Network Device Interpretation # 201802

Audit of management activities related to cryptographic keys

Status: ☒ *Active* □ *Inactive*

Date: *24-Aug-2018*

End of proposed Transition Period (to be updated after TR2TD process): *24-Sep-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): *NDcPP v2.0e, FWcPP v2.0e, ND SD v2.0e*

Affected Section(s): *FAU_GEN.1*

Superseded Interpretation(s): *None*

Issue:

The PP says, "If (optionally) management of keys is provided by the TOE then this is specified in FMT_SMF.1" However FMT_SMF.1 does not provide a selection to do this. Additionally, the PP identifies the requirement FMT_MTD.1/CryptoKeys as optional, however audit records for these types of events are specified as required in FAU_GEN.1: "Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged)". Lastly, there appears to be an inconsistency with the additional information required in the audit record. FAU_GEN.1 says, "in addition to the action itself a unique key name or key reference shall be logged)." Section A.1 Audit Events for Optional SFRs: does not identify any additional information for the optional requirement FMT_MTD.1/CryptoKeys.

<u>Suggestions are as follows:</u>

- Provide an option in FMT_SMF.1 to select management of keys to provide for the optional SFR: FMT_MTD.1/CryptoKeys;

- In FAU_GEN.1: remove "Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged)" from the list of required events to provide for FMT_MTD.1/CryptoKeys being optional. When the optional SFR is claimed, the auditable event will be listed in Table 2 as already instructed in Section A.1; and

- Specify any additional audit record content in Section A.1 Audit Events for the Optional SFRs: for FMT_MTD.1/CryptoKeys.

Resolution:

The NIT acknowledges the issue described in the 'Issue' section but regards the proposed change as major change that should be performed in a future version of the NDcPP. In particular since FMT_MTD.1/CryptoKeys should be shifted to the selection-based SFR section of the NDcPP when there is an explicit selection in FMT_SMF.1. As an intermediate resolution the following changes shall be performed:

NDcPP V2.0e, FWcPP V2.0e, FAU_GEN.1, Application Note 1

The following paragraphs shall be added to Application Note 1:

"The requirement to audit the "Generating/import of, changing, or deleting of cryptographic keys" refers to all types of cryptographic keys which are intended to be used longer than for just one session (i.e. it does not refer to ephemeral keys/session keys). The requirement applies to all named changes independently from how they are invoked. A cryptographic key could e.g. be generated automatically during initial start-up without administrator intervention or through administrator intervention. This requirement also applies to the management of cryptographic keys by adding, replacing or removing trust anchors in the TOE's trust store. In all related cases the changes to cryptographic keys need to be audited together with a unique key name, key reference or unique identifier for the corresponding certificate."

NDcPP V2.0e, FWcPP V2.0e, FAU_GEN.1, Application Note 2

The following paragraph shall be deleted from Application Note 2:

"The TSS should identify what information is logged to identify the relevant key for the administrative task of generating/import of, changing, or deleting of cryptographic keys."

Rationale:

All changes to persistent cryptographic keys need to be audited. All affected keys need to be uniquely identified in the audit log.

Changes to temporary keys like ephemeral keys/session keys don't need to be audited since related events that need to be audited are explicitly defined for the related SFRs (e.g. FTP_ITC.1, FTP_TRP.1, FCS_*).

The updated application note is intended to clarify the focus of the audit requirement which not only applies to active and direct administrator intervention but also to automated key generation as well as key management through administration of X.509 certificates. It is expected that all TOEs compliant with the cPP should be capable of some sort of key management within the clarified scope. Therefore the audit requirement has been kept 'as-is' as a general mandatory requirement.

Further Action:

None

Action by Network iTC:

None