Canon MFP Security Chip

FIPS140-2 Security Policy

Version 1.19
2020/12/07
Canon Inc.

Non-proprietary Security Policy

Contents

Trademark Notice

- Canon and the Canon logo are trademarks of Canon Inc.
- All names of companies and products contained herein are trademarks or registered trademarks of the respective companies.

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 FIPS140-2 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 FIPS140-2 Security Policy
Version	1.19
Issuer	Canon Inc.
Date of issue	2020/12/07

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
XTS	XEX encryption mode with tweak and ciphertext stealing
CO	Crypto Officer
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standards
Canon MFP/printer	A general term that refers to a Canon brand multifunction peripheral 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 General

2.1 Security Level

Table 2 described in Section 3.1 shows the security level met by the Canon MFP Security Chip for each of the specified areas.

2.2 Certificate Caveat

When operated in FIPS mode. No assurance of the minimum strength of generated keys per Note *1 to Table 7.

3 Cryptographic Module Specification

3.1 Cryptographic Module Overview

The Canon MFP Security Chip is a cryptographic module designed and implemented to meet the FIPS140-2 Level 2 security requirements. Table 2 shows the security level met by the Canon MFP Security Chip for each of the specified areas.

Table 2 Security level for each security requirement (FIPS140-2)

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

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 XTS-AES 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.

The Canon MFP Security Chip is a “multi-chip embedded cryptographic module” and the cryptographic boundary is the surface of the package. The following shows the hardware and firmware comprising the Canon MFP Security Chip(As described in Section 3.2, all elements of the module are enclosed in a single package).

Name of the cryptographic module	Canon MFP Security Chip
Hardware version	3.0
Firmware version	3.00, 3.00(V05L00)

Figure1 and Figure2 show the appearance of the Canon MFP Security Chip. The physical boundary of the Canon MFP Security Chip is the surface of the package.

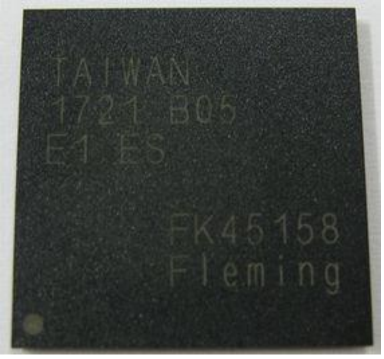

Figure 1 Appearance of the Canon MFP Security Chip

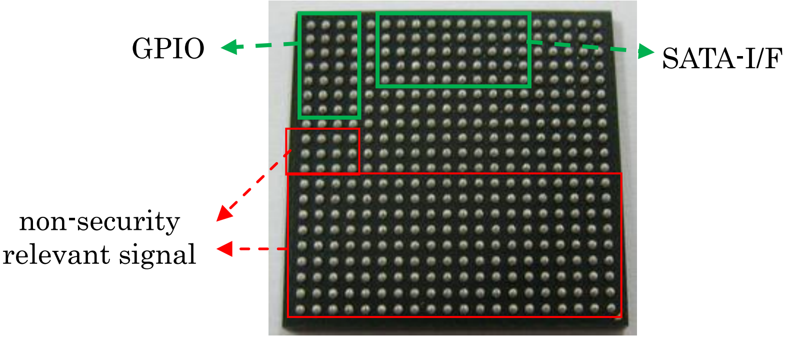

Figure 2 Appearance of Canon MFP Security Chip (Bottom view)

3.2 Cryptographic Module Description

In addition to the cryptographic process, the Canon MFP Security Chip has SATA HOST and SATA DEVICE interface. Figure 3 shows an example of configuration for cryptographic module operation. The red line in the figure shows the cryptographic boundary.

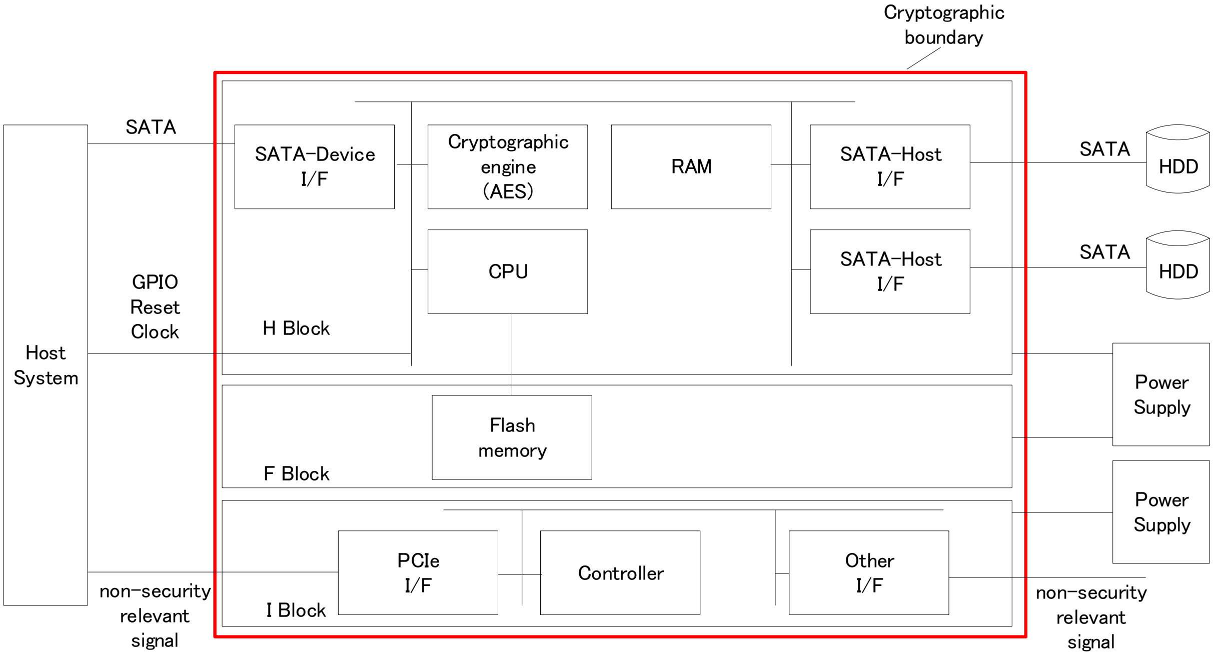

Figure 3 Example of operational configuration of Canon MFP Security Chip

The Canon MFP Security Chip is located between the host system and storage device. The host system is a system to use the services provided by the Canon MFP Security Chip, while the storage device is a memory device to store data encrypted by the Canon MFP Security Chip. The Canon MFP Security Chip also has a mirroring function thus it is possible to connect two storage devices. However, the second storage device is optional and it is possible to operate with only one storage device. Serial ATA is used as the interface between the host system and Canon MFP Security Chip, and between the Canon MFP Security Chip and storage device.

The Canon MFP Security Chip consists of three blocks: H block for the main process of the cryptographic module; F block where flash memory is mounted; and I block not related to the services provided by the cryptographic module. The Canon MFP Security Chip consists of two dies: H and I blocks sit on one die, and F block, on the other. All of these elements are enclosed in a single package, making up the cryptographic chip. All the security services of the cryptographic module are implemented in H block and F block. Firmware and CSP data to be executed in H block are stored in the flash memory in F block. I block does not have any physical I/F with H and F blocks, including the power supply. Therefore, it is not possible to access CSPs from I block and there is no impact on input/output of the cryptographic module. I block has no impact on the security of the Canon MFP Security Chip and thus explicitly excluded from the FIPS140-2 requirements.

The following shows the role of each component of H and F blocks:

Table 3 Roles of components of the Canon MFP Security Chip

Component	Role
RAM	Volatile memory that stores data and programs.
CPU	Executes programs stored in memory.
Flash memory	Non-volatile memory that stores the firmware controlling the Canon MFP Security Chip as well as CSPs.
SATA-Device I/F SATA-Host I/F	Interface to process SATA I/O for the Canon MFP Security Chip.
Cryptographic engine	Handles AES encryption and decryption.

3.3 Mode of Operation

The Canon MFP Security Chip supports FIPS140-2 approved mode implementing security functions approved by CMVP and non-FIPS140-2 approved mode implementing no cryptography.
The Canon MFP Security Chip operates in non-FIPS140-2 approved mode just after shipping. It transitions to FIPS140-2 approved mode by using the “Transition to Approved mode” service to be described later.
If “Change mode” service is used in FIPS140-2 approved mode, the module will transition to non-FIPS140-2 approved mode.

3.4 Cryptographic Algorithm

The Canon MFP Security Chip provides the following approved algorithms in FIPS140-2 approved mode.

Table 4 Approved algorithms available on the Canon MFP Security Chip

Algorithm	Description	Spec	CAVP Certificate	Usage
XTS-AES	Encryption/Decryption Key Strength: 128 bits, 256 bits	FIPS PUB 197 SP800-38E	#C217	Used in encryption/decryption of data stored in storage device.
SHA-256	Size: 256 bit	FIPS PUB 180-4	#4547	Used in Hash_DRBG random bit generation, response generation for Device Identification and Authentication, and RSA digital signature verification.
RSA	Signature Verification Modulus: 2048 bit	FIPS PUB 186-4 PKCS#1	#3059	Used for firmware verification.
Hash_DRBG		SP 800-90A	#2300	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-FIPS140-2 approved but allowed algorithm, NDRNG. NDRNG is used in generating the seed value for approved DRBG. Minimum entropy provided by the NDRNG is 5bits per 8bits. Total 896 bits random data is provided by NDRNG to Hash_DRBG for key generation, and it includes 560 bits (=896 bits x 5 bits/8 bits) entropy.

4 Cryptographic Module Ports and Interfaces

This section describes the physical ports of the Canon MFP Security Chip, 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.

Table 5 Ports and interfaces

Port	Description	Interface type
SATA-Device	I/F with the host system	Control Input Status Output Data Input Data Output
SATA-Host	I/F with the storage device(s)	Data Input Data Output
Power supply	Power supply	Power supply
GPIO	GPIO I/O	Status Output
Reset	Reset signal Input	Control Input
Clock	Clock Input	Control Input

Information that passes through the logical I/F are as follows;
・Data input:Plaintext user data, Ciphertext user data, "Authentication ID" (plaintext) sent from the host, "CO authentication information" (plaintext) sent from the host, "Key seed" (plaintext) sent from the host, Challenge device authentication, Response for host authentication, new firmware image for Update firmware service.

・Data output: Plaintext user data, Ciphertext user data, "Key seed" (plaintext) sent into the host, Challenge for host authentication, Response for device authentication.

・Control Input: Non-data portion of the ATA command sent from the host, clock and reset signals

・Status Output: Non-data portion of the response to the ATA command from the host, module status output from GPIO (non-security relevant)

5 Roles, Services, and Authentication

5.1 Roles

The Canon MFP Security Chip supports two distinct operator roles, USER and CO. The following table shows each role. The Canon MFP Security Chip does not provide the maintenance service, so no MAINTENANCE role is supported. It does not support concurrent use by multiple operators or bypass function.

Table 6 Roles supported by the Canon MFP Security Chip

Role	Description	Auth. Type	Auth. Data	Approved security function to use
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 7.	Role-based	Shared secret	Hash_DRBG SHA-256 Encryption Decryption
CO	CO performs configuration of secret information and update of firmware of the Canon MFP Security Chip. CO is allowed use of the services associated with CO as described in Table 7.	Role-based	Shared secret	Hash_DRBG SHA-256 RSA

5.2 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.

- USER authentication (Shared Secret)

  Uses challenge-response authentication based on Authentication ID defined in 10.1. USER authentication is referred to as "Device Identification and Authentication" service. 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.
  Response value is calculated by concatenating challenge and authentication ID, and then calculating hash values.

- CO authentication (Shared Secret)

  Uses challenge-response authentication based on CO authentication information defined in section 10.1. The Canon MFP Security Chip generates challenge from DRBG and performs CO authentication using the response value notified by the host system.
  Response value is calculated by concatenating challenge and authentication ID, and then calculating hash values.

For the shared secret, both CO authentication and USER authentication use a 32-byte random number, so the probability that a random attempt will succeed is $1/2^{256}$, which is less than the objective of 1/1,000,000. The module is capable of performing CO authentication every 60 milliseconds, and USER authentication, every 120 milliseconds. Therefore, the probability that multiple consecutive random authentication attempts will be successful during a one-minute period is $1000/2^{256}$ and $500/2^{256}$ respectively, both of which are less than the objective of 1/100,000.

5.3 Services

This section describes the cryptographic services provided by the Canon MFP Security Chip. Table 7 and Table 8 show the services provided in FIPS140-2 approved mode and non-FIPS140-2 approved mode, respectively.
See Table 11 for individual access rights for all CSPs and the method for authenticating each roles, regarding CSP used by each service and respective operator roles allowed to use the service.
Also, see Table 6 for the method used for authentication to each operator role.

Table 7 Services provided in FIPS140-2 approved mode

Role	Service	Description	Algorithm	Input	Output
USER	AES encryption	Encrypts and writes data to the storage device(s).	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
CO	Configure secret information	Configures the authentication ID and CO authentication information, and generates the key seed for AES cryptographic key generation. Writes the Host-originated CSPs to Flash memory.	Hash_DRBG	Extended ATA command for setting 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 secret information received from the host system in plaintext form. *1		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.
CO	Update firmware	Updates firmware of the cryptographic module. For firmware update, the new firmware image for firmware updating is stored to the non-running firmware storage space of the two storage spaces. After receiving all of the	RSA SHA-256	Extended ATA command for updating firmware	Result is transmitted to the host system.

		firmware data, the Canon MFP Security Chip verifies the received digital signature. In case the verification succeeds, the Canon MFP Security Chip deletes the secret information, returns a success status and switches to non-FIPS140-2 approved mode. Then, the next start-up, the Canon MFP Security Chip starts with the new firmware. The new firmware launches for the first time after the device is reset. If verification fails, the Canon MFP Security Chip discards the new firmware, returns an error, and quits the firmware update. In that case, the Canon MFP Security Chip will continue to operate with the pre-update firmware.			
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	Show status	Shows the version of the cryptographic module and its current status.		Extended ATA command for show status	Status is transmitted to the host system.
None	Zeroize secret	Clears (zeroizes) secret		Extended ATA	Result is

	information	information.		command for clearing secret information	transmitted to the host system.
None	Change mode	Clears (zeroizes) all CSPs and transitions to non-FIPS140-2 approved mode. This service is equivalent to "Perform zeroisation" service that zeroizes all unprotected CSPs		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 USER authentication	Result is transmitted to the host system.
CO	CO authentication	Performs CO authentication with challenge-response authentication. The Canon MFP Security Chip provides services to CO only when authentication succeeds.	Hash_DRBG SHA-256	Extended ATA command for CO authentication	Result is transmitted to the host system.
None	Self-test	Performs self-tests.		Reset signal	Interrupt notification to the host system, plus extended ATA command for show status.

*1 When this service is used, there is no assurance of the minimum strength of generated keys. It is strongly recommended that the “Key seed” generated by the module itself and output by the “Output secret information” service is input in this service.

Table 8 Services provided in non-FIPS140-2 approved mode

Role	Service	Description	Algorithm	Input	Output
None	Process ATA commands	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. Data is exchanged 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	Show status	Shows status of the Canon MFP Security Chip.		Extended ATA command to show status	Status is transmitted to the host system.
None	Transition to Approved mode	Transitions to FIPS140-2 approved mode after conducting a Self-tests.		Extended ATA command for transition to FIPS140-2 approved mode	Result is transmitted to the host system.
None	Perform self-test	Executes self-tests.		Reset signal	Interrupt notification to the host system, plus extended ATA command for show status.

The initial state is non-FIPS140-2 approved mode, and then transitions to FIPS140-2 approved mode by running the "Transition to Approved mode" service. It is possible to determine if the cryptographic module is in FIPS140-2 approved mode or in non-FIPS140-2 approved mode by using Show status service. If Change mode service is used in FIPS140-2 approved mode, the module will transition to non-FIPS140-2 approved mode.

6 Software/Firmware Security

At the start-up, the Canon MFP Security Chip performs an integrity test of the firmware using digital signature of RSA 2048 bit. By resetting the Canon MFP Security Chip, it is possible to perform an on-demand integrity test of the firmware.

It is also possible for CO to update the firmware by completely replacing it using Update firmware service. When the firmware is updated, the firmware to be updated is verified by digital signature of RSA 2048 bit. In case the verification succeeds, the Canon MFP Security Chip zeroizes CSPs and starts with new firmware after a reset.

7 Operational Environment

The Canon MFP Security Chip operates in limited operational environment. It has a function to update firmware but the firmware to be updated has to be the one approved by CMVP. In case other firmware is loaded, it is considered outside of the scope of this certification. The firmware will be completely replaced by the update function.

8 Physical Security

The Canon MFP Security Chip is a multi-chip embedded module where all the components are enclosed in a package and sealed by opaque plastic mold (coating). Therefore, in order to see inside of the Canon MFP Security Chip, it is necessary to remove at least a part of the plastic mold thus tamper evidence will be left if an attempt to remove the mold is made.

9 EMI/EMC

EMI/EMC conformance test of the Canon MFP Security Chip was performed using a MFP, which implements the Canon MFP Security Chip, in an FCC recognized accredited laboratory. It was confirmed that the cryptographic module conforms to FCC 47 CFR Part15 Subpart B：Class A.

10 Cryptographic Key Management

10.1 Definition of Critical Security Parameters (CSPs)

The following tables show CSPs handled by the Canon MFP Security Chip. Key seed, authentication ID and CO authentication information are collectively called “secret information”. There are no cryptographic algorithms and its parameters with an expiration date in this module.

Table 9 CSP list

CSP	Description	Key	Algorithm	Import/ Export	Stored at:	Stored in:
AES cryptographic keys	“Symmetric Key” for encryption/decryption, generated by using Approved Hash_DRBG shown in Table 4.	[Strength] 128bit, 256bit In XTS-AES, keys of the same key length exist in pairs. [Length] 128bit*2, 256bit*2	XTS-AES See Table 4 for algorithm Certification number.	N/A	RAM	Plaintext
Key seed	The Seed value used in AES Cryptographic key generation can be generated/input by the following methods: (1) Generated by the instantiation function of Hash_DRBG in Table 4 by “Configure secret information” in CO Role, that uses random number from "non-FIPS140-2 approved NDRNG described in Section 3.4" as entropy_input and nonce. (2) Input from the Host System by "Input secret information" in CO Role. The importing Key seed requires to have 256 bits of strength. The “Input secret information” service assumes that the Key	N/A	Hash_DRBG	Import/ Export	Flash	Plaintext

	seed output by the “Output secret information” service from this module is input.					
Authentication ID	ID for mutually authenticating the Canon MFP Security Chip and the host system, for Device Identification and Authentication. Set by configure secret information service.	N/A	N/A	Import	Flash	Plaintext
CO authentication information	Information for CO authentication. Set by configure secret information service. It is possible to set different authentication information for each service and the cryptographic module can retain multiple sets of authentication information.	N/A	N/A	Import	Flash	Plaintext
DRBG internal state	Internal state information used for challenge generation, for Device Identification and Authentication. It is generated by the instantiation function of Hash_DRBG in Table 4, that uses random number from "non-FIPS140-2 approved NDRNG described in Section 3.4" as entropy_input and nonce, in power on sequence. And it is updated whenever the generation function of Hash_DRBG is called.	N/A	N/A	N/A	RAM	Plaintext

Table 10 Public Key list

Public Key	Description	Key	Algorithm	Import/Export	Stored at:	Stored in:
Vendor public key	Public key for verification to load the firmware. Stored when manufacturing the Canon MFP Security Chip.	[Strength] 112bit [Length] 2048bit	RSA See Table 4 for algorithm Certification number.	N/A	Flash	Plaintext

Table 11 shows the CSPs related to the services provided by the Canon MFP Security Chip and types of operation for the CSP.

The types of access shown in the table are defined as follows: R=Read, W=Write, E=Execute, 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. In addition, there is no means for accessing CSPs, logically or physically, except for the ones shown in Table 11.
Zeroization of CSP is performed by overwriting the area where corresponding CSP is stored with 0 or 1.

Table 11 CSPs and the services

Role	Service	CSP	Type
USER	AES encryption	AES cryptographic keys	E
USER	AES decryption	AES cryptographic keys	E
None	Process ATA command	N/A	N/A
None	Initialization	AES cryptographic keys	W
		Key seed	E
		DRBG internal state	W
None	Zeroize AES key	AES cryptographic keys	Z
None	Behavior settings	N/A	N/A
None	Show status	N/A	N/A
CO	Configure secret information	Authentication ID, key seed, AES cryptographic keys	W
		CO authentication information, DRBG internal state	E/W
None	Zeroize secret information	Key seed, authentication ID, AES cryptographic keys	Z
CO	Output secret information	Key seed	R
		CO authentication information	E
CO	Input secret information	Key seed, AES cryptographic keys	W
		CO authentication information	E
CO	Change CO authentication information	CO authentication information	E/W
None	Change mode	CO authentication information, key seed, authentication ID, DRBG internal state, AES cryptographic keys	Z
USER	Device Identification and Authentication	Authentication ID	R
		DRBG internal state	E/W
CO	CO authentication	CO authentication information	R
		DRBG internal state	E/W
CO	Update firmware	Vendor public key, CO authentication information, key seed, authentication ID, DRBG internal state, AES cryptographic keys	Z
None	Self-test	N/A	N/A

11 Self-Tests

The Canon MFP Security Chip has Power-up self-test and conditional self-test functions. Table 12 shows tests to be performed in self-test.

Table 12 Self-test

Test item	Test method	Test type
AES Encryption	Known answer test	Power-up

	(XTS:2*256bit key)	(Cryptographic Algorithm Self-Test)
AES Decryption	Known answer test (XTS:2*256bit key)	Power-up (Cryptographic Algorithm Self-Test)
Hash_DRBG	Known answer test (instantiate/generate)	Power-up (Cryptographic Algorithm Self-Test)
SHA-256	Known answer test	Power-up (Cryptographic Algorithm Self-Test)
RSA signature	Known answer test using 2048 bit RSA digital signature	Power-up (Cryptographic Algorithm Self-Test)
Firmware Integrity Test	Firmware integrity test using 2048 bit RSA digital signature	Power-up (software/firmware integrity test)
Boot Loader Integrity Test	Boot Loader integrity test using CRC Check(32bit)	Power-up (software/firmware integrity test)
Hash_DRBG	Continuous random bit generator test	Conditional (Continuous random bit generator test)
NDRNG	Conduct Repetition Count Test and Adaptive Proportion Test based on SP800-90B. Conduct the same test upon Power-up.	Conditional and Power-up (Health test)
CSP Integrity Test	Secret information integrity test using CRC Check(32 bit)	Conditional (critical functions test)
Firmware Load Test	Firmware verification with 2048 bit RSA digital signature when loading firmware	Conditional (Software/Firmware Load Test)

11.1 Power-up Self-test

When the power is turned on, the Canon MFP Security Chip performs power-up self-test automatically. It performs the firmware integrity tests, Algorithm known answer tests and NDRNG health test shown in Table 12 as the power-up self-test.

In case the result of the firmware integrity tests, Algorithm known answer tests and NDRNG health test is an error, the Canon MFP Security Chip transitions to an error state immediately, and after that, no data can be written to, or read from, the storage device(s). Status of the error state can be obtained by Show status service. In order to recover from an error state, it is necessary to contact the vendor to repair the cryptographic module.
On-demand power-up self-test can be performed by resetting the Canon MFP Security Chip.

11.2 Conditional Self-test

The Canon MFP Security Chip provides the test for Hash_DRBG continuous random bit

generator test, NDRNG health test, test for critical functions, and test for firmware loading as the conditional self-test shown in Table 12.
Hash_DRBG continuous random bit generator test is conducted every time before using the Hash_DRBG pseudo-random number generator.
NDRNG health test is conducted when performing seed generation.
The Canon MFP Security Chip also provides a management function of secret information as a critical function. It implements CSP Integrity Test shown in Table 12 as critical functions test. In CSP Integrity Test, each time secret information stored in the flash memory is read, the integrity of the secret information is confirmed by using 32 bit CRC.
The Canon MFP Security Chip has the update firmware function and the firmware load test shown in Table 12 is performed when updating the firmware.

In case the result of the conditional self-test is an error, the Canon MFP Security Chip immediately transitions to an error state, and after that, no data can be written to, or read from, the storage device(s). The status of the error state can be obtained by using Show status service. In order to recover from an error state, it is necessary to contact the vender to repair the Canon MFP Security Chip.
In case the transition to the error state is made as a result of the conditional self-test, it is possible to recover from an error state by transitioning to non-FIPS140-2 approved mode using Change mode service. If the Firmware load test fails, the Canon MFP Security Chip will terminate the firmware update and continue to work with the existing firmware.
No bypass test is implemented because the Canon MFP Security Chip does not have a bypass function.

12 Design Assurance

12.1 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 first runs "Transition to Approved mode" service in non-FIPS140-2 approved mode, and the Canon MFP Security Chip transitions to FIPS140-2 approved mode after conducting Self-test. Then, 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, the CO should set both CO authentication information and authentication ID at the same time. The CO authentication information should be a 32 byte value that cannot easily be guessed and the authentication ID should also be a 32 byte value that cannot easily be guessed.
> Upon receiving a request for this service, the Canon MFP Security Chip writes the authentication ID and CO authentication information to flash memory, and generates the key seed for AES cryptographic key generation. The Canon MFP Security Chip specifies the key size by the [INSTALL SECRET INFO] extended ATA command in the “Configure secret information” service. Show status service can be used to determine the current operating mode. In response, the operator receives status information from the Canon MFP Security Chip indicating whether it is on FIPS140-2 approved mode or non-FIPS140-2 approved mode.

The administrator 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 administrator shall inspect the coating for any signs of tampering. If the administrator discovers tamper evidence, the Canon MFP Security Chip should not be used.

12.2 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 cryptographic module to transition to non-FIPS140-2 approved mode. The Canon MFP Security Chip zeroizes the Vendor Public Key used so far, after the firmware update has been completed successfully.

12.3 Guidance Documents

Provide the following private document as Crypto officer guidance and User guidance.

- Canon MFP Security Chip Firmware specification

13 Mitigation of Other Attacks

The Canon MFP Security Chip does not implement functions to mitigate the impact of other types of attacks.

END