Network Device Interpretation # 201725

Typo in FCS_SSHS_EXT.1.4

Status: ☒ *Active* ☐ *Inactive*

Date: *28-Oct-2017*

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

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

Affected Document(s): *NDcPP V2.0*

Affected Section(s): *FCS_SSHS_EXT.1.4*

Superseded Interpretation(s): *None*

Issue:

Issue: Typo in FCS_SSHS_EXT.1.4. aes123-cbc is an invalid encryption algorithm.

Proposed Resolution: Change aes123-cbc to aes128-cbc.

Rationale: See RFC 4253 section 6.3.

Resolutions:

The NIT acknowledges the issue described in the 'Issue' section. The following changes shall be applied.

For NDcPP V2.0 in FCS_SSHS_EXT.1.4 change aes123-cbc to aes128-cbc.

Rationale:

As stated in the 'Issue' section above.

Further Action:

None

Action by Network iTC:

None