Network Device Interpretation # 25

Re-Use of FIPS test results

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, ND SD V1.0, FW SD V1.0*

Affected Section(s): *FCS_COP.1*

Superseded Interpretation(s): *None*

Issue:

1. *The question, at this point, deals with FCS_COP.1(3), which is worded almost identically between the two PPs, but where the test Assurance Activity has expanded from: 'The evaluator shall use "The Secure Hash Algorithm Validation System (SHAVS)" as a guide in testing the requirement above.' to an Evaluation Activity with over a page worth of "Short Message Test - Bit-oriented Mode", "Short Message - Byte-oriented Mode, "Selected Long Message" tests, and a "Pseudorandomly Generated Message Test" specifications.*
2. *Similarly, in the past, evaluator responses to the NDPP test AA have been of the sort: "The TOE has been FIPS approved. The SHA certificate numbers are ABD and XYZ covering all evaluated models.”*
3. *With the significantly expanded Test EAs, can we assume that FIPS testing will still be acceptable?*
4. *Will evaluators have to provide any further detail/explanations related to the new "Short Message, Long Message, Pseudorandom", etc., test specifications beyond the FIPS claims accepted for NDPP evaluations?*
5. *And, oh, will it be the Evaluation Activity Report (i.e., EAR) not an AAR from now on?*

Resolution:

While the FCS_COP requirements map to the algorithm testing requirements as defined by the NIST Validation System documents, given that this is a cPP and not a national PP, it would not be appropriate to point to national standards, such as FIPS 140-2, as a validation requirement.

While FIPS algorithm certificates are evidence that the tests required in the evaluation activities have been successfully demonstrated, the decision to accept FIPS algorithm certificates (and indeed location of algorithm certificate listing within any report not specified in CEM) is the purview of each national scheme.

Rationale:

None

Further Action:

None

Action by Network iTC:

None