Network Device Interpretation # 202109

Clarification for NTP MAC keys

Status: ☒ *Active* ☐ *Inactive*

Date: *21-Mar-2022*

End of proposed Transition Period (to be updated after TR2TD process): *21-Mar-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): *NDcPP v2.2e*

Affected Section(s): *FCS_NTP_EXT.1.2, FAU_GEN.1, FCS_CKM.4, FPT_SKP_EXT.1*

Superseded Interpretation(s): *None*

Issue:

BACKGROUND:

FCS_NTP_EXT.1.2 allows message authentication using SHA and/or AES-based message authentication, for NTP.

This message authentication requires the use of a pre-shared secret either for concatenated to the message before being input to a SHA function or as the AES symmetric key for AES-based Message Authentication.

ISSUE:

The hash of a pre-shared secret is not characterized as a keyed operation by ISO/IEC 10118-3:2004, despite RFC 5905's designation of the NTP pre-shared secret as "keys". AES based operations do utilize keys but there is no symmetric key generation SFR in this PP. This leads to ambiguity as to the pre-shared secret(s) being subject to FCS_CKM.4 (crypto key destruction), FAU_GEN.1.1 (auditing), FPT_SKP_EXT.1 (protection from disclosure). This likely leads to inconsistencies in evaluations since we believe most industry implementations would not be compliant if those values are characterized as cryptographic keys. We seek additional clarification in the Application note as to the applicability of these other SFRs to the pre-shared secrets associated with NTP.

Resolution:

The SFRs FAU_GEN.1, FCS_CKM.4 and FPT_SKP_EXT.1 shall be applied to all cryptographic keys that are related to secure communication (i.e. related to FTP_TRP.1, FTP_ITC.1, FPT_ITT.1). The NTP

requirements have been introduced in NDcPP V2.1 as a rather 'standalone' set of requirements with 'no audit requirements' specified in the ECD section for FCS_NTP_EXT.1 and no dependencies on FCS_CKM - in contrast to the corresponding sections for secure communication protocols like TLS. As NTP keys are not intended to be used for encryption of sensitive information, the level of protection is different compared to other pre-shared keys. It has therefore not been intended that NTP keys are treated as other pre-shared keys in the context of NDcPP.

Rationale:

see Resolution

Further Action:

None

Action by Network iTC:

None