# Certification Report

Buheita Fujiwara, Chairman
Information-Technology Promotion Agency, Japan

**Target of Evaluation**

| | |
|---|---|
| Application date/ID | September 27, 2005 (ITC-5069) |
| Certification No. | C0050 |
| Sponsor | Canon Inc. |
| Name of TOE | Canon MFP Security Chip |
| Version of TOE | 1.00 |
| PP Conformance | None |
| Conformed Claim | EAL3 |
| TOE Developer | Canon Inc. |
| Evaluation Facility | Japan Electronics and Information Technology Industries Association, Information Technology security center (JEITA ITSC) |

This is to report that the evaluation result for the above TOE is certified as follows.
July 4, 2006

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center
Information-Technology Promotion Agency, Japan

**Evaluation Criteria, etc.:** This TOE is evaluated in accordance with the following criteria prescribed in the "General Requirements for IT Security Evaluation Facility".

- Common Criteria for Information Technology Security Evaluation Version 2.1 (ISO/IEC 15408:1999)
- Common Methodology for Information Technology Security Evaluation Version 1.0
- CCIMB Interpretations (as of 01 December 2003)

**Evaluation Result: Pass**

"Canon MFP Security Chip version 1.00" has been evaluated in accordance with the provision of the "IT Product Security Certification Procedure" by Information-Technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

## Table of Contents

1. Executive Summary ..... 1
1.1 Introduction ..... 1
1.2 Evaluated Product ..... 1
1.2.1 Name of Product ..... 1
1.2.2 Product Overview ..... 1
1.2.3 Scope of TOE and Overview of Operation ..... 2
1.2.4 TOE Functionality ..... 4
1.3 Conduct of Evaluation ..... 4
1.4 Certificate of Evaluation ..... 4
1.5 Overview of Report ..... 5
1.5.1 PP Conformance ..... 5
1.5.2 EAL ..... 5
1.5.3 SOF ..... 5
1.5.4 Security Functions ..... 5
1.5.5 Threat ..... 6
1.5.6 Organisational Security Policy ..... 6
1.5.7 Configuration Requirements ..... 6
1.5.8 Assumptions for Operational Environment ..... 7
1.5.9 Documents Attached to Product ..... 7
2. Conduct and Results of Evaluation by Evaluation Facility ..... 8
2.1 Evaluation Methods ..... 8
2.2 Overview of Evaluation Conducted ..... 8
2.3 Product Testing ..... 8
2.3.1 Developer Testing ..... 9
2.3.2 Evaluator Testing ..... 10
2.4 Evaluation Result ..... 11
3. Conduct of Certification ..... 12
4. Conclusion ..... 13
4.1 Certification Result ..... 13
4.2 Recommendations ..... 13
5. Glossary ..... 14
6. Bibliography ..... 16

# 1. Executive Summary

## 1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “Canon MFP Security Chip version 1.00” (hereinafter referred to as “the TOE”) conducted by Japan Electronics and Information Technology Industries Association, Information Technology security center (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, Canon Inc.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to “1.5.9 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

## 1.2 Evaluated Product

### 1.2.1 Name of Product

The target product by this Certificate is as follows:

| | |
|---|---|
| Name of Product: | Canon MFP Security Chip |
| Version: | 1.00 |
| Developer: | Canon Inc. |

### 1.2.2 Product Overview

The TOE is the Canon MFP Security Chip, which is provided to users as a TOE-mounted Security Kit.
With this TOE, the built-in hard drives of Canon’s multifunction products and printers can be protected from confidential information leaks through theft of the hard drive with no trade-off in extensibility, versatility, convenience or performance.
The TOE offers the following security functions for hard drive data protection.

- HDD Data Encryption
- Cryptographic Key Management
- Device Identification and Authentication

### 1.2.3 Scope of TOE and Overview of Operation

#### 1.2.3.1 TOE Scope

The TOE is the entire Canon MFP Security Chip, as depicted in Figure 1-1.

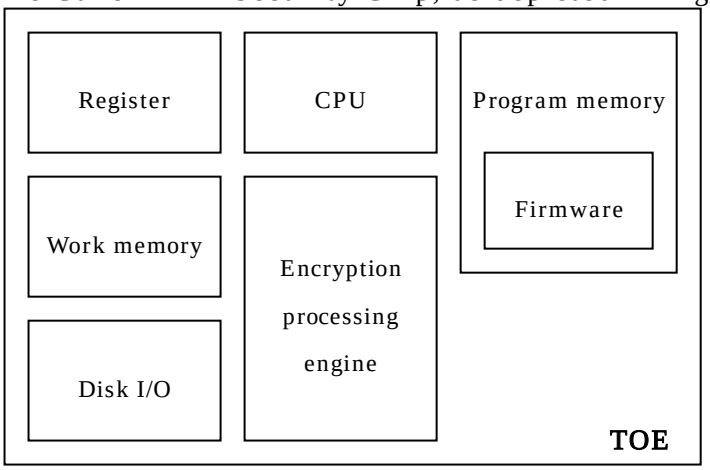


**Figure 1-1: TOE physical composition**

Table 1-1 describes the roles of the components composing the TOE.

**Table 1-1: Roles of TOE components**

| Name | Role |
|---|---|
| Register | Temporarily stores program instructions and computation results. |
| Work memory | Stores data and programs. |
| CPU | Executes programs stored in memory. |
| Program memory | Stores firmware that controls the TOE. |
| Disk I/O | An interface that processes I/O requests to the TOE. |
| Encryption processing engine | Encrypts and decrypts data. |

1.2.3.2 TOE Operational Overview

Figure 1-2 shows the logical configuration of the TOE.

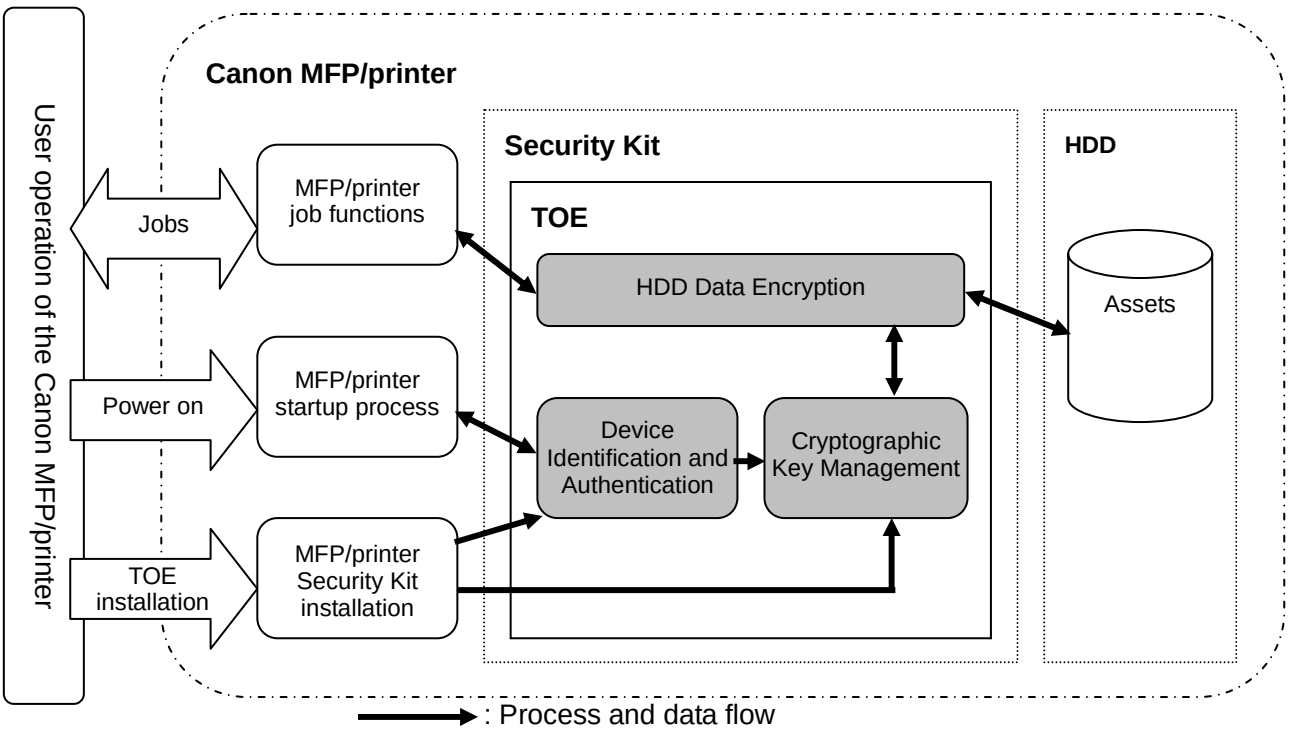


**Figure 1-2: TOE logical configuration**

As depicted in Figure 1-2, users use the TOE through operation of the Canon MFP/printer.

(1) By installing the TOE into the Canon MFP/printer, the user can register seed information for use by the Cryptographic Key Management function and an authentication ID for use by the Device Identification and Authentication function, thanks to the Canon MFP/printer Security Kit installation process. The term "registered device" will be used hereafter to refer to a Canon MFP/printer that is registered by the Canon MFP/printer Security Kit installation process as the original host of the Security Kit.
Of note, an authentication ID contains identification information about the Canon MFP/printer having the Security Kit for which it has been issued.

(2) By powering on the Canon MFP/printer, the user can confirm if the Canon MFP/printer he is using is the "registered device", thanks to the Device Identification and Authentication function.
If the Canon MFP/printer being used is confirmed as the "registered device", the TOE generates a cryptographic key for use by the HDD Data Encryption function, using the Cryptographic Key Management function.

(3) By using the Canon MFP/printer's job functions, such as copying and printing, the user can encrypt and decrypt data writes and reads to/from the HDD, thanks to the HDD Data Encryption function.

### 1.2.4 TOE Functionality

The TOE has the following security functions.

- Allowing the TOE to operate only in the Canon MFP/printer in which the TOE was installed first
- Encrypting input data and writing encrypted data to the HDD in response to HDD write commands
- Reading data from the HDD and decrypting it in response to HDD read commands

## 1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as “IT Security Evaluation and Certification Scheme”[2], “IT Security Certification Procedure”[3] and “Evaluation Facility Approval Procedure”[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined “Canon MFP Security Chip Security Target version 1.08” as the basis design of security functions for the TOE (hereinafter referred to as “the ST”)[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex C of CC Part 1 (either of [5], [8], [11] or [14]) and Functional Requirements of CC Part 2 (either of [6], [9], [12] or [15]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10], [13] or [16]) as its rationale. Such evaluation procedure and its result are presented in “Canon MFP Security Chip Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”)[22]. Further, evaluation methodology should comply with the CEM Part 2 (either of [17], [18] or [19]). In addition, the each part of CC and CEM shall include contents of interpretations (either of [20] and [21]).

## 1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated June, 2006 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body

prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

## 1.5 Overview of Report

### 1.5.1 PP Conformance

There is no PP to be conformed.

### 1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

### 1.5.3 SOF

This ST claims a minimum strength of function level of “SOF-basic”.
This claim is appropriate, because the attack potential of an attacker anticipated in the operational environment for the TOE is defined to be low.

### 1.5.4 Security Functions

Security functions of the TOE are as follow.

- **HDD Data Encryption**
  The TOE performs the following cryptographic operations.
  - Encryption of data writes to the HDD
  - Decryption of data reads from the HDD

  The cryptographic keys and the cryptographic algorithm used for these cryptographic operations are as follows.
  - Cryptographic keys of “256 bits” length
  - The “AES algorithm” that meets FIPS PUB 197

- **Cryptographic Key Management**
  The TOE generates cryptographic keys for use by the HDD Data Encryption function according to the following specifications:
  - The algorithm used for cryptographic key generation is a “FIPS186-2-compliant cryptographic key generation algorithm”.
  - The generated cryptographic key has a length of “256 bits”.

  Cryptographic key management is conducted as follows:
  - Upon startup, the TOE reads the seed information stored in non-volatile memory and generates a cryptographic key.
  - The TOE stores the generated cryptographic key in volatile memory.

  The non-volatile memory where the seed information is stored cannot be accessed from outside the TOE. Also, the cryptographic key is stored in volatile memory and hence disappears upon power-off of the Canon MFP/printer.

- **Device Identification and Authentication**

  Upon startup, the TOE confirms that it is connected to the “registered device” using the authentication ID. To prevent reuse of authentication data related to the authentication mechanism employed for registered device authentication, a standard challenge-and-response authentication scheme is used: a pseudo-random number is generated as a challenge every time the TOE is activated.

  [Authentication ID registration]
  At the time of installation of the Security Kit, the TOE receives an authentication ID from the Canon MFP/printer and saves it to the Flash ROM on the Security Kit.

  [Identification and authentication procedure]
  Upon startup, the TOE generates a pseudo-random number and passes it to the Canon MFP/printer as a challenge code. The Canon MFP/printer then calculates the response based on the authentication ID and the challenge and passes it to the TOE. The TOE performs the same calculation to verify the response.
  If the TOE cannot confirm that it is connected to the “registered device”, the TOE prohibits HDD access.

### 1.5.5 Threat

This TOE assumes such threats presented in Table 1-2 and provides functions for countermeasure to them.

**Table 1-2 Assumed Threats**

| Identifier | Threat |
|---|---|
| T.HDD_ACCESS | A malicious individual may attempt to disclose the data on the HDD by removing the HDD and directly accessing it using a disk analysis tool or another Canon MFP/printer. |
| T.WRONG_BOARD | A malicious individual may attempt to disclose the data on the HDD by moving the Security Kit and the HDD from the “registered device” to another Canon MFP/printer and accessing the HDD via the Security Kit. |

### 1.5.6 Organisational Security Policy

There are no organisational security policies required for using the TOE.

### 1.5.7 Configuration Requirements

The TOE operates mounted on the Security Kit and the Security Kit operates installed in a B Series-ready Canon MFP/printer. Installable Security Kits can be identified in the Canon MFP/printer option list (a list of available options for every model in the Canon MFP/printer lineups).
Users can refer to this option list to find out if and which model in the Security Kit B Series lineup is available for their Canon MFPs/printers. However, it should be noted that there is no Security Kit in the B-series lineup that works with any Canon MFP/printer that does not support the Security Kit B Series boards.

### 1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3. The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

**Table 1-3 Assumptions in Use of the TOE**

| Identifier | Assumptions |
|---|---|
| **A.UNIQUE_INFO** | Any Canon MFP/printer that supports the Security Kit B Series shall retain a unique authentication ID and seed information without alteration. |

### 1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- HDD Data Encryption Kit-B Series Installation Procedure Version 000 (Japanese/English)
- HDD Data Encryption Kit-B Series Reference Guide Version 000 (Japanese)
- HDD Data Encryption Kit-B Series Reference Guide Version 000 (English)

# 2. Conduct and Results of Evaluation by Evaluation Facility

## 2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM Part 2 in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM Part 2.

## 2.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on October, 2005 and concluded by completion the Evaluation Technical Report dated June, 2006. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on February and March, 2006 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on March, 2006.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

## 2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

### 2.3.1 Developer Testing

1) Developer Test Environment

Figure 2-1 and Figure 2-2 show the test configurations used by the developer.

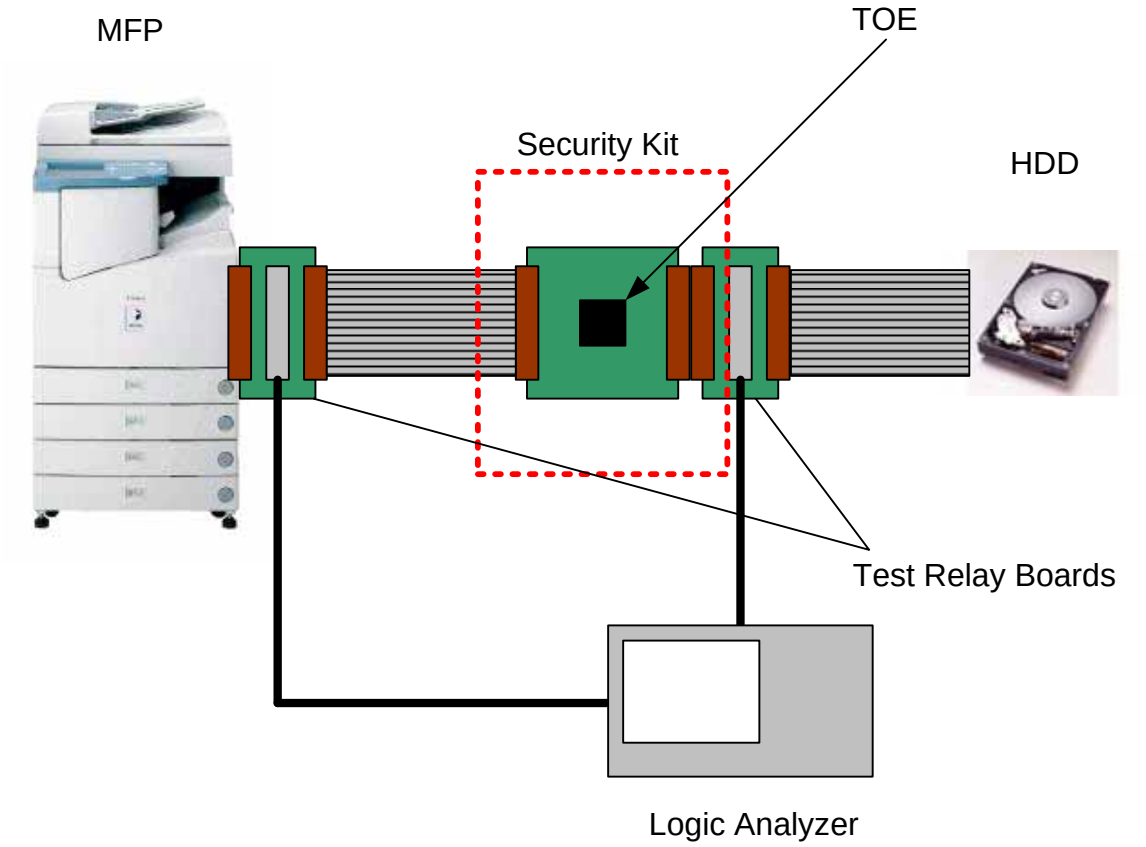


**Figure 2-1: Developer test configuration (MFP-level testing)**

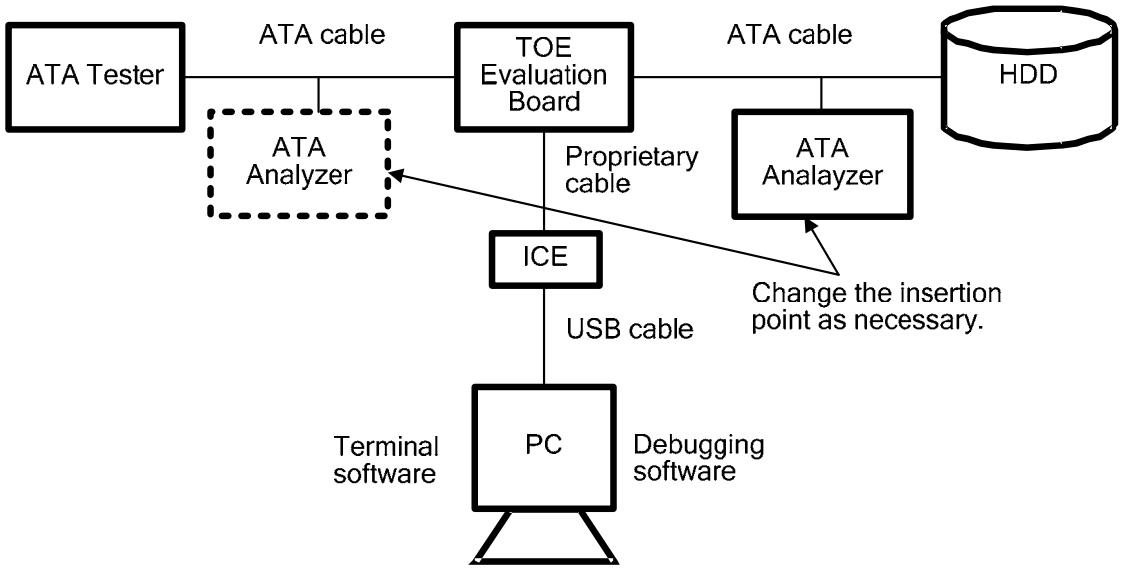


**Figure 2-2: Developer test configuration (firmware-level testing)**

2) Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

a. Test configuration

The configurations of the tests performed by the developer are shown in Figures 2-1 and 2-2.
Figure 2-1 shows the same TOE test environment as the TOE configuration identified in the ST.
The behavior of the TOE in the test environment shown in Figure 2-2 has been confirmed by the evaluator to be consistent with the behavior of the TOE under the configuration identified in the ST.

b. Testing Approach

For the testing, following approach was used.
1. In the MFP-level testing, perform and observe standard operations that are assumed to be performed by human users.
2. In the MFP-level testing, check interface signals using a logic analyzer via test relay boards.
3. In the firmware-level testing, send commands and data directly to the TOE, with an ATA tester as a simulated host. Also, use an ICE to read/write information to/from the TOE's internal memory and check ATA interface signals using an ATA analyzer.

c. Scope of Testing Performed

Testing is performed 62 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

d. Result

The evaluator confirmed consistencies between the expected test results and the actual test results provided by the developer. The Evaluator confirmed the developer testing approach performed and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

### 2.3.2 Evaluator Testing

1) Evaluator Test Environment

The evaluator used test configurations that are identical to those used by the developer.

2) Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

The configurations of the tests performed by the evaluator are shown in Figures 2-1 and 2-2. The evaluator tests were performed in environments identical to the developer test environments.

b. Testing Approach

The evaluator adopted the same testing approach as the developer.

c. Scope of Testing Performed

The evaluator performed 40 tests in total: 12 independent tests and 28 sampled developer tests.

The evaluator devised independent testing with the following taken into account.

1. Supplement the developer tests regarding important security functions (HDD Data Encryption, Cryptographic Key Management and Device Identification and Authentication).
2. Test all security functions.

The evaluator sampled the developer tests with the following taken into account.

1. Include in the testing of all security functions standard operations and operations assumed to be performed by malicious individuals.
2. Include tests that stimulate all TSFI.

d. Result

All evaluator testing conducted is completes correctly and could confirm the behaviour of the TOE. The evaluator also confirmed that all the test results are consistent with the behaviour.

## 2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM Part 2 by submitting the Evaluation Technical Report.

## 3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification review, which were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification review were solved in the ST and the Evaluation Technical Report.

# 4. Conclusion

## 4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL3 assurance requirements prescribed in CC Part 3.

## 4.2 Recommendations

None

# 5. Glossary

The abbreviations used in this report are listed below.

| | |
|---|---|
| CC: | Common Criteria for Information Technology Security Evaluation |
| CEM: | Common Methodology for Information Technology Security Evaluation |
| EAL: | Evaluation Assurance Level |
| PP: | Protection Profile |
| SOF: | Strength of Function |
| ST: | Security Target |
| TOE: | Target of Evaluation |
| TSF: | TOE Security Functions |

The glossaries used in this report are listed below.

Canon MFP/printer:
A general term that refers to a Canon-made multifunction product or printer.

HDD: In this report, this term refers to the built-in hard disk drive of a Canon MFP/printer, unless otherwise noted.

Security Kit: A board with a security chip that is aimed at providing security enhancements. It has a physical interface to a Canon MFP/printer and its HDD.
In this report, this term refers to a Security Kit in the Security Kit B Series lineup.

Security Kit B Series:
A collective term for a specific series of Security Kits using the TOE as a security chip. The B-series Security Kits are completely identical in terms of functionality and the security chip used: they only differ in the product name and the board shape that has a different design for each target Canon MFP/printer model.

The Security Kit B Series includes the following products.
English version: HDD Data Encryption Kit-B Series
French version: Kit d'encryptage des données disque dur-Série B

Disk analysis tool:
A general term that refers to any tool that allows viewing the contents of sectors on hard drives.

Logic analyzer:
A tool that collects data that flows through interfaces.

ATA tester: A tool that sends and receives data and commands that are compliant to ATA, which is the standard HDD interface.

ATA analyzer: A tool that is connected between ATA cables to check ATA interface signals.

ICE: Short for In-Circuit Emulator. A tool that helps debugging by emulating the CPU's behavior.

## 6. Bibliography

[1] Canon MFP Security Chip Security Target version 1.08 (June 29, 2006) Canon Inc.

[2] IT Security Evaluation and Certification Scheme, July 2005, Information-Technology Promotion Agency, Japan EC-01

[3] IT Security Certification Procedure, July 2005, Information-Technology Promotion Agency, Japan EC-03

[4] Evaluation Facility Approval Procedure, July 2005, Information-Technology Promotion Agency, Japan EC-05

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-00-031

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031 (Translation Version 1.2 January 2001)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032 (Translation Version 1.2 January 2001)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033 (Translation Version 1.2 January 2001)

[11] ISO/IEC15408-1: 1999 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model JIS

[12] ISO/IEC 15408-2: 1999 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:1999 - Information technology - Security techniques – Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] JIS X 5070-1: 2000 - Security techniques - Evaluation criteria for IT security - Part 1: General Rules and general model

[15] JIS X 5070-2: 2000 - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[16] JIS X 5070-3: 2000 - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999

[18] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology Version 1.0 August 1999 (Translation Version 1.0 February 2001)

[19] JIS TR X 0049: 2001 – Common Methodology for Information Technology Security Evaluation

[20] CCIMB Interpretations (as of 01 December 2003)

[21] CCIMB Interpretations (as of 01 December 2003) (Translation Version 1.0 August 2004)

[22] Canon MFP Security Chip Evaluation Technical Report Version 1.9, June 29, 2006, Japan Electronics and Information Technology Industries Association, Information Technology security center