Network Device Interpretation # 201662

Make TLSS tests using ECDHE optional

Status:	☒ *Active*	□ *Inactive*

Date: *7-Feb-2017*

Type of Document:	☒ *Technical Decision*	□ *Technical Recommendation*
Approved by:	☒ *Network iTC Interpretations Team*	□ *Network iTC*

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

Affected Section(s): *FCS_TLSS_EXT.1.3, FCS_TLSS_EXT.2.3*

Superseded Interpretation(s): *None*

Issue:

The NDcPP Supporting Document mandates a test using ECDHE ciphersuites while the NDcPP presents the inclusion of the ECDHE ciphersuites as an option in a selection.

The NDcPP identifies FCS_TLSS_EXT.1.3 as the following:

FCS_TLSS_EXT.1.3 The TSF shall generate key establishment parameters using RSA with key size 2048 bits and [selection: 3072 bits, 4096 bits, no other size] and [selection: over NIST curves [selection: secp256r1, secp384r1] and no other curves; Diffie-Hellman parameters of size 2048 bits and [selection: 3072 bits, no other size]; no other].

FCS_TLSS_EXT.1.3 identifies the following test:

"The evaluator shall attempt a connection using an ECDHE ciphersuite and a configured curve and, using a packet analyzer, verify that the key agreement parameters in the Key Exchange message are the ones configured. (Determining that the size matches the expected size for the configured curve is sufficient.) The evaluator shall repeat this test for each supported NIST Elliptic Curve and each supported Diffie-Hellman key size".

Proposed resolution: In the NDcPP Supporting Document identify the test for FCS_TLSS_EXT.1.3 as optional depending whether or not the TOE supports ECDHE ciphersuites.

Resolution:

The intention of FCS_TLSS_EXT.1.3 and FCS_TLSS_EXT.2.3 testing is to verify claims of supporting specific key establishment protocols. If, for example, no claim of ECDHE support is made, it follows that ECDHE does not need to be tested. If someone nevertheless were to attempt to connect using ECDHE cipher, the expected outcome is a failure to negotiate TLS channel when such connection is forced.

To further clarify this point, description for Test 1 for FCS_TLSS_EXT.1.3 and FCS_TLSS_EXT.2.3 shall be modified as follows:

"The evaluator shall attempt establishing connection using each claimed key establishment protocol (RSA, DH, ECDHE) with each claimed parameter (RSA key size, Diffie-Hellman parameters, supported curves) as selected in FCS_TLSS_EXT.1.3 (or FCS_TLSS_EXT.2.3). For example, determining that the RSA key size matches the claimed size is sufficient to satisfy this test. The evaluator shall ensure that each supported parameter combination is tested.

Note that this testing can be accomplished in conjunction with the other testing activities."

Rationale:

FCS_TLSS_EXT.1.3 and FCS_TLSS_EXT.2.3 define support for EC to be selectable, and therefore there should not be mandatory tests of this selectable functionality in the evaluation activities.

Further Action:

None

Action by Network iTC:

None