JISEC

Guideline for Certification Application

with HCD-PP Conformance

Version 1.6

Old Version

Note: This document is only referential. Refer to the latest version when using this guideline.

This document is a guideline for certification application under Japan Information Technology Security Evaluation and Certification Scheme (JISEC), by using the "Protection Profile for Hardcopy Devices, Version 1.0," which is a Protection Profile (PP) developed by the MFP Technical Community with U.S. and Japanese Certification Bodies in September 2015.

The applicant is required to confirm each item of this guideline with the relevant parties, including the Evaluation Facility, prior to submitting a certification application.

Japan Information Technology Security Evaluation and Certification Scheme, Information-technology Promotion Agency, Japan (IPA)

Issued on August 1, 2019

Contents

Revision History

Version	Date	Major Changes
1.0	2016/8/26	・Initial creation
1.1	2017/4/26	・Update of the contents of "Description Items for Evaluator Testing Policy Outline document"
1.2	2017/6/28	・Addition of descriptions of "HCD-PP 1.0 as a certified PP" and "Notes for ST creation"
1.3	2018/6/6	・Addition of "2.3.3. Temporary treatment regarding FDP_DSK_EXT.1" ・Addition of "3. Confirming documents to be submitted upon certification application"
1.4	2019/1/10	・Modification of the description of entropy source
1.5	2019/4/10	・Addition of "2.3.4. Treatment regarding FCS_RBG_EXT.1 Test"
1.6	2019/8/1	・Addition of "2.3.5. Treatment regarding FCS_IPSEC_EXT.1.1" ・Addition of "4. Supplement regarding evaluation"

1. Introduction

This document is the guideline for a certification application of IT products that are conformant to the "Protection Profile for Hardcopy Devices, Version 1.0 dated September 10, 2015" (hereinafter referred to as the "HCD-PP 1.0") under Japan Information Technology Security Evaluation and Certification Scheme (JISEC) (hereinafter referred to as "this Scheme").

Chapter 2 describes how to write documents/ materials submitted for an application and the utilization of the Japan Cryptographic Module Validation Program.

Chapter 3 describes points to be checked regarding the submitted documents or materials under this Scheme.

2. Supplementary for application

This Chapter describes necessary description items and interpretations of the application of HCD-PP 1.0 under this Scheme, regarding materials that are submitted with application documents when an applicant makes a certification application for HCD-PP 1.0 conformance.

2.1. Application of Errata

For using HCD-PP 1.0 as certified PP, the following Errata[1] needs to be applied.

- HCD-PP 1.0

  Name: Protection Profile for Hardcopy Devices
  Version: 1.0 dated September 10, 2015
  Certification Identification: JISEC-C0553

- Errata

  Name: Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

Errata can be downloaded from the following JISEC webpages:

- HCD-PP 1.0 certification information page: URL

(Japanese)
https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_it7627.html
(English)
https://www.ipa.go.jp/security/jisec/jisec_e/certified_pps/c0553/c0553_it7627.html

Cautions when ST is created with the use of Errata-applied HCD-PP 1.0 are shown below:

A. PP Claim

As PP that is conformant, write the Errata identification in addition to the HCD-PP 1.0 Name and Version.

[1] This Errata will correct errors of indications regarding functional requirements, dependency and definitions of extended components and/or deficiency of terms definition, in order to satisfy evaluation of PP in CC/CEM.

Example:

PP Claim

PP to which this ST and TOE are conformant is as follows:

PP Name : Protection Profile for Hardcopy Devices

PP Version : 1.0 dated September 10, 2015

Errata : Protection Profile for Hardcopy Devices - v1.0
Errata #1, June 2017

B. Conformance rationale

That the rules indicated with "Conformance to this Protection Profile" (paragraphs from 14 to 20) of HCD-PP 1.0 are conformed is written in the HCD-PP 1.0 language.

In addition, also describe that TOE type of the TOE is consistent with that of HCD-PP 1.0.

Example:

Conformance Claim Rationale

The following conditions that the PP requires are met. It is "Exact Conformance" as the PP requires. Therefore, the TOE type is consistent with the PP.

- Required Uses
  Printing, Scanning, Network communications, Administration
- Conditionally Mandatory Uses
  Storage and retrieval, Field-Replaceable Nonvolatile Storage
- Optional Uses
  None

C. Extended components definition

If corrections of the definition of extended components or dependencies are indicated by Errata, they will be corrected to the descriptions of Errata.

D. Security Functional Requirements

If, in SFR, corrections of their indications or dependencies are indicated by Errata, they will be corrected to the descriptions of Errata.

2.2. Documents to be submitted upon certification application

2.2.1. Documents required for submission

When submitting a certification application for the MFPs that are conformant to the HCD-PP 1.0, an applicant is required to submit the following documentations, in addition to the documents for normal certification applications. (Refer to Chapter 5 of the "Guidance on IT Security Certification" (CCM-02-A).) Store them in electronic media such as CD-R and submit them.
Note that these documentations are not publicized.

1. Entropy Description [Appendix E]

   The Entropy Description is a documentation provided by the developer to ensure that a random bit generation function, used in the MFP that is a target of evaluation (TOE), provides sufficient entropy required. The details of this Entropy Description are described in **Appendix E** of the HCD-PP 1.0.

   Entropy sources can be rationales for the TOE security functions, so unless their validity can be confirmed in the process of the evaluation, the evaluation work is not allowed to be continued. Confirming the validity of generating entropy sources in advance by the relevant parties will prevent the evaluation work from being interrupted and turning back to the previous evaluation process.

   Since it is necessary to describe the information on each entropy source in the ST as well, the developer is required to confirm the requirements of the HCD-PP 1.0.

   In addition, results of the test that was performed to validate the entropy source shall be written on the Entropy Description. However, in the case where third-party products [2] other than the developer's are used as entropy sources, and where the documentation contains a description that fails to fully satisfy the requirements of Appendix E, the developer should refer to "2.3.1 Supplementary information when depending on third-party products for entropy sources."

[2] Even though the entropy source is not implemented by the developer but is something like an open-source product, if amount of the raw entropy can be obtained, it will not correspond to a "third-party product."

2. Key Management Description [Appendix F]

Key Management Description is a documentation provided by the developer to ensure that the encryption keys used for the MFPs which are the targets of evaluation are properly protected. The items that need to be included in this Key Management Description are described in Appendix F of the HCD-PP 1.0.

Key management is related to the TOE design, so in the case where its insufficiencies are found in the process of evaluation, the evaluation work is not allowed to be continued. Confirming the appropriateness of key management in advance by the relevant parties will prevent the evaluation work from being interrupted and turning back to the previous evaluation process. Therefore, it is an important input to efficiently and properly conduct evaluations.

3. Evaluator Testing Policies Outline document

In addition to the above Appendixes, the developer is required to submit an outline which describes the information of the testing required for evaluation in terms of assurance activities of the HCD-PP 1.0, upon agreement with the Evaluation Facility on what kind of tools, methods, or tests to be used for confirmation.

In case the requirements for conducting these tests are not clear enough, it is our concern that it might cause an extension of the evaluation work or a withdrawal of the certification application. The developer shall fully comprehend the contents of the testing performed when selecting the Evaluation Facility and it is the developer's responsibility to confirm the testing requirements and policies before submitting a certification application.

Refer to "2.2.2 Description Items for Evaluator Testing Policy Outline document" for the details.

2.2.2. Description Items for Evaluator Testing Policy Outline document

In this document, describe the following items in order to indicate that the developer has judged that the tests required in HCD-PP 1.0 can be performed within the planned period:

A. Planned start date and end date of a test

If the planned period from the application date to the end date of a test exceeds six months, write the reasons.

B. Test Policy by Security Functional Requirement

B.1. Items to be tested

- Identification of test objects

If there are multiple implementations of the same cryptographic algorithm in the TOE, for example, all implementations to be tested will be written.

Example: for RSASSA-PSS using SHA-256, Signature Verification Function, composed of multiple cryptographic algorithms, all the underlying cryptographic algorithms shall be fully described.

- Scope of the supports of test objects

In the specifications regarding the cryptographic algorithm, parameter range/ function that the tested objects support, such as length of GCM mode IV of AES or presence or absence of reseed function of DRBG are written.

B.2. Test Environment

- Composition of devices to be used

If a module modified for a test is used, for example, the name of the module and the modification policy are written. If a substitute environment such as PC is used, the composition of the hardware/ software is also written.

B.3. The content of a test

- Overview of the test to be performed

The explanation that a test according to the assurance activities of HCD-PP 1.0 is performed is written. If supplementation with additional tests is required in the assurance activities, the method of the additional tests or reasons why an additional is unnecessary will be written. Specific conditions in the test for cryptographic algorithm such as length of GCM mode IV of AES or presence or absence of the prediction resistance of DRBG are written.

B.4. Test tools

● Names and purposes of tools used for a test

The purposes of tools are specifically written like "this tool is used for capturing network packets"

Note: never fail to write the security functionality requirements of the following HCD-PP 1.0:

◆ For all the applications:
- FCS_CKM.4 Cryptographic key destruction
- FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
- FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
- FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

◆ When the following "Conditionally Mandatory Requirements (Appendix B) " is included:
- FDP_DSK_EXT.1 Extended: Protection of Data on Disk
- FDP_FXS_EXT.1 Extended: Fax separation

◆ When the following "Selection-based Requirements (Appendix D) " is included:
- FCS_IPSEC_EXT.1 Extended: IPsec selected
- FCS_TLS_EXT.1 Extended: TLS selected

2.3. Interpretation in this Scheme

2.3.1. Supplementary information when depending on third-party products for entropy sources

This section prescribes an approach, under this Scheme, when the developer fails to satisfy the requirements to be described in the Entropy Description by using third-party products as entropy sources.
However, when using a third-party product, if the developer can obtain amount of the raw entropy and can satisfy the requirements to be described for the Entropy Description, it will not fall under this Section.

In principle, when sufficient entropy cannot be provided, there will be a possibility of a problem in the security of encryption. Therefore, the amount of entropy is one of the major concerns in evaluation. However, at present, many developers depend on third-party products for entropy sources, and some of those products have not acquired objective evaluation and certification even for the amount of entropy.
When third-party products are used under this Scheme, it is recommended to use products that have been verified to provide sufficient entropy under Japan Cryptographic Module Validation Program (JCMVP), etc. At the same time, we allow the following tentative approaches regarding entropy evaluation because we believe it is now a transition period for entropy evaluations under this Scheme.

1. Entropy Description [Appendix E]

   In the Entropy Description, the developer itself shall explain at least the following content regarding how an appropriate amount of entropy could be obtained based on the information provided by the manufacturer of the third-party product.

   - Design Description
     - Identification of the third-party product containing the entropy source and its Manufacturer
     - How the entropy source of the third-party product is handled and how it is input as DRBG seeds.

● Entropy Justification

- Amount of the entropy of the third-party product [3]
- How the seed of sufficient amount of entropy is provided in the design from the entropy source to the DRBG.

● Operating Conditions

- Guaranteed operational conditions of the entropy source of the third-party product [4]

● Health Testing

- Specifications of health test of the entropy source of the third-party product [5]
- Specifications for occurrence of failures such as significant decrease in the entropy source and the TOE behaviors based on the specifications.

2. TOE Summary Specification [Security Target]

In the Security Target, it is necessary for the procurement entities to be able to recognize that the evaluation on the entropy source of this product has been conducted based on what kind of information. The developer shall at least include the following information in the TOE Summary Specification of the ST regarding the entropy source.

- The identification and manufacturer of the third-party product which contains the entropy source
- Specification of the amount of entropy of the entropy source (such as an excerpt from the product specification)
- Usage of the entropy source (an explanation of satisfying SFRs)

[3] Determine amount of entropy based on the specifications of the third-party product, the standards to which the product conforms, or thesis about amount of entropy of the product and such.

[4] Describe that satisfying the operation-ensuring conditions of the TOE will satisfy the operation-ensuring conditions of the entropy source.

[5] Describe specifications of health test of the third-party product as far as the developer discloses. If health test of monitoring (from outside the third-party product) decrease of output data within the third-party product after post-processing is performed, pay attention to the content of the post-processing. If DRBG is used for post-processing, a failure will not always be able to be detected by monitoring deviation of post-processing data.

In the description, the developer itself shall explain how to acquire the appropriate amount of entropy, based on the information provided by the manufacturer of the third-party product.

The following shows examples of the TOE Summary Specification.

In order to collect entropy of more than or equal to 256 bits, B chip by A company is used. In the specification of the physical random bit generator of B chip, it outputs random bit of 16 bits for each generation request of random bit string. At this point, there is a fact that B chip, including the random bit generation function, has been evaluated and certified based on the CC, and it is clear from the SFR description in the ST of B chip that the physical random bit generator of B chip provides minimum entropy of more than or equal to 5 bits per 8 bits, in its outputs. Therefore, the TOE requests a random bit string to B chip 52 times, and concatenating the obtained 52 random bit strings of 16 bits results in a bit string of 832 bits. This bit string is assumed to contain entropy of 520 (=832*5/8) bits. This bit string is input as an Entropy Input to HMAC_DRBG that uses HMAC-SHA-512.

2.3.2. Utilization of Japan Cryptographic Module Validation Program (JCMVP)

This section prescribes the utilization policies of verification results under Japan Cryptographic Module Validation Program (JCMVP) when evaluating the appropriateness of cryptographic algorithm based on the HCD-PP 1.0.

IPA operates JCMVP that verifies in accordance with the international standards[6] that cryptographic algorithms are correctly implemented in cryptographic modules and IPA is in the position to ensure that JCMVP is appropriately and strictly operated. Thus, it is allowed to refer to the verification results of JCMVP and to make them as rationales in the evaluations under this Scheme.

[6] ISO/IEC 18367: 2016. Standards created based on the content of the conformance test of cryptographic algorithm implemented by JCMVP and North America CAVP.

It is the evaluator's responsibility to evaluate regarding to which part of each security function and how the cryptographic algorithm implementation will be implemented and to ensure that the verification results of JCMVP are applicable.

2.3.3. Temporary treatment regarding FDP_DSK_EXT.1

Regarding FDP_DSK_EXT.1, use of Field-Replaceable Self Encrypting Nonvolatile Storage Devices (SED) conforming to FDE EE cPP can be selected. However, as of May 2018, due to limited availability of SED products that conform to FDE EE cPP, this Scheme allows SEDs that are verified by JCMVP to be used instead, subject to meeting the following conditions.
Note that the applicable period of this special treatment will be decided considering the market trend or other factors. We will notify the end date of the treatment via the JISEC websites when it is decided.

1. SED that can be substituted

   Field-Replaceable Nonvolatile Storage Devices such as hard disk verified by JCMVP

   Note: the encryption function for the stored data shall be within the certification scope.

2. Description of ST

   The followings shall be explicitly written in TSS:
   - Certificate Number of JCMVP
   - The end terminal of a key chain required by FCS_KYC_EXT.1 shall be BEV in the border of HCD and SED.

3. Evaluation of TOE

   The assurance activities (paragraphs from 962 to 966) against the test may not be performed.

2.3.4. Treatment regarding FCS_RBG_EXT.1 Test

The description of FCS_RBG_EXT.1 Test is written based on the old specification of “The NIST SP 800-90A Deterministic Random Bit Generator Validation System (DRBGVS)” of North America CAVP’s. From the viewpoint that test

results with appropriate referential implementation used should be used, it is permitted that first and second descriptions of the 277th paragraph of HCD-PP 1.0 will be replaced to the following description in order to conform to the latest DRBGVS specification[7].

> If the RBG has prediction resistance enabled, each trial consists of the following functions called in sequence: (1) instantiate DRBG, (2) generate `ReturnedBitsLen` random bits, (3) generate `ReturnedBitsLen` random bits, (4) uninstantiate. Here `ReturnedBitsLen` denotes the number of returned bits from each call to the generate function. The evaluator verifies that the `ReturnedBitsLen` random bits in step (3) is the expected value.

Moreover, it is also permitted that first and second descriptions of the 278th paragraph of HCD-PP 1.0 will be replaced to the following description.

> If the RBG does not have prediction resistance, each trial consists of the following functions called in sequence: (1) instantiate DRBG, (2) reseed, (3) generate `ReturnedBitsLen` random bits, (4) generate `ReturnedBitsLen` random bits, (5) uninstantiate. Here `ReturnedBitsLen` denotes the number of returned bits from each call to the generate function. The evaluator verifies that the `ReturnedBitsLen` random bits in step (4) is the expected value.

2.3.5. Treatment regarding FCS_IPSEC_EXT.1.1

FCS_IPSEC_EXT.1.1, described in the paragraphs 1126-1131 of HCD-PP 1.0, requires IPsec implementation as specified in RFC 4301; and its assurance activity is assumed that an administrator can configure any action of DISCARD, BYPASS or PROTECT in an SPD entry. On the other hand, however, the usage of the evaluated MFPs does not necessarily require BYPASS.

---

[7] The description of 2/14/13 of Update Log of DRBGVS is the relevant part. "Specifications of Cryptographic Algorithm Implementation Testing - Random Number Generators - (ATR-01-E-EN)" of JCMVP's has been revised to support the latest DRBGVS specification.

Therefore, this Scheme allows that the following description is an alternative to the paragraphs 1126-1131 of HCD-PP 1.0.

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

Application Note:

RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g., encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the packet). The SPD can be implemented in various ways, including router access control lists, firewall rulesets, a "traditional" SPD, etc. Regardless of the implementation details, there is a notion of a "rule" that a packet is "matched" against and a resulting action that takes place.

While there must be a means to order the rules, a general approach to ordering is not mandated, as long as the SPD can distinguish the IP packets and apply the rules accordingly. There may be multiple SPDs (one for each network interface), but this is not required.

Assurance Activity:

TSS:

The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet) and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.

As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is

non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.

Operational Guidance:

The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.

Test:

The evaluator uses the guidance documentation to configure the TOE to carry out the following tests:

a) Test 1: The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and (if configurable) allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected

behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation.

b) Test 2: The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.

Note that this treatment is the same contents as the following technical decision of NIAP.

Item	Title	Publication Date
TD0157	FCS_IPSEC_EXT.1.1 - Testing SPDs	2017/06/15

3. Confirming documents to be submitted upon certification application

This Scheme requires checking the contents indicated in this Chapter regarding the ST, Entropy Description, Key Management Description and Evaluator Testing Policy Outline document that were submitted for the application.
This check is aimed at ensuring quality at the time of application, not at the entire, detailed checks. Note that the final assurance will be determined by the Evaluation Facility based on documentation submitted for the evaluation.

3.1. Check Items for ST

1. Whether the scope, characteristics and assumed use environment of the TOE are according to the designation of HCD-PP 1.0 (sections 1.3 and 1.4)
2. Whether, in SFR, the dependency corrected by Errata is applied
3. Whether there is no obvious violation of being Exact Conformance

   No redundant security objectives for the operational environment (that does not exist in HCD-PP 1.0) exists in the ST.

   All SFRs that are required in HCD-PP 1.0 (including Conditionally Mandatory Requirements exist in the ST.

   No redundant SFRs (that do not exist in HDC-PP 1.0) exist in the ST.
4. Whether all necessary items needed when entropy source depends on a third-party product are described
5. Whether the key management description is consistent with the relevant parts

   The following SFR is selected correctly according to the selection of FCS_KYC_EXT.1.

   - FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(f), FCS_KDF_EXT.1, FCS_COP.1(i)

3.2. Check items for Entropy Description

1. Whether all the entropy sources and noise sources listed in FCS_RBG_EXT.1 are dealt with in the Entropy Description
2. As the derivation of randomness, whether an appropriate noise source is used

   There is technical rationale for obtaining entropy from the noise source.
3. Whether a method for obtaining unprocessed (raw) data for a testing purpose is appropriate

   (Supplementary) Unprocessed (raw) data refers to the output from a noise source expressed in numerical value.

4. Whether operational conditions are appropriately described

   (Supplementary) Being able to relate environmental conditions (which are Operational conditions such as temperature, voltage, frequency, option composition, etc.) which may affect the amount of entropy to the TOE-assumed use environment is one of standards regarding appropriateness.

5. Whether seed for generating random bit has adequate amount of entropy

   A test of the amount of entropy is conducted within the scope of the operational conditions.

   In the processing from a noise source until obtaining seed to generate random bit, the amount of entropy obtained from the noise source adequately remain on the seed.

6. Whether the frequency and conditions of health tests are appropriate, and the behavior of the TOE when entropy source failure is detected is described

3.3. Check items for Key Management Description

1. Whether the diagram and explanation of the entire key chain are described
2. Whether all Keys, etc. (DEK or BEV, KEK, Keying materials) related to the encryption of Field-Replaceable Nonvolatile Storage Devices are dealt with in the Key Management Description.
3. Whether the reason for being "Field-Replaceable Nonvolatile Storage Device" is appropriate

   Appropriateness here is not about the implementation method of a storage device, but about whether the reason is in accordance with the note 4 of HCD-PP 1.0 (excerption below):

   A "Field-Replaceable Nonvolatile Storage Device" is any Field-Replaceable Unit (FRU) for which the primary purpose is to provide nonvolatile storage. This OSP does not apply to storage devices that are a non-field-replaceable component of a larger FRU that is not primarily used for storage.

   (Supplementary) "Field-Replaceable Nonvolatile Storage Devices" may be described in the ST as well.

4. Whether a Key is appropriately generated

   (Supplementary) There are lots of conditions to meet for an asymmetric key, and therefore, multiple complex asymmetric-key-generating algorithms

are presented to meet the conditions. It means that after completion of selection of SFR there may still be freedom of selection.
For example, in FIPS 186-4 that FCS_CKM.1(a) refers to, for generating FFC key pair and ECC key pair, two methods, by generating random bits as many as the number of the bits of the necessary private keys or by generating the random bits of 64 more bits than needed for the private key, are specified.
In FIPS 186-4 referred to by NIST SP 800-56B that FCS_CKM.1(a) refers to, there are many options left for generating RSA key pair.

5. Whether Key, etc. are appropriately protected

With non-protected status (plaintext), that key shall not be stored in Field-Replaceable Nonvolatile Storage Device.

6. Whether strength of Key, etc. are appropriate

Inputs from the outside and the entropy source described in the Entropy Description are the source of the strength.

(Supplementary) For FCS_CKM.1(a), any of standards of cryptographic algorithms left for selections requires random bit generation with DRBG for generating an asymmetric key. This is because FCS_CKM.1(a) has implicit dependency to FCS_RBG_EXT.1 that isn't shown in the HCD-PP 1.0 relationship.

Consistent with Key chain

(Supplementary) Attention must be paid to that, depending on a processing of the key chain, the strength may be reduced after its processing.

7. Whether validation of Key, etc. are appropriately performed

When validation (authentication of users or devices) is performed as a condition for TOE to use a key, those authentications shall not become factors to compromise the key security. (As for an example of compromising, brute force against authentication will disclose the values of passwords that are used as sub mask.)

(Supplementary) The following is applied to verification:

- Function of FCS_PCC_EXT.1, FCS_COP.1(h)

8. Whether Key, etc. are appropriately destroyed

For all keys, etc., their storage locations are described.

Key chain and storage locations of key, etc. shall be consistent with when keys, etc. become unnecessary and how they are destroyed.

(Supplementary) Note that all keys, etc. related to encryption of the Field-Replaceable Nonvolatile Storage shall be described about destruction, wherever they are stored.

3.4. Check items for Evaluator Testing Policy Outline document

1. Whether the period from the application date to the planned end date of a test is not overly long

   (Supplementary) If this period exceeds 6 months without rational reasons, some inefficiency in the preparation is suspected.

2. Whether appropriate reference implementation is used for the test of cryptographic algorithm

   (Supplementary) The followings are examples of appropriate reference implementation:

   - A tool (JCATT) approved by JCMVP
   - A tool approved by CMVP

For security functional requirements hereinafter, confirm with the individual Evaluator Testing Policy.

3.4.1. FCS_CKM.4

1. Whether necessary test objects are all covered

   Keys and keying materials that apply to everything in the followings have become test objects.

   - Exist in nonvolatile storages
   - Deleting by designating locations is possible.

2. Whether a test environment and test tools are appropriate

   The values of test-applied keys or keying materials can be recorded.

   Content of a nonvolatile storage can be dumped.

3. The scope of dumping is appropriate

When a range to be dumped is part of a nonvolatile storage, it is made clear that the range is appropriate.

3.4.2. FCS_COP.1(a)

1. Whether necessary test objects are all covered

   All implementations of the symmetrical key encryption for communication are to be tested.

   (Supplementary) The following elements of the SFR are the requirements for symmetrical key encryption for communication.

   - FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.6 in FCS_IPSEC_EXT.1
   - FCS_TLS_EXT.1.1 in FCS_TLS_EXT.1
   - FCS_SSH_EXT.1.4 in FCS_SSH_EXT.1

2. Whether a testing environment and testing tools are appropriate

   To the cryptographic - function implementations, inputting/ outputting data designated by the Specifications of Cryptographic Algorithm Implementation Testing - Symmetric-Key Cryptography - (ATR-01-B-EN), AESAVS, etc. is possible.

3.4.3. FCS_COP.1(b)

1. Whether necessary test objects are all covered

   All implementations regarding signature generation/ verification are applied.

   (Supplementary) The following elements of the SFR are applied to the requirements of signature generation/ verification.

   - FCS_IPSEC_EXT.1.10 in FCS_IPSEC_EXT.1
   - FCS_SSH_EXT.1.2 in FCS_SSH_EXT.1
   - FCS_TLS_EXT.1.1 in FCS_TLS_EXT.1
   - FPT_TUD_EXT.1.3 in FPT_TUD_EXT.1

2. Whether a testing environment and testing tools are appropriate

   To the cryptographic-function implementations, inputting/ outputting data designated by Specifications of Cryptographic Algorithm Implementation Testing - Key Establishment Schemes - (ATR-01-F-EN), DSA2VS, etc. is possible.

3.4.4. FCS_RBG_EXT.1

1. Whether necessary test objects are all covered

All DRBGs listed in the SFR are to be tested.

2. Whether a testing environment and testing tools are appropriate

Inputting/ outputting data against DRBG is possible.

3.4.5. FDP_DSK_EXT.1

1. Whether necessary test objects are all covered

The area (the followings are exempted) of a Field-Replaceable Nonvolatile Storage Device has become a test object.

- Storage devices that have been certified (or to be certified) by FDE EE cPP conformance
- Storage devices whose data-encrypting function has been certified (or to be certified) by JCMVP
- The area that is described in TSS as encryption-not-applied area (check the relevant information on the Key Management Description and confirm that information that should be protected by encryption does not exist.)

2. Whether a testing environment and testing tools are appropriate

Data can be read from the area of the storage device where users' document data and confidential TSF data are written.

The key and keying materials that had been used for encryption can be acquired.

The read data can be decrypted with the acquired key and keying materials by the testing tools.

(Supplementary) Attention should be paid to the consistency between the encrypting method (sector unit, block level, file level) and data-decrypting method. Decrypting may fail without the consistency.

3.4.6. FDP_FXS_EXT.1

1. Whether a testing environment and testing tools are appropriate

A data-communication-enabled modem is used.

(Supplementary) Attention should be paid to "analog-line supported or digital-line supported."

2. Whether the contents of an additional test (or an additional test is unnecessary) and its reasons are appropriate

(Supplementary) For example, when the FAX-communication protocol is extended, a test for that extended protocol is necessary.

3.4.7. FCS_IPSEC_EXT.1

1. Whether a testing environment and testing tools are appropriate

Capturing IP packets, interpreting them as the protocol of IPsec and sending them after modifying are possible.

(Supplementary) Attention should be paid to either of IPv4 or IPv6 or both regarding what the TOE supports. A testing environment according to what the TOE supports is needed.

(Supplementary) When IKEv2 is selected for FCS_IPSEC_EXT.1.5, the environment where NAT is available is needed.

3.4.8. FCS_TLS_EXT.1

1. Whether a testing environment and testing tools are appropriate

Interpreting the communication contents of TCP as the protocol of TLS, modifying and sending them are possible.

(Supplementary) Attention should be paid to either of IPv4 or IPv6 or both regarding what the TOE supports. A testing environment according to what the TOE supports is needed.

4. Supplement regarding evaluation

4.1. Evaluation Technical Report

HCD-PP 1.0 requires that evaluations shall be performed in accordance with the assurance activities described therein. Therefore, HCD-PP 1.0 should be described as the evaluation methods and evaluation criteria which are described in the evaluation technical report.

Furthermore if you apply an interpretation to change the assurance activities of the PP, such as "2.3.3. Temporary treatment regarding FDP_DSK_EXT.1", please additionally describe the identification of this guideline and the section number of the applied interpretation.

Interpretations to be subject to this supplement:

- 2.3.3. Temporary treatment regarding FDP_DSK_EXT.1
- 2.3.4. Treatment regarding FCS_RBG_EXT.1 Test
- 2.3.5. Treatment regarding FCS_IPSEC_EXT.1.1