Correction Number	CP-338
Log Summary: Add AES to DICOM TLS negotiation	
Type of Modification Addition	Name of Standard PS 3.15 2003

Rationale for Correction

The Rijndael encryption system has been approved by the US government as a US replacement for the DES standard. It has now been incorporated into the TLS standard by means of RFC-3268. The rationale for changing DICOM is the same as the rationale used for the TLS modifications. The following text is from the rationale for RFC-3268, with my additions in italics:

1. RC2, RC4, and IDEA are all subject to intellectual property claims. RSA Security Inc. has trademark rights in the names RC2 and RC4, and claims that the RC4 algorithm itself is a trade secret. Ascom Systec Ltd. owns a patent on the IDEA algorithm.

2. Triple DES is much less efficient than more modern ciphers.

3. Now that the AES process is completed there will be commercial pressure to use the selected cipher. The AES is efficient and has withstood extensive cryptanalytic efforts. The AES is therefore a desirable choice. *This efficiency improvement is particularly important when images are encrypted. The computational demands for 128-bit AES are only 10-30% of those for 3DES. Current production microprocessors can encrypt using AES and transmit at 100 Mbit-sec speeds without needing special hardware assists.*

4. Currently the DHE ciphersuites only allow triple DES (along with some "export" variants which do not use a satisfactory key length). At the same time the DHE ciphersuites are the only ones to offer forward secrecy.

Sections of documents affected

PS 3.15 Section 2, Annex B

Correction Wording:

Add the following section to PS 3.15 Section 2 Normative References

RFC-3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002.

Add the following section to PS 3.15 Annex B

B.3 THE AES TLS SECURE TRANSPORT CONNECTION PROFILE

An implementation that supports the AES TLS Secure Transport Connection Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security Version 1.0 protocol. Table B.3-1 specifies mechanisms that shall be supported if the corresponding features within TLS are supported by the Application Entity. The profile does not require the implementation to support all of the features (entity authentication, encryption, integrity checks) of TLS. Other mechanisms may also be used if agreed to by negotiation during establishment of the TLS channel.

Table B.3-1 Minimum Mechanisms for TLS Features

Supported TLS Feature	Minimum Mechanism
Entity Authentication	RSA based Certificates

Two cyphersuite options shall be offered during TLS negotiation by applications that comply with this profile:

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

The application shall offer both options. The AES version shall be preferred. The fallback to 3DES is offered so that this profile can interoperate easily with applications that only support the 3DES cyphersuite.

IP ports on which an implementation accepts TLS connections, or the mechanism by which this port number is selected or configured, shall be specified in the Conformance Statement. This port shall be different from ports used for other types of transport connections (secure or unsecure).

Note: It is strongly recommended that systems supporting the AES TLS Secure Transport Connection Profile use as their port the registered port number “2762 dicom-tls” for the DICOM Upper Layer Protocol on TLS: (decimal).

The Conformance Statement shall also indicate what mechanisms the implementation supports for Key Management.

The profile does not specify how a TLS Secure Transport Connection is established, or the significance of any certificates exchanged during peer entity authentication. These issues are left up to the Application Entity, which presumably is following some site specified security policy. The identities of the certificate owners can by used by the application entity for audit log support, or to restrict access based on some external access rights control framework. Once the Application Entity has established a Secure Transport Connection, then an Upper Layer Association can use that secure channel.

Note: There may be an interaction between PDU size and TLS Record size that impacts efficiency of transport. The maximum allowed TLS record size is smaller than the maximum allowed PDU size.

When an integrity check fails, the connection shall be dropped per the TLS protocol, causing both the sender and the receiver to issue an A-P-ABORT indication to the upper layers with an implementation-specific provider reason. The provider reason used shall be documented in the conformance statement.

Note: An integrity check failure indicates that the security of the channel may have been compromised.