Network Device Interpretation # 201661

Mandatory use of X.509 certificates

Status: ☒ *Active* □ *Inactive*

Date: *30-Mar-2017*

Type of Document: ☒ *Technical Decision* □ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* □ *Network iTC*

Affected Document(s): *NDcPP V1.0, FWcPP V1.0*

Affected Section(s): *FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3*

Superseded Interpretation(s): *None*

Issue:

In the NDcPP v1.0, there are several FIA_X509_EXT SFRs. Their appearance in FIA class seems to imply the use of X509 certificate for user authentication. However, inclusion of FIA_X509_EXT SFRs in Figure 1 of NDcPP and exclusion of them in Figure 2 of NDcPP seem to suggest that X509 is only used to support FPT_ITC.1 and FTP_TRP.1, i.e. for protection of communication.

Because of the ambiguity and lack of application note for the use of FIA_X509_EXT SFRs, I am writing to seek CB's interpretation:

- *Is it mandatory for the TOE to implement user authentication with X.509 certificates in order to be NDcPP compliant?*
- *Is it mandatory for the TOE to implement client/server authentication with X.509 certificates in order to be NDcPP compliant?*

Specifically, the TOE uses SSH for administration. There are two types of authentication involved in SSH:

- *Server authentication for SSH transport layer protocol (RFC 4253)*
- *User authentication for SSH authentication protocol (RFC 4252)*

Both RFC 4253 and RFC 4252 don't specify support of X.509 certificates. Instead, X.509 certificate support is specified in RFC 6187.

Many SSH implementations, for example OpenSSH, don't support X.509. You may find claim of OpenSSH support of X.509 by searching the Web; however, it is added as patch; it is not included in the official OpenSSH package – I verified it by downloading OpenSSH 6.9p1 source code and inspecting it.

Thus, if mandatory, the developer may have to invest a lot of resources in adding implementation of X.509 certificate support to SSH.

More alarming is the FCS_SSHS_EXT.1 definition: The inclusion of RFC 6187 (which specifies SSH X.509 certificate support) is optional not mandatory (see FCS_SSHS_EXT.1.1) and x509v3- cipher-suites are optional and not mandatory (see FCS_SSHS_EXT.1.5). If the developer doesn't choose it, it is still fine with FCS_SSHS_EXT. However, we cannot claim FIA_X509_EXT, which seems to be mandatory.*

If a network device includes TLS and SSH implementation, however, it only supports X.509 certificate for TLS, but not for SSH. Is that OK?

Resolution:

There are no SFRs in the NDcPP mandating X.509 based user authentication. Although the X.509 related extended components have been made part of the FIA class this does not imply that X.509 based user authentication is required.

Regarding the use of X.509 certificates for client/server authentication refer to the Technical Decision regarding RfI#201610.

In response to the specific question in the last paragraph of the Issue section above:
If no protocols requiring X.509 certificates are selected for SSH, SSH does not need to use X.509. All other protocols selected for FPT_ITC.1 and FTP_TRP.1 need to support X.509 as specified in the SFRs.

Rationale:

As stated in the 'Resolution' section.

Further Action:

None

Action by Network iTC:

None