Certification Report

Koji Nishigaki, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	2008-03-27 (ITC-8217)
Certification No.	C0215
Sponsor	Canon Inc.
Name of the TOE	Canon MFP Security Chip
Version of the TOE	2.00
PP Conformance	None
Conformed Claim	EAL3
Developer	Canon Inc.
Evaluation Facility	Information Technology Security Center Evaluation Department

This is to report that the evaluation result for the above TOE is certified as follows.
2009-06-17

Takumi Yamasato, Technical Manager
Information Security Certification Office
IT Security Center

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 2.3
- Common Methodology for Information Technology Security Evaluation Version 2.3

Evaluation Result: Pass

"Canon MFP Security Chip Version 2.00" has been evaluated in accordance with the provisions of the "IT 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 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of "Canon MFP Security Chip Version 2.00" (hereinafter referred to as the “TOE") conducted by Information Technology Security Center Evaluation Department (hereinafter referred to as the "Evaluation Facility"), and it reports to the sponsor, Canon Inc.

Readers of the Certification Report are advised to read the corresponding ST and manuals attached to the TOE (please refer to "1.5.9 Documents Attached to Product" for further details) 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 the ST. The operational conditions and functional specifications are also described in the documents 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 an 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 the CC and the CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product of this Certificate is as follows:

Name of Product: Canon MFP Security Chip
Version: 2.00
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 HDD Data Encryption Kit. With this TOE, the built-in hard drives of Canon’s multifunction products and printers can be protected from confidential information leaks through a theft of the hard drive without damaging 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 shown in Figure 1-1.

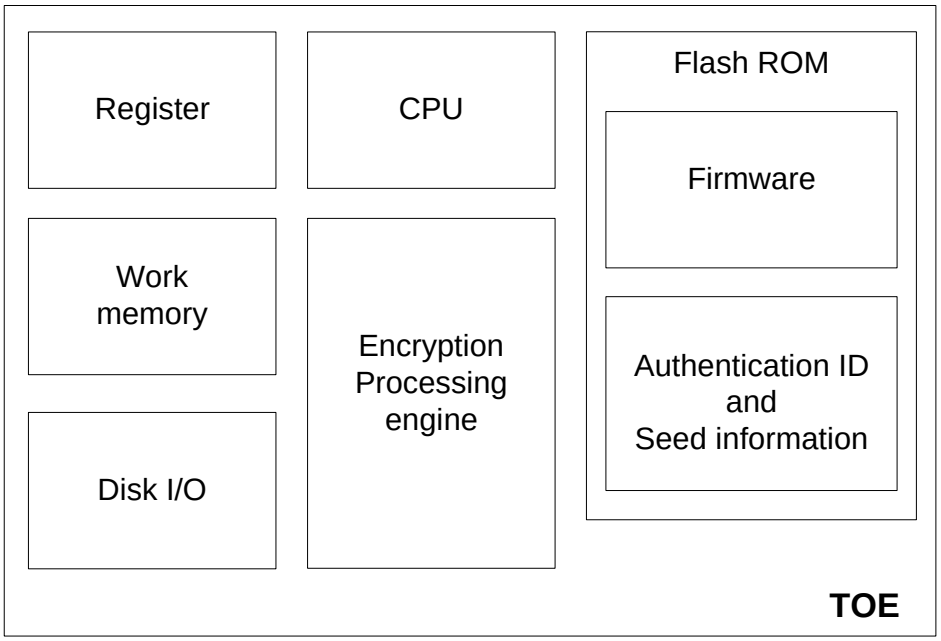

Figure 1-1: TOE physical composition

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 computational results.
Work memory	Volatile memory which stores data and programs; it also stores cryptographic key.
CPU	Executes programs stored in memory.
Flash ROM	Non-volatile memory which stores TOE controlling firmware; it also stores authentication ID and seed information.
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.

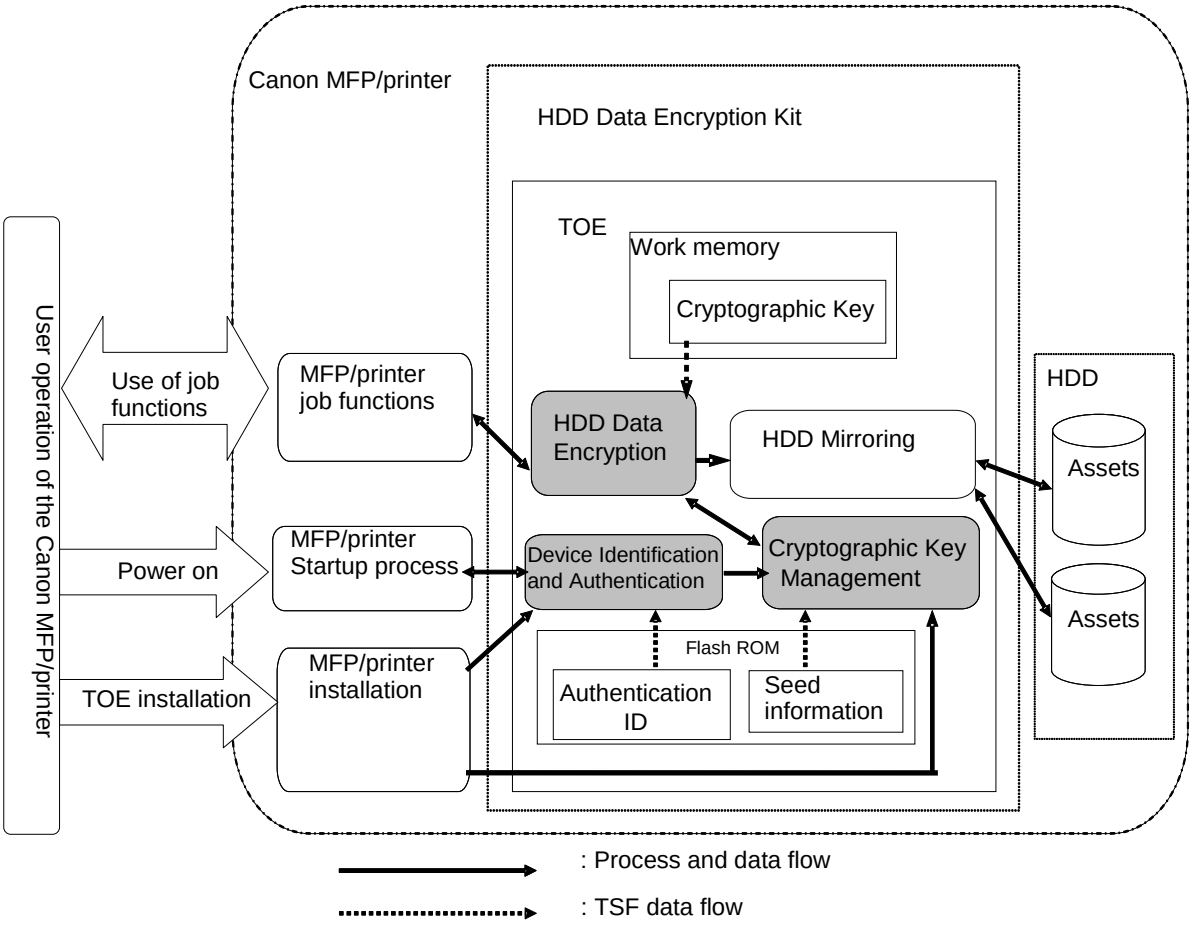

Figure 1-2: TOE operational overview

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

(1) When users install the TOE into the Canon MFP/printer, the Canon MFP/printer can register in Flash ROM, the seed information for use by the Cryptographic Key Management function as well as an authentication ID for use by the Device Identification and Authentication function, thanks to the Canon MFP/printer 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 installation process as the original host of the TOE. Note that an authentication ID contains information which can identify the Canon MFP/printer with the HDD Data Encryption Kit installed.

(2) Once a user powers on the Canon MFP/printer, the TOE can confirm whether the Canon MFP/printer in use is the "registered device", thanks to the Device Identification and Authentication function. If it is confirmed as the "registered device", the TOE generates a cryptographic key to be used by the HDD Data Encryption function in work memory, using the Cryptographic Key Management function.

(3) When a user uses the Canon MFP/printer's job functions, such as copying and printing, the TOE can encrypt and decrypt data to be written to/read from the HDD, thanks to the HDD Data Encryption function.

The TOE also has a mirroring function that allows data to be written simultaneously to two HDDs and data to be read from one HDD, along with the execution of those Canon MFP/printer job functions. In this case, the TOE

encrypts data to be written to both HDDs and decrypts data to be read from one HDD. Note, however, that the TOE can operate in either a single-HDD or dual-HDD configuration.

1.2.4 TOE Functionality

The TOE has the following security functions.

- Limiting 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 them to output 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 were evaluated by the 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].

The scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall satisfy 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 the CEM.

More specifically, the Evaluation Facility examined "Canon MFP Security Chip Security Target" as the basic design of security functions for the TOE (hereinafter referred to as the " ST")[1], the evaluation deliverables in relation to the development of the TOE, and the development, manufacturing and shipping sites of the TOE. The Evaluation Facility evaluated if the TOE satisfies both Annex B of the CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of the CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE satisfy Assurance Requirements of the CC Part 3 (either of [7], [10] or [13]) 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") [18]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

1.4 Certification

The Certification Body verified the Evaluation Technical Report and Observation Report prepared by the Evaluation Facility as well as evaluation evidential materials, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. Certification review was also prepared for those concerns found in the certification process. Evaluation was completed with the Evaluation Technical Report dated 2009-06 submitted by the Evaluation Facility, and those problems

pointed out by the Certification Body were fully resolved and confirmed that the TOE evaluation was appropriately conducted in accordance with the CC and the CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded 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 the TOE defined by this ST is EAL3 conformance.

1.5.3 SOF

This ST claims "SOF-basic" as a minimum strength of function level of the TOE.
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

The security functions of the TOE are described below.

- HDD Data Encryption

  The TOE performs the following cryptographic operations.
  > Encryption of data to be written to the HDD
  > Decryption of data to be read 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 Flash ROM and regenerates a cryptographic key.
  > The TOE stores the generated cryptographic key in work memory.

  The Flash ROM, where the seed information is stored, cannot be accessed from outside the TOE. In addition, the cryptographic key is stored in volatile work 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 the 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 new challenge every time the TOE is activated.

[Authentication ID registration]
At the time of installation of the HDD Data Encryption Kit, the TOE receives an authentication ID from the Canon MFP/printer and saves it to the Flash ROM on the HDD Data Encryption 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 code, 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 the threats identified in Table 1-1 and provides functions to counter them.

Table 1-1 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 HDD Data Encryption Kit and the HDD from the "registered device" to another Canon MFP/printer and accessing the HDD via the HDD Data Encryption Kit. (Refer to the note on T.WRONG_BOARD below.)

Note on T.WRONG_BOARD
In order to counter this threat, the TOE must be capable of identifying each individual Canon MFP/printer. To do this, the TOE-mounted Canon MFP/printer must have an "authentication ID" that is unique to each device.

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 after being mounted on the HDD Data Encryption Kit. The HDD Data Encryption Kit operates after being installed in a Canon MFP/printer, which supports the HDD Data Encryption & Mirroring Kit C Series. Installable HDD Data Encryption 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).

As shown in Figure 1-3, the TOE-mounted HDD Data Encryption & Mirroring Kit C Series is installed in a way that allows all communication between the motherboard and the HDD in the Canon MFP/printer, to take place via the TOE.

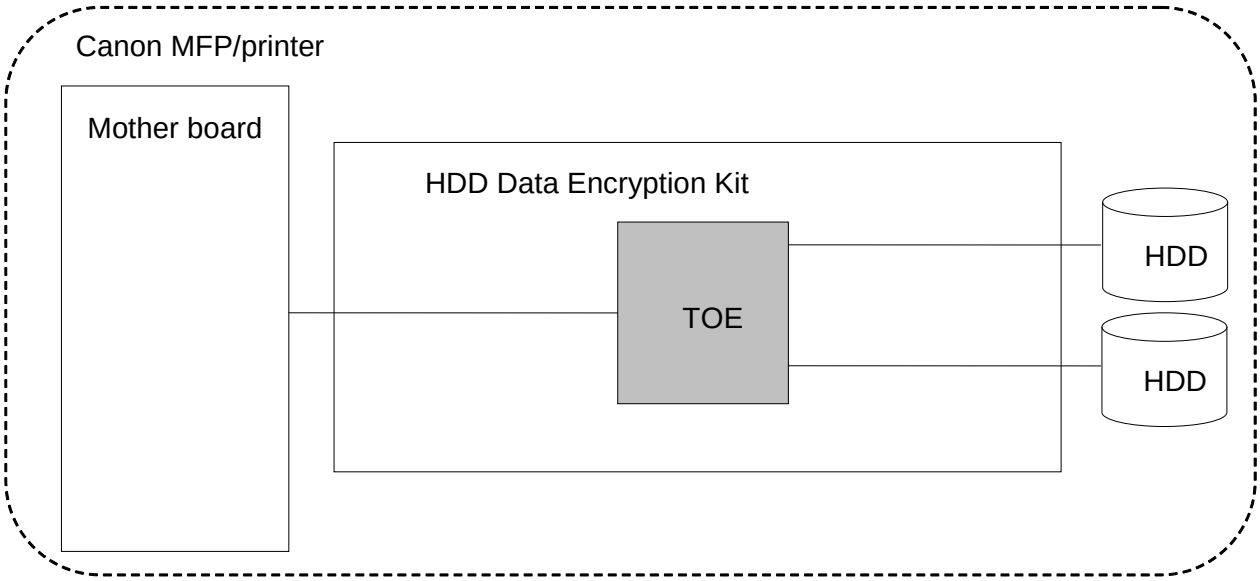

Figure 1-3: TOE, HDD Data Encryption Kit, Canon MFP/printer configuration

The interface between the TOE and the HDD Data Encryption & Mirroring Kit C Series, and the interface between the HDD Data Encryption & Mirroring Kit C Series and the Canon MFP/printer or the HDD, are Serial ATA.

Users can refer to the option list to find out if and which model in the HDD Data Encryption & Mirroring Kit C Series lineup is available for their Canon MFP/printer. However, it should be noted that there is no HDD Data Encryption Kit in the C series lineup that works with any Canon MFP/printer that does not support the HDD Data Encryption & Mirroring Kit C Series.

1.5.8 Assumptions for Operational Environment

There are no assumptions for the operational environment required for using the TOE.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

- HDD Data Encryption Kit-C Series Installation Procedure (Japanese/English) FT1-0323-000
- HDD Data Encryption Kit Reference Guide (Japanese) FT5-2437 (000)
- HDD Mirroring Kit Reference Guide (Japanese) FT5-2439 (000)
- Attached document "Caution" (Japanese) FT5-2438 (000)
- HDD Data Encryption Kit Reference Guide (English) USRM1-4642-00
- HDD Mirroring Kit Reference Guide (English) USRM1-4650-00
- Attached document "Caution" (English) FT5-2441 (000)

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance requirements in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. It describes the overview of the TOE as well as the contents and the verdict of the evaluation by each work unit prescribed in the CEM.

2.2 Overview of Evaluation Conducted

The history of evaluation conducted is presented in the Evaluation Technical Report as follows.

Evaluation has started on 2008-08 and concluded upon completion the Evaluation Technical Report dated 2009-06. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluation conducted. Additionally, the Evaluation Facility directly visited the development and manufacturing sites on 2009-03 and 2009-04 and examined procedural status conducted in relation to each work unit for configuration management, delivery, operation, and lifecycle by investigating records and interviewing staff. As for some portions of procedural status conducted in relation to work unit for delivery and operation, the Evaluation Facility determined that the result that was examined on 2008-03, 2008-04 and 2008-07 as the evaluation of another TOE (that assurance level is same as the TOE) was also reliable at present, and accepted the result as the evaluation of the TOE.

Further, the Evaluation Facility executed a sampling check of the conducted testing by the developer and the evaluator testing by using developer testing environment at developer site on 2009-04.

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

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

2.3 Product Testing

An overview of the developer testing evaluated by the evaluator and the evaluator testing conducted by the evaluator is 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.

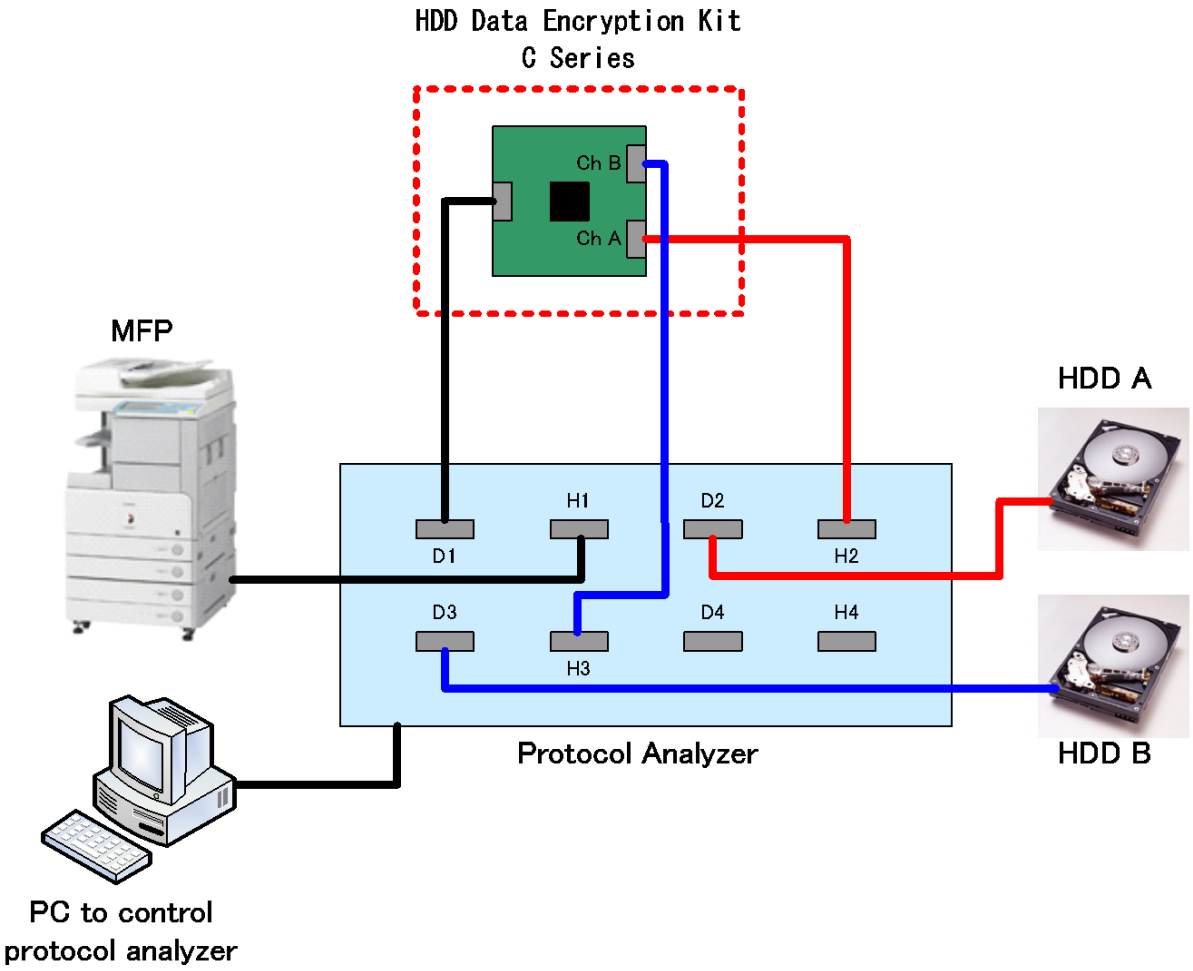

Figure 2-1: Developer test configuration (MFP-level testing)

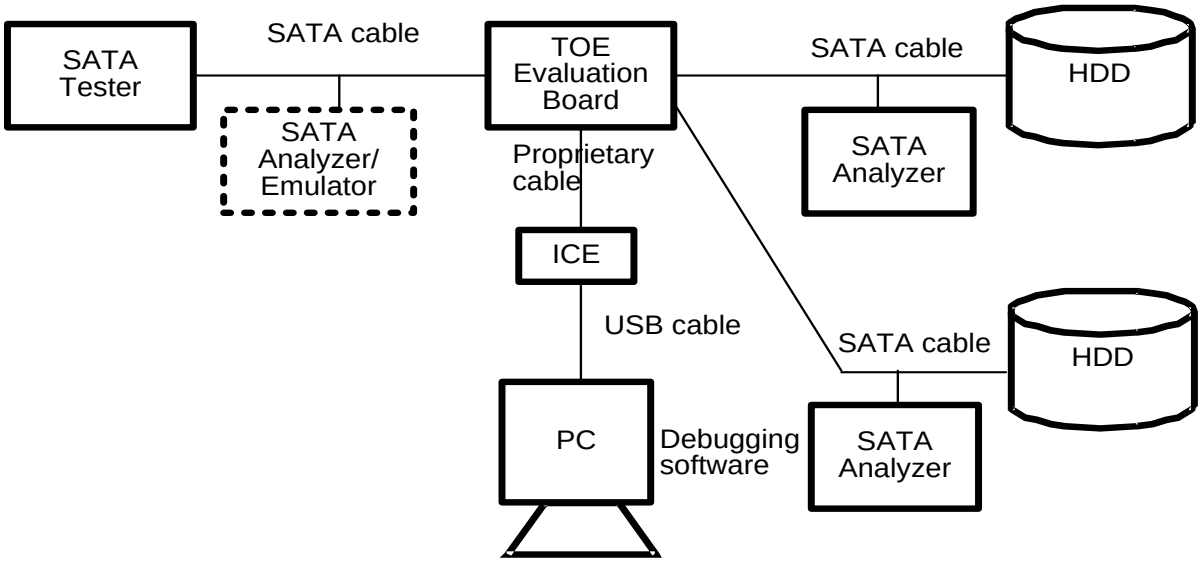

Figure 2-2: Developer test configuration (firmware-level testing)

2) Outline of Developer Testing

An outline of the developer testing is as follows:

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

c. The Scope of Testing Performed

Testing is performed on 155 items by the developer.
The coverage analysis was performed and verified that the security functions and external interfaces described in the functional specification were thoroughly tested. Then, the depth analysis was performed and verified that the subsystems and subsystem interfaces described in the high-level design were all thoroughly tested.

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 the legitimacy of items performed, and confirmed consistency 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) Outline of Evaluator Testing

An outline of the evaluator testing is as follows:

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 the environments identical to the developer test environments.

b. Testing Approach

The evaluator adopted the same testing approach as the developer did.

c. The Scope of Testing Performed

The evaluator conducted a total of 56 items of testing; namely, 16 items devised by the evaluator and 40 items from sampling of developer testing.
The evaluator devised the independent testing by taking into account the following.

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

The evaluator sampled the developer tests by taking into account the following.

1. For all security functions, to include normal operations and operations assumed to be performed by malicious individuals.
2. To include tests that stimulate all TSFI.

Additionally, the evaluator devised and carried out 8 penetration tests in terms of potential vulnerabilities, failures, unanticipated operation, and use of maintenance mode.

d. Result

All evaluator testing conducted has been completed correctly, and the behavior of the TOE was confirmed. The evaluator also confirmed that all the test results are consistent with the behavior.

2.4 Evaluation Result

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

3. Conduct of Certification

The following certification was conducted based on the materials submitted by Evaluation Facility during the 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 the certification process were prepared as certification reviews, which were sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in the Observation Report and certification reviews 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 the CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE satisfies EAL3 assurance requirements prescribed in the CC Part 3.

4.2 Recommendations

4.2.1 Notice on the scope of the security functions and the assets as the target of Evaluation

Regarding the mirroring function of the TOE, there are two notifications described below.

- Although the TOE has a mirroring function, this function is not evaluated as a security function.
- According to the mirroring setting, the scope of encrypted data input/output (whether the encrypted data are input/output from/to one HDD or two HDDs) is changed. However, this scope setting is not the target to be protected.

4.2.2 Notice on the roles of the TOE to counter the threats

Readers of this report should understand a note on T.WRONG_BOARD, which is the threat to be countered by the TOE. See "1.5.5 Threat" for more details.

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.
Disk analysis tool	A general term that refers to any tool that allows viewing the contents of sectors on hard drives.
HDD	In this report, this term refers to the built-in hard disk drive of a Canon MFP/printer, unless otherwise noted.
HDD Data Encryption Kit	A board with a security chip that is aimed at providing security enhancement. It has a physical interface to a Canon MFP/printer and its HDD.
HDD Data Encryption & Mirroring Kit C Series	A collective term for a specific series of HDD Data Encryption Kits using the TOE as a security chip. The C-series HDD Data Encryption 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. In this report, the term "HDD Data Encryption Kit" refers to any HDD Data Encryption Kit C Series lineup. The HDD Data Encryption Kit C Series includes the following products. English version: HDD Data Encryption & Mirroring Kit-C Series French version: Kit d'encryptage et d' écriture des données disque dur-Série C
ICE	Short for In-Circuit Emulator. A tool that helps debugging by emulating the CPU's behavior.

List of Supported Options	A list that indicates the support status of HDD Data Encryption Kit C Series, and the HDD Data Encryption Kits that are available for each Canon MFP/Printer model. Consumers will find this list in their Canon MFP/printer product catalogs.
Protocol analyzer	A tool that captures data being transferred through interface, inserted between the Host (referring to Canon MFP/printer in this report) and the TOE or between the TOE and the HDD.
SATA analyzer	A tool that is connected between SATA cables to check SATA interface signals.
SATA tester	A tool that sends/receives data and commands that are compliant with SATA, which is the standard HDD interface.
Serial ATA	Serial ATA is a standard for connecting a storage device, which uses serial transmission to transfer data. It offers faster data transfer compared with the traditionally-used Parallel ATA. It can be abbreviated as SATA.

6. Bibliography

[1] Canon MFP Security Chip Security Target Version 1.05 (February 2, 2009) Canon Inc.

[2] IT Security Evaluation and Certification Scheme, May 2007, Information-technology Promotion Agency, Japan CCS-01

[3] IT Security Certification Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-02

[4] Evaluation Facility Approval Procedure, May 2007, Information-technology Promotion Agency, Japan CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16] ISO/IEC 18045:2005 Information Technology - Security techniques - Methodology for IT security evaluation

[17] Canon MFP Security Chip Evaluation Technical Report Version 2.6, June 4, 2009, Information Technology Security Center Evaluation Department