essien Ge, Jeroen Medema	Initial draft based on WG-14 proposal.
2026/3/10	Version 02	Rob Horn, Essien Ge, Alexander Zhang	Update per WG-14 discussion and format refine.

Open Issues

1.	What strategy will be used to specify profile support for old legacy signatures and products that only support the old legacy signatures. The addition of signature profiles introduces problems with how to describe the support for legacy of decades of old signatures. There are two basic strategies: - The new profiles mandate support for the old legacy signature algorithm verification in the profile that allows the new signatures. Remove the legacy signature algorithms from the list of allowed algorithms for new signatures. This allows a profile to be claimed for a transitional product that will not generate new signatures with the legacy algorithms, but will verify signatures with the legacy algorithms. This is the style chosen by NIST recommendations for transition. They have two tables, one for signing and one for verifying. - The new profiles mandate the support of the new algorithms for signing and verifying. A product claiming only this profile will not be able to verify legacy signatures. Products that can verify legacy signatures can add this information in their conformance claim. These products could also claim support for both the old Basic signatures and the new signature profiles. Those products could continue to sign with the legacy algorithms. This might be needed to accommodate transitional configurations and archives. This supplement proposes the second strategy. Another possibility is, with the second strategy, can we allow an implementation to be compliant to the digital signature profile as signer or as verifier separately? Like SCU and SCP. In this way the benefit of the 1st strategy is combined. Currently PS3.2 this is not clearly supporting this. The strategy choice also impacts the anticipated requirements for PQ signature algorithms. The algorithm analysis and recommendations are in process within the research community.

Closed Issues

1.	

Scope and Field of Application

This Supplement introduces cryptographic update to DICOM Digital Signatures and Secure Media Storage by adding support for modern algorithms while maintaining backward compatibility.

In recent years, regulations concerning security and privacy have become increasingly prominent across countries and regions (e.g., EU GDPR, US FDA Cybersecurity Guidance, China Data Security Law, Personal Information Protection Law, and Cryptography Law). These require strengthened confidentiality, integrity, and authenticity of medical data.

The current Digital Signature Profiles (PS3.15 Section 6.3 and Annex C) and Media Storage Security Profiles (PS3.15 Section 6.4 and Annex D) were drafted many years ago. Some of the legacy cryptography technologies are still being used, e.g. 3DES and SHA-1, meanwhile, it lacks support of the newer cryptography algorithm e.g. ECDSA/EdDSA for digital signature, up-to-date cryptography technologies such as authenticated encryption (e.g. AES-CCM/GCM), and newer key management technologies such as KEM. Certificate format used is still X.509_1993(X.509 V2) which is no longer supported in most CA, systems and libraries, X.509 V3 is now widely used now.

The content in this supplement includes:

- Add 4 new RSA based Digital Signature Profiles by deprecating legacy algorithms such as SHA-1 and add newer algorithms such as SHA-3 family and upgrade certificate to X.509 V3.
- Add 4 new Digital Signature Profiles which are based on Elliptic Curve algorithms.
- Add one new Media Storage Security Profile, which supersedes the current mechanism in Basic Media Storage Security Profile, but use up-to-date algorithms, and add support of more key management technologies including Key Agreement (e.g., ECDH) and Key Encapsulation Mechanisms (KEM).
- Add one new Media Storage Security Profile using CMS Authenticated-Enveloped-Data with Authenticated Encryption (e.g., AES-GCM, AES-CCM).

Backward compatibility is maintained: legacy algorithms remain supported for verification/decryption.

This Supplement affects PS3.2, PS3.3, PS3.6, PS3.10, PS3.11 and PS3.15.

PS 3.2

Update PS3.2 N.8.4.3 Media Storage Security Profiles as follows:

N.8.4.3 Media Storage Security Profiles

[List here any Media Storage Security Profile your product may support. Mark this section as N/A if your product does not support any Media Storage Security profile.]

See Section N.1.4 Media Services for information on supported Secure Media Storage Application Profiles and secured media.

Table N.8-4 details the encryption mechanisms that are supported with secure media.

[In Table N.8-4, all the Profiles not supported can be deleted. But it is also permitted to keep them for transparency reasons and mark them with "N". **If multiple media security profiles are supported for the implementation, the mapping between the security profile and the encryption algorithm each one supports is indicated in the column “Media storage security profile applicable” for each algorithm]**

Table N.8-4. Content Encryption used for Secured Media

Encryption	File Set Creator/File Set Updater	File Set Reader	Media storage security profile applicable
AES			
Triple-DES			
[Other encryption]			

[In case of using Basic Media Storage Security Profile or Basic Media Storage Security Profile 2025, the Table N.8-5 shall be included here to disclose the content type used. In Table N.8-5, all the Profiles not supported can be deleted. But it is also permitted to keep them for transparency reasons and mark them with "N".**If multiple media security profiles are supported for the implementation, the mapping between the security profile and the content type each one support is indicated in the column “Media storage security profile applicable” for each algorithm]**

Table N.8-6. Digest Algorithms used for Secured Media

Digest Algorithms	File Set Creator/File Set Updater	File Set Reader	Media storage security profile applicable
SHA-1			
SHA256			
SHA384			
SHA512			
SHA3-256			
SHA3-384			
SHA3-512			
[Other digest algorithm]			

PS 3.3

Update PS3.3 2.5 United States National Institute of Standards and Technology (NIST)

2.5 United States National Institute of Standards and Technology (NIST)

[FIPS PUB 46] NIST. . Data Encryption Standard (DES). Withdrawn . http://csrc.nist.gov/publications/fips/archive/fips46-3/fips46-3.pdf .

[FIPS PUB 81] NIST. . DES Modes of Operation. Withdrawn .

[FIPS PUB 180-4] NIST. August 2015. Secure Hash Standard (SHS). http://doi.org/10.6028/NIST.FIPS.180-4 .

[FIPS PUB 202] NIST. August 2015. SHA-3 Standard. http://doi.org/10.6028/NIST.FIPS.202 .

[NIST 800-131A] NIST. March 2019. NIST SP 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths. https://doi.org/10.6028/NIST.SP.800-131Ar2

[NIST 800-57] NIST. May 2020. NIST SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 – General. https://doi.org/10.6028/NIST.SP.800-57pt1r5

Update PS3.3 C.12.1.1.3 Digital Signatures Macro

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 top level 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).

The attribute definitions in the table below are being changed in CP2596. What do we want to show here? Old version, a guess, nothing yet?

Table C.12-6. Digital Signatures Macro Attributes

Attribute Name	Tag	Type	Attribute Description
MAC Parameters Sequence	(4FFE,0001)	3	A Sequence of Items that describe the parameters used to calculate a MAC for use in Digital Signatures. One or more Items shall be included in this Sequence.

>MAC ID Number	(0400,0005)	1	A number, unique within this SOP Instance, used to identify this MAC Parameters Sequence (4FFE,0001) Item from an Item of the Digital Signatures Sequence (FFFA,FFFA).
>MAC Calculation Transfer Syntax UID	(0400,0010)	1	The Transfer Syntax UID used to encode the values of the Data Elements included in the MAC calculation. Only Transfer Syntaxes that explicitly include the VR and use Little Endian encoding shall be used. Note Certain Transfer Syntaxes, particularly those that are used with compressed data, allow the fragmentation of the pixel data to change. If such fragmentation changes, Digital Signatures generated with such Transfer Syntaxes could become invalid.
>MAC Algorithm	(0400,0015)	1	The algorithm used in generating the MAC to be encrypted to form the Digital Signature. For Defined Terms, see Table C.12.1.1.3.1.2-1, "Defined Terms for MAC Algorithm (0400,0015)".
>Data Elements Signed	(0400,0020)	1	A list of Data Element Tags in the order they appear in the Data Set that identify the Data Elements used in creating the MAC for the Digital Signature. See Section C.12.1.1.3.1.1.
Digital Signatures Sequence	(FFFA,FFFA)	3	Sequence holding Digital Signatures. One or more Items are permitted in this Sequence.
>MAC ID Number	(0400,0005)	1	A number used to identify which MAC Parameters Sequence Item was used in the calculation of this Digital Signature.
>Digital Signature UID	(0400,0100)	1	A UID that can be used to uniquely reference this signature.
>Digital Signature DateTime	(0400,0105)	1	The date and time the Digital Signature was created. The time shall include an offset (i.e., time zone indication) from Coordinated Universal Time. Note This is not a certified timestamp, and hence is not completely verifiable. An application can compare this date and time with those of other signatures and the validity date of the certificate to gain confidence in the veracity of this date and time.
>Certificate Type	(0400,0110)	1	The type of certificate used in (0400,0115). Defined Terms: X509_1993_SIG **X509_V3** Note Digital Signature Security Profiles (see PS3.15) may require the use of a restricted subset of these terms.
>Certificate of Signer	(0400,0115)	1	A certificate that holds the identity of the entity producing this Digital Signature, that entity's public key or key identifier, and the algorithm and associated parameters with which that public key is to be used. Algorithms allowed are specified in Digital Signature Security Profiles (see PS3.15).

			Note As technology advances, additional encryption algorithms may be allowed in future releases. Implementations should take this possibility into account. When symmetric encryption is used, the certificate merely identifies which key was used by which entity, but not the actual key itself. Some other means (e.g., a trusted third party) must be used to obtain the key.
>Signature	(0400,0120)	1	The MAC generated as described in Section C.12.1.1.3.1.1 and encrypted using the algorithm, parameters, and private key associated with the Certificate of the Signer (0400,0115). See Section C.12.1.1.3.1.2.
>Digital Signature Algorithm	**(xxxx, yyyy)**	3	**The algorithm used to generate the Digital Signature. If this element is absent, this means that the used algorithm is RSA.** **Defined Terms:** **RSA** **ECDSA** **EdDSA**
>Elliptic Curve	**(xxxx, zzzz)**	**1C**	**The curve used in generating the digital signature.** **Defined Terms:** **NIST Curve P-256** **NIST Curve P-384** **NIST Curve P-521** **Ed25519** **Ed448** **Shall be present when the Digital Signature Algorithm (xxxx,yyyy) is ECDSA or EdDSA.**
>Certified Timestamp Type	(0400,0305)	1C	The type of certified timestamp used in Certified Timestamp (0400,0310). Required if Certified Timestamp (0400,0310) is present. Defined Terms: CMS_TSP Internet X.509 Public Key Infrastructure Time Stamp Protocol Note Digital Signature Security Profiles (see PS3.15) may require the use of a restricted subset of these terms.
>Certified Timestamp	(0400,0310)	3	A certified timestamp of the Digital Signature (0400,0120) Value, which shall be obtained when the Digital Signature is created. See Section C.12.1.1.3.1.3.
>Digital Signature Purpose Code Sequence	(0400,0401)	3	The purpose of this Digital Signature. Only a single Item is permitted in this Sequence.
>>Include Table 8.8-1 "Code Sequence Macro Attributes"			BCID 7007 "Signature Purpose".

Kommentiert [JM1]: It is my guess this is a new value. New values will be decided on by WG-06, so enter (xxxx,yyyy) as a placeholder for this one, and (xxxx,zzzz) for the next one. References can be done by using the placeholder value, see at Elliptic Curve.

Kommentiert [AZ2]: Is there any concern in adding these two macros?

Kommentiert [EG2R2]: In X509 certificate there can also be relevant information embeded, however we think it may be much easier for signature verifier to use if we put the directly here.

CP2596 makes changes to PS3.3 C.12.1.1.3.1.2 Signature makes changes that are needed

PS 3.6

Update PS3.6 6 Registry of DICOM Data Elements

6 Registry of DICOM Data Elements

Tag	Name	Keyword	VR	VM	
(0400,0005)	MAC ID Number	MACIDNumber	US	1	
(0400,0010)	MAC Calculation Transfer Syntax UID	MACCalculationTransferSyntaxUID	UI	1	
(0400,0015)	MAC Algorithm	MACAlgorithm	CS	1	
(0400,0020)	Data Elements Signed	DataElementsSigned	AT	1-n	
(0400,0100)	Digital Signature UID	DigitalSignatureUID	UI	1	
(0400,0105)	Digital Signature DateTime	DigitalSignatureDateTime	DT	1	
(xxxx,yyyy)	**Digital Signature Algorithm**	**Digital Signature Algorithm**	**CS**	**1**	
(xxxx,zzzz)	**Elliptic Curve**	**Elliptic Curve**	**CS**	**1**	

PS 3.10

Update 7.4 Secure DICOM File Format as follows:

7.4 Secure DICOM File Format

A Secure DICOM File shall contain a single DICOM File encapsulated with the Cryptographic Message Syntax as defined in IETF STD 70 [RFC5652] **and [RFC 5083**]. Depending on the cryptographic algorithms used for encapsulation, a Secure DICOM File can provide one or more the following security properties:

- Data Confidentiality (by means of encryption)
- Data Origin Authentication (by means of certificates and digital signatures)
- Data Integrity (by means of digital signatures **or authenticated encryption**)

In addition, a Secure DICOM File offers the possibility to communicate encryption keys and certificates to the intended recipients by means of key transport, key agreement, ~~or~~ **preshared** symmetric key-encryption key ~~schemes~~, **password-based key derivation, or key encapsulation mechanism**.

PS 3.11

Update D.3.5 Security Parameters

D.3.5 Security Parameters

The STD-GEN-SEC-CD, STD-GEN-SEC-DVD-RAM and STD-GEN-SEC-BD Media Storage Application Profiles require that **the implementation support at least one of DICOM Meidia Storage Security Profiles defined in Annex D of PS3.15**, and the all DICOM Files in the File-set including the DICOMDIR be Secure DICOM Files encapsulated in accordance with the requirements of the ~~**Basic**~~ DICOM Media **Storage** Security ~~**Profile**~~ **Profiles** it supports ~~**as defined in PS3.15**~~.

Note These Media Storage Application Profiles do not place any consistency restrictions on the use of the Basic DICOM Media Security Profile with different DICOM Files of one File-set. For example, readers should not assume that all Files in the File-set can be decoded by the same set of recipients. Readers should also not assume that all secure Files use the same approach (hash key or digital signature) to ensure Integrity or carry the same originators' signatures.

Update H.3.5 Security Parameters

H.3.5 Security Parameters

The STD-GEN-SEC-DVD Media Storage Application Profiles require that the implementation support **at least one of DICOM Meidia Storage Security Profiles defined in Annex D of PS3.15, and** all DICOM Files in the File-set including the DICOMDIR be Secure DICOM Files encapsulated in accordance with the requirements of the ~~**Basic**~~ DICOM Media **Storage** Security ~~**Profile**~~ **Profiles** it ~~**supports as defined in PS3.15**~~.

Note These Media Storage Application Profiles do not place any consistency restrictions on the use of the Basic DICOM Media Security Profile with different DICOM Files of one File-set. For example, readers should not assume that all Files in the File-set can be decoded by the same set of recipients. Readers should also not assume that all secure Files use the same approach (hash key or digital signature) to ensure Integrity or carry the same originators' signatures.

PS 3.15

Add 4 new RSA-based Digital Signature Profiles, while update the cryptography algorithm used.

C.X1 Base RSA Digital Signature Profile 2026

The Base RSA Digital Signature Profile 2026 outlines the use of RSA to generate a Digital Signature by signing a Message Digest. 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 SHA256, SHA384, SHA512, SHA3-256, SHA3-384, or SHA3-512 hashing functions to generate a Message Digest, which is then signed using a private RSA key. All validators of digital signatures shall be capable of using a Message Digest generated by any of the hashing functions specified (SHA256, SHA384, SHA512, SHA3-256, SHA3-384, or SHA3-512.

The RSA key pair to sign/verify the signature shall have a modulus length of 3072 bit or above.

The data to be signed shall be padded to a block size matching the RSA key size. The creator shall support one of the digital signature padding schemes defined in [RFC 8017], i.e. RSASSA-PSS or RSASSA-PKCS1-v1_5, and the validator shall support both. The Value of MAC Algorithm (0400,0015) shall be set to either "SHA256", "SHA384”,"SHA512" "SHA3-256", "SHA3-384" or "SHA3-512”. 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] signature certificate. The Value of the Certificate Type (0400,0110) Attribute shall be set to "X509_V3". A site-specific policy determines how the [ITU-T X.509] certificates are generated, authenticated, and distributed.

Kommentiert [EG3]: Use PSS padding

Kommentiert [EG4]: Should we support PKCS V1.5?

Kommentiert [EG5]: Use X509_V3 instead. X509_1993(X509 v2 is no longer supported in most systems)

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 [RFC 3161].

C.X2 Creator RSA Digital Signature Profile 2026

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 2026 may include a Creator RSA Digital Signature with every SOP Instance that it creates; however, the implementation is not required to do so.

The creator of a digital signature shall use one of the SHA256, SHA384, SHA512, SHA3-256, SHA3-384, or SHA3-512 hashing functions to generate a Message Digest, which is then signed using a private RSA key. All validators of digital signatures shall be capable of using a Message Digest generated by any of the hashing functions specified (SHA256, SHA384, SHA512, SHA3-256, SHA3-384, or SHA3-512.

The RSA key pair to sign/verify the signature shall have a modulus length of 3072 bit or above.

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

a. the SOP Class and Instance UIDs
b. the SOP Creation Date and Time, if present
c. the Study and Series Instance UIDs
d. any Attributes of the General Equipment Module that are present
e. any Attributes of the Overlay Plane Module, Curve Module or Graphic Annotation Module that are present
f. any Attributes of the General Image Module and Image Pixel Module that are present
g. any Attributes of the SR Document General Module and SR Document Content Module that are present
h. any Attributes of the Waveform Module and Waveform Annotation Module that are present
i. any Attributes of the Multi-frame Functional Groups Module that are present
j. any Attributes of the Enhanced MR Image Module that are present
k. any Attributes of the MR Spectroscopy Module that are present
l. any Attributes of the Raw Data Module that are present
m. any Attributes of the Enhanced CT Image Module that are present
n. any Attributes of the Enhanced XA/XRF Image Module that are present
o. any Attributes of the Segmentation Image Module that are present
p. any Attributes of the Encapsulated Document Series Module that are present
q. any Attributes of the X-Ray 3D Image Module that are present
r. any Attributes of the Enhanced PET Image Module that are present

s. any Attributes of the Enhanced US Image Module that are present
t. any Attributes of the Surface Segmentation Module that are present
u. any Attributes of the Surface Mesh Module that are present
v. any Attributes of the Structured Display Module, Structured Display Annotation Module, and Structured Display Image Box Module that are present
w. any Attributes of the Implant Template Module that are present
x. any Attributes of the Implant Assembly Template Module that are present
y. any Attributes of the Implant Template Group Module that are present
z. any Attributes of the Point Cloud Module that are present
aa. any Attributes of the Enhanced Mammography Image Module that are present
ab. any Attributes of the Tractography Results Modules that are present
ac. any Attributes of the Volumetric Graphic Annotation Module that are present
ad. any Attributes of the Microscopy Bulk Simple Annotations Module that are present
ae. any Attributes of the Waveform Presentation State Relationship Module that are present
af. any Attributes of the Structured Waveform Annotation Module that are present
ag. any Attributes of the Textual Waveform Annotation Module that are present
ah. any Attributes of the Displayed Waveform Segment Module that are present
ai. any Attributes of the Montage Activation Module that are present
aj. any Attributes of the Waveform Presentation Montage 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 Series 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 Encapsulated STL IOD Modules table.

The Digital Signature shall be created using the methodology described in the Base RSA Digital Signature Profile 2026. 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.

Creator RSA Digital Signatures bear no direct relationship to other Digital Signatures. However, other Digital Signatures, such as the Authorization Digital Signature, may be used to collaborate the timestamp of a Creator RSA Digital Signature.

C.X3 Authorization RSA Digital Signature Profile 2026

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 digital signature shall use one of the SHA256, SHA384, SHA512, SHA3-256, SHA3-384, or SHA3-512 hashing functions to generate a Message Digest, which is then signed using a private RSA key. All validators of digital signatures shall be capable of using a Message Digest generated by any of the hashing functions specified (SHA256, SHA384, SHA512, SHA3-256, SHA3-384, or SHA3-512.

The RSA key pair to sign/verify the signature shall have a modulus length of 3072 bit or above.

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

a. the SOP Class and Instance UIDs
b. the Study and Series Instance UIDs
c. any Attributes whose Values are verifiable by the technician or physician (e.g., their Values are displayed to the technician or physician)
d. any Attributes of the Overlay Plane, Curve or Graphic Annotation modules that are present
e. any Attributes of the General Image and Image Pixel modules that are present
f. any Attributes of the SR Document General and SR Document Content modules that are present
g. any Attributes of the Waveform and Waveform Annotation modules that are present
h. any Attributes of the Multi-frame Functional Groups module that are present
i. any Attributes of the Enhanced MR Image module that are present
j. any Attributes of the MR Spectroscopy modules that are present
k. any Attributes of the Raw Data module that are present
l. any Attributes of the Enhanced CT Image module that are present
m. any Attributes of the Enhanced XA/XRF Image module that are present
n. any Attributes of the Segmentation Image module that are present
o. any Attributes of the Encapsulated Document module that are present
p. any Attributes of the X-Ray 3D Image module that are present
q. any Attributes of the Enhanced PET Image module that are present
r. any Attributes of the Enhanced US Image module that are present
s. any Attributes of the Surface Segmentation module that are present
t. any Attributes of the Surface Mesh Module that are present
u. any Attributes of the Structured Display, Structured Display Annotation, and Structured Display Image Box modules that are present
v. any Attributes of the Implant Template module that are present
w. any Attributes of the Implant Assembly Template module that are present
x. any Attributes of the Implant Template Group module that are present
y. any Attributes of the Point Cloud Module that are present
z. any Attributes of the Enhanced Mammography Image module that are present
aa. any Attributes of the Volumetric Graphic Annotation Module that are present

The Digital Signature shall be created using the methodology described in the Base RSA Digital Signature Profile 2026. The Application Entity shall determine the identity of the technician or physician and obtain their certificate through a site-specific procedure such as a login mechanism or a smart card.

Authorization 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 collaborate the timestamp of an Authorization RSA Digital Signature.

C.X4 Structured Report RSA Digital Signature Profile 2026

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 Digital Signatures that follow this profile shall include a Digital Signature Purpose Code Sequence Attribute (0400,0401).

The RSA key pair to sign/verify the signature shall have a modulus length of 3072 bit or above.

As a minimum, an implementation shall include the following Attributes in generating the Digital Signature required by this profile:

a. the SOP Class UID
b. the Study and Series Instance UIDs
c. all Attributes of the General Equipment Module that are present
d. the Current Requested Procedure Evidence Sequence
e. the Pertinent Other Evidence Sequence
f. the Predecessor Documents Sequence
g. the Observation DateTime
h. all Attributes of the SR Document Content Module that are present

If the Verification Flag is set to "VERIFIED" (and the SOP Instance UID can no longer change) at least one of the Digital Signatures profile shall have the purpose of (5, ASTM-sigpurpose, "Verification Signature") and shall also include the following Attributes in addition to the above Attributes:

a. the SOP Instance UID
b. the Verification Flag
c. the Verifying Observer Sequence
d. the Verification DateTime

Note The system may also add a Creator ECC-based Digital Signature 2026, which could cover other Attributes that the machine can verify.

All occurrences of Referenced SOP Instance MAC Sequence (0400,0403) shall have the Value of MAC Algorithm (0400,0015) set to either "SHA256", "SHA384”,"SHA512" "SHA3-256", "SHA3-384" or "SHA3-512”.

The Digital Signature shall be created using the methodology described in the Base RSA Digital Signature Profile 2026. 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.

Add 4 New ECC-based Digital Signature Profiles equivalent to the 4 RSA-based ones

C.X5 Base ECC-based Digital Signature Profile

The Base ECC-based Digital Signature Profile outlines the use of ECDSA (Elliptic Curve Digital Signature Algorithm) or EdDSA (Edwards-Curve Digital Signature Algorithm). 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 ECDSA or EdDSA as defined in [FIPS 186-5]. To create an ECDSA or EdDSA digital signature, the digital signature creator should use a hash function to generate a message digest, which is then signed using a private ECDSA or EdDSA key. The recommended hash functions are SHA-2 family hash functions (SHA256, SHA384, or SHA512) defined in [FIPS 180-4] and SHA-3 family hash functions (SHA3-256, SHA3-384, or SHA3-512) defined in [FIPS 202]. To sign the message digest using ECDSA or EdDSA, the digital signature creator should select an elliptic curve according to [NIST 800-186] to generate ECDSA or EdDSA key pair and execute the signing process. The recommended elliptic curves are Curve P-256, Curve P-384, Curve P-521, Ed25519, and Ed448.

The Value of MAC Algorithm (0400,0015) shall be set to either "SHA256", "SHA384", "SHA512", "SHA3-256", "SHA3-384", or "SHA3-512". The public key associated with the private key as well as the identity of the Application Entity or equipment manufacturer that owns the ECDSA or EdDSA 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.

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 [RFC 3161].

C.X6 Creator ECC-based Digital Signature Profile

The creator of a DICOM SOP Instance may generate signatures using the Creator ECC-based 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 ECC-based Digital Signature Profile may include a Creator ECC-based Digital Signature with every SOP Instance that it creates; however, the implementation is not required to do so.

The creator of a digital signature shall use ECDSA or EdDSA as defined in [FIPS 186-5]. To create an ECDSA or EdDSA digital signature, the digital signature creator should use a hash function to generate a message digest, which is then signed using a private ECDSA or EdDSA key. The recommended hash functions are SHA-2 family hash functions (SHA256, SHA384, or SHA512) defined in [FIPS 180-4] and SHA-3 family hash functions (SHA3-256, SHA3-384, or SHA3-512) defined in [FIPS 202]. To sign the message digest using ECDSA or EdDSA, the digital signature creator should select an elliptic curve according to [NIST 800-186] to generate ECDSA or EdDSA key pair and execute the signing process. The recommended elliptic curves are Curve P-256, Curve P-384, Curve P-521, Ed25519, and Ed448.

Note Local rules and regulations may further restrict the hashing functions or elliptic curves that are permitted. For example, China may require SM3 hash function and SM2 elliptic curve cryptography. 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 ECC-based Digital Signature:

a. the SOP Class and Instance UIDs
b. the SOP Creation Date and Time, if present
c. the Study and Series Instance UIDs
d. any Attributes of the General Equipment Module that are present
e. any Attributes of the Overlay Plane Module, Curve Module or Graphic Annotation Module that are present
f. any Attributes of the General Image Module and Image Pixel Module that are present
g. any Attributes of the SR Document General Module and SR Document Content Module that are present
h. any Attributes of the Waveform Module and Waveform Annotation Module that are present
i. any Attributes of the Multi-frame Functional Groups Module that are present
j. any Attributes of the Enhanced MR Image Module that are present
k. any Attributes of the MR Spectroscopy Module that are present
l. any Attributes of the Raw Data Module that are present
m. any Attributes of the Enhanced CT Image Module that are present
n. any Attributes of the Enhanced XA/XRF Image Module that are present
o. any Attributes of the Segmentation Image Module that are present
p. any Attributes of the Encapsulated Document Series Module that are present
q. any Attributes of the X-Ray 3D Image Module that are present
r. any Attributes of the Enhanced PET Image Module that are present
s. any Attributes of the Enhanced US Image Module that are present
t. any Attributes of the Surface Segmentation Module that are present
u. any Attributes of the Surface Mesh Module that are present
v. any Attributes of the Structured Display Module, Structured Display Annotation Module, and Structured Display Image Box Module that are present
w. any Attributes of the Implant Template Module that are present
x. any Attributes of the Implant Assembly Template Module that are present
y. any Attributes of the Implant Template Group Module that are present
z. any Attributes of the Point Cloud Module that are present
aa. any Attributes of the Enhanced Mammography Image Module that are present
ab. any Attributes of the Tractography Results Modules that are present
ac. any Attributes of the Volumetric Graphic Annotation Module that are present
ad. any Attributes of the Microscopy Bulk Simple Annotations Module that are present
ae. any Attributes of the Waveform Presentation State Relationship Module that are present
af. any Attributes of the Structured Waveform Annotation Module that are present
ag. any Attributes of the Textual Waveform Annotation Module that are present
ah. any Attributes of the Displayed Waveform Segment Module that are present
ai. any Attributes of the Montage Activation Module that are present
aj. any Attributes of the Waveform Presentation Montage 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 Series 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 Encapsulated STL IOD Modules table.

The Digital Signature shall be created using the methodology described in the Base ECC-based Digital Signature Profile. Typically the certificate and associated private key used to produce Creator ECC-based 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 ECC-based Digital Signature, and the SCU shall support verification of such signatures.

Creator ECC-based Digital Signatures bear no direct relationship to other Digital Signatures. However, other Digital Signatures, such as the Authorization Digital Signature, may be used to collaborate the timestamp of a Creator ECC-based Digital Signature.

C.X7 Authorization ECC-based 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 ECC-based 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 creator of a digital signature shall use ECDSA or EdDSA as defined in [FIPS 186-5]. To create an ECDSA or EdDSA digital signature, the digital signature creator should use a hash function to generate a message digest, which is then signed using a private ECDSA or EdDSA key. The recommended hash functions are SHA-2 family hash functions (SHA256, SHA384, or SHA512) defined in [FIPS 180-4] and SHA-3 family hash functions (SHA3-256, SHA3-384, or SHA3-512) defined in [FIPS 202]. To sign the message digest using ECDSA or EdDSA, the digital signature creator should select an elliptic curve according to [NIST 800-186] to generate ECDSA or EdDSA key pair and execute the signing process. The recommended elliptic curves are Curve P-256, Curve P-384, Curve P-521, Ed25519, and Ed448.

As a minimum, an implementation shall include the following Attributes in generating the Authorization ECC-based Digital Signature:

a. the SOP Class and Instance UIDs
b. the Study and Series Instance UIDs
c. any Attributes whose Values are verifiable by the technician or physician (e.g., their Values are displayed to the technician or physician)
d. any Attributes of the Overlay Plane, Curve or Graphic Annotation modules that are present
e. any Attributes of the General Image and Image Pixel modules that are present
f. any Attributes of the SR Document General and SR Document Content modules that are present
g. any Attributes of the Waveform and Waveform Annotation modules that are present
h. any Attributes of the Multi-frame Functional Groups module that are present
i. any Attributes of the Enhanced MR Image module that are present
j. any Attributes of the MR Spectroscopy modules that are present
k. any Attributes of the Raw Data module that are present
l. any Attributes of the Enhanced CT Image module that are present
m. any Attributes of the Enhanced XA/XRF Image module that are present
n. any Attributes of the Segmentation Image module that are present
o. any Attributes of the Encapsulated Document module that are present
p. any Attributes of the X-Ray 3D Image module that are present

q. any Attributes of the Enhanced PET Image module that are present
r. any Attributes of the Enhanced US Image module that are present
s. any Attributes of the Surface Segmentation module that are present
t. any Attributes of the Surface Mesh Module that are present
u. any Attributes of the Structured Display, Structured Display Annotation, and Structured Display Image Box modules that are present
v. any Attributes of the Implant Template module that are present
w. any Attributes of the Implant Assembly Template module that are present
x. any Attributes of the Implant Template Group module that are present
y. any Attributes of the Point Cloud Module that are present
z. any Attributes of the Enhanced Mammography Image module that are present
aa. any Attributes of the Volumetric Graphic Annotation Module that are present

The Digital Signature shall be created using the methodology described in the Base ECC-based Digital Signature Profile. The Application Entity shall determine the identity of the technician or physician and obtain their certificate through a site-specific procedure such as a login mechanism or a smart card.

Authorization ECC-based Digital Signatures bear no direct relationship to other Digital Signatures. However, other Digital Signatures, such as the Creator ECC-based Digital Signature, may be used to collaborate the timestamp of an Authorization ECC-based Digital Signature.

C.X8 Structured Report ECC-based 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 Digital Signatures that follow this profile shall include a Digital Signature Purpose Code Sequence Attribute (0400,0401).

As a minimum, an implementation shall include the following Attributes in generating the Digital Signature required by this profile:

a. the SOP Class UID
b. the Study and Series Instance UIDs
c. all Attributes of the General Equipment Module that are present
d. the Current Requested Procedure Evidence Sequence
e. the Pertinent Other Evidence Sequence
f. the Predecessor Documents Sequence
g. the Observation DateTime
h. all Attributes of the SR Document Content Module that are present

If the Verification Flag is set to "VERIFIED" (and the SOP Instance UID can no longer change) at least one of the Digital Signatures profile shall have the purpose of (5, ASTM-sigpurpose, "Verification Signature") and shall also include the following Attributes in addition to the above Attributes:

e. the SOP Instance UID
f. the Verification Flag
g. the Verifying Observer Sequence
h. the Verification DateTime

Note The system may also add a Creator ECC-based Digital Signature, which could cover other Attributes that the machine can verify.

All occurrences of Referenced SOP Instance MAC Sequence (0400,0403) shall have the Value of MAC Algorithm (0400,0015) set to either "SHA256", "SHA384", "SHA512", "SHA3-256", "SHA3-384", or "SHA3-512".

The Digital Signature shall be created using the methodology described in the Base ECC-based 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 ECC-based Digital Signatures bear no direct relationship to other Digital Signatures. However, other Digital Signatures, such as the Creator ECC-based Digital Signature, may be used to corroborate the timestamp of a Structured Report ECC-based Digital Signature.

Add D.X1 Basic DICOM Media Security Profile 2026

D.X1 Basic DICOM Media Security Profile 2026

The 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 uses the enveloped-data content type as defined in Cryptographic Message Syntax (CMS) in IETF STD 70 [RFC 5652] and [RFC 3370] .

This profile also provides mechanisms to manage the content encryption key needed for the encryption and decryption of Secure DICOM File, by making use of the key management technologies supported by CMS in [RFC 5652] or [RFC 9629], See details in D.2.3.

> Note: This profile supersedes the mechanism in Basic DICOM Media Security Profile, except that the allowed algorithms are updated and the key management methods are extended.

D.X1.1 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 IETF STD 70 [RFC 5652], [RFC 3370] , [RFC 3565] and [RFC 9629].

The encrypted content of the Enveloped-data content type shall be one of the following choices:

- Signed-data content type;
- Digested-data content type.

The digested-data content type provides data integrity protection while signed-data content type provide data integrity protection as well as data origin authentication.

For signed-data content type, one or more digital signatures can exist, which allow multi-party to sign the content.

In both cases, the EncapsulatedContentInfo shall exist to carry the original DICOM file as an octet string.

D.X1.2 Cryptography Algorithm

The content should be encrypted using AES [RFC 3565] with an encryption key of length 128 bits or above, CBC or CTR mode are recommended to be used. Readers claiming conformance to this profile shall be capable of decrypting Secure DICOM Files using AES.

SHA256, SHA384, SHA512, SHA3-256, SHA3-384, or SHA3-512 should be used as the digest algorithms for both digested-data content type and signed-data content type.

If signed-data content type is used, RSA [RFC 8017], ECDSA [FIPS 186-5], or EdDSA [RFC 8032] should be used as the digital signature algorithms.

Note: RSA, if used, should have a modulus length of 2048 bit or above.

The recommended elliptic curves are Curve P-256, Curve P-384, or Curve P-521 for ECDSA, Ed25519, or Ed448 for EdDSA.

There are no specific requirements for the combination of digital signature algorithm and digest algorithm in this profile. The implementation may follow the state-of-the-art guidelines in relevant standards, e.g. from NIST or RFC. A general recommendation would be that the security length to be matched, e.g. using ECDSA Curve P-256 with SHA256 as both are considered with 128-bit security length. [NIST 800-57] provides some guidance on security length for NIST approved algorithms.

The algorithms used for key management are different according to the key management technologies used, the relevant requirements are specified in D.2.3.

D.X1.3. Key Management Technologies

Key management technologies are used to manage the content encryption key used for content encryption and decryption.

[RFC 5652] provides 4 key management technologies. [RFC 9629] adds one additional, i.e., Key Encapsulation Mechanism (KEM). The profiles allow the use of all the key management technologies defined in [RFC 5652] or [RFC 9629]. An implementation shall use one of the following key management technologies:

- Key Transport in the form of KeyTransRecipientInfo,
- Key Agreement in the form of KeyAgreeRecipientInfo
- Previously distributed Symmetric KEK (key-encryption keys) in the form of KEKRecipientInfo
- Password-based Key Derivation in the form of PasswordRecipientInfo
- Key Encapsulation Mechanism in the form of KEMRecipientInfo

The key transportation method involves using an asymmetric key to encrypt the symmetric content encryption key. When utilizing this approach, RSA-OAEP [RFC 8017] is recommended for encrypting the content encryption key, with RSA employing a modulus length of at least 2048 bits.

For the key agreement method, Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) should be used to establish the content encryption key.

When a symmetric Key Encryption Key (KEK) is employed, AES with a key size of 128 bits or greater should be used to encrypt the content encryption key; in this context, the AES-KW (Key Wrap mode) algorithm is recommended.

For password-based key derivation, PBKDF2 should be utilized. Additional requirements on using password-based key derivation method is listed in D.X1.3.1.

For the KEM method, RSA-KEM [RFC 9690] and ML-KEM [FIPS 203] may be used.

D.X1.3.1 Password-based Key Derivation

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. 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.
2. 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 PS3.5), 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").

Add D.X2 DICOM Media Security Profile – Authenticated Encryption

D.X2 DICOM Media Security Profile – Authenticated Encryption

The 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 uses the authenticated-enveloped-data content type to provide integrity and confidentiality in a single step through Authenticated Encryption, as specified in Cryptographic Message Syntax (CMS) by IETF STD 70 [RFC 5652] and [RFC 5083].

Note: Authenticated encryption (AE) is any encryption scheme which simultaneously assures the data confidentiality and authenticity. Examples of encryption modes that provide AE are GCM, CCM. Many AE schemes allow the message to contain "associated data" (AD) which is not made confidential, but is integrity protected, so also known as authenticated encryption with associated data (AEAD).

This profile also provides mechanism to manage the content encryption key needed for the encryption and decryption of Secure DICOM File, by making use of the key management technologies supported by CMS in [RFC 5652] or [RFC 9629]. See details in D.3.3.

D.X2.1 Encapsulation of a DICOM File in a Secure DICOM File

A Secure DICOM File conforming to this security profile shall contain an authenticated-enveloped-data content type of the Cryptographic Message Syntax defined in [RFC 5083].

The EncryptedContent in authEncryptedContentInfo shall exist to carry the original DICOM file as an octet string.

D.X2.2 Cryptography Algorithm

AES [RFC 3565] with an encryption key of length 128 bits or above shall be used for authenticated encryption of the content. GCM or CCM mode shall be used according to [RFC 5084]. Readers claiming conformance to this profile shall be capable of decrypting Secure DICOM Files using AES.

The algorithms used for key management are different according to the key management technologies used, the relevant requirements are specified in D.3.3.

A Secure DICOM File conforming to this security profile shall contain an authenticated-enveloped-data content type of the Cryptographic Message Syntax defined in [RFC 5083].

The EncryptedContent in authEncryptedContentInfo shall exist to carry the original DICOM file as an octet string.

D.X2.2 Cryptography Algorithm

AES [RFC 3565] with an encryption key of length 128 bits or above shall be used for authenticated encryption of the content. GCM or CCM mode shall be used according to [RFC 5084]. Readers claiming conformance to this profile shall be capable of decrypting Secure DICOM Files using AES.

The algorithms used for key management are different according to the key management technologies used, the relevant requirements are specified in D.3.3.

D.X2.3. Key Management Technologies

Key management technologies is used to manage the content encryption key used for content encryption and decryption.

[RFC 5652] provides 4 key management technologies. [RFC 9629] adds one additional, i.e. Key Encapsulation Mechanism (KEM). The profiles allow the use of all the key management technologies defined in [RFC 5652] or [RFC 9629]. An implementation shall use one of the following key management technologies:

- Key Transport in the form of KeyTransRecipientInfo,
- Key Agreement in the form of KeyAgreeRecipientInfo
- Previously distributed Symmetric KEK (key-encryption keys) in the form of KEKRecipientInfo
- Password-based Key Derivation in the form of PasswordRecipientInfo

- Key Encapsulation Mechanism in the form of KEMRecipientInfo

The key transportation method involves using an asymmetric key to encrypt the symmetric content encryption key. When utilizing this approach, RSA-OAEP [RFC 8017] is recommended for encrypting the content encryption key, with RSA employing a modulus length of at least 2048 bits.

For the key agreement method, Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) should be used to establish the content encryption key.

When a symmetric Key Encryption Key (KEK) is employed, AES with a key size of 128 bits or greater should be used to encrypt the content encryption key; in this context, the AES-KW (Key Wrap mode) algorithm is advised.

For password-based key derivation, PBKDF2 should be utilized. Additional requirements on using password-based key derivation method is listed in D.2.3.1.

For the KEM method, RSA-KEM [RFC 9690] and ML-KEM [FIPS 203] may be used.

D.X2.3.1 Password-based Key Derivation

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. 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.
2. 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 PS3.5), 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").

PS 3.3

Update PS3.3 C.12.1.1.3.1.2 Signature

C.12.1.1.3.1.2 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 (0400,0020) appears. Data shall be formed into a byte stream and presented to the algorithm specified by MAC Algorithm (0400,0015) for computation of the MAC according to the following rules:

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 incorporate 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.

Note Since the Value Length of Data Elements with a VR of SQ can be either explicit or undefined, the Value Lengths of such Data Elements are left out of the MAC calculation. Similarly, the Value Length of Data Elements with a VR of OB with an undefined length are also left out so that they are handled consistently. If such Data Elements do come with undefined lengths, including the Item Tags that separate the Items or fragments insures that Data Elements cannot be moved between Items or Fragments without compromising the Digital Signature. For those Data Elements with explicit lengths, if the length of an Item changes, the added or removed portions would also impact the MAC calculation, so it is not necessary to include explicit lengths in the MAC calculation. It is possible that including the Value Lengths could make cryptanalysis easier.

After the fields of all the Data Elements in the Data Elements Signed list have been placed into the byte stream presented to the MAC Algorithm according to the above rules, all of the Data Elements within the Digital Signatures Sequence Item except the Certificate of Signer (0400,0115), Signature (0400,0120), Certified Timestamp Type (0400,0305), and Certified Timestamp (0400,0310) shall also be encoded according to the above rules, and presented to the MAC algorithm (i.e., the Attributes of the Digital Signature Sequence Item for this particular Digital Signature are also implicitly included in the list of Data Elements Signed, except as noted above).

The resulting MAC code after processing this byte stream by the MAC Algorithm is then encrypted as specified in the Certificate of Signer and placed in the Value of the Signature Data Element.

Notes

1. The Transfer Syntax used in the MAC calculation may differ from the Transfer Syntax used to exchange the Data Set.
2. Digital Signatures require explicit VR in order to calculate the MAC. An Application Entity that receives a Data Set with an implicit VR Transfer Syntax may not be able to verify Digital Signatures that include Private Data Elements or Data Elements unknown to that Application Entity. This also true of any Data Elements whose VR is UN. Without knowledge of the Value Representation, the receiving Application Entity would be unable to perform proper byte swapping or be able to properly parse Sequences in order to generate a MAC.
3. If more than one entity signs, each Digital Signature would appear in its own Digital Signatures Sequence Item. The Digital Signatures may or may not share the same MAC Parameters Sequence Item.
4. The notion of a notary public (i.e., someone who verifies the identity of the signer) for Digital Signatures is partially filled by the authority that issued the Certificate of Signer.

Table C.12.1.1.3.1.2-1 lists the Defined Terms for MAC Algorithm (0400,0015).

Table C.12.1.1.3.1.2-1. Defined Terms for MAC Algorithm (0400,0015)

Defined Term	Reference
RIPEMD160	[ISO/IEC 10118-3] **Note** **Security standards such as [NIST 800-131A] and [NIST 800-57] recommend security strength of 112 bit or above for Message Digest in digital signature. The security strength of RIPEMD160 is less than or equal to 80 bit and as a result no longer considered secure anymore. It is recommended to be used only for legacy products for backward compatibility purposes.**
MD5	[RFC1321] Note ~~See also security considerations in [RFC6151]. The use of MD5 is no longer recommended~~ **has been proved to be insecure, subject to collision attacks, see [Wang-Yu 2005]. I deprecated and disallowed for use in digital signature according to [RFC6151]. It i recommended to be used only for legacy products for backward compatibility purposes.**
SHA1	[FIPS PUB 180-4] **Note** **SHA-1 has been proved to be insecure, subject to collision attacks, see [Wang-Yin-Yu 2005]. It is deprecated and disallowed for use in digital signature according to [NIST 800-131A]. It is recommended to be used only for legacy products for backward compatibility purposes.**
SHA224	[FIPS PUB 180-4]
SHA256	[FIPS PUB 180-4]
SHA384	[FIPS PUB 180-4]

Kommentiert [JM6]: Perhaps reformulate to mimic the text that is used below: “It is not to be used unless for backward compatibility with legacy products.” Do the same for the two items below.

Kommentiert [JM6R2]: Second thought: you might use “should” here, as it is normative. Not sure whether that is accepted, though, so perhaps leaving it as proposed is best.

Defined Term	Reference
SHA512	[FIPS PUB 180-4]
SHA512_224	[FIPS PUB 180-4]
SHA512_256	[FIPS PUB 180-4]
SHA3_224	[FIPS PUB 202]
SHA3_256	[FIPS PUB 202]
SHA3_384	[FIPS PUB 202]
SHA3_512	[FIPS PUB 202]

Note Security Profiles (see PS3.15) may restrict or extend the list of MAC algorithms that are permitted or required by a specific profile.

PS 3.11

Update D.3.5 Security Parameters

D.3.5 Security Parameters

The STD-GEN-SEC-CD, STD-GEN-SEC-DVD-RAM and STD-GEN-SEC-BD Media Storage Application Profiles require that **the implementation support at least one of DICOM Media Storage Security Profiles defined in Annex D of PS3.15, and** the all DICOM Files in the File-set including the DICOMDIR be Secure DICOM Files encapsulated in accordance with the requirements of the ~~**Basic**~~ DICOM Media **Storage** Security ~~**Profile**~~ **Profiles** **it** supports ~~**as defined in PS3.15**~~.

Note These Media Storage Application Profiles do not place any consistency restrictions on the use of the Basic DICOM Media Security Profile with different DICOM Files of one File-set. For example, readers should not assume that all Files in the File-set can be decoded by the same set of recipients. Readers should also not assume that all secure Files use the same approach (hash key or digital signature) to ensure Integrity or carry the same originators' signatures.

Kommentiert [JM7]: Is this indeed what you want? I'd say the word "supports" should be kept.

Kommentiert [EG7R2]: You are right! This is a mistake happens when I intended to delete as defined in PS3.15 to avoid duplication.

Update H.3.5 Security Parameters

H.3.5 Security Parameters

The STD-GEN-SEC-DVD Media Storage Application Profiles require that **the implementation support at least one of DICOM Media Storage Security Profiles defined in Annex D of PS3.15, and** all DICOM Files in the File-set including the DICOMDIR be Secure DICOM Files encapsulated in accordance with the requirements of the ~~**Basic**~~ DICOM Media **Storage** Security ~~**Profile**~~ **Profiles** **it** supports ~~**as defined in PS3.15**~~.

Note These Media Storage Application Profiles do not place any consistency restrictions on the use of the Basic DICOM Media Security Profile with different DICOM Files of one File-set. For example, readers should not assume that all Files in the File-set can be decoded by the same set of recipients. Readers should also not assume that all secure Files use the same approach (hash key or digital signature) to ensure Integrity or carry the same originators' signatures.

Kommentiert [JM8]: As previous comment.

Kommentiert [EG8R2]: Keep as above.

Update I.3.4 Security Parameters

I.3.4 Security Parameters

The STD-DVD-SEC-MPEG2-MPML Media Storage Application Profiles require that **the implementation support at least one of DICOM Media Storage Security Profiles defined in Annex D of PS3.15, and** all DICOM Files in the File-set including the DICOMDIR be Secure DICOM Files encapsulated in accordance with the requirements of the ~~**Basic**~~ DICOM Media **Storage** Security ~~**Profile**~~ **Profiles it** supports ~~**as defined in PS3.15**~~.

Kommentiert [JM9]: As previous comment.

Kommentiert [EG9R2]: Keep as above.

Note These Media Storage Application Profiles do not place any consistency restrictions on the use of the Basic DICOM Media Security Profile with different DICOM Files of one File-set. For example, readers should not assume that all Files in the File-set can be decoded by the same set of recipients. Readers should also not assume that all secure Files use the same approach (hash key or digital signature) to ensure Integrity or carry the same originators' signatures.

Update J.3.5 Security Parameters

J.3.5 Security Parameters

The STD-GEN-SEC-USB-JPEG, STD-GEN-SEC-MMC-JPEG, STD-GEN-SEC-CF-JPEG, STD-GEN-SEC-SD-JPEG, STD-GEN-SEC-USB-J2K, STD-GEN-SEC-MMC-J2K, STD-GEN-SEC-CF-J2K and STD-GEN-SEC-SD-J2K Media Storage Application Profiles require that **the implementation support at least one of DICOM Media Storage Security Profiles defined in Annex D of PS3.15, and** all DICOM Files in the File-set including the DICOMDIR be Secure DICOM Files encapsulated in accordance with the requirements of the ~~**Basic**~~ DICOM Media **Storage** Security ~~**Profile**~~ **Profiles it** supports ~~**as defined in PS3.15**~~.

Kommentiert [JM10]: As previous comment.

Kommentiert [EG10R2]: Keep as above.

Note These Media Storage Application Profiles do not place any consistency restrictions on the use of the Basic DICOM Media Security Profile with different DICOM Files of one File-set. For example, readers should not assume that all Files in the File-set can be decoded by the same set of recipients. Readers should also not assume that all secure Files use the same approach (hash key or digital signature) to ensure Integrity or carry the same originators' signatures.

Update M.3.5 Security Parameters

M.3.5 Security Parameters

The STD-GEN-SEC-BD Media Storage Application Profiles require that **the implementation support at least one of DICOM Media Storage Security Profiles defined in Annex D of PS3.15, and** all DICOM Files in the File-set including the DICOMDIR be Secure DICOM Files encapsulated in accordance with the requirements of the ~~**Basic**~~ DICOM Media **Storage** Security ~~**Profile**~~ **Profiles it** supports ~~**as defined in PS3.15**~~.

Kommentiert [JM11]: As previous comment.

Kommentiert [EG11R2]: Keep as above.

Note These Media Storage Application Profiles do not place any consistency restrictions on the use of the Basic DICOM Media Security Profile with different DICOM Files of one File-set. For example, readers should not assume that all Files in the File-set can be decoded by the same set of recipients. Readers should also not assume that all secure Files use the same approach (hash key or digital signature) to ensure Integrity or carry the same originators' signatures.

Update N.3.4 Security Parameters

N.3.4 Security Parameters

The STD-GEN-SEC-BD-MPEG4-LV42 Media Storage Application Profiles require **the implementation support at least one of DICOM Media Storage Security Profiles defined in Annex D of PS3.15, and** all DICOM Files in the File-set including the DICOMDIR be Secure DICOM Files encapsulated in accordance with the requirements of the ~~**Basic**~~ DICOM Media **Storage** Security ~~**Profile**~~ **Profiles it** supports ~~**as defined in PS3.15**~~.

Kommentiert [JM12]: As previous comment.

Kommentiert [EG12R2]: Keep as above.

Note

These Media Storage Application Profiles do not place any consistency restrictions on the use of the Basic DICOM Media Security Profile with different DICOM Files of one File-set. For example, readers should not assume that all Files in the File-set can be decoded by the same set of recipients. Readers should also not assume that all secure Files use the same approach (hash key or digital signature) to ensure integrity or carry the same originators' signatures.

PS 3.15

E Attribute Confidentiality Profiles (Normative)

Add new attributes to table E.1-1

Table E.1-1. Application Level Confidentiality Profile Attributes

Attribute Name	Tag	Retd. (from PS3.6)	In Std. Comp. IOD (from PS3.3)	Basic Prof.	Rtn. Safe Priv. Opt.	Rtn. UIDs Opt.	Rtn. Dev. Id. Opt.	Rtn. Inst. Id. Opt.	Rtn. Pat. Chars. Opt.	Rtn. Long. Full Dates Opt.	Rtn. Long. Modif. Dates Opt.	Clean Desc. Opt.	Clean Struct. Cont. Opt.	Clean Graph. Opt.
Accession Number	(0008,0050)	N	Y	Z										
…														
Digital Signature Algorithm	**(xxxx,yyyy)**	**N**	**Y**	**X**										
Elliptic Curve	**(xxxx,zzzz)**	**N**	**Y**	**X**										