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: Final Text, 23 March 2018

Developed pursuant to DICOM Work Item 2017-04-D

Table of Contents

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. This does not make implementations that conform to the Basic TLS Profile non-compliant with DICOM. It means that DICOM will no longer update or encourage use of this profile.

The motivations for this are multiple:

1) Regulations and recommendations from US-FIPS, US-NIST (800-43 rev1), IETF, UK, and others are that more current versions of TLS be used. As of 2017 the US regulations for government purchases and recommendations for public use are that TLS 1.2 should be used, TLS 1.1 shall be supported, and TLS 1.0 may be used for compatibility with old systems that have not been upgraded. The draft updates for 800-43 indicate that it is likely to require that TLS 1.2 shall be supported on new purchases, and it may remove permission for use of TLS 1.0 within government networks. The motivations of the regulators and experts include:
   a. security problems with TLS 1.0 (see RFC 7457) and less significant problems with TLS 1.1. (The Basic TLS Secure Transport Connection Profile specifies TLS 1.0).
   b. implementation specific issues with some widely deployed implementations. These have bugs that are related to specific TLS versions that can be avoided by using more current versions.
   c. Configuration management concerns. It is easy to make mistakes when manually configuring TLS options. Some TLS implementations make it easy to mistakenly enable 56-bit DES or disable other important security features. Having a single good set of configuration options that is widely implemented and supported reduces the risks of configuration errors.
2) The DICOM Profiles provide a simple name for use during procurement. The profiles should be consistent with
   a. current regulations and recommendations,

b. future looking considerations based on advice from experts like NIST and IETF, and
c. installed base considerations like compatibility with existing equipment.

3) The DICOM Profiles need to consider what will lead to the fewest implementation and deployment mistakes. The Basic TLS Secure Transport Connection Profile is no longer a configuration that will be commonly requested or a standard configuration.

The old AES TLS Secure Transport Connection Profile is retired for the same reasons. Implementations that use it will interoperate with the BCP195 TLS Profile because it is one of the acceptable TLS 1.0 configurations that can be negotiated for legacy compatibility. Implementations that use it will not interoperate with the Non-Downgrading BCP195 TLS Profile.

The old ISCL Secure Transport Connection Profile is retired. The standard that it refers to has been withdrawn in Japan. A replacement profile is being developed under a different supplement.

The BCP 195 recommendation is acceptable for the current US-FIPS, US-NIST, IETF, UK, and many other government and commercial recommendations. These are expected to be updated. BCP195 is slightly stricter than some of these recommendations. For example, BCP195 says TLS 1.2 shall be supported, while US FIPS regulations currently say TLS 1.2 should be supported. BCP195 is expected to be a widely recognized name and a widely implemented configuration due to the influence of the many regulations and recommendations that it meets.

Some of the proposed government and existing commercial recommendations are more demanding. Some require disabling the downgrade to TLS 1.0 that is permitted by BCP 195. A few require disabling the downgrade to TLS 1.1 or disallow the negotiation some of the weaker encryption alternatives. The Non-Downgrading BCP 195 profile is a way to address these recommendations.

Some concerns were raised about the potential for IETF changing BCP 195 in a way that would invalidate these profiles. The IETF Process is explained in BCP 9 The Internet Standards Process, https://tools.ietf.org/html/bcp9. When an RFC or BCP is replaced by an incompatible version it also gets a new number. It may be retained as an old but valid RFC, like IPv4, or labelled historic. The historic label is similar to DICOM’s retired label. The IETF has a good history of following this practice carefully and replacing RFC’s only for very good reasons.

The IHE ATNA profile will need some editorial revision to reflect these changes. That CP will be submitted and refer to the BCP195 TLS Profile as a basic reference.

Changes to NEMA Standards Publication PS 3.15-2017d

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

[RFC7525] IETF. May 2015. Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). http://tools.ietf.org/html/rfc7525.

[BCP195] IETF. May 2015. Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). http://tools.ietf.org/html/bcp195.

…

Replace Annex B.1 as shown

B.1 THE BASIC TLS SECURE TRANSPORT CONNECTION PROFILE

Retired, see PS 3.15, 2017x

Replace Annex B.2 as shown

B.2 ISCL 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.

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.

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 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.

> 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.

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 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 BCP195 TLS Profile use the registered port number "2762 dicom-tls" for the DICOM Upper Layer Protocol on TLS. If both the Non-Downgrading BCP195 TLS Profile and the BCP195 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.