Network Device Interpretation # 201701rev2

TLS Encryption Algorithms

Status: ☒ *Active* ☐ *Inactive*

Date: *10-Apr-2017*

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *NDcPP V1.0, FWcPP V1.0*

Affected Section(s): *FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1, FCS_TLSS_EXT.1.1, FCS_TLSS_EXT.2.1, FCS_TLSS_EXT.1.3, FCS_TLSS_EXT.2.3*

Superseded Interpretation(s): *RfI#(2016)11rev2*

Issue:

For a TOE that only implement TLS v1.2 is TLS_RSA_WITH_AES_128_CBC_SHA support mandatory? NDcPPv2 (draft) moved TLS_RSA_WITH_AES_128_CBC_SHA into optional ciphersuites list, could this be applied to NDcPPv1?

Resolution:

The NIT acknowledges that there are some security related concerns regarding AES-CBC mode and therefore supports making TLS_RSA_WITH_AES_128_CBC_SHA optional. 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:

"The TSF shall implement [selection: *TLS 1.2 (RFC 5246)*, *TLS 1.1 (RFC 4346)*] supporting the following ciphersuites:

- *[selection:*
  - *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*
  - *TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*
  - *TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268*
  - *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*
  - *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*
  - *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*
  - *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*
  - *TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*
  - *TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246*

- *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

]."

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

"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. Note that RFC 5246 makes TLS_RSA_WITH_AES_128_CBC_SHA a mandatory ciphersuite, but it is treated as optional for the purposes of conformance with this cPP (i.e. the selection of 'TLS 1.2 (RFC 5246)' will be accepted as conformant with this SFR even if TLS_RSA_WITH_AES_128_CBC_SHA is not one of the ciphersuites listed in the ST)."

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

"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. Note that RFC 5246 makes TLS_RSA_WITH_AES_128_CBC_SHA a mandatory ciphersuite, but it is treated as optional for the purposes of conformance with this cPP (i.e. the selection of 'TLS 1.2 (RFC 5246)' will be accepted as conformant with this SFR even if TLS_RSA_WITH_AES_128_CBC_SHA is not one of the ciphersuites listed in the ST)."

As a consequence of this change, FCS_TLSS_EXT.1.3 and FCS_TLSS_EXT.2.3 need to be updated accordingly as well as follows:

The TSF shall [selection: perform RSA key establishment with key size [selection: 2048 bits, 3072 bits, 4096 bits]; generate EC Diffie-Hellman parameters over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves; generate Diffie-Hellman parameters of size [selection: 2048, bits, 3072 bits]].

The corresponding sections in the extended component definition need to be updated accordingly.

Rationale:

As stated in the 'Issue' section. The updated wording for FCS_TLSS_EXT.1.3 and FCS_TLSS_EXT.2.3 in the resolution to this RfI also covers the resolution for RfI#201611/RfI#11rev2. To avoid conflicting SFR definition this resolution therefore superseds RfI#201611/RfI#11rev2.

Further Action:

None

Action by Network iTC:

None