# Network Device Interpretation # 201715

TLS server testing - Empty Certificate Authorities list

**Status:** ☒ *Active* ☐ *Inactive*

**Date:** *10-Oct-2017*

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

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

**Affected Document(s):** *ND SD V.1.0, ND SD V2.0*

**Affected Section(s):** *FCS_TLSS_EXT.2.4, FCS_TLSS_EXT.2.5, Test 4*

**Superseded Interpretation(s):** *None*

**Issue:**

*Background*

*The CCTL is working with a vendor of a network appliance intending to claim conformance to [cPPND]. The appliance supports TLS communication as a server.*

*The testing in [SD] for FCS_TLSS_EXT.2.4/FCS_TLSS_EXT.2.5 Test 4 requires the following:*

*"Test 4: The evaluator shall configure the client to send a certificate that does not chain to one of the Certificate Authorities (either a Root or Intermediate CA) in the server's Certificate Request message. The evaluator shall verify that the attempted connection is denied."*

*The issue is that this test cannot be performed unless the TOE sends a list of Certificate Authorities in its Certificate Request message. There are implementations of TLS that do not send this list of Certificate Authorities as is the case with network appliance to be evaluated. Section 7.4.4 of RFC 5246 states the list of Certificate Authorities in the Certificate Request can be empty:*

*"certificate_authorities A list of the distinguished names [X501] of acceptable certificate_authorities, represented in DER-encoded format. These distinguished names may specify a desired distinguished name for a root CA or for a subordinate CA; thus, this message can be used to describe known roots as well as a desired authorization space. If the certificate_authorities list is empty, then the client MAY send any certificate of the appropriate ClientCertificateType, unless there is some external arrangement to the contrary."*

*The test in its current form, by not being conditional, requires a TLS implementation that RFC 5246 defines as optional.*

*CCTL Proposal*

*The CCTL proposes the following interpretations when evaluating a network appliance that acts as a TLS server for conformance to [cPPND]:*

*FCS_TLSS_EXT.2.4/FCS_TLSS_EXT.2.5 Test 4 – The CCTL proposes that this test should be conditional on whether or not the TOE sends a Certificate Authorities list in its Certificate Request message. The successful testing of FCS_TLSS_EXT.2.4/FCS_TLSS_EXT.2.5 Test 3 will demonstrate that the TOE will still not accept peer certificates when the server is unable to validate the certification path of the client certificate.*

**Resolutions:**

The NIT proposes the following changes which shall be implemented if accepted by the Network iTC (sentence to be removed in case this recommendation is accepted).

*The NIT acknowledges the issue described in the 'Issue' section above. Therefore FCS_TLSS_EXT.2.4/ FCS_TLSS_EXT.2.5 Test 4 shall be made conditional. Test 4 shall be changed as follows:*

"Test 4: If the TOE supports sending a non-empty Certificate Authorities list in its Certificate Request message, the evaluator shall configure the client to send a certificate that does not chain to one of the Certificate Authorities (either a Root or Intermediate CA) in the server's Certificate Request message. The evaluator shall verify that the attempted connection is denied. If the TOE doesn't support sending a non-empty Certificate Authorities list in its Certificate Request message, this test shall be omitted."

**Rationale:**

*As stated in the 'Issue' section.*

**Further Action:**

*None*

**Action by Network iTC:**

*None*