

Network Device Interpretation # 202609

Separation of Test Definitions for DTLSv1.2 and v1.3 (renegotiation)

Status: ☒ *Active* ☐ *Inactive*

Date: 9-Jul-2026

End of proposed Transition Period (to be updated after TR2TD process): 3-Aug-2026

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_DTLSC_EXT.1.9, Test 4 and FCS_DTLSS_EXT.1.11, Test 4*

Superseded Interpretation(s): *None*

Issue:

DTLS Clients

The test activity for DTLS Clients, that reject renegotiation, are not accurate for DTLS 1.2.

The test activity for FCS_DTLSC_EXT.1.9, Test 4 requires the TSF to terminate the DTLS session after receiving a DTLS 1.2 renegotiation request. For DTLS 1.2, the TLS Client is required only to reject the request to renegotiate the DTLS 1.2 session.

Specifically, a TOE with a DTLS 1.2 Client does not take an action to terminate the DTLS session when the DTLS 1.2 Client does not support renegotiation and receives a Hello Request message. The DTLS 1.2 Client is expected only to ignore renegotiation request sent from the DTLS server. No further action is required by the DTLS 1.2 Client.

This behavior is different from DTLS 1.3. When a DTLS 1.3 Client receives a Hello Request, the DTLS 1.3 Client is expected to issue a fatal alert (Unexpected Message) and terminate the DTLS session. This is because in DTLS 1.3 there is no support for renegotiation. Attempts to initiate DTLS 1.2 renegotiation within a DTLS 1.3 session are forbidden. For TOEs with a DTLS 1.3 Client, the test activity for FCS_DTLSC_EXT.1.9 Test 4 is accurate.

DTLS Servers

The test activity for DTLS Servers, that reject renegotiation, are not accurate for DTLS 1.2.

The test activity for FCS_DTLSS_EXT.1.9, Test 4 requires the TSF to terminate the DTLS session after

receiving a DTLS 1.2 Client Hello renegotiation request. For DTLS 1.2, the DTLS Server is required only to reject the request to renegotiate the DTLS 1.2 session.

Specifically, a TOE with a DTLS 1.2 Server does not take an action to terminate the DTLS session when the DTLS 1.2 Server receives a Client Hello renegotiation request sent from the Client. The DTLS 1.2 Server is expected only to ignore the request to perform renegotiation. No further action is required by the DTLS 1.2 Server.

This behavior is different from DTLS 1.3. When a DTLS 1.3 Server receives a Client Hello renegotiation request, the DTLS 1.3 Server is expected to issue a fatal alert (Unexpected Message) and terminate the DTLS session. This is because in DTLS 1.3 there is no support for renegotiation. Attempts to perform DTLS 1.2 renegotiation within a DTLS 1.3 session are forbidden. For TOEs with a DTLS 1.3 Server, the test activity for FCS_DTLSS_EXT.1.9 Test 4 is accurate.

Resolution:

FCS_DTLSC_EXT.1.9, Test 4:

{old}

Test 4 [conditional]: If "reject...renegotiation attempts" is selected, then for each selected DTLS version, the evaluator shall initiate a DTLS session between the so-configured TSF and a test server that is configured to perform a compliant handshake, followed by a hello reset request. The evaluator shall confirm that the TSF completes the initial handshake successfully but terminates the DTLS session after receiving the hello reset request. Note: It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

{/old}

{new}

Test 4a [conditional, for DTLS 1.3 only]: The evaluator shall initiate a DTLS session between the TSF and a test DTLS 1.3 server that completes a compliant DTLS 1.3 handshake, followed by a hello request message. The evaluator shall observe that the TSF completes the initial DTLS 1.3 handshake successfully but terminates the session on receiving the hello request message.

It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

Test 4b [conditional, if the TOE supports DTLS 1.2 and rejects DTLS 1.2 renegotiation attempts]: The evaluator shall initiate a DTLS session between the so configured TSF and a test DTLS 1.2 server that is configured to perform a compliant handshake, followed by a hello request. The evaluator shall confirm that the TSF completes the initial handshake successfully but does not initiate renegotiation after receiving the hello request.

{/new}.

FCS DTLSS EXT.1.11, Test 4:

{old}

Test 4 [conditional]: If "reject...renegotiation attempts" is selected, then for each selected DTLS version, the evaluator shall follow the operational guidance as necessary to configure the TSF to negotiate the version and reject renegotiation. The evaluator shall initiate a valid initial session for the specified version, send a valid ClientHello on the non-renegotiable DTLS channel, and observe that the TSF terminates the session. Note: It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

{/old}

{new}

Test 4a [conditional, if the TOE supports DTLS 1.3]: The evaluator shall follow the operational guidance as necessary to configure the TSF to negotiate DTLS 1.3. The evaluator shall initiate a valid initial DTLS 1.3 session, send a valid client hello on the non-renegotiable DTLS channel, and observe that the TSF terminates the session.

Note: It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

Test 4b [conditional, if the TOE supports DTLS 1.2 and rejects DTLS 1.2 renegotiation attempts]: The evaluator shall follow the operational guidance as necessary to configure the TSF to negotiate DTLS 1.2 and reject renegotiation. The evaluator shall initiate a valid initial DTLS 1.2 session, send a valid ClientHello on the non-renegotiable DTLS channel, and observe that the TSF does not perform renegotiation of the DTLS channel.

{/new}

Rationale:

See issue section

Further Action:

None

Action by Network ITC:

None