Network Device Interpretation # 201809

FCS_DTLS Mandatory Cipher Suites

Status: ☒ *Active* ☐ *Inactive*

Date: *16-Jul-2018*

End of proposed Transition Period (to be updated after TR2TD process): *16-Jul-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): *NDcPPv2.0, FWcPPv2.0*

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

Superseded Interpretation(s): *None*

Issue:

The Application Note for all DTLS SFRs states that TLS_RSA_WITH_AES_128_CBC_SHA is required if claiming compliance with RFC 6347. RFC 6347 does not mandate this ciphersuite, so it is unclear why this ciphersuite would be required.
Proposed Resolution:
Delete "TLS_RSA_WITH_AES_128_CBC_SHA is not mandatory for NDcPP v2.0 compliance; however, it is required if claiming compliance with RFC 6347."
Resolution:

The NIT acknowledges the issue described in the 'Issue' section above. The first paragraph of the application notes for FCS_DTLSC_EXT.1.1, FCS_DTLSS_EXT.1.1 and FCS_DTLSS_EXT.2.1 shall therefore be modified as follows:

<old>"The ciphersuites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the ciphersuites that are supported. It is necessary to limit the ciphersuites that can be used in an evaluated configuration administratively on the server in the test environment. TLS_RSA_WITH_AES_128_CBC_SHA is not mandatory for ND cPP v2.0 compliance; however, it is required if claiming compliance with RFC 6347."</old>

shall be replaced by

<new>"The ciphersuites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the ciphersuites that are supported. It is necessary to limit the ciphersuites that can be used in an evaluated configuration administratively on the server in the

test environment. Even though RFC 5246 and RFC 6347 mandate implementation of specific ciphers, there is no requirement to implement TLS_RSA_WITH_AES_128_CBC_SHA in order to claim conformance to this cPP. "</new>

The first paragraph of the application note for FCS_DTLSC_EXT.2.1 shall be modified as follows:

<old>"The ST author should select the ciphersuites that are supported. It is necessary to limit the ciphersuites that can be used in an evaluated configuration administratively on the server in the test environment. TLS_RSA_WITH_AES_128_CBC_SHA is not mandatory for ND cPP v2.0 compliance; however, it is required if claiming compliance with RFC 6347."</old>

shall be replaced by

<new>"The ciphersuites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the ciphersuites that are supported. It is necessary to limit the ciphersuites that can be used in an evaluated configuration administratively on the server in the test environment. Even though RFC 5246 and RFC 6347 mandate implementation of specific ciphers, there is no requirement to implement TLS_RSA_WITH_AES_128_CBC_SHA in order to claim conformance to this cPP. "</new>

The first paragraph of the application notes for FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1, FCS_TLSS_EXT.1.1 and FCS_TLSS_EXT.2.1 shall therefore be modified as follows:

<old>"The ciphersuites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the ciphersuites that are supported. It is necessary to limit the ciphersuites that can be used in an evaluated configuration administratively on the server in the test environment. TLS_RSA_WITH_AES_128_CBC_SHA is not mandatory for ND cPP v2.0 compliance; however, it is required if claiming compliance with RFC 5246."</old>

shall be replaced by

<new>"The ciphersuites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the ciphersuites that are supported. It is necessary to limit the ciphersuites that can be used in an evaluated configuration administratively on the server in the test environment. Even though RFC 5246 mandates implementation of specific ciphers, there is no requirement to implement TLS_RSA_WITH_AES_128_CBC_SHA in order to claim conformance to this cPP. "</new>

Rationale:

RFC 6347 Section 4 states "instead of presenting DTLS as a new protocol, we present it as a series of deltas from TLS 1.2 [TLS12]. Where we do not explicitly call out differences, DTLS is the same as in [TLS12]." Given that text, RFC 6347 inherits the mandatory-to-implement ciphersuite text from TLS 1.2 (see RFC5246).

Even though RFC 5246 and RFC 6347 mandate implementation of specific ciphers, there is no requirement to implement TLS_RSA_WITH_AES_128_CBC_SHA in order to claim conformance to this cPP.

Further Action:

None

Action by Network iTC:

None