# Network Device Interpretation # 202202

Mutual and Non-Mutual Auth TLSC Testing

**Status:** ☒ *Active* □ *Inactive*

**Date:** *29-Aug-2022*

**End of proposed Transition Period (to be updated after TR2TD process):** *29-Sep-2022*

**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 v2.2*

**Affected Section(s):** *NDSD 3.6.1.3, 3.6.3.3, 4.2.1.3, and 4.2.8.3*

**Superseded Interpretation(s):** *None*

**Issue:**

Issue: Mutual and Non-Mutual Auth TLSC Testing:

There are some potentially conflicting and ambiguous test requirements in the NDcPP2.2e supporting document when TLSC mutual authentication is claimed.

The FCS_TLSC_EXT.2 Supporting document section 3.6.3.3 Tests consists of the following:

"For all tests in this chapter the TLS server used for testing of the TOE shall be configured to require mutual authentication.

FCS_TLSC_EXT.2.1

(covered by FCS_TLSC_EXT.1.1 Test 1 and testing for FIA_X.509_EXT.*)."

It seems there are no actual test cases "in this chapter", but rather a suggestion that the testing is already addressed elsewhere. This begs the question of whether or when the caveat about the server being configured for mutual authentication might apply.

The FCS_TLSC_EXT.1 Supporting document section 4.2.8.3 Tests indicates:

"For all tests in this chapter the TLS server used for testing of the TOE shall be configured not to require mutual authentication." prior to a list of essentially mutual-authentication-agnostic test cases.

The caveat for FCS_TLSC_EXT.1 is problematic if, for example, the TOE always requires mutual authentication. By requiring the server to not require mutual authentication would lead to a series of test failures, while whether mutual authentication is configured or not is largely irrelevant to the purpose of those test cases.

It is possible 1) for a TOE to not support mutual authentication (and not claim FCS_TLSC_EXT.2) in which case there is no problem; 2) for a TOE to always require mutual authentication (e.g., for an FTP_ITT channel) in which case the FCS_TLSC_EXT.1 caveat could be a problem; or 3) support but not require mutual authentication (the most common case), leaving us uncertain how mutual authentication must be tested.

In the previous NDcPP, the matter of the server configuration in regard to mutual authentication was left unspecified for the majority of FCS_TLSC_EXT  test cases.  Rather, the test cases for FCS_TLSC_EXT.2.5 directly and unambiguously addressed the possibilities of non-mutual authentication and mutual authentication.  It is unclear why this approach was abandoned.

We believe that it is unnecessarily redundant to repeat all of the FCS_TLSC_EXT.1 test cases with mutual auth configured when claiming FCS_TLSC_EXT.2.

We suggest that one of the following courses should be followed:

1) The caveat for FCS_TLSC_EXT.2.1 should be rewritten to indicate that it replaces the caveat in FCS_TLSC_EXT.1 changing the required configuration of the server to require mutual auth. This is a simple change and serves to ensure that mutual authentication is tested, but does not address non-mutual authentication.
2) Both caveats identified above about configuring the server with or without mutual authentication should be removed and FCS_TLSC_EXT.2 should be revised to reintroduce the test cases from the previous version of FCS_TLSC_EXT.2.5 to actively and directly test that mutual authentication works as claimed and the client has the correct behavior when the server requests a certificate from the client.

**Resolution:**

The NIT acknowledges the issue.

The intent of FCS_[D]TLSC_EXT.1 are twofold:

1) To ensure that TOE [D]TLS clients can securely communicate with a [D]TLS server while authenticating the [D]TLS server; and
2) To act as a common baseline for TOE [D]TLS clients that are capable of mutually authenticating themselves to a [D]TLS server.

A TOE which claims FCS_[D]TLS_EXT.2 is required to also claim FCS_[D]TLSC_EXT.1 and be able to show conformance with all Assurance Activities of FCS_[D]TLSC_EXT.1 and FCS_[D]TLSC_EXT.2 for the channel(s) which support [D]TLS mutual authentication.

Mutual authentication support via FCS_[D]TLSC_EXT.2 can be claimed when the TOE is capable of such functionality.

FCS_[D]TLSC_EXT.1 test cases are designed to be met by TOE [D]TLS clients regardless of whether they can engage in mutual authentication or not.  Therefore, paragraph 359 and 536 in the Supporting Document shall be struck:

**<remove>**

~~For all tests in this chapter the [D]TLS server used for testing of the TOE shall be configured not to require mutual authentication.~~

**</remove>**

Paragraph 292 in the Supporting Document shall be replaced with the following:

**<old>**

(covered by FCS_DTLSC_EXT.1.1 Test 1 and testing for FIA_X.509_EXT.*).

**</old>**

**<new>**

Test 1: The evaluator shall establish a connection to a peer server that is configured for mutual authentication (i.e. sends a server Certificate Request (type 13) message). The evaluator observes that the TOE DTLS client sends both client Certificate (type 11) and client Certificate Verify (type 15) messages during its negotiation of a DTLS channel and that Application Data is sent.

In addition, all other testing in FCS_DTLSC_EXT.1 and FIA_X509_EXT.* must be performed as per the requirements.

**</new>**

Section 3.6.3.3 in the Supporting Document shall be replaced with the following:

**<old>**

For all tests in this chapter the TLS server used for testing of the TOE shall be configured to require mutual authentication.

FCS_TLSC_EXT.2.1

(covered by FCS_TLSC_EXT.1.1 Test 1 and testing for FIA_X.509_EXT.*).

**</old>**

**<new>**

For all tests in this chapter the TLS server used for testing of the TOE shall be configured to require mutual authentication.

FCS_TLSC_EXT.2.1

Test 1: The evaluator shall establish a connection to a peer server that is configured for mutual authentication (i.e. sends a server Certificate Request (type 13) message). The evaluator observes that the TOE TLS client sends both client Certificate (type 11) and client Certificate Verify (type 15) messages during its negotiation of a TLS channel and that Application Data is sent.

In addition, all other testing in FCS_TLSC_EXT.1 and FIA_X509_EXT.* must be performed as per the requirements.

**</new>**

**Rationale:**

*The intent of FCS_[D]TLSC_EXT.1 was to provide a common baseline of functionality for TOE [D]TLS clients regardless of whether they supported mutual authentication.  FCS_[D]TLSC_EXT.2 was meant to supplement the requirements for those [D]TLS clients which could also support mutual authentication.*

**Further Action:**

*None*

**Action by Network iTC:**

*None*