Canon MFP Security Chip

ISO/IEC 19790 Security Policy

Version 1.06
2015/03/30
Canon Inc.

Table of Contents

List of Figures

List of Tables

1 Introduction

This security policy (hereinafter referred to as SP) is the security policy for the hardware cryptographic module developed by Canon called the Canon MFP Security Chip. This document describes how the Canon MFP Security Chip meets the ISO/IEC 19790 Level 2 security requirements. This SP is a non-proprietary document.

1.1 Reference

This section provides basic information about this SP.

Title	Canon MFP Security Chip ISO/IEC 19790 Security Policy
Version	1.06
Issuer	Canon Inc.
Date of issue	2015/03/30

1.2 Terms and Abbreviations

The following terms and abbreviations are used throughout this SP.

Table 1 Terms and abbreviations

Term/abbreviation	Description
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CO	Crypto Officer
CSP	Critical Security Parameter
PSP	Public Security Parameter
FIPS	Federal Information Processing Standards
Canon MFP/printer	A general term that refers to a Canon brand multifunction product or printer.
Serial ATA (SATA)	A standard for connecting storage devices, based on serial transmission technology.
Storage device	Refers to the storage device on the Canon MFP/printer such as HDD/SSD.

2 Cryptographic Module Description

2.1 Cryptographic Module Overview

The Canon MFP Security Chip handles cryptography for the storage device of the Canon MFP/printer. The Canon MFP Security Chip realizes high-speed data encryption/decryption through a serial ATA interface, using AES CBC mode. This allows the Canon MFP/printer's storage device to be protected against the risk of information leakage, without compromising objectives such as extensibility, flexibility, usability, and high performance.

Details of the approved cryptographic module are given below.

Title	Canon MFP Security Chip
Developer	Canon Inc.

The cryptographic module is a multi-chip embedded module, consisting of the cryptographic chip, the printed circuit board on which the chip is mounted, and the tamper-evident epoxy coating covering the cryptographic chip. The module does not contain the other components on the board. The cryptographic module comes in two types depending on the board on which the chip is mounted, but the chip itself is the same.

The hardware and firmware details of the cryptographic module are given below.

Hardware version	FK4-1731A, FK4-1731B
Firmware version	2.10

The cryptographic boundary is defined as the perimeter of the board. The areas of the board not covered by the epoxy coating are explicitly excluded from the requirements of ISO/IEC 19790, because they are non-security relevant.

Figure 1 and Figure 2 show the exterior of the cryptographic module. Figure 1 shows the FK4-1731A module. The red dashed box in the figure shows the security relevant portion covered within the epoxy coating.

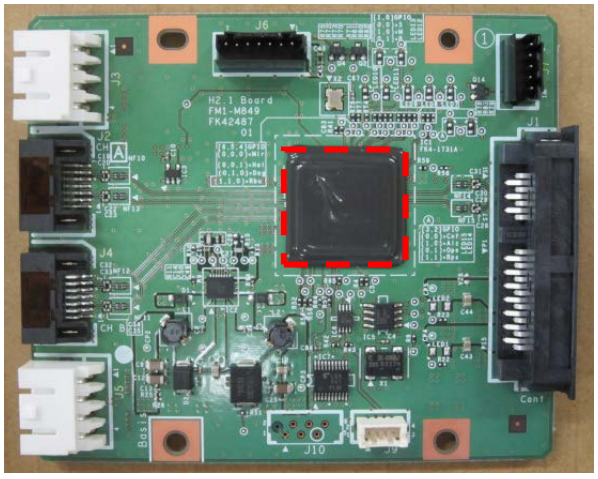
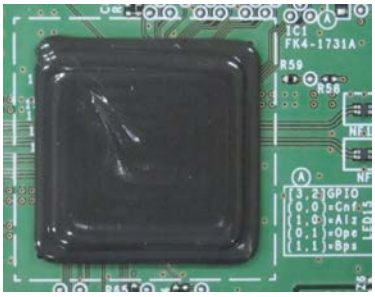
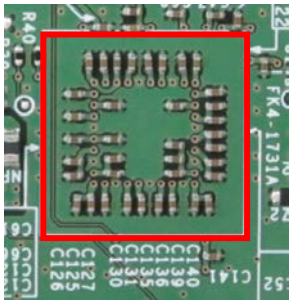


Figure 1 Exterior of Canon MFP Security Chip (FK4-1731A)

Figure 2 shows an enlargement of the area boxed in red in the previous figure. The figure shows the top side and bottom side of the FK4-1731A and FK4-1731B modules, respectively. FK4-1731A and FK4-1731B below, differ only in that each has a different board. The red box in the figure of the bottom side shows the area of the cryptographic chip.

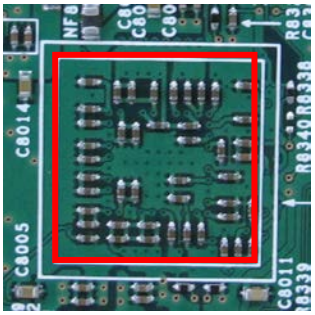


(FK4-1731A: top side)



(FK4-1731A: bottom side)

(FK4-1731B: top side)



(FK4-1731B: bottom side)

Figure 2 Exterior of Canon MFP Security Chip

2.2 Security Level

The Canon MFP Security Chip is a cryptographic module designed and implemented to meet the ISO/IEC 19790 Level 2 security requirements. Table 2 below shows the security level met by the Canon MFP Security Chip for each of the specified areas.

Table 2 Canon MFP Security Chip security requirements

Security requirements section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Role, Service, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

2.3 Cryptographic Module Specification

In addition to cryptography, the Canon MFP Security Chip implements the SATA HOST and SATA DEVICE interfaces. Figure 3 is an example operational diagram of the Canon MFP Security Chip.

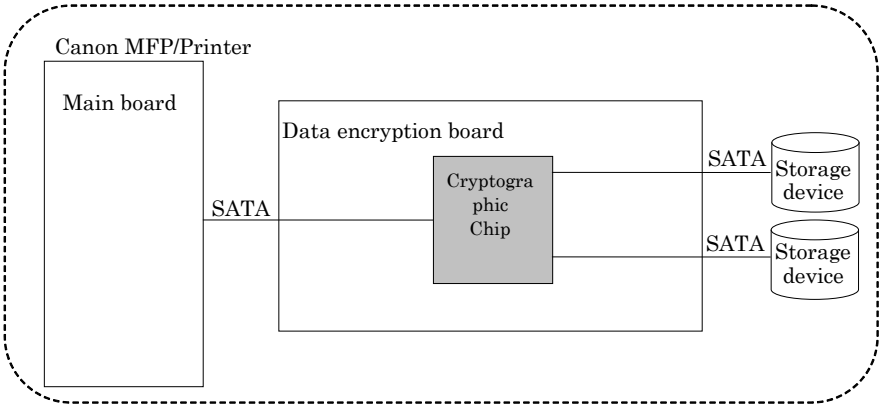


Figure 3 Example operational diagram of Canon MFP Security Chip

The "main board" in Figure 3 is the Canon MFP/printer's own board. The Canon MFP Security Chip is located on a different board (data encryption board), and connects to the main board. The "storage device" contains the data that is encrypted by the Canon MFP Security Chip. The Canon MFP Security Chip features the mirroring function, and allows two storage devices to be connected. However, the second storage device is optional, and only one

is required for normal operation. The interface between the main board and the Canon MFP Security Chip, and between the Canon MFP Security Chip and the storage device, is Serial ATA. The diagram in Figure 3 is provided as an example only, and not meant to restrict where the cryptographic module may be mounted. Hereinafter, the system that is served by the Canon MFP Security Chip ("main board" in Figure 3), is referred to as host system.

The following is a component diagram of the Canon MFP Security Chip, consisting of two dies. The FlashROM sits on one die, with all other components on another die. All of these elements are enclosed in a single package, making up the cryptographic chip.

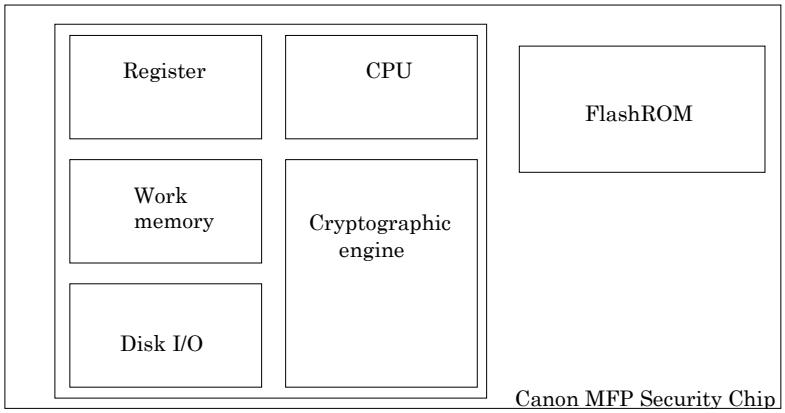


Figure 4 Canon MFP Security Chip component diagram

The role of each component is described below.

Table 3 Role of components of the Canon MFP Security Chip

Component	Role
Register	Temporarily stores program instructions and calculations.
Work memory	Volatile memory that stores data and programs. Cryptographic keys are stored here.
CPU	Executes programs stored in memory.
FlashROM	Non-volatile memory that stores the firmware controlling the Canon MFP Security Chip. Authentication ID and DRBG internal state are stored here.
Disk I/O	Interface that handles I/O requests to the Canon MFP Security Chip.
Cryptographic engine	Handles AES encryption and decryption.

When the Canon MFP Security Chip is powered on, a cryptographic key is automatically calculated using a key seed, and stored in work memory. The authentication ID is the information that allows the Canon MFP Security Chip to uniquely identify the connected host system or Canon MFP/printer. This authentication ID, initially received from the Canon MFP/printer when the Canon MFP Security Chip is first installed, is preserved in FlashROM. Since the cryptographic key is stored in volatile 'work' memory, stored keys are lost (or zeroized) upon power loss. Therefore, at each power up, the above process is repeated, and the cryptographic key is recalculated and stored in work memory.

2.4 Cryptographic Module Ports and Interfaces

This section describes the physical ports of the cryptographic module, and how they relate to the data input/output and power supply interfaces. In terms of the logical interface, the Canon MFP Security Chip operates upon ATA commands that are input from the host system. Each ATA command is associated with a different interface, namely Data Input, Data Output, Control Input, and Status Output.

2.4.1 System

Table 4 Pin descriptions (System)

Pin symbol	Description	Interface type
SYS_CLKIN	External clock input	Control input
SYS_INITXI	Reset input for configuration initialization	Control input

2.4.2 FR Peripheral I/F

Table 5 Pin descriptions (FR Peripheral I/F)

Pin symbol	Description	Interface type
FR_SIN	Serial data input for debug log	Control input
FR_SOUT	Serial data output for debug log	Status output
FR_GPIO	GPIO input/output	Control input/ Status output

2.4.3 SATA Host PHY I/F

Table 6 Pin descriptions (SATA Host PHY I/F)

Pin symbol	Description	Interface type
REFCLK_H	External clock input	Control input
RXPLUSA_H	High-speed serial receive data pin	Data input
RXMINUSA_H	High-speed serial receive data pin	Data input
TXPLUSA_H	High-speed serial transmit data pin	Data output
TXMINUSA_H	High-speed serial transmit data pin	Data output
RXPLUSB_H	High-speed serial receive data pin	Data input
RXMINUSB_H	High-speed serial receive data pin	Data input
TXPLUSB_H	High-speed serial transmit data pin	Data output
TXMINUSB_H	High-speed serial transmit data pin	Data output
VDDSATA_H	Digital 1.2V power source pin	Power input
VSSSATA_H	Digital GND pin	Power input
VDD1IO_H	Analog 1.2V power supply pin for high-speed IO	Power input
VSS1IO_H	Analog GND pin for high-speed IO	Power input
VDD1ANA_H	Analog 1.2V power source pin for PLL	Power input
VDD33ANA_H	Analog 3.3V power supply pin for bias	Power input
VDD33PLL_H	Analog 3.3V power source pin for PLL	Power input
VSS1ANA_H	Analog GND pin for PLL	Power input

VSSRESREF_H	Analog GND pin for securing external resistor	Power input
RESREF_H	Input pin for securing external resistor	Control input

2.4.4 SATA Device PHY I/F

Table 7 Pin descriptions (SATA Device PHY I/F)

Pin symbol	Description	Interface type
REFCLK_D	External clock input	Control input
RXPLUSA_D	High-speed serial receive data pin	Data input/ Control input
RXMINUSA_D	High-speed serial receive data pin	Data input/ Control input
TXPLUSA_D	High-speed serial transmit data pin	Data output/ Status output
TXMINUSA_D	High-speed serial transmit data pin	Data output/ Status output
VDDSATA_D	Digital 1.2V power source pin	Power input
VSSSATA_D	Digital GND pin	Power input
VDD1IO_D	Analog 1.2V power supply pin for high-speed IO	Power input
VSS1IO_D	Analog GND pin for high-speed IO	Power input
VDD1ANA_D	Analog 1.2V power source pin for PLL	Power input
VDD33ANA_D	Analog 3.3V power supply pin for bias	Power input
VDD33PLL_D	Analog 3.3V power source pin for PLL	Power input
VSS1ANA_D	Analog GND pin for PLL	Power input
VSSRESREF_D	Analog GND pin for securing external resistor	Power input
RESREF_D	Input pin for securing external resistor	Control input

2.4.5 SATA PHY I/F (Common)

Table 8 Pin descriptions (SATA PHY I/F (Common))

Pin symbol	Description	Interface type
REFCLK_HD	Reference clock input	Control input

2.4.6 TEST I/F

Table 9 Pin descriptions (TEST I/F)

Pin symbol	Description	Interface type
TEST	Test pin	Control input
VPD	Feedthrough current prevention pin	Control input
TCK	JTAG test clock input	Control input
TMS	TAP controller mode select input	Control input
TRST	JTAG test reset input	Control input
TDI	JTAG test data input	Data input
TDO	JTAG test data output	Data output

2.4.7 Power Supply

Table 10 Pin descriptions (Power supply)

Pin symbol	Description	Interface type
VDE	3.3V power supply pin	Power input
VDD	1.2V power supply pin	Power input
VSS	GND pin	Power input
PLLVDD	APLL dedicated 1.2V power supply pin	Power input
PLLVSS	APLL dedicated GND pin	Power input
FLVDE	FLASH 3.3V power supply pin	Power Input

2.5 Roles, Services, and Authentication

2.5.1 Roles

The Canon MFP Security Chip supports two distinct operator roles, USER and CO (Cryptographic Officer). The following table shows each role and its associated services. The Canon MFP Security Chip does not provide the maintenance service, so no MAINTENANCE role is supported.

Table 11 Roles supported by the Canon MFP Security Chip

Role	Description	Authentication Type	Authentication Data
USER	USER represents users of the encryption/decryption service of the Canon MFP Security Chip. USER is allowed use of the AES encryption/decryption services as described in Table 13.	Role-based	Shared secret
CO	CO performs configuration of secret information of the Canon MFP Security Chip. CO is allowed use of the services associated with CO as described in Table 13. CO authentication is required prior to use of these services.	Role-based	Shared secret

2.5.2 Services

This section describes the cryptographic services provided by the Canon MFP Security Chip. The Canon MFP Security Chip supports FIPS140-2 approved mode of operation implementing the security functions validated by JCMVP, as well as non-FIPS140-2 approved mode of operation implementing no cryptography. The Canon MFP Security Chip in FIPS140-2 approved mode provides the approved algorithms described in the following table.

Table 12 Approved algorithms available on the Canon MFP Security Chip

Approved Algorithm	Spec	CAVP Certificate	Usage
AES Encryption/Decryption Mode: CBC Key Length: 128bit,256bit	FIPS PUB 197	#2907	Used in encryption/decryption of data stored in storage device.
SHA-256	FIPS PUB 180-4	#2601	Used in Hash_DRBG random bit generation, and response generation for Device Identification and Authentication.
Hash_DRBG	SP 800-90A	#638	Used in cryptographic key generation, and challenge generation for Device Identification and Authentication.

The Canon MFP Security Chip in FIPS140-2 approved mode additionally provides one other non-approved but allowed algorithm, NDRNG. NDRNG is used in generating the seed value for approved DRBG.

Table 13 and Table 14 below describe the services provided on the Canon MFP Security Chip. Table 13 describes the services provided in FIPS140-2 approved mode, and Table 14 describes those provided in non-FIPS140-2 approved mode.

Table 13 Services provided in FIPS140-2 approved mode

Role	Service	Description	Algorithm	Input	Output
USER	AES encryption	Encrypts and writes data to the storage device.	AES Encryption	ATA write command	Encrypted data is transmitted to the storage device. If mirroring is enabled, encrypted data is sent to both storage devices.
USER	AES decryption	Reads data from the storage device and decrypts.	AES Decryption	ATA read command	Decrypted data is transmitted to the host system

None	Process ATA command	Supported* ATA commands received from the host system are analyzed and transmitted to storage. Unsupported commands are not transmitted. * ATA write/read commands are excluded.		ATA command, excluding ATA write/read commands and extended ATA commands.	Result is transmitted to the host system.
None	Initialization	Initializes the Canon MFP Security Chip. The cryptographic key is calculated using the key seed, and stored in work memory within the module.	Hash_DRBG	Reset signal	-
None	Zeroize AES key	Clears the cryptographic key stored in volatile memory.		Power off	-
None	Behavior settings	Configures the behavior settings of the Canon MFP Security Chip.		Extended ATA command for behavior settings	Result is transmitted to the host system.
None	Output status	Outputs status of the Canon MFP Security Chip.		Extended ATA command for status output	Status is transmitted to the host system.
CO	Configure secret information	Configures the authentication ID, and generates the key seed for AES cryptographic key generation.	Hash_DRBG	Extended ATA command for setting secret information	Result is transmitted to the host system.
None	Zeroize secret information	Clears (zeroizes) secret information.		Extended ATA command for clearing secret information	Result is transmitted to the host system.
CO	Output secret information	Key seed is output in plaintext form from the cryptographic module.		Extended ATA command for output of secret information	Secret information is transmitted to the host system.
CO	Input secret information	Replaces the key seed, with the one received from the host system in plaintext form.		Extended ATA command for input of secret information	Result is transmitted to the host system.

CO	Change CO authentication information	Modifies CO authentication information.		Extended ATA command for modifying CO authentication information	Result is transmitted to the host system.
None	Change mode	Clears (zeroizes) all CSPs and transitions to non-FIPS140-2 approved mode.		Extended ATA command for changing mode	Result is transmitted to the host system.
USER	Device Identification and Authentication	Uses challenge-response authentication to identify/authenticate that the connection is with the correct host system. The Canon MFP Security Chip provides services such as encryption/decryption, only when authentication succeeds.	Hash_DRBG SHA-256	Extended ATA command for controlling the authentication function	Result is transmitted to the host system.
None	Perform self-test	Executes a self test.		Reset signal	Interrupt notification to the host system, plus extended ATA command for status output.

Table 14 Services provided in non-FIPS140-2 approved mode

Role	Service	Description	Algorithm	Input	Output
None	Process ATA command	Supported ATA commands received from the host system are analyzed and transmitted to storage. Unsupported commands are not transmitted. ATA write/read commands are included in this service, handling data in plaintext form.		ATA command	Result is transmitted to the host system.

None	Behavior settings	Configures the behavior settings of the Canon MFP Security Chip.		Extended ATA command for behavior settings	Result is transmitted to the host system.
None	Output status	Outputs status of the Canon MFP Security Chip.		Extended ATA command for status output	Status is transmitted to the host system.
CO	Configure secret information	Configures the authentication ID, generates the key seed for AES cryptographic key generation, then transitions to FIPS140-2 approved mode.	Hash_DRBG	Extended ATA command for setting secret information	Result is transmitted to the host system.
None	Perform self-test	Executes a self test.		Reset signal	Interrupt notification to the host system, plus extended ATA command for status output.

The Canon MFP Security Chip operates in non-FIPS140-2 approved mode in its initial state. It makes the transition to FIPS140-2 approved mode by using the configure secret information service. Output status service can be used to determine the current operating mode: FIPS140-2 approved mode or non-FIPS140-2 approved mode. Conversely, the Canon MFP Security Chip makes the transition back to non-FIPS140-2 approved mode by using the change mode service.

2.5.3 Operator Authentication

Before providing any of the services associated with USER and CO respectively, the Canon MFP Security Chip performs role-based authentication by shared secret. The authentication mechanism differs for each role, as follows.

- CO authentication
  Authentication is based on CO authentication information defined in section 2.8.1.
- USER authentication
  Uses challenge-response authentication based on Authentication ID defined in 2.8.1. USER authentication is referred to as Device Identification and Authentication. In Device Identification and Authentication, the challenge generated from the DRBG and a response value derived from the challenge and the authentication ID, are used to mutually identify/authenticate the host system and the Canon MFP Security Chip.

For the shared secret, CO authentication uses a 4 byte random number, and USER authentication uses a 30 byte random number, so the probability that a random attempt will

succeed is $1/2^{32}$ and $1/2^{240}$ respectively, both of which are less than 1/1,000,000 as the objective. The module is capable of performing CO authentication every 100 milliseconds, and USER authentication every 3 milliseconds. Therefore, the probability that multiple consecutive random authentication attempts will be successful during a one-minute period is $600/2^{32}$ and $20000/2^{240}$ respectively, both of which are less than 1/100,000 as the objective. As such, in terms of the strength of the authentication mechanism, the Canon MFP Security Chip provides sufficient level of strength.

2.6 Physical Security

The Canon MFP Security Chip is a multi-chip embedded module, consisting of the cryptographic chip and the board on which the chip is mounted. The cryptographic chip is covered within an opaque, hard, tamper-evident epoxy coating (shown in Figure 2). Attempts to gain access to the internal components of the cryptographic module will require removal of at least one part of the coating, so that no attempt to remove the coating can succeed without physically deforming the coating, showing evidence of tampering.

2.7 Operational Environment

The Canon MFP Security Chip has no firmware update utility, and runs in a single operating environment only.

2.8 Cryptographic Key Management

2.8.1 Definition of Critical Security Parameters (CSPs)

The tables below list the CSPs and PSP handled by the Canon MFP Security Chip. The key seed, authentication ID, and CO authentication information are collectively termed Secret Information.

Table 15 CSP list

CSP	Description
AES cryptographic key	Key for encryption/decryption. Cryptographic key is stored in volatile work memory in plaintext form.
Key seed	Seed value used for AES cryptographic key calculation. This information is stored in Flash ROM in plaintext form.
Authentication ID	ID for mutually authenticating the Canon MFP Security Chip and the host system, for Device Identification and Authentication. This information is stored in FlashROM in plaintext form.
CO authentication information	Information for CO authentication. This information is stored in Flash ROM in plaintext form.
DRBG internal state	Internal state used for challenge generation, for Device Identification and Authentication. Updated each time random bit generation takes place. This information is stored in FlashROM.

Table 16 PSP list

PSP	Description
Challenge-response	The challenge value and response value, for Device Identification and Authentication. Temporarily stored in work memory, during Device Identification and Authentication. These are public values, or PSP as defined in ISO/IEC 19790.

Table 17 defines the relationship between access to CSPs and the services available on the Canon MFP Security Chip.

The types of access shown in the table are defined as follows: R=Read, W=Write, and Z=Zeroize. Read access is internal only, contained within the module itself. In other words, there is no direct access from outside of this module.

Table 17 Relationship between access to CSPs and the services

Service	CSP	Type
AES encryption	AES cryptographic key	R
AES decryption	AES cryptographic key	R
Process ATA command	N/A	N/A
Initialization	AES cryptographic key	W
	Key seed	R
Zeroize AES key	AES cryptographic key	Z
Behavior settings	N/A	N/A
Output status	N/A	N/A
Configure secret information	Authentication ID, key seed, AES cryptographic key	W
	CO authentication information, DRBG internal state	R/W
Zeroize secret information	Key seed, authentication ID, AES cryptographic key	Z
Output secret information	Key seed	R
	CO authentication information	R
Input secret information	Key seed, AES cryptographic key	W
	CO authentication information	R
Change CO authentication information	CO authentication information	R/W
Change mode	CO authentication information, key seed, authentication ID, DRBG internal state, AES cryptographic key	Z
Device Identification and Authentication	Authentication ID	R
	DRBG internal state	R/W
	Challenge-response	R/W
Perform self-test	N/A	N/A

2.9 Self-Tests

The Canon MFP Security Chip performs various self-tests (power-up self-tests and conditional self-tests). The self-tests are detailed in Table 18 below.

Table 18 Self test

Test item	Test method	Test type
AES Encryption	Known answer test	Power-Up
AES Decryption	Known answer test	Power-Up
Hash_DRBG	Known answer test	Power-Up
SHA-256	Known answer test	Power-Up
Firmware Integrity Test	Firmware integrity test using 32 bit CRC	Power-Up
Hash_DRBG	Continuous random bit generator test	Conditional
NDRNG	Continuous random number generator test	Conditional
CSP Integrity Test	Integrity tests of secret information and DRBG internal state by 32 bit CRC	Conditional

2.9.1 Power-Up Tests

When the Canon MFP Security Chip is powered up, it automatically performs the power-up self-tests. The power-up self-tests performed by the Canon MFP Security Chip are detailed in Table 18.

If any of the tests returns an error, the Canon MFP Security Chip immediately enters the error state and can no longer read from or write to any storage device. Error status may be acquired using the output status service. Recovery from error state will require repair of the Canon MFP Security Chip by notifying/contacting your vendor.

The power-up self-tests can be invoked on-demand by resetting the Canon MFP Security Chip.

2.9.2 Conditional Tests

The Canon MFP Security Chip implements the conditional self-tests shown in Table 18. The Hash_DRBG and NDRNG continuous random number generator tests are performed before each use of the Hash_DRBG pseudo-random bit generator. Also, as a critical security function, the Canon MFP Security Chip performs management of secret information and DRBG internal state, and therefore implements the CSP Integrity Test in Table 18 as a critical function test. The CSP Integrity Test uses 32bit CRC to test the integrity of the secret information and DRBG internal state, before reading secret information or DRBG internal state stored in FlashROM.

If any of the conditional self-tests returns an error, the Canon MFP Security Chip immediately enters the error state and can no longer read from or write to any storage device.

Error status may be acquired using the output status service. Recovery from error state will require repair of the Canon MFP Security Chip by notifying/contacting your vendor.

The Canon MFP Security Chip does not support a bypass capability, so no bypass test is available.

2.10 Mitigation of Other Attacks

The Canon MFP Security Chip does not provide any other additional mechanisms to mitigate attacks.

3 Secure Operation

3.1 Initial Set-Up

The Canon MFP Security Chip operates in non-FIPS140-2 approved mode in its initial state. To use the Canon MFP Security Chip in FIPS140-2 approved mode, the CO shall perform the following.

The CO uses the configure secret information service, to set secret information to the Canon MFP Security Chip. The Canon MFP Security Chip, in its initial state, does not have default CO authentication information and default authentication ID. In the service, CO should set both CO authentication information and authentication ID at the same time. The CO authentication information should be a 4 byte value that cannot easily be guessed and the authentication ID should be a 30 byte value that cannot easily be guessed. Upon receiving a request for this service, the Canon MFP Security Chip writes the authentication ID to FlashROM, and generates the key seed for AES cryptographic key generation. Afterwards, it makes the transition to FIPS140-2 approved mode.
Output status service can be used to determine the current operating mode. In response, the CO receives data from the Canon MFP Security Chip indicating either FIPS140-2 approved mode or non-FIPS140-2 approved mode.

The operator shall periodically perform tamper evidence inspection of the Canon MFP Security Chip. Physical access to the contents of the module cannot be gained without removing at least one part of the coating that covers the cryptographic chip. The operator shall inspect the coating for any signs of tampering. If the operator discovers tamper evidence, the cryptographic module should not be used.

3.2 Zeroization

The Canon MFP Security Chip zeroizes all CSPs when it switches to non-FIPS140-2 approved mode. The change mode service is used to cause the module to transition to non-FIPS140-2 approved mode.

END