Network Device Interpretation # 202414

Definition of a Known-good Implementation for FCS_CKM.2 Tests

Status: ☒ *Active* ☐ *Inactive*

Date: *10-Mar-2025*

End of proposed Transition Period (to be updated after TR2TD process): *10-Mar-2025*

Type of Change: ☐ Immediate application ☒ Minor change ☐ Major change

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

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

Affected Document(s): *NDcPP v3.0e, NDSD v3.0*

Affected Section(s): *FCS_CKM.2*

Superseded Interpretation(s): *None*

Issue:

Issue:

The question is what exactly is intended/expected for testing against "a known good implementation" in the context of the FCS_CKM.2 tests for which there is no explicit algorithm validation requirement (i.e. no ACVP testing required).

RSA-based key establishment

> *82. The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 by using a known good implementation for each protocol*
>
> *selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that*
>
> *uses RSAES-PKCS1-v1_5.*

FFC Schemes using "safe-prime" groups

> *83. The evaluator shall verify the correctness of the TSF's implementation of safe-prime groups by using a known good implementation for each protocol selected*
>
> *in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses safe- prime groups. This test must be performed for each safe-prime group that each*
>
> *protocol uses.*

My previous understanding was that using a well-accepted library (e.g. openssl) to demonstrate compatibility with the TOE through testing for the claimed protocols would demonstrate the implementation was acceptable, but it's possible that this is incorrect and some alternative testing is needed, so rather than make a guess at arguing what is allowed for this, I figured it made more sense to go straight to the source.

For FFC testing, now that there is actually ACVP testing for safe prime key generation/verification and KAS-FFC-SSC 800-56Ar3 my thought is that this could be argued as satisfying the "known good implementation" requirement, but I didn't know if that was overkill. But since there is no RSAES-PKCS1-v1_5 RSA key establishment testing to my knowledge, I'm not actually sure what the "correct" way to test FCS_CKM.2 RSA claims would be in that case.

Proposed resolution:

None

Resolution:

The NIT rejects this RFI due to the difficulties in reaching consensus regarding the definition of a "known-good" implementation that would be acceptable to all Schemes.

Rationale:

What constitutes an approved implementation is a Scheme decision, therefore the NIT is unable to provide a definitive answer to this question.

Further Action:

None

Action by Network iTC:

None