DICOM Correction Proposal

<table>
<thead>
<tr>
<th>STATUS</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Last Update</td>
<td>2016/09/11</td>
</tr>
<tr>
<td>Person Assigned</td>
<td>Robert Horn</td>
</tr>
<tr>
<td>Submitter Name</td>
<td>Victor Derks \ <a href="mailto:victor.derks@ge.com">victor.derks@ge.com</a></td>
</tr>
<tr>
<td>Submission Date</td>
<td>2013-12-6</td>
</tr>
</tbody>
</table>

Correction Number CP-1353

Log Summary: Secure Transport Connection Profile should allow higher TLS versions

Name of Standard
PS 3 2016c, Part 15

Rationale for Correction:
The DICOM standard defines a set of secure transport connection profiles. These profiles utilize the TLS 1.0 protocol. Newer versions of TLS have been released to address security weaknesses in older TLS versions (see for example http://en.wikipedia.org/wiki/Transport_Layer_Security). The DICOM standard still requires that TLS 1.0 needs to be used for the DICOM secure transport connection profiles. This result is a connection which has known security issues. By allowing higher versions DICOM systems can establish a more secure connection.

Note 1: TLS 1.2 is compatible with TLS 1.0, but to prevent connection problems systems should be able to use TLS 1.0 to connect to legacy systems.

Note 2: The SYSLOG-TLS profile (PS 3.5-2011, A.6.) already requires usage of TLS 1.2 or later.

Correction Wording:

Modify Section 2, Normative References


RFC5246 Transport Layer Security (TLS) 1.2

RFC5424 The Syslog Protocol

...  

RFC7525 Recommendations for Secure Use of Transport Layer Security (TLS)

Modify Annex B.1 as shown

An implementation that supports the Basic TLS Secure Transport Connection Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security Version 1.0 protocol. **TLS version 1.2 or later is recommended.** Table B.1-1 specifies mechanisms that shall be supported if the corresponding features within TLS are supported by the Application Entity.

Modify Annex B.1 as shown

Notes:
1. It is strongly recommended that systems supporting the Basic TLS Secure Transport Connection Profile use as their port the registered port number “2762 dicom-tls” for the DICOM Upper Layer Protocol on TLS: (decimal).

2. Earlier revisions of the standard required TLS 1.0. This version has known security weaknesses. It is up to the implementation to define the policy of accepting connections from systems that use TLS 1.0. RFC7525 Recommendations for Secure Use of Transport Layer Security (TLS) provides suggestions for proper use of TLS 1.2 and appropriate fallback rules.

Modify Annex B.3 The AES TLS Secure Transport Connection Profile

An implementation that supports the AES TLS Secure Transport Connection Profile shall utilize the framework and negotiation mechanism specified by the Transport Layer Security Version 1.0 protocol. **TLS version 1.2 or later is recommended.** Table B.3-1 specifies mechanisms that shall be supported if the corresponding features within TLS are supported by the Application Entity.

Modify Annex B.3 as shown

Notes:

1. It is strongly recommended that systems supporting the Basic TLS Secure Transport Connection Profile use as their port the registered port number “2762 dicom-tls” for the DICOM Upper Layer Protocol on TLS: (decimal).

2. Earlier revisions of the standard required TLS 1.0. This version has known security weaknesses. It is up to the implementation to define the policy of accepting connections from systems that use TLS 1.0. RFC7525 Recommendations for Secure Use of Transport Layer Security (TLS) provides suggestions for proper use of TLS 1.2 and appropriate fallback rules.