The Printer Working Group

Imaging Device Security

November 15, 2018

PWG November 2018 Virtual Face-to-Face

Agenda

When	What
9:00 – 9:05	Introductions, Agenda review
9:05 – 10:50	Review status of HCD PP v1.1 and HCD iTC
10:50 – 11:00	Wrap Up / Next Steps

Intellectual Property Policy

“This meeting is conducted under the rules of the PWG IP policy”.

- Refer to the IP statements in the plenary slides

Officers

- Chair:
  - Alan Sukert (Xerox)
- Vice-Chair:
  - Brian Smithson (Ricoh)
- Secretary:
  - Alan Sukert (Xerox)

Status of HCD PP Version 1.1

- Made a draft (Version 1.0.2) that includes the current NIAP Technical Decisions against the HCD PP, Errata #1 changes and other changes previously approved by the HCD TC at the April 25, 2018 and May 8, 2018 meetings
  - Resolve some inconsistencies and SFR dependencies
  - Consistency with NDcPP v2.0 changes
  - Correct some obvious (to us) omissions
- Goal at the Oct 29, 2018 meeting was to have final review and approval of Version 1.1 so we can submit it by the end of 2018 to NIAP and JISEC for their review and approval
  - Get agreement with NIAP and JISEC on process for getting HCD PP Version 1.1 approved as soon as possible. Goal is to get Version 1.1 approved in 1Q 2019

Status of HCD PP Version 1.1 Changes Previously Approved

- Incorporation of the 7 NIAP Technical Decisions against the HCD PP
- Incorporation of the findings documented in Errata #1 issued by JISEC
- Eliminated the requirement to support TLS 1.0 in FSC_TLS_EXT_1.1 in both sections A.9.12 and D.2.2Made all cipher suites optional in FSC_TLS_EXT_1.1 in both sections A.9.12 and D.2.2 – that meant eliminating the ‘None’ option under Optional Cipher Suites so that at least one had to be supported

Status of HCD PP Version 1.1 Changes Previously Approved

- Added to the last selection in FCS_COP.1.1(e) in section D.1.2 so the SFR now reads **FCS_COP.1.1(e) Refinement:** The TSF shall perform **key wrapping** in accordance with a specified cryptographic algorithm **AES in the following modes [selection: *KW, KWP, GCM, CCM*]** and the cryptographic key size **[selection: *128 bits, 256 bits*]** that meet the following: [**ISO/IEC 18033-3 (AES), [selection: *NIST SP 800-38F, ISO/IEC 19772, no other standards***]]. **[selection: *NIST SP 800-38F, ISO/IEC 19772, no other standards***]].

Status of HCD PP Version 1.1 Changes Previously Approved

- Added to FCS_COP.1.1(i) in section D.1.14 so the SFR now reads as follows: **FCS_COP.1.1(i) Refinement:** The TSF shall perform **key transport** in accordance with a specified cryptographic algorithm **RSA in the following modes [selection: *KTS-OAEP, KTS-KEM-KWS*]** and the cryptographic key size **[selection: *2048, 3072*]** bits that meet the following**: NIST SP 800-56B, Revision 1**.

Status of HCD PP Version 1.1 Changes Previously Approved

- Added to FCS_PCC_EXT.1.1 in section D.4.1 so it now reads as follows: **FCS_PCC_EXT.1.1** A password used by the TSF to generate a password authorization factor shall enable up to [assignment: *positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: *other supported special characters*]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [HMAC-[selection: *SHA-256, SHA-384, SHA-512*]], with [assignment: *positive integer of 1000 or more*] iterations, and output cryptographic key sizes [selection: *128, 256*] bits that meet the following: [**NIST SP 800-132**].

Status of HCD PP Version 1.1 Changes Previously Approved

- Change the TSS Assurance Activity for SFR FTP_ITC.1 in section 4.13.1 to read as follows: The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Status of HCD PP Version 1.1 Changes Previously Approved

- Change old paragraph 1451 in Appendix F to read "A description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device's main SOC or separate co-processor, for software: initialization of the product, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions associated with the Master Boot Record (MBRs), partition tables, etc.)). The description should also include the data flow from the device's host interface to the device's persistent media storing the data, information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted Master Boot Record area). The description should be detailed enough to verify all platforms to ensure that when the user enables encryption, the product encrypts all Field-Replaceable nonvolatile storage devices. It should also describe the platform's boot initialization, the encryption initialization process, and at what moment the product enables the encryption.

Status of HCD PP Version 1.1 Changes Previously Approved

- Change old paragraph 987 in the KMD Assurance Activity in FDP_DSK_EXT.1 in section B.1.3 to read “The evaluator shall verify the KMD provides sufficient instructions to ensure that when the encryption is enabled, the TOE encrypts all Field-Replaceable Nonvolatile Storage Devices. The evaluator shall verify that the KMD describes the data flow from the interface to the Device’s persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted area).”
- Changed the last sentence in Test Assurance Activity 5. for FPT_TUD.EXT.1 to read: (The evaluator shall also check those cases where digital signature verification mechanism, and if only selected in **FPT_TUD_EXT.1.3** the hash verification mechanism**,** fail.)

Status of HCD PP Version 1.1 Changes Previously Approved

- Change two instances in the Assurance Activity for FAU_SAR.1 to read as follows:

  TSS:

  The evaluator shall check to ensure that the TSS contains a description that audit records can be viewed only by an Administrator and functions to view audit records.

  Test:

  The evaluator shall also perform the following tests:

  The evaluator shall check to ensure that the forms of audit records are provided as specified in the operational guidance by retrieving audit records in accordance with the operational guidance.

  The evaluator shall check to ensure that no users other than an Administrator can retrieve audit records.

Status of HCD PP Version 1.1 Changes Previously Approved

- Add the following Test Assurance Activity to FMT_SMF.1:

  Test:

  The evaluator shall also perform the following test:

  The evaluator shall check to ensure that U.NORMAL is not permitted to operate the management functions. Note: This test can be partially or completely fulfilled by performing the Test Assurance Activity in FMT_MOF.1 depending on the list of management functions in FMT_MOF.1 and FMT_SMF.1.

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Reverse decision to include NIAP TD 0074 and make FCS_CKM.1(a) a mandatory SFR again

  Rationale: TD0074 changed FCS_CKM.1(a) Asymmetric Key Generation from a required SFR to a vendor-optional SFR. It was issued by NIAP, but without any rationale.

  Without a stated rationale for the change, or at least an example of a TOE that doesn't generate any asymmetric keys, is difficult to understand why the change is needed.

  Further, FCS_CKM.1(a) is a firm dependency of IPsec, TLS, and SSH, which means that it should be a firm dependency in any conforming TOE.

Decision: Not in v1.1; Defer to next revision of HCD PP as a “parking lot” issue to be considered

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Delete the test activity added to FMT_SMF.1

  Rationale: FMT_SMF.1 should be consistent with the union of FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1.

  The proposed test activity for FMT_SMF.1 looks extra and contradictory. For example, FMT_MTD.1 may permit every U.NORMAL to change her/his own password. Likewise, FMT_MSA.1 could permit every U.NORMAL to flag her/his own stored document as "protected", not to delete it accidentally. I believe that these examples both denote a legitimate action and conflict with the proposed test activity for FMT_SMF.1.

  Current FMT_SMF.1's application note says --- "The management functions should be restricted to the authorized identified role in FMT_MOF.1, FMT_MTD.1, FMT_MSA.1."

Decision: Withdraw the original proposal to add the test activity to FMT_SMF.1; leave as is

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Previously approved addition of the following test to the Test Assurance Activity in FAU_STG.4:

  The evaluator shall check that the actions specified in FAU_STG.4.1 are performed when the audit log is full.

    A follow-up comment: There was a follow-on comment that this new test is the same as the existing test case "The evaluator shall check to ensure that the processing defined in the SFR is appropriately performed to audit records."

Decision: Rather than including a new test, revise the exiting test in Version 1.1 to read "evaluator shall check to ensure that audit records are processed in accordance with the SFR."

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Make all cipher suites optional in FSC_TLS_EXT_1.1 in both sections A.9.12 and D.2.2 – that means eliminating the 'None' option under Optional Cipher Suites so that at least one has to be supported

    Rationale: Consistency with NDcPP v2.0

Decision: Accepted for inclusion in V1.1

- Patch the labels of "Trusted update selection" in the 1st figure in Appendix H

Decision: Appendix H is no longer needed and is difficult to maintain, so we will delete it in V1.1

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Change the key sizes selection in FCS_CKM.1(b) to an assignment

  Rationale: Was a comment that we need to restrict key size to a certain minimum length (e.g., 112 bits)

  FCS_COP.1(a) and FCS_COP.1(d) provide that the encryption keys shall be either 128- or 256-bit long.

  Our SFRs refer several communication standards, most of which specify size of keys. For instance, TLS 1.2 (RFC 5246) provides that HMAC-SHA1 keys shall be exactly 20-octet long, as was reported to JBMIA.

  It may be a good idea to add some general guidelines such as SP800-171 into the *App Notes* or somewhere even if we have already restricted key sizes specific enough outside FCS_CKM.1(b).

Decision: Not in v1.1; Defer to next revision of HCD PP as a "parking lot" issue to be considered

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- **FCS_CKM.1.1(b) Refinement:** The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified**
  cryptographic key sizes [assignment: key sizes (in bits)**] that meet the following: No Standard**

  Rationale: FCS_CKM.1(b) should be consistent with both FCS_COP.1(a) and FCS_COP.1(g)

Decision: Not in v1.1; Defer to next revision of HCD PP as a "parking lot" issue to be considered

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- TLS 1.1 and TLS 1.3
  - Should we remove TLS 1.1 as a allowable TLS version and should we add TLS 1.3 in FCS_TLS_EXT.1

  Arguments:

  - With TLS 1.3 having been formally released as an RFC, we are seeing customers starting to ask about how quickly we can provide support for TLS 1.3. Given that fact, we need to at least consider whether we should add TLS 1.3 to the FCS_TLS_EXT.1 SFR as one of the TLS versions that could be supported.
  - In an inverse vain, industry is now focusing their "guns" on TLS 1.1 as being an insecure version of TLS; we are getting questions from customers on whether TLS 1.1 can be disabled or removed on our products. Given that the push within industry is starting to become a ground swell to remove TLS 1.1 we should also consider whether we should eliminate TLS 1.1 as a requirement in FCS_TLS_EXT.

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- TLS 1.1 and TLS 1.3
  - Arguments (cont):
    - NDcPP iTC is working on TLS 1.3 support. If we add it in on our own, we would also be obliged to examine the assurance activities to determine if any would not apply to 1.3, or if additional activities specific to 1.3 should be added. Perhaps the best approach would be to check with NIAP/IPA to see what advice they have regarding 1.3.
    - TLS 1.1 is already optional. Any vendor that wants to remove it is able to now. Vendors might choose to support it but allow it to be disabled. In that case, the CC evaluated configuration could require it to be disabled, so 1.1 would not be considered in the evaluation.

Decision: No change for now. Will reconsider for next update to HCD PP and/or when NIAP issues updated TLS Package that addresses TLS 1.1 and TLS 1.3

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Change Predicated on NIAP NDcPP Technical Decisions:
  - Based on TD0290: Physical interruption of Trusted Path/Channel, suggesting the following minor change to the Assurance Activity for the FTP_ITC.1 SFR:

The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Rationale: Consistency with NIAP TD0290

Decision: Accepted for inclusion in v1.1

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- SFR Dependencies:
  - FCS_COP.1(g) should be dependent on FCS_COP.1(c)

    Rationale: FCS_COP.1(c) deals with hash algorithms and FCS_COP.1(g) is about keyed-hash message authentication (and FCS)COP.1(h) which is also about keyed-hash message authentication is dependent on FCS)COP.1(c)
  - FPT_KYP_EXT.1 should be dependent on FCS_KYC_EXT.1

    Rationale: FCS_KYP_EXT.1 references FCS_KYC_EXT.1 directly in FCS_KYP_EXT.1.1

Decision: Both were accepted for inclusion in v1.1

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Parking Lot Issues from HCD PP v1.0 Development:
  - **Assurance Activity for FAU_STG_EXT.1.1 includes activities for missing requirements**: The description of the item is “There is no SFR to provide local audit storage, so the AA "*The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and “cleared” periodically by sending the data to the audit server.*" is inappropriate.

  Options:

  - Remove this AA paragraph
  - Add an FAU_STG_EXT.2
  - Create one of more new SFR components (FAU_STG_EXT.3 or FAU_STG_EXT.4)

Decision: No change for now. May reconsider for next update to HCD PP

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- More Parking Lot Issues from HCD PP v1.0 Development:
  - **FCS_SNI_EXT.1 is a Conditionally Mandatory Requirement** (wants to move to Appendix B): The rationale presented is "FCS_SNI_EXT.1 is required if manual password entry is supported"
  - **FCS_PCC_EXT.1 is a Conditionally Mandatory Requirement** (wants to move to Appendix B): The rationale presented is "FCS_PCC_EXT.1 is required if manual password entry is supported".
  - **Add CCM to storage encryption**: It is not totally clear to me what SFRs this pertains to, but in going through the HCD PP it appears to me that this is being addressed in the context of FCS_CKM.1(b) and FCS_KYC_EXT.1. This request came from Lexmark but was endorsed by JISEC

Decision: No change for now on any of the three proposals. May reconsider for next update to HCD PP

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- More Parking Lot Issues from HCD PP v1.0 Development:
  - **Clarify SFR applicability**: This relates to the FDP_RIP.1(a) SFR about overwrite and the fact that it doesn't address SSDs and SEMs. The suggestion was to add an app note similar to the note for FCS_CKM.4 that stated "*Note that keys material stored using storage technologies that do not support direct overwrites of locations and onetime programmable memories are excluded from the requirement to satisfy this SFR."* I know that in the HCD PP both FDP_RIP SFRs are optional, but including an applicable app note similar to the FCS_CKM.1 note would help reinforce the optional nature of this SFR and when it should or should not apply

Decision: No change for now. May reconsider for next update to HCD PP

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Consistent with the change already approved in Appendix F for HCD PP v1.1:
  - In Appendix F, paragraph 1452, that paragraph should be revised to read "The process for destroying keys when they are no longer needed by describing the storage location of all keys and the protection of all keys stored in Field-Replaceable nonvolatile memory."

Decision: Accepted for inclusion in v1.1

- Make FAU_STG.1 a mandatory rather than an optional SFR.

  Would need to add some sentences to clarify what is to be protected and how to test this.

Decision: No change for now. May reconsider for next update to HCD PP

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Issues Raised By Japanese Labs & Vendors:
  - Inconsistency between FCS_CKM.1(b) and FCS_COP.1(g).

    FCS_COP.1.1(g) requires us to assign the key length, but FCS_CKM.1.1(b) requires us to select 128 bits or 256 bits for the key length. That's why, if we use 160 bit length key for HMAC, we cannot claim the key generation conformance with FCS_CKM.1(b).

    We might need another FCS_CKM.1 for HMAC.
  - Inconsistency of SFR dependencies

    There seem to be a lot of inconsistencies on SFR dependencies in HCD PP v1.0.

    For example, FCS_COP.1(c) is contained in "D.3 Trusted Update". However, this SFR should be applied also for Storage encryption as found in Application Note paragraph 1304. As Errata #1 added FCS_COP.1(c) as dependency for FCS_TLS_EXT.1, FCS_COP.1(c) might be described in "4.5 Class FCS: Encryption Support".

Decision: Defer both as a “parking lot” issues to be considered for discussion for next update of HCD PP

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- FCS_CKM.4 inconsistency between the SFR and Assurance Activities for Testing: Test 1 has two cases, overwrite or power-cycle; but the SFR has three cases, overwrite, power-cycle, or garbage collection.
- FCS_HTTPS_EXT.1.3 case is somewhat oddly worded: consider "If a peer cert is presented, the TSF shall [not require client auth] if the peer certificate is deemed invalid". Not sure what to propose instead.
- For FCS_CKM.2, refer to RFC5246 as well as NIST SP 800-56B

  Rationale: Allow RSA for TLS key establishment for a while if we add FCS_CKM.2

Decision: For all three, we basically said “not now”. May look at these again for next update to HCD PP

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- In the App Note for FCS_COP.1(c) **Cryptographic operation (Hash Algorithm)**, it is stated as follows:

  The hash selection should be consistent with the overall strength of the algorithm used for FCS_COP.1(d). (SHA 256 should be chosen for AES 128-bit keys, SHA 512 should be chosen for AES-256-bit keys) The selection of the standard is made based on the algorithms selected.

  - Two questions:
    - Is the reference to FCS_COP.1(d) **Cryptographic operation (AES Data Encryption/Decryption)** correct?
    - Should this SFR be selected with FCS_SNI_EXT?

Decision: We again basically said “not now”. May look at this again for next update to HCD PP.

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Add assurance activities specified for the FCS_COP.1(i) Cryptographic operation (Key Transport) SFR

  FCS_COP.1(a) not consistent with NDcPP: In the HCD PP FCS_COP.1(a) references *NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D* while NDcPP v2.0 for the corresponding SFR (FCS_COP.1.1) references *ISO 18033-3*

Decision: Proposal rejected

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- FCS_CKM.1(a) not consistent with NDcPP and MDF PP 2.0

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: **[selection:**
• RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
• ECC schemes using "NIST curves" [selection: P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
• FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1
] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

While HCD PP v1.0 for FCS_CKM.1.1 has

The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with [selection:**
• NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;
• NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")
• NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSAbased key establishment schemes **and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.**

Decision: Consider for next update to HCD PP

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

Proposals For HCD PP v1.1
From JBMIA

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Differences from ND cPP v2.0; we need to consider how or when the differences would be solved.

	HCD PP v1.0	ND cPP v2.0	Issues
FCS_CKM.1(a) Cryptographic Key Creation	DH Gr.14 for IKE cannot be selected. FFDHE for TLS cannot be selected. Requirement is defined with SP800-56A,B w/o revision	DH Gr.14 was added as an option with TD0291 FFDHE for TLS cannot be selected. Requirement is defined with FIPS 186-4	• Even though DH Gr.14 is required by FCS_IPSEC_EXT, it isn't selectable in HCD PP v1.0. • FFDHE for TLS cannot be selected, even though some cipher suites using FFDHE can be selected in TLS. • Revisions of SP800-56A,B are not specified. • SP800-56 is appropriate for Key Generation?
FCS_CKM.2 Cryptographic Key Establishment	No definition	Requirement is defined with SP800-56A,B w revision	• The current version of CKM.2 is good enough? If CKM.2 is added, RSA for TLS key establishment, which doesn't conform with SP800-56B, cannot be implemented.
FCS_IPSEC_EXT (IKE DH Group)	DH Gr. 5 can be selected.	N/A	• Equivalent security for DH Gr.5 doesn't fulfill the strength required by NIST.

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Proposal for DH key exchange support

DH group 14 for IKE, and ffdhe for TLS should be selectable in FCS_CKM.1.

DH group 5 for IKE should be removed from FCS_IPSEC_EXT.

As for FCS_IPSEC_EXT,

FCS_IPSEC_EXT1.9 in HCD PP should be replaced FCS_IPSEC_EXT1.11 of ND cPP v2.0.

As for IKE and TLS,

In order to support DH Gr.14 and ffhde in FCS_CKM.[1,2], there are two options.

1. If the requirement is defined with FIPS 186-4, then;

"***FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3***"

"***FFC Schemes using ffdhe that meet the following: RFC 7919***"

should be added as options.

2. If the requirement is defined with SP800-56A, then;

the ***revision 3*** should be specified.

For both case, the following Assurance Activity Test should be added.

Testing for FFC Schemes using Diffie-Hellman group 14 is done as part of testing in FCS_IPSEC_EXT.1.9.   Testing for TLS ffdhe2048 is done as part of testing in FCS_TLS_EXT.1.1"

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Combination of referred Standard and FCS_CKM.2 - consider which standard should be referred in FCS_CKM.x, and if CKM.2 should be added. following table shows options to be considered

#	options	comments	Pros
1	CKM.1 is defined with SP800-56. CKM.2 is not added. SP800-56A should be specified with Rev.3.	SP800-56A Rev.3 allows us to remove DH Gr.5, and covers IKE Gr.14 and TLS ffdhe 2048.	Regarding DH, both IKE and TLS can be defined correctly. No need to add RFC reference.
2	CKM.1 is defined with FIPS186-4. CKM.2 is not added.	RFC reference for IKE and TLS should be added to the selection.	The requirement for Key generation is defined strictly.
3	CKM.1 is defined with FIPS186-4. CKM.2 is defined with SP800-56B(Rev1) or SP800-56A(Rev.3).	In CKM.1, RFC references for DH of IKE and TLS should be added. Issue of RSA for TLS key establishment will remain.	The requirements for Key Creation and Key Exchange is defined clearly.

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- The current version of FCS_IPSEC_EXT1.9

HCD PP v1.0

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP))*, [assignment: *other DH groups that are implemented by the TOE]*, *no other DH groups*].

ND cPP v2.0

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection: 14 (2048-bit MODP), 19 (256-bit Random ECP), 20 (384-bit Random ECP), 24 (2048-bit MODP with 256-bit POS)].

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- The current definition of FCS_CKM.1 and of FCS_CKM.2 (which is not currently in the HCD PP)
- The current definition of FCS_COP.1(d)
- Proposed Additions/Modifications to FCS_COP.1(b)
- Proposed Additions/Modifications to FCS_COP.1(d)

Decision: For all of these proposals from JBMIA we determined the proposals needed more research before we can make a final determination

Proposals for HCD PP v1.1 Discussed at Oct 29th HCD PP Meeting

- Proposed Additions/Modifications by JBMIA to SFRs:
  - Some SFRs have multiple dependent selections, e.g. FCS_COP.1.1(d), but the dependency is not explicitly described. Readers might confuse the dependency.
  - Some iterations of SFRs use different expression patterns for similar items, e.g. "AES used in [selection: ...] mode" in FCS_COP.1.1(d) and "AES in the following modes [selection: ...]" in FCS_COP.1.1(e). Readers might misunderstand essential differences between iterations.
  - We suggest to add a table with an explanation into Application Note of each SFR , as written in blue letters in the following example, to clarify the dependency. And we also suggest to use a same expression pattern for similar items.

Decision: All three proposals were rejected

Proposals for HCD PP v1.1 Since Oct 29th HCD PP Meeting (from JBMIA)

- FCS_SNI_EXT.1
  - Should be a “Conditionally Mandatory” SFR based on storage encryption and not a “Selection-Based” SFR
  - In FCS_SNI_EXT.1.3, missing a ‘Selection’ in the SFR text
  - Consider adding FCS_KYC_EXT.2 from FDE cPPs

  Will consider all three proposals via email for inclusion in v1.1

Potential Topics for Next Update to HCD PP Beyond v1.1

- Remove cipher suites with RSA Key Assignment – when NIST approves and NIAP enforces the new updates to NIST SP 800-131A and NIST SP 800-56B
- New NIAP TLS Package
  - Based on NDcPP
  - Separates TLS as a client SFRs from TLS as a server SFRs
- Audit Log Server Requirements
- 3rd Party Entropy Sources
- Key Destruction SFR
- TPMs and SSDs used in the TOE
- EAL Claim for HCD PP
- Requirements around use of X.509 Certificates
- Password Policies to meet NIST SP 800-171 and the new California Password Law

Potential Topics for Next Update to HCD PP Beyond v1.1

- Removal of support for SHA
- Password Policy Applicability (normal vs. admin users)
- Wi-Fi Support
- SNMPv3 Support
- Kerberos Support
- S/MIME Support
- SMBv3 Support
- Internationally-friendly crypto requirements that don’t rely on FIPS
- Incorporation of GDPR and privacy implications
- Syncing with updates to NDcPP and three FDE cPPs

Potential Topics for Next Update to HCD PP Beyond v1.1

- Consider Changes in NDcPP v2.1
  - Main substantive changes appear to be:
    - Deletion of support for 192-bit TLS cipher suites and addition of two new TLS_DHE_RSA cipher suites
    - New SFR for NTP
    - Addition of new encryption algorithms, authentication implementations and key exchange methods for SSH
    - **Audit Events.** All generation/import/change of long-term cryptographic keys (i.e. not session keys) need to be audited, including those that are automatically generated by the TOE
    - Added additional management functions for possible selection, some of which we might want to look at for inclusion in HCD PP

Formation of an iTC to Generate an HCD cPP

- HCD cPP is needed to address the fact that European countries are still requiring “EAL” CC certifications which is forcing some vendors to certify the same MFP twice – once against the HCD PP which has no EAL and once against 2600.2 which is at EAL2
- The CCDB (Common Criteria Development Board) approved the formation of a CCDB HCD Working Group at request of Korea. This is an important step towards creating an HCD iTC to generate an HCD cPP.
- However, JISEC wants the HCD TC to apply directly to CCDB for formation of the iTC at its Spring 2019 Meeting
  - Will require generation of two artifacts to send to CCDB at least one month before the meeting:
    - A final ESR (Essential Security Requirements) document
    - Terms of References which addresses how the iTC will function
- The HCD TC will have to work out the disparity in approach between the Korean and Japanese Schemes

Formation of an iTC to Generate an HCD cPP

- Other Considerations:
  - JISEC has archived the 2600.1 PP for HCDs that most Japanese vendors were certifying HCDs against
  - For now JISEC is allowing certification against the 2600.2 PP for HCDs, but CCDB will discuss archiving all PPs developed against older versions of the Common Criteria (current version is v3.1R5 and 2600 PPs were developed against v3.1R3) at its Spring 2019 Meeting

Expected Timeline for HCD PP v1.1 and Beyond

- HCD PP Version 1.1
  - Still need to understand the process for getting v1.1 update approved by NIAP and JISEC
    - NIAP position appears to be to incorporate v1.1 changes into new HCD cPP
    - JISEC says to follow the same process used to approve HCD PP v1.0
  - Goal is to have the contents of HCD PP v1.1 ready and approved by the HCD TC by the end of 2018 and approved by NIAP/JISEC in 1Q 2019
    - Will work on logistics on how to get HCD TC approval of v1.1 contents

Expected Timeline for HCD PP v1.1 and Beyond

- HCD cPP Version 1.0
  - With CCDB approval to initiate an HCD WG, the next step will be to create the HCD iTC and generate an HCD cPP
  - Want to finalize ESR and have a draft Terms of Reference by EOY 2018
  - Goal is to have formation of the HCD iTC approved by the CCDB at its Spring 2019 Meeting
    - Determine who should be on the initial core team for the HCD iTC and how to recruit additional members
    - Want to have membership from vendors, CCTLs and maybe even Schemes
    - Looking for support from Korean, Japanese, US, Canadian and Swedish Schemes if possible
    - May be able to have the first HCD iTC meeting at the Spring 2019 CCUF Workshop

Wrap Up/ Next Steps

- Submit “Final” HCD PP Version 1.1 to NIAP/JISEC for approval as soon as possible
  - Goal is to get Version 1.1 approved by 1Q 2019
- Generate membership and draft Terms of Reference (TOR) for a proposed HCD iTC by EOY 2018
- Finalize the ESR and TOR
- Submit ESR and TOR to CCDB for approval no later than Mar 2019 (earlier if possible)
- Work to have HCD iTC in place by April 2019
- Work on a plan for what will go into HCD cPP v1.0
  - Do we make HCD cPP v1.0 essentially HCD PP v1.1 with some key updates?
  - If not, what should go into HCD cPP v1.0?
  - How do we integrate the new NIAP TLS Package?
- Set up iTC meeting cadence and process for reviewing/approving proposed inclusions in HCD cPP