Network Device Interpretation # 202012

Guidance on how to handle FIA_AFL.1

Status: ☒ *Active* ☐ *Inactive*

Date: *14-Sep-2020*

End of proposed Transition Period (to be updated after TR2TD process): *14-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): *ND cPP v2.1; ND cPP v2.2e*

Affected Section(s): *FIA_UAU.1, FIA_PMG_EXT.1*

Superseded Interpretation(s): *None*

Issue:

NDcPP version 2.1 previously mandated “a local password-based” authentication mechanism in FIA_UAU_EXT.2.1. In NDcPP v2.2e, the SFR was changed to put “password-based” in a selection along with other methods. Our interpretation of this is that a local password-based authentication mechanism is longer strictly required by the NDcPP and that an alternative mechanism is acceptable so long as the credential being validated is local to the TOE. There was no change to the Application Note or the EAs for this SFR so that does not aid in understanding the intent.

If it is the case that a local password-based authentication method is not actually mandatory, it is then unclear how FIA_PMG_EXT.1 is supposed to be addressed, as that is still a mandatory requirement on the assumption that passwords are always used. The laboratory therefore has the following questions:

1. Is the update to FIA_UAU_EXT.2.1 intended to permit a TOE where the only administrator authentication is non-password-based (e.g. the TOE solely supports PKI-based local authentication)?

2. If this is permitted, what is the appropriate way for the ST to handle FIA_PMG_EXT.1 in this situation?

Added note from submitter: This also impacts FIA_AFL.1 so the second part of the question would need to add that we would be looking for guidance on how that should be handled (since FIA_AFL.1 only applies to password credentials and so it’s unclear how it would be handled if the only credentials are non-password-based).

Resolution:

1. FIA_UAU_EXT.2.1 applies solely to how the administrator logs in at the local console. Passwords were made selection based to allow TOEs that have difficulty determining whether an incoming connection is local or remote to provide a mechanism to prevent administrative lockout.
   As FIA_AFL.1 is a mandatory SFR, it is expected that the TOE provides at least one remote password-based authentication mechanism using credentials managed by the TOE.
2. FIA_PMG_EXT.1, FIA_AFL.1, and FMT_SMF.1 are all mandatory SFRs that the TOE will need to meet.

Rationale:

Exact conformance mandates that all mandatory SFRs are implemented by a TOE.

Further Action:

In future versions of the cPP, models of authentication need to be reviewed and revamped to consider different use cases and enterprise deployment scenarios.

Action by Network iTC:

None