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........ i
B.Y THE BEST CURRENT PRACTICE TLS SECURE CONNECTION PROFILE 2
B.X THE BEST CURRENT PRACTICES PLUS RESTRICTIONS TLS SECURE TRANSPORT CONNECTION PROFILE........ 3

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 Best Practices 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 Best Practices 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 Best Practices TLS Profile.

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

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.

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 Best Practices TLS Profile, see B.y.

Add Annex B.y, Best Practices TLS Profile

B.Y THE BEST PRACTICES TLS PROFILE

An implementation that supports the Best Practices TLS Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security protocol. It shall comply with the BCP195 best current practices 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 best current practice 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. These ports shall be different from ports used for other types of transport connections (secure or unsecure).

Note: It is strongly recommended that systems supporting the Best Practices TLS Profile use the registered port number "2762 dicom-tls" for the DICOM Upper Layer Protocol on TLS: (decimal).

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

The profile does not further specify how a TLS Secure Transport Connection is established, or the significance of any certificates exchanged during peer entity authentication. These issues are left up to the Application Entity, which presumably is following some site specified security policy. The identities of the certificate owners can be used by the application entity for audit log support, or to restrict access based on some external access rights control framework. Once the Application Entity has established a Secure Transport Connection, then an Upper Layer Association can use that secure channel.

Note There may be an interaction between PDU size and TLS Record size that impacts efficiency of transport. The maximum allowed TLS record size is smaller than the maximum allowed PDU size.

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 BEST PRACTICES TLS PROFILE

An implementation that supports the Non Downgrading Best Practices TLS Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security protocol. It shall comply with the BCP195 best current practices 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

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. These ports shall be different from ports used for other types of transport connections (secure or unsecure).

Note: It is strongly recommended that systems supporting the Best Practices TLS Profile use the registered port number "2762 dicom-tls" for the DICOM Upper Layer Protocol on TLS: (decimal).

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

The profile does not further specify how a TLS Secure Transport Connection is established, or the significance of any certificates exchanged during peer entity authentication. These issues are left up to the Application Entity, which presumably is following some site specified security policy. The identities of the certificate owners can be used by the application entity for audit log support, or to restrict access based on some external access rights control framework. Once the Application Entity has established a Secure Transport Connection, then an Upper Layer Association can use that secure channel.

Note There may be an interaction between PDU size and TLS Record size that impacts efficiency of transport. The maximum allowed TLS record size is smaller than the maximum allowed PDU size.

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.