Network Device Interpretation # 201801

Clarification about FCS_TLSC_EXT.1.1, Test 2

Status: ☒ *Active* ☐ *Inactive*

Date: *23-Oct-2018*

End of proposed Transition Period (to be updated after TR2TD process): *23-Oct-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 v2.0e, ND SD v2.1*

Affected Section(s): *FCS_DTLSC_EXT.1.1, FCS_DTLSC_EXT.2.1, FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1*

Superseded Interpretation(s): *None*

Issue:

Issue:

FCS_TLSC_EXT.1.1 Test 2 pertains to testing the behaviour of TLS clients when connecting to a TLS server that presents a certificate with or without the Server Authentication purpose in the extendedKeyUsage field. The PP itself does not clearly define the requirement.

The test item as provided in the supporting document reads:

"Test 2: The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field."

This test is self-contradictory. On one hand, it appears to require that the evaluator use a certificate with the extension and then "an otherwise valid server certificate that lacks the Server Authentication purpose". But it also directs that the certificates should be "identical except for the extendedKeyUsage field."

One interpretation of this test would be to generate two valid certificates, one with and one without the extension. However, for the certificates to be valid, both the extendedKeyUsage field and the CA signature would be different. It is also likely that the software used to create the certificates would refuse *to create two certificates with the same serial number. It would therefore not be possible for them to be "identical except for the extendedKeyUsage field."*

Another interpretation would be to modify the certificate in flight, similar to the requirements for other tests. This could be used to meet the "should be identical except for the extendedKeyUsage field", but the certificate may be rejected by the client due to an invalid CA signature instead of the absence of the field.

Complicating interpretation is the fact that "otherwise valid" could be interpreted as the certificate is invalid due to the absense of the extendedKeyUsage field or because it has been modified by removing the field.

Proposed Resolution:

If the intent is to ensure that TLS clients only connect with TLS servers when the server presents a certificate containing the Server Authentication purpose in the extendedKeyUsage field, the test should clearly state that objective. It should also clearly articulate that two valid certificates must be used, one with the extension and one without. The statement that "Ideally, the two certificates should be identical except for the extendedKeyUsage field." should be reworded as, "To the extent possible when creating the certificates, as much of the information in the certificates as possible should be the same."

Resolution:

The NIT acknowledges the issue described in the 'Issue' section above. Therefore SD shall be changed to clarify the intent of this test.

FCS_DTLSC_EXT.1.1, FCS_DTLSC_EXT.2.1, FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1 Test 2 shall be modified as follows:

<old>Test 2: The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field. </old>

<new>

The goal of the following test is to verify that the TOE accepts only certificates with appropriate values in the extendedKeyUsage extension, and implicitly that the TOE correctly parses the extendedKeyUsage extension as part of X.509v3 server certificate validation.

Test 2: The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage extension and verify that a connection is established. The evaluator shall repeat this test using a different, but otherwise valid and trusted, certificate that lacks the Server Authentication purpose in the extendedKeyUsage extension and ensure that a connection is not established. Ideally, the two certificates should be similar in structure, the types of identifiers used, and the chain of trust. </new>

Rationale:

Interception and modification of traffic/certificates "in flight" is not mandatory or necessary to satisfy any certificate-related testing requirements. It is sufficient to reconfigure the IT entities in the test environment to present different certificates that would satisfy test objectives. In implementing Test 2 it is recommended to create two similar certificates signed by the same CA, one with the extendedKeyUsage extension containing Server Authentication and one without, and then use the same authorized IT entity to present them to the TOE.

It is not acceptable to simply edit an existing certificate to change the purpose in the extendedKeyUsage extension, as doing so will result in an invalid certificate due to a signature mismatch. Consequently, it would not be possible to attribute a connection rejection to the extendedKeyUsage extension parsing.

Further Action:

None

Action by Network iTC:

None