Supplement XXX

CRYPTOGRAPHY UPDATE FOR DIGITAL SIGNATURE AND MEDIA STORAGE SECURITY

DICOM WORKING GROUP 14

FIRST READ

ALEXANDER ZHANG, ESSIEN GE, JEROEN MEDEMA, ROB HORN

MAR.13, 2026

Background

- 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 algorithm are still being used, e.g. 3DES, MD5 and SHA-1, meanwhile, it may be worthwhile to support of the newer cryptography algorithm e.g. ECDSA/EdDSA for digital signature, SHA3 for digest, up-to-date cryptography technologies such as authenticated encryption (e.g. AES-CCM/GCM), and newer key management technologies such as KEM.

Updates to Digital Signature Profiles

- Updates to PS3.15 Annex C: Digital Signature Profiles
- Updates to Digital signature Macro in PS3.3
- Dependent updates in PS3.6 and PS3.15(de-id)

Updates to PS3.15 Annex C: Digital Signature Profiles

- Add 4 new RSA based Digital Signature Profiles using new algorithm
  - Use the current mechanism in existing RSA Digital signature profiles.
  - For Support SHA-2 and SHA-3(new) family, deprecate MD5/SHA1/RIPEMD160.
  - Add requirements on RSA modulus sizes to 3072 or above to be align with NIST 800-131r3
  - Use X509_V3 certificate format.
- Add 4 new Digital Signature Profiles which are based on Elliptic Curve algorithms.
  - Digital signature algorithm: ECDSA, EdDSA
  - ECC Curves: Curve P-256, Curve P-384, Curve P-521, Ed25519, and Ed448
  - Digest algorithm: SHA256, SHA384, SHA512, SHA3-256, SHA3-384, SHA3-512

Updates to Digital signature Macro in PS3.3 and PS3.6

- Add 2 new data elements to indicate digital signature algorithm and ECC curve
- Add X509_V3 in Certificate Type (0400,0110)
- Update PS3.6 accordingly due to new data elements.

			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.

			See Section C.12.1.1.3.1.2.
>Digital Signature Algorithm	**(0400, 0125)**	3	**The algorithm used to generate the Digital Signature. If this element is not appear, meaning the algorithm used is RSA.** **Defined Terms:** **RSA** **ECDSA** **EdDSA**
>Elliptic Curve	**(0400, 0130)**	**3C**	**If Digital Signature Algorithm is ECDSA or EdDSA, this attribute shall be defined to refer to the specific curves used in generating the digital signature.** **Defined Terms:** **NIST Curve P-256** **NIST Curve P-384** **NIST Curve P-521** **Ed25519** **Ed448**

Updates to Media Storage Security Profiles

- Updates to PS3.15 Annex D: Media Storage Security Profiles
- Updates to PS3.2 Conformance Statement
- Dependent updates to PS3.10 and PS3.11

Updates to PS3.15 Annex D: Media Storage Security Profiles

- Add one new Media Storage Security Profile, which supersede 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).

Updates to PS3.2, PS3.10 and PS3.11

- Update PS3.2 Annex D conformance statement template as now there're multiple media storage profiles.
- Update the reference to Media Storage Security Profiles in PS3.10 and PS3.11. (e.g. the previous version link directly to Basic Media Security Profile.)

Open issues

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 2nd 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 SOP 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.