Network Device Interpretation # 202509

FCS_TLSS_EXT.1.3 Test 2 DHE Ciphersuite Conditionality

Status: ☒ *Active* ☐ *Inactive*

Date: *13-Oct-2025*

End of proposed Transition Period (to be updated after TR2TD process): Click here to enter a date.

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): *NDSD v3.0e*

Affected Section(s): *FCS_TLSS_EXT.1.3 Test 2, FCS_DTLSS_EXT.1.3 Test 2*

Superseded Interpretation(s): *None*

Issue:

The entirety of FCS_TLSS_EXT.1.3 Test 2 is currently conditional on support for DHE ciphersuites. Since DHE ciphersuites are not supported in TLS 1.3, this causes confusion on the applicability of this test case for TLS 1.3.

Further, TLS 1.3 does not support 'standard' (non-FF) Diffie Hellman parameters, only FFDHE according to RFC 8446. An update to the wording of the test has been suggested for clarity in applicability and what parameters need to be tested. The tests are additionally suggested to be split into different test cases specifically for each TLS version.

Proposed resolution:

Suggested Updates to test cases:
Test 2a: [conditional] If the TOE supports TLS 1.2 and DHE ciphersuites, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use each supported Diffie-Hellman parameter size.

The evaluator shall attempt a connection using a supported DHE ciphersuite.The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the message are the ones configured Diffie-Hellman parameter size(s).

Test 2b: [conditional] If the TOE supports TLS 1.3 and 'ffdhe' parameters are selected, the evaluator shall repeat the following test for each supported FFDHE parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use each supported Finite Field Diffie-Hellman parameter size.

The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Share Extension Message where the KeyShareServerHello structure contains a KeyShareEntry structure with an opaque key_exchange value whose Length is consistent with the configured Finite Field Diffie-Hellman parameter size(s).

Resolution:

The following changes shall be applied:

SD section 4.2.7.3, FCS_TLSS_EXT.1.3 and FCS_TLSS_EXT.1.4, Test 2:

{old}

Test 2 [conditional]: If DHE ciphersuites are supported, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE ciphersuite.

For TLS 1.2, the evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the message are the ones configured Diffie-Hellman parameter size(s).

For TLS 1.3, the evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Share Extension Message where the KeyShareServerHello structure contains a KeyShareEntry structure with an opaque key_exchange value whose Length is consistent with the configured Diffie-Hellman parameter size(s).

{/old}

{new}

Test 2a: [conditional] If the TOE supports TLS 1.2 and DHE ciphersuites, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use each supported Diffie-Hellman parameter size.

The evaluator shall attempt a connection using a supported DHE ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the ones configured Diffie-Hellman parameter size(s).

Test 2b: [conditional] If the TOE supports TLS 1.3 and 'ffdhe' parameters are selected, the evaluator shall repeat the following test for each supported FFDHE parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use each supported Finite Field Diffie-Hellman parameter size.

The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Share Extension Message where the KeyShareServerHello structure contains a KeyShareEntry structure with an opaque key_exchange value whose Length is consistent with the configured Finite Field Diffie-Hellman parameter size(s).

{/new}

SD section 4.2.2.3, FCS_DTLSS_EXT.1.3 and FCS_DTLSS_EXT.1.4, Test 2:

{old}

Test 2 [conditional]: If DHE ciphersuites are supported, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE ciphersuite.

For DTLS 1.2, the evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the configured Diffie-Hellman parameter size(s).

For DTLS 1.3, the evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Share Extension Message where the KeyShareServerHello structure contains a KeyShareEntry structure with an opaque key_exchange value whose Length is consistent with the configured Diffie-Hellman parameter size(s).

{/old}

{new}

Test 2a: [conditional] If the TOE supports DTLS 1.2 and DHE ciphersuites, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use each supported Diffie-Hellman parameter size.

The evaluator shall attempt a connection using a supported DHE ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the configured Diffie-Hellman parameter size(s).

Test 2b: [conditional] If the TOE supports DTLS 1.3 and 'ffdhe' parameters are selected, the evaluator shall repeat the following test for each supported FFDHE parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use each supported Finite Field Diffie-Hellman parameter size.

The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Share Extension Message where the KeyShareServerHello structure contains a KeyShareEntry structure with an opaque key_exchange value whose Length is consistent with the configured Finite Field Diffie-Hellman parameter size(s).

{/new}

Rationale:

The NIT acknowledges that the test description should be clarified if the applicability of the test case is confusing. Since FCS_DTLSS_EXT.1.3 Test 2 contains the same wording, that description should also be updated.

Further Action:

None

Action by Network iTC:

None