JISEC

Guideline for Certification Applications and Evaluations with the "collaborative Protection Profile for Hardcopy Devices" Conformance

Version 1.2

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

Issued on May 7, 2025

JISEC

Contents

JISEC

Revision History

Version	Date	Major changes
1.0	2023/10/3	- Initial creation
1.1	2024/6/3	- Being compatible with HCDcPP V1.0e - Adding guidelines for testing Root of Trust cryptographic functions
1.2	2025/5/7	- Adding JISEC policy on technical decisions for HCD-iTC

1 Introduction

This document is the guideline for a certification application and evaluation of IT products that are conformant to the "collaborative Protection Profile for Hardcopy Devices" (hereinafter referred to as the "HCDcPP") under the IT Security Evaluation and Certification Scheme (JISEC) (hereinafter referred to as "this Scheme").

1.1 Target Protection Profile

This guideline targets the following documents.

Table 1 Target Documents

Target Documents	Name	Version	Abbreviations in this document
Protection Profile	collaborative Protection Profile for Hardcopy Devices	1.0e	**[HCDcPP]**
Supporting Document	Supporting Document Mandatory Technical Document Evaluation Activities for collaborative Protection Profile for Hardcopy Devices	1.0e	**[HCD SD]**

1.2 HCD-iTC Technical Decision Application Policy

Technical Decisions ("TDs") for **[HCDcPP]** and **[HCD SD]** from HCD-iTC have been published.

* URL of "Hardcopy Devices iTC Technical Decisions"
  https://hcd-itc.github.io/TD/tech-dec.html

JISEC's policy for applying TDs for HCD-iTC is as follows:

* On the date of receipt of the certification application, all TDs listed on the “Hardcopy Devices iTC Technical Decisions” page that correspond to the versions of **[HCDcPP]** and **[HCD SD]** shall be applied in principle. TDs newly published during the evaluation and certification process may be applied, but are not mandatory.
  TDs found to be defective during evaluation and certification process may not be applied.
  The validity of the TDs applied and not applied will be approved by passing the evaluation and certification.

The applicant and the Evaluation Facility should correspond as follows:

* Applicant
  Applicable TDs shall be listed in the ST. For details on how to list them, refer to Section 2.2.1.1.1.

* Evaluation Facility
  Regardless of whether they are listed in the ST, all applicable TDs in the Evaluation Technical Report shall be listed, and their applicability or non-applicability shall be justified. For details on how to list them, refer to Section 3.3.1.

1.3 Terms

Table 2 shows the terms used in this guideline.

Table 2 Terms

Terms	Definitions
CC	Common Criteria
ETR	Evaluation Technical Report
HCDcPP	collaborative Protection Profile for Hardcopy Devices
HCD-iTC	Hardcopy Device International Technical Community
JCMVP	Japan Cryptographic Module Validation Program
JISEC	Japan Information Technology Security Evaluation and Certification Scheme
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TD	Technical Decision
Entropy Documentation	Evaluation documentation that meets the requirements in "Appendix E: Entropy Documentation and Assessment" of **[HCDcPP]**
Components List	Evaluation documentation (lists of hardware and software components in the TOE) that meets the requirements in "6.6.1.1. Evaluation Activity (Documentation)" of **[HCD SD]**
Key Management Description	Evaluation documentation that meets the requirements in "Appendix F: Key Management Document" of **[HCDcPP]**
Configuration List	Evaluation documentation for Security Assurance Requirements ALC_CMS.1 in CC
Evaluation Activity	Evaluation Activity of **[HCD SD]**

1.4 Referenced documents

Table 3 shows the documents referred to in this guideline.

Table 3 Referenced documents

	Name	Abbreviations in this document
[1]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.	**[CC]**
[2]	Common Methodology for Information Technology Security Evaluation: Evaluation methodology Version 3.1, Revision 5, April 2017, CCMB-2017-04-004	**[CEM]**

2 Certification Application

This chapter describes the documents to be prepared and submitted by an applicant upon certification application for IT products that are conformant to the HCDcPP, as well as any supplementary information to each document.

For interpretation of this scheme regarding the documents required for certification applications, refer to Chapter 4.

2.1 Documents required for submission

In addition to the documents listed in Section 5.1 of the "Guidance on IT Security Certification" (CCM-02-A), the documents listed in Table 4 must be submitted upon certification application.

The following are some points to be noted on the documents in Table 4.

- The descriptions and notes for each document are shown in Section 2.2.
- The documents should be submitted in electronic media. When submitting, make it clear that each document is being submitted by means of a file list or folder/file name.
- The timing of submitting the documents is either at the time of certification application or at the time of Evaluation Technical Reports. In addition, some documents need to be re-submitted when the documents are updated.
- This Scheme will use each submitted document only for certification application as well as confirmation for validity of evaluations. Note that it will not be published on the list of certified products on JISEC website.

Table 4 Additional documents required for submission

Timing of Submission	Document Name	Resubmission for renewal	Public availability
At the time of certification application	Entropy Documentation	Necessary	Closed to the public
	Key Management Description		
	Evaluator Testing Policy Outline document	Unnecessary	
At the time of Evaluation Technical Report	Components List	Necessary	Closed to the public
	Configuration List		
	Guidance Documentation		

2.2 Supplemental information on documents to be submitted

This section provides descriptions and notes on the documents to be submitted (Security Target and documents in Table 4).

2.2.1 Security Target

2.2.1.1 Conformance claim

2.2.1.1.1 PP claim

As a PP that conforms to the following example, the name and version of **[HCDcPP]** should be indicated.

In addition, a list of applicable TDs should be described. The list should include the ID and title of the TDs applicable to [HCDcPP] and [HCD SD].

As indicated in Section 1.2, all TDs that are publicly available on the date of receipt of the certification application should be applied in principle.

Example:

PP claim
The PP to which this ST is conformant is as follows:
Name: collaborative Protection Profile for Hardcopy Devices
Version: 1.0e

The following Technical Decision of the HCD-iTC shall be applied.

ID	Title
HCD0010	Clarification on FPT_SBT_EXT.1 Root of Trust

2.2.1.1.2 Conformance Rationale

As shown in the following example, it should be described in the terms of **[HCDcPP]** that it conforms to the rules shown in the "Conformance to this Protection Profile" of "**2. CC Conformance Claims**" in **[HCDcPP]**.

It should be further described that the TOE type of the TOE is consistent with the TOE type of **[HCDcPP]**.

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, Copying, Configuration, Auditing, Verifying firmware/software updates, Verifying HCD function
> - Conditionally Mandatory Uses
>   Sending PSTN faxes, Receiving PSTN faxes, Storing and retrieving Documents, Nonvolatile Storage Devices
> - Optional Uses
>   Image Overwrite, Wipe Data

2.2.2 Entropy Documentation

The Entropy Documentation is a documentation provided by the developer to ensure that a random number generation function, used in the target of evaluation, provides sufficient entropy required. The details of this Entropy Documentation are described in **Appendix E** of **[HCDcPP]**.

This **Appendix E** requires that the developer measure the minimum entropy of the raw data of the entropy source. However, if a third-party entropy product is used as the entropy source and the developer is unable to obtain the raw data of the entropy source, it is acceptable for the developer to estimate the minimum entropy.

In such a case, the developer is required to provide an estimate of the minimum entropy and an assumption in the Entropy Documentation and Security Target.

If minimum entropy is estimated, the TOE summary specification for the Security Target should include the following.

＊ Manufacturer and identification of third-party products containing entropy

sources

* Estimated minimum entropy of entropy sources
* Rationales of Estimation

  For example, specifications of a third-party product, standards to which the product conforms, or publications on the amount of entropy of the product, which provide the rationale for estimating the minimum entropy.

2.2.3 Key Management Description

Key Management Description is a documentation provided by the developer to ensure that the encryption keys used in 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 **[HCDcPP]** and in the section "KMD" of the evaluation activity for each SFR in **[HCD SD]**.

2.2.4 Evaluator Testing Policy Outline document

For the testing required by the evaluation activities in **[HCD SD]**, the applicant is required to agree with the Evaluation Facility on what tools, techniques and tests will be used to verify the testing and submit an outline of this information in the form of an Evaluator Testing Policy Outline document.

The developer shall fully comprehend the contents of the testing performed, and it is the developer's responsibility to confirm the Evaluation Facility's testing requirements and policies before submitting a certification application.

In this document, the following items should be described in order to indicate that the developer has judged that the tests required in **[HCD SD]** can be performed within the planned period:

A. Planned start date and end date of a test

The planned period dates of the start and end of the test should be described.

If the period between the date of application and the anticipated date of completion of the test exceeds 6 months, its reason should also be described.

B. Test Policy by Security Functional Requirement

For the Security Functional Requirements shown in Table 5, the following B.1 through B.4 should be described.

B.1 Items to be tested

* TOE Identification

  The identification of all TOE models to be tested should be described.

If the TOE includes more than one TOE model and some of these models are selected for testing, the rationale for selecting the TOE models for testing should also be stated.

(For example, a representative model for each considering differences in language, printing speed, model name, options installed, etc., can be selected.)

* Identification of cryptographic algorithm name and implementation

For testing cryptographic algorithms, the name of the cryptographic algorithm and the identification (name and version, etc.) of the cryptographic implementation containing the algorithm should be described.

When testing multiple implementations of the same cryptographic algorithm, the identification of all implementations to be tested should be stated.

B.2 Test Environment

* Composition of devices to be used

The composition of devices to be used for the test should be described.

If a module modified for a test is used, the name of the module and the modification policy should be described.

If a substitute environment such as PC is used, the composition of the hardware/software should also be described.

B.3 The content of a test

* Overview of the test to be performed

An explanation of the tests that will be performed in accordance with the evaluation activities of **[HCD SD]** should be described.

If the supplementation with additional tests is required in the evaluation activities, the method of additional tests or the rationales on which additional tests are not required should be described.

In the case of cryptographic algorithm tests, the specific conditions of the test, such as the IV length for GCM mode of AES, enabling/disabling predictability for DRBG, should be described.

B.4 Test tools to be used

* Identification and purposes of tools used for a test

The identification and purpose of the tools to be used should be described.

The identification of tools should include the name and version, while the purpose should include the role of the tools, such as "used to capture network packets."

Table 5 Security Functional Requirements that Need to be Included in the Evaluator Testing Policy Outline document

∗ **For all the applications:**

FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys)
FCS_CKM.1/AKG Cryptographic Key Generation (for asymmetric keys)
FCS_CKM.2 Cryptographic Key Establishment
FCS_CKM.4 Cryptographic key destruction
FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)
FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)
FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)
FPT_SBT_EXT.1 Secure Boot

∗ **If the following Conditionally Mandatory Requirements are included**

FDP_DSK_EXT.1 Protection of Data on Disk
FDP_FXS_EXT.1 Fax separation

∗ **If the following Optional Requirements are included**

FPT_WIPE_EXT Data Wiping
FCS_TLSC_EXT.2 TLS Client support for mutual authentication
FCS_TLSS_EXT.2 TLS Server support for mutual authentication
FCS_DTLSC_EXT.2 DTLS Client support for mutual authentication
FCS_DTLSS_EXT.2 DTLS Server support for mutual authentication

∗ **If the following Selection-Based Requirements are included**

FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)
FCS_COP.1/KeyWrap Cryptographic operation (Key Wrapping)
FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption)
FCS_COP.1/KeyTransport Cryptographic operation (Key Transport)
FCS_IPSEC_EXT.1 IPsec selected
FCS_TLSC_EXT.1 TLS Client Protocol without mutual authentication
FCS_TLSS_EXT.1 TLS Server Protocol without mutual authentication
FCS_DTLSC_EXT.1 DTLS Client Protocol without mutual authentication
FCS_DTLSS_EXT.1 DTLS Server Protocol without mutual authentication
FCS_SSHC_EXT.1 SSH Client
FCS_SSHS_EXT.1 SSH Server
FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)
FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning
FCS_KDF_EXT.1 Cryptographic Key Derivation
FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication)
FIA_X509_EXT.1 X.509 Certificate Validation
FIA_X509_EXT.2 X.509 Certificate Authentication
FIA_X509_EXT.3 X509 Certificate Requests

2.2.5 Components List

The components list is a list of hardware and software components that compose the TOE provided by the developer for vulnerability assessment.

The contents to be included in the components list are described in Section **6.6.1.1. Evaluation Activity (Documentation)** of **[HCD SD]**.

2.2.6 Configuration List

The Configuration List is the documentation provided by the developer in the evaluation of ALC_CMS.1.

The set of items to be included in the Configuration List is described in **ALC_CMS.1-1** of **CEM**. As follows:

a) the TOE itself;

b) the evaluation evidence required by the SARs in the ST.

Note that an above item b) includes the evaluation documentation (Entropy Documentation, Key Management Description, Components List, etc.) required by the evaluation activity in **[HCD SD]**.

2.2.7 Guidance Documentation

The Guidance Documentation is the guidance documents that constitute the TOE.

Guidance Documentation that describes what is required for the following evaluations should be submitted.

- Guidance Documentation used in the evaluation of ADV and AGD classes for **[CEM]** and **[HCD SD]**
- Guidance Documentation used to evaluate **Guidance Documentation** for **[HCD SD]** evaluation activities.

If the TOE contains multiple guidance document sets with equivalent content, such as one for Japan and one for overseas, it is possible to submit only one of the guidance document sets.

If selecting the one of guidance document set, however, a document that describes the rationales for selection and the summary of differences from other sets should also be submitted.

3 Evaluation

This chapter provides supplementary information for the evaluator in conducting an evaluation of HCDcPP conformance.

For interpretation of this scheme regarding evaluation, refer to Chapter 4.

3.1 Supplementary information on evaluation methods

The evaluation of HCDcPP compliance is performed according to the description in **[HCD SD]**.

In **[HCD SD]**, in addition to the various evaluation activities described in **[HCD SD]**, the evaluation described in **[CEM]** is also required.

However, the evaluation of the following assurance components is performed by replacing the content described in **[CEM]** with the content described in **[HCD SD]**.

- ADV_FSP.1
- AVA_VAN.1

3.2 Supplementary Information on the tests of Cryptographic Algorithm

This section provides supplementary information on the evaluation activities described in **[HCD SD]** for testing the adequacy of cryptographic algorithm implementations.

3.2.1 Utilization of Japan Cryptographic Module Validation Program (JCMVP)

The appropriateness of cryptographic algorithm implementation should be tested in the evaluator test.

However, it is allowed to use the results of the cryptographic algorithm confirmation of the "Japan Cryptographic Module Validation Program (JCMVP)" operated by IPA.

JCMVP is a scheme to verify that cryptographic algorithms are appropriately implemented with in accordance with the international standards[1]. IPA ensures that JCMVP is appropriately and strictly operated.

Therefore, the results of JCMVP are regarded as equivalent to the evaluator tests.

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.

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

3.2.2 Reuse of Test Results

The same implementation of cryptographic module may be used in multiple models of TOEs or different TOEs.

Even in such cases, as a general rule, each TOE model should be tested in the manner required by **[HCD SD]** to confirm the appropriateness of the implementation of each TOE model.

However, it is acceptable to reuse the test results of one TOE model as the test results of another TOE model if the following conditions are met.

* **Conditions for reuse of test results**

  The implementation of the cryptographic algorithm in the TOE that reuses the test results must satisfy all of the following conditions.

  However, if the implementation is hardware, reuse of test results is allowed by satisfying both clause 1 and clause 2.

  1. the identification (name, version, etc.) must be identical to the tested implementation
  2. the same implementation as the tested implementation is called and working
  3. the binary code is identical to the tested implementation
  4. the operating environment is identical to the tested implementation

  If the test results are to be reused, the following information corresponding to the above conditions for reuse should also be included in the evaluation activity's report of evaluation results.

* **What to report when reusing test results**

  1. identification of the tested implementations and identification of the implementations that reuse test results
  2. rationales that the same implementation as the tested implementation is called and working in the TOE that reuses the test results
  3. rationales of identity (e.g., hash values) at the binary level of the tested implementations and the implementations that reuse test results
  4. the operating environment (e.g., specific processor, OS, etc.) of the tested implementations and the implementations that reuse test results

3.3 Supplementary information to the Evaluation Technical Report

This section provides supplementary information on the Evaluation Technical Report.

3.3.1 Evaluation Criteria

As shown in **Section 3.1**, **[HCDcPP]** requires that the evaluation described in **[HCD SD]** also be performed.

Therefore, the Evaluation Methodology and Criteria to be included in the Evaluation Technical Report should describe **[HCD SD]** in addition to **[CC]** and **[CEM]**.

Example:

> Evaluation Criteria, etc.
> 1. Common Criteria for Information Technology Security Evaluation, Version 3.1 Release 5
> 2. Common Methodology for Information Technology Security Evaluation, Version 3.1 Release 5
> 3. Supporting Document Mandatory Technical Document Evaluation Activities for collaborative Protection Profile for Hardcopy Devices, Version 1.0e

In addition, all TDs for the relevant versions of [HCDcPP] and [HCD SD] that are publicly available on HCD-iTC must be listed on the date of receipt of the certification application. Note that the list must include TDs that are not listed in the ST. If any TDs are published and applied after the date of receipt of the certification application, those TDs must be added to the list.

The list should include each TD's ID, title, applicable/non-applicable, and rationale for justification in case of non-applicability.

Example:

> The following shows whether the HCD-iTC's Technical Decision is applicable or not and the rationale for its justification:

ID	Title	Applicability (Y/N)	Rationale for justification
HCD0010	Clarification on FPT_SBT_EXT.1 Root of Trust	Y	
:	:	:	:
HCD00xx	Clarification on ・・・	N	Applicable SFR not claimed

When applying the interpretation in “4 Interpretation of this scheme” of this guideline, the identification of this guideline and the identification of the items of interpretation applied (e.g., “4.1 Measures related to the testing of Root of Trust cryptographic functions”) should also be indicated.

3.3.2 How to report evaluation results

The Evaluation Technical Report should include the following three types of reports.

To ensure that each report is easily identifiable as a separate report, either a dedicated chapter for each report or an individual report should be provided.

A. Report on the evaluation results of [CEM]

The evaluation results of the evaluation replacing the contents of **[CEM]** or **[CEM]** as shown in Section 3.1 of this guideline should be described and reported as per **Section 8.5.5.3.4** of **[CEM]**.

However, if reporting requirements are shown in **[HCD SD]**, as in AVA_VAN.1, the results in a manner that also meets those requirements should be reported.

B. "Public-facing report" of AVA evaluation

AVA_VAN.1 requires a "public-facing report" that does not contain confidential information, in addition to the regular Evaluation Technical Report.

The "public-facing report" should contain the information required in **”A.3. Reporting”** of **[HCD SD]**, separately from the regular Evaluation Technical Report.

For the time being, "public-facing reports" will not be open to the public under this Scheme.

C. Reporting the results of the evaluation of evaluation activities

The evaluation results of the evaluation activities shown in Section 3.1 of this guideline should be described in such a way that the evaluation is reproducible and meets the following

- The correspondence between the individual requirements of the evaluation activities and the evaluation results in **[HCD SD]** should be easily discernible.
- For evaluation activities related to **TSS, KMD, and Guidance Documentation**, include information to identify the evaluation part of the

evaluation evidence document by name of the evidence document and its chapter/section number, etc.

An example of the content of a report of evaluation activity is shown below.

Example of the Report of Evaluation Activity in **[HCD SD]**:

2. Evaluation Results of TSS Evaluation Activities

・・・

2.6.5 FPT_TUD_EXT.1 Trusted Update

Evaluation Activity The evaluator shall check to ensure that the TSS contains a description of mechanisms that verify software for update when performing updates, which is consistent with the definition of the SFR.
Evaluation Results [ST] "7.1 Trusted Update" includes...
Evaluation Activity The evaluator shall check to ensure that the TSS identifies interfaces for administrators to obtain the current version of the TOE as well as interfaces to perform updates.
Evaluation Results [ST] "7.1 Trusted Update" includes...

2.6.6. FTA_SSL.3 TSF-initiated termination

・・・

4 Interpretation of this scheme

This chapter provides the interpretation regarding **[HCDcPP]** or **[HCD SD]** in this scheme. For interpretation (Technical Decision) based on HCD-iTC, refer to Section 1.2.

4.1 Measures related to the testing of Root of Trust

[HCD SD] requires evaluator testing for the various cryptographic algorithms specified in the SFR.

However, the cryptographic functions implemented within the Root of Trust are exceptionally described as follows

Note: Testing of cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1) may not be feasible and independent testing may not be available. In this situation, contact the CC Scheme.

This section prescribes the treatment under the scheme in cases where the above note (hereinafter referred to as the “Note for Root of Trust.”) are applicable.

The scheme requires the following actions when the Note for Root of Trust in **[HCD SD]** is applicable.

* Description of Root of Trust information to the Security Target
  The information to identify the Root of Trust product or implementation (e.g., information that uniquely identifies the product) should be specified in the TOE summary specification for the Security Target.

* Evaluation and Report for Root of Trust
  The evaluator should examine the TOE to verify the following and report the results in the Evaluation Technical Report.
  - The information specifying the Root of Trust in the TOE summary specification and the Root of Trust implemented in the TOE must be identical.
  - The applicable cryptographic functions must be implemented in the Root of Trust of the TOE. (Note: It is acceptable to confirm specifications related to the specified Root of Trust. However, if there are any configurations in the specifications of the Root of Trust product or implementation, it should be confirmed how they are appl

to the TOE.)

- Inability to perform the tests required by **[HCD SD]** for the applicable cryptographic functions