Digital Imaging and Communications in Medicine (DICOM)

Supplement 204 – TLS Security Profiles

Prepared by:

DICOM Standards Committee, Working Group 6
1300 N. 17th Street
Rosslyn, Virginia 22209 USA

VERSION: Public Comment Draft 9 September, 2017

This is a draft document. Do not circulate, quote, or reproduce it except with the approval of NEMA.
Developed pursuant to DICOM Work Item 2017-04-D
Table of Contents

Scope and Field of Application ................................................................................................. i
Changes to NEMA Standards Publication PS 3.15-2017d......................................................... ii
B.Y THE BCP195 TLS PROFILE............................................................................................... 2
B.X THE NON-DOWGRADING BCP195 TLS PROFILE......................................................... 2

Scope and Field of Application

Two new Secure Connection profiles are added to make DICOM consistent with the latest RFCs and best practices for TLS security. These are:

1. A BCP195 TLS Profile that requires compliance with the IETF BCP 195 Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS).
   This profile requires that TLS negotiation start with the strong security protection parameters, and allows progressive negotiation of weaker protection down to a minimum protection limit.

2. A Non-Downgrading BCP195 TLS Profile that does not permit negotiation of weaker protections.
   This profile will refuse a connection that is not the initial strong level of protection.

The old Basic TLS Secure Transport Connection Profile is retired. IETF considers it inadequate security, because the methods for breaking in are well known. Implementations that use it will not interoperate with the BCP195 TLS Profile.

The old AES TLS Secure Transport Connection Profile is retired. Implementations that use it will not interoperate with the Non-Downgrading BCP195 TLS Profile. Implementations that use it will interoperate with the BCP195 TLS Profile because it is acceptable as one of the lower levels of protection that can be negotiated.

The old ISCL Secure Transport Connection Profile is retired.

A concern was raised that future changes to BCP195 may lead to compliance problems or interoperability problems. The IETF policies have been to preserve interoperability as a very high priority, and to change the standard's ID when a non-interoperable is made. This is reflected in the design of BCP195. It preserves interoperability with all of the versions of TLS issued since 1999. Systems using these older versions cannot claim compliance with BCP195, but BCP195 includes a specified downgrade sequence in the connection negotiation so that a BCP195 compliant system will continue to be able to communicate using the older TLS version.

When an incompatible change is made, another DICOM profile will need to be defined. This does not appear likely in the near term.
Changes to NEMA Standards Publication PS 3.15-2017d

Digital Imaging and Communications in Medicine

Modify Section 2, Normative References


RFC5246 Transport Layer Security (TLS) 1.2


RFC5424 The Syslog Protocol

Replace Annex B.1 as shown

B.1 The Basic TLS Secure Transport Connection Profile

Retired, see PS 3.15, 2017x

Replace Annex B.3 as shown

B.3 The AES TLS Secure Transport Connection Profile

Retired, see PS 3.15, 2017x

Note: applications implementing the AES TLS Secure Transport Connection Profile will connect and interoperate with implementations of the BCP195 TLS Profile, see B.y.

Replace Annex B.2 as shown

B.2 ISCL Secure Transport Connection Profile

Retired, see PS 3.15, 2017x

Add Annex B.y, BCP195 TLS Profile
B.Y THE BCP195 TLS 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.

IP 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 IP 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 strongly recommended that systems supporting the 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.

The profile does not specify a key management infrastructure. The conformance statements for the AE’s document how each AE can perform key management, e.g., certificate provisioning. If there is a common key management solution, then this profile assures that connections can be established.

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 Annex B.x

B.X THE NON-DOWNGRADING BCP195 TLS 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.

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 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

  Note: Additional cipher suites are permitted in the negotiation.

IP 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 IP 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 strongly recommended that systems supporting the BCP195 TLS Profile use the registered port number "2762 dicom-tls" for the DICOM Upper Layer Protocol on TLS. If both BCP195 TLS Profile and the Non-Downgrading BCP195 TLS Profile are supported, it is recommended that they use different port numbers.

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

The profile does not specify a key management infrastructure. The conformance statements for the AE's document how each AE can perform key management, e.g., certificate provisioning. If there is a common key management solution, then this profile assures that connections can be established.

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.