Network Device Interpretation # 17

FIPS 186-4 compliance of third party crypto libraries

Status: ☒ *Active* □ *Inactive*

Date: *30-Jun-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): *FCS_CKM.1*

Superseded Interpretation(s): *None*

Issue:

*As many of you know, the US leverages NIST CAVP/CMVP testing in evaluation of the cryptographic requirements in PPs. Recently, we received a request for clarification that stated that many vendors opt to rely on third party libraries to perform all of their cryptographic functions and that there are *zero* third party libraries available that meet FCS_CKM.1 (specifically the FIPS 186-4) in the cPP.*

Our research has shown that there are third party libraries that have recent certificates (at least one as recent as 2 weeks ago). However, we understand that it can take time to roll the latest versions into products. So, we could allow for a grace period (until 1 January 2016) if necessary. I'd like to get the iTC's input on this before we move forward. Thanks for your insight and support!

Resolution:

Making the compliance to the requirements of FIPS 186-4 mandatory has been a deliberate decision. The requirement needs to be fulfilled to be able to claim NDcPP compliance.

Rationale:

None

Further Action:

None

Action by Network iTC:

None