DICOM Correction Proposal

<table>
<thead>
<tr>
<th>STATUS</th>
<th>Draft Final Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Last Update</td>
<td>2017/11/06</td>
</tr>
<tr>
<td>Person Assigned</td>
<td>Rob Horn</td>
</tr>
<tr>
<td>Submitter Name</td>
<td>Rob Horn</td>
</tr>
<tr>
<td>Submission Date</td>
<td>2017-02-14</td>
</tr>
</tbody>
</table>

Correction Number     CP-1703

Log Summary: TLS Security Note for Web Services

Name of Standard     PS3.18 2017d

Rationale for Correction:
The current WADO URI does not specify any security considerations. That section is missing. This adds a note referencing the IETF security recommendations for TLS. An alternative approach is to add a security section and put this information there.

[Comment: Hologic: [RFC7525] should be added to Section 3.2 (IETF), not Section 3.1 (ISO & IEC). FIXED.]

[Comment: Hologic: Section 4 Terms and Definitions: HTTP and HTTPS definitions need to be updated with the 'or later' version phrasing. FIXED.]

Correction Wording:

Add to Section 3.2


Modify Section 4.0 as shown

HTTP The term HTTP as used in this Standard means the Hypertext Transport Protocol versions 1.0, 1.1 or 2 or later. See [RFC1945], [RFC7230] and [RFC7540].

HTTPS The term HTTPS as used in this Standard means the Hypertext Transport Protocol Secure versions 1.0, 1.1 or 2 or later. See [RFC2818] and [RFC7230].

Modify Section 6.0 as shown

DICOM Web Services use the HTTP and HTTPS protocols as its transport medium. Web Services supports versions 1.0, 1.1 and 2 or later of the protocol. If an origin server supports version 2, it shall also support version 1.1. If an origin server supports version 1.1, it shall also support version 1.0.

It is recommended that user agents that want to use HTTP/2 first initiate an HTTP/1.1 connection to the origin server and then upgrade to HTTP/2. If the upgrade fails then the user agent can still use the HTTP/1.1 connection. [RFC7540] Section 3 explains how to initiate HTTP/2 connections.

Note: HTTPS may mean any SSL or TLS version and options. The IETF [RFC7525] TLS Recommendations cover selection of TLS versions and options. There may also be national or local regulations that apply, and site specific risk analysis may affect the selection. TLS version
1.2 or later is often required and always recommended. Earlier versions are known to be vulnerable to well publicized attacks. All SSL versions are known to be vulnerable to well publicized attacks.