Network Device Interpretation # 201729

DTLS server testing - Empty Certificate Authorities list

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Mar-2018*

End of proposed Transition Period (to be updated after TR2TD process): *4-Jun-2018*

Type of Change: ☐ Immediate application ☒ Minor change ☐ Major change

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_DTLSS_EXT.2.7, FCS_DTLSS_EXT.2.8, Test 4*

Superseded Interpretation(s): *None. Note that this RfI is linked to RfI#201715rev2 which is covering the issue for the TLS Server case and which is replacing RfI#201715(rev1).*

Issue:

Background

The CCTL is working with a vendor of a network appliance intending to claim conformance to [cPPND]. The appliance supports DTLS communication as a server. (This RfI covers the same issue as RfI#201715 but related to DTLS instead of TLS).

The testing in [SD] for FCS_DTLSS_EXT.2.7/FCS_DTLSS_EXT.2.8 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 DTLS 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 DTLS implementation that RFC 5246 defines as optional.

CCTL Proposal

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

FCS_DTLSS_EXT.2.7/FCS_DTLSS_EXT.2.8 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_DTLSS_EXT.2.7/FCS_DTLSS_EXT.2.8 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 acknowledges the issue described in the 'Issue' section above but is of the opinion that Test 4 shouldn't be made conditional but generalized to cover all possible scenarios. Test 4 shall therefore be changed as follows:

*<old>"*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.*"</old>*

shall be replaced by

*<new>"*Test 4: The aim of this test is to check the response of the server when it receives a client identity certificate that is signed by an impostor CA (either Root CA or intermediate CA). To carry out this test the evaluator shall configure the client to send a client identity certificate with an issuer field that identifies a CA recognised by the TOE as a trusted CA, but where the key used for the signature on the client certificate does not in fact correspond to the CA certificate trusted by the TOE (meaning that the client certificate is invalid because its certification path does not in fact terminate in the claimed CA certificate). The evaluator shall verify that the attempted connection is denied.*"</new>*

Rationale:

The original wording of the test was too strict so that it couldn't be performed for all possible implementations. The objective of the test is though, to ensure that the TOE doesn't accept a client identity certificate that is signed by an impostor CA. Therefore the test case has been rewritten to ensure that it can be performed by different types of implementation.

Further Action:

None

Action by Network iTC:

None