Digital Imaging and Communications in Medicine (DICOM)

Supplement 206 – Extended BCP195 TLS Profile

Prepared by:

DICOM Standards Committee, Working Group 6

1300 N. 17th Street

Rosslyn, Virginia 22209 USA

VERSION: Final Text, 2018/11/09

Developed pursuant to DICOM Work Item 2017-04-D

Table of Contents

Scope and Field of Application

This supplement adds a new Secure Connection profile to make DICOM consistent with the latest recommendations from the Japanese CRYPTREC committee by recommending support for all the ciphersuites included in the CRYPTREC recommendation.

The Extended BCP195 TLS Profile requires compliance with the IETF BCP195 Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) plus support for the additional cypher suites specified by the CRYPTREC committee. This profile requires that TLS negotiation start with the strong security protection parameters, and allows progressive negotiation of weaker protection down to a specified minimum protection limit.

The CRYPTREC Committee validated the strength of cipher suites and identified 12 cipher suites that can be used with TLS 1.2, including some cipher suites not included in BCP195. In addition, a key length requirement that is stricter than BCP195 is specified.

Changes to NEMA Standards Publication PS 3.15-2018d

Digital Imaging and Communications in Medicine

Modify Section 2, Normative References

RFC3853 S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)

RFC5246 Transport Layer Security (TLS) 1.2

RFC5424 The Syslog Protocol

CRYPTREC (Cryptography Research and Evaluation Committee) GL-3001-2.0 “Guidelines for Configuration of SSL/TLS Ver 2.0” (2018.5) http://www.cryptrec.go.jp/report/cryptrec-gl-3001-2.0.pdf (Japanese only)

…

Modify Annex B.9, BCP195 TLS SECURE TRANSPORT CONNECTION PROFILE

B.9 BCP195 TLS SECURE TRANSPORT CONNECTION PROFILE

An implementation that supports the BCP195 TLS Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security protocol. It shall comply with BCP195 from the IETF.

Note

1. BCP195 is currently also published as RFC7525 Recommendations for Secure Use of Transport Layer Security (TLS). 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.**

Modify Annex B.10 NON-DOWNGRADING BCP195 TLS SECURE TRANSPORT CONNECTION PROFILE

B.10 NON-DOWNGRADING BCP195 TLS SECURE TRANSPORT CONNECTION PROFILE

An implementation that supports the Non-Downgrading BCP195 TLS Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security protocol. It shall comply with BCP195 from the IETF with the additional restrictions enumerated below.

Notes:

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.**

Add Annex B.11 Extended BCP195 TLS Profile Secure Transport Connection Profile

B.11 EXTENDED BCP195 TLS PROFILE SECURE TRANSPORT CONNECTION PROFILE

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 BCP195 from the IETF with the additional restrictions enumerated below.

Notes: 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 BCP195 requirements. They change some of the "should" recommendations in the RFC into requirements.

- Implementations shall not negotiate TLS version 1.1 [RFC4346] or TLS version 1.0 [RFC2246]
- Implementations shall not negotiate DTLS version 1.0 [RFC4347]
- 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 BCP195 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.