Certification Report

Tatsuo Tomita, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation (TOE)

Application Date/ID	2015-02-20 (ITC-5534)
Certification No.	C0506
Sponsor	Canon Inc.
TOE Name	HDD Data Encryption Kit E-Series
TOE Version	2.10
PP Conformance	None
Assurance Package	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.

2016-04-25

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

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

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

Evaluation Result: Pass

"HDD Data Encryption Kit E-Series" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" 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

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "HDD Data Encryption Kit E-Series, Version 2.10" (hereinafter referred to as the "TOE") developed by Canon Inc., and the evaluation of the TOE was finished on 2016-04-13 by Information Technology Security Center, Evaluation Department (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, Canon Inc., and provide security information to procurement entities and consumers who are interested in the TOE.

Readers of the Certification Report are advised to read the Security Target (hereinafter referred to as the "ST") that is provided along with this report. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the TOE are described in the ST.

This Certification Report assumes "procurement entities who purchase the TOE" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the TOE conforms, and does not guarantee an individual IT product itself.

1.1 Product Overview

An overview of the TOE functions and operational conditions is described as follows. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package of the TOE is EAL3.

1.1.2 TOE and Security Functionality

The TOE is an optional hardware product to encrypt data to be stored in the HDD mounted on Canon Multifunction Printer (hereinafter referred to as "MFP") and Single Function Printer (hereinafter referred to as "SFP").

The TOE provides functions to encrypt data to be stored in the HDD and to test these encryption capabilities.

Regarding these security functionalities, the validity of the design policy and the accuracy of the implementation were evaluated within the scope of the assurance package. Threats and assumptions that the TOE assumes are described in the following sections.

1.1.2.1 Threats and Security Objectives

The TOE assumes the following threat and provides the security functions to counter them.

Administrators can detach the HDD of Canon MFP/SFP to which the TOE is attached. Therefore, there is a threat of unauthorized reading data from the detached HDD.

To prevent unauthorized access to the data in the detached HDD, the TOE provides data encryption function and other security functions to support it.

1.1.2.2 Configuration and Assumptions

The evaluated product is assumed to be operated under the following configuration and assumptions.

The TOE is used by mounting on the following Canon MFP/SFP.

- imagePRESS C10000VP, imagePRESS C8000VP
- imagePRESS C65, imagePRESS C650

It is assumed that the Canon MFP/SFP to which the TOE is attached will be located in a controlled environment where it is protected from unauthorized physical access.

1.1.3 Disclaimers

The following functions provided by the TOE are outside the scope of the assurance provided by this evaluation.

- Functions of the TOE to identify and authenticate the Canon MFP/SFP registered at the time of installation

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed on 2016-04, based on functional requirements and assurance requirements of the TOE according to the publicized documents "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report [13] and the Observation Reports prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the TOE evaluation was conducted in accordance with the prescribed procedure. The certification oversight reviews were also prepared for those concerns found in the certification process. Those concerns pointed out by the Certification Body were fully resolved, and the Certification Body confirmed that the TOE evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]). The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the Evaluation Facility and fully concluded certification activities.

2. Identification

The TOE is identified as follows:

TOE Name:	HDD Data Encryption Kit E-Series
TOE Version:	2.10
Developer:	Canon Inc.

The following two products are included in the HDD Data Encryption Kit E-Series. These two products are different in names only, and their components are the same.

- HDD Data Encryption & Mirroring Kit-E1
  This product is for imagePRESS C10000VP and imagePRESS C8000VP.

- HDD Data Encryption & Mirroring Kit-E2
  This product is for imagePRESS C65 and imagePRESS C650.

Users can verify that a product is the evaluated and certified TOE by the following means.

1) TOE Name

Users can verify that the name printed in the outer package of the product is as follows. Note that "HDD Data Encryption & Mirroring Kit-E1" is common for Japan and other countries.

- HDD Data Encryption & Mirroring Kit-E1:

  (Japanese name) HDD Data Encryption/Mirroring Kit-E1
  (English name) HDD Data Encryption & Mirroring Kit-E1
  (French name) Kit d'encryptage et d'écriture du disque dur-E1

- HDD Data Encryption & Mirroring Kit-E2 (for Japan):

  (Japanese name) HDD Data Encryption/Mirroring Kit-E2

- HDD Data Encryption & Mirroring Kit-E2 (for other countries than Japan):

  (English name) HDD Data Encryption & Mirroring Kit-E2
  (French name) Kit d'encryptage et d'écriture du disque dur-E2

2) Version

Users can verify the version of the TOE by displaying the version information on the control panel of the Canon MFP/SFP to which the TOE is attached according to the procedure specified in the TOE guidance and confirming that the "Canon MFP Security Chip" is "2.10."

3. Security Policy

This chapter describes security function policies that the TOE adopts to counter threats, and organizational security policies.

To prevent unauthorized access to data on the HDD detached from Canon MFP/SFP, the TOE provides a function to encrypt data to be stored in the HDD.

In addition, the TOE provides the function to generate hard-to-guess cryptographic keys and the self-test function to verify that the encryption function works properly, in order to support the encryption function

3.1 Security Function Policies

The TOE possesses the security functions to counter the threats shown in Section 3.1.1 and to satisfy the organizational security policies shown in Section 3.1.2.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The TOE assumes the threat shown in Table 3-1 and provides the security functions to counter them.

Table 3-1 Assumed Threat

Identifier	Threat
T.HDD_ACCESS	User Data on the HDD may be exposed if an attacker wrongfully obtains HDD removed from Canon MFP/SFP and directly accesses the HDD using a disk analysis tool because HDD can be detached.

Note:
Based on the assumptions described in Chapter 4, attackers cannot remove the HDD by themselves. However, the HDDs removed by administrators are outside the scope of the assumptions, and the above threat therefore may exist.

3.1.1.2 Security Function Policies against Threats

The TOE counters the threat shown in Table 3-1 by the following security function policy. The details of each security function are described in Chapter 5.

1) Countermeasures against threat "T.HDD_ACCESS"

The TOE counters the threat by the following functions: "HDD data encryption function" and "Cryptographic key management function."

"HDD data encryption function" of the TOE encrypts data to be written in the HDD and

decrypts data to be read from the HDD. Either 128-bit or 256-bit AES is used as the encryption algorithm.

The "Cryptographic key management function" of the TOE generates cryptographic keys using random number generation algorithm in accordance with Hash_DRBG in SP800-90A [14].

With these functions, the TOE prevents unauthorized exposure of data from the HDD by encrypting data to be written in the HDD using cryptographic keys whose randomness is assured.

3.1.2 Organizational Security Policies and Security Function Policies

3.1.2.1 Organizational Security Policies

The organizational security policy required in use of the TOE is shown in Table 3-2.

Table 3-2 Organizational Security Policy

Identifier	Organizational Security Policy
P.TSF_VERIFICATION	Self-test must be performed to detect failed HDD data encryption functions and broken cryptographic keys.

3.1.2.2 Security Function Policies to Organizational Security Policies

The TOE provides the security functions to satisfy the organizational security policy shown in Table 3-2. Details of each security function are described in Chapter 5.

1) Means of organizational security policy "P.TSF_VERIFICATION"

This policy is realized by "Self-test function."

"Self-test function" of the TOE performs known answer tests for encryption algorithm used in "HDD data encryption function" and "Cryptographic key management function." In addition, the integrity of the software code in the TOE and the key seed information to be used for cryptographic key generation is verified.

With this function, the TOE detects failed HDD data encryption function and broken cryptographic keys.

4. Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment to operate the TOE as useful information for the assumed readers to determine the use of the TOE.

4.1 Usage Assumptions

Table 4-1 shows the assumption to operate the TOE. The effective performances of the TOE security functions are not assured unless this assumption is satisfied.

Table 4-1 Assumption in Use of the TOE

Identifier	Assumption
A.PHYSICAL_ACCESS_MANAGED	Canon MFP/SFP to which the TOE is attached is installed in a controlled environment where physical access to the TOE by people with harmful intent is restricted.

4.2 Environmental Assumptions

The TOE is an optional product for Canon MFP/SFP and is used by attaching to Canon MFP/SFP. The overview of the internal configuration of Canon MFP/SFP to which the TOE is attached is shown in Figure 4-1.

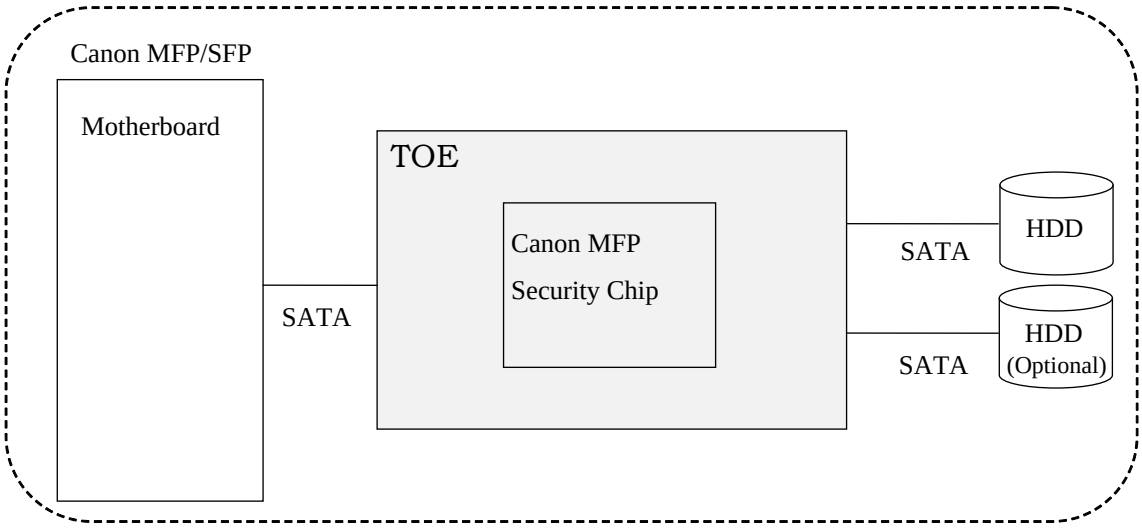

Figure 4-1 Operational Environment of the TOE

The TOE is shown at the center of Figure 4-1. The TOE consists of a circuit board, on which Canon MFP Security Chip is mounted in order to implement the security functions, and cables required for its connection. The TOE is connected between the motherboard and HDD in Canon MFP/SFP using SATA interfaces.

The operational environment of the TOE consists of the following components.

1) Canon MFP/SFP

The followings are the models of Canon MFP/SFP that support the TOE. Note that the size of cryptographic keys supported is different for each model.

- Models that support cryptographic key size of 128 bits:
  imagePRESS C10000VP, imagePRESS C8000VP

- Models that support cryptographic key size of 256 bits:
  imagePRESS C65, imagePRESS C650

2) HDD

The TOE provides the mirroring function, and two HDDs can be connected. However, the use of the mirroring function is not mandatory, and the system can be operated with only one HDD.

It should be noted that the reliability of Canon MFP/SFP shown in this configuration is outside the scope of this evaluation. Those are assumed to be trustworthy.

4.3 Clarification of Scope

The size of cryptographic keys, either 128 bits or 256 bits, is specified depending on the model of Canon MFP/SFP and cannot be changed by users.

5. Architectural Information

This chapter explains the scope and the main components (subsystems) of the TOE.

5.1 TOE Boundary and Components

Figure 5-1 shows the configuration of Canon MFP/SFP with the TOE attached.

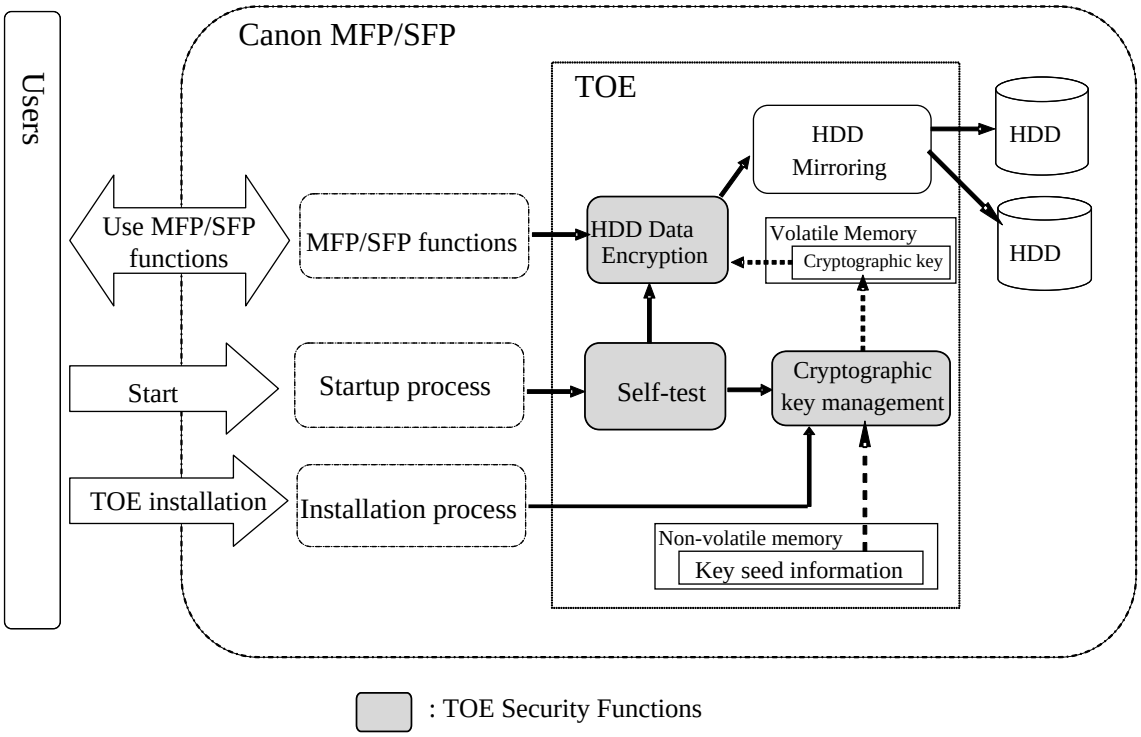

Figure 5.1 TOE boundary

The TOE consists of "HDD data encryption function," "Cryptographic key management function" and "Self-test function" which are security functions, and "HDD mirroring function" which is a general function. These functions work automatically when users operate Canon MFP/SFP.

Security functions of the TOE are described as follows.

1) HDD data encryption function

This is a function to encrypt data to be written in the HDD and to decrypt data to be read from the HDD. Either 128-bit or 256-bit AES is used as the encryption algorithm.

2) Cryptographic key management function

This is a function to generate cryptographic keys to be used in the HDD data encryption function. A random number generation algorithm in accordance with Hash_DRBG in SP800-90A is used to generate cryptographic keys. SHA-256 is used as the hash function.

When the TOE is installed, it generates key seed information, using the information specified from Canon MFP/SFP and variation of HDD access time, and stores the information.

Then, the TOE generates cryptographic keys from the key seed information. Cryptographic keys generated are stored in the volatile memory and disappear when the power of the device is turned off. Next time the device is turned on, the TOE will generate the same cryptographic key from the key seed information stored in it.

3) Self-test function

This is a function to perform the following self-test when the TOE is started.

- CRC verification of the firmware and key seed information in the TOE
- Known answer test (for each AES/Hash_DRBG/SHA-256 algorithm)

Startup process of the TOE is performed in the following cases, and the operation stops if an error occurs in the self-test.

- When the power is turned on (Canon MFP/SFP is not involved)
- When a reset command is issued from Canon MFP/SFP

5.2 IT Environment

The TOE operates on Canon MFP/SFP.

Canon MFP/SFP performs the following operations to the TOE.

- When the TOE is installed, it instructs the TOE of the cryptographic key size and information to be used for key seed generation.
- It issues a reset command to the TOE during the startup process of Canon MFP/SFP.
- It writes data to the HDD and reads data from the HDD in response to user operations.

Canon MFP/SFP will perform the above operations automatically, so users are not required to make any special settings or operations to use the TOE.

6. Documentation

The identification of documents attached to the TOE is listed below. TOE users are required to fully understand and comply with the following documents in order to satisfy the assumptions.

1) In case of "HDD Data Encryption & Mirroring Kit-E1"

All the guidance documents listed in Table 6-1 are attached.

Table 6-1 List of Guidance Documents

Number	Name	Version
1	HDD Data Encryption & Mirroring Kit-E Series Installation Procedure HDD Data Encryption & Mirroring Kit-E Series Installation Procedure (in Japanese)	FT2-0299(010)
2	HDD Data Encryption Kit Users Guide (in Japanese)	FT6-1331(010)
3	HDD Mirroring Kit Users Guide (in Japanese)	FT6-1335(000)
4	Make sure to read this notice before using this product. (in Japanese)	FT6-1332(000)
5	HDD Data Encryption & Mirroring Kit-E Series User Documentation	FT6-1333(010)
6	Make sure to read this notice before using this product.	FT6-1334(000)

2) In case of "HDD Data Encryption & Mirroring Kit-E2" (for Japan)

The guidance documents No.1, No.2, No.3 and No.4 listed in Table 6-1 are attached.

3) In case of "HDD Data Encryption & Mirroring Kit-E2" (for other countries than Japan)

The guidance documents No.1, No.5 and No.6 listed in Table 6-1 are attached.

7. Evaluation conducted by Evaluation Facility and Results

7.1 Evaluation Facility

Information Technology Security Center, Evaluation Department that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which is agreed on mutual recognition with ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

7.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance components in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report. The Evaluation Technical Report explains the summary of the TOE as well as the content of the evaluation and the verdict of each work unit in the CEM.

7.3 Overview of Evaluation Activity

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

The evaluation has started on 2015-02 and concluded upon completion of the Evaluation Technical Report dated 2016-04. 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 evaluator directly visited the development and manufacturing sites on 2015-06, 2015-07, 2015-08, 2015-09, 2016-02 and 2016-03, and examined procedural status conducted in relation to each work unit for configuration management, delivery and development security by investigating records and interviewing staff. Furthermore, the evaluator conducted the sampling check of the developer testing and the evaluator testing by using the developer testing environment at the developer site on 2015-06, 2015-09 and 2016-02.

Concerns found in evaluation activities for each work unit were all issued as the Observation Reports, and those were reported to the developer. Those concerns were reviewed by the developer, and all the concerns were solved eventually.

Concerns that the Certification Body found in the evaluation process were described as the certification oversight reviews, and those were sent to the Evaluation Facility. After the Evaluation Facility and the developer examined them, those concerns were reflected in the Evaluation Technical Report.

7.4 IT Product Testing

The evaluator confirmed the validity of the testing that the developer had performed. As a result of the evidence shown in the process of the evaluation and those confirmed validity, the evaluator performed the reproducibility testing, additional testing and penetration testing based on vulnerability assessments judged to be necessary.

7.4.1 Developer Testing

The evaluator evaluated the integrity of the developer testing that the developer performed and the documentation of actual testing results. The content of the developer testing evaluated by the evaluator is explained as follows.

1) Developer Testing Environment

The developer performed two types of tests: a test to confirm the details of the TOE operation without using Canon MFP/SFP (hereinafter referred to as "firmware level testing") and a test to confirm the operation of the TOE in its operational environment by using Canon MFP/SFP (hereinafter referred to as "MFP level testing").

Figures 7-1 and 7-2 show configurations of those tests performed by the developer, and Tables 7-1 and 7-2 show components of each configuration.

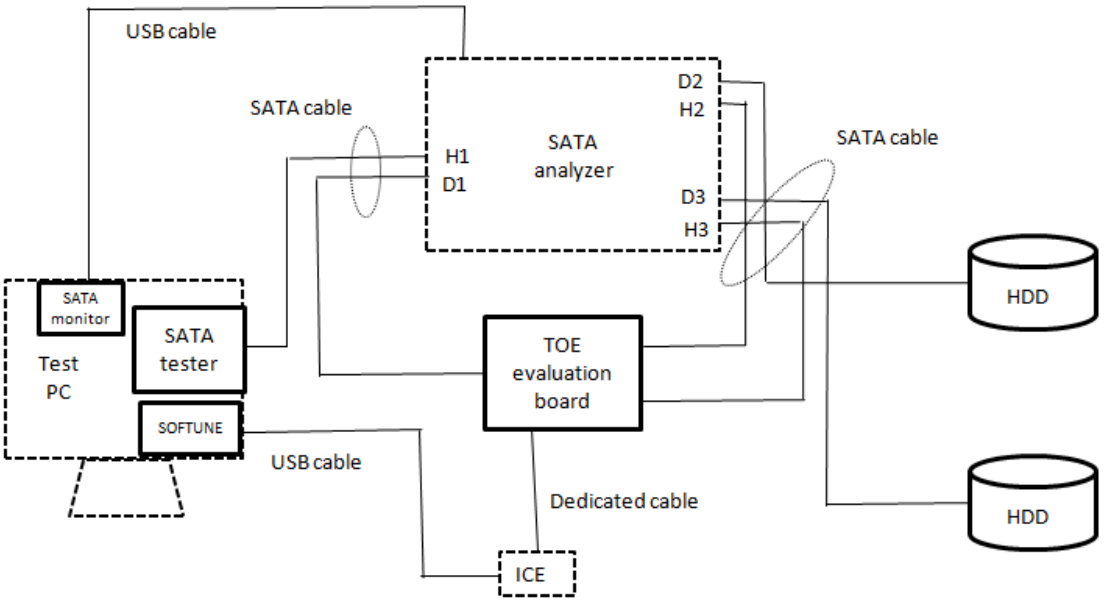

Figure 7-1 Configuration of the Developer Testing (Firmware level testing)

Table 7-1 Components of the Developer Testing (Firmware level testing)

Name		Description
TOE evaluation board		It is used in place of the TOE. It is the same as the TOE except for the followings. - There is no cover to physically protect Canon MFP Security Chip. - There is a connector for ICE connection.
Test PC		It is used to issue SATA commands to the TOE instead of Canon MFP/SFP and to operate SATA analyzer and ICE. - A PC with Windows 7 Professional SP1 installed *The following software is installed.
	SATA tester	It sends/receives SATA commands according to the specified script. - DriveMaster2012Pro by TOYO Corp.
	SATA monitor	It controls SATA analyzer and displays data of SATA interfaces. - LeCroy SATA Protocol Suite Software version 4.20
	Debugger (SOFTUNE)	It controls ICE and debugs the TOE firmware. - Fujitsu FR IDE Softune Workbench V60L08
SATA analyzer		It acquires data of SATA interfaces between the test PC and TOE evaluation board, and between the TOE evaluation board and HDD. - Catalyst STX-431
ICE		ICE MB2198 for Fujitsu FR
HDD		- Western Digital WD30EZRX (used for various tests) - Western Digital WD10EURX (used for random number entropy measurement)

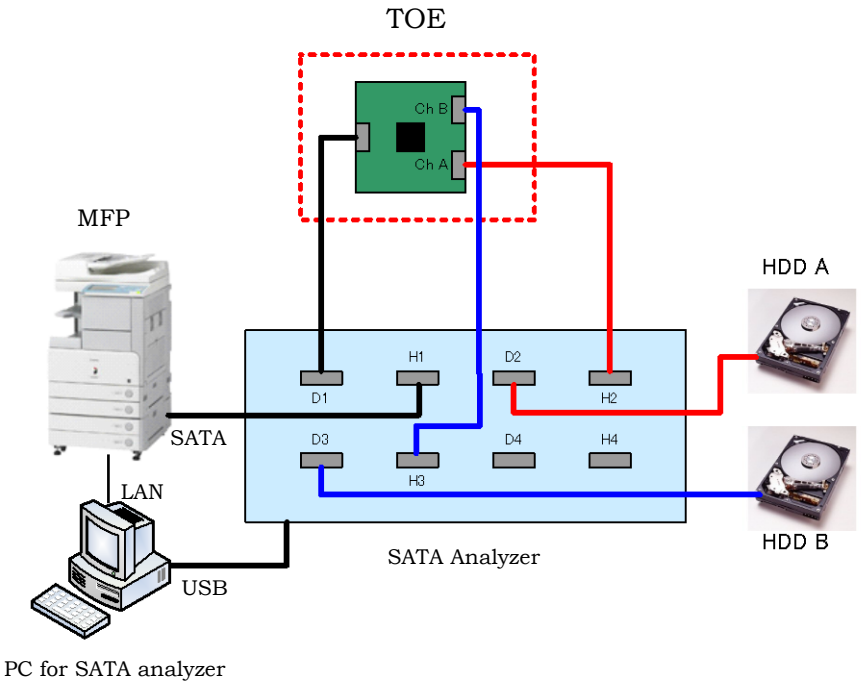

Figure 7-2 Configuration of the Developer Testing (MFP level testing)

Table 7-2 Components of the Developer Testing (MFP level testing)

Name	Description
TOE	- HDD Data Encryption & Mirroring Kit-E1, Version 2.10 - HDD Data Encryption & Mirroring Kit-E2, Version 2.10 *In the test to check the case when the self-test fails, the firmware modified for the test was installed on the TOE evaluation board shown in Table 7-1.
MFP HDD A HDD B	The MFP with the TOE attached. The following two models were used. a) imagePRESS C10000VP, version 10.02 - imagePRESS Server B5000, which is a required option, is installed - HDD A (standard): Western Digital WD2500HHTZ - HDD B (optional): Western Digital WD2500HHTZ b) imagePRESS C650, version 30.52 - HDD A (standard): Western Digital WD10EURX - HDD B (optional): Western Digital WD10EURX

SATA analyzer		It acquires data of SATA interfaces between the MFP and TOE, and between the TOE and HDD. - Catalyst STX-431
PC for SATA analyzer		It is used to operate SATA analyzer (via USB) and install MFP (via LAN). - A PC with Windows 7 Professional SP1 installed *The following software is installed.
	SATA monitor	It controls SATA analyzer and displays data of SATA interfaces. - LeCroy SATA Protocol Suite Software version 4.00
	Maintenance tool	It is used to install software and data for MFP to the HDD to be encrypted. - SST version 4.72J

In the firmware level testing and part of the MFP level testing, TOE evaluation board was used instead of the TOE. The evaluator considers that there is no problem to use it in the developer testing because the only difference of the TOE and TOE evaluation board is if there are physical cover and connector or not. The evaluator also determines that the test results are not affected by the addition of ICE and SATA analyzer.

Among all the models that support the TOE, the models of Canon MFP/SFP tested by the developer are imagePRESS C10000VP and imagePRESS C650 only. The evaluator determines that it is sufficient to test those models only in the developer testing because the same software is installed in the other models that are not tested in the developer testing.

Therefore, it can be considered that the developer testing was performed in the same TOE testing environment as the TOE configuration identified in the ST.

2) Summary of the Developer Testing

A summary of the developer testing is as follows.

a. Developer Testing Outline

An outline of the developer testing is as follows.

<Developer Testing Approach>

(1) Behavior that can be confirmed with the external interface provided by the TOE

For the external interface of the TOE, the developer makes entries by using the test PC or MFP to verify the response and MFP operation. In addition, the developer verifies data of SATA interfaces by using SATA monitor.

(2) Behavior that cannot be confirmed with the external interface provided by the TOE

For the internal data of the TOE that cannot be verified using the interface provided by the TOE, the developer uses a debugger for confirmation.

Further, the developer verifies self-test and encryption algorithms by using the firmware modified to test the module as follows:

- The developer verifies the self-test with the same approach as (1) using the firmware modified to always fail in the self-test.

- The developer obtains the results of execution using firmware modified to execute the input to/output from the module with extended command of SATA interfaces using SATA tester. The developer verifies that the encryption algorithms as specified are implemented by comparing the acquired data with known answers and by analyzing such data.

<Developer Testing Tools>

Table 7-3 shows tools used in the developer testing.

Table 7-3 Developer Testing Tools

Tool Name	Outline and Purpose of Use
SATA monitor + SATA analyzer *See Tables 7-1 and 7-2.	It displays data of SATA interfaces between the test PC/MFP and TOE, and between the TOE and HDD.
SATA tester *See Table 7-1	It sends/receives SATA commands according to the specified script.
Debugger + ICE *See Table 7-1	It sets breakpoints in the TOE process and displays data in process.
Firmware for the developer testing	Firmware modified for the developer testing. The modules to be tested are the same as the TOE. - For self-test verification (7 types) - For encryption algorithm verification (3 types) - For random number entropy measurement (1 type)

<Content of the Performed Developer Testing>

Various inputs were provided to the TOE in order to verify that the security functions operate in accordance with the specification.

It was confirmed that the results match the known answers for encryption algorithms: AES, Hash_DRBG and SHA-256. In addition, the entropy of information to be used in the generation of key seed information was measured, and it was confirmed that the requirements of SP800-90A are satisfied.

b. Scope of the Performed Developer Testing

The developer testing was performed by the developer on 206 items for the firmware level testing and on 7 items for MFP level testing. By the coverage analysis, it was verified that all security functions and external interfaces described in the functional specification had been sufficiently tested. By the depth analysis, it was also verified that all the subsystems and subsystem interfaces described in the TOE design had been sufficiently tested.

c. Result

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

7.4.2 Evaluator Independent Testing

The evaluator performed the sample testing to reconfirm the execution of security functions by the test items extracted from the developer testing. In addition, the evaluator performed the evaluator independent testing (hereinafter referred to as the "independent testing") to gain further assurance that security functions are certainly implemented, based on the evidence shown in the process of the evaluation. The independent testing performed by the evaluator is explained as follows.

1) Independent Testing Environment

The configuration of the independent testing performed by the evaluator is the same as the configuration of the developer testing. The independent testing was performed in the same environment as the TOE configuration identified in the ST.

The components and testing tools used in the independent testing environment were the same as those used in the developer testing, and their validity confirmation and behavior tests were performed by the evaluator.

2) Summary of the Independent Testing

A summary of the independent testing is as follows.

a. Viewpoints of the Independent Testing

Viewpoints of the independent testing that the evaluator designed from the developer testing and the provided evaluation documentation are shown below.

<Viewpoint of Independent Testing>

(1) The evaluator verifies the input variations and combinations that were not tested by the developer.

(2) The evaluator verifies the behaviors and configurations that were not tested by the developer.

(3) For the sample testing, the evaluator extracts test items from those of the developer testing based on the following viewpoints.

- Verifying the interfaces related to security functions.

- Verifying the testing with different testing approach.

b. Independent Testing Outline

An outline of the independent testing that the evaluator performed is as follows.

<Independent Testing Approach>

The same testing approach as the developer testing was used for the independent testing.

<Independent Testing Tools>

The same testing tools as those used in the developer testing with additional tools for independent testing were used. Table 7-4 shows additional tools used in the independent testing.

Table 7-4 Additional Tools for Independent Testing

Tool Name	Outline and Purpose of Use
Firmware for the independent testing	Firmware modified for the independent testing. The modules to be tested are the same as the TOE. - For self-test verification (4 types) - For encryption algorithm verification (3 types)

<Content of the Performed Independent Testing>

The evaluator performed the sample testing on 21 items (19 items for firmware level testing and 2 items for MFP level testing), and the additional testing on 19 items (14 items for firmware level testing and 5 items for MFP level testing) from the above viewpoints of independent testing.

Table 7-5 shows viewpoints of the independent testing and the content of the testing corresponding to them.

Table 7-5 Content of the Performed Independent Testing

Viewpoint	Outline of the Independent Testing
Viewpoint (1) (Firmware level)	- The evaluator verifies that the self-test function works in accordance with the specification using the firmware modified in different places from the developer testing. - The evaluator verifies the known answers that were not verified by the developer for each encryption algorithm. - The evaluator verifies series of actions by executing multiple SATA commands in combination on the assumption that the MFP is used.
Viewpoint (1) (MFP level)	- The evaluator verifies the testing for cryptographic generation, which was performed by turning on the power by the developer, through recovery operation from MFP sleep mode.

Viewpoint (2) (Firmware level)	- The evaluator verifies that, after failing in the self-test, attempting to write in the HDD fails with error, and no data can be written in the HDD.
Viewpoint (2) (MFP level)	- The evaluator verifies the testing performed in the HDD mirroring configuration by the developer with single HDD configuration. - The evaluator verifies that data encryption function works properly by attempting to write data to HDD/read data from HDD from the MFP while the data are being copied between two HDDs for mirroring settings.

c. Result

All the independent testing performed by the evaluator was correctly completed, and the evaluator confirmed the behavior of the TOE. The evaluator confirmed consistencies between the expected behavior and all the testing results.

7.4.3 Evaluator Penetration Testing

The evaluator devised and performed the necessary evaluator penetration testing (hereinafter referred to as the "penetration testing") on the potentially exploitable vulnerabilities of concern under the assumed environment of use and attack level from the evidence shown in the process of the evaluation. The penetration testing performed by the evaluator is explained as follows.

1) Summary of the Penetration Testing

A summary of the penetration testing performed by the evaluator is as follows.

a. Vulnerability of Concern

The evaluator searched into the provided documentation and the publicly available information for the potential vulnerabilities, and then identified the following vulnerabilities which require the penetration testing.

(1) There is a concern that the encryption function may be disabled by using the interfaces for administrator and maintenance of Canon MFP/SFP.

Note that, for cryptographic keys, the evaluator determines that attackers with the assumed attack potential cannot obtain or guess the cryptographic keys and key seed information under the operational environments that satisfy the assumptions, based on the analysis of the mechanism to generate cryptographic keys, the developer testing and independent testing for the mechanism.

b. Penetration Testing Outline

The evaluator performed the following penetration testing to identify potentially exploitable vulnerabilities.

<Penetration Testing Environment>

The penetration testing was conducted in the same environment as the evaluator independent testing.

<Content of the Performed Penetration Testing>

Table 7-6 shows a vulnerability of concern and the content of the corresponding penetration testing.

Table 7-6 Content of the Performed Penetration Testing

Vulnerability	Penetration Testing Outline
Vulnerability (1)	The evaluator examined the menus for administrators and operation mode for maintenance in the MFP and verified that no operation related to the TOE exists, except for the mirroring ON/OFF operation in the maintenance mode.

c. Result

In the penetration testing performed by the evaluator, the evaluator did not find any exploitable vulnerabilities that attackers who have the assumed attack potential could exploit.

7.5 Evaluated Configuration

The TOE operates by being attached to Canon MFP/SFP that supports the TOE, and there are no other conditions for configuration such as settings.

7.6 Evaluation Results

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

In the evaluation, the following were confirmed.

- Security functional requirements: Common Criteria Part 2 Conformant

- Security assurance requirements: Common Criteria Part 3 Conformant

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components.

- All assurance components of EAL3 package

The result of the evaluation is only applied to those which are composed by the TOE corresponding to the identification described in Chapter 2.

7.7 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to procurement entities.

8. Certification

The Certification Body conducted the following certification based on the materials submitted by the Evaluation Facility during the evaluation process.

1. Contents pointed out in the Observation Reports shall be adequate.

2. Contents pointed out in the Observation Reports shall properly be solved.

3. The submitted documentation was sampled, the content was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report.

4. Rationale of the 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 the certification oversight reviews, and those were sent to the Evaluation Facility.

The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the ST and the Evaluation Technical Report and issued this Certification Report.

8.1 Certification Result

As a result of verification of the submitted Evaluation Technical Report, Observation Reports and related evaluation documentation, the Certification Body determined that the TOE satisfies all assurance requirements for EAL3 in the CC Part 3.

8.2 Recommendations

The TOE supports two cryptographic key sizes: 128 bits and 256 bits. However, the size of cryptographic key to be used is specified by the Canon MFP/SFP to which the TOE is attached, and the key size cannot be changed. The procurement entities who are interested in the TOE need to confirm the key size that can be used before making decisions for purchase.

9. Annexes

There is no annex.

10. Security Target

The Security Target [12] of the TOE is provided as a separate document along with this Certification Report.

HDD Data Encryption Kit E-Series Security Target, Version 1.18, April 8, 2016, Canon Inc.

11. Glossary

The abbreviations relating to the CC 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
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the TOE used in this report are listed below.

ICE	In-Circuit Emulator
MFP	Multifunction Printer
SATA	Serial ATA
SFP	Single Function Printer

The definitions of terms used in this report are listed below.

Canon MFP Security Chip	ASIC to realize the security functions of the TOE.

12. Bibliography

[1] IT Security Evaluation and Certification Scheme Document, June 2015, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2015, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2015, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001 (Japanese Version 1.0, November 2012)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002 (Japanese Version 1.0, November 2012)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003 (Japanese Version 1.0, November 2012)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004 (Japanese Version 1.0, November 2012)

[12] HDD Data Encryption Kit E-Series Security Target, Version 1.18, April 8, 2016, Canon Inc.

[13] CANON HDD Data Encryption Kit E-Series Evaluation Technical Report, Version 1.23, April 13, 2016, Information Technology Security Center, Evaluation Department

[14] NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015, National Institute of Standards and Technology