Network Device Interpretation # 201709

Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4

Status: ☒ *Active* ☐ *Inactive*

Date: *1-Aug-2017*

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

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

Affected Document(s): *ND SD V1.0, ND SD V2.0*

Affected Section(s): *FCS_DTLSC_EXT.1.2/FCS_DTLSC_EXT.2.2 Tests 1-4 (ND SD V2.0), FCS_TLSC_EXT.1.2/FCS_TLSC_EXT.2.2, Tests 1-4 (ND SD V1.0, ND SD V2.0)*

Superseded Interpretation(s): *None*

Issue:

The current wording for FCS_TLSC_EXT.x.2 Test 1, Test 2, Test 3, and Test 4 is as follows:

- Test 1: The evaluator shall present a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. The evaluator shall verify that the connection fails.

- Test 2: The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type.

- Test 3: The evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contains the SAN extension. The evaluator shall verify that the connection succeeds.

- Test 4: The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds.

Test 1 is fully redundant, as SAN is always checked first. That is, Test 1 is a SAN check failure. Test 2 is also a SAN check failure. Test 3 is a CN check. Test 4 is SAN over CN preference check. If Test 1 fails, so will Test 2 or Test 3.

Proposed Resolution:

It is suggested consolidating and restructuring Test 1 - Test 4 to have one test for CN check, one test for SAN check, and one test for preference of SAN over CN.

Resolution:

The NIT acknowledges the issue described in the 'Issue' section above. The NIT supports the point of view that after negative testing of the scenario of SAN not matching the reference identifier but CN matching the reference identifier (i.e. Test 4) a negative test of SAN not matching the reference identifier and CN not matching the reference identifier (i.e. Test 1) does not seem to add any value. On the other hand the scenario of SAN extension not present and CN not matching the reference identifier needs to be tested. FCS_DTLSC_EXT.1.2/FCS_DTLSC_EXT.2.2 Test 1(ND SD V2.0), FCS_TLSC_EXT.1.2/FCS_TLSC_EXT.2.2 Test 1 (ND SD V1.0, ND SD V2.0) shall therefore be replaced by the following test:

"Test 1: The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails.
Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1."

Since some systems might require the presence of a SAN, *FCS_DTLSC_EXT.1.2/FCS_DTLSC_EXT.2.2 Test 3(ND SD V2.0), FCS_TLSC_EXT.1.2/FCS_TLSC_EXT.2.2 Test 3 (ND SD V1.0, ND SD V2.0)* shall be made conditional by applying the following change:
"Test 3 [conditional]: If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted."

Rationale:

According to RFC 6125 chap 6.4.4. the CN should only be checked if the SAN is not present (i.e. the SAN extension is missing). For valid certificates the CN field has to be present. So the following checks need to be applied.

Check 1: Is SAN extension present? If yes, verify if SAN matches the reference identifier; if not, verify if the CN matches the reference identifier.

Check 2: If the SAN extension is present, verify if the SAN matches the reference identifier. If the SAN matches the reference identifier than accept the certificate without checking the CN. If the SAN does not match the reference identifier reject the certificate without checking the CN.

Check 3: If the SAN extension is not present, then verify if the CN matches the reference identifier. If the CN matches the reference identifier accept the certificate. If the CN does not match the reference identifier reject the certificate. [Remark: Some systems might mandate the presence of the SAN].

This leads to the need for the following tests:

1.) The SAN extension is not present and …

    a. …the CN matches the reference identifier-> connection successful [Test 3]

    b. …the CN does not match the reference identifier -> connection is rejected [Replacement for Test 1]

2.) The SAN extension is present and …

    a. … the SAN matches the reference identifier and the CN does not match the reference identifier -> connection successful [Test 2]

    b. … the SAN does not match the reference identifier and the CN matches the reference identifier -> connection is rejected [Test 4]

If test 2.a) can be verified, checking for the combination SAN matches and CN matches should not bring any additional value [Test not present].

If test 2.b) can be verified, checking for the combination SAN does not match and CN does not match should not bring any additional value [original Test 1].

Further Action:

None

Action by Network iTC:

None