DICOM Correction Proposal

STATUS	Letter Ballot
Date of Last Update	2024/01/14
Person Assigned	R Horn
Submitter Name	Lawrence Tarbox (for WG-14), LRTarbox@uams.edu
Submission Date	2023/04/04

Correction Number CP-2312
Log Summary: Address late-breaking change to BCP-195
Name of Standard PS3.15
Rationale for Correction: Early implementers (notably Marco Eichelberg) pointed out that BCP-195 now also refers to RFC 9325, which obsoletes RFC 7525. RFC 9325 addresses certain vulnerabilities discovered in the use of RFC 7525. BCP-195 with RFC 9325 was issued during the ballot cycle for the new profiles. Since not many have implemented the new profiles, we felt it important to correct it early on. Note that this means ALPN will be required. That change to BCP-195 took place while we balloting the supplement. (The one implementer who tried to implement at that time was unable to incorporate ALPN. Now that we have an IANA number for DICOM, they have implemented ALPN.)
Correction Wording:

Remove the reference to 7525 in section 2 Normative References and add a reference to 9325

[RFC 6763] IETF. February 2013. *DNS-Based Service Discovery*. http://www.rfc-editor.org/info/rfc6763 .

~~**[RFC 7525] Sheffer Y, Holz R, and Saint-Andre P. May 2015. *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*. BCP 195. Updated by RFC 8996 and Errata. http://www.rfc-editor.org/info/rfc7525 .**~~

[RFC 8446] IETF. August 2018. *The Transport Layer Security (TLS) Protocol Version 1.3*. http://www.rfc-editor.org/info/rfc8446 .

[RFC 8553] IETF. *DNS AttrLeaf Changes: Fixing Specifications That Use Underscored Node Names*. http://www.rfc-editor.org/info/rfc8553 .

[RFC 8633] IETF. *RFC8633 Network Time Protocol Best Current Practices*. http://www.rfc-editor.org/info/rfc8633 .

[RFC 8996] Moriarty K and Farrell S. March 2021. *Deprecating TLS 1.0 and TLS 1.1*. BCP 195. http://www.rfc-editor.org/info/rfc8996 .

[RFC 9325] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, November 2022.

[BCP 195] IETF. *Information on BCP 195*. References ~~**RFC 7525 and**~~ RFC 8996 **and RFC 9325**. http://www.rfc-editor.org/info/bcp195 .

Swap the reference to 7525 with 9325 in Annex B12

B.12 BCP 195 RFC 8996, 9325 TLS SECURE TRANSPORT CONNECTION PROFILE

An implementation that supports the BCP 195 RFC 8996**, 9325** TLS Secure Transport Connection Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security protocol. It shall comply with [BCP 195] which includes [RFC 8996], and [RFC **9325** ~~**7525**~~] ~~**as modified by [RFC 8996]**~~. In the context of this profile, “client” refers to the entity initiating the TLS connection and “server” refers to the entity that is responding to that TLS connection initiation request. This may differ from the role that the entity might play in any DICOM transactions over the TLS connection.

Swap the reference to 7525 with 9325 in Annex B13

B.13 MODIFIED BCP 195 RFC 8996, 9325 TLS SECURE TRANSPORT CONNECTION PROFILE

An implementation that supports the Modified BCP 195 RFC 8996**, 9325** TLS Secure Transport Connection Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security protocol. It shall comply with [BCP 195] which includes [RFC 8996], and [RFC **9325** ~~**7525**~~] ~~**as modified by [RFC 8996]**~~ with the additional restrictions enumerated below. In the context of this profile, “client” refers to the entity initiating the TLS connection and “server” refers to the entity that is responding to that TLS connection initiation request. This may differ from the role that the entity might play in any DICOM transactions over the TLS connection.