Canon MFP Security Chip
Security Target

Version 1.08
June 29, 2006

Canon Inc.

This document is a translation of the security target written in Japanese, which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

Revision History

Version	Date	Reason for Change	Author	Reviewer	Approver
1.00	Sep 22, 2005	First draft.	Shigeeda Date of creation: Sep 22, 2005	Shigeeda Date of review: Sep 22, 2005	Makitani Date of approval: Sep 22, 2005
1.01	Nov 04, 2005	Changes made based on comments.	Shigeeda Date of creation: Nov 04, 2005	Shigeeda Date of review: Nov 04, 2005	Makitani Date of approval: Nov 04, 2005
1.02	Nov 09, 2005	Changes made based on comments.	Shigeeda Date of creation: Nov 09, 2005	Shigeeda Date of review: Nov 09, 2005	Makitani Date of approval: Nov 09, 2005
1.03	Nov 11, 2005	Changes made based on comments.	Shigeeda Date of creation: Nov 11, 2005	Shigeeda Date of review: Nov 11, 2005	Makitani Date of approval: Nov 11, 2005
1.04	Feb 07, 2006	Changes made based on comments.	Shigeeda Date of creation: Feb 07, 2006	Shigeeda Date of review: Feb 07, 2006	Makitani Date of approval: Feb 07, 2006
1.05	Feb 21, 2006	Corrected assurance measure names.	Shigeeda Date of creation: Feb 21, 2006	Shigeeda Date of review: Feb 21, 2006	Makitani Date of approval: Feb 21, 2006
1.06	Apr 03, 2006	Changes made based on comments.	Shigeeda Date of creation: Apr 03, 2006	Shigeeda Date of review: Apr 03, 2006	Makitani Date of approval: Apr 03, 2006
1.07	Apr 13, 2006	Changes made based on comments.	Shigeeda Date of creation: Apr 13, 2006	Shigeeda Date of review: Apr 13, 2006	Makitani Date of approval: Apr 13, 2006
1.08	Jun 29, 2006	Changes made based on comments.	Shigeeda Date of creation: Jun 29, 2006	Shigeeda Date of review: Jun 29, 2006	Makitani Date of approval: Jun 29, 2006

Table of Contents

List of Figures

List of Tables

1. ST Introduction

This chapter presents ST identification information, an overview of the ST, claims of CC conformance and referenced documents, as well as notations, terms and abbreviations used in this document.

1.1 ST Identification

1.1.1 ST Identification and Management

Title:	Canon MFP Security Chip Security Target
ST version:	1.08
Date of creation:	June 29, 2006
Authors:	Canon Inc.

1.1.2 TOE Identification and Management

Name:	Canon MFP Security Chip
TOE version:	1.00
Manufacturer:	Canon Inc.

1.1.3 CC Identification

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

1.2 ST Overview

This ST describes the security chip that is mounted on the Security Kit B Series option boards for Canon's multifunction products and printers.

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

The TOE offers the following security functions for hard drive data protection.

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

1.3 CC Conformance

This ST conforms to the following CC specifications.

- CC Part 2 conformant
- CC Part 3 conformant
- EAL3 conformant

There are no Protection Profiles claimed to which this ST is conformant.

1.4 References

- Common Criteria for Information Technology Security Evaluation – Part 1: Information and general model, dated August 1999, version 2.1, CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part1, 99/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part2, 99/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part3, 99/12
- CCIMB Interpretations (as of 01 December 2003)

1.5 Notations, Terms and Abbreviations

1.5.1 Notations

The assumptions, threats and organizational security policies in Chapter 3 and the security objectives in Chapter 4 are denoted with labels in **boldface** type and subsequent definitions in regular type.

1.5.2 Terms and Abbreviations

The terms and abbreviations used in this ST are defined in Table 1.1.

Table 1.1: Terms and abbreviations

Abbrev and Terms	Definition
Canon MFP/printer	A general term that refers to a Canon-made multifunction product or printer.
HDD	The built-in hard disk drive of a Canon MFP/printer.
Security Kit	A board with a security chip that is aimed at providing security enhancements. It has a physical interface to a Canon MFP/printer and its HDD.
Security Kit B Series	A collective term for a specific series of Security Kits using the TOE as a security chip. The Security Kits in the B Series lineup 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 the following part of this ST, the term “Security Kit” refers to any Security Kit in the B Series lineup. The Security Kit B Series includes the following products. ▪ English version: HDD Data Encryption Kit-B Series ▪ French version: Kit d'encryptage des données disque dur-Série B
Disk analysis tool	A general term that refers to any tool that allows viewing the contents of sectors on hard drives.

2. TOE Description

This chapter describes the product type, an overview and the scope of the TOE, as well as the assets to be protected by the TOE.

2.1 Product Type

The TOE is an encryption security chip. It is an IT product designed for mounting on the Security Kit B Series boards that enhance the security of Canon MFPs/printers.

2.2 Overview

2.2.1 Purpose of Use of the TOE

When a Canon MFP/printer is used, user input data is stored in the HDD.
This TOE is used for the purpose of countering the problem of leakage of HDD data by way of theft of the HDD. By using the TOE, data writes to the HDD can be encrypted without limiting the extensibility and processing performance of the Canon MFP/printer.

2.2.2 Persons Associated with the TOE

Persons associated with the TOE are identified as follows.
No special roles or privileges are required for using the TOE.

- User
  Any person using a Canon MFP/printer. Users can benefit from the functions of the TOE by installing the Security Kit into a Canon MFP/printer and using its capabilities, e.g., copying, printing and scanning.

2.2.3 Method of Use of the TOE

The TOE is provided to users as a Canon MFP/printer Security Kit and the Security Kit is used as installed in a Canon MFP/printer. Once the Security Kit installed, any HDD access that occurs through the use of the Canon MFP/printer capabilities will be done via the TOE.

Note that direct HDD access bypassing the TOE is not allowed, nor is the reuse of the Security Kit by reinstalling it into a different Canon MFP/printer.

2.2.4 Operating Environment of the TOE

The TOE operates mounted on the Security Kit and the Security Kit operates installed in a B Series-ready Canon MFP/printer. Installable Security Kits can be identified in the Canon MFP/printer option list (a list of available options for every model in the Canon MFP/printer lineups).

Users can refer to this option list to find out if and which model in the Security Kit B Series lineup is available for their Canon MFPs/printers. However, it should be noted that there is no Security Kit in the B-series lineup that works with any Canon MFP/printer that does not support the Security Kit B Series boards.

2.3 TOE Configuration

2.3.1 Physical Configuration of the TOE

The TOE is the entire Canon MFP Security Chip, as depicted in Figure 2.1.

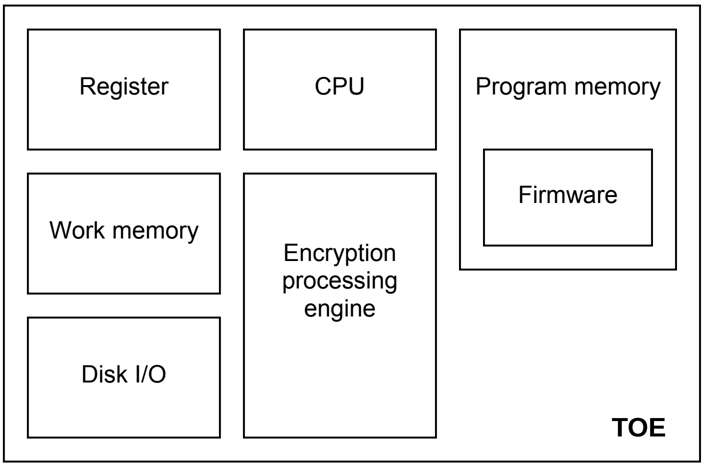

Figure 2.1: TOE physical configuration

Table 2.1 describes the roles of the components composing the TOE.

Table 2.1: Roles of TOE components

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

2.3.2 Logical Configuration of the TOE

Figure 2.2 shows the logical configuration of the TOE.

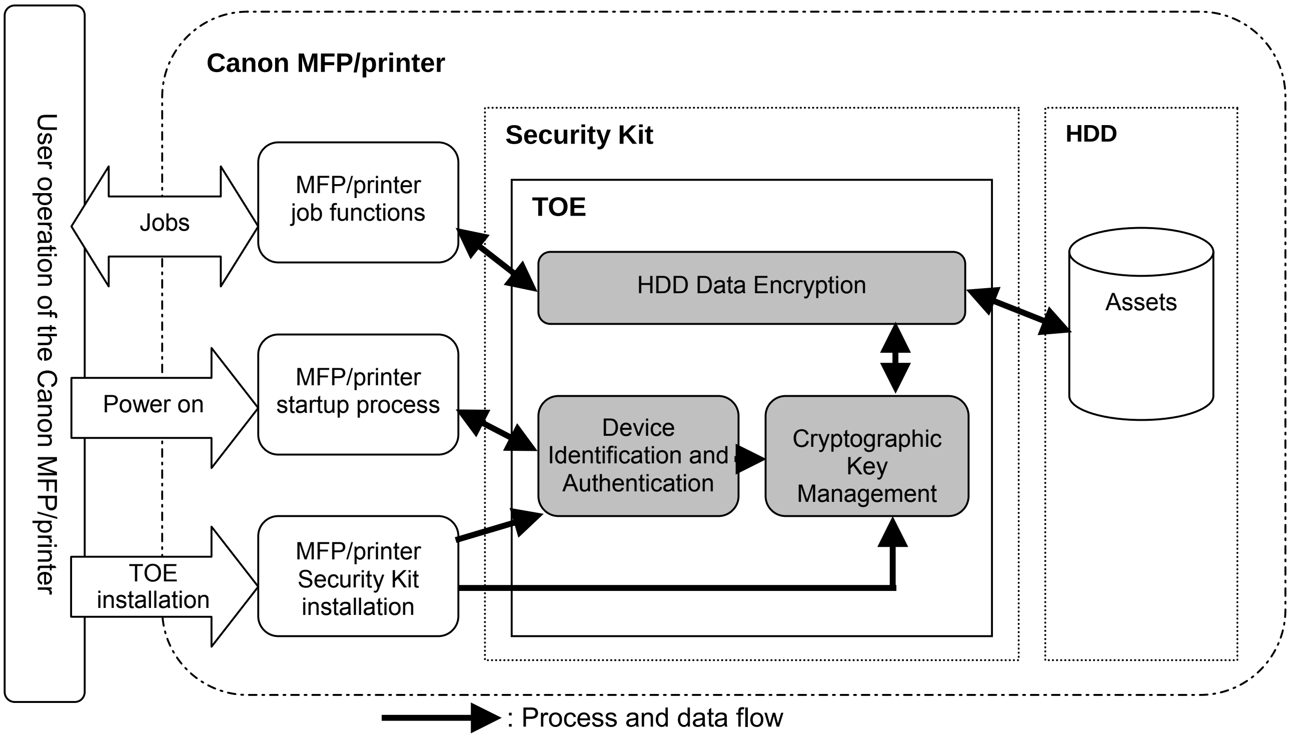
User operation of the Canon MFP/printer
Canon MFP/printer
Jobs
Power on
TOE installation
MFP/printer job functions
MFP/printer startup process
MFP/printer Security Kit installation
Security Kit
TOE
HDD Data Encryption
Device Identification and Authentication
Cryptographic Key Management
HDD
Assets
: Process and data flow

Figure 2.2: TOE logical configuration

As depicted in Figure 2.2, users use the TOE through operation of the Canon MFP/printer.

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

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

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

The TOE provides the security functions summarized below. As can be seen in Figure 2.2, there is no other way for users to impact the TOE security functions than operating the Canon MFP/printer. Therefore, in the context of execution of the TOE security functions, the TOE treats the user and the Canon MFP/printer being used by the user equally.

➢ **HDD Data Encryption**
This function encrypts data writes to the HDD and decrypts data reads from the HDD.

- **Cryptographic Key Management**
  This function generates and manages cryptographic keys for use by the HDD Data Encryption function.
  It generates cryptographic keys using part of the information registered at the time of TOE installation as seed information. Cryptographic keys are stored in volatile memory and hence disappear when the Canon MFP/printer is powered off.

- **Device Identification and Authentication**
  This function confirms if the Canon MFP/printer with the TOE currently installed is the “registered device”, using part of the information registered at the time of TOE installation as an authentication ID.
  It prohibits any HDD access via the TOE unless it confirms that the TOE is connected to the “registered device”, which means if the Canon MFP/printer being used by the user is truly the “registered device”, the user will be granted unlimited access to the HDD via the TOE.

Note that there is no logical function that impacts the TOE security functions in any other configuration areas on the Security Kit than the TOE.

2.4 Assets

The TOE provides functions to protect the Canon MFP/printer built-in HDD from the risk of being removed and analyzed.
That is, the assets to be protected by the TOE are any data that is written to the HDD as a result of a user’s use of the Canon MFP/printer.

3. TOE Security Environment

This chapter describes the assumptions, threats and organizational security policies that are applicable to the TOE.

3.1 Assumptions

A.UNIQUE_INFO

Any Canon MFP/printer that supports the Security Kit B Series shall retain a unique authentication ID and seed information without alteration.

3.2 Threats

The following assumes that the attack potential of the attacker is low.

T.HDD_ACCESS

A malicious individual may attempt to disclose the data on the HDD by removing and directly accessing the HDD using a disk analysis tool or another Canon MFP/printer.

T.WRONG_BOARD

A malicious individual may attempt to disclose the data on the HDD by moving the Security Kit and the HDD from the “registered device” to another Canon MFP/printer and accessing the HDD via the Security Kit.

3.3 Organizational Security Policies

There are no organizational security policies with which the TOE must comply.

4. Security Objectives

4.1 Security Objectives for the TOE

This section describes the security objectives for the TOE to counter the threats and achieve the organizational security policies.

O.CRYPTO

The TOE shall prevent the data on the HDD from being analyzed even if the HDD is directly accessed using a disk analysis tool, i.e., the TOE shall perform the following processing:

- ➢ Encrypting data writes to the HDD
- ➢ Decrypting data reads from the HDD

O.BOARD_AUTH

The TOE shall prevent any attempt to access the HDD via the TOE from any other Canon MFP/printer than the “registered device” from succeeding, i.e., the TOE shall perform the following processes:

- ➢ Confirming that it is connected to the “registered device”
- ➢ Permitting HDD access via itself only when it is connected to the “registered device”

4.2 Security Objectives for the Environment

OE.UNIQUE_INFO

A unique authentication ID and seed information shall be provided by the B Series-ready Canon MFP/printer in which the TOE is used.

5. IT Security Requirements

5.1 TOE Security Requirements

This section describes the security requirements that the TOE must satisfy.

5.1.1 TOE Security Functional Requirements

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

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*]
- FIPS 186-2

[assignment: *cryptographic key generation algorithm*]
- A FIPS 186-2-based cryptographic key generation algorithm

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

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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*]
- 256 bits

[assignment: *list of cryptographic operations*]
- Encryption of data writes to the HDD
- Decryption of data reads from the HDD

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

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement: “User” → Registered device

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.4.1

The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism(s)*].

[assignment: *identified authentication mechanism(s)*]

- The authentication mechanism employed for registered device authentication

Dependencies: No dependencies.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement: “User” → Registered device

Dependencies: No dependencies.

FPT_RVM.1 Non-bypassibility of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

5.1.2 TOE Security Assurance Requirements

The TOE assurance level claimed in this ST is EAL3. The assurance components are listed in Table 5.1. The assurance elements within each assurance component claimed are conformant to CC Part 3.
Note that the ASE class has been adopted such that its assurance requirements must be satisfied regardless of the target assurance level.

Table 5.1: TOE assurance requirements components

TOE Security Assurance Requirement		Component
Configuration management	CM capabilities	ACM_CAP.3
	CM scope	ACM_SCP.1
Delivery and operation	Delivery	ADO_DEL.1
	Installation, generation and start-up	ADO_IGS.1
Development	Functional specification	ADV_FSP.1
	High-level design	ADV_HLD.2
	Representation correspondence	ADV_RCR.1
Guidance documents	Administrator guidance	AGD_ADM.1
	User guidance	AGD_USR.1
Life cycle support	Development security	ALC_DVS.1
Tests	Coverage	ATE_COV.2
	Depth	ATE_DPT.1
	Functional tests	ATE_FUN.1
	Independent testing	ATE_IND.2
Vulnerability assessment	Misuse	AVA_MSU.1
	Strength of TOE security functions	AVA_SOF.1
	Vulnerability analysis	AVA_VLA.1

5.2 Security Requirements for the IT Environment

There are no security requirements for the IT environment that the TOE requires.

5.3 Strength of Security Functions

The minimum strength of function level for the TOE security functions is SOF-basic. The security functional requirements to which the claimed strength of function rating applies are FIA_UAU.2, FIA_UAU.4 and FIA_UID.2, and the strength of function level for these requirements is SOF-basic.

Of note, the cryptographic algorithm employed by the TOE is outside the scope of the strength of TOE security functions.

6. TOE Summary Specification

This chapter describes the TOE summary specification.

6.1 TOE Security Functions

This section explains the TOE security functions. As each function description is accompanied by an indication of the corresponding security functional requirement(s), the security functions described below do satisfy the TOE security functional requirements described in Section 5.1.1.

6.1.1 HDD Data Encryption Function (**F.HDD_CRYPTO**)

The HDD Data Encryption function consists of a set of the following security functions.

Security Function Specification	SFR
The TOE performs the following cryptographic operations: ▪ Encryption of data writes to the HDD ▪ Decryption of data reads from the HDD The cryptographic keys and the cryptographic algorithm used for these cryptographic operations are as follows. ▪ Cryptographic keys of “256 bits” length ▪ The “AES algorithm” that meets FIPS PUB 197	FCS_COP.1 FPT_RVM.1

6.1.2 Cryptographic Key Management Function (**F.KEY_MANAGE**)

The Cryptographic Key Management function consists of a set of the following security functions.

Security Function Specification	SFR
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 “FIPS 186-2-compliant cryptographic key generation algorithm”. ▪ The generated cryptographic key has a length of “256 bits”. Cryptographic key management is conducted as follows: ▪ Upon startup, the TOE reads the seed information stored in non-volatile memory and generates a cryptographic key. ▪ The TOE stores the generated cryptographic key in volatile memory. The non-volatile memory where the seed information is stored cannot be accessed from outside the TOE. Also, the cryptographic key is stored in volatile memory and hence disappears upon power-off of the Canon MFP/printer.	FCS_CKM.1 FPT_RVM.1

6.1.3 Device Identification and Authentication Function (**F.KIT_CHECK**)

The Device Identification and Authentication function consists of a set of the following security functions.

Security Function Specification	SFR
Upon startup, the TOE confirms that it is connected to the “registered device” using the authentication ID. To prevent reuse of authentication data related to the authentication	FIA_UAU.2 FIA_UAU.4

mechanism employed for registered device authentication, a standard challenge-and-response authentication scheme is used: a pseudo-random number is generated as a challenge every time the TOE is activated. [Authentication ID registration] At the time of installation of the Security Kit, the TOE receives an authentication ID from the Canon MFP/printer and saves it to the Flash ROM on the Security Kit. [Identification and authentication procedure] Upon startup, the TOE generates a pseudo-random number and passes it to the Canon MFP/printer as a challenge code. The Canon MFP/printer then calculates the response based on the authentication ID and the challenge and passes it to the TOE. The TOE performs the same calculation to verify the response. If the TOE cannot confirm that it is connected to the “registered device”, the TOE prohibits HDD access.	FIA_UID.2 FPT_RVM.1

6.2 Strength of Security Functions

In this TOE, the only IT security function that is realized by a probabilistic or permutation mechanism and subject to a strength of function analysis is F.KIT_CHECK, and the strength of function for the IT security function is SOF-basic.

6.3 Assurance Measures

This section explains the TOE security assurance measures. As shown in Table 6.1, these assurance measures satisfy the TOE security assurance requirements described in Table 5.1.
Of note, the assurance measure for the ASE class requirements is this Security Target.

Table 6.1: TOE assurance measures

TOE Security Assurance Requirement		Component	Assurance Measure
Configuration management	CM capabilities	ACM_CAP.3	▪ Canon MFP/Printer Security Chip Configuration Management Plan 1 ▪ Canon MFP/Printer Security Chip Configuration Management Plan 2 ▪ Canon MFP/Printer Security Chip Evaluation Evidence List
	CM scope	ACM_SCP.1	
Delivery and operation	Delivery	ADO_DEL.1	▪ Canon MFP/Printer Security Chip Delivery Procedures 1 ▪ Canon MFP/Printer Security Chip Delivery Procedures 2
	Installation, generation and start-up	ADO_IGS.1	▪ HDD Data Encryption Kit-B Series Installation Procedure (Japanese/English)
Development	Functional specification	ADV_FSP.1	▪ Canon MFP/Printer Security Chip Firmware Functional Specification
	High-level design	ADV_HLD.2	▪ Canon MFP/Printer Security Chip Firmware High-Level Design ▪ HERMIT Hardware Manual
	Representation correspondence	ADV_RCR.1	▪ Canon MFP/Printer Security Chip Representation Correspondence
Guidance	Administrator guidance	AGD_ADM.1	▪ HDD Data Encryption Kit-B Series

documents	User guidance	AGD_USR.1	Reference Guide (Japanese) ▪ HDD Data Encryption Kit-B Series Reference Guide (English)
Life cycle support	Development security	ALC_DVS.1	▪ Canon MFP/Printer Security Chip Firmware Development Security Rules
Tests	Coverage	ATE_COV.2	▪ Canon MFP/Printer Security Chip Test Coverage Analysis
	Depth	ATE_DPT.1	▪ Canon MFP/Printer Security Chip Analysis of the Depth of Testing
	Functional tests	ATE_FUN.1	▪ Canon MFP/Printer Security Chip Test Specification ▪ Canon MFP/Printer Security Chip Test Procedures ▪ Canon MFP/Printer Security Chip Test Results
	Independent testing	ATE_IND.2	▪ Canon MFP Security Chip
Vulnerability assessment	Misuse	AVA_MSU.1	▪ HDD Data Encryption Kit-B Series Installation Procedure (Japanese/English) ▪ HDD Data Encryption Kit-B Series Reference Guide (Japanese) ▪ HDD Data Encryption Kit-B Series Reference Guide (English)
	Strength of TOE security functions	AVA_SOF.1	▪ Canon MFP/Printer Security Chip Vulnerability Analysis
	Vulnerability analysis	AVA_VLA.1	

7. PP Claims

There are no PPs claimed to which this ST is conformant.

8. Rationale

8.1 Security Objectives Rationale

Table 8.1 shows the mapping between the TOE security environment and the security objectives.

Table 8.1: Mapping between TOE security environment and security objectives

TOE security environment / Security objective	T.HDD_ACCESS	T.WRONG_BOARD	A.UNIQUE_INFO
O.CRYPTO	X		
O.BOARD_AUTH		X	
OE.UNIQUE_INFO			X

The following describes the rationale to justify the mapping shown in Table 8.1: Mapping between TOE security environment and security objectives.

T.HDD_ACCESS

T.HDD_ACCESS is a threat that a malicious individual may attempt to disclose the data on the HDD by removing and directly accessing the HDD using a disk analysis tool or another Canon MFP/printer.
To counter this threat, the data on the HDD must be protected from analysis by way of direct HDD access.
In this TOE, O.CRYPTO ensures that data writes and reads to/from the HDD are encrypted and decrypted and hence it is impossible to analyze the data on the HDD by way of direct HDD access bypassing the TOE.
As such, this threat can be countered by satisfying the security objective O.CRYPTO.

T.WRONG_BOARD

T.WRONG_BOARD is a threat that a malicious individual may attempt to disclose the data on the HDD by moving the Security Kit and the HDD from the “registered device” to another Canon MFP/printer and accessing the HDD via the Security Kit.
To counter this threat, the HDD must be protected from access via the TOE from any other Canon MFP/printer than the “registered device”.
In this TOE, O.BOARD_AUTH ensures that the TOE permits HDD access via itself only when and if it confirms upon startup that it is connected to the “registered device” and hence HDD access via the TOE is not allowed from any other Canon MFP/printer than the “registered device”.
As such, this threat can be countered by satisfying the security objective O.BOARD_AUTH.

A.UNIQUE_INFO

A.UNIQUE_INFO is an assumption that the TOE must be used in a B Series-ready Canon MFP/printer that can provide a unique authentication ID and seed information.
To achieve this assumption, a unique authentication ID and seed information have to be provided by the B Series-ready Canon MFP/printer in which the TOE is used.
OE.UNIQUE_INFO specifies that a unique authentication ID and seed information shall be provided by the B Series-ready Canon MFP/printer in which the TOE is used.
As such, this assumption can be achieved by satisfying the security objective OE.UNIQUE_INFO.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements

Table 8.2 shows the mapping between the security objectives and the TOE security functional requirements.

Table 8.2: Mapping between security objectives and TOE security functional requirements

Security objective / **TOE security requirement**	O.CRYPTO	O.BOARD_AUTH
FCS_CKM.1	X	
FCS_COP.1	X	
FIA_UAU.2		X
FIA_UAU.4		X
FIA_UID.2		X
FPT_RVM.1	X	X

The following describes the rationale to justify the mapping shown in Table 8.2: Mapping between security objectives and TOE security functional requirements.

O.CRYPTO

This security objective requires that HDD writes and reads be encrypted and decrypted.
As for the cryptographic keys to be used for encryption and decryption, FCS_CKM.1 ensures that “256-bit long cryptographic keys” that meet “FIPS 186-2” are generated in accordance with a “FIPS 186-2-based cryptographic key generation algorithm”.
As for the actual encryption and decryption operations, FCS_COP.1 ensures that HDD writes are encrypted and HDD reads are decrypted in accordance with the “AES encryption algorithm” as defined in “FIPS PUB 197” using “256-bit long cryptographic keys”.
Furthermore, FPT_RVM.1 ensures that the cryptographic key generation specified by FCS_CKM.1 and the cryptographic operation specified by FCS_COP.1 are unfailingly enforced and succeed.
As such, O.CRYPTO can be achieved.

O.BOARD_AUTH

This security objective requires that the TOE permit HDD access via itself only when and if it confirms upon startup that it is connected to the “registered device”.
FIA_UAU.2 and FIA_UID.2 ensure that the TOE performs identification and authentication of the registered device and permits HDD access only if it determines that it is the “registered device”. The authentication mechanism that is used for authentication of the registered device is the “authentication mechanism employed for registered device authentication”, and FIA_UAU.4 ensures that reuse of authentication data is prevented.
Furthermore, FPT_RVM.1 ensures that the identification and authentication specified by FIA_UAU.2 and FIA_UID.2 and the prevention of authentication data reuse specified by FIA_UAU.4 are unfailingly enforced and succeed.
As such, O.BOARD_AUTH can be achieved.

8.2.2 Dependencies of TOE Security Functional Requirements

Table 8.3 shows the dependencies of the TOE security functional requirements.

Table 8.3: TOE security functional requirements dependencies

#	SFR	Hierarchical to	Dependencies	Refer to	Remarks
1	FCS_CKM.1	No other components	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	2	Since the TOE does not have an interface that allows read-out of cryptographic keys from outside the TOE, there is no threat of illegal read-out of cryptographic keys. That is, cryptographic key destruction is not required as a function of the TOE. Therefore, FCS_CKM.4 is not required.
					There are no security-related attributes in this TOE, e.g., key type and expiration period. Therefore, FMT_MSA.2 is not applicable.
2	FCS_COP.1	No other components	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	1	Since the TOE does not have an interface that allows read-out of cryptographic keys from outside the TOE, there is no threat of illegal read-out of cryptographic keys. That is, cryptographic key destruction is not required as a function of the TOE. Therefore, FCS_CKM.4 is not required.
					There are no security-related attributes in this TOE, e.g., key type and expiration period. Therefore, FMT_MSA.2 is not applicable.
3	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	5	FIA_UID.2 is hierarchical to FIA_UID.1.
4	FIA_UAU.4	No other components	No dependencies		
5	FIA_UID.2	FIA_UID.1	No dependencies		
6	FPT_RVM.1	No other components	No dependencies		

8.2.3 Interactions between TOE Security Functional Requirements

Table 8.4 shows the security functional requirements that are not required to be in an explicit dependent relationship but have been selected for mutual support purposes.

Table 8.4: Interactions between TOE security functional requirements

#	SFR	Mutual Support
1	FCS_CKM.1	FPT_RVM.1
2	FCS_COP.1	FPT_RVM.1
3	FIA_UAU.2	FPT_RVM.1
4	FIA_UAU.4	FPT_RVM.1
5	FIA_UID.2	FPT_RVM.1
6	FPT_RVM.1	None

FPT_RVM.1 <Non-bypassibility>

FPT_RMV.1 ensures that the security functional requirements for cryptographic key generation, cryptographic operation and challenge-and-response authentication are all invoked and succeed before each function within the TSC is allowed to proceed. The security functional requirements to be covered are FCS_CKM.1, FCS_COP.1, FIA_UAU.2, FIA_UAU.4 and FIA_UID.2.
As such, since FPT_RVM.1 supports the non-bypassibility of FCS_CKM.1, FCS_COP.1, FIA_UAU.2, FIA_UAU.4 and FIA_UID.2, the security objectives O.CRYPTO and O.BOARD_AUTH are achieved.

<Domain separation>

In this TOE, there is no subject that accesses an object on behalf of a user and hence no access control or information flow control is enforced. Therefore, the functional requirement FPT_SEP.1 that protects the TSF from interference and tampering by untrusted subjects is not required.

<Disabling>

This TOE has no functions related to security management, including the starting and stopping of security functions, hence, it requires no functional requirement that protects the TSF from disabling of security functions.

8.2.4 Rationale for Minimum Strength of Function Level

Since the attack potential of an attacker anticipated in the operational environment for the TOE is defined to be low, the method of attack would be to use some public interface, public information and disk analysis tools (commercially available ones). Low-level attacks can be countered by such TOE enforcing security measures as encryption and "registered device" confirmation, therefore, it can be said that the TOE security objectives are resistant to low-level attacks. As such, since being resistant to low-level attacks, the TOE security objectives are consistent with the minimum strength of function of SOF-basic.

Also, specific functional requirements (FIA_UAU.2, FIA_UAU.4 and FIA_UID.2) have a strength of function of SOF-basic and are consistent with the minimum strength of function of SOF-basic.

8.2.5 Rationale for Security Assurance Requirements

This TOE is a commercially available IT product that provides security features to Canon MFPs/printers, aimed at countering the threat of data leakage through HDD theft by low-level attackers. For that reason, the TOE is required to ensure resistance against low-level attacks by unspecified persons. Accordingly, in addition to the security assurance efforts that are made during the development process, e.g., identification of external interfaces, specification of function internal structures, confirmation of security functions through tests, and vulnerability assessment, additional security assurance efforts also need to be made from other aspects, e.g., development environment and prevention of misuse. Therefore, EAL3 is an appropriate evaluation assurance level for the TOE.

8.3 TOE Summary Specification Rationale

8.3.1 Appropriateness of Security Functional Requirements for TOE Summary Specification

Table 8.5 shows the appropriateness of the mapping between the security functional requirements and the TOE summary specification.

Table 8.5: Mapping between TOE summary specification and security functional requirements

TOE summary specification / Security functional requirement	F.HDD_CRYPTO	F.KEY_MANAGE	F.KIT_CHECK
FCS_CKM.1		X	
FCS_COP.1	X		
FIA_UAU.2			X
FIA_UAU.4			X
FIA_UID.2			X
FPT_RVM.1	X	X	X

The following describes the rationale to justify the mapping shown in Table 8.5: Mapping between TOE summary specification and security functional requirements.

FCS_CKM.1

FCS_CKM.1 is a functional requirement that “256-bit long cryptographic keys” that meet “FIPS 186-2” be generated in accordance with a “FIPS 186-2-based cryptographic key generation algorithm”.
F.KEY_MANAGE generates 256-bit long cryptographic keys using a FIP 186-2-compliant cryptographic key generation algorithm. Therefore, FCS_CKM.1 is achieved.

FCS_COP.1

FCS_COP.1 is a functional requirement that encryption of HDD writes and decryption of HDD reads be performed in accordance with the “AES encryption algorithm” that is compliant with “FIPS PUB 197” using “256-bit long cryptographic keys”.
F.HDD_CRYPTO performs encryption of HDD writes and decryption of HDD reads in accordance with the AES encryption algorithm as defined in FIPS PUB 197 using 256-bit long cryptographic keys. Therefore, FCS_COP.1 is achieved.

FIA_UAU.2

FIA_UAU.2 is a functional requirement that the TSF require the registered device to be successfully authenticated before use.

F.KIT_CHECK confirms upon startup of the TOE that the TOE is connected to the “registered device” using a challenge-and-response authentication scheme. Therefore, FIA_UAU.2 is achieved.

FIA_UAU.4

FIA_UAU.4 is a functional requirement that the TSF prevent reuse of authentication data related to the “authentication mechanism employed for registered device authentication”.
F.KIT_CHECK allows the “authentication mechanism employed for registered device authentication” to be instantiated and achieved as a challenge-and-response authentication process, and the “prevention of reuse of authentication data” to be achieved by generating a pseudo-random number as a challenge upon each startup of the TOE. Therefore, FIA_UAU.4 is achieved.

FIA_UID.2

FIA_UID.2 is a functional requirement that the TSF require the registered device to be successfully identified before use.
F.KIT_CHECK identifies the registered device by performing a challenge-and-response authentication using the authentication ID that was received from the Canon MFP/printer at the time of installation of the Security Kit. Therefore, FIA_UID.2 is achieved.

FPT_RVM.1

FPT_RVM.1 is a functional requirement that the TSP enforcement functions be invoked without being bypassed.
F.HDD_CRYPTO unifies the paths for HDD writes and reads and hence encrypts/decrypts every data via the TOE, an encryption chip. Therefore, the non-bypassibility of the TSP is ensured in F.HDD_CRYPTO.

F.KEY_MANAGE generates a cryptographic key for use by F.HDD_CRYPTO when the power button, which is a physical switch, is pressed. Since there is no other interface to F.KEY_MANAGE than the power button and its method of use is simply to turn it on or off, F.KEY_MANAGE cannot be bypassed at the time of power-on of the Canon MFP/printer. Therefore, the non-bypassibility of the TSP is ensured in F.KEY_MANAGE.

F.KIT_CHECK enforces a challenge-and-response authentication when the power button, which is a physical switch, is pressed. Since there is no other interface to F.KIT_CHECK than the power button and its method of use is simply to turn it on or off, F.KIT_CHECK cannot be bypassed at the time of power-on of the Canon MFP/printer. Therefore, the non-bypassibility of the TSP is ensured in F.KIT_CHECK.

8.3.2 Rationale for Strength of Function Level for Security Functions

The strength of function level for the specific TOE security functional requirements, FIA_UAU.2, FIA_UAU.4 and FIA_UID.2, is SOF-basic.
Also, the strength of function level for the IT security function, F.KIT_CHECK, is SOF-basic.
Therefore, the strength of function level for the specific TOE security functional requirements is consistent with that for the IT security function.

8.3.3 Rationale for Assurance Measures

As shown in Table 6.1, all the TOE security assurance requirements are met by the set of documents that are provided as assurance measures.
The following describes the rationale for why the EAL3 assurance requirements are satisfied by the assurance measures.

ACM_CAP.3 Authorization controls

[Assurance Measures]
- Canon MFP/Printer Security Chip Configuration Management Plan 1

- Canon MFP/Printer Security Chip Configuration Management Plan 2
- Canon MFP/Printer Security Chip Evaluation Evidence List

[Assurance Requirement Rationale]
The assurance measures, “Canon MFP/Printer Security Chip Configuration Management Plan 1”, “Canon MFP/Printer Security Chip Configuration Management Plan 2” and “Canon MFP/Printer Security Chip Evaluation Evidence List”, specify the naming convention, a list of configuration items and the method for uniquely identifying all configuration items, for TOE version identification purposes. Therefore, the ACM_CAP.3 assurance requirement is satisfied.

ACM_SCP.1 TOE CM coverage

[Assurance Measures]

- Canon MFP/Printer Security Chip Configuration Management Plan 1
- Canon MFP/Printer Security Chip Configuration Management Plan 2
- Canon MFP/Printer Security Chip Evaluation Evidence List

[Assurance Requirement Rationale]
The assurance measures, “Canon MFP/Printer Security Chip Configuration Management Plan 1”, “Canon MFP/Printer Security Chip Configuration Management Plan 2” and “Canon MFP/Printer Security Chip Evaluation Evidence List”, specify the coverage of management of TOE configuration items. Therefore, the ACM_SCP.1 assurance requirement is satisfied.

ADO_DEL.1 Delivery procedures

[Assurance Measures]

- Canon MFP/Printer Security Chip Delivery Procedures 1
- Canon MFP/Printer Security Chip Delivery Procedures 2

[Assurance Requirement Rationale]
The assurance measures, “Canon MFP/Printer Security Chip Delivery Procedures 1” and “Canon MFP/Printer Security Chip Delivery Procedures 2”, specify the procedures for keeping the integrity of the TOE when distributing the TOE to a user’s site. Therefore, the ADO_DEL.1 assurance requirement is satisfied.

ADO_IGS.1 Installation, generation and start-up

[Assurance Measures]

- HDD Data Encryption Kit-B Series Installation Procedure (Japanese)/HDD Data Encryption Kit-B Series Installation Procedure (English)

[Assurance Requirement Rationale]
The assurance measure, “HDD Data Encryption Kit-B Series Installation Procedure” (Japanese/English), specifies the installation procedures and the startup check method that are used for secure configuration of the TOE. Therefore, the ADO_IGS.1 assurance requirement is satisfied.

ADV_FSP.1 Informal functional specification

[Assurance Measures]

- Canon MFP/Printer Security Chip Firmware Functional Specification

[Assurance Requirement Rationale]
The assurance measure, “Canon MFP/Printer Security Chip Firmware Functional Specification”, specifies the specifications of all external interfaces to the TOE security functions. Therefore, the ADV_FSP.1 assurance requirement is satisfied.

ADV_HLD.2 Security enforcing high-level design

[Assurance Measures]

- Canon MFP/Printer Security Chip Firmware High-Level Design
- HERMIT Hardware Manual

[Assurance Requirement Rationale]
The assurance measure, “Canon MFP/Printer Security Chip Firmware High-Level Design”, divides the TSF into subsystems and specifies the specifications of the subsystems and the inter-subsystem interfaces. Also, “HERMIT Hardware Manual” describes the hardware information necessary for firmware development. Therefore, the ADV_HLD.2 assurance requirement is satisfied.

ADV_RCR.1 Informal correspondence demonstration

[Assurance Measures]

- Canon MFP/Printer Security Chip Representation Correspondence

[Assurance Requirement Rationale]
The assurance measure, “Canon MFP/Printer Security Chip Representation Correspondence”, describes the complete correspondence of the TOE security functions at all levels (summary specification – functional specification – high-level design). Therefore, the ADV_RCR.1 assurance requirement is satisfied.

AGD_ADM.1 Administrator guidance

[Assurance Measures]

- HDD Data Encryption Kit-B Series Reference Guide (Japanese)
- HDD Data Encryption Kit-B Series Reference Guide (English)

[Assurance Requirement Rationale]
The assurance measures, “HDD Data Encryption Kit-B Series Reference Guide” (Japanese) and “HDD Data Encryption Kit-B Series Reference Guide” (English), specify the interfaces available to TOE users, the method of use, including warnings, to operate the TOE in a secure manner, and the actions to be taken by users in the event of TOE failure. Therefore, the AGD_ADM.1 assurance requirement is satisfied.

AGD_USR.1 User guidance

[Assurance Measures]

- HDD Data Encryption Kit-B Series Reference Guide (Japanese)
- HDD Data Encryption Kit-B Series Reference Guide (English)

[Assurance Requirement Rationale]
The assurance measures, “HDD Data Encryption Kit-B Series Reference Guide” (Japanese) and “HDD Data Encryption Kit-B Series Reference Guide” (English), specify the interfaces available to TOE users and the method of use, including warnings, to operate the TOE in a secure manner. Therefore, the AGD_USR.1 assurance requirement is satisfied.

ALC_DVS.1 Identification of security measures

[Assurance Measures]

- Canon MFP/Printer Security Chip Firmware Development Security Rules

[Assurance Requirement Rationale]
The assurance measure, “Canon MFP/Printer Security Chip Firmware Development Security Rules”, specifies all the physical, procedural, personnel and other security measures that are used to protect the TOE in its development environment. Therefore, the ALC_DVS.1 assurance requirement is satisfied.

ATE_COV.2 Analysis of coverage

[Assurance Measures]

- Canon MFP/Printer Security Chip Test Coverage Analysis

[Assurance Requirement Rationale]
The assurance measure, “Canon MFP/Printer Security Chip Test Coverage Analysis”, describes the sufficiency and completeness of the tests on the TOE security functions and external interfaces. Therefore, the ATE_COV.2 assurance requirement is satisfied.

ATE_DPT.1 Testing: high-level design

[Assurance Measures]

- Canon MFP/Printer Security Chip Analysis of the Depth of Testing

[Assurance Requirement Rationale]
The assurance measure, “Canon MFP/Printer Security Chip Analysis of the Depth of Testing”, describes the sufficiency and completeness of the tests on the TOE subsystems and inter-subsystem interfaces. Therefore, the ATE_DPT.1 assurance requirement is satisfied.

ATE_FUN.1 Functional testing

[Assurance Measures]

- Canon MFP/Printer Security Chip Test Specification
- Canon MFP/Printer Security Chip Test Procedures
- Canon MFP/Printer Security Chip Test Results

[Assurance Requirement Rationale]
The assurance measures, “Canon MFP/Printer Security Chip Test Specification”, “Canon MFP/Printer Security Chip Test Procedures” and “Canon MFP/Printer Security Chip Test Results”, describe the test plans for the TSF, test procedures and test results. Therefore, the ATE_FUN.1 assurance requirement is satisfied.

ATE_IND.2 Independent testing – sample

[Assurance Measures]

- Canon MFP Security Chip

[Assurance Requirement Rationale]
The assurance measure, Canon MFP Security Chip, reproduces the TOE security function test environment and provides test resources. Therefore, the ATE_IND.2 assurance requirement is satisfied.

AVA_MSU.1 Examination of guidance

[Assurance Measures]

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

[Assurance Requirement Rationale]
The assurance measures, “HDD Data Encryption Kit-B Series Installation Procedure” (Japanese/English), “HDD Data Encryption Kit-B Series Reference Guide” (Japanese) and “HDD Data Encryption Kit-B Series Reference Guide” (English), describe the method of use of the TOE to help TOE users not place the TOE in a non-secure state due to misuse. Therefore, the AVA_MSU.1 assurance requirement is satisfied.

AVA_SOF.1 Strength of TOE security function evaluation

[Assurance Measures]

- Canon MFP/Printer Security Chip Vulnerability Analysis

[Assurance Requirement Rationale]
The assurance measure, “Canon MFP/Printer Security Chip Vulnerability Analysis”, describes a strength of TOE security function analysis for the security mechanisms of the TOE security functions. Therefore, the AVA_SOF.1assurance requirement is satisfied.

AVA_VLA.1 Developer vulnerability analysis

[Assurance Measures]

- Canon MFP/Printer Security Chip Vulnerability Analysis

[Assurance Requirement Rationale]
The assurance measure, “Canon MFP/Printer Security Chip Vulnerability Analysis”, describes that security vulnerabilities cannot be exploited in the intended environment for the TOE. Therefore, the AVA_VLA.1

assurance requirement is satisfied.

8.4 PP Claim Rationale

There is no PP referenced by this ST.

(End of Document)