# Digital Imaging and Communications in Medicine (DICOM)

*Supplement 230: Update BCP Secure Communications Profiles*

*Prepared by:*

**DICOM Standards Committee, Working Group 14**

1300 N. 17th Street, Suite 900

Rosslyn, Virginia 22209 USA

Status: Public Comment, June 28, 2022

Developed pursuant to DICOM Work Item 2021-12-02A

# Table of Contents

## Document History

| | | | |
|---|---|---|---|
| 2022/01/22 | Version 0 | LRT | Initial version |
| 2022/03/28 | Version 1 | LRT | Incorporating comments from March WG-06 meeting, plus additional cleanup |
| 2022/04/26 | Version 2 | LRT | Incorporating Japanese recommendations, some cleanup, plus incorporating changes discussed in the April WG-14 meeting |
| 2022/05/24 | Version 3 | LRT | Incorporating suggestions by WG members, including reviews from Japan and Rob Horn, as discussed in the May WG-14 meeting |
| 2022/06/23 | Version 4 | KD | Edits made during the WG-06 meeting. |
| 2022/06/28 | Public Comment | LRT | Edits before going to public comment. |

## Open Issues

| | |
|---|---|
| 10 | Should these profiles address client authentication?<br>Neither of the new profiles mention anything about bi-directional mutual authentication, which is explicitly called for in the IHE ATNA profile. The profile could mention the topic but not make any normative requirements.  Or we could double the number of profiles (one with mutual bidirectional authenticate required, one without) to make it more convenient to determine from the conformance claim what the implementation supports.  An implementation could theoretically support both, but then the conformance statement should clarify when one is used over the other. |

## Closed Issues

| | |
|---|---|
| 1 | Should the profiles be modified, or should old ones be retired and replaced by new ones?<br>**Decision:** This supplement proposes to retire and replace. |
| 2 | Should we wait to incorporate the ongoing syslog discussions?<br>IETF has an ongoing syslog discussion regarding BCP 195 and syslog.  It is not clear whether or not the changes being discussed would impact the DICOM secure transport profile.  If they issue a new RFC before this supplement is finalized, and if the changes would impact the secure transport profiles, we should add the changes.<br>**Decision:** Don’t wait.  If there is an impact, address at a later date. |
| 3 | Should we refer to BCP-195 generically, just saying, ‘look at BCP to see the latest RFPs that apply? |

| | |
|---|---|
| | In the future should we just require some write-up in the conformance statement about which RFCs referred to by BCP an implementation supports instead of trying to track BCP-195 through changing profiles? Or switch to something where we are not tracking a changing BCP 195 set of standards? Of course, since BCP-195 does not change that often, maybe creating new profiles every half decade or so is not that problematic.<br>**Decision:** BCP is updating at about 5 year intervals. That seems appropriate for just reviewing and creating new profiles as appropriate. |
| 5 | Should the extended BCP profile allow use of TLS versions newer than 1.3?<br>For the extended BCP profile, the document currently allows versions of TLS newer than TLS 1.3. However, the original source documents from Japan do not mention this. Is it OK to allow for newer TLS versions, or does that present an interoperability issue? Perhaps we should explicitly state 'server implementations shall support TLS 1.3' leaving newer versions optional?<br>Japan comment:<br>In the future, when new versions of TLS become available, the Cryptrec/IPA guidelines should be updated to specify the requirements for using the new versions of TLS. Therefore, we do not believe that new TLS versions should be mentioned at this time.<br>**Decision:** Chose to not explicitly call out support of newer versions, instead making the existing versions required by the server. This does allow negotiating newer versions (often happens automatically) if both server and client agree. |
| 6 | Should the extended BCP profile allow use of newer cryptographic algorithms?<br>For the extended BCP profile, the suggestion from the Japanese source documents is that only the listed, approved cryptographic algorithms and cipher suites may be used, which is good for interoperability. But should that be relaxed to allow for optional support of more modern algorithms if they appear?<br>Japan comment:<br>Should not be mentioned for the same reasons as in Open Issue 5.<br>**Decision:** see issue 5 |
| 7 | Should the extended BCP profile explicitly disallow unsafe cryptographic algorithms?<br>The extended BCP profile outlines what cryptographic algorithms cannot be used. This may be unnecessary since the underlying RFCs do not mention them as being allowed. However, the underlying RFCs do not strictly forbid them, and many toolkits support them. We decided to call them out specifically a subtle reminder to implementers to turn them off. Is that OK?<br>**Decision:** Keep the 'cannot be used' list in the profile. |
| 8 | Is listing both the allowed cryptographic algorithms and the required cypher suites redundant?<br>The extended BCP profile lists both the allowed cryptographic algorithms and what combinations are allowed as cipher suites in which TLS protocol versions. This is a bit redundant but may make clearer what is or isn't allowed. Should we toss one of the two representations out? Or pick one as normative and turn the other into a note?<br>Japan comment: |

| | |
|---|---|
| | The cipher suite whitelist does not include cipher suites consisting of all combinations of cipher algorithms recommended for use. This may be redundant, but we have not been able to determine if there is any impact by removing the list.<br>**Decision:** Leave both lists in, but the general list becomes more informational, whereas support of specific combinations are required. This leaves the negotiation of key exchange and signature algorithm open, as it is in BCP. The two sides can choose whichever key exchange and signature algorithm they have in common, as long as they do not chose ones in the excluded list. |
| 9 | Do we need DTLS 1.2 in the references?<br>The BCP also specifies use of DTLS 1.2, which is a UDP-based protocol. We do not explicitly mention it in the profiles, but we do include the older version in the references section. Is there any part of DICOM that uses UDP which warrants a more explicit mention of DTLS? If not, we should remove the DTLS reference. If yes, we need to update the DTLS reference.<br>**Decision:** Remove the DTLS reference, since DICOM does not use it. |
| 11 | Should we add to the defined terms section terminology from the RFCs that is used in the profiles?<br>Should we retain references that are indirect from other RFCs? In particular, for base RFCs like this one, should it be retained?<br>**Decision:** No. Keep to direct references and add 2nd order if REALLY useful. |

# Scope and Field of Application

This Supplement adds two new Secure Transport Connection Profiles and retires several others.

The IETF recently updated the Best Current Practice document called BCP-195. The new document no longer allows downgrading to TLS 1.0 or 1.1, which necessitates DICOM retiring Secure Transport Connection Profiles that are based on those protocols. The new version of BCP-195 is more in line with DICOM's B.10 Non-Downgrading BCP 195 Secure Transport Connection Profile.

In addition, the Japanese government has modified their guidelines for "high-security type" devices, hence the old Extended BCP 195 profile (B.11) is also now out of date, needs to be retired, and a new profile created that reflects the new revisions.

# Part 15

***Modify Section 2 Bibliography as shown***

# 2 Normative References

[ECMA 235] ECMA. March 1996. *The ECMA GSS-API Mechanism*. http://www.ecma-international.org/publications/standards/Ecma-235.htm .

~~**[ANSI X9.52] ANSI. 1998. *Triple Data Encryption Algorithm Modes of Operation*.**~~

[DNS-SD] Cheshire S.. *DNS Self-Discovery*. http://www.dns-sd.org/ .

~~**[FIPS 46] National Institute of Standards and Technology. *Data Encryption Standard (DES)*.**~~

~~**[FIPS 81] National Institute of Standards and Technology. *DES Modes of Operation*.**~~

[FIPS 180-1] National Institute of Standards and Technology. 17 April 1995. *SHA-1: Secure Hash Standard*.

[FIPS 180-2] National Institute of Standards and Technology. 1 August 2002. *SHA-2: Secure Hash Standard*.

~~**[ISCL V1.00] MEDIS-DC. *Integrated Secure Communication Layer V1.00*.**~~

[ITU-T X.509] ITU. *Information technology - Open Systems Interconnection - The directory: Public-key and attribute certificate frameworks*. http://www.itu.int/rec/T-REC-X.509 . ITU-T Recommendation X.509 is similar to ISO/IEC 9594-8 1990. However, the ITU-T recommendation is the more familiar form, and was revised in 1993 and 2000, with two sets of corrections in 2001. ITU-T was formerly known as CCITT..

[RFC 1035] IETF. *Domain Name System (DNS)*. http://tools.ietf.org/html/rfc1035 .

[RFC 2030] IETF. *Simple Network Time Protocol (SNTP) Version 4*. http://tools.ietf.org/html/rfc2030 .

[RFC 2131] IETF. *Dynamic Host Configuration Protocol*. http://tools.ietf.org/html/rfc2131 .

[RFC 2132] IETF. *Dynamic Host Configuration Protocol Options*. http://tools.ietf.org/html/rfc2132 .

[RFC 2136] IETF. *Dynamic Updates in the Domain Name System (DNS UPDATE)*. http://tools.ietf.org/html/rfc2136 .

[RFC 2181] IETF. *Clarifications to the DNS Specification*. http://tools.ietf.org/html/rfc2181 .

[RFC 2219] IETF. *Use of DNS Aliases for Network Services*. http://tools.ietf.org/html/rfc2219 .

~~**[RFC 2246] IETF. *Transport Layer Security (TLS) 1.0 Internet Engineering Task Force*. TLS is derived from SSL 3.0, and is largely compatible with it.. http://tools.ietf.org/html/rfc2246 .**~~

[RFC 2251] IETF. *Lightweight Directory Access Protocol (v3)*. http://tools.ietf.org/html/rfc2251 .

[RFC 2313] IETF. March 1998. *PKCS #1: RSA Encryption, Version 1.5*. http://tools.ietf.org/html/rfc2313 .

[RFC 2437] IETF. October 1998. *PKCS #1: RSA Cryptography Specifications - Version 2.0*. http://tools.ietf.org/html/rfc2437 .

[RFC 2563] IETF. *DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients*. http://tools.ietf.org/html/rfc2563 .

[RFC 2782] IETF. *A DNS RR for specifying the location of services (DNS SRV)*. http://tools.ietf.org/html/rfc2782 .

[RFC 2827] IETF. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. http://tools.ietf.org/html/rfc2827 .

[RFC 2849] IETF. *The LDAP Data Interchange Format (LDIF)*. http://tools.ietf.org/html/rfc2849 .

[RFC 2898] IETF. September 2000. *PKCS #5: Password-Based Cryptography Specification Version 2.0*. http://tools.ietf.org/html/rfc2898 .

[RFC 3161] IETF. March 2000. *Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)*. http://tools.ietf.org/html/rfc3161 .

[RFC 3164] IETF. August 2001. *The BSD syslog Protocol*. http://tools.ietf.org/html/rfc3164 .

[RFC 3211] IETF. December 2001. *Password-based Encryption for CMS*. http://tools.ietf.org/html/rfc3211 .

[RFC 3268] IETF. June 2002. *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*. http://tools.ietf.org/html/rfc3268 .

[RFC 3447] IETF. February 2003. *PKCS #1 RSA Cryptography Specifications Version 2.1*. http://tools.ietf.org/html/rfc3447 .

[RFC 3370] IETF. August 2002. *Cryptographic Message Syntax (CMS) Algorithms*. http://tools.ietf.org/html/rfc3370 .

[RFC 3565] IETF. July 2003. *Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)*. http://tools.ietf.org/html/rfc3565 .

[RFC 3851] IETF. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*. http://tools.ietf.org/html/rfc3851 .

[RFC 3853] IETF. *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)*. http://tools.ietf.org/html/rfc3853 .

[RFC 3881] IETF. September 2004. *Security Audit and Access Accountability Message - XML Data Definitions for Healthcare Applications*. http://tools.ietf.org/html/rfc3881 .

[RFC 4033] IETF. March 2005. *DNS Security Introduction and Requirements*. http://tools.ietf.org/html/rfc4033 .

[RFC 4034] IETF. March 2005. *Resource Records for the DNS Security Extensions*. http://tools.ietf.org/html/rfc4034 .

[RFC 4035] IETF. March 2005. *Protocol Modifications for the DNS Security Extensions*.

~~**[RFC 4346] IETF. April 2006. *The Transport Layer Security (TLS) Protocol - Version 1.1*. http://tools.ietf.org/html/rfc4346 .**~~

~~**[RFC 4347] IETF. April 2006. *Datagram Transport Layer Security*. http://tools.ietf.org/html/rfc4347 .**~~

[RFC 5246] IETF. August 2008. *The Transport Layer Security (TLS) Protocol Version 1.2*. http://tools.ietf.org/html/rfc5246 .

[RFC 5424] IETF. *The Syslog Protocol*. http://tools.ietf.org/html/rfc5424 .

[RFC 5425] IETF. *Transport Layer Security (TLS) Transport Mapping for Syslog*. http://tools.ietf.org/html/rfc5425 .

[RFC 5426] IETF. *Transmission of Syslog Messages over UDP*. http://tools.ietf.org/html/rfc5426 .

[RFC 5652] IETF. September 2009. *Cryptographic Message Syntax*. http://tools.ietf.org/html/rfc5652 .

[RFC 5905] IETF. *Network Time Protocol Version 4: Protocol and Algorithms Specification*. http://tools.ietf.org/html/rfc5905 .

[RFC 5906] IETF. *Network Time Protocol Version 4: Autokey Specification*. http://tools.ietf.org/html/rfc5906 .

[RFC 6762] IETF. February 2013. *Multicast DNS*. http://tools.ietf.org/html/rfc6762 .

[RFC 6763] IETF. February 2013. *DNS-Based Service Discovery*. http://tools.ietf.org/html/rfc6763 .

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

[RFC 8446] IETF. August 2018. *The Transport Layer Security (TLS) Protocol Version 1.3*. http://tools.ietf.org/html/rfc8446 .

[RFC 8553] IETF. *DNS AttrLeaf Changes: Fixing Specifications That Use Underscored Node Names*. http://tools.ietf.org/html/rfc8553 .

[RFC 8633] IETF. *RFC8633 Network Time Protocol Best Current Practices*. http://tools.ietf.org/html/rfc8633 .

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

[BCP 195] **IETF, *Best Community Practices 195*, https://www.rfc-editor.org/info/bcp195 (References RFC 7525 and RFC 8996)** ~~**IETF. *Recommendations for Secure Use of Transport Layer***~~

~~***Security (TLS) and Datagram Transport Layer Security (DTLS).***~~
~~**https://tools.ietf.org/html/bcp195.**~~

[CRYPTREC] CRYPTREC: Cryptography Research and Evaluation Committees, Japan, https://www.cryptrec.go.jp/en/index.html

[IPA] IPA: Information-technology Promotion Agency, Japan, https://www.ipa.go.jp/index-e.html

***Modify Section B.3***

### B.3 AES TLS Secure Transport Connection Profile

Retired. See PS3.15 2018a.

~~**Note**~~

~~**Applications implementing the AES TLS Secure Transport Connection Profile will connect and interoperate with implementations of the BCP 195 TLS Profile; see Section B.9 "BCP 195 TLS Secure Transport Connection Profile".**~~

***Modify Section B.9***

### B.9 BCP 195 TLS Secure Transport Connection Profile

**Retired. See PS3.15 <insert revision date>**

~~**An implementation that supports the [BCP 195] TLS Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security protocol. It shall comply with [BCP 195] from the IETF.**~~

~~**Note**~~

~~**1. [BCP 195] is currently also published as [RFC 7525]. Both provide suggestions for proper use of TLS 1.2 and allow appropriate fallback rules.**~~

~~**2. Existing implementations that are compliant with the DICOM AES TLS Secure Connection Profile are able to interoperate with this profile. This profile adds significant recommendations by the IETF, but does not make them mandatory. This is the IETF recommendation for upgrading an installed base.**~~

~~**3. A device may support multiple different TLS profiles. DICOM does not specify how such devices are configured in the field or how different TLS profile-related rules are specified. The site will determine what configuration is appropriate.**~~

~~**4. The DICOM profiles for TLS describe the capabilities of a product. Product configuration may permit selection of a particular profile and/or additional negotiation rules. The specific ciphersuite used is negotiated by the TLS implementation based on these rules.**~~

~~**5. TLS 1.2 [RFC 5246] and TLS 1.3 [RFC 8446] incorporate requirements for cipher suites, signature methods, etc.**~~

~~**TCP ports on which an implementation accepts TLS connections, or the mechanism by which these port numbers are selected or configured, shall be stated in the Conformance Statement. The TCP ports on which an implementation accepts TLS connections for DICOMweb shall be different**~~

**~~from those on which an implementation accepts TLS connections for DIMSE. The HTTP/HTTPS connection for DICOMweb can be shared with other HTTP/HTTPS traffic.~~**

**~~Note~~**

**~~It is recommended that systems supporting the BCP 195 TLS Profile use the registered port number "2762 dicom-tls" for the DICOM Upper Layer Protocol on TLS.~~**

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

**~~Implementers should take care to manage the risks of downgrading to less secure obsolescent protocols or cleartext protocols. See [BCP 195], Section 5.2 "Opportunistic Security".~~**

***Modify Section B.10***

### B.10 Non-Downgrading BCP 195 TLS Secure Transport Connection Profile

Retired.  See PS3.15 <insert revision date>

**~~An implementation that supports the Non-Downgrading BCP 195 TLS Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security protocol. It shall comply with [BCP 195] from the IETF with the additional restrictions enumerated below.~~**

**~~Note~~**

**~~1. A device may support multiple different TLS profiles. DICOM does not specify how such devices are configured in the field or how different TLS profile-related rules are specified. The site will determine what configuration is appropriate.~~**

**~~2. The DICOM profiles for TLS describe the capabilities of a product. Product configuration may permit selection of a particular profile and/or additional negotiation rules. The specific ciphersuite used is negotiated by the TLS implementation based on these rules.~~**

**~~The following additions are made to [BCP 195] requirements. They change some of the "should" recommendations in the RFC into requirements.~~**

**~~• Implementations shall not negotiate TLS version 1.1 [RFC 4346] or TLS version 1.0 [RFC 2246]~~**

**~~• Implementations shall not negotiate DTLS version 1.0 [RFC 4347]~~**

**~~• In cases where an application protocol allows implementations or deployments a choice between strict TLS configuration and dynamic upgrade from unencrypted to TLS-protected traffic (such as STARTTLS), clients and servers shall prefer strict TLS configuration.~~**

**~~• Application protocols typically provide a way for the server to offer TLS during an initial protocol exchange, and sometimes also provide a way for the server to advertise support for TLS (e.g., through a flag indicating that TLS is required); unfortunately, these indications are sent before the communication channel is encrypted. A client shall attempt to negotiate TLS even if these indications are not communicated by the server.~~**

- ~~The following cipher suites shall all be supported:~~
- ~~TLS_DHE_RSA_WITH_AES_128_GCM_SHA256~~
- ~~TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256~~
- ~~TLS_DHE_RSA_WITH_AES_256_GCM_SHA384~~
- ~~TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384~~
- ~~Additional cipher suites of similar or greater cryptographic strength may be supported.~~

~~TCP ports on which an implementation accepts TLS connections, or the mechanism by which these port numbers are selected or configured, shall be stated in the Conformance Statement. The TCP ports on which an implementation accepts TLS connections for DICOMweb shall be different from those on which an implementation accepts TLS connections for DIMSE. The HTTP/HTTPS connection for DICOMweb can be shared with other HTTP/HTTPS traffic.~~

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

~~Note~~

~~It is recommended that systems supporting the Non-Downgrading BCP 195 TLS Profile use the registered port number "2762 dicom-tls" for the DICOM Upper Layer Protocol on TLS. If both the Non-Downgrading BCP 195 TLS Profile and the BCP 195 TLS Profile are supported, it is recommended that they use the well known port numbers on different IP addresses.~~

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

~~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.~~

*Modify Section B.11*

## B.11 Extended BCP 195 TLS Profile Secure Transport Connection Profile

Retired. See PS3.15 <insert revision date>

~~An implementation that supports the Extended BCP 195 Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security protocol. It shall comply with [BCP 195] from the IETF with the additional restrictions enumerated below.~~

~~Note~~

~~1. A device may support multiple different TLS profiles. DICOM does not specify how such devices are configured in the field or how different TLS profile-related rules are specified. The site will determine what configuration is appropriate.~~

~~2. The DICOM profiles for TLS describe the capabilities of a product. Product configuration may permit selection of a particular profile and/or additional negotiation rules. The specific ciphersuite used is negotiated by the TLS implementation based on these rules.~~

~~**The following additions are made to [BCP 195] requirements. They change some of the "should" recommendations in the RFC into requirements.**~~

- ~~**Implementations shall not negotiate TLS version 1.1 [RFC 4346] or TLS version 1.0 [RFC 2246]**~~

- ~~**Implementations shall not negotiate DTLS version 1.0 [RFC 4347]**~~

- ~~**In cases where an application protocol allows implementations or deployments a choice between strict TLS configuration and dynamic upgrade from unencrypted to TLS-protected traffic (such as STARTTLS), clients and servers shall prefer strict TLS configuration.**~~

- ~~**Application protocols typically provide a way for the server to offer TLS during an initial protocol exchange, and sometimes also provide a way for the server to advertise support for TLS (e.g., through a flag indicating that TLS is required); unfortunately, these indications are sent before the communication channel is encrypted. A client shall attempt to negotiate TLS even if these indications are not communicated by the server.**~~

- ~~**The following cipher suites shall all be supported:**~~

- ~~**TLS_DHE_RSA_WITH_AES_128_GCM_SHA256**~~

- ~~**TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**~~

- ~~**TLS_DHE_RSA_WITH_AES_256_GCM_SHA384**~~

- ~~**TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**~~

- ~~**One or more of the following cipher suites should be supported:**~~

- ~~**TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384 (0xC0, 0x7D)**~~

- ~~**TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256 (0xC0,0x7C)**~~

- ~~**TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0,0x2C)**~~

- ~~**TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384 (0xC0,0x87)**~~

- ~~**TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384 (0xC0,0x8B)**~~

- ~~**TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0,0x2B)**~~

- ~~**TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256 (0xC0,0x86)**~~

- ~~**TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256 (0xC0,0x8A)**~~

- ~~**No other cipher suites shall be used.**~~

- ~~**When DHE is used by key exchange, the key length shall be 2048 bits or more.**~~

- ~~**When ECDHE is used by key exchange, the key length shall be 256 bits or more.**~~

~~**TCP ports on which an implementation accepts TLS connections, or the mechanism by which these port numbers are selected or configured, shall be stated in the Conformance Statement. The TCP ports on which an implementation accepts TLS connections for DICOMweb shall be different from those on which an implementation accepts TLS connections for DIMSE. The HTTPS connection for DICOMweb can be shared with other HTTP/HTTPS traffic.**~~

~~**Note**~~

~~**It is recommended that systems supporting the Extended BCP 195 TLS Profile use the registered port number "2762 dicom-tls" for the DICOM Upper Layer Protocol on TLS.**~~

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

~~**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.**~~

***Add Section B.12***

### B.12 BCP 195 RFC 8996 TLS Secure Transport Connection Profile

An implementation that supports the BCP 195 RFC 8996 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 7525] as modified by [RFC 8996].

Note

1. A device may support multiple TLS profiles. DICOM does not specify how such devices are configured in the field or how different TLS profile-related rules are specified. The site will determine what configuration is appropriate.
2. Whenever possible, TLS 1.3 or higher is preferred.
3. The DICOM profiles for TLS describe the capabilities of a product. Product configuration may permit selection of a particular profile and/or additional negotiation rules. The specific ciphersuite used is negotiated by the TLS implementation based on these rules.

In cases where an application protocol allows implementations or deployments a choice between strict TLS configuration and dynamic upgrade from unencrypted to TLS-protected traffic (such as STARTTLS), clients and servers shall prefer strict TLS configuration.

Application protocols typically provide a way for the server to offer TLS during an initial protocol exchange, and sometimes also provide a way for the server to advertise support for TLS (e.g., through a flag indicating that TLS is required). Unfortunately, these indications are sent before the communication channel is encrypted.

A client shall attempt to negotiate TLS even if the above indications are not communicated by the server.

The following cipher suites shall all be supported:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Additional cipher suites of similar or greater cryptographic strength may be supported.

The TCP ports on which an implementation accepts TLS connections for DICOMweb shall be different from those on which an implementation accepts TLS connections for DIMSE. The HTTP/HTTPS connection for DICOMweb can be shared with other HTTP/HTTPS traffic.

Note

It is recommended that systems supporting this Profile use the registered port number "2762 dicom-tls" for the DICOM Upper Layer Protocol on TLS.

The Conformance Statement shall indicate:

- TCP ports on which an implementation accepts TLS connections, or the mechanism by which these port numbers are selected or configured
- what mechanisms the implementation supports for Key Management.

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.

***Add Section B.13***

### B.13 Extended BCP 195 RFC 8996 TLS Secure Transport Connection Profile

An implementation that supports the Extended BCP 195 RFC 8996 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 7525] as modified by [RFC 8996] with the additional restrictions enumerated below.

Note

1. A device may support multiple TLS profiles. DICOM does not specify how such devices are configured in the field or how different TLS profile-related rules are specified. The site will determine what configuration is appropriate.
2. The DICOM profiles for TLS describe the capabilities of a product. Product configuration may permit selection of a particular profile and/or additional negotiation rules. The specific ciphersuite used is negotiated by the TLS implementation based on these rules.

Servers shall support both TLS 1.2 and TLS 1.3. Clients only need to support one of them. TLS 1.3 shall be the preferred protocol version. Implementations may fall back to TLS 1.2 if the client does not support TLS 1.3.

In cases where an application protocol allows implementations or deployments a choice between strict TLS configuration and dynamic upgrade from unencrypted to TLS-protected traffic (such as STARTTLS), clients and servers shall prefer strict TLS configuration.

Application protocols typically provide a way for the server to offer TLS during an initial protocol exchange, and sometimes also provide a way for the server to advertise support for TLS (e.g., through a flag indicating that TLS is required); unfortunately, these indications are sent before the communication channel is encrypted.

A client shall attempt to negotiate TLS even if the above indications are not communicated by the server.

The following cryptographic algorithms shall <u>not</u> be used:

- Key Exchange
  - DH
  - ECDH
  - RSAES PKCS#1 v1.5 (RSA)
- Signature
  - GOST R 34.10-2012
- Block Cipher

  - RC2
  - EXPORT-RC2
  - IDEA
  - DES
  - EXPORT-DES
  - GOST 28147-89
  - Magma
  - 3-key Triple DES
  - Kuznyechik
  - ARIA
  - SEED
- Block Cipher Mode of Operation
  - CBC
  - CTR-OMAC
- Stream Cipher
  - RC4, EXPORT-RC4
- Hash Function
  - MD5
  - SHA-1
  - GOST R 34.11-2012

The following cryptographic algorithms are permitted:

- Key Exchange
  - ECDHE
  - DHE
- Signature
  - ECDSA
  - RSASSA PKCS#1 v1.5 (RSA)
  - RSASSA-PSS
- Block Cipher
  - AES
  - Camellia
- Block Cipher Mode of Operation
  - GCM
  - CCM
  - CCM_8
- Stream Cipher
  - ChaCha20-Poly 1305
- Hash Function
  - SHA-256
  - SHA-384

When DHE is used for Key Exchange, the key length shall be 2048 bits or more. Cipher suites containing DHE shall not be selected when using implementations that do not allow explicit setting of the DHE key length.

When ECDHE is used for Key Exchange, the key length shall be 256 bits or more.

Servers shall support all of the following cipher suites for TLS 1.3. Clients that support TLS 1.3 may choose any of the following cipher suites.

- TLS-AES_256-GCM-SHA384
- TLS_CHACHA20_POLY1305_SHA256

- TLS_AES_128-GCM_SHA256
- TLS_AES_128-CCM_SHA256
- TLS_AES_128-CCM_8_SHA256

Note: In TLS 3.0 Key Exchange and Signature, algorithms are not specified in the cipher suite negotiation. Implementations may choose from the allowed list above.

Servers shall support all of the following cipher suites for TLS 1.2. Clients that support TLS 1.2 may choose any of the following cipher suites.

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CAMELLIA_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_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM-8

The above cipher suites are preferred. Support for the following cipher suites is permitted as a fallback but not required.

- 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_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

When using TLS 1.2, cipher suites other than those listed above are not permitted.

The following requirements apply to Certificates:

- If the subject public key algorithm is RSA, the key length shall be 2048 bits or more.
- If the subject public key algorithm is ECC, the key length shall be 256 bits or more.
- If the certificate signature algorithm is RSA, the key length shall be 2048 bits or more.
- If the certificate signature algorithm is ECDSA, the key length shall be 256 bits or more.
- The hash function shall be SHA-256 or greater.

The TCP ports on which an implementation accepts TLS connections for DICOMweb shall be different from those on which an implementation accepts TLS connections for DIMSE. The HTTP/HTTPS connection for DICOMweb can be shared with other HTTP/HTTPS traffic.

Note

> It is recommended that systems supporting this Profile use the registered port number "2762 dicom-tls" for the DICOM Upper Layer Protocol on TLS.

The Conformance Statement shall indicate:

- TCP ports on which an implementation accepts TLS connections, or the mechanism by which these port numbers are selected or configured
- what mechanisms the implementation supports for Key Management.

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.