|  |  |  |  |
| --- | --- | --- | --- |
| **Item Title** | Consolidated iTC Feedback – DNcPPv2 SD | **Reviewer** | iTC Editorial Team |
| **Item Identifier** | *NDcPPv2 Supporting Document* | **Review Date** | 24 March 2016 |
| **Version; Date:** | *1.0-3; 03-16* |  |  |

**Notes :-**

|  |  |  |
| --- | --- | --- |
| Severity | 1 | **Significant** - Impact the correct or efficient operation of the item. Needs discussion during a review meeting. |
| 2 | **Moderate** - Normally clarifications or proposed improvements to the item which are unlikely to impact other areas. Probably doesn’t need discussing at a review meeting. |
| 3 | **Minor** - Does not affect the correct operation or interpretation of the item. These are usually syntax and format errors which have no effect on the meaning or interpretation of the item. |

**This is a public commenting process: the text of comments and responses may be distributed, or made available in other ways during the process, without restriction. If you wish to submit private comments then please contact the iTC Chair or Technical Editors directly.**

| **No.** | **Location** | **Comment** | **Suggested Change** | **Severity** | **Action** |
| --- | --- | --- | --- | --- | --- |
|  | ND SD, Pages 42 and 45 | Test 2 of FCS\_SSHC\_EXT.1.6 and FCS\_SSHS\_EXT.1.6. The use of “none” MAC algorithm. Most SSH client and server don’t support configuring “none” as a valid option. In addition, if we are only selecting AES-GCM and not AES-CBC, would the integrity check be built into the GCM mode?  If we don’t even allow hmac-md5, why would we allow “none”? | Remove Test 2. | 1 | The tests for FCS\_SSHC\_EXT.1.4-6 and FCS\_SSHS\_EXT.1.4-6 have been updated to specify using an algorithm not supported by the TOE (rather than a specific named algorithm) in each case. |
|  | ND SD, Pages 46 and 50 | Test 3 of FCS\_TLSC\_EXT.1.1 and FCS\_TLSC\_EXT.2.1. This looks like an ill-attempt at taking a test case for the TLS server and trying to convert it for a TLS client. In this case, the TLS server will disconnect the connection first because of no shared ciphersuite. If you have a RFC-conforming TLS server, it will detect the mismatch (i.e., send ECDSA cert but only select RSA ciphersuite) and will terminate the connection. What this test is asking is force the TLS server to select a ciphersuite (RSA) that is not supported by the server certificate (ECDSA) and this is not something normal TLS server will do. The TLS server will kills the handshake before the TLS client (TOE) will have the chance to disconnect. | We should do what we did for the next test 4 and append “Test [3] in FCS\_TLSS\_EXT.1.1 or FCS\_TLSS\_EXT.2.1 can be used as a substitute for this test.” Or just remove this test completely. | 1 | No Change.  The test is as intended. |
|  | ND SD, Pages 62 and 50 | Test 3 of FIA\_X509\_EXT.1/ITC.  “The evaluator shall test that the TOE can properly handle revoked certificates-–conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the **TOE** certificate and revocation of the **TOE** intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds.”  This should be the **peer** certificate. If we are establishing a secure ITC channel, we need to check the revocation status of the other endpoint (i.e., peer) certificate. To make sure it has not been revoked before we establish a secure connection. Why are we checking the TOE certificate? That is the responsibility of the peer which is not part of the TOE. | “The evaluator shall test that the TOE can properly handle revoked certificates-–conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the **peer** certificate and revocation of the **peer** intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds.” | 1 | Test 3 language updated with ‘peer’ instead of TOE |
|  | ND SD, Pages 63 and 64 | Test 4 of FIA\_X509\_EXT.1/ITT. Like the previous test 3, should add “No testing is required if no revocation method is selected.” | Append this: “No testing is required if no revocation method is selected.” Or to be consistent just make the test [conditional]. | 1 | **N**IT Rfi#9 has resulted in significant updates to the FIA\_X509\_EXT.1 text which includes references to revocation. The commenter is recommended to review the new SD draft and provide further feedback if this comment has not been fully addressed by these changes. |
|  | ND SD Page 66 | There are several tests added under FMT\_MOF.1 that say as an unauthenticated user try to make these configuration changes. I think this is not necessary because if you can gain unauthorized access to the TOE without authenticating then FIA\_UIA\_EXT would be a failure. | Re-write or remove tests to make applicable | 1 | Tests associated with FMT\_MOF.1 and FMT\_MTD.1 have been modified to remove reference to tests being carried out “without user authentication at all”. |
|  | ND SD,  Section 2.7.3.1  Page 82 | TSS: Missing this “If the TOE is not a distributed TOE then no evaluator action is necessary.” | Add “If the TOE is not a distributed TOE then no evaluator action is necessary.” | 2 | No change, CPC is only applicable in a distributed TOE |
|  | Page 42, Para 201 | The test case for FCS\_SSHC\_EXT.1.8 is a duplicate of the FCS\_SSHS\_EXT.1.8 test case and, as such, is a test for the TOE acting as an SSH server, not as an SSH client.  The test case for FCS\_SSHC\_EXT.1.8 needs to be rewritten to test the TOE when the TOE acts as an SSH client. | I cannot suggest a true appropriate change because the PP’s FCS\_SSHC\_EXT.1.8 is vague on whether the TOE is required to count incoming packets, outgoing packets, or both. This is a PP issue that it needs to be address first. (SSH uses separate keys for incoming and outgoing packets.)  If I use the FCS\_SSHS\_EXT.1.8 (SSH server) test case as the model, this test case counts the TOE’s incoming packets. If the SSH client should only count the incoming packets, then my suggested wording is:  “The evaluator shall configure the TOE to create a log entry when a rekey occurs. The evaluator shall connect to the TOE with an SSH server and cause 2^28 packets to be transmitted from the SSH server to the TOE, and subsequently review the audit log to ensure that a rekey occurred.”  But I think that the requirement should be clarified first for both FCS\_SSHC\_EXT.1.8 and FCS\_SSHS\_EXT.1.8 before any test cases are modified. | 1 | The test description has been updated as described in NIT Decision RfI#24. |
|  | Page 45, Para 228, FCS\_SSHS\_EXT.1.8 | Given the PP’s FCS\_SSHS\_EXT.1.8 wording, how was it determined that only the incoming packets would be counted and cause an SSH rekey?  The requirement is unclear if incoming packets, outgoing packets, or both should be counted. (SSH uses separate keys for incoming and outgoing packets.) | n/a | 3 | As noted for comment ‎7 above, the test description has been updated as described in NIT Decision RfI#24. |
|  | Page 22 section FCS\_CKM.4 | The FCS\_CKM.4 Evaluation Activity’s TSS section seems to have additional zeroization requirements beyond that required by FCS\_CKM.4. The PP’s FCS\_CKM.4 only requires “cryptographic keys” to be zeroized whereas the Evaluation Activity’s FCS\_CKM.4 requires “key material” to be zeroized. Key material typically includes intermediate data used during key generation (such as seeds) and during key establishment. This Evaluation Activity appears to go beyond what is required by the PP.  Please harmonize the PP’s FCS\_CKM.4 wording with Evaluation Activity’s FCS\_CKM.4 wording. | If only cryptographic keys are to be zeroized, then replace “key material” with “cryptographic keys” in the Evaluation Activity’s FCS\_CKM.4.  If “key material” is to be zeroized, then change the text of the PP’s FCS\_CKM.4. | 2 | FCS\_CKM.4 (and its Evaluation Activities) has been rewritten for this version, and is subject to ongoing discussions for future versions of the cPP. The commenter is requested to review the updated FCS\_CKM.4 language and provide feedback accordingly. |
|  | Support Document v1.0,  Section 2.2.8.1 Tests, Para#111 | SD states: “The evaluator shall also confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.”  Most network devices would not support configurable RNG. As written, this mandates inclusion of pointless “The TOE does not require RNG configuration.” Statement to enable evaluator to report confirming this. | Change applicable wording to state the following:  “If the RNG is configurable, the evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring this functionality” | 1 | No change. The previous sentence in the same paragraph specifies “If the RNG is configurable…” and so adding this to the second sentence would be redundant. |
|  | Support Document v1.0, Section 2.4.10, FMT\_SMF.1 Specification of Management Functions, para#319 | SD states: “ The security management functions for FMT\_SMF.1 are distributed throughout the cPP and are included as part of the requirements in…”  As written, this requirement is often interpreted by validators as mandating verifying EACH possible configuration parameter or presenting equivalence argument.  Our lab routinely receives validator objections over definitions of management functions and requests for further testing and auditing on a larger set of configurable parameters. For a typical network device it is not practical to test every possible configuration function as applicable to each role. Such testing would not provide meaningful increase in security assurance. | We request a more narrowly defined Assurance Activity associated with FMT\_SMF.1. One that stresses ‘security-relevant administrative actions’ and ‘configuration changes of SF”.  Specifically, FMT\_SMF.1 mentions “Ability to administer the TOE” but fails to specify what is considered administration.  Possible solution:  Define “ability to administer” in a way that does not lead to overly broad interpretation.  For example, replace “Ability to administer the TOE locally and remotely;” with “Ability to put the TOE into evaluated configuration;”. | 2 | This section has been updated to be clearer that tests are expected to be performed as part of the testing of other managed SFRs (unless there are management functions not already covered in those tests). |
|  | *SD, FCS\_SSHC\_EXT.1.2* | FCS\_SSHC\_EXT.1.2 has been changed to keep public key authentication as mandatory but password authentication has been made optional. The SD has not been updated accordingly. | Correct SD TSS FCS\_SSHC\_EXT.1.2 and Tests FCS\_SSHC\_EXT.1.2 sections accordingly. | 1 | SD updated to reflect optional password-based authentication |
|  | comments in SD | There are several comments contained in the SD. They should be covered in the body of the document and the comments should be removed. | Check comments and remove them for final version. | 3 | Editorial comments will be removed for final version. |
|  | ND-SD: FCS\_TLSC\_EXT.1.3 - Test 1 | The last sentence in the paragraph had an extra period at the end. | Remove the extra period | 3 | Typo corrected |
|  | ND-SD: FCS\_TLSC\_EXT.2.1 – Test 3 | “(for example, send a ECDSA…” | Replace “a” with “an” | 3 | Typo corrected |
|  | ND-SD: 2.3.3.3 – Test 1 | “for the login method.For that credential/login method,” | Add space between the period and the word “For” | 3 | Typo corrected |
|  | ND-SD: 3.3.2.1 – Paragraph 441 | The word “administrator” is misspelled “…how the adminstrator verifies…” | Replace with “administrator” | 3 | Typo corrected |
|  | ND-SD: A.1 Introduction – Paragraph 462 | The word “activities” is misspelled “…correspond to each of these activites.”. | Replaced with “activities” | 3 | Typo corrected |
|  | ND-SD: 2.2.4 FCS\_COP.1 | Encryption is misspelled in (AES Data Encyption/Decryption) | Replaced with “Encryption” | 3 | Typo corrected |
|  | NDcPP and ND-SD: **FCS\_SSHS\_EXT.1.8** | There are other ways to meet the intent of this requirement besides sending over 2^28 packets to a device. For example, showing that a rekey occurs after a specified time period and justification that no more than 2^28 packets will be transmitted in that time. | Consider updating the SFR and/or Test in SD to accommodate other testing methods that still ensure the threat is mitigated. | 2 | As noted for comment ‎7 above, the test description has been updated as described in NIT Decision RfI#24. |
|  | ND-SD:  FPT\_TUD | Test 2 - 2 requires the testing of an update for "an image without published hash". In some cases, this would be a non-test because without a hash value documented there is nothing for the admin to validate the hash value against. | Modify Test 2 – 2) to remove the no hash option. However, the admin guidance should instruct the admin not to attempt the installation of an update unless they have a published hash from the developer. The guidance would also tell them how to obtain the published hash, how the hash is generated for the update, and how the admin compares the hash. | 2 | The test description has been updated as described in NIT Decision RfI#26, to improve the description of test cases for updates using published hashes. There is also an update to the guidance to add an explicit check to ensure that it explains how to obtain the published hash (there is already a requirement to describe how to perform an update). |
|  | ND-SD:  FIA\_X509 when FCS\_IPSEC is selected. | FIA\_X509\_EXT.1.1 tests e, f, and g require modification of certificates presented to the TOE, and demonstration that the certificates fail to validate. While these tests are possible for TLS, HTTPS, and code signing, in IPsec/IKE (both v1 and v2), the certificates are exchanged within the encrypted IKE\_SA/Phase1\_SA. Thus, it’s not possible for a MITM to change/corrupt the certificates presented to the TOE. | Clearly indicate the non-applicability of the tests for IKEv1 and IKEv2. | 1 | No change.  The tests are about ensuring the behavior of the TOE when encountering malformed or invalid X.509 certificates regardless of protocol. The certificates do not have to be changed via MITM: the relevant certificates can be modified on the sending entity.  See NIT RfI#28. |
|  |  |  |  |  |  |