DICOM Change Proposal

STATUS	Assigned
Date of Last Update	2026/01/05
Person Assigned	steven.nichols@gehealthcare.com
Submitter Name	steven.nichols@gehealthcare.com
Submission Date	2025/10/22

Change Number	CP-2592
Log Summary: Correct TLS1.2 cipher suite	
Name of Standard PS3.15	
Rationale for Change: PS3.15 contains a cipher-suite named TLS_DHE_RSA_WITH_AES_256_GCM_CCM_8 as optional for TLS 1.2. This does not match any IANA-registered TLS cipher suite. The valid name is TLS_DHE_RSA_WITH_AES_256_CCM_8 per [RFC 6655]	
Change Wording:	

Modify PS3.15 Section B.13 Modified BCP 195 RFC 8996, 9325 TLS Secure Transport Connection Profile as indicated:

B.13 Modified BCP 195 RFC 8996, 9325 TLS Secure Transport Connection Profile

…

Servers shall support all of the following cipher suites for TLS 1.2. Clients shall support at least one of the cipher suites defined below.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

The following list of cipher suites may be used, but support is not mandatory for both servers and clients.

- TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384

- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CCM
- ~~**TLS_DHE_RSA_WITH_AES_256_GCM_CCM_8**~~ **TLS_DHE_RSA_WITH_AES_256_CCM_8**
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_AES_128_CCM_8

…