# HDD Data Encryption Kit E-Series
# Security Target

Version 1.18
2016/04/08

Canon Inc.

This document is a translation of the evaluated and certified security target written in Japanese.

# Table of Contents

# 1 ST Introduction

This chapter describes ST reference, TOE reference, TOE overview, notational conventions, terms and abbreviations, TOE description, scope of the TOE, and assets to be protected.

## 1.1 ST Reference

This section provides the Security Target (ST) identification information.

ST name: HDD Data Encryption Kit E-Series Security Target
Version: 1.18
Issued by: Canon Inc.
Date of Issue: 2016/04/08

## 1.2 TOE Reference

This section provides the TOE identification information.

TOE name: HDD Data Encryption Kit E-Series
Version: 2.10
Created by: Canon Inc.

The TOE can be identified by one of the following product names:
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
Japanese name: HDD Data Encryption/Mirroring Kit-E2
*English name: HDD Data Encryption & Mirroring Kit-E2
French name: Kit d'encryptage et d'écriture du disque dur-E2

## 1.3 Notational Conventions, and Terms and Abbreviations

### 1.3.1 Notational Conventions

In sections Organizational Security Policies (Chapter 3), Assumptions (Chapter 3), and Security Objectives (Chapter 4), each label is indicated in **bold** typeface, followed by the definition in normal typeface.
In Security Requirements (Chapter 6), details are underlined.

### 1.3.2 Terms and Abbreviations

Table 1 defines terms and abbreviations used in the ST.

**Table 1 —Terms and Abbreviations**

| Terms/Abbreviations | Description |
|---|---|
| Canon MFP/SFP | A collective name for Canon MFPs (Multi Function Printers) and SFPs (Single Function Printers) |
| HDD | Hard disk drive mounted on Canon MFP/SFP |
| HDD Data Encryption & Mirroring Kit | "HDD Data Encryption & Mirroring Kit" is the product name of "HDD Data Encryption Kit E-Series", which is the TOE provided as an option product according to the type of connection with supported MFP/SFP. |
| Disk analysis tool | A collective name for tools to look at the contents of HDD sectors. |
| Key seed information | Information to generate cryptographic keys. At the start-up, the TOE regenerates cryptographic keys using the key seed information stored in it. |

| Terms/Abbreviations | Description |
|---|---|
| List of supported options | A list containing the support status of HDD Data Encryption Kit E-Series and the HDD Data Encryption Kit E-Series installable to each Canon MFP/SFP.<br>To be distributed to consumers as the product sales catalogue for Canon MFP/SFP. |
| Serial ATA | A standard for HDD connection and uses serial transmission mode. |

## 1.4 TOE Overview

The TOEs are option products for Canon MFP/SFP. They are IT products designed to encrypt data in the HDD of Canon MFP/SFP.

### 1.4.1 Purpose of Use of the TOE

The TOE is used to counter the problems of leakage of data stored in the HDD of Canon MFP/SFP. By using the TOE, the data to write in the HDD can be encrypted without compromising scalability and processing performance of Canon MFP/SFP.

### 1.4.2 Operational Environment of the TOE

This section describes hardware/software required when using the TOE, except for the TOE itself.
To use the TOE, Canon MFP/SFP is required. For each Canon MFP/SFP model, there is a list of supported options to provide information on option products that can be installed. Canon MFP/SFP on which the TOE can be installed is identified by this list.
Users can find out if a Canon MFP/SFP model supports the TOE and which TOE can be installed on a particular MFP/SFP. Note that there are two products of HDD Data Encryption Kit E-series: HDD Data Encryption & Mirroring Kit-E1 and HDD Data Encryption & Mirroring Kit-E2. The product that can be installed depends on the model of Canon MFP/SFP.
Following table shows the Canon MFPs/SFPs on which the TOE can be installed.

**Table 2 — Canon MFP/SFP Supported by the TOE**

| Product Name of the TOE | Supporting Canon MFP/SFP |
|---|---|
| Japanese name: HDD Data Encryption/Mirroring Kit-E1<br>English name: HDD Data Encryption & Mirroring Kit-E1<br>French name: Kit d'encryptage et d'écriture du disque dur-E1 | imagePRESS C10000VP<br>imagePRESS C8000VP |
| Japanese name: HDD Data Encryption/Mirroring Kit-E2<br>English name: HDD Data Encryption & Mirroring Kit-E2<br>French name: Kit d'encryptage et d'écriture du disque dur-E2 | imagePRESS C65<br>imagePRESS C650 |

Canon MFPs are multifunction printers that provide job functions such as copy, print, Universal Send, fax, I-Fax functions while Canon SFPs are printer products that provide print function only. Canon MFP/SFP writes document and other data to HDD and reads document and other data stored in HDD when executing job functions. The TOE protects data to write in HDD by encrypting them.

### 1.4.3 How to use the TOE

The TOEs are option products for Canon MFP/SFP and are provided to users as HDD Data Encryption Kit for Canon MFP/SFP. To use the TOE, it should be installed on a Canon MFP/SFP. Once the TOE is installed, HDD access using functions of Canon MFP/SFP is automatically made via the TOE.

### 1.4.4 Primary Security Functions of the TOE

The TOE provides the following security functions to protect HDD.

- HDD data encryption function
- Cryptographic key management function
- Self-test function

## 1.5 TOE Description

This section describes the stakeholders of the TOE, assets to be protected, and scope of the TOE.

### 1.5.1 Stakeholders of the TOE

The following is the stakeholder of the TOE. Note that no special role and privilege are necessary to use the TOE.

- Users
  Users of Canon MFP/SFP. They use the functions of the TOE by installing HDD Data Encryption Kit to Canon MFP/SFP and using the functions of Canon MFP/SFP such as copy, printer and scanner functions.

### 1.5.2 Assets to be Protected

Assets of the TOE is User Data

#### 1.5.2.1 User Data

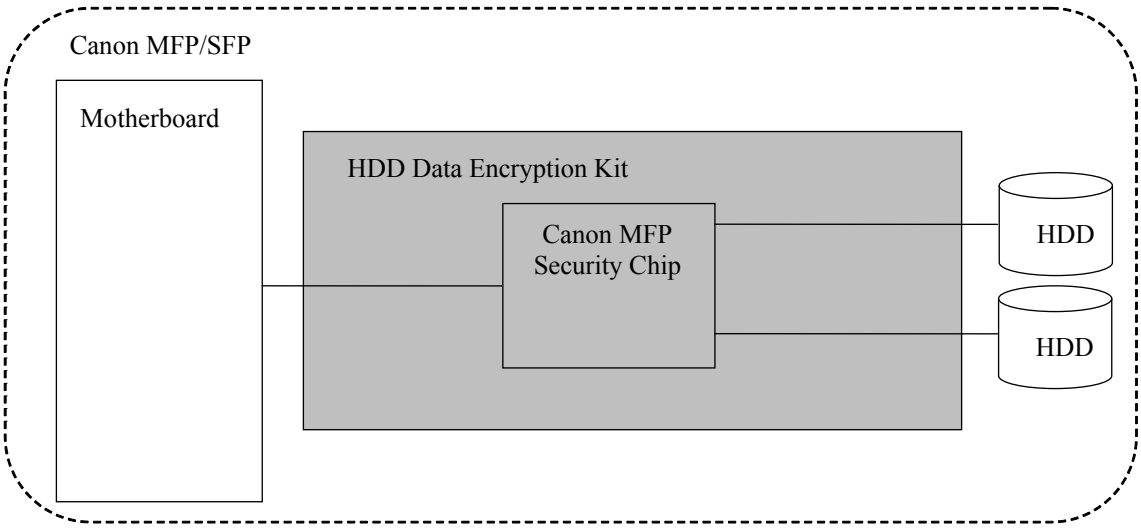
The TOE provides functions to protect data stored in the HDD of Canon MFP/SFP from being analyzed.
In other words, the assets to be protected by the TOE are the data to be written in the HDD while users are using Canon MFP/SFP. Such data are hereinafter called User Data.

### 1.5.3 Scope of the TOE

#### 1.5.3.1 Physical Scope of the TOE

Figure 1 shows the environment to use the TOE. The shaded area in the figure indicates the TOE. The TOE consists of a PCB on which Canon MFP Security Chip to implement TOE security functions is mounted, and connecting cables. The TOE is located between the motherboard and HDD of Canon MFP/SFP. Once the TOE is installed, the HDD is always accessed via the TOE. Serial ATA is used as the interface between the motherboard and TOE, and between the TOE and HDD.

**Figure 1 Use Environment of the TOE**




The following is the role of each component shown in Figure 1.

**Table 3 —List of Components**

| Name | Role |
|---|---|
| Motherboard | A PCB in Canon MFP/SFP. HDD Data Encryption Kit is attached to it. |
| HDD Data Encryption Kit | The TOE |
| Canon MFP Security Chip | ASIC to implement the security functions of the TOE. |
| HDD | Disk where data are stored. 2 HDDs can be used because the TOE has mirroring function. However, 2 HDDs are not a requirement. It is possible to operate with only 1 HDD.<br>HDDs can be detached easily by users. |

The following are the guidance documents included in the TOE. Guidance documents for Japan or for other countries than Japan are included. The difference between the guidance documents for Japan and other countries is the language alone and the contents of the documents are the same. Note that, HDD Data Encryption & Mirroring Kit-E1 is common for all destinations and all the following six guidance documents are included.

(For Japan)
- HDD Data Encryption Kit Users Guide FT6-1331(010)
- HDD Mirroring Kit Users Guide FT6-1335(000)
- Make sure to read this notice before using this product FT6-1332(000)

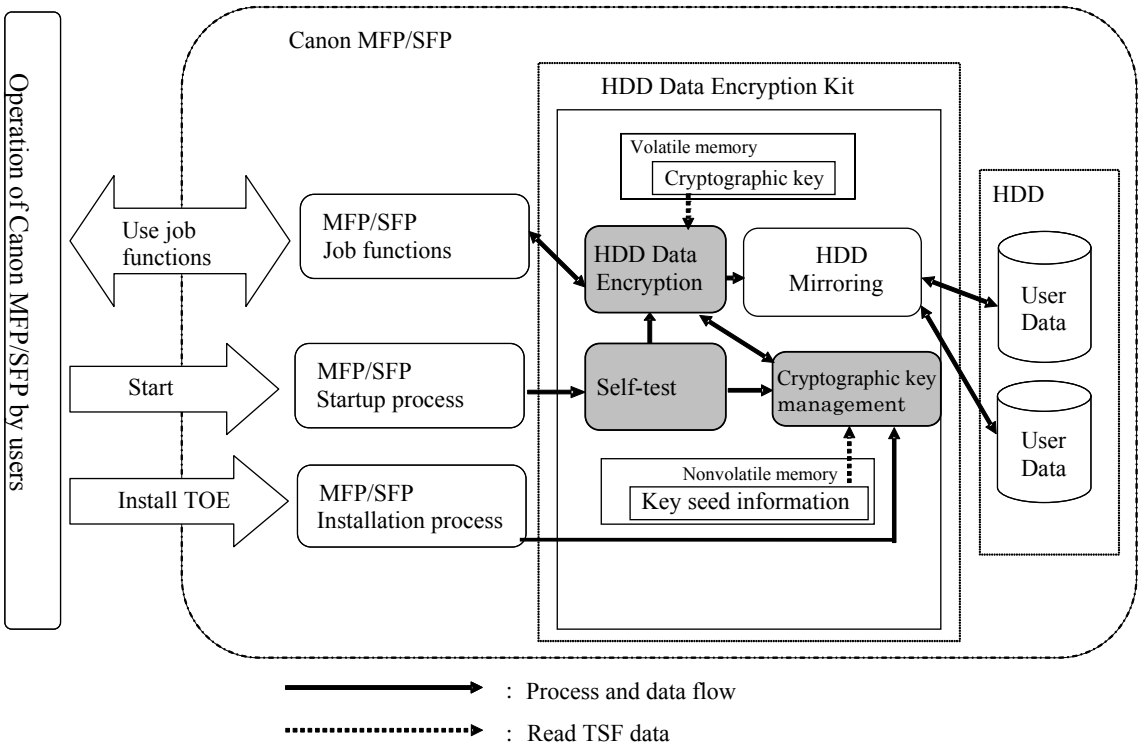
(For other countries than Japan)
- HDD Data Encryption & Mirroring Kit-E Series User Documentation FT6-1333(010)
- Make sure to read this notice before using this product. FT6-1334(000)

(Common)
- HDD Data Encryption & Mirroring Kit-E Series Installation Procedure FT2-0299(010)

### 1.5.3.2 Logical Scope of the TOE

Figure 2 shows the logical configuration of the TOE. Note that the shaded area in the figure indicates the security functions of the TOE.

**Figure 2 Logical Configuration of the TOE**




The followings are the security functions provided by the TOE. As shown in Figure 2, users have no means to affect the security functions of the TOE except for operating functions of Canon MFP/SFP.

■ HDD data encryption function

HDD data encryption function encrypts data to write in the HDD and decrypts data to read from the HDD.

- Cryptographic key management function

  Cryptographic key management function generates a cryptographic key used in the HDD data encryption function and manages it. Cryptographic key management function generates a cryptographic key using key seed information registered at the time of TOE installation. Cryptographic key is stored in the volatile memory and disappear when the power of Canon MFP/SFP is turned off.

- Self-test function

  Self-test function confirms if the encryption/decryption of HDD data encryption function operates properly. The TOE automatically runs this function when the power of Canon MFP/SFP is turned on. If the self-test fails, the TOE will stop operating immediately.

The following is the general function provided by the TOE.

- HDD mirroring function

  HDD mirroring function maintains the same data in two HDDs and uses one of them as the backup in case of an error.

  This function operates only if two HDDs are used and HDD mirroring function is set to “ON” in Canon MFP/SFP.

# 2 Conformance Claims

This chapter describes CC conformance claim, PP conformance claim and package claim.

## 2.1 CC Conformance Claim

The ST conforms to the following Common Criteria (CC).

- CC version:

  Part 1: Introduction and general model Version 3.1 Release 4 [Japanese version 1.0]

  Part 2: Security functional components Version 3.1 Release 4 [Japanese version 1.0]

  Part 3: Security assurance components Version 3.1 Release 4 [Japanese version 1.0]
- CC conformance:

  Part 2 and Part 3 conformant

## 2.2 PP Conformance Claim

There is no PP for which this ST claims conformance.

## 2.3 Package Claim

This ST conforms to the following packages:

- Conformant functional requirement package: None
- Conformant assurance requirement package: EAL3 conformant

# 3 Security Problem Definition

This chapter describes threats, threat agents, organizational security policies and assumptions.

## 3.1 Threats

The following threat is described.

**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.

## 3.2 Threat Agents

Threat agents (attackers) are defined as follows.

People who obtain removed HDD and attempt an unauthorized access to User Data in the HDD using a disk analysis tool, etc. with harmful intent.
Threat agents are assumed to have a limited/basic level of attack potential.

## 3.3 Organizational Security Policies

The following describes the organizational security policies that the TOE must follow.

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

## 3.4 Assumptions

The following describes assumptions that the TOE should meet.

**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 Security Objectives

This chapter describes security objectives for the TOE and security objectives for operational environment.

## 4.1 Security Objectives for the TOE

This section describes security objectives for the TOE to countermeasure threats and realize organizational security objectives.

**O.CRYPTO**
The TOE makes data not analyzable even if HDD is accessed directly using a disk analysis tool. In other words, the TOE performs the following processes.

- Encrypt data to write in the HDD.
- Decrypt data to read from the HDD.

**O.CORRECT_TSF_OPERATION**
The TOE performs a self-test of HDD data encryption function to confirm that HDD data encryption functions operate properly and cryptographic key is not broken.

## 4.2 Security Objectives for Operational Environment

This section describes security objectives for operational environment.

**OE.PHYSICAL_ACCESS_MANAGED**
Canon MFP/SFP to which the TOE is attached should be installed in an environment where the TOE is protected from physical access being made by people with harmful intent.

## 4.3 Security Objectives Rationale

Table 4 shows relationship of the security objectives to TOE security environments.

**Table 4 —Correlation of TOE Security Environment and Security Objectives**

| Threats, policies, assumptions / Security objectives | T.HDD_ACCESS | P.TSF_VERIFICATION | A.PHYSICAL_ACCESS_MANAGED |
|---|---|---|---|
| O.CRYPTO | ✓ | | |
| O.CORRECT_TSF_OPERATION | | ✓ | |
| OE.PHYSICAL_ACCESS_MANAGED | | | ✓ |

The following shows the rationale for Table 4 – Correlation of TOE Security Environment and Security Objectives.

**T.HDD_ACCESS**
T.HDD_ACCESS is countered by O.CRYPTO. User data in the HDD is protected from unauthorized exposure by bypassing the TOE and accessing the HDD directly using a data analysis tool because data to write in the HDD are encrypted and data to read from the HDD are decrypted by O.CRYPTO.

**P.TSF_VERIFICATION**
P.TSF_VERIFICATION is enforced by O.CORRECT_TSF_OPETATION. The TOE performs a self-test to confirm that HDD data encryption function works properly and cryptographic key is not broken by O.CORRECT_TSF_OPETATION.

**A.PHYSICAL_ACCESS_MANAGED**
A.PHYSICAL_ACCESS_MANAGED is realized by OE.PHYSICAL_ACCESS_MANAGED.
OE.PHYSICAL_ACCESS_MANAGED ensures that Canon MFP/SFP with the TOE attached is installed in an environment where the TOE is protected from the physical access by people with harmful intent.

# 5 Extended Components Definition

This ST does not define any requirements for extended security functions.

# 6 Security Requirements

This chapter describes TOE security functional requirements, security assurance requirements and rationale for security requirements.

## 6.1 TOE Security Functional Requirements

Requirements for security functions provided by the TOE are described as follows.

### FCS_CKM.1 Cryptographic key generation

**Hierarchical to:** No other components

**Dependencies:** [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

**FCS_CKM.1.1** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

[assignment: *list of standards*]
- Not specified

[assignment: *cryptographic key generation algorithm*]
- Random number generation algorithm based on SP800-90A using Hash_DRBG

[assignment: *cryptographic key sizes*]
- 128 bits or 256 bits

### FCS_COP.1 Cryptographic operation

**Hierarchical to:** No other components

**Dependencies:** [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

**FCS_COP.1.1** The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

[assignment: *list of standards*]
- FIPS PUB 197

[assignment: *cryptographic algorithm*]
- AES

[assignment: *cryptographic key sizes*]
- 128 bits or 256 bits

[assignment: *list of cryptographic operations*]

- Encryption of data to write in the HDD
- Decryption of data to read from the HDD

### FPT_TST.1 TSF testing

**Hierarchical to:** No other components

**Dependencies:** No dependencies

**FPT_TST.1.1** The TSF shall run a suite of self tests [selection: *during initial start-up*, *periodically during normal operation*, *at the request of the authorized user*, *at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: *the TSF*, [assignment: *parts of TSF*]].

[selection: *the TSF*, [assignment: *parts of TSF*]]
- [assignment: *parts of TSF*]

[assignment: *parts of TSF*]
- Cryptographic algorithms used for the HDD data encryption and Cryptographic key generation

[selection: *during initial start-up*, *periodically during normal operation*, *at the request of the authorized user*, *at the conditions* [assignment: *conditions under which self test should occur*]]
- *during initial start-up*

**FPT_TST.1.2** The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: *parts of TSF data*], *TSF data*].

[selection: [assignment: *parts of TSF data*], *TSF data*]
- [assignment: *parts of TSF data*]

[assignment: *parts of TSF data*]
- Key seed information

**FPT_TST.1.3** The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF*].

[selection: [assignment: *parts of TSF*], *TSF*]
- [assignment: *parts of TSF*]

[assignment: *parts of TSF*]
- TSF executable code

## 6.2 Security Assurance Requirements

The assurance level required by this ST for the TOE is EAL3. Assurance component configuration is shown in Table 5. Assurance elements for each required assurance component is as required by CC Part3.

**Table 5 — List of Required TOE Assurance Components**

| Assurance class | Assurance component |
|---|---|
| ADV: Development | ADV_ARC.1 Security architecture description |
| | ADV_FSP.3 Functional specification with complete summary |
| | ADV_TDS.2 Architectural design |
| AGD: Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |

| Assurance class | Assurance component |
|---|---|
| ALC: Life-cycle support | ALC_CMC.3 Authorization controls |
| | ALC_CMS.3 Implementation representation CM coverage |
| | ALC_DEL.1 Delivery procedures |
| | ALC_DVS.1 Identification of security measures |
| | ALC_LCD.1 Developer defined life-cycle model |
| ASE: Security Target evaluation | ASE_CCL.1 Conformance claims |
| | ASE_ECD.1 Extended components definition |
| | ASE_INT.1 ST introduction |
| | ASE_OBJ.2 Security objectives |
| | ASE_REQ.2 Derived security requirements |
| | ASE_SPD.1 Security problem definition |
| | ASE_TSS.1 TOE summary specification |
| ATE: Tests | ATE_COV.2 Analysis of coverage |
| | ATE_DPT.1 Testing: basic design |
| | ATE_FUN.1 Functional testing |
| | ATE_IND.2 Independent testing - sample |
| AVA: Vulnerability assessment | AVA_VAN.2 Vulnerability analysis |

## 6.3 Security Requirement Rationale

### 6.3.1 Correlation of Security Objectives and Security Functional Requirements

Table 6 - Correlation of Security Objectives and Security Functional Requirements shows security functional requirements for each security objective.

**Table 6 —Correlation of Security Objectives and Security Functional Requirements**

| Security objectives / Security functional requirements | O.CRYPTO | O.CORRECT_TSF_OPERATION |
|---|---|---|
| FCS_CKM.1 | ✓ | |
| FCS_COP.1 | ✓ | |
| FPT_TST.1 | | ✓ |

### 6.3.2 Security Functional Requirements Rationale

The following shows rationale for Table 6 – Correlation of Security Objectives and Security Functional Requirements.

**O.CRYPTO**
This security objective specifies encryption of data to write in the HDD and decryption of data to read from the HDD.
For cryptographic keys used for encryption or decryption, “cryptographic keys with the size of 128 bits or 256 bits” are generated by FCS_CKM.1 using “random number generation algorithm based on SP800-90A using Hash_DRBG”.
For actual encryption and decryption operations, FCS_COP.1 encrypts data to write in the HDD or decrypts data to read from the HDD using “cryptographic keys with the size of 128 bits or 256 bits” in accordance with an “encryption algorithm AES” to meet “FIPS PUB197”.

O.CRYPTO is addressed as above.

**O.CORRECT_TSF_OPERATION**
This security objective specifies self-tests to be performed to verify that HDD data encryption functions work properly in the operational environment and cryptographic key is not broken.
With FPT_TST.1, the TOE performs self-tests to confirm that encryption algorithm used in HDD data encryption and cryptographic key generation works properly and to verify executable codes thereby verifying the integrity of HDD data encryption functions. In addition, the integrity of key seed information is verified to confirm that the cryptographic key is not broken because the cryptographic key is regenerated using the key seed information stored in the TOE.

O.CORRECT_TSF_OPERATION is addressed as above.

### 6.3.3 Dependencies of Security Functional Requirements

Dependencies of Security Functional Requirements are shown in Table 7 – Dependencies of Security Functional Requirements.

**Table 7 —Dependencies of Security Functional Requirements**

| Functional requirement | Dependencies required by CC | Dependencies satisfied by ST | Reason for not satisfying dependencies |
|---|---|---|---|
| FCS_CKM.1 | [FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 | FCS_COP.1 | Reason for not claiming FCS_CKM.4: The TOE is protected against physical access by means of OE.PHYSICAL_ACCESS_MANAGED and it is not possible to retrieve the cryptographic key. Therefore, cryptographic keys are managed safely without functional destruction. |
| FCS_COP.1 | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 | FCS_CKM.1 | Reason for not claiming FCS_CKM.4: The TOE is protected against physical access by means of OE.PHYSICAL_ACCESS_MANAGED and it is not possible to retrieve the cryptographic key. Therefore, cryptographic keys are managed safely without functional destruction. |
| FPT_TST.1 | No dependencies | No dependencies | N/A (Dependencies not required) |

## 6.4 Security Assurance Requirement Rationale

The TOE is a commercial IT product that provides security functions to Canon MFP/SFP and its purpose is to counter unauthorized exposure of data caused by data analysis of HDD by attackers with limited/basic attack potential. As a result, assurance for protection from attacks at limited/basic level by unspecified people is

required for the TOE. Therefore, security should be assured from the perspective of development environment and prevention of misuse in addition to the efforts to assure security in the development processes such as identification of external interfaces, specification of internal structure of functions, confirmation of security functions by testing, and analysis of vulnerabilities. Evaluation assurance level of EAL3 is thus required.
All the security assurance requirement sets required for EAL3 are adopted. As such, all the dependencies of TOE security assurance requirements are satisfied.

# 7 TOE Summary Specification

This chapter describes TOE summary specification.

## 7.1 TOE Security Functions

This section describes security functions of the TOE. As in the case with the TOE security functional requirements indicated for each function, security functions described in this section satisfy the TOE security functional requirements described in Chapter 6.1.

### 7.1.1 HDD Data Encryption Function (F.HDD_CRYPTO)

HDD data encryption function provides the following security functions.

| Specification of security functions | Requirements for security functions |
|---|---|
| The TOE performs the following encryption operations:<br>■ Encrypt data to write in the HDD.<br>■ Decrypt data to read from the HDD.<br><br>Cryptographic key and encryption algorithm used for encryption operations are as follows:<br>■ Cryptographic keys with the size of “128 bits” or “256 bits”.<br>■ “AES algorithm” in accordance with FIPS PUB 197 | FCS_COP.1 |

### 7.1.2 Cryptographic Key Management Function (F.KEY_MANAGE)

Cryptographic key management function provides the following security functions.

| Specification of security functions | Requirements for security functions |
|---|---|
| Based on the following specification, the TOE generates cryptographic keys used for HDD data encryption functions.<br>■ Algorithm used to generate cryptographic keys is “a random number generation algorithm based on SP800-90A using Hash_DRBG”<br>■ The size of the cryptographic keys to be generated is “128 bits” or “256 bits”.<br><br>Cryptographic key is managed as follows:<br>■ At the startup, the TOE reads the key seed information stored in the TOE and regenerates the cryptographic key.<br>■ After generating the cryptographic key, the TOE stores it in the volatile memory.<br><br>Cryptographic key is retained only in the volatile memory and thus disappear when the power of the device is turned off. | FCS_CKM.1 |

The size of the key to be generated is uniquely specified by Canon MFP/SFP to which the TOE is attached as shown in Table 8.

**Table 8 — Key Size for Supported Canon MFP/SFP**

| Key size | Canon MFP/SFP |
|---|---|
| 128 bits | imagePRESS C10000VP<br>imagePRESS C8000VP |
| 256 bits | imagePRESS C65<br>imagePRESS C650 |

### 7.1.3 Self-test Function (F.SELF_TEST)

Self-test function provides the following security functions.

| Specification of security functions | Requirements for security functions |
|---|---|
| The TOE executes the self-test function automatically at the startup and verifies the integrity of HDD data encryption function. Followings are the contents of the verification performed in the self-test:<br>■ Verification of integrity of executable codes<br>Verify the integrity by 32-bit CRC check when reading the firmware stored in the TOE.<br>■ Verification of integrity of encryption algorithm<br>With known answer test, verify if the AES algorithm used by HDD data encryption function works properly.<br>With known answer test, verify if random number generation computed by the firmware works properly.<br>With known answer test, verify if hash function used for random number generation works properly.<br>■ Verification of integrity of TSF data<br>Verify the integrity by 32-bit CRC check when reading the key seed information stored in the TOE.<br><br>In case the self-test fails, the TOE transitions to an error state and no access to the HDD via the TOE becomes possible. | FPT_TST.1 |

END