Network Device Interpretation # 202421

Other authentication mechanisms in FIA_UIA_EXT.1.3

Status: ☒ *Active* □ *Inactive*

Date: *13-Jan-2025*

End of proposed Transition Period (to be updated after TR2TD process): *31-Mar-2025*

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 v3.0e*

Affected Section(s): *FIA_UIA_EXT.1.3*

Superseded Interpretation(s): *None*

Issue:

Application Note 19 is used to determine if other SFRs should be included as part of the evaluation or not. The second paragraph of the application note covers when to include certain password based SFRs (i.e., FIA_AFL.1, FIA_PMG_EXT.1, FPT_APW_EXT.1). The condition for their inclusion is based upon the selections of "Web GUI password" or "SSH password". The issue is the SFR has an assignment for “other authentication mechanism” which can include other password-based mechanisms. For example, thick clients and thin client applications that are used to manage the TOE would not be web browser based and may not even be GUI based. These types of clients may still rely on a TSF based password-based mechanism.

As of now, the Application Note 19 does not make it clear that these requirements should be evaluated under NDcPP v3.0e. These requirements would have been applicable for an evaluation against the NDcPP v2.2e. We do not believe it was intended to exclude these password based SFRs (i.e., FIA_AFL.1, FIA_PMG_EXT.1, FPT_APW_EXT.1) from being evaluated for their use with management applications that do not fit in the ‘Web GUI’ or ‘SSH client’ molds.

We recommend that Application Note 19 is updated to state:

If "Web GUI password", "SSH password", or an assignment which uses a TSF password-based mechanism is selected for remote authentication mechanism the ST author specifies an appropriate cryptographic protocol in FTP_TRP.1/Admin (e.g., "HTTPS" or "SSH") and includes FIA_AFL.1, FIA_PMG_EXT.1, FPT_APW_EXT.1 from Appendix B.

NIAP TRRT Response:

The TRRT agrees that Application Note 19 in NDcPP3.0E needs clarification regarding password requirements for non-GUI and non-Web password-based remote authentication mechanisms. This will be forwarded to the NIT for resolution.

Resolution:

After investigating authentication SF across multiple cPP versions, the NiT concluded that NDcPPv3.0 changes intended to both make local authentication optional and to further clarify acceptable remote authentication methods. Specifically, the assignment for “other authentication mechanism” in FIA_UIA_EXT.1.3 in the context of remote authentication was meant to be used to claim integration with an external identity provider. Therefore, the following changes shall be applied:

In NDcPPv3.0e, Section 6.5.1.1, FIA_UIA_EXT.1.3 shall be replaced as follows:

{old}

FIA_UIA_EXT.1.3 The TSF shall provide the following remote authentication mechanisms [selection: Web GUI password, SSH password, SSH public key, X.509 certificate, [assignment: other authentication mechanism]] and local authentication mechanisms [selection: none, password-based, [assignment: other authentication mechanism]].

Application Note 19

The TOE must support at least one remote authentication mechanism. Remote authentication mechanisms are defined as those that occur using a cryptographic protocol specified in FTP_TRP.1/Admin. Local authentication mechanisms are defined as those that occur at a local administrative interfaces using a console. If no local authentication mechanism is supported by the TOE, the ST author shall select "none" from the final selection. See Application Note 23 for examples of compliant local administrative interfaces.

The ST author selects the authentication mechanisms necessary to support remote administration. If "Web GUI password" or "SSH password" is selected for remote authentication mechanism the ST author specifies an appropriate cryptographic protocol in FTP_TRP.1/Admin (e.g., "HTTPS" or "SSH") and includes FIA_AFL.1, FIA_PMG_EXT.1, FPT_APW_EXT.1 from Appendix B.

The ST author selects the authentication mechanisms necessary to support remote administration. If "Web GUI password" or "SSH password" is selected for remote authentication mechanism the ST author specifies an appropriate cryptographic protocol in FTP_TRP.1/Admin (e.g., "HTTPS" or "SSH") and includes FIA_AFL.1, FIA_PMG_EXT.1, FPT_APW_EXT.1 from Appendix B.

…

{/old}

{new}

FIA_UIA_EXT.1.3 The TSF shall provide the following remote authentication mechanisms [selection: Web GUI password, SSH password, SSH public key, X.509 certificate] and **[selection: no other mechanism,**

external authentication server]. **The TSF shall provide the following** local authentication mechanisms: [selection: none, password-based, [assignment: other authentication mechanism]].

Application Note 19

An authentication process consists of two basic steps: identification step (presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem); verification step (presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed).

Remote authentication **is when a user associated with the Security Administrator role remotely communicates with the TOE for the purpose of security management over** a cryptographic protocol specified in FTP_TRP.1/Admin. Local authentication mechanisms are defined as those that occur at a local administrative interfaces using a console. If no local authentication mechanism is supported by the TOE, the ST author shall select "none" from the final selection. See Application Note 23 for examples of compliant local administrative interfaces.

The TOE must support at least one authentication mechanism where the verification step is processed locally, as such “external authentication server” should not be the only available authentication method.

The ST author selects the authentication mechanisms necessary to support remote administration. If "Web GUI password" or "SSH password" is selected for remote authentication mechanism the ST author specifies an appropriate cryptographic protocol in FTP_TRP.1/Admin (e.g., "HTTPS" or "SSH") and includes FIA_AFL.1, FIA_PMG_EXT.1, FPT_APW_EXT.1 from Appendix B.

If integration with an external X.500 Directory is supported and enabled, the "external authentication server" must be selected and an appropriate cryptographic protocol with each "authentication server" must be selected in FTP_ITC.1. Since the identity verification step is performed remotely, FIA_AFL.1, FIA_PMG_EXT.1, FPT_APW_EXT.1 requirements are not enforced by the TOE and therefore are not applicable to the “external authentication server” selection.

{/new}

Rationale:

Open ended “other authentication mechanism” is too broad to be acceptable, as there are deprecated crypto authentication mechanisms like NTLM protocol, that could be, but should not be claimed. Ambiguity in defining this SF could lead to remote authentication approaches that are enabled in the product but are not claimed, which is not acceptable.

Additionally, if a thick client is performing the verification step, then such client implements user identification and authentication SF and cannot be considered part of the OE. In such circumstances it would be incorrect to claim it using ‘other authentication mechanism’.

Further Action:

MINT to define requirements to integrate with other types of identity providers (IdP) and to investigate feasibility of enabling 2FA claims.

Action by Network iTC:

None