Network Device Interpretation # 57

Channel for Secure Update

Status: ☒ *Active* ☐ *Inactive*

Date: *21-Nov-2016*

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

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

Affected Document(s): *ND cPP V1.0, FW cPP V1.0*

Affected Section(s): *FPT_TUD_EXT.1, FTP_ITC.1*

Superseded Interpretation(s): *None*

Issue:

1. Is the TOE required to have a secure connection (FTP_ITC.1) to an external update server, or can the connection be unsecured and simply rely on the trusted update mechanisms in the PP (Signature/Hash)?

2. If the TOE uses HTTPS (which is using TLS) to connect to an external update server as per FTP_ITC.1, does it require mutual X.509 authentication?

3. If the TOE uses TLS to connect to an external update server as per FTP_ITC.1, does it require mutual X.509 authentication?

Resolution:

The trusted update mechanism is expected to rely on the signature/hash based integrity protection. It is therefore not mandatory to use a secure channel according to FTP_ITC.1 for the communication between the TOE and an external update server.

In response to questions 2 and 3 above: The ST author could use the assignment within the selection in FTP_ITC.1 to add the communication to an external update server, but this is optional. In this case it is up to the ST author to select the secure communication protocol and if TLS is chosen it is up to the ST author, whether TLS with or without mutual authentication is chosen. For details please refer to the Technical Decision regarding Rfl#34. Note that if FTP_ITC.1 is used for communication with an external update server the signature/hash based integrity protection mechanism as required by FTP_TUD_EXT.1.3 still needs to be applied.

Rationale:

See Resolution

Further Action:

None

Action by Network iTC:

None.