# Network Device Interpretation # 36

Checking validity of peer certificates for HTTPS servers

**Status:** ☒ *Active* ☐ *Inactive*

**Date:** *9-Nov-2016*

**Type of Document:** ☒ *Technical Decision* ☐ *Technical Recommendation*

**Approved by:** ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

**Affected Document(s):** ND cPP V1.0, FW cPP V1.0, ND SD v1.0

**Affected Section(s):** *FCS_HTTPS_EXT.1.3*

**Superseded Interpretation(s):** *None*

**Issue:**

*FCS_HTTPS_EXT.1.3 requires all NDcPP TOEs to check the validity of an HTTPS peer certificate. This requirement makes sense when you are an HTTPS client connecting to an HTTPS server (the classic example of this is connecting to a device via a web browser). However, when the TOE is acting as an HTTPS, server this does not make sense. HTTPS clients need to check the validity of server certificates but servers do not need to do the same thing for client certificates if they don't use mutual authentication. This is similar to the reason the FCS_TLS_EXT.* requirement was broken into FCS_TLSS_EXT.* and FCS_TLSC_EXT.*. Since mutual authentication isn't required by the NDcPP, FCS_HTTPS_EXT.1.3 should be a selection based requirement for servers.*

*Proposed Resolution:*

*Move FCS_HTTPS_EXT.1.3 to be selection-based since the requirement to check peer certificate validity does not apply to HTTPS servers which do not use mutual authentication.*

**Resolution:**

The NIT follows the argument made and recommends modification of FCS_HTTPS_EXT.1.3 and the related Application Note as follows:

**FCS_HTTPS_EXT.1.3** The TSF shall establish the connection only if [selection: *the peer presents a valid certificate during handshake, the peer initiates handshake*].

### *Application Note 51*

*Select 'the peer presents a valid certificate' if the TOE acts as a client, or if mutual certificate-based authentication is enforced when the TOE acts as a client or a server. Certificate validity must be determined according to FIA_X509_EXT.1/Rev if HTTPS is used for FPT_TRP.1/Admin or FTP_ITC.1, and on FIA_X509_EXT.1/ITT if HTTPS is used for FPT_ITT.1.*

*Select 'the peer initiates handshake' if the TOE acts as a server that does not enforce mutual certificate-based authentication. It is understood that in such cases peer authentication is achieved by other means.*

The Supporting document should be modified as follows:

**FCS_HTTPS_EXT.1 HTTPS Protocol**

The following TSS requirement should be inserted above the existing tests for FCS_HTTPS_EXT.1.

**TSS**

**FCS_HTTPS_EXT.1.3**

The evaluator shall check that the TSS describes how peer authentication is implemented when HTTPS protocol is used.

The Test 2 requirement in paragraph 117 should also be modified as follows:

117 If '*the peer presents a valid certificate during handshake*' is selected in FCS_HTTPS_EXT.1.3, then certificate validity shall be tested in accordance with testing performed for FIA_X509_EXT.1 if HTTPS is used for FTP_TRP.1 or FTP_ITC.1.

**Rationale:**

*No objections have been raised in the commenting period from Oct. 24th to Nov. 7th 2016. Status has therefore been changed to Technical Decision on Nov. 9th 2016.*

**Further Action:**

*None*

**Action by Network iTC:**

*Revise NDcPP, FWcPP and ND SD accordingly.*