# Network Device Interpretation # 202405

Clarification of audit selections in FMT_SMF.1.1

**Status:** □ *Active* ☒ *Inactive*

**Date:** 5-Aug-2024

**End of proposed Transition Period (to be updated after TR2TD process):** 5-Sep-2024

**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):** ND cPP v3.0e

**Affected Section(s):** FMT_SMF.1.1

**Superseded Interpretation(s):** *None*

**Issue:**

**Issue:** Nearly Identical Selections (NIAP#1589)

The NDcPP3.0e appears to have a repeated claim under FMT_SMF.1.1 but only 1 has a definition in application note 23

Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full); &

Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full, changes to local audit storage size);

Application Note 23

.......... the selection "Ability to configure audit behaviour" includes the relevant management functions from FMT_MOF.1/Services and FMT_MOF.1/Functions, (for all of these SFRs that are cPP_ND_v3.0e, 06-Dec-2023 77 included in the ST) and is intended to cover security relevant configuration options (if any) to the audit behaviour (like changes to the behaviour when the local audit storage space is full).

**Resolution:**

The NIT agrees that the SFR and application note do not clearly differentiate between the various audit options in FMT_SMF.1.1. To clarify the SFR:

<old>

- [selection:

- Ability to start and stop services;
- Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);
- Ability to modify the behaviour of the transmission of audit data to an external IT entity;
- Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;
- Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full, changes to local audit storage size);
- Ability to manage the cryptographic keys;

</old>

<new>

- [selection:
  - Ability to start and stop services;
  - Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size);
  - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
  - Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;
  - Ability to manage the cryptographic keys;

</new>

Changes to Application Note 23:

<old>
The option “Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates” includes the relevant management functions from FMT_MOF.1/ManualUpdate and FPT_TUD_EXT.1. Based on selections in FPT_TUD_EXT.1.2, FMT_MOF.1/AutoUpdate must be included if the option “Ability to enable or disable automatic checking for updates or automatic updates” is included in the ST. Similarly, the selection “Ability to configure audit behaviour” includes the relevant management functions from FMT_MOF.1/Services and FMT_MOF.1/Functions, (for all of these SFRs that are included in the ST) and is intended to cover security relevant configuration options (if any) to the audit behaviour (like changes to the behaviour when the local audit storage space is full). The option "Ability to modify the behaviour of the transmission of audit data to an external IT entity" is intended to cover the management functionalities related to the transmission of local audit information to an external IT entity.
</old>

<new>
The option “Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates” includes the relevant management functions from FMT_MOF.1/ManualUpdate and FPT_TUD_EXT.1. Based on selections in FPT_TUD_EXT.1.2, FMT_MOF.1/AutoUpdate must be included if the option “Ability to enable or disable automatic checking for updates or automatic updates” is included in the ST.

The selection “Ability to configure local audit behaviour” includes the relevant management functions from FMT_MOF.1/Services and FMT_MOF.1/Functions, (for all of these SFRs that are included in the ST) and is intended to cover security relevant configuration options (if any) to the audit behaviour (like changes to the behaviour when the local audit storage space is full). The option "Ability to modify the behaviour of the transmission of audit data to an external IT entity" is intended to cover the management functionalities related to the transmission of local audit information to an external IT entity.
</new>

**Rationale:**

It appears that “Ability to configure audit behavior” and “Ability to configure local audit behavior” are redundant.  “Ability to configure local audit behavior” was added in v3.0 – defer to the new and more specific.

**Further Action:**

*None*

**Action by Network iTC:**

*Update in new version of cPP*