Network Device Interpretation # 202009

DTLS - clarification of Application Note 63

Status: ☒ *Active* □ *Inactive*

Date: *4-Aug-2020*

End of proposed Transition Period (to be updated after TR2TD process): *4-Sep-2020*

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): *NDcPPv2.2*

Affected Section(s): *FCS_DTLSC_EXT.1.1, Application Note 63*

Superseded Interpretation(s): *None*

Issue:

Version 2.1 made it clear that "If the TOE only transmits application-layer data to an external entity using a trusted channel provided by DTLS, (i.e. transmits syslog over DTLS) then FCS_DTLSC_EXT.1 should be selected. If the application layer communication is bi-directional, that is, the TOE both transmits and receives application data or is managed by the DTLS Server, then FCS_DTLSC_EXT.2 is required."

While this is still clear in the header text for A.7.1.1 and B.3.1.1, in v2.2e text was added to App note 63 stating that, " FCS_DTLSC_EXT.1 should only be used if the TOE transmits application-layer data to an external entity using a trusted channel provided by DTLS without receiving application data that needs to be protected." This is confusing and misleading when read in isolation as it is incorrect at face value.

Proposed Resolution

Modify the App note text to: "FCS_DTLSC_EXT.1 should only be used ***without FCS_DTLSC_EXT.2*** *if the TOE transmits application-layer data to an external entity using a trusted channel provided by DTLS without receiving application data that needs to be protected." [changed text in* ***bold****]*

Resolution:

The issue identified in the 'Issue' section is acknowledged. The modified Application Note 63 does contradict the introductory text for DTLSC and DTLSS in chapter B.3.1.1 as well as precedents set by earlier technical resolutions like RfI#201905. The NIT position is that protocol level mutual authentication is an optional requirement with (D)TLS.

Therefore, the last paragraph in Application Note 63 for FCS_DTLSC_EXT.1.1

<old>

"FCS_DTLSC_EXT.1 should only be used if the TOE transmits application-layer data to an external entity using a trusted channel provided by DTLS without receiving application data that needs to be protected."

</old>

shall be modified as follows:

<new>

"FCS_DTLSC_EXT.1 without FCS_DTLSC_EXT.2 should be claimed if the TOE transmits application-layer data to an external server using a trusted channel provided by DTLS. FCS_DTLSC_EXT.1 together with FCS_DTLSC_EXT.2 should be claimed if the TOE implements protocol-level mutual authentication using X.509v3 certificates with DTLS. "

</new>

Rationale:

As part of NDcPPv2.2 updates the way mutual authentication is claimed was reworked. In the previous versions of the cPP there were two independent components for implementation with and without mutual authentication. In the NDcPPv2.2 these components were made hierarchical to reduce duplication within the cPP. As part of this reorganization, some application notes were edited for clarity and this includes Application Note 63.

The last paragraph of Application Note 63 in NDcPPv2.2 provides instructions when to use DTLSC with and without mutual authentication. This contradicts the instructions in the introductory text for the use of DTLS provided in chapter B.3.1.1 which says the following:

"The decision whether to include the support for protocol-level mutual authentication in the scope of the evaluation is regarded as part of the TOE boundary definition. These SFRs can be included in a conforming ST at the discretion of the ST author, even if the conformance statement of the cPP requires exact conformance. It is not mandatory to implement mutually authenticated DTLS in order to conform to this cPP."

This is in agreement with earlier Technical Decisions like RfI#201905 which states the same as the instructions provided in chapter B.3.1.1.

The NIT also clarified the intention of the original instruction with the author of the DTLS chapter that has been first integrated into NDcPPv2.0. It was confirmed that this instruction was meant as a guideline but not a requirement when mutual authentication shall be used with DTLS.

Further Action:

None

Action by Network iTC:

None